ENTERPRISE SECURITY IN iOS
Lecture 20b

COMPSCI 702
Security for Smart-Devices

Nalin Asanka Gamagedara Arachchilage

Slides from Muhammad **Rizwan** Asghar

April 28, 2021

APPLE BUSINESS

- Apple's iOS-based devices have gained popularity among consumers
  - "Apple devices are easiest to manage in the enterprise"

- More enterprises have started allowing employees to access and store enterprise data on these devices

ENTERPRISE CONCERNS

- Enterprises have to manage devices that may be used to access or store the sensitive enterprise data
  - Enterprise owned devices
  - Bring Your Own Device (BYOD)
- This introduces the new security risks, e.g.,
  - Misplaced devices
  - Lost devices
  - Stolen devices
- Basically, the sensitive enterprise data could be at risk

ENTERPRISE NEEDS

- Control over devices by a number of ways
  - Configuring devices (e.g., auto-lock)
  - Managing data and app restrictions (e.g., no access to camera)
  - Applying rules
    - Strong passcode (8 characters)
    - Remote wipe (after 10 tries)
- Avoiding issues in case of BYOD
  - Users can do unsafe things – say, installing/updating third party apps

NAÏVE APPROACH

- IT admins can do configurations manually
- Unfortunately, there are issues with a manual configuration
  - It is labour-intensive and
  - Error-prone
- Do we have a better solution?

iOS CONFIGURATION MANAGEMENT

- iOS-based devices are managed through the creation and installation of configuration profiles
- These profiles contain settings configured by an administrator for installation on a user's device
- Configuration profiles are centrally managed using
  - Apple's iPhone Configuration Utility (a free utility)
  - Mobile Device Management (MDM) System

iPHONE CONFIGURATION UTILITY

- A graphical utility for iPhone configuration
  - It lets administrators create and manage configuration profiles
- These profiles can be installed onto iOS devices
  - Over a USB connection
  - By sending via email or
  - By hosting them on a web server
- Issue: not scalable
  - It only manages a limited number of devices

MDM SYSTEMS

- Used to manage a large number of devices
- Apple offers an MDM system in Lion Server through the Profile Manager service
- This service works well for
  - Workgroups and
  - Small and Medium-sized Enterprises (SMEs)
- For large organisations, a commercial third party MDM solution would likely work best

CONFIGURATION PROFILES

- An XML property list file
  - Known as plist
- Values stored in Base64
- The plist data may optionally be signed and encrypted
  - RFC 3852 – Cryptographic Message Syntax (CMS)
  - If sensitive information (e.g., a password) has to be sent over a network then it should be encrypted

PROFILE METADATA

- The configuration profile metadata includes
  - The human-readable name
  - Description of the profile
  - Creating organisation
  - Some other fields

- The configuration payloads are the most important portions of the profile

SOME CONFIGURATION PROFILE PAYLOAD TYPES

Payload	Description
Removal Password	Password to remove locked profiles from the device
Passcode Policy	Defines whether a passcode is required to unlock the device and how complex this passcode must be
E-mail	Configures the user's email account
Restrictions	Restricts the user from performing certain actions – e.g., using the camera
Calendar Subscription	Subscribes the user to a shared calendar
VPN	Specifies a Virtual Private Network (VPN) configuration
WiFi	Configures the device to use the specified 802.11 network

CONFIGURATION PAYLOADS

- Removal password
  - The password needed to turn off the configuration profile
  - Configurations can also be set with “Never remove” – have to clear the device to get rid of it
- Passcode policy
  - It specifies how complex a passcode should be
  - If there is no existing passcode or the existing one is not complex enough then the user is asked to set a new passcode

