Wireless Authentication with AD/LDAP, Radius, 802.1x and captive portals

The NSRC Auth demo kit

Sebastian Büttrich, NSRC
edit: June 2011

http://creativecommons.org/licenses/by-nc-sa/3.0/
What is the problem?

• Many campus networks have no personalized access control at all – just shared keys / passwords

• Campus networks that implement user authentication often suffer from
  – Multiple sign on
  – Repeated sign on when moving in network
  – Inconsistent user databases/lists – some on wireless APs, some in backend, some maybe just on paper
We can fix this!

- We can build **single sign-on**
- We can have **flexible solutions** while maintaining **one central user database**
- We can authenticate regardless of how the user is accessing the network – **wired, wireless on laptop, smart phone**
- We can do that in a way that **grows with your networks** – you can do small text files today and full Active Directory integration next year
Suggestion for a best practice

• **Backend user stores:**
  – LDAP, Active Directory, etc
  – SQL databases
  – Text based lists

• **RADