Creating Security for BYOD
Current Approaches

Patrik Ekdahl
Ericsson Research - Security
Bring Your Own Device

“BYOD refers to the act of employees using their personal mobile devices for work-related purposes.”

- Mason report 2012

Drivers

- Consumerisation
  - IT departments are too slow to adopt.

- Personalisation
  - need for employees to feel unique.

- Work-life integration
  - traditional workday no longer exists.
  - drive for more flexible technology solutions.

- Productivity enhancement
  - using familiar technologies
  - increased availability

- Cost
History

- 2000: Blackberry 957
- 2007: iPhone
- 2008: HTC Dream
- 2010: Several larger companies implement BYOD policies
- 2012: NIST draft on guidelines for BYOD security.
Corporate access

Blackberry style

Internet

VPN

Corporation network

BES

Mail Server

Internet Gateway

Internal Data
Corporate access

Blackberry style

Internet

VPN

WiFi-Browser

Corp. network

BES

Mail Server

Internet Gateway

Internal Data
Corporate access

Mobile Device Management style

MDM Application

Mail
Calendar

Prop. Data Access

TLS

Corp. network

MDM Frontend

Internal Data
Exchange Server

Ericsson External
Today’s landscape

IT’s support of BYOD
(All devices, US SMEs)

Don’t know
4%

Yes
45%

No
51%

Reality
In more than 90 % of the companies, people bring their own SmartPhone.

Source: iGillottResearch 2013
Some more numbers..

(from a UniSys survey 2012)

72% of IT executives surveyed say that employees are using unsupported devices or apps because of personal preference, not because they need them to do critical work.
Some more numbers..

(from a UniSys survey 2012)

72% of IT executives surveyed say that employees are using unsupported devices or apps because of personal preference, not because they need them to do critical work.

but what does IT know..? According to another survey..

IT more likely to block Angry Birds than to provide secured alternatives to public cloud storage.
72% of IT executives surveyed say that employees are using unsupported devices or apps because of personal preference, not because they need them to do critical work.

but what does IT know..? According to another survey..

IT more likely to block Angry Birds than to provide secured alternatives to public cloud storage.

75% of IT organizations don't let people use their own apps for work purposes, with a substantial subset saying such usage should be grounds for dismissal.
Some more numbers..

(from a UniSys survey 2012)

72% of IT executives surveyed say that employees are using unsupported devices or apps because of personal preference, not because they need them to do critical work.

but what does IT know..? According to another survey..

IT more likely to block Angry Birds than to provide secured alternatives to public cloud storage.

75% of IT organizations don't let people use their own apps for work purposes, with a substantial subset saying such usage should be grounds for dismissal.

38% percent of the employees decided to ignore such edicts. These people are the ones who drive the business and tend to be in positions of authority.
Device owner

• Execute any apps they like.
• Trust that data will not be viewed/erased by enterprise actions.
• Detach from an enterprise without losing personal data.

Information owners

• Trust the device to
  • protect data
  • access data
  • process data
  • store data
• Terminate access to their data at any time
Device architecture

Application Contexts
- APP-1
- APP-2
- APP-3
- APP-4
- APP-5

OS Context
- Kernel

Firmware Context
- Bootloader, Initialization Code

Hardware Context
- Application Processor, Baseband Processor, Memories, Peripherals, ROM Code
Information Domains

- Application Contexts
  - APP-1
  - APP-2
  - APP-3
  - APP-4
  - APP-5

- OS Context
  - Kernel

- Firmware Context
  - Bootloader, Initialization Code

- Hardware Context
  - Application Processor, Baseband Processor, Memories, Peripherals, ROM Code
Information Domains

- **Hardware Context**: Application Processor, Baseband Processor, Memories, Peripherals, ROM Code
- **Firmware Context**: Bootloader, Initialization Code
- **OS Context**: Kernel
- **Application Contexts**: APP-1, APP-2, APP-3, APP-4, APP-5
- **Information Contexts**: IO-1, IO-2, IO-3, IO-4, IO-5
Data access
Data access

Information Contexts

IO-1

Application Contexts

APP-1

IO-2

APP-2

IO-3

APP-3

IO-4

APP-4

IO-5

APP-5
Data access

Policies
and a Policy Enforcement Engine (PEnE)
Sealing the information

Rich OS

APP-1  APP-2  APP-3

IO-1  IO-2  IO-3

Rich Environment  Trusted Environment

Policy Enf. Engine
Sealing the information

Rich Environment

Trusted Environment

Rich OS

Policy Enf. Engine

APP-1
APP-2
APP-3
IO-1
IO-2
IO-3
Measuring

APP-1 | APP-2 | APP-3

Rich OS

Rich Environment

Policy Enf. Engine

IO-1 | IO-2 | IO-3

Trusted Environment
Measuring

APP-1  APP-2  APP-3

IO-1  IO-2  IO-3

Rich OS

Policy Enf. Engine

Rich Environment  Trusted Environment
Check point

APP-1  |  APP-2  |  APP-3  

Rich OS

Rich Environment

IO-1  |  IO-2  |  IO-3  

Policy Enf. Engine

Trusted Environment

Wednesday, April 17, 13
Rich Environment

- Execute any apps they like.
- Trust that data will not be viewed/erased by enterprise actions.
- Detach from an enterprise without loosing personal data.

Trusted Environment

- Trust the device to protect data
- Access data
- Process data
- Store data
- Terminate access to their data at any time
Trusted Applications

Rich OS

APP-1
APP-2
APP-3

Trusted Kernel (with PEnE)

TA-1
TA-2
TA-3

Secure Storage

Rich Environment

Trusted Environment
Anchoring

- Roots of trust
- Execution
- Storage
- Verification
- Reporting
- Measurement
- Isolation from Rich OS
- Narrow well-defined API

Trusted Environment
Management

Trusted Kernel (with PEnE)
Secure Storage

Trusted Environment
Corporate Server

- Install / uninstall
- Key provisioning
- State enquiring

Rich OS

APP-1  APP-2  APP-3

TA-1  TA-2  TA-3

Trusted Kernel (with PEnE)

Secure Storage

Rich Environment

Trusted Environment
Management

Corporate Server

Administration data packages

• Install / uninstall
• Key provisioning
• State enquiring

Rich OS

• TLS connection
• Data fetch
• State reporting

APP-1  APP-2  APP-3

TA-1  TA-2  TA-3

Trusted Kernel (with PEnE)

Secure Storage

Rich Environment

Trusted Environment

Wednesday, April 17, 13
Check point

Rich OS

Rich Environment

Trusted Kernel (with PEnE)

Secure Storage

Trusted Environment
Execute any apps they like.
Trust that data will not be viewed/erased by enterprise actions.
Detach from an enterprise without loosing personal data.

Trust the device to
- protect data
- access data
- process data
- store data
- Terminate access to their data at any time
Standardization efforts
Conclusions

Using a Trusted Execution Environment we can build a owner-controlled BYOD solution with hardware anchored trust.

- Non-proprietary solution exists
- Multiple stakeholders
- Device Owner is in control
- No need for BES
- Hardware anchored separation
  - Information
  - Execution
- Remote administration