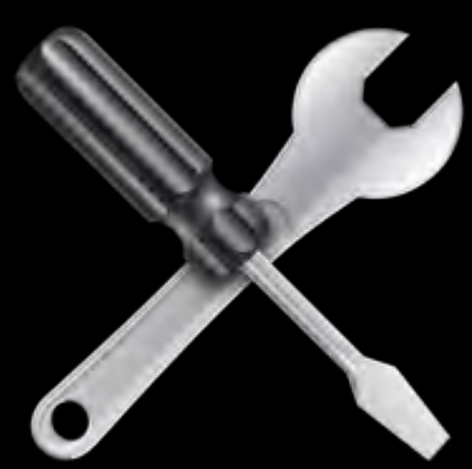
# World 2011

# Managing iOS Devices



**Andrew Wellington**
Division of Information
The Australian National University

AUC

XWII

# About Me

- Mac OS X Systems Administrator
- Division of Information (Central IT)
- Mostly manage servers (about 50 servers)
  - File services
  - Lab management
  - Lecture recording
  - Collaboration (Wiki)
  - Miscellaneous other services

AUC

XWIKI

# Overview

- What is the problem
- What can we do about it
- What should we do about it
- What tools can help us solve the problem

# State of Mobile Devices

- Many universities have previously been managing Blackberry or Windows Mobile style devices
- Most have explosive growth in iOS devices for both staff and students
- Significant numbers of iOS devices are personally owned
- Want to be able to manage some aspects of device without onerous restrictions on user

# What are we concerned about

## Data Security

- iOS sandboxes data between apps
- Potentially sensitive data can still be shared in various ways
  - Screenshot of application
  - Saving information to photo roll, address book or other iOS services
  - App supports saving to external services (eg, Dropbox)
- iTunes device backups can be encrypted

# What are we concerned about

## Network Security

- iOS devices can be connected to a variety of network environments
  - Trusted WiFi (University, secured home network)
  - Untrusted WiFi (hotels, McDonald's, etc)
  - Carrier 3G, EDGE or GPRS network
  - Virtual Private Networks (VPN)
- Can move between networks while operation is in progress
- Each service may have different requirements for security

# What are we concerned about

## Device Loss or Theft

- Highly portable devices lead to significantly increased risk of theft or loss
- Possible countermeasures:
  - Encrypt contents of device
  - Require passcode for access to device
  - Able to perform remote wipe
- Backups of the data on the device

# Management Methods

- A number of methods can be used for iOS management
  - End-User Self Managed
  - Enterprise Configuration Profile Administered
  - Mobile Device Management (MDM) Administered

# Management Methods

## End-User Self-Managed

- The user or support staff manually configure the device

| Advantages | Disadvantages |
|---|---|
| •End user choice and customisation<br>•Opt-in use of each service<br>•Limited IT overheads for initial deployment<br>•Well suited to personally owned devices with few services | •No way to enforce security policies<br>•Complex configuration for some services<br>•Variation in end-user skills and knowledge<br>•Increased support complexity through variations in configuration |

# Management Methods

## Enterprise Configuration Profile Managed

- Configured once with a “Configuration Profile”

| Advantages | Disadvantages |
| --- | --- |
| • Automatic device configuration<br>• Security and device policy enforcement<br>• Extra settings and policies not in the GUI<br>• Tighter security and policy compliance<br>• Less effort for initial configuration of each device<br>• Ability to remote wipe device with Exchange ActiveSync if you auto-configure an Exchange account | • Requires manual installation on each device<br>• Password based accounts still require password entry on first use<br>• Difficult to change configuration after initial deployment |

