X

World 2012

Web-based iOS Configuration Management

Tim Bell
Trinity College,
University of Melbourne

tbell@trinity.unimelb.edu.au
@timb07

About me
… and why I'm here

- **Linux System Administrator**

- **Responsibility for**

  - **Debian Linux servers**

  - **Networks (including wireless)**

- **Some experience with web app development**

- **Mac and iOS user**

Trinity College's use of iPads

- **700 international students**

  - **one year Foundation Studies program**

  - **iPad provided during orientation**

  - **students keep iPad at end of program**

- **100 staff**

  - **iPad replaced every two years**

XW12

History of iPads at Trinity

- **August 2010: Pilot with 44 students**

  - **Described in X World 2011 talk by Trent Anderson**

- **2011: review of pilot, and approval for full program**

- **August 2011–now: rollout of 540 student iPads so far, including 90 this week**

AUC

XW12

Overview of talk

- **Review of Trinity's initial approach using iPhone Configuration Utility (iPCU)**

- **Overview of configuration management for iOS devices**

- **"iOS Configurator" web app and demo**

- **Under the hood**

- **Security**

- **Customisation**

- **Issues and conclusion**

AUC

Initial approach

- Generate profile template with iPCU

- Edit template to insert template variables in place of PayloadUUID entries

- Python script that:

  - iterates over list of usernames & looks up in LDAP

  - uses template to generate and save customised username.mobileconfig file

- Load saved username.mobileconfig files into iPCU

- Manually configure each iPad with iPCU over USB

Problems with initial approach

- **Manual; labour-intensive for IT staff**

- **Doesn't scale to 700 students**

- **Template preparation fiddly, hard to test**

- **Clear-text password in LDAP**

- **Reconfiguration requires manual update**

Configuration management
… for iOS devices

- See Andrew Wellington's X World 2011 talk for excellent overview

    - http://auc.edu.au/media/xw11/xw11-slides-wellington.pdf

- Or Wednesday's session by Micah Baker

- What follows is only a brief overview of the main options

AUC

XW12

Configuration management
… for iOS devices

- **Manual management**

- **Configuration profile**

  - **via iPCU**

  - **Apple Configurator**

  - **Lion Server Profile Manager**

Configuration management
… for iOS devices

- **Mobile Device Management (MDM)**

  - **Lion Server Profile Manager**

  - **Commercial solutions:**

    - **http://www.enterpriseios.com/wiki/ Comparison_MDM_Providers**

Build your own
(that's the way in education)

- Requirements:

