

Deploying Wireless Suitable For Education

Alexander Clouter <ac56@soas.ac.uk>

Information Technology Department
School of Oriental and African Studies

LMN Event - 7th May 2009

Outline

Making users accountable in an open network.

- 1 Give Me Wifi, Now!
 - “Tab A into Socket B”
 - Adding Authentication
- 2 802.1X Port Based AAA
 - Where To Solve Our Problem
 - What Makes It Tick
- 3 What About the Small Print?
 - Visitors
 - Vendor Equipment
 - Where to Find Help

Todo List Item 153: Provision Wifi

God Said Let There Be Wireless...

Wireless is Dead Easy to Deploy:

- built to act identically to Ethernet
- workstation connects¹ to wireless access point
- once connected, DHCP kicks in
- user gets 'interwebs' and hopefully rarely bothers you

This is workable if:

- you use DHCP, which of course we all do, right?
- network is VLAN aware, otherwise headaches will ensue
- you have a RADIUS server (FreeRADIUS, MS IAS, ...)

¹using 'magic'

Todo List Item 153: Provision Wifi

God Said Let There Be Wireless...

Wireless is Dead Easy to Deploy:

- built to act identically to Ethernet
- workstation connects¹ to wireless access point
- once connected, DHCP kicks in
- user gets 'interwebs' and hopefully rarely bothers you

This is workable if:

- you use DHCP, which of course we all do, right?
- network is VLAN aware, otherwise headaches will ensue
- you have a RADIUS server (FreeRADIUS, MS IAS, ...)

¹using 'magic'

What About Security?

Encryption in a wireless network?

- encryption only provides privacy
- meaningless unless you know who's at the other end
- as sysadmins we care about authentication

In Regards to 'Security', In Practise We Find

Open Network == WEP == WPA-PSK (Personal)

Why is this?

- security is not just for the users
- it's about your `abuse@` mailbox too

What About Security?

Encryption in a wireless network?

- encryption only provides privacy
- meaningless unless you know who's at the other end
- as sysadmins we care about authentication

In Regards to 'Security', In Practise We Find

Open Network == WEP == WPA-PSK (Personal)

Why is this?

- security is not just for the users
- it's about your `abuse@` mailbox too

What About Security?

Encryption in a wireless network?

- encryption only provides privacy
- meaningless unless you know who's at the other end
- as sysadmins we care about authentication

In Regards to 'Security', In Practise We Find

Open Network == WEP == WPA-PSK (Personal)

Why is this?

- security is not just for the users
- it's about your `abuse@` mailbox too

MAC Restricted

Open Network's (inc WEP/WPA-PSK) give authzn only

- JANET mails abuse@
- you have no idea who is who on your network
- violated the AUP

We need some networking sysadmin 'duct tape'...

- what about workstation MAC addresses?
- create table listing MAC ↔ User
- populate AP's with trusted MAC address table
- abuse@ → IP → DHCP → MAC → User

Problems:

- maintaining MAC address table is very painful
- MAC addresses are trivially spoofed and captured

MAC Restricted

Open Network's (inc WEP/WPA-PSK) give authzn only

- JANET mails abuse@
- you have no idea who is who on your network
- violated the AUP

We need some networking sysadmin 'duct tape'...

- what about workstation MAC addresses?
- create table listing MAC ↔ User
- populate AP's with trusted MAC address table
- abuse@ → IP → DHCP → MAC → User

Problems:

- maintaining MAC address table is very painful
- MAC addresses are trivially spoofed and captured

MAC Restricted

Open Network's (inc WEP/WPA-PSK) give authzn only

- JANET mails abuse@
- you have no idea who is who on your network
- violated the AUP

We need some networking sysadmin 'duct tape'...

- what about workstation MAC addresses?
- create table listing MAC ↔ User
- populate AP's with trusted MAC address table
- abuse@ → IP → DHCP → MAC → User

Problems:

- maintaining MAC address table is very painful
- MAC addresses are trivially spoofed and captured

Web Redirect (WRD)

Hotspots do not care about MAC addresses, should we?

