Australian Catholic University
Brisbane Sydney Canberra Ballarat Melbourne

ACU National

Implementing eduroam at ACU

Lessons Learnt

Stephen Walsh
ITCS, ACU National

Australian Catholic University
Brisbane Sydney Canberra Ballarat Melbourne

Background

ACU National

Wireless at ACU was "walled garden" style, using Cisco 1100/1200 AP's, running into VLANs and using ACL's to restrict traffic to the VPN server.

Vulnerable to ICMP ping proxying and tunnelling.

Temporary wireless access required user accounts and setup on foreign laptops, with no control over the laptop when the person left.

Initial WZCS setup was campus specific, and limited success was had with a setup script.

Background

ACU National

Proof of Concept started in Mid-December 2005,With first part of January spent on Certificate issues, and first successful staff login on 24th January, and first student login on the 2nd February.

ACU Federated mid February, with final test completed from Hawthorn Campus of Swinburne on 16th March 2006.

ACU was the first Eduroam site to implement against a Windows 2003 AD backend, and the only site to date to use D-Link AP's.

Australian Catholic University
Brisbane Sydney Canberra Ballarat Melbourne

Background

ACU National

- Proof of concept ran OEM hardware (P3/400) and Redhat 9, with FreeRadius compiled from source, and was located at Mount St Mary Campus (msmradius)

- Due to NAT and router issues, server was replaced with OEM (Athlon XP 1800) box located in Signadou Campus, Canberra (sigradius)

- sigradius server ran FC3, with FreeRadius 1.0.1 from YUM repository.

- Hardware availability issues arose in February, resulting in decommissioned Cisco MCS being used for production (acuradius), running FC4 and FR1.0.4

Certificates

ACU National

2 Certificates are needed for the EAP conversation, a Root cert on the server, and a matching certificate on the client (or supplicant) machine.

When the supplicant associates, it is prompted for a username. This is used for routing, and once the destination server has been contacted, it sends an AUTH-CHALLENGE back to the supplicant. The Supplicant replies with the certificate, and if it matches(AUTH-ACCEPT), a SSL tunnel is created using TKIP, and the EAP conversation is started.

A script is provided with FreeRADIUS, but to generate certificates you need to have a good knowledge of PKI and OpenSSL.

Certificate is optional, but you run the risk of Federation Poisoning

Australian Catholic University
Brisbane Sydney Canberra Ballarat Melbourne

Security at the AP

ACU National

A security algorithm is needed for communication when exchanging user details.

Open – All traffic is clear.

WEP – Hackable. All Traffic is still clear

WPA/TKIP – WPA encrypts layers 3 7,leaving only the MAC in the clear. TKIP uses a key scheme based on RC4, with per packet key mixing, integrity checks and autonomous re keying, ensuring that each packet is sent with it's own unique encryption key. Whilst this still allows MAC spoofing, more traffic is needed to allow to crack the encryption and keys.

The Certificate script

ACU National

Our first attempt at producing certificates prompted a rewrite out of sheer frustration. Initial plan was for a ncurses-based menu, but settled on bash for regression compliance. First bug report came in from a site in France, who was running a very early version of Bash, causing script to fail as being to fancy.

The script provides a basic interface for creating certificates. The script was released on the 17th January, 2006, and received over 3000 hits in 24 hours, from places as far afield as Slovenia, Croatia, Finland and ARPANET.

In March, 2006 Alan DeKok from FreeRadius contacted me for permission to include the script in the next version of FreeRadius.

Australian Catholic University
Brisbane Sydney Canberra Ballarat Melbourne

LDAP trickery

ACU National

```
Ldap {
        server = 123.123.123.123
        Identity = “ou=<binduser>,cn=acustaff,dc=acu,dc=edu,dc=au"
        password = <bind_user_password>
        basedn = “cn=people,dc=acu,dc=edu,dc=au>
        filter = "(uid=%{Stripped-User-Name:-%{User-Name}})"
        tls_cacertfile = </path/to/certificate of the CA for your LDAP server >
        tls_randfile = /dev/urandom
        access_attr = "dialupAccess"
        dictionary_mapping = ${raddbdir}/ldap.attrmap
        ldap_connections_number = 5
        password_attribute = userPassword
}
```

2003 AD LDAP trickery

ACU National

```
Ldap Canberra{
        server = 123.123.123.123
        Identity = “ou=<binduser>,cn=student,dc=acu,dc=edu,dc=au"
        password = <bind_user_password>
        basedn = “ou=users,cn=canberra,dc=student,dc=acu,dc=edu,dc=au”
        filter = "(uid=%{Stripped-User-Name:-%{User-Name}})"
        tls_cacertfile = </path/to/certificate of the CA for your LDAP server >
        tls_randfile = /dev/urandom
        access_attr = "dialupAccess"
        dictionary_mapping = ${raddbdir}/ldap.attrmap
        ldap_connections_number = 5
        password_attribute = userPassword
}
```

Australian Catholic University
Brisbane Sydney Canberra Ballarat Melbourne

What we learnt

ACU National

- Red Hat 9 %^#$@ for this sort of thing.
- AP’s need to be either NAT’d or DMZ’d for security.
- Border Routers need lots of memory for NAT handling (128Mb is good, 256Mb is better.).
- Trust the developer when he tells you it can’t be done.
- Don’t trust the developer when he tells you it can’t be done.
- Communication is important within the team and within ITS as a whole.
- Don’t try to packet sniff between the AP and the Radius server.
- Keep packet grabs of transactions from before, during and after to aid as fault finding.

Australian Catholic University
Brisbane Sydney Canberra Ballarat Melbourne

What's left

ACU National

- Easier Log Access for Helpdesk staff
- SNMP integration
- Removing W2k3 LDAP trickery
- Automation of Supplicant/Certificate installation
- Yet another rewrite of the script
- Real World Disaster recovery test.

Australian Catholic University
Brisbane Sydney Canberra Ballarat Melbourne

Questions

ACU National