802.1X Deployment Tool Case Study at Swansea University

By Gareth Ayres
25/11/2009

SWANSEA UNIVERSITY
PRIFYSGOL ABERTAWE
www.swansea.ac.uk

Contents

Introduction

Swansea University provides a wireless internet service (SWIS) using the 802.11g standard that covers all of its campus buildings, halls of residence on campus, Student Village and Beck House Residence.

The wireless system previously used a PPTP VPN connection over an open (unsecured) wireless network in order to provide security to wireless users. A new wireless system was developed which made use of more secure and efficient standards to secure the wireless traffic and authentication. This system was based on 802.1X with WPA-Enterprise encryption and a FreeRadius/LDAP authentication system. The new system also adhered to the Janet Roaming Service requirements and therefore offered a number of benefits to the previous system.

There was however one substantial hurdle to overcome in order to switch to the new wireless system: **client configuration**. The users of the wireless network invariably consist of a mixture of device types and operating system types and versions. The ideal solution to this situation would be a supplicant that could be deployed preconfigured to most operating systems, but currently no such supplicant exists.

Fortunately most operating systems come with a built in supplicant. The next issue faced is then the configuration of the built in supplicant. At Swansea the majority of operating systems of users are Windows based and as of Windows XP SP3 it is possible to utilise a WLAN API that comes preinstalled on all Windows devices to configure the Windows supplicant.

As a solution to the configuration of thousands of Windows devices we developed a tool that interacts with the WLANAPI and configures devices automatically. By using a tool this also allows for additional check (security/updates) to be made as well as additional configuration options such as proxy settings.

This case study details Swansea experience of using the deployment tool on more than 6000 devices over a 4 week period at the start of the 2009/2010 academic year.

Swansea Wireless System

This section will provide an overview of the wireless infrastructure, device types and usage levels of the wireless system at swansea.

Wireless Infrastructure

The wireless infrastructure at Swansea is built on a Cisco platform of 4 Wireless Service Module controllers in a 6509 with a Wireless Controller Server used for management of the ~800 LWAP Access Points that are placed around the campus and halls of residence.

Authentication is achieved using a typical FreeRadius backend with MySQL and LDAP providing account information and accounting. The system also allows for Janet Roaming Service logins through the Eduroam SSID.