- user connects and opens browser for first time
- session hijacked and redirected to login page
- access granted for *X* hours, could not be simpler

Problems:

- AP ↔ workstation is not encrypted - user grumblings
- user credentials are trivially captured via MitM
- session stealing via IP spoofing possible ('Evil Twin' also)
- PAP used as authentication method at backend

Web Redirect (WRD)

Hotspots do not care about MAC addresses, should we?

- user connects and opens browser for first time
- session hijacked and redirected to login page
- access granted for *X* hours, could not be simpler

Problems:

- AP ↔ workstation is not encrypted - user grumblings
- user credentials are trivially captured via MitM
- session stealing via IP spoofing possible ('Evil Twin' also)
- PAP used as authentication method at backend

Where To Solve This Problem

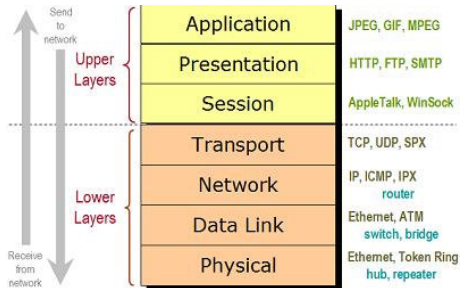
So far, our 'duct tape' keeps coming undone. What now?

- MAC Restrict → L2
- Web Redirect → L3
- Need to look lower!

802.1X operational glue: L1 ↔ L2

- originally created for wired
- vendors cried out about WEP
- 'WPA Enterprise' ~ 802.11i

'WPA2 Enterprise' (aka 802.11i) = 802.11 + 802.1X



Where To Solve This Problem

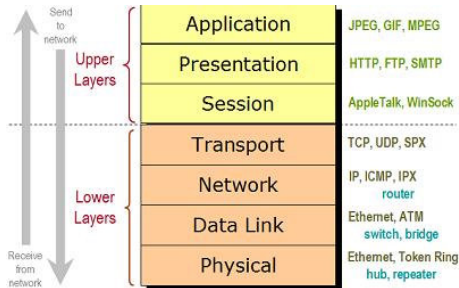
So far, our 'duct tape' keeps coming undone. What now?

- ~~MAG Restrict~~ → L2
- ~~Web Redirect~~ → L3
- **Need to look lower!**

802.1X operational glue: L1 ↔ L2

- originally created for wired
- vendors cried out about WEP
- 'WPA Enterprise' ~ 802.11i

'WPA2 Enterprise' (aka 802.11i) = 802.11 + 802.1X



Where To Solve This Problem

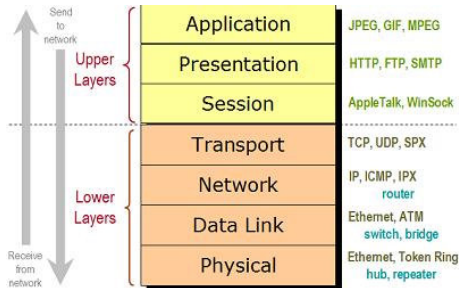
So far, our 'duct tape' keeps coming undone. What now?

- ~~MAG Restrict~~ → L2
- ~~Web Redirect~~ → L3
- **Need to look lower!**

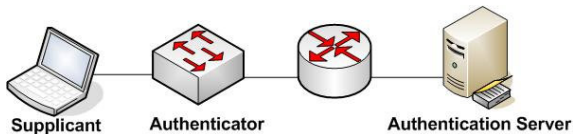
802.1X operational glue: L1 ↔ L2

- originally created for wired
- vendors cried out about WEP
- 'WPA Enterprise' ~ 802.11i

'WPA2 Enterprise' (aka 802.11i) = 802.11 + 802.1X



Overview of Systems Used In 802.1X

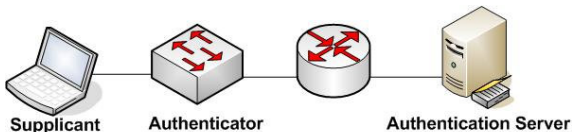


supplicant: workstation, printer, coffee machine, ...

authen: wifi AP, wired switch or even VPN conc.

auth serv: RADIUS server

How Does This 802.1X Malarkey Work Then?



