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
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
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
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
- Or Wednesday’s session by Micah Baker
- What follows is only a brief overview of the main options
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:
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
“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
Demo
Login

iPad configuration setup
Please login with your Trinity username and password.

Username: 
Password: 
Login
Download

iPad configuration setup
(Logged in as Tim Bell (bhat); logout)

Configuration profile for your device:
download now

Other sites of interest:
- Trinity Portal
- TCFS IT Orientation Information
Install Profile

Trinity College bhat
Trinity College, The University of Melbourne

Description:
* Wireless Setup
* Email Setup
* Calendar Setup
* Contact Setup

Received: 03/07/2012
Contains:
- 2 Certificates
- Wi-Fi Network
- CalDAV Account
- Web Clip
- Exchange Account
- Password Policy

More Details
Administration demo
Django admin page
Profile configuration

Django administration

Change tcgroup

Name: staff_it_test

Priority: 1

Template:

```xml
<?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>
        </dict>
    </array>
</dict>
</plist>
```
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/](http://djangoproject.com/)
- Simple, powerful, efficient (and I knew it)
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
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
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
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
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 $\Rightarrow$ tempting to use for staff accounts $\Rightarrow$ unacceptable risk

• Possible improvement: signed profiles
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