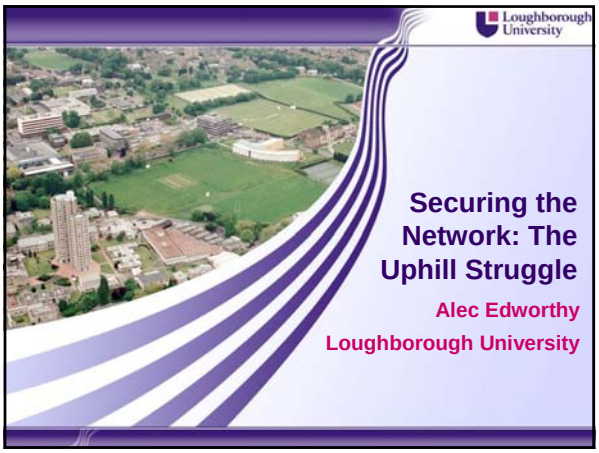


Securing the Network: The Uphill Struggle

Alec Edworthy
Loughborough University

Securing the Network: The Uphill Struggle

- Why do we bother
- What options are available
- How we developed our solution
- Problems and quirks we discovered
- Future plans

Why bother?

- Complying with local and JANET AUPs
- Transmission of malicious content
- Downloading of copyrighted materials
- Bandwidth abuse
- Inconvenience of disconnected PCs

Network Security - a brief summary

- Wireless networks adopted security early
  - MAC address restrictions
  - WEP
  - WPA/WPA2 PSK
  - WPA/WPA2 Enterprise
- Wired networks have always relied on physical security
  - Locked doors - offices, wiring closets, networking cabinets
  - Swipe card access restrictions
  - Inaccessible wiring
  - Restricted cabling - cable ties, padlocks, special brackets
  - CCTV

What options are available?

- Physical restrictions
  - Hiding sockets behind panels or using specialised brackets (like with pay phones in public areas)
  - Gluing cables into sockets - messy and not easily reversed
- DHCP server restrictions
  - Build a list of authorised clients and only handout addresses to them
- Switch port restrictions
  - Restrict switch ports to one MAC address and enable sticky MAC addresses
  - VLAN Policy Management Server (VMPS)
  - 802.1X

Scaling the solutions

- Physical restrictions
  - Locked doors and swipe card access stop non-staff/students (except where propped open!) but don't stop ingress of 3rd party hardware
  - Physically restraining connectors helps but requires extra work
- DHCP server restrictions
  - Effort of building and maintaining lists of MAC addresses - with over 1,400 lab PCs and a yearly turnover of around 200 PCs it becomes difficult to manage
  - Swapping PCs requires alterations to the MAC address list
- Switch port restrictions
  - Swapping PCs with sticky MAC requires switch config changes, annoying the year round, especially in the summer with turnover

What is 802.1X

- Provides a flexible authentication mechanism based on EAP
- Four main states,
  - Unauthorised – non-EAP related traffic blocked during authentication
  - Authorised - e.g. a permitted staff/student PC
  - Guest - e.g. Visitor's laptop
  - Authentication Failed - e.g. devices or users who have been banned
- Can provide different VLANs based on the state (further extendable via VLAN overrides via RADIUS etc)
- Used by most 802.11 wireless access points
  - WPA/WPA2 PSK - the AP carries out the authentication
  - WPA/WPA2 Enterprise - authentication handed by separate server

Cisco Switch Config – Base switch config

```
aaa new-model
aaa group server radius RADIUS-SERVERS
 server <RADIUS Server IP> auth-port 1812 acct-port 1813
 ...
aaa authentication dot1x default group RADIUS-SERVERS
aaa authorization network default group RADIUS-SERVERS
aaa accounting dot1x default start-stop group RADIUS-SERVERS

dot1x system-auth-control
dot1x guest-vlan supplicant

radius-server host <IP> auth-port 1812 acct-port 1813 \
  key 7 <secret>
...
radius-server source-ports 1645-1646
radius-server retransmit 2
radius-server timeout 2
radius-server deadtime 10
radius-server vsa send authentication
```


Cisco Switch Config – Per port config

```
interface FastEthernet0/1
 dot1x port-control auto
 dot1x timeout quiet-period 5
 dot1x timeout tx-period 1
 dot1x timeout reauth-period server
 dot1x timeout supp-timeout 1
 dot1x timeout server-timeout 5
 dot1x max-req 3
 dot1x max-reauth-req 1
 dot1x reauthentication
 switchport access vlan <VLAN number>
 dot1x guest-vlan <VLAN number>
 dot1x auth-fail vlan <VLAN number>
```


802.1X is looking good!

- Benefits of 802.1X
  - Standard switch port configuration in a lab means moving or replacing PCs requires no reconfiguration
  - Only correctly configured and authorised hardware is usable in the lab - students' laptops can be blocked or restricted as required
- Drawbacks of 802.1X
  - Configuring 1,400 PCs is not a small task
  - Demands a certain standard of networking equipment and setup
    - Managed switches
    - One device per switch port
  - Requires a backend server infrastructure - radius servers, etc
  - Makes wake on LAN much more difficult to implement

How to configure 1,400 PCs...