# Management Methods

## Mobile Device Management (MDM) Administered

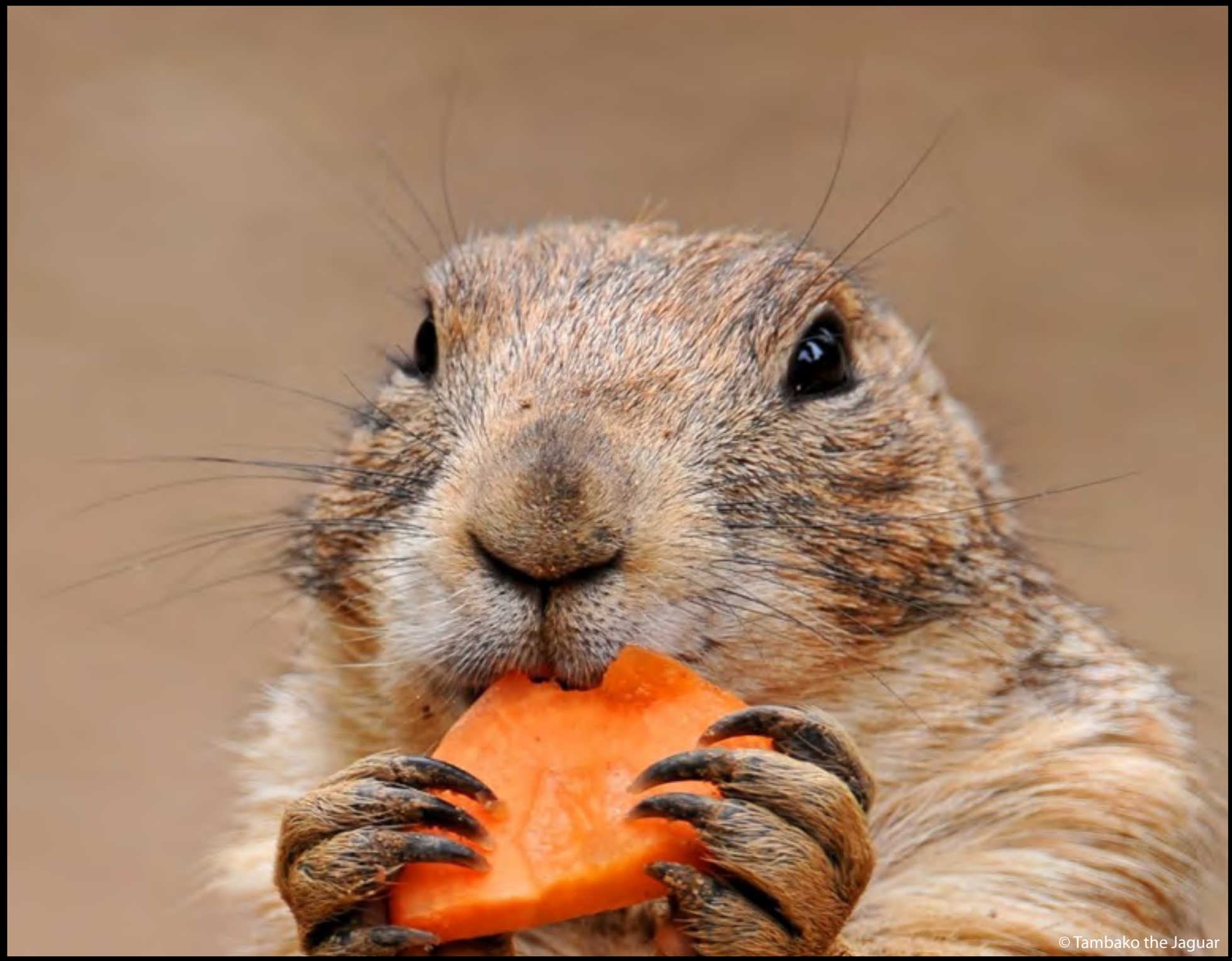
- Once enrolled a server can push configuration profile changes to the device
- Server can also query device for configuration information

| Advantages | Disadvantages |
|---|---|
| • Everything a configuration profile can do<br>• Ability to reconfigure device over the air<br>• Ability to remotely reset and clear device passcodes<br>• Ability to remotely wipe device without Exchange accounts<br>• MDM service available in Mac OS X Lion | • Requires an MDM server configured and running<br>• Requires Apple iOS Enterprise account<br>• Password based accounts still require password entry on initial use<br>• Some MDM vendors charge high fees |

# Existing Self Sufficient Users

- Many users will have configured at least some services themselves
- We still want to apply some restrictions
- Many users own their own devices
- How do we get these users to join our managed setup

# Managing Personal Devices



© Tambako the Jaguar

AUC

XWII

# Configuration Profiles

- XML plist format

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://
www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
   <key>PayloadContent</key>
      <array>
       <dict>
           <key>PayloadDescription</key>
           <string>Configures your iPhone for Xworld
               services</string>
           <key>PayloadDisplayName</key>
           <string>Configuration Profile</string>
           <key>PayloadIdentifier</key>
           <string>com.example.profile</string>
             <key>PayloadOrganization</key>
             <string>X World</string>
             [...]
```

# Configuration Profiles

- XML plist format
- Contains one or more payloads
  - Mail, Exchange, CalDAV, CardDAV accounts etc
  - Certificates, VPN settings, etc
  - Passcode requirements
  - Security restrictions
- Created with a variety of tools
  - iPhone Configuration Utility
  - Lion Profile Server
  - Custom server
  - Commercial management solution


AUC

XWIKI

# Demo

iPhone Configuration Utility

AUC

XWII

# Supported Management Properties

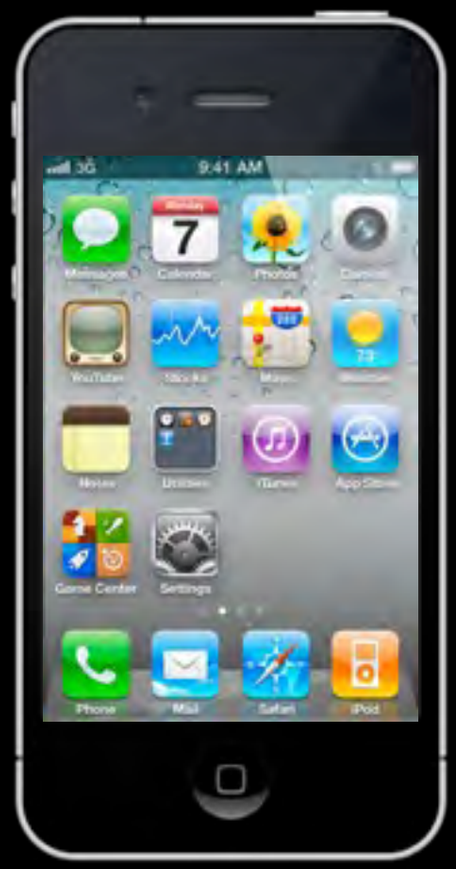
| Accounts and Settings | Restrictions | Policies |
|---|---|---|
| • Exchange ActiveSync<br>• IMAP / POP Email<br>• VPN<br>• WiFi<br>• LDAP<br>• CalDAV<br>• Subscribed Calendars<br>• Certificates and Identities<br>• Web Clips<br>• APN Settings | • Access to iTunes Music Store<br>• Access to explicit media in iTunes Store<br>• Use of Safari and security preferences<br>• Use of YouTube<br>• Use of App Store and in-app purchase<br>• Installing Apps<br>• Ability to screen capture<br>• Automatic sync while roaming<br>• Use of voice dialing<br>• Enforce encrypted iTunes backup<br>• Use of the camera | • Require passcode<br>• Allow simple passcode value<br>• Require alphanumeric passcode value<br>• Passcode length<br>• Number of complex characters in passcode<br>• Maximum passcode age<br>• Time before auto-lock<br>• Number of unique passcodes before reuse<br>• Grace period for device lock<br>• Number of failed attempted before wipe<br>• Allow Configuration Profile removal by user<br>• Configuration Profile removal passcode |

# Over the Air Enrolment

- User logs in to a web portal
- Deliver a configuration profile for device
- SCEP creates a certificate for the device

# Over the Air Enrolment

## How it works

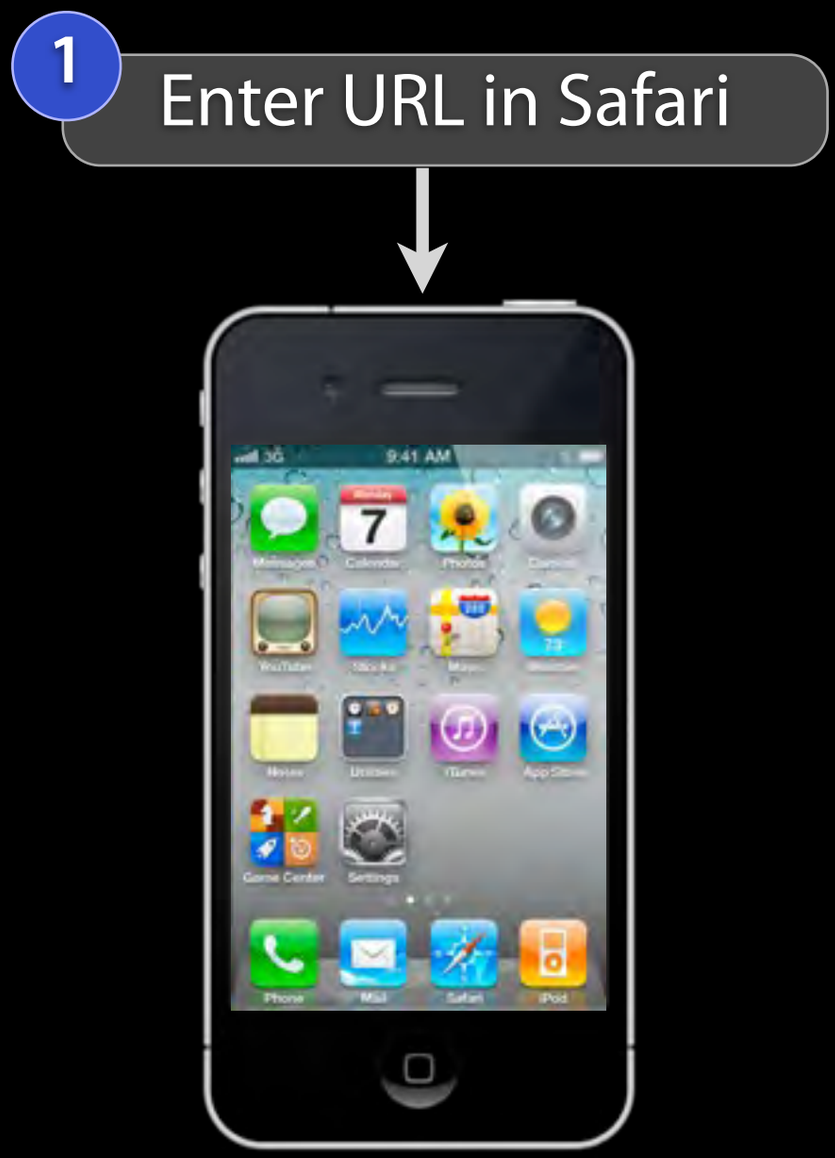



AUC

XWII

# Over the Air Enrolment

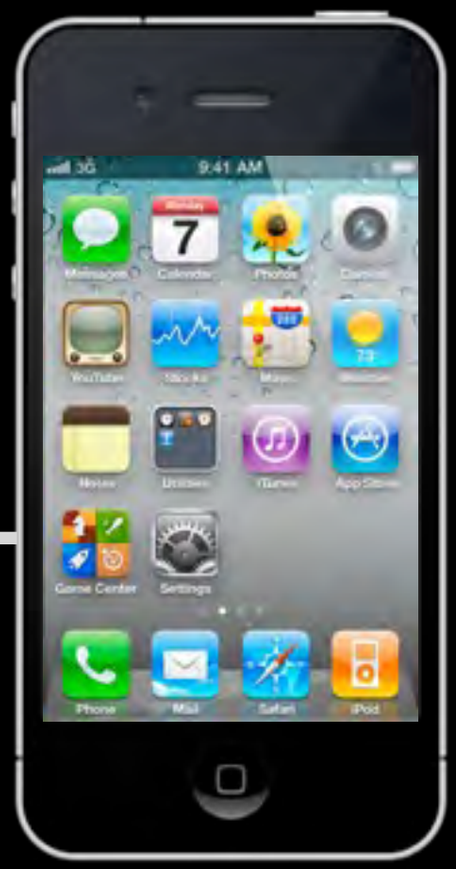
## How it works



# Over the Air Enrolment

## How it works

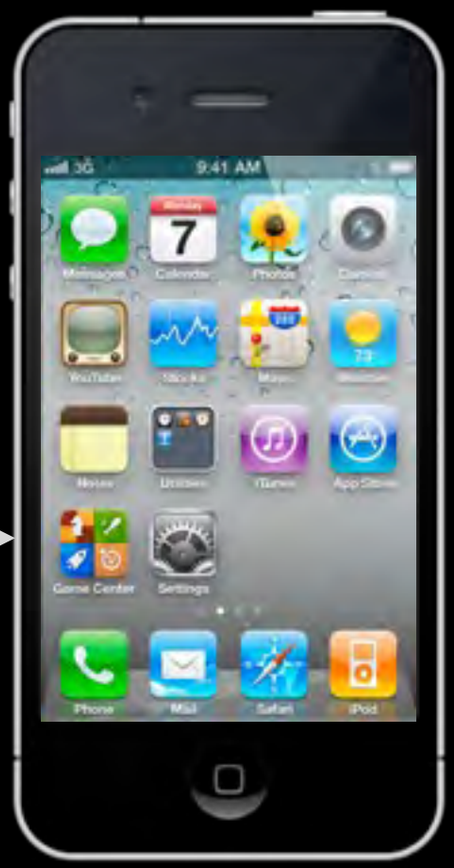
1. Enter URL in Safari
2. Log in



# Over the Air Enrolment

## How it works

1. Enter URL in Safari
2. Log in
3. Authenticate device



# Over the Air Enrolment

## How it works

1. Enter URL in Safari
2. Log in
3. Authenticate device
4. Enrol device (SCEP)

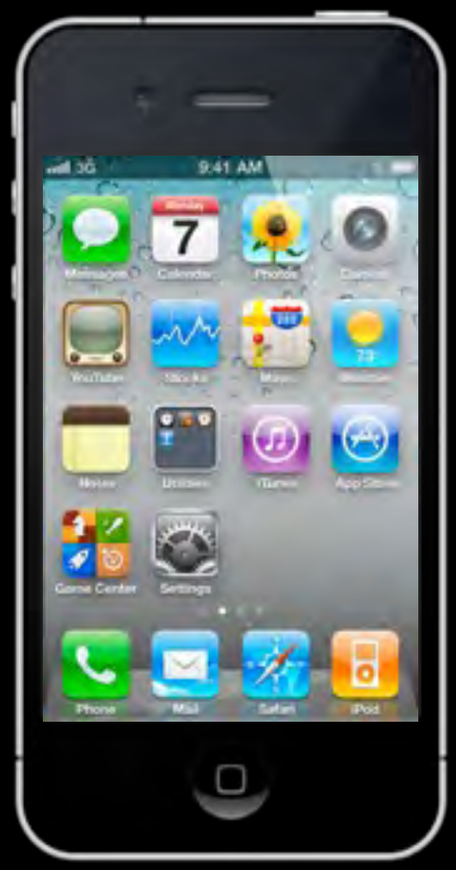
Profile service

Certificate authority

# Over the Air Enrolment

## How it works

1. Enter URL in Safari
2. Log in
3. Authenticate device
4. Enrol device (SCEP)
5. Make encrypted device profile



Profile service

Certificate authority

CONFIG

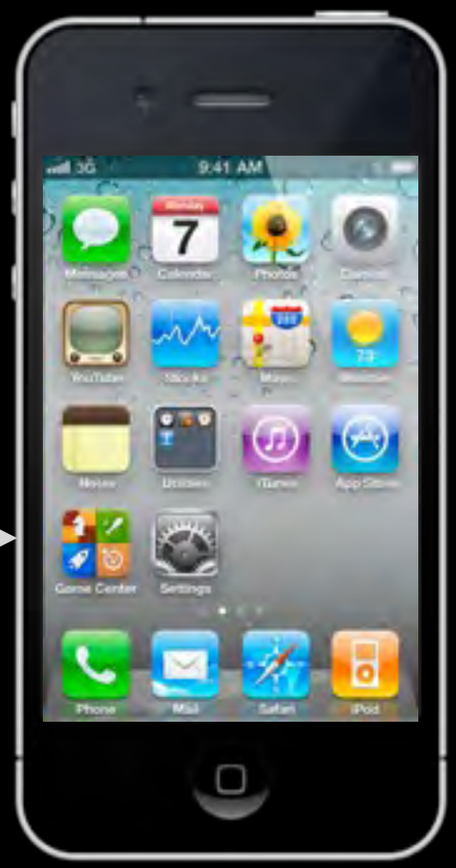
AUC

XWIKI

# Over the Air Enrolment

## How it works

1. Enter URL in Safari
2. Log in
3. Authenticate device
4. Enrol device (SCEP)
5. Make encrypted device profile
6. Install profile




Profile service

Certificate authority

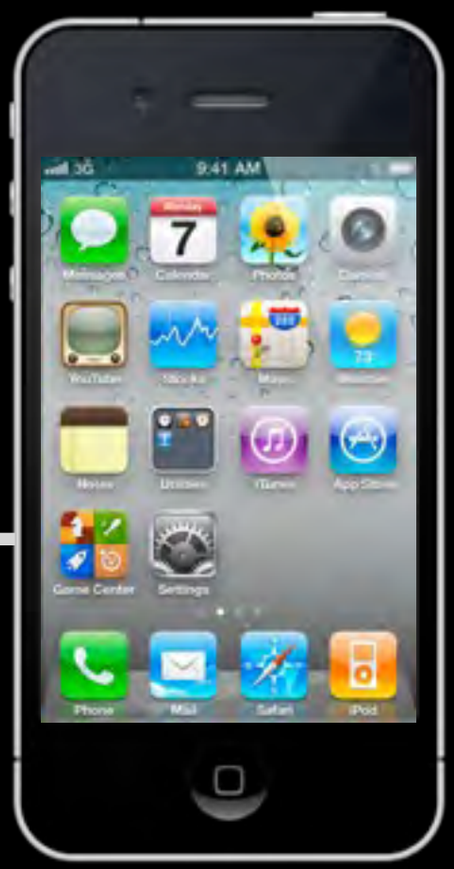
AUC

XWIKI

# Over the Air Enrolment

## How it works

1. Enter URL in Safari
2. Log in
3. Authenticate device
4. Enrol device (SCEP)




Profile service

Certificate authority

5. Make encrypted device profile
6. Install profile
7. Confirm installation

AUC

XWII

# Mobile Device Management

- Manage iOS devices transparently over the air
- Send configuration changes on demand
- Works with any network connection (WiFi, 3G, etc)
- Connection must allow HTTPS and APNS connections
  - Ensure you have a **real** SSL certificate

# Mobile Device Management

## Remote Commands

- Install or remove configuration profiles
- Install or remove provisioning profiles
- Lock device
- Remove passcode
- Remote wipe

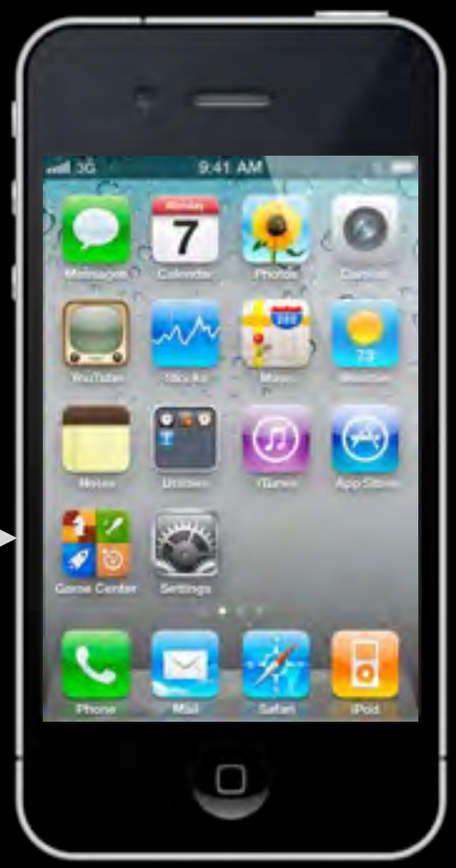
# MDM Capabilities

| Device Information | Network Information | Compliance | Applications | Management |
|---|---|---|---|---|
| • Unique device identifier (UDID)<br>• Device name<br>• iOS build and version<br>• Model name and number<br>• Serial number<br>• Capacity and space available<br>• IMEI<br>• Modem firmware | • ICCID (SIM)<br>• Bluetooth MAC address<br>• Wi-Fi MAC address<br>• Current carrier network<br>• Carrier settings version<br>• Phone number<br>• Data roaming setting | • Configuration profiles available<br>• Certificates installed and expiry dates<br>• List of all restrictions enforced<br>• Hardware encryption capability<br>• Passcode present | • Applications installed<br>• App ID, name, version, size, App data size<br>• Provisioning profiles installed (with expiry dates) | • Remote wipe<br>• Remote lock<br>• Clear passcode<br>• Update configuration<br>• Update provisioning profiles |

# Mobile Device Management

## How it works

1 OTA Enrolment





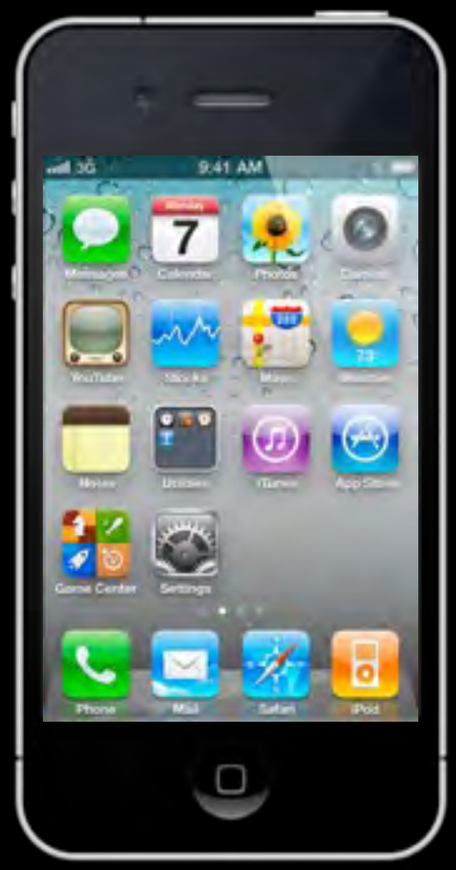
AUC

XWII

# Mobile Device Management

## How it works

1. OTA Enrolment
2. Create MDM Profile



AUC

XWII

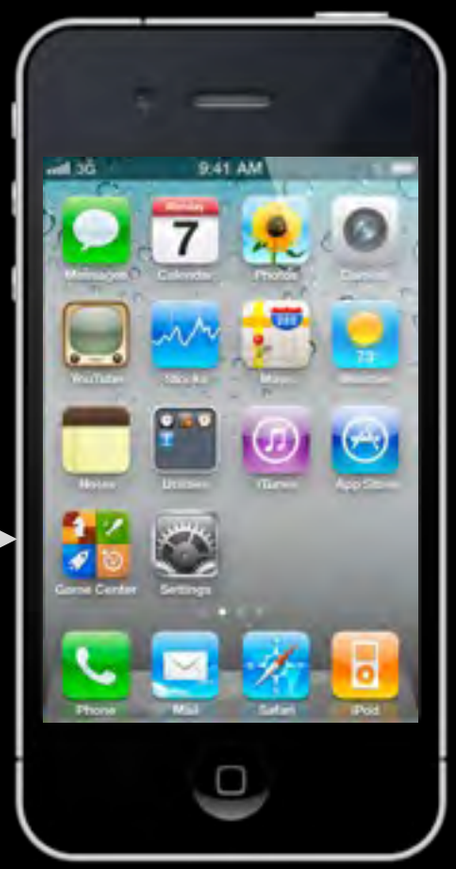
# Mobile Device Management

## How it works

3 Install MDM Profile

1 OTA Enrolment

2 Create MDM Profile



AUC

XWII

# Mobile Device Management

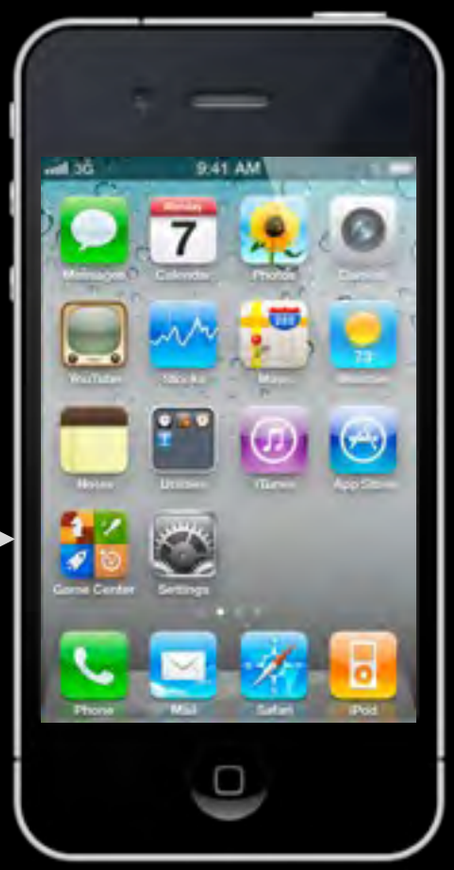
## How it works

3 Install MDM Profile

1 OTA Enrolment

4 Bind to MDM Server

2 Create MDM Profile



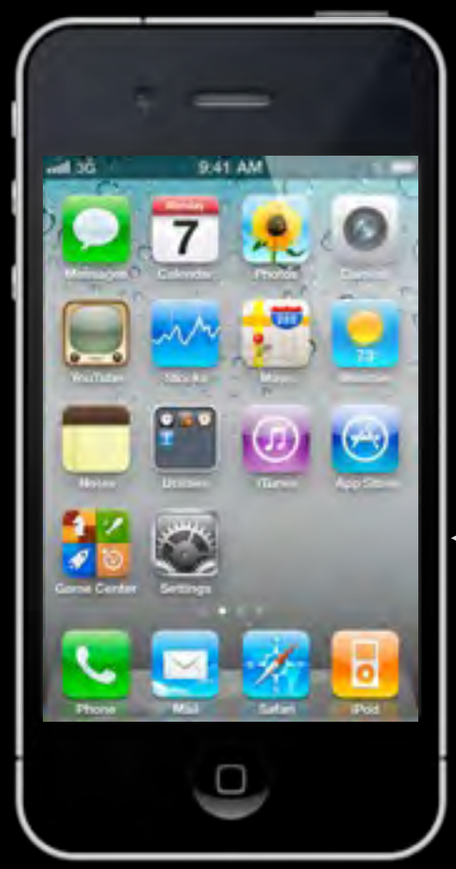

AUC

XWII

# Mobile Device Management

## How it works

1. OTA Enrolment
2. Create MDM Profile
3. Install MDM Profile
4. Bind to MDM Server
5. Send Push Notification



MDM Service

Apple Push Notification Service

AUC

XWIKI

# Mobile Device Management

## How it works

1. OTA Enrolment
2. Create MDM Profile
3. Install MDM Profile
4. Bind to MDM Server

MDM Service

Apple Push Notification Service

5. Send Push Notification
6. Connect to MDM Server (HTTPS)

AUC

XWII

# Mobile Device Management

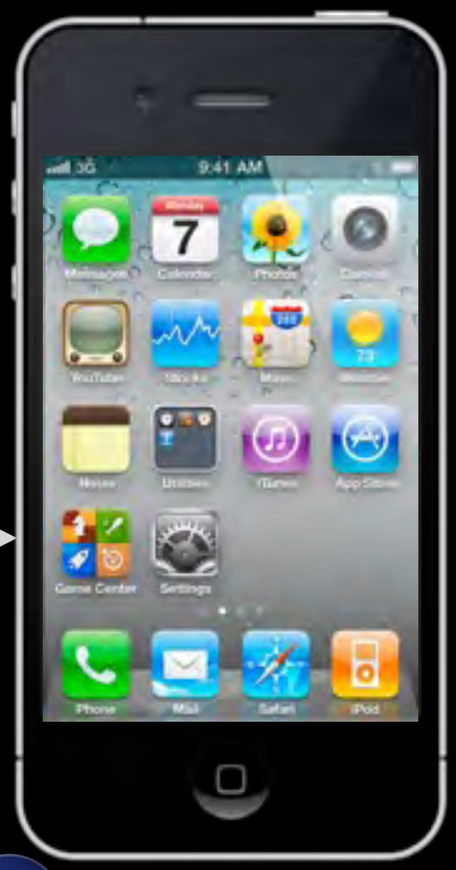
## How it works

3 Install MDM Profile

1 OTA Enrolment

4 Bind to MDM Server

2 Create MDM Profile



7 Run commands

MDM Service

Apple Push Notification Service

5 Send Push Notification

6 Connect to MDM Server (HTTPS)

AUC

XWII

# Demo

Mobile Device Management

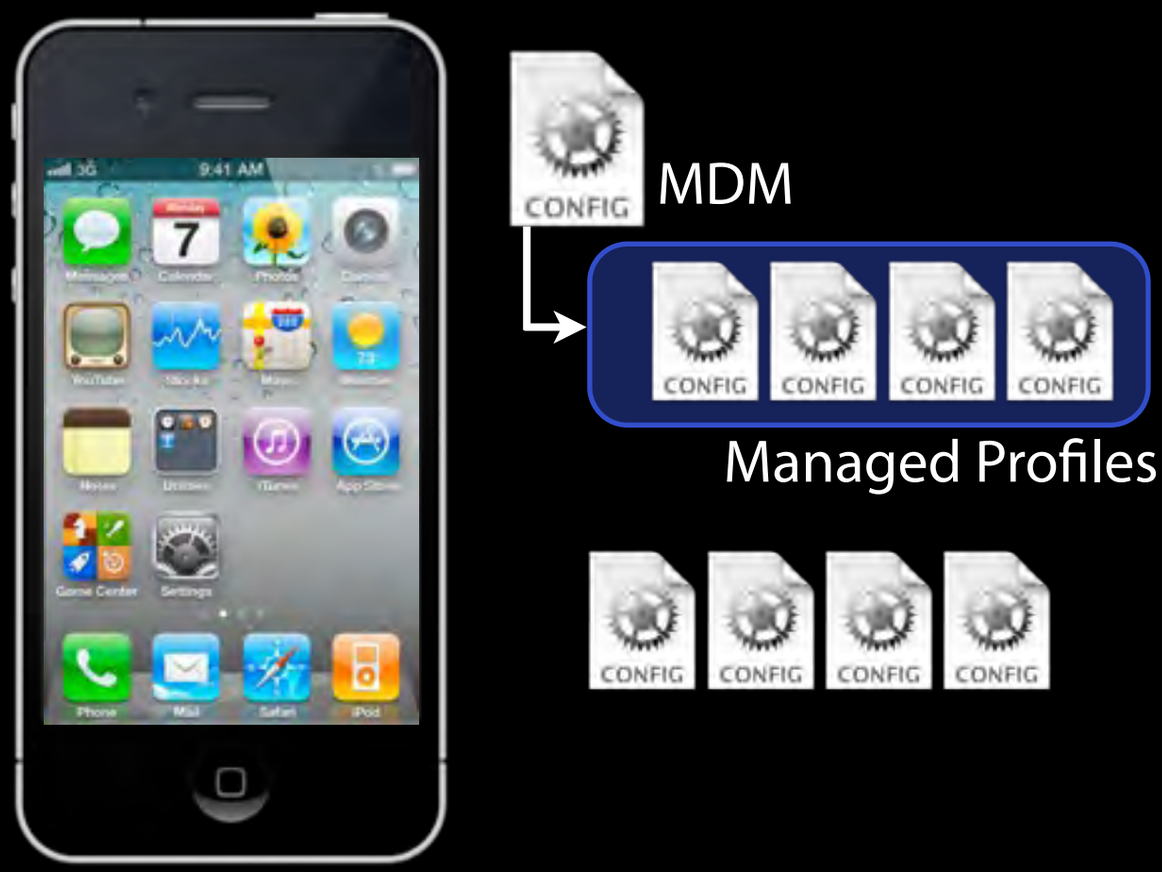
AUC

XWII

# Mobile Device Management

## How Profiles Work

- The top level “MDM” profile is the parent of child profiles
- The top level profile can be removed by user at any time, but removes all child profiles



# Mobile Device Management

## How Profiles Work

- MDM server can query information about all profiles
- Can only remove or replace profiles that are children of the MDM root profile
- Individual child profiles can be locked to disallow user removal without removing the parent profile

# Internal App Distribution

- You will need an “Enterprise” iOS Developer account
- Use a configuration profile to install a web clip linking to a website that provides your own “app catalogue”
- Install a provisioning profile allowing your app to run
- Package applications using Xcode into an IPA with manifest
- User can install applications from the app catalogue
- Not available for App Store apps

# Potential Solutions

## Mac OS X Lion Profile Server

- Provides a web interface to push configuration profiles to devices using the Apple Push Notification Service (APNS)
- Self service interface for users to lock, reset passcode and wipe devices they registered
- Can apply settings to devices based on user, group user is a member of, device or device groups
- Low cost, high functionality option

# Potential Solutions

## Casper

- Can integrate with Macs, PCs and iOS
- Android coming soon
- Provides built in support for app distribution
- Supports invitations via SMS and email
- Cost can be variable depending on modules purchased

# Potential Solutions

## AirWatch

- Supports management of iOS, Android, Blackberry, Windows Mobile, Symbian
- Can be deployed locally or via software as a service