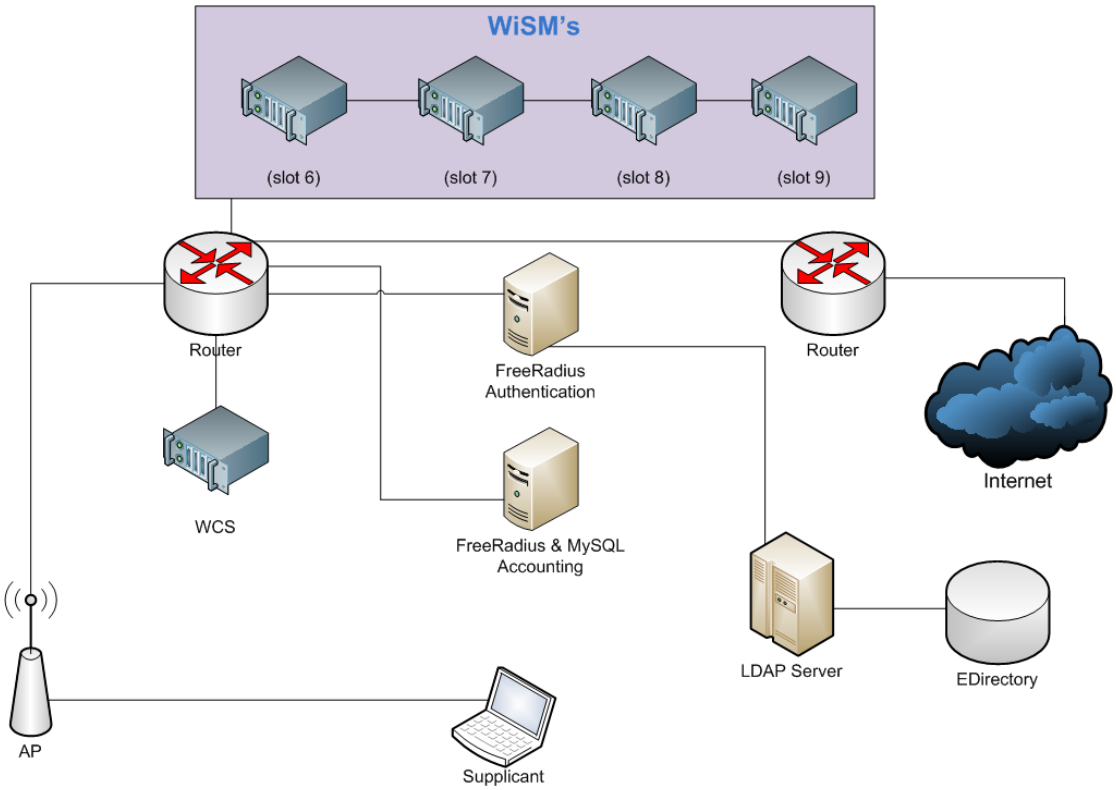

Figure 1 – Swansea Wireless Infrastructure

Wireless Users

The only means of internet access from the university halls of residence is wireless, so a large proportion of wireless users are students. Staff and limited visitors also use the wireless system.

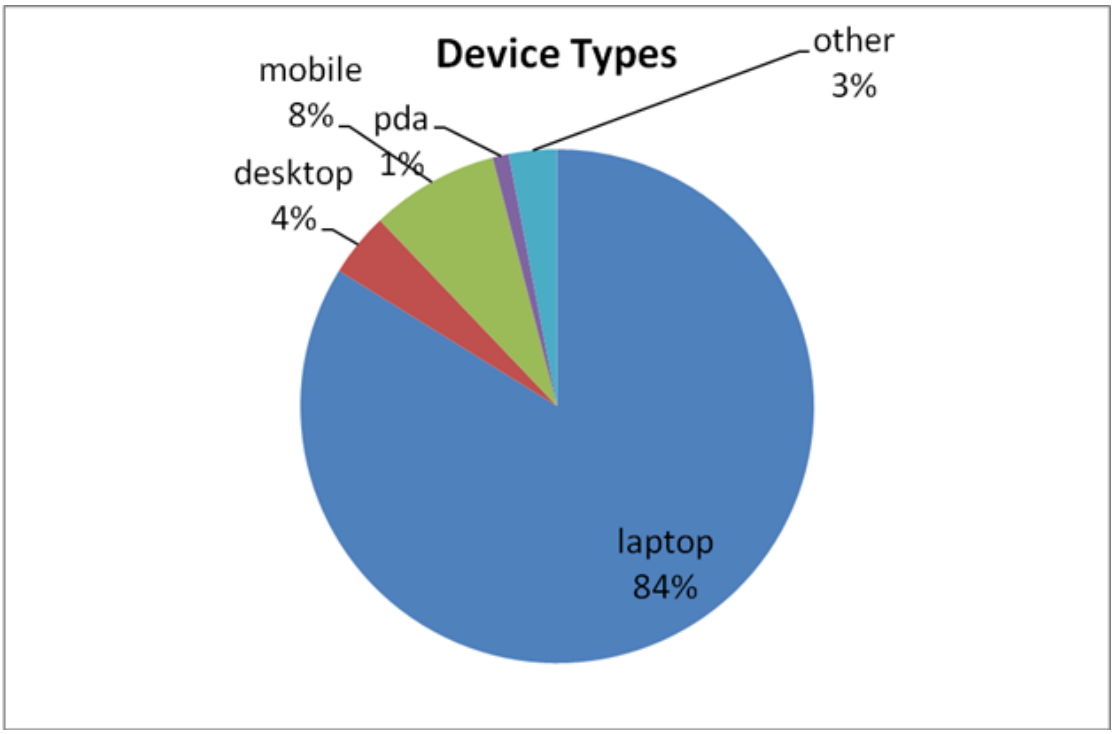

Figure 2 –Device Types as of 30/10/2009

As can be seen from figure 2 the device types of the wireless users is mainly laptops with some mobile phones and desktops also. This is obtained from a sample of registrations from October and September 2009, of which 5497 (84%) of devices registered were laptops.

Similarly the operating system types for the same dates can be seen in figure 3. The majority of users have Windows Vista or XP, with iPhones, Macs and Linux devices trailing behind. The combined percentage of 74% equates to **5208** devices which would need to be configured.