EAPOL Start



EAP Request [A Identity]



EAP Response [S Identity]



EAP Request [OTP: OTP Challenge]



EAP Request [OTP: OTP Password]

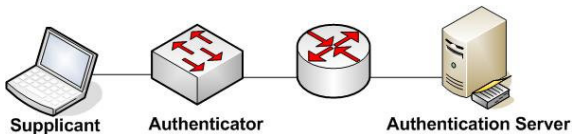


EAP Success



Port authorized!

Important Points Regarding 802.1X

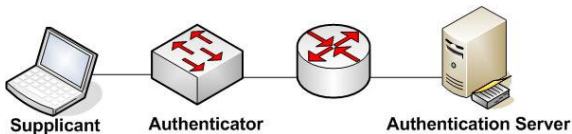


- supplicant:**
- needs to 'speak' EAP - legacy via mac-auth
 - user or machine based auth?
 - how to prime workstations?
- authen:**
- rogue AP's?
- auth serv:**
- auth backend can be anything
 - not necessarily your RADIUS server

On pain of death, you must:

- use a valid server side cert on RADIUS server
- client validates both root CA used and hostname

Important Points Regarding 802.1X

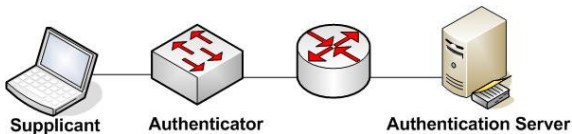


- supplicant:**
- needs to 'speak' EAP - legacy via mac-auth
 - user or machine based auth?
 - how to prime workstations?
- authen:**
- rogue AP's?
- auth serv:**
- auth backend can be anything
 - not necessarily your RADIUS server

On pain of death, you must:

- use a valid server side cert on RADIUS server
- client validates both root CA used and hostname

Important Points Regarding 802.1X

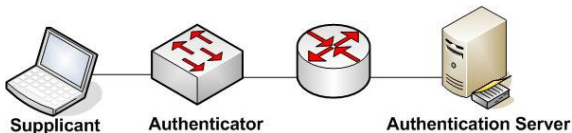


- supplicant:**
- needs to 'speak' EAP - legacy via mac-auth
 - user or machine based auth?
 - how to prime workstations?
- authen:**
- rogue AP's?
- auth serv:**
- auth backend can be anything
 - not necessarily your RADIUS server

On pain of death, you must:

- use a valid server side cert on RADIUS server
- client validates both root CA used and hostname

Important Points Regarding 802.1X



- supplicant:**
- needs to 'speak' EAP - legacy via mac-auth
 - user or machine based auth?
 - how to prime workstations?
- authen:**
- rogue AP's?
- auth serv:**
- auth backend can be anything
 - not necessarily your RADIUS server

On pain of death, you must:

- use a valid server side cert on RADIUS server
- client validates both root CA used and hostname

How Does This Help Though

- no need to maintain whitelists
- user credentials 'bootstrap' host authentication
- EAP provides encryption keys for AP ↔ workstation
- MitM/Evil Twin attacks are not possible - check certificate!
- MAC spoofing not profitable - this is security
- 100% certainty pinning `abuse@` to workstation/user

Bonuses, Especially for Wired 802.1X:

- per session policy (vlan, bw, qos, quota, fw, ...)
- full accounting data on workstation, but so what?
 - live historical (dis)connect and location
 - queries via SQL, but so what, I don't know SQL?
 - someone in admin department probably does though
 - SQL → Excel → Access → Leased WS Location



How Does This Help Though

- no need to maintain whitelists
- user credentials 'bootstrap' host authentication
- EAP provides encryption keys for AP ↔ workstation
- MitM/Evil Twin attacks are not possible - check certificate!
- MAC spoofing not profitable - this is security
- 100% certainty pinning `abuse@` to workstation/user

