Mobile Security
14-829 – Fall 2013

Patrick Tague

Class #23 – BYOD

Carnegie Mellon University
Silicon Valley

Bring Your Own Device

- BYOD is the broad idea of supporting personal computing devices in enterprise scenarios
  - Not just smartphones; this has been happening for decades, smartphones just enhance the problem
- Primary security concerns:
  - Conducting company business on personal devices
  - Carrying user traffic through corporate intranet
  - Manageability of non-manageable devices...

Why Support BYOD?

- More personal devices →
  - Fewer corporate devices
  - Fewer IT services employees
- Access to corporate data on personal phones →
  - More productive employees

Everyone has a different idea of what the big issues are with BYOD, so let's look at a few.

BYOD Challenges

According to [Trend Micro, 2011]

- Management of user-liable devices
- Exposure of stored corporate data
- Leakage of corporate data via apps
- Introduction of malware / bad data

User Device Management

- Management of user-liable devices provides:
  - Richer user experience around corporate actions → happier employees → higher productivity
  - Control of device actions → reduced exposure to security risks

Corporate Data Storage

- Protection against data exposure to unauthorized third parties:
  - Data recovered from lost/stolen mobile devices
  - Fines due to data breaches
  - Loss of reputation

Application Data Leakage

- Since the device is used for personal apps and corporate apps:
  - Corporate data transferred off device no longer belongs to the company
  - Corporate data can easily leak through personal app channels (e.g., email, SMS, etc.)

Malware

- Personal devices can transport malicious code or data into the corporate network
  - Possibly affecting internal operations
  - Possibly transiting to other devices / data
  - …

Solution Requirements

According to [ZK Research, 2012]

- In managing user devices, a network-based solution is more manageable than an endpoint solution (IT owns the network)
- Requirements:
  - Unified connectivity policies for wired / wireless
  - Integrated network and data security
  - Vendor-agnostic solutions, integrated into existing IT
  - High availability and reliability
  - Robust unified communications
  - Broad range of managed services

Deeper BYOD Security Model

~[Traver, Hsu, Schlau, Knox; 2012]

- The team created a BYOD solution evaluation plan including:
  - Treatment of corporate data
  - Device management policy
  - Device infrastructure requirements
  - Personnel requirements
  - Organizational infrastructure requirements

Corporate Data Treatment

- Corporate data should never be stored on personal devices, nor transferred to others
- Corporate data should not be processed on personal devices
- Data access should be restricted using appropriate access control mechanisms
- Data access should be logged including the user and process / app that accesses it

Personal Device Policies

- A successful BYOD deployment should force:
  - Full device encryption
  - Anti-virus/malware detection / prevention
  - Password policy, including length/complexity/etc.
  - Timely software / OS updates
  - Application restrictions in the corporate environment

Device Infrastructure

- Devices in a BYOD deployment should:
  - Transmit data only when encrypted and authentic
  - Have their network behaviors/interactions logged
  - Have connections managed/controlled on a per-user or per-device basis
  - Be properly enrolled / dis-enrolled by IT
  - Obey graceful exit (both end of day and position)
  - Prevent unauthorized transit of data into the network
  - Seamlessly swap between mobile and laptop

Personnel Requirements

- Users should be properly trained on how they can/should use their devices
- There should be a BYOD support infrastructure and/or staff
- Users' sensitive information should be restricted from BYOD management (except for emergencies, forensic cases, etc.)
- Disaster reporting/resolution system should be in place (e.g., lock phone when lost, allow restricted use when servers go down, etc.)

Organization Infrastructure

- Applications should be properly vetted, then blacklisted / whitelisted
- Network should block unauthorized transit of mobile data into the network
- Allow devices to access the Internet (via WiFi)
- Allow access to corporate email (granted this is an accepted weak point in the security model)
- Possess and act in accordance with an end-user licensing agreement for managing organizational infrastructure and data

What tools are available for companies to use for BYOD management?

Component Tools

- Securing data and operations under BYOD involves active management of devices or isolation of sensitive activities and data

- Possible components:
  - Mobile device management (MDM)
  - Virtual desktop infrastructure (VDI)
  - Virtual private network (VPN)

MDM

- Mobile device management is all about policy
  - Enforce encryption
  - Disable sensors
  - Mandate password strength and usage
  - Control application usage based on context (no Angry Birds while at work)
  - Distribution / enforcement of configuration (use the secure WiFi)
  - Device provisioning
  - Lock / wipe features for lost/stolen devices
- Ex: MaaS360, AirWatch, Mobile Iron

VDI

- Virtual Device Infrastructure, essentially built around the idea of virtual desktop, keeps data and processing in corporate hands instead of on the device
  - Uses a remote connection to a virtual machine (virtual desktop agent) and software on the client device (virtual desktop client)
  - Personal device has no access to corporate data due to strong isolation
- Ex: Citrix VDI-in-a-Box, Citrix VDI XenDesktop, VMware vSphere Hypervisor, Microsoft HyperV

VPN

- Virtual Private Networking uses secure tunnels through the Internet or public network
  - Protection of data, software, config, etc. while in transport
  - No actual protection on the endpoints, just the tunnel

None of these tools meet all of the requirements of the security model...

No Single Solution

- None of these components solves all of the problems of BYOD
- Need a more comprehensive solution to provide everything organizations are looking for

- But, what are they looking for?
  - Some of the tools are vague about what they provide (e.g., “it should protect the company's data”)

- Need a better set of requirements or specifications (→ adversary model?)

How to determine if a device should be allowed into a corporate environment?

Solution Evaluation

According to [Intel IT, 2012]

- Framework for deciding whether a device / configuration is allowable to use in an enterprise scenario, based coarsely on:
  - Security
  - Manageability
  - Productivity
  - Performance
  - Ease of Use
- For each feature, 0 = not present/met, 1 = present and minimally supported, 2 = meets or exceeds best-in-class standards

Security Evaluation

- Features included in the security evaluation criteria:
  - Power-on password (i.e., access control)
  - Data encryption, w/ state reported via MDM API
  - Separation / isolation of data
  - Enterprise VPN
  - Secure credential storage / management
  - Endpoint intrusion/malware detection

Manageability Evaluation

- Features included in the manageability evaluation criteria:
  - Enterprise management / MDM capability
  - Device property discovery
  - OTA application installation, activation, etc.
  - Enforceable configuration
  - Seamless delivery of proprietary apps
  - Status reporting, auto-configuration
  - Backup and restore

Productivity Evaluation

- Features included in the productivity evaluation criteria:
  - Intelligent and timely updates
  - Blended social interface
  - Broadcast updates
  - Mature, up-to-date tools and apps
  - Quick / timely task management
  - Offline support

Performance Evaluation

- Features included in the performance evaluation criteria:
  - Sufficient battery life (> 2 days preferred)
  - Responsiveness, no lag, quick startup
  - Application multitasking w/o loss of state
  - Rich media, camera, HD video support + controls
  - Screen size sufficient for good UX
  - Access to multiple communications modes
  - Sufficient RAM and storage capacity

Ease-of-Use Evaluation

- Features included in the ease-of-use evaluation criteria:
  - Intuitive and easy to use UI
  - Easy updates to OS, firmware, apps
  - Fluid switching among task, app, social, web, etc.
  - Support for multiple/extendable input options

Question to consider:

Is BYOD a generally solvable issue, or are we destined to settle for the "least unreasonable" solution?

Nov 18:
Exam