  - Automatic

  - Scalable to 700 students

  - Simple template preparation

  - No need to store clear-text password

  - Reconfiguration at any time

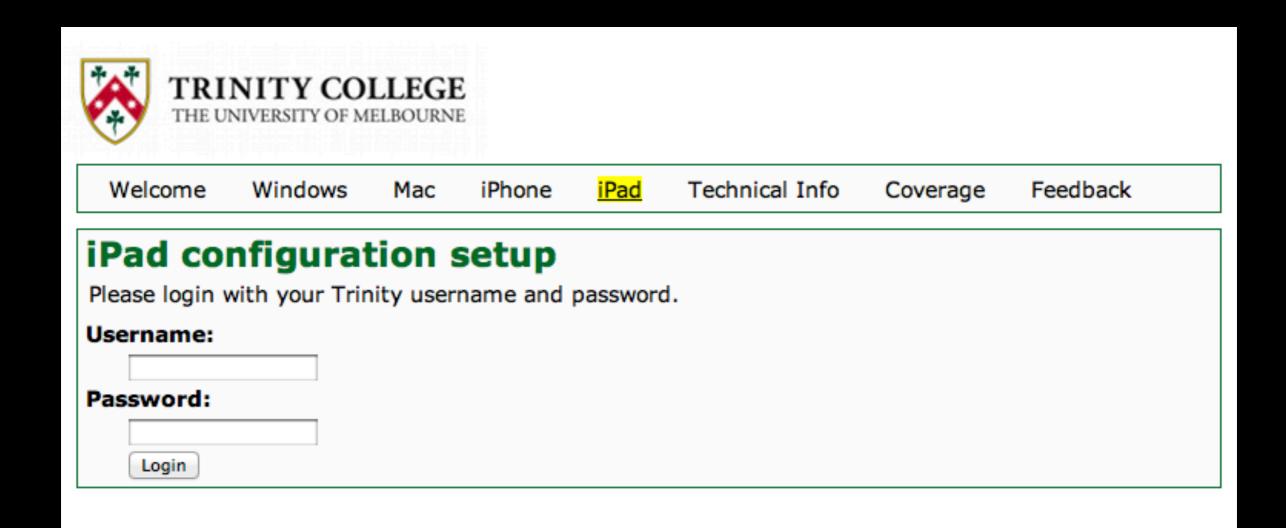 - Quick to implement

AUC

XW12

"iOS Configurator"

A web app

- **Django web framework**

- **165 lines of Python (incl. comments)**

- **229 lines in settings**

- **1 week development**

- **Runs on Linux VM with 1 GB RAM**

- **Apache, mod_wsgi, MySQL, OpenLDAP**

- **Accessed over HTTPS on open wireless**

AUC

XW12

Demo

Login

TRINITY COLLEGE
THE UNIVERSITY OF MELBOURNE

| Welcome | Windows | Mac | iPhone | iPad | Technical Info | Coverage | Feedback |

iPad configuration setup

Please login with your Trinity username and password.

Username:

[   ]

Password:

[   ]

[Login]

Download

Install

Administration demo

AUC

XW12

Django admin page

Profile configuration

Django administration

Home › Mobileconfig › Tcgroups › staff_it_test (1)

Change tcgroup

History

Name: staff_it_test

Priority: 1

Template:

```
<?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 security-related items.</string>
             <key>PayloadDisplayName</key>
```

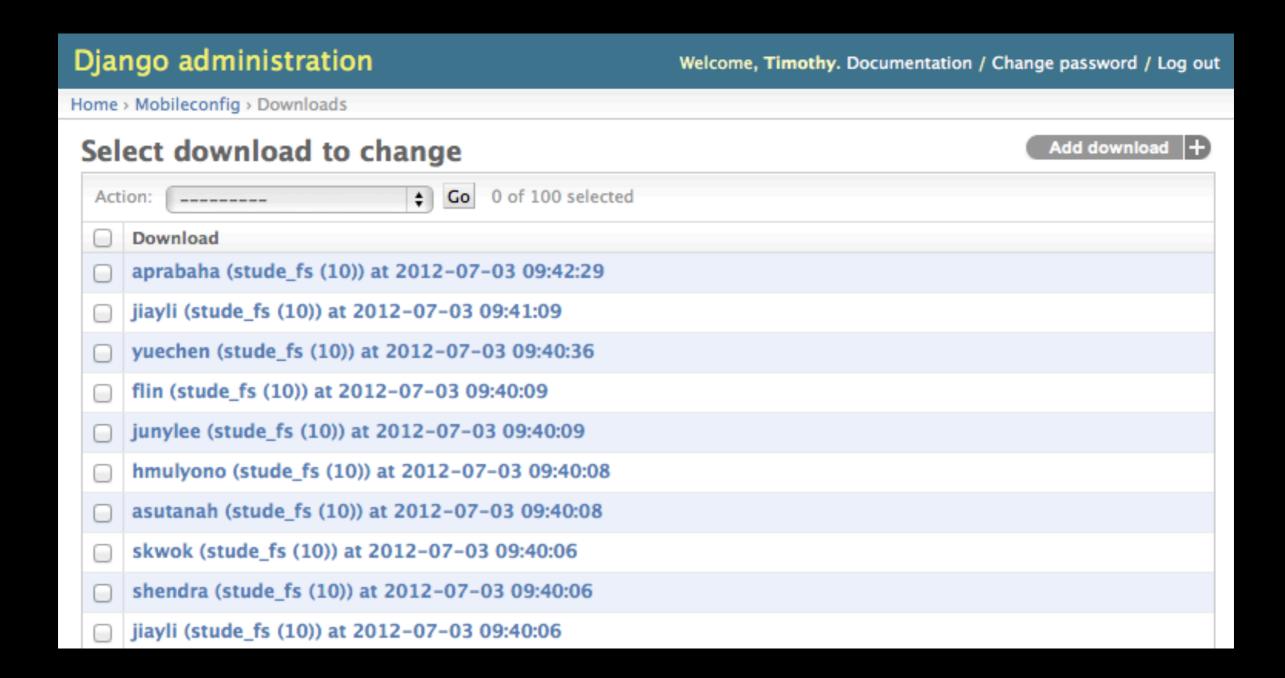✖ Delete   Save and add another   Save and continue editing   Save