Figure 4 shows the usage pattern of unique users for a two year period between August 2007 and August 2009. The term dates can clearly be identified from the rise and falls in usage, as can the increase in popularity of the wireless network as time progresses.

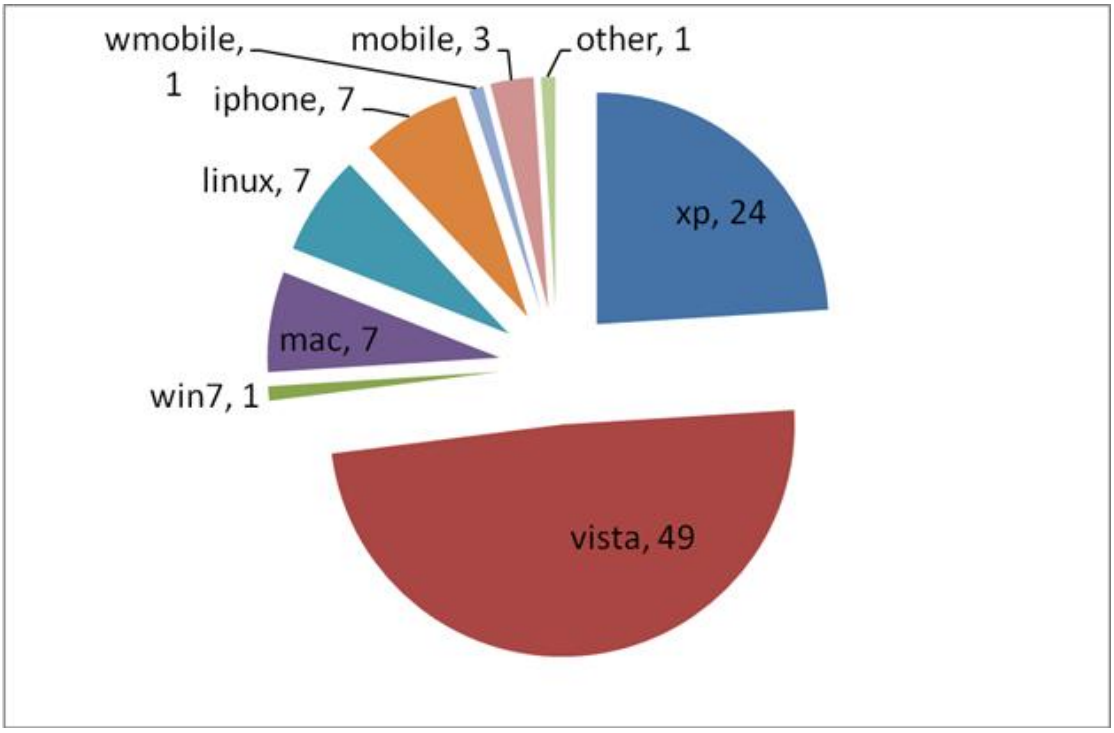

Figure 3 – Operating System types as of 30/10/2009

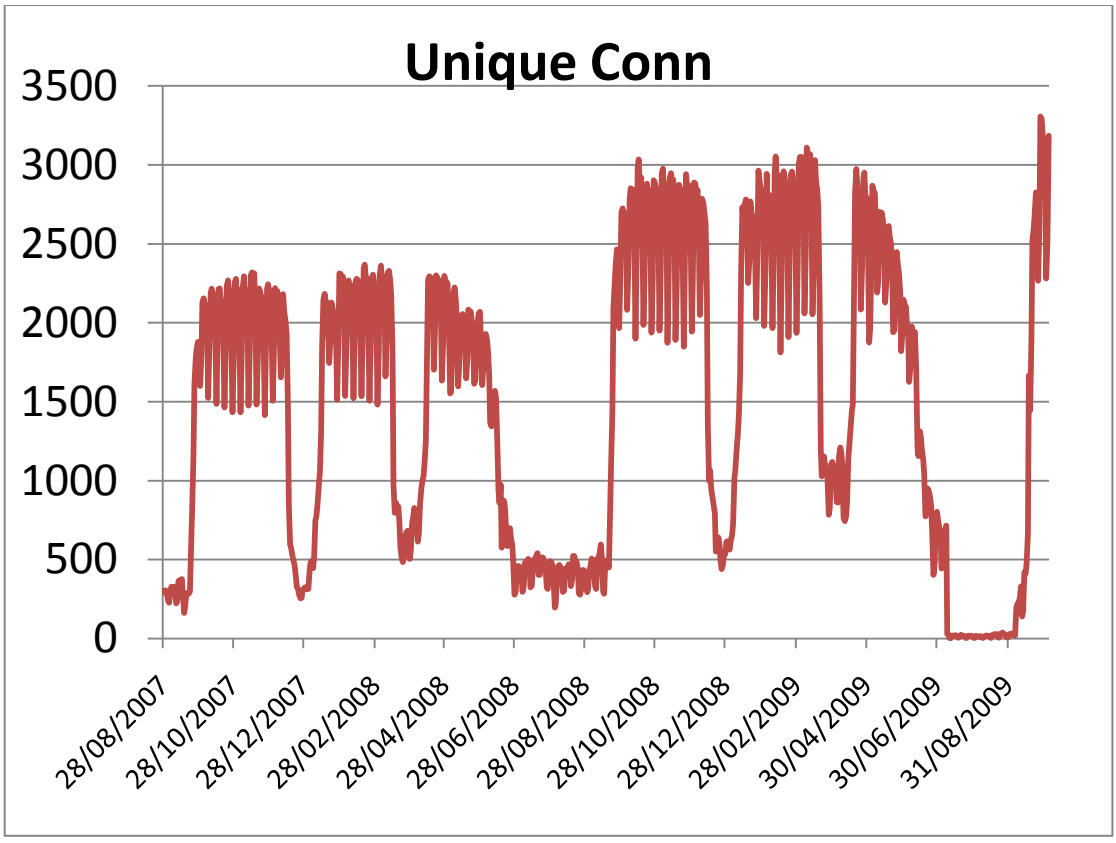

Figure 4 – Unique wireless users per day August 2007 – 2009

The Deployment Tool

The deployment tool (SU1X) was developed to aid the configuration of the 5000-6000 Microsoft Windows devices used on the wireless network. The primary goal of the deployment tool is to configure a Windows device to use the 802.1x Wireless settings of the institution as well as applying any additional settings.

The tool takes around 20 seconds to run and configure a machine. This saves significant time over manual configuration as well as requiring less support from IT Support staff.

Overview of Tool Usage

The deployment tool can be broken down into two distinct applications:

1. The wireless settings capture tool
2. The deployable configuration tool

The capture tool is run on a machine that has been manually configured for use on the wireless network, and is fully functional. The capture tool will then capture the configuration settings and save them to a XML file which is then distributed with the deployable tool.

The deployable tool is then packaged with the XML file and an edited INI file into a self extracting executable which is then distributed to clients.

The packaged tool can then be distributed to any Windows XP (SP3), Vista or Windows 7 users. Once the tool is run on a users machine, it performs a number of checks and applies the settings. The tool also displays information to the user on how to connect and automatically associated them to the network prompting them to log in.

Tool Customisation

The tool allows for complete customisation through editing an INI file that is distributed with the tool. This allows for the customisation of logos, pictures and text displayed by the tool in order for institutions to customise the tool to match their institutions look and feel. Swansea version of the tool can be seen in figure 5.

