Protecting Your Data on Mobile Devices

Mario de Boer
GARTNER

Session ID: DAS-106
Session Classification: Intermediate

RSA CONFERENCE EUROPE 2012

Some Have a Grim View on Security

Agenda

- What's really new about risks for mobile devices?
- What controls cannot be missed on your list of requirements?
- How do data protection architectures compare?
- Why and when would you improve on existing platform security controls?
- How do current container solutions help in protecting your data?

What's really new about risks for mobile devices?

Threat Agents

Malware

Threat Type: Logical

Coexists with user

Examples:

- Redsn0w Jailbreak
- FoncyDropper
- ZitMo

Thief

Threat Type: Physical

Exclusive access

Example:

- Plenty in the room

Evil Maid

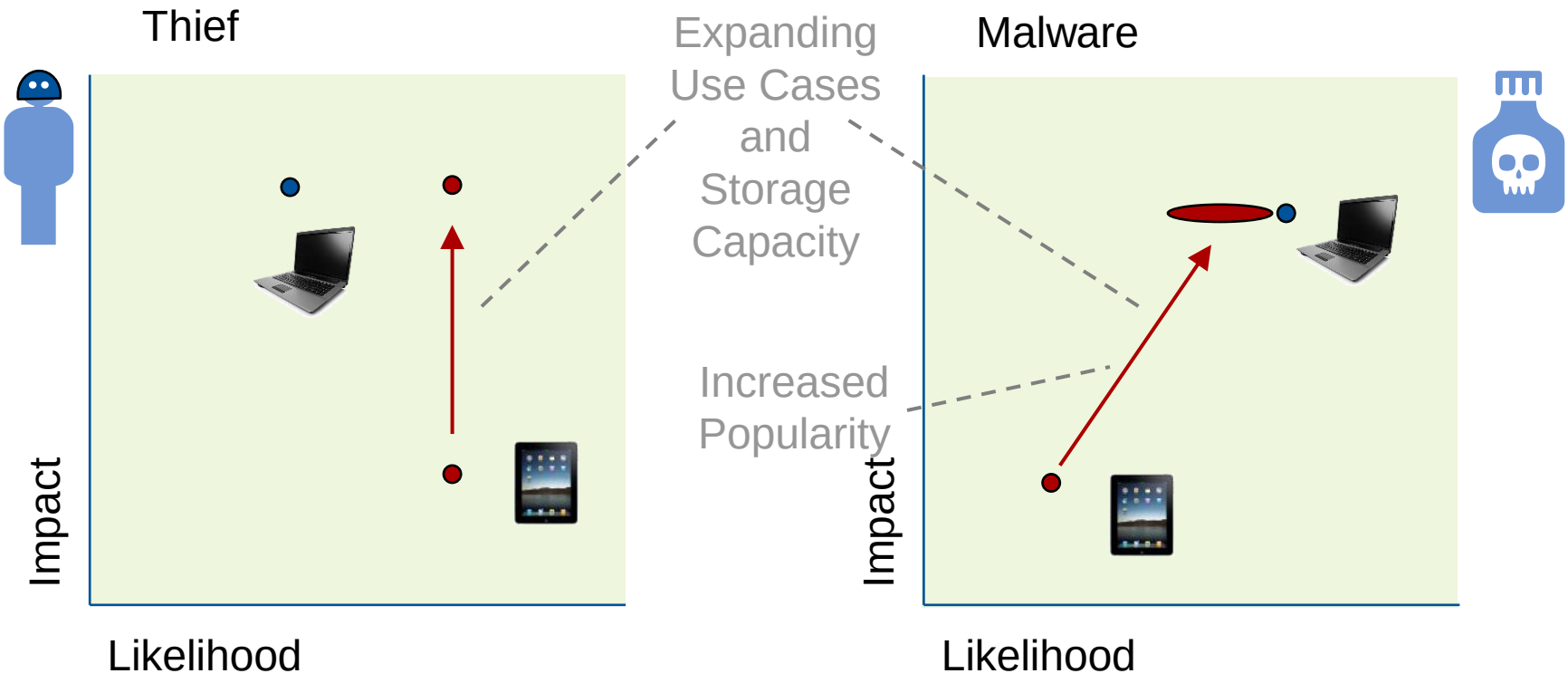
Threat Type: Physical

Coexists with user

Examples:

- Stealing a file system

Old Risks, in New Context



It is only a matter of time before the first large data breach concerning a mobile device receives media attention

