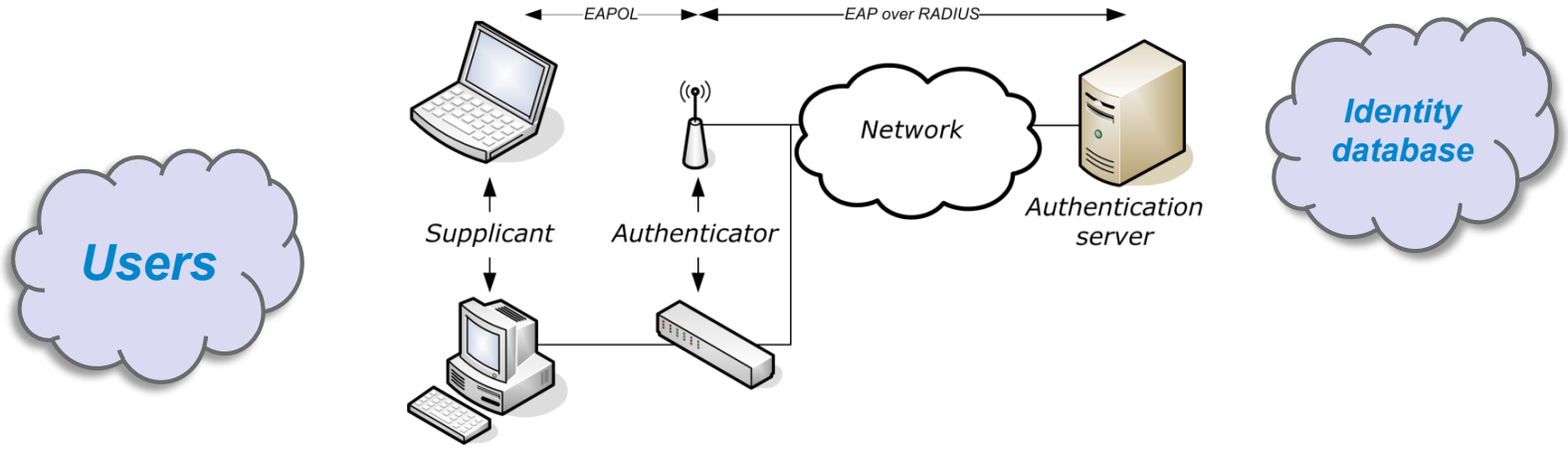
University of BRISTOL

Challenges for wide scale 802.1x deployment

March 2010

James J J Hooper

802.1x architecture

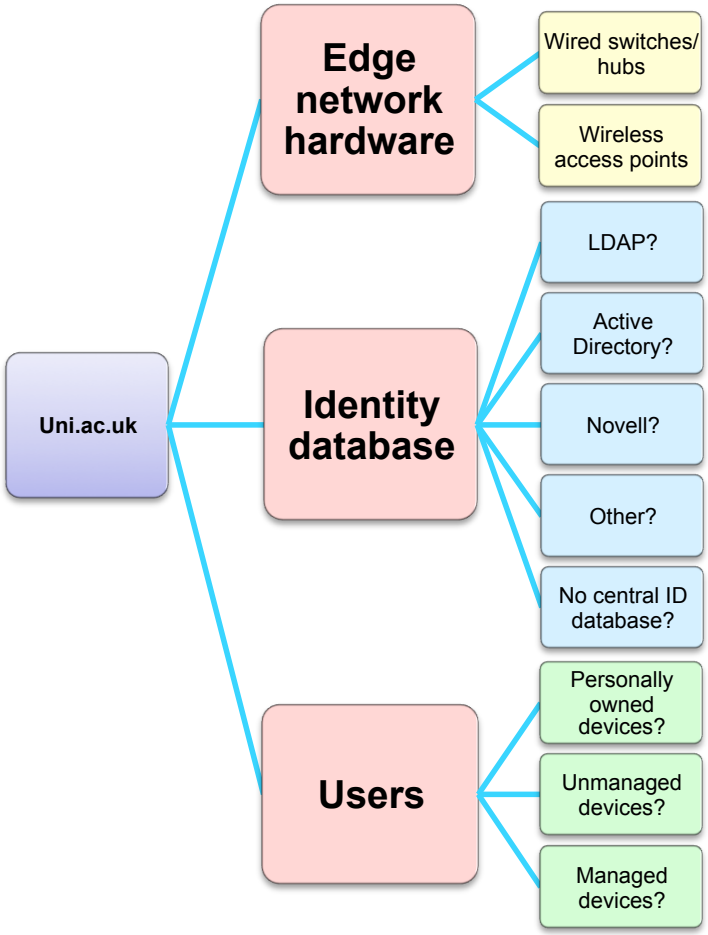


User » Supplicant » Authenticator » Authentication Server » Identity database

- Securely controlled access
- Potential for traffic encryption
- Enables NAP / NAC / TNC
- Not just a network on/off switch

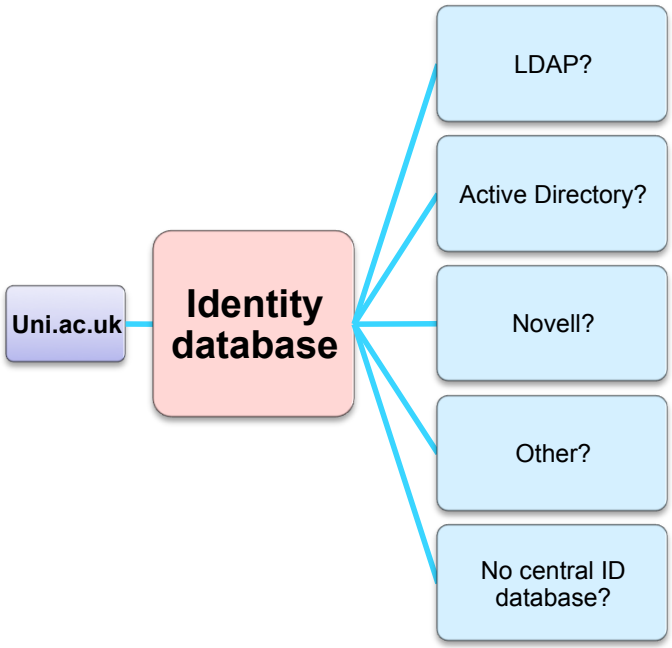
[Supplicant, authenticator, authentication server diagram adapted from: http://commons.wikimedia.org/wiki/File:Wat_is_EAP.png]

Planning: Existing elements



- Edge network devices need to be 802.1x capable.
