MOBILE INNOVATION – FROM PREDICTIONS TO REALITY

Deloitte Digital Series Conference

31 January 2017

Deloitte. Digital

This presentation is incomplete without the accompanying discussion

SECURITY FOR MOBILE APPLICATIONS: WHERE DO WE STAND?

A brief overview of threats, vulnerabilities and key recommendations

Maxime Verac, Senior Manager, Deloitte Luxembourg

AGENDA

- Brief overview of the threats specific to mobile devices and applications
- Main vulnerabilities observed in practice
- What can you do when you manage the devices (to protect internal apps)?
- What can you do for unmanaged devices (to protect customer-facing apps)?

Thank you for being part of a passive and non-intrusive demo (otherwise please disable your Wi-Fi now)

SPECIFIC THREATS

1 Who is using the device?

Theft, loss or even device sharing should be considered in the threat model

2 Malware

Mobile malware are on the rise (year after year), with multiple motives (e.g. ad traffic, mobile ransomware, theft of personal data or credentials)

3 Traffic interception

So called man-in-the-middle attacks mostly target Wi-Fi connectivity; they are easy to set-up and generally successful due lack of user awareness

4 Complex patch management

Operating System fragmentation (particularly on Android) and lack of users' willingness to update their devices lead to many vulnerable devices

5 Phishing and SMiShing

Users are less likely to detect phishing attacks on mobile devices and may also become victims of SMiShing

MAIN VULNERABILITIES OBSERVED IN PRACTICE

Vulnerability	Most affected threat scenario
Weak server authentication "Pinning" of cryptographic certificate authenticating the servers is not or not properly implemented	**Man-in-the-middle attack** Such applications will be vulnerable to man-in-the-middle attacks if the users connect to rogue Wi-Fi hotspots
Insufficient data protection Screenshot blurring and third party keyboards prevention are not systematically enforced	**Malware** Many malware are disguised as legitimate third party keyboards which in reality leak information
Risky execution environment Jailbreaking and rooting detection are often missing and the execution environment is rarely assessed for risks	**Patching complexity & malware** Many applications run on vulnerable operating systems without any means to detect and act upon it

KEY CONTROLS FOR MANAGED DEVICES

1 Specific awareness

Users need to be aware of specific threats targeting mobile devices (e.g. traffic interception, phishing, malware, etc.)

2 Operating system vulnerability management

Only allow supported version of operating systems and ensure security updates are applied within reasonable timeframe

3 Monitoring of execution environment

In addition of the sandboxing controls often implemented, rely on your Enterprise Mobility Management (or MDM) platform to ensure the environment is secured: detection of root/jailbreak, monitoring of suspicious applications (with dynamic blacklisting), monitoring of suspicious networks, etc.

KEY CONTROLS AT APPLICATION LEVEL

1 Specific awareness

Users and developers need to be aware of specific threats targeting mobile users (e.g. traffic interception, phishing, malware, etc.). Include security awareness messages in customer facing applications

2 Security must be integrated in the development lifecycle (SDLC)

In particular, a risk assessment should be performed before developing mobile applications and at least risks from the OWASP Mobile Top 10 should be considered

3 Monitoring of execution environment

Integrate controls within your application to ensure the mobile device executing the application can be trusted (detection of root/jailbreak, monitoring of suspicious applications). Ensure strong server authentication is enforced at application level (i.e. certificate pinning)

Deloitte.
Digital