- Initially only considered IT Services labs and PCs
- All were running Windows XP SP2 (early 2007)
- Managed via Active Directory 2003 so GPOs were a possibility
- Unfortunately wired 802.1X configuration via an add-in was not an option at this time
- How hard can it be to configure it another way though...
- ...quite difficult is the answer!

Hacking the Windows XP registry

- Start with no wired 802.1X configuration
- Dump the registry in plain text
- Configure 802.1X
- Dump the registry in plain text again
- Compare the two files - around 350,000 lines each!
- Discover just how much Windows loves to adjust the registry

Finally, the magic is found!

- Key:

```
[HKLM\SOFTWARE\Microsoft\EAPOL\Parameters\Interfaces\{GUID}]
```

- Value: “1”
- Data:

```
hex:05,00,00,00,00,00,00,00,00,00,c0,19,00,00,00,20,00,00,00,11,22,33,\
  11,22,33,11,22,33,11,22,33,11,22,33,11,22,33,11,22,33,11,22,33,11,\
  22,33,11,22,0d,00,00,00,28,00,00,00,00,00,00,28,00,00,00,05,00,00,00,00,\
  00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00,00,19,00,00,00,56,00,00,00,01,00,00,00,56,00,00,00,01,00,00,\
  00,00,00,00,01,00,00,00,2d,00,00,00,15,00,00,00,01,00,00,00,14,00,00,00,\
  58,4b,ef,04,bd,45,90,1f,a0,4a,0d,ec,a7,bd,69,4d,5c,d2,27,0f,00,00,01,00,00,\
  00,17,00,00,00,1a,00,00,00,01,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
  00,00,00,00
```

- Now to find the GUID programatically... Google to the rescue!

A scriptable, working solution

- VBScript deployed to selected OUs via an AD Group Policy
- Find the GUIDs of all the network interfaces marked as wired
- For each GUID, check for the existence of the “1” key and create or overwrite as necessary
- Check the SupplicantMode and AuthMode values resetting them if necessary
- If changes have been made then prompt for a reboot
- All well and good, until the screen saver kicks in - reboot prompt and settings vanish!

Successful deployment - 2007/8

- Initially deployed to three IT Services labs - approx. 80 PCs
- Then extended to all other IT Services labs across the campus - approx. 300 more PCs
- Later deployed to selected third party labs - approx. 320 more PCs
- No major complaints, a few lab managers with teething problems
- Biggest task - reconfiguring all those switch ports!

Continuing the good work

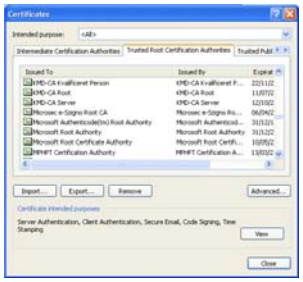
- 2007/8 was a success so 2008/9 sees the rollout continue
- Labs project builds a new core image, sends it out for testing, 802.1X still works, everyone’s happy
- Then along comes Service Pack 3 and a new way to configure 802.1X
- Unfortunately this was missed during QA’ing and not picked up until after the deployment started!
- No more registry hacking needed - now uses XML profiles and Network Shell

XML for the win

```
<?xml version="1.0"?>
<LANProfile xmlns="http://www.microsoft.com/networking/LAN/profile/v1">
  <MSM>
    <security>
      <OneXEnforced>false</OneXEnforced>
      <OneXEnabled>true</OneXEnabled>
      <OneX xmlns="http://www.microsoft.com/networking/OneX/v1">
        <cacheUserData>false</cacheUserData>
        <authMode>machine</authMode>
        <EAPConfig><EapHostConfig xmlns=""http://www.microsoft.com/
provisioning/EapHostConfig""><EapMethod><Type xmlns=""http://
www.microsoft.com/provisioning/EapCommon"">25</Type><VendorId
xmlns=""http://www.microsoft.com/provisioning/EapCommon"">0</
VendorId><VendorType xmlns=""http://www.microsoft.com/provisioning/
EapCommon"">0</VendorType><AuthorId xmlns=""http://www.microsoft.com/
provisioning/EapCommon"">0</AuthorId></
EapMethod><ConfigBlob>0100000056000000010000000100000001000000 2D00000015
0000000100000014000000584BEF04BD45901FA04A0DECA7BD694D5CD2270F0000010000
00170000001A0000000100000000000000000000000000000000</ConfigBlob></
EapHostConfig></EAPConfig>
      </OneX>
    </security>`
  </MSM>
</LANProfile>
```


Other Service Pack 3 foibles

- Certificates - how many would you like?
- Some PCs had one,
- Some had more than one,
- Some had none at all!
- To this day we do not know why this happens - nor do Education Support Centre or Microsoft themselves!



What the coming year holds

- The rollout of Active Directory 2008 means no more VBScripts
- Wired 802.1X configuration now handed via true GPOs
- Aiming for 100% uptake of 802.1X in third party labs
- Looking to also rollout PXE booting, Wake on LAN and Multicast OS image deployment...
- But that's a story for another day!

Any Questions?

Alec Edworthy

http://www.lboro.ac.uk/it