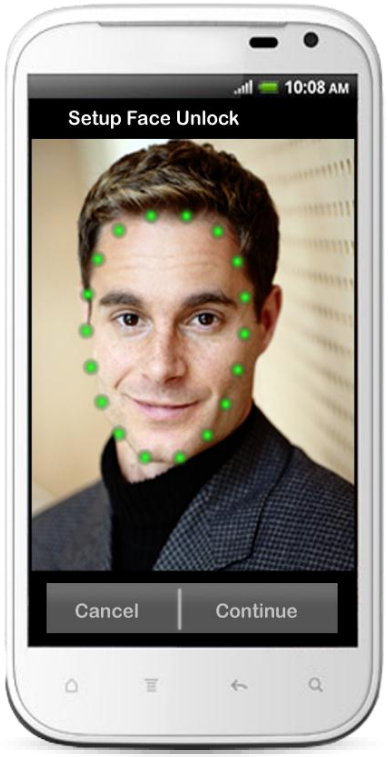
What controls cannot be missed on your list of requirements?

Access Control

- Aims to reduce the risk of **Thieves** and **Evil Maids** by preventing logical access to device

- Consider:
  - Methods: PIN, password, swipe, face unlock, hardware token, other biometrics

  - Policies to enforce: Password policies on complexity/history/delay, inactivity timer
  - Risks of keyloggers and other spyware
  - Limitations facing laboratory attacks that circumvent authentication



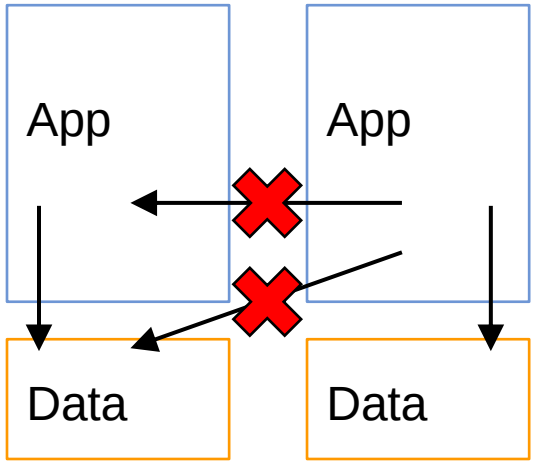
Encryption

- Aims to reduce the risk of **Thieves** and **Evil Maids** by preventing logical access to extracted information

- Consider:
  - Encryption and keys in hardware or software?
  - Keys derived from device and/or passcode?
  - What information is encrypted?
  - Cache management
  - Known weaknesses and third party validations

Application Controls

- Aim to reduce the risk of **Malware** and **Evil Maids** by preventing direct logical access to applications and their data



- Consider:
  - Application and data isolation
  - Signatures
  - Key management and encryption APIs
  - Management hooks
  - Application store controls
  - Kill switch: Remotely kill an application on all devices