- Provides its own API to integrate your own custom software
- Could be a bit expensive
- Can transfer from software as a service to locally hosted

# Potential Solutions

## Equinix Tarmac

- All the usual MDM support
- Designed for iOS specifically
- Licensing on a per-device basis
- Deploys on Mac or Windows based server

# Potential Solutions

Lots more

- There's a lot of 3rd party software available:

  http://www.apple.com/iphone/business/integration/mdm/

Absolute Software
MFORMATION
airwatch
MobileIron
BoxTone Mobile Service Management
mobiquant Enterprise mobile cloud management & Security
equinux TARMAC
silverback
Psystems
SYBASE An SAP Company
IBELEM
Tangoe
IIJ Internet Initiative Japan
Trellia
JAMF software
ubitexx mobile business
MaaS360 by Fiberlink
zenprise
McAfee

# What approach to use

## iPhone Configuration Utility

- Small workgroup
- Up to about 20 devices
- Little change in services offered
- Manual handling of each device is OK

AUC

XWII

# What approach to use

## Configuration Profiles

- Simple setup
- Support many devices
- Little change in services or configuration offered
- No support for querying device information

- Store your configuration profiles on a webserver of your choice
- Potentially write custom web app to select correct config profile


AUC

XWIKI

# What approach to use

## MDM Service

- Flexible setup
- Support many devices
- Future changes to services supported
- Query devices and know their current status

# Q&A

**Andrew Wellington**
Mac OS X Systems Administrator
Systems and Desktop Services
Division of Information
The Australian National University

E: andrew.wellington@anu.edu.au

AUC

XW10

# World 2011