- EAP Types: How credentials are stored in your ID database affects which EAP types you can use.
- Supplicant choice: Device and user nature influences which supplicant will be best for you.

Planning: ID DB & EAP types



- The hash used to store credentials in your ID database affects which EAP types you can use:

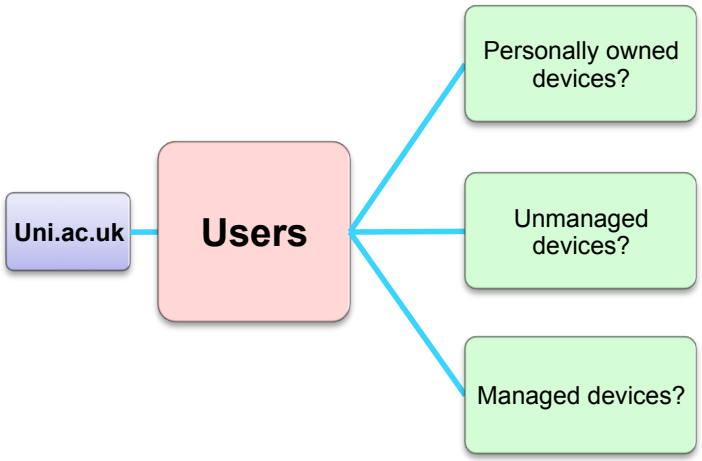
Passwords stored as → Compatible EAP types ↓	Plain text	NT hash	MD5 hash	SHA1 hash	Unix Crypt
PAP	☺	☺	☺	☺	☺
CHAP	☺	X	X	X	X
Digest	☺	X	X	X	X
MS-CHAP	☺	☺	X	X	X
PEAP	☺	☺	X	X	X
EAP-MSCHAPv2	☺	☺	X	X	X
Cisco LEAP	☺	☺	X	X	X
EAP-GTC	☺	☺	☺	☺	☺
EAP-MD5	☺	X	X	X	X
EAP-SIM	☺	X	X	X	X

- Which methods are available to communicate with the ID DB?