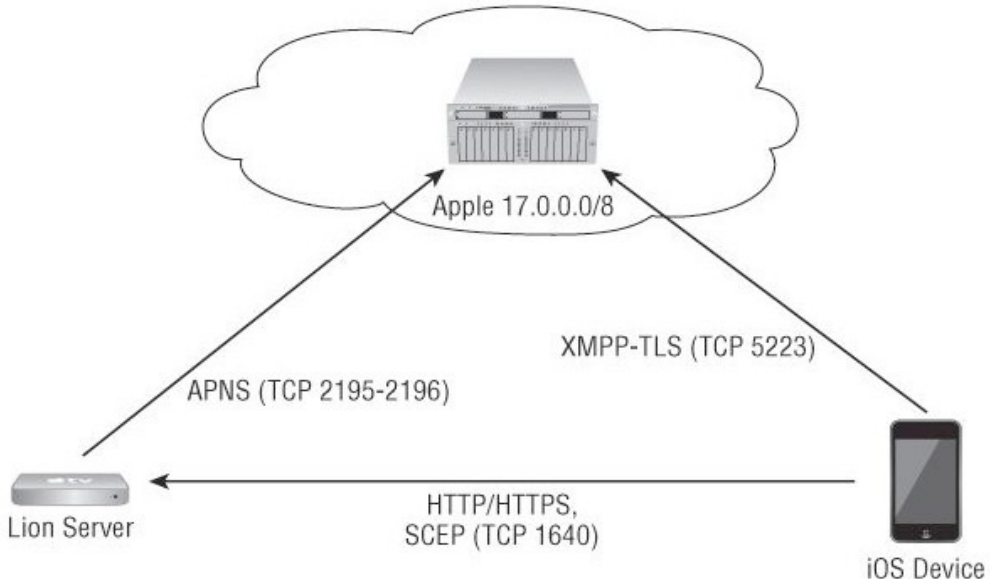
PASSCODE POLICY

Source: "iOS Hacker's Handbook"

DISTRIBUTING THE PROFILES USING THE iPHONE CONFIGURATION UTILITY

- Puts a root Certificate Authority (CA) in the keychain
- Each device connected over USB has its certificate created
  - This certificate is used to encrypt configuration profiles
- It can also use email or the web to send profiles

DISTRIBUTING VIA MDM



- 3 components
  - iOS device
  - Organisation's MDM server
  - Apple's Push Notification Service (APNS)

Source: "iOS Hacker's Handbook"

HOW MDM WORKS

- A pub-sub model is used in this case
- The MDM server tells the APNS to publish a notification (on a particular topic)
- Devices inform the APNS which topics they are subscribing to
- The notification is sent to the subscribed devices
- The device then establishes a connection to the MDM server over HTTPS
- A remote wipe command can be initiated by MDM, Exchange or iCloud

ENTERPRISE APPS

- An enterprise provisioning profile can be loaded along with the configuration profile
  - Then, the in-house enterprise apps can be distributed Over The Air (OTA) or through MDM
  - Enterprise provisioning profiles have to be renewed annually

THE KILL SWITCH & HARDWARE MODIFICATIONS

- The kill switch worries some companies
  - What if Apple wants to shut our apps down?

- Some companies do not trust software restrictions
  - Instead of relying on configuration profiles (say to turn cameras or WiFi off) companies can purchase special hardware (say iPads without cameras or WiFi)

SUMMARY

- Enterprises need to have control over devices which connect to their systems
- IT admins can do configurations manually, but it is labour-intensive and error-prone
- Configuration profiles can be installed automatically on devices to enforce policies and manage restrictions
- These can be distributed and centrally managed through the Configuration Utility or MDM systems

RESOURCES

- **White Paper on iOS Security**
  https://www.apple.com/business/docs/iOS_Security_Guide.pdf

- **iOS Hacker's Handbook**
  Charlie Miller, Dionysus Blazarkis, Dino Dai Zovi, Stefan Esser,Vincenzo Iozzo, Ralf-Philipp Weinmann
  John Wiley & Sons, Inc., 2012

- **Apple Device Management**
  https://www.apple.com/ipad/business/it/#management

ACKNOWLEDGEMENT

- Some slides are based on the presentation shared by Robert Sheehan, thanks to him!

Questions?

Thanks for your attention!