Bonuses, Especially for Wired 802.1X:

- per session policy (vlan, bw, qos, quota, fw, ...)
- full accounting data on workstation, but so what?
 - live historical (dis)connect and location
 - queries via SQL, but so what, I don't know SQL?
 - someone in admin department probably does though
 - SQL → Excel → Access → Leased WS Location

How Does This Help Though

- no need to maintain whitelists
- user credentials 'bootstrap' host authentication
- EAP provides encryption keys for AP ↔ workstation
- MitM/Evil Twin attacks are not possible - check certificate!
- MAC spoofing not profitable - this is security
- 100% certainty pinning `abuse@` to workstation/user

Bonuses, Especially for Wired 802.1X:

- per session policy (vlan, bw, qos, quota, fw, ...)
- full accounting data on workstation, but so what?
 - live historical (dis)connect and location
 - queries via SQL, but so what, I don't know SQL?
 - someone in admin department probably does though
 - SQL → Excel → Access → Leased WS Location

Dealing with Guests

Ad-hoc accounts creates problems:

- its time consuming - especially if for a 'day-pass'
- too much access? when to delete the account?
- rarely get advanced notice - you too eh?

Academics:

- okay if member of '.ac.uk'
- typically only want Internet access
- two '.ac.uk' identities is awkward
- RADIUS + proxying + glue → 'eduroam'

Joe Public:

- JANET AUP means identifying them
- DPA in a 'public' network (JANET is 'private')
- solved via alternative connectivity
- VLANs + alt. SSID + alt uplink
(BTOpenzone/The Cloud)

Dealing with Guests

Ad-hoc accounts creates problems:

- its time consuming - especially if for a 'day-pass'
- too much access? when to delete the account?
- rarely get advanced notice - you too eh?

Academics:

- okay if member of '.ac.uk'
- typically only want Internet access
- two '.ac.uk' identities is awkward
- RADIUS + proxying + glue → 'eduroam'

Joe Public:

- JANET AUP means identifying them
- DPA in a 'public' network (JANET is 'private')
- solved via alternative connectivity
- VLANs + alt. SSID + alt uplink
(BTOpenzone/The Cloud)

Dealing with Guests

Ad-hoc accounts creates problems:

- its time consuming - especially if for a 'day-pass'
- too much access? when to delete the account?
- rarely get advanced notice - you too eh?

Academics:

- okay if member of '.ac.uk'
- typically only want Internet access
- two '.ac.uk' identities is awkward
- RADIUS + proxying + glue → 'eduroam'

Joe Public:

- JANET AUP means identifying them
- DPA in a 'public' network (JANET is 'private')
- solved via alternative connectivity
- VLANs + alt. SSID + alt uplink
(BTOpenzone/The Cloud)

Sysadmin Mantra

Sysadmin Mantra

All Hardware Sucks, All Software Sucks. Some Sucks Less. . .

Remember, when the glossy brochures hit:

- you do not own all the kit on your network
- installing client software is not scalable
 - some solutions expect client AD membership!
- focus on isolation/detection, not prevention/NAC

Most importantly!

- Once deployed, your workload is equal/less than it is now

Considerations

Things to consider:

- single MAC/DHCP/ARP enforcement (wired mainly)
- multiple SSID's per AP
- 'thick' or 'thin' AP's
- flexibility of RADIUS server - FreeRADIUS proxying?
- non-'enterprise' clients connecting - non-Dell/Intel NICs
- supplicant to use - MS, Open1x, SecureW2, OS X, ...
- non-802.1X kit - VoIP, printers, door entry, ...
- avoid NAT if at all possible - "Makes Baby Jesus Cry"

Lot to absorb, so where to find help?

JANET Wireless Technology Advisory Service

Central Website at <http://www.ja.net/wtas>

- email service@ja.net - ask for JANET WTAS
- training courses
- lots of documentation, examples, case-studies
- JISCMail mailing list - wireless-admin@