





  
**Waking up securely:  
A story of Wake on LAN & 802.1X**  
**Alec Edworthy**  
**Loughborough University**



**Waking up Securely: A story of Wake on LAN and 802.1X**

- Background
- What is Wake on LAN and why use it?
- Developing our solution
- Problems and quirks
- Future Plans


2



**Background - Many, geographically diverse, secure PCs**

- Over 1,400 lab PCs across the 437 acre campus,
  - 347 managed by IT Services
  - 160 managed by the Library
  - Rest managed by other support services or academic departments
  - Around 76 individual labs across campus
- Most labs protected using 802.1X security
- Monthly patching cycle, with phased rollouts
  - One local IT Services lab
  - All other IT Services labs
  - All labs across campus


3



**Background - Patching the old way**

- Patches installed using startup scripts
- Staff used to have to visit each lab to power up PCs
- Time and resource consuming exercise
- Had to be done before lectures start and allow enough time to install patches and reboot
- Occasional interruptions caused complaints from staff and students
- Labs left powered up and so wasting electricity


4



### What is Wake on LAN?

- Wake on LAN (WoL) allows devices to be powered up remotely
- Uses *Magic Packets* sent to port 9/udp
- Double-edged green sword,
  - Allows PCs to be "turned off" when not used but still available at a moment's notice
  - "Off with WoL" uses more power than "off" e.g.
    - 21.5-inch iMac uses 0.77W "off", 1.94W when "sleeping"
    - Less power efficient PCs around 3W "off" and 4W "off with WoL"
  - Power .v. convenience balance - most situations see a power use drop with increased convenience


5



### Security, convenience, cost - pick two

- Staff & Student PC Services team examined a number of existing packages including Microsoft's SCCM
- Most had at least one show-stopping drawback
  - Main issue related to 802.1X - PC is on one VLAN when powered on, another when powered off
  - Some would have meant a major expenditure or buy into new technology
- As with 802.1X, a home grown solution was looking good


6



### What happens during boot-up in our labs

- Our original 802.1X deployment used a startup script
  - Detected wired network interfaces
  - Prepared and applied an 802.1X configuration using XML
  - Started the wired 802.1X service
- Unreliable execution lead to logging and reporting
- Presented this information on a webpage for Staff and Student PC Services team to review
- Realised I was sat on a gold mine of information and possibilities

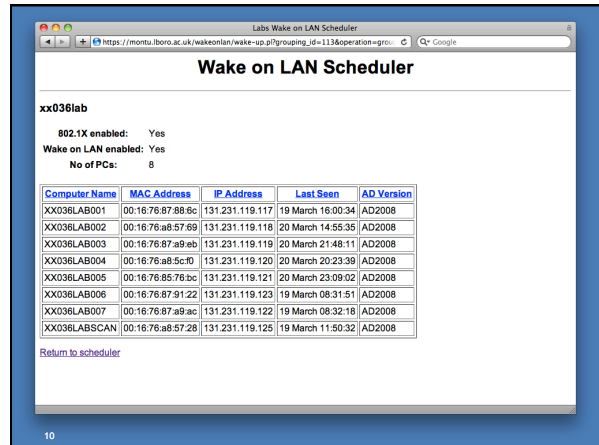
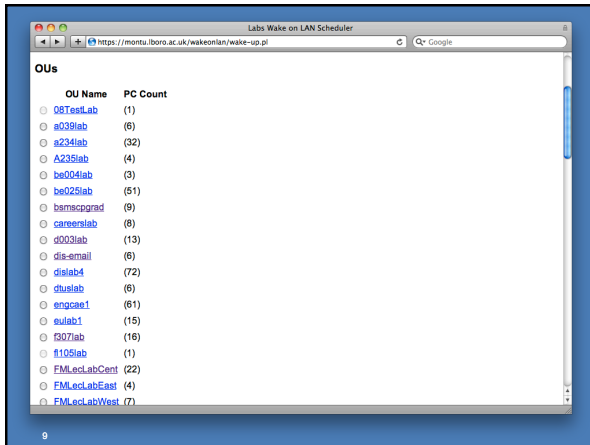
7



### Extending the call home

- Extended the "call home" script to also collect the MAC address of the PC
- Harnessed our Active Directories to find which organisational unit (OU) a PC lived in given its NetBIOS name
- Now when a PC calls home we know,
  - its name (NetBIOS)
  - where it lives physically (AD OU)
  - who it is and where it lives on the network (MAC & IP address)
  - when it last booted up
- Mix in some Perl, MySQL, Apache and what do you get...