Communication method	Compatible EAP Types
ntlm_auth (part of Samba - used to communicate with MS Active Directory or a Samba Domain Controller)	PAP, MS-CHAP, EAP-MS-CHAPv2, PEAP
LDAP (Binding as the user authenticating)	PAP
PAM	PAP

Based on information from http://deployingradius.com - a good source of information about RADIUS & EAP types.

Planning: Supplicant choice

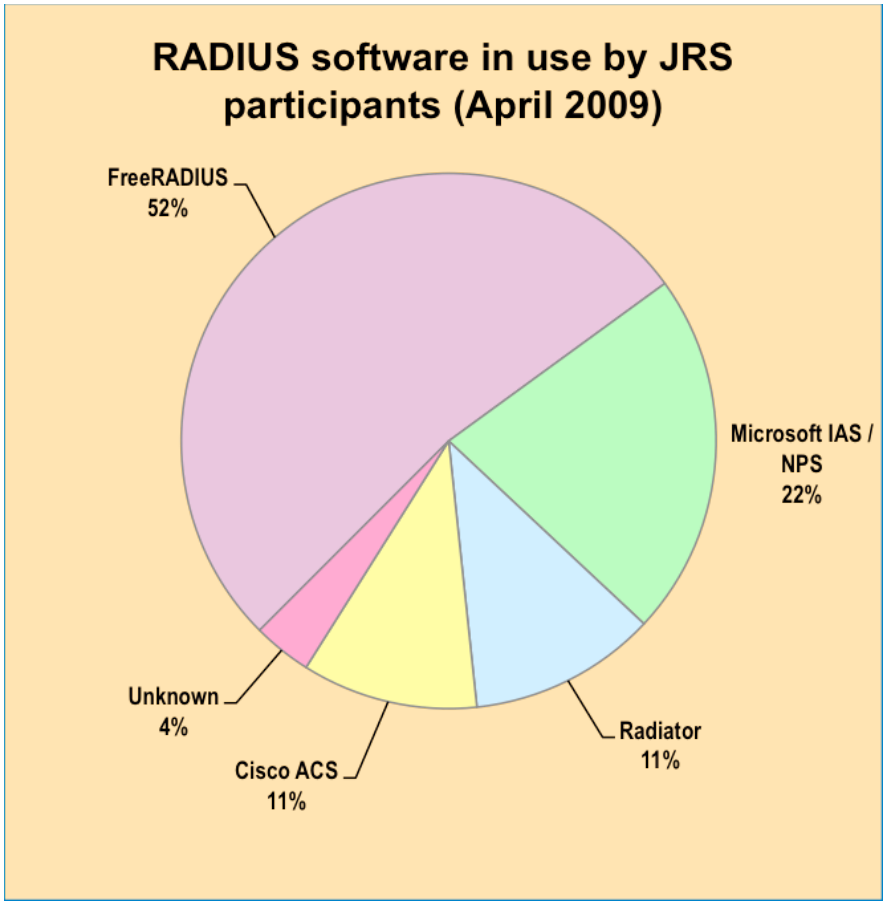


- Just provide user information?
- Use the OS built in one?
- Provide a supplicant program? (Mandate it?)
- Pre-configured?
- Use a “Configuration Wizard”?
- Consider personally owned machines and mobile devices

Planning: New elements

- RADIUS / EAP servers
- Resilience & scalability
- Management & monitoring
- Expectations