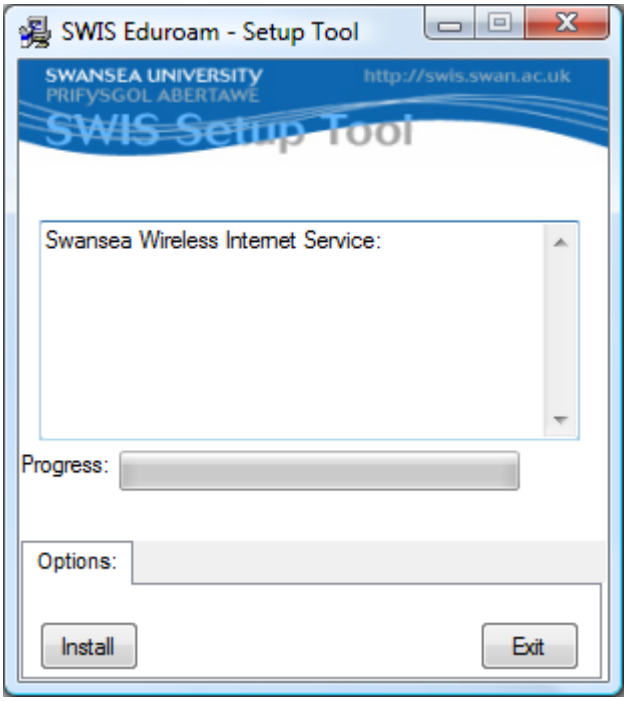

Figure 5 – Swansea Deployment Tool

Tool Distribution

The tool needs to be distributed to users. There are numerous ways of doing this, but at Swansea the tool was provided as a download upon successful registration through the open setup wireless network. The tool then dissociated the user from the setup network and connected them to the secure network.

Tool Features

Features of the current tool:

- Configuration of any 802.1X wireless settings
- Configuration of automatic or manual proxy server settings for IE and Firefox
- Removal of setup SSID
- Automatic connection of Secure SSID
- Popup with instructions and hints on how to connect and fill in username
- Works in Windows XP (SP3), Vista, Windows 7

Deployment at Swansea

Figure 6 shows the tool deployment process at Swansea. A comparison between the automatic and manual process is shown with estimations of time taken for each step shown in box brackets.