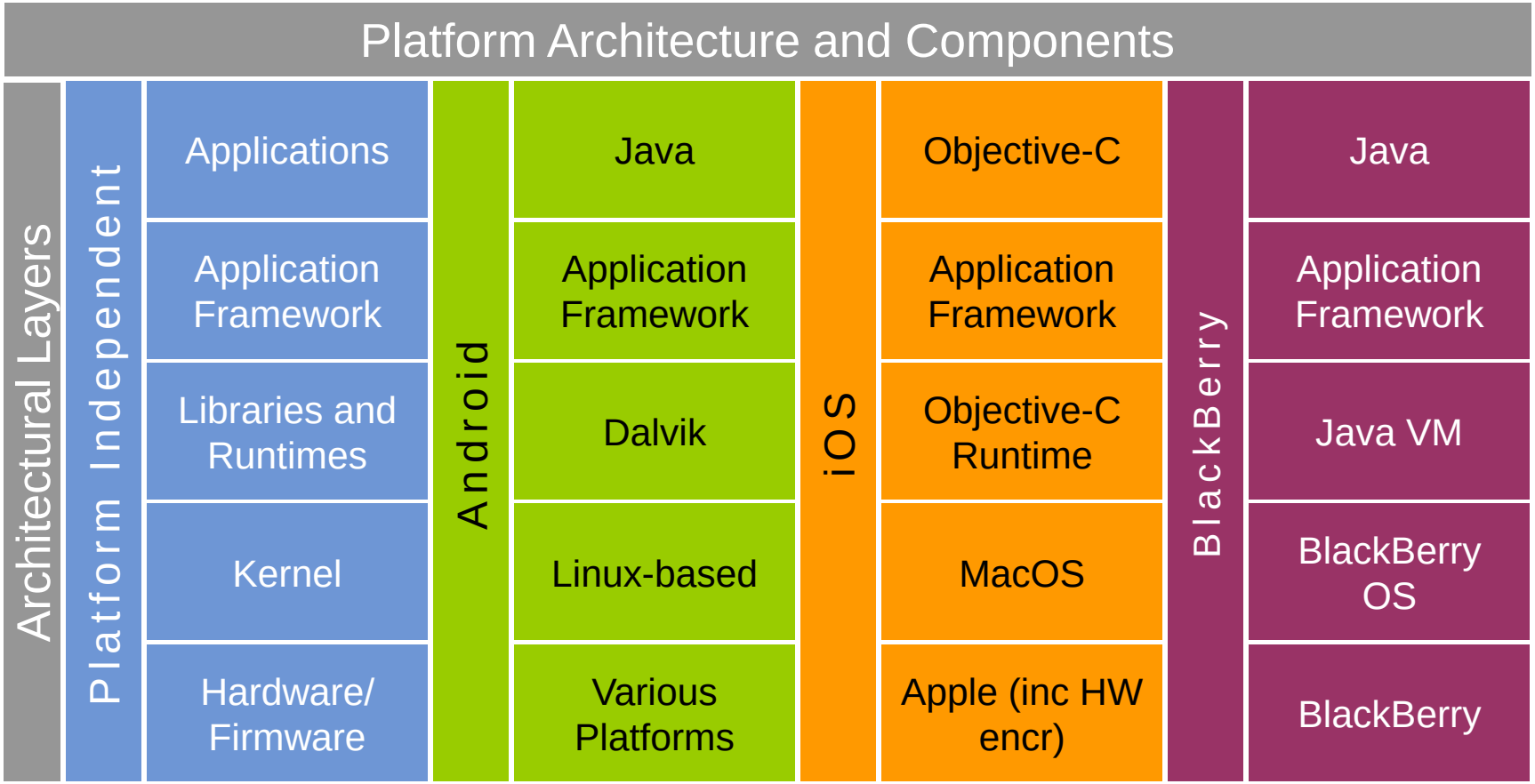
Remote and Local Wipe

- Aims to reduce the risk of **Thieves** by remotely or locally wiping applications and data

- Consider:
  - Full vs. partial wipe
  - Local vs. remote wipe
  - What information is wiped?
  - The wiping method
  - How to confirm completion?

How do data protection architectures compare?

Platform Architecture



Android Security

- **User** controls the security
- Key elements:
  - Linux process and file isolation
  - Permissions based
- Concerns:
  - Fragmentation of the platform over OEMs
  - Encryption support dependent on OEM
  - Content providers accessible by default
  - Open source components and uncurated appstores may lead to malware
  - Permissions rely on people's judgment

iOS Security

- **Apple** controls the security

- Key elements:
  - Curated Appstore
  - Sandboxing
  - Hardware encryption, always on
  - OTA updates

- Concerns:
  - Vulnerabilities in OS that lead to jailbreak
  - Few mechanisms that limit the access of an app
  - Data protection not used by all applications and not validated

BlackBerry Security

- **Administrator** controls the security

- Key elements:
  - Best in class mobile management and security
  - Data protection capabilities
  - No jailbreaks for BB smartphones

- Concerns:
  - AppWorld is vetted but its use not mandated, leading to potential for malware
  - Apps may have extensive access, without jailbreak
  - Management is key, e.g., encryption is optional

Why and when would you improve on existing platform security controls?