8



**From calling home to wake up call**

- What does WoL need to work?
  - MAC address of the PC
  - Broadcast address of the network the PC is on
- Also need to consider forwarding of broadcast packets across VLANs and routers
  - In Cisco parlance `ip directed-broadcast <acl number>` e.g.
 

```
interface Vlan314
description Central park labs
...
ip directed-broadcast 101
...

access-list 101 permit udp host 158.125.10.3 any eq discard
access-list 101 deny ip any any
```

**Wake up ET!**

- Despite all the automation, some human intelligence is still needed
  - Backend system can learn a new OU grouping but has to be told what the service and guest VLANs are
- Initially provided waking on a per-OU basis
- Later extended to include super groups
  - All Haslegrave PC labs
  - All IT Service PC labs
  - All PC labs
- Wake up calls can be scheduled for anytime on any day

Labs Wake on LAN Scheduler

https://montu.lboro.ac.uk/wakeonlan/wake-up.pl

W145lab (7)

w171lab (21)

w172lab (23)

w225lab (10)

xx002lab (29)

xx023lab (20)

xx031lab (23) (d)

xx031lab (41) (d)

xx036lab (8) (d)

yy001lab (9)

zz004lab (6)

zz014lab (16)

Time: 03:03 (24 hour clock)

Date: 22 / March / 2010

(The time according to montu is: 13.25:43)

**Pending Jobs**

Grouping	Wake Time	Status	Requestor	Cancel
n326lab	22 March 2010 03:00	Pending	ccae	Cancel

### Timing is everything


- Wake on LAN packets are port 9/udp
- Send them too fast and they may get dropped during periods of heavy network activity (e.g. backups)
- Originally sent one per second - OK on a per-lab basis
- Not so good if waking all labs - 23 minutes?
- Finally settled on,
  - Ten packets per second
  - Two sweeps (with a two minute delay)
- Maximum time around 7 minutes

### Reporting

- Staff and Student PC Services team very pleased... but always want more!
- Some PCs patched, some didn't - did we wake them all?
- Produce a report broken down into,
  - PCs which woke successfully
  - PCs which didn't wake successfully
  - PCs which woke but failed 802.1X
- Initially produced manually - rapidly moved to automate

### Patching the green way


- Patching carried out using SCCM
- Maintenance windows - no more patching during lectures
- Power-save software - shuts down PCs automatically
- PCs wake automatically, patch themselves, reboot as necessary and then shutdown again
- No more interrupted lectures
- No more wasted staff time visiting labs across campus
- Almost everyone is happy!



### Other uses

- Wake on LAN isn't just for patching...
- Powering up large, or older, labs for lectures
  - Thereby saves lab managers from having to visit labs before lectures
- Ad-hoc collection of statistics and other data from PCs
  - Power up the PC, remote desktop into it, collect the files and shut it down
- Deployment of specialised software packages for specific courses etc.


17



### Problems

- Wake on LAN is not 100% reliable
- Some WoL packets may just get ignored
- Some PCs may be physically turned off at the wall
- If not shutdown correctly then they do not wake up
- Some PCs may still be turned on (and so didn't *technically* wake up)
- Backend relies on human intelligence - humans are always a flaw in the system!

18



### Future Plans

- Day-to-day maintenance is automated
  - New PCs
  - New labs (almost)
  - PCs moving from one lab to another
- Some manual intervention still needed
  - Yearly pruning of replaced PCs
  - Test/development PCs appear but never disappear
- Improve the success rate,
  - Targeted labs 90-100% success

19





## Any Questions?

**Alec Edworthy**  
<http://www.lboro.ac.uk/it>