Planning: RADIUS servers

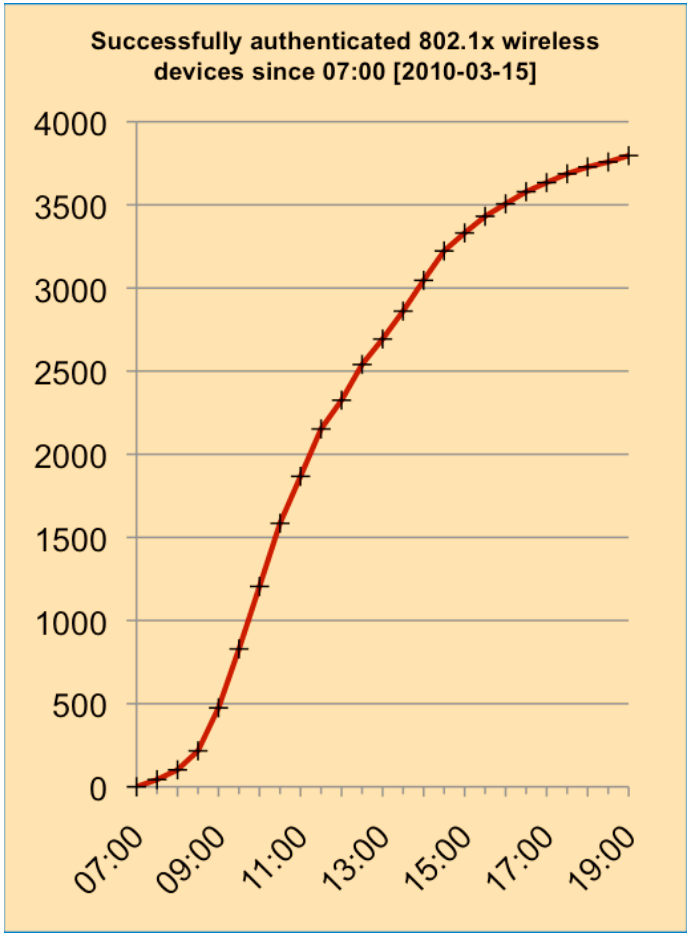


- Must be capable of communicating with your identity database
- Must support the desired EAP types
- Be flexible enough to implement any access / proxying policies you need.
- **Microsoft IAS / NPS** is included with MS Server OSs
- **FreeRADIUS** is open source. It's actively developed, fast, modular, scalable and has an extensive feature set.
- **Cisco ACS** comes as software to run on Windows, or as an appliance.
- **Radiator** is purchasable and runs on a variety of OSs. Radiator is used on the JRS UK national RADIUS proxy servers.

Planning: Resilience, scalability, monitoring and management

- The consequences of system failure are considerable
- After the initial setup, users really like 802.1x wireless
- Monitor the whole chain and each element individually:

  User » Supplicant » Authenticator » Authentication Server » Identity database



Expectations

- Wired 802.1x doesn't generally provide encryption over the wire
- Non-802.1x compatible devices – policy & technical options
- The average end user doesn't know about the settings required to make it work.
- Learning curve.

Bristol's implementation (1/3)

- Wireless: 4 SSIDs
  - An open unauthenticated SSID - captive portal, providing instructions for users and "setup wizards" for the most popular OSs.
  - eduroam - 802.1x wireless for staff, students & qualifying visitors.
  - An 802.1x SSID – solely for machines under the control of a wireless group policy – machine authentication only.
  - A PSK + web-redirect authenticated SSID for those that can't use eduroam / JANET (ADSL backhaul to the Internet).
- Wired:
  - Completed a small trial of Windows machines doing machine authentication. Further expansion is planned for the future.

Bristol's implementation (2/3)