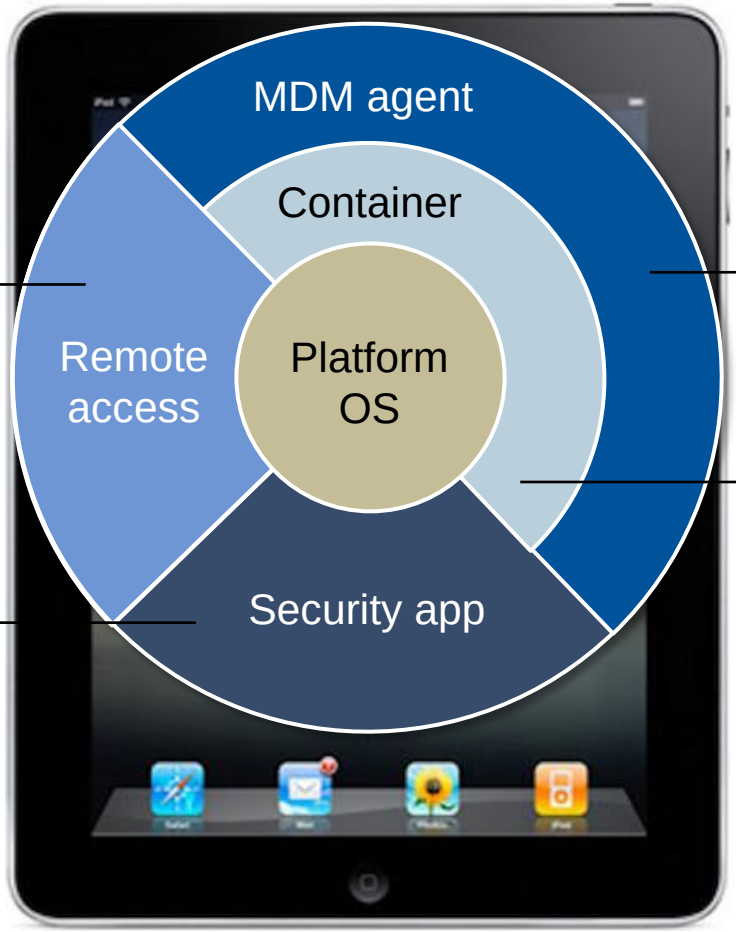
When More Is Required

- Consider additional controls if any of the following applies:
  - If required controls are immature or inconsistent
  - If required controls are missing
  - If your threat landscape includes actors other than ad hoc thieves

- Consider relying on pure platform controls if each of the following apply:
  - You use modern, up-to-date, platforms
  - Access control, encryption and wipe is configured per best practices
  - Application controls are used to protect integrity and thwart malware
  - Applications used for business are securely developed
  - Your threat actors do not include laboratory attacks or the information is not highly sensitive

Solution Approaches for Protecting Data

Provide Remote Access to Business Applications and Information



Centrally Manage Security Settings Across Mobile Devices

Use Client Applications That Implement Specific Security Functions on the Device

Use Client Applications That Include Security Controls Independent of Platform

How do current container solutions help in protecting your data?

Managed Containers

- Separation of information and applications, providing
  - Access control
  - Encryption
  - Wipe
  - Isolation
  - Secure connections
  - Central management (policies and content)

- Container controls: **unified** across platforms, **granular** and **stronger** than platform controls

Containers: Strengths and Weaknesses

Strengths

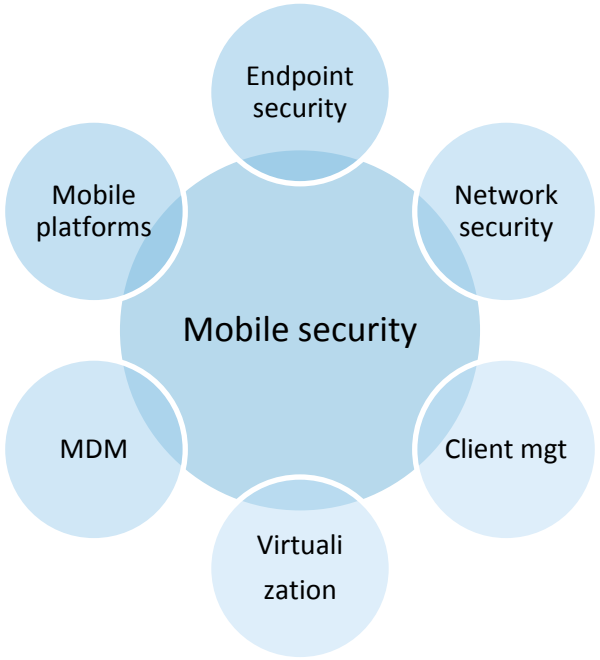
- Fill gaps in platform security
- Additional layer of defense
- Uniformity across platforms
- Isolation of business data and apps (BYO)

Weaknesses

- Market is in flux
- Lack of surety
- Cost
- Scalability wrt applications
- User experience
- Use cases only partially covered
- Variations in technology

Ready for the Future?

- Market flux in MDM and container market
- Mobile platform evolution
- SAAS management platforms
- BYOC beyond BYOD
- Solutions to completer use cases
- No short term data-level protection and client virtualization solutions



Action Plan and Recommendations

How to Apply What You Have Learned Today

- Upon your return
  - Review your mobile security strategy for data protection
  - Review your existing security policies for mobility aspects
- Next 90 days
  - Formulate data protection requirements for mobile devices
  - Architect solutions with an optimal balance of mobile platform controls, application controls, remote access and user experience
- Next 12 months
  - Track managed container market and device platform evolutions
  - Revisit architecture

Recommendations

- ✓ Understand the risks and the threats you are trying to protect against and accept that some risks cannot be mitigated
- ✓ Manage handheld diversity depending on security features
- ✓ Do not invest in any fancy additional controls, unless they implement missing platform requirements and you understand their added value
- ✓ Make sure that the apps (and libs) you use for your business data are secure