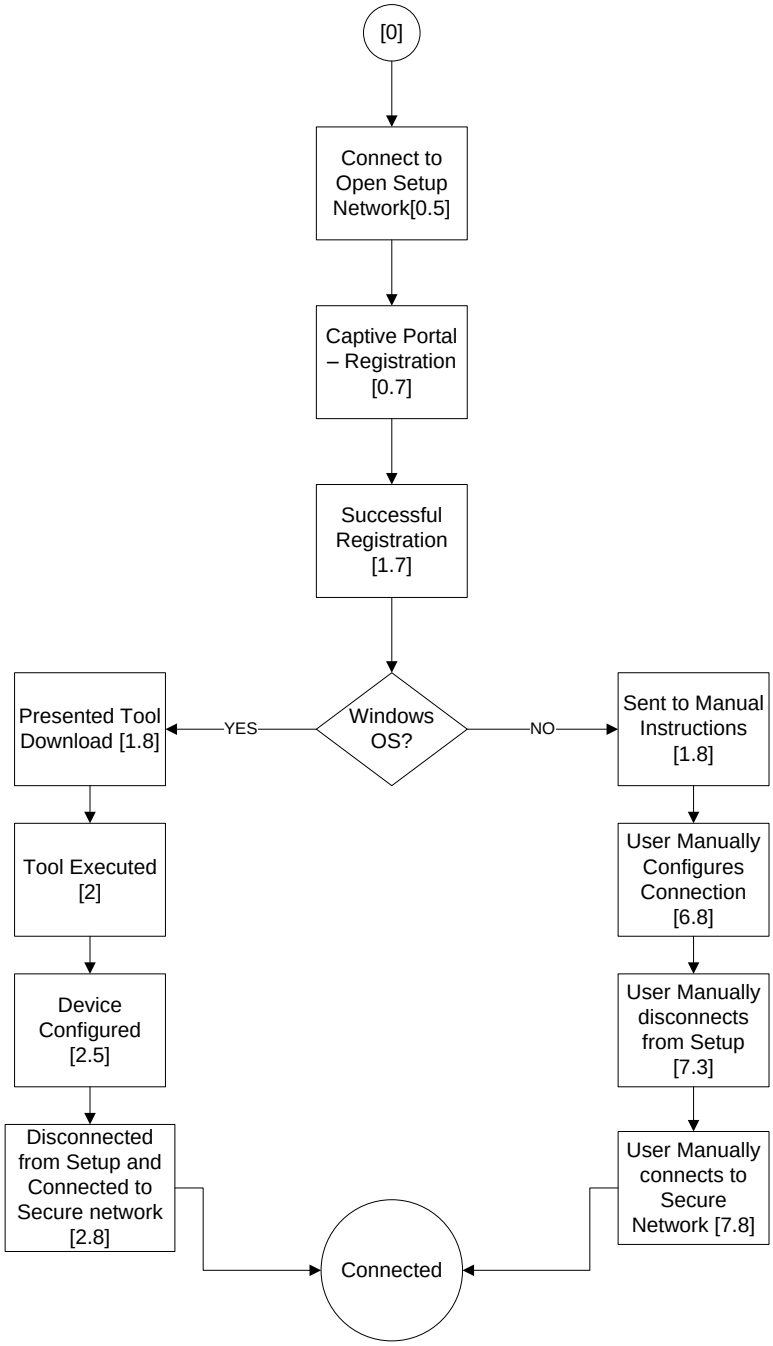

Figure 6 – Tool Deployment Process as Swansea

The savings from automation is well established in the computing industry and the tool worked as expected, reducing support staff involvement and speeding up the registration process.

It can be seen in figure 7 (an adjusted graph from Friday before the start of Fresher's week when the students move in to halls of residence) that the configuration process this year was as effective as the previous years where a well developed VPN deployment tool was used.

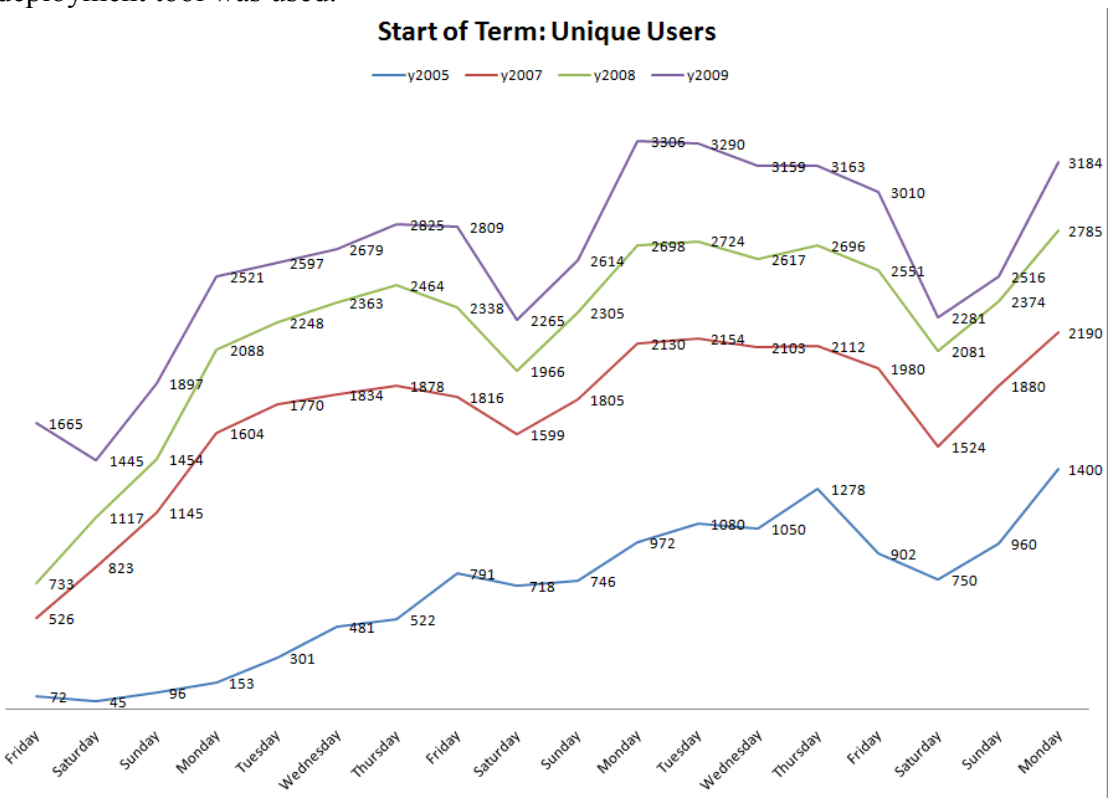

Figure 7 – Stat of term connected users comparison

Problems

There were only a few problems identified as a result of the deployment tool.

- The tool failed to detect some Asian wireless adapters and displayed an error message. This was identified as a result in a different returned string on some implementations of the WLANAPI and has now been resolved
- The tool was identified by some version of Avast Antivirus as a possible threat. Turning real-time protection off to run the tool run this. This problem went away with a antivirus signatures update as was a result of the exe packing being falsely identified as a possible virus.