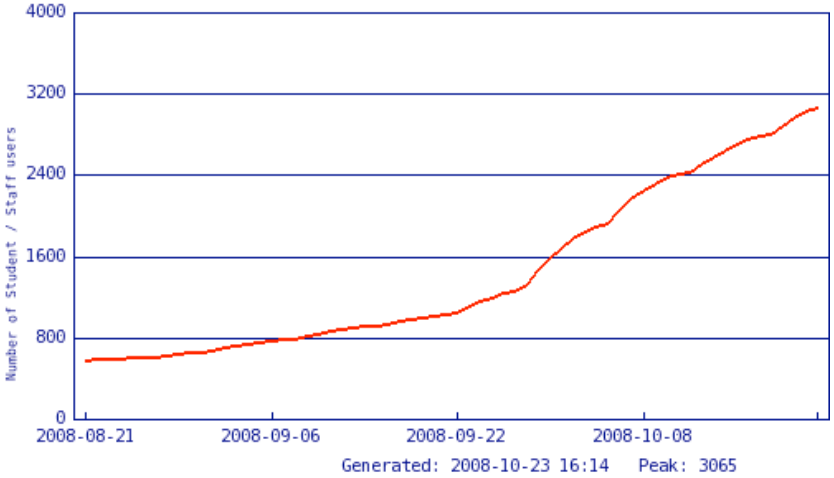
- EAP types:
  - Active directory is used as the credential store, so we support the MSCHAPv2 based types: **PEAP, TTLS/MSCHAPv2**
  - PEAP is natively supported in Windows. PEAP & TTLS/MSCHAPv2 are natively supported in Apple OS X & Linux.
- Supplicant:
  - We don't provide a separate supplicant program
  - We do use **Cloudpath XpressConnect**
  - Provide instructions for all popular OSs: http://www.wireless.bris.ac.uk/eduroam
  - Provide detailed generic instructions: http://www.wireless.bris.ac.uk/getconnected/services/eduroam/go-anything/

Bristol's implementation (3/3)

- RADIUS servers:
  - A long time ago we tried Win 2000 MS IAS with FreeRADIUS in front.
  - **FreeRADIUS** – Provides massive flexibility, very reliable.
  - **Samba** (ntlm_auth) – Allows FreeRADIUS to validate credentials against Active Directory
  - FreeRADIUS is also configured to connect to various other databases for user authorisation.
- Monitoring & Management:
  - RADIUS servers monitored via "**status-server**" requests.
  - EAP functionality tested with **eapol_test** (part of *wpa_supplicant*)
  - SNMP monitor of servers, with Nagios+Cacti for visualisation.
  - Certwatch to warn when certificates are about to expire.
  - Monitor DBs (tools depending on which DB)

Successes

- Self-help web pages and automatic setup wizards, including Cloudpath XpressConnect:
- Three weeks into the 2008 academic year, over 3000 users had connected themselves via WPA2 802.1x, even though the captive portal + VPN based wireless service was still available



- Machine authenticated wireless deployed via Group Policy:
- Deployment of laptops instead of desktops for staff becoming more common
- End users can not ‘break’ the wireless settings
- Use at conferences, home Wi-Fi unaffected

- Since changing to 802.1x wireless, user ratings have increased:
- 2007: 74% of users rated the wireless service as good/excellent
- 2009: 87% of users rated the wireless service as good/excellent

[University of Bristol wireless service users surveys 2007 & 2009. 454 (19.7%) and 745 (11.5%) respondents (response rate) respectively]

Problems

- Enforcement of certificate verification
- Spurious realms
- Timers
- User account lock outs
- Authentication DB reliability, authorisation DB speed
- NIC Drivers + OS hotfixes
- WOL, PXE boot, Unattended builds
- Active Directory schema
- IP space – more devices than users & many users

Further information

- Mailing lists:
  wireless-admin@jiscmail.ac.uk
  wireless-trapeze@jiscmail.ac.uk
  wireless-lan@listserv.educause.edu

  freeradius-users@lists.freeradius.org

  Contact support@ja.net if you need help implementing **eduroam** at your site.

- Web:
  http://wiki.freeradius.org – FreeRADIUS Wiki

  http://deployingradius.com – Deploying RADIUS: The book

  http://www.ja.net/roaming - JANET Roaming / eduroam

  http://www.eduroam.org/downloads/docs/GN2-08-230-DJ5.1.5.3-eduroamCookbook.pdf - GEANT2 Eduroam Cookbook

  http://www.cisco.com/univercd/cc/td/doc/solution/macauthb.pdf - Cisco's answer to non-802.1x capable devices

  http://su1x.sf.net - Windows native supplicant configuration tool (Gareth Ayres at Swansea University)

  http://open1x.sf.net – Open source supplicant for Windows & Linux

Challenges for wide scale 802.1x deployment

James J J Hooper

University of BRISTOL