XW12

Download log

Under the hood
Django

- Web application framework written in Python

- "MTV": Model, Template, View

- ORM (object-relational mapper): models stored in DB (MySQL, Postgres, etc.)

- Built-in template engine for rendering HTML

- Runs on Linux, Mac OS X, …

- http://djangoproject.com/

- Simple, powerful, efficient (and I knew it)

AUC

Under the hood
User interaction

- Capture username and password at login

- Authenticate against LDAP

- Lookup name and group info from LDAP

- Choose config profile based on group

- Substitute captured details into config profile template

- Provide config profile download

AUC

XW12

Under the hood
Administration

- **Use iPCU to create profile**

  - **Use template variables: $TCUSER, $TCPASS, $TCFULLNAME**

- **Export the profile as a .mobileconfig file**

- **Use Django admin to set up "tcgroup" object for group**

- **Paste the .mobileconfig file into the template field**

Under the hood
Templates

- **$TCUSER, $TCPASS, $TCFULLNAME**

- **When saving a tcgroup object (via admin), PayloadUUIDs are turned into template variables; from this:**

```
<key>PayloadUUID</key>
<string>0D657A8F-42F6-4652-ADF3-EDD52A4C3899</string>
```

- **to this:**

```
<key>PayloadUUID</key>
<string>$TCUUID1</string>
```

Security
Fundamentals

- **Run over HTTPS:**

  - **Commercial SSL cert**

  - **Secure authentication and profile download**

- **Django sessions and CSRF protection**

- **Users get to see what the profile contains before installing it**

XW12

Security
Profiles with cleartext passwords

- Profile can't be viewed, but can be obtained via other means

- Other configuration methods don't provide ways to include passwords in profiles

- We wanted to be able to include them:

  - Simplify setup

  - Student accounts are low risk (for us)

- You need to do your own risk assessment

AUC

XW12

Security
Profiles with cleartext passwords

- Precautions:

    - Require passcode lock with reasonable timeout

    - If an iPad is lost, change user password

    - Password policy requires password not used for other services

- Keychain would be better, but even Keychain passwords aren't secure: http://sit.sit.fraunhofer.de/studies/en/sc-iphone-passwords-faq.pdf

Customisation
…because you do things differently

- Authentication backend (e.g. AD)

- Choose profile based on other attributes or complex rules

- Offer multiple profiles

- Demo: http://10.0.1.90:8000/ (on XWorld C wireless network)

AUC

XW12

Issues

- **Need to delete profile and re-download to update**

- **No integration with password changing; need to update (see above)**

- **Including passwords in profiles improves the user experience ⇒ tempting to use for staff accounts ⇒ unacceptable risk**

- **Possible improvement: signed profiles**

AUC

XW12

Conclusion

- **iOS Configurator in production at Trinity for one year**

- **Great return on time investment**

- **Hoping to release under Open Source license (pending approval)**

  - **Contact me if you're interested in it**

- **Tim Bell <tbell@trinity.unimelb.edu.au>**

- **@timb07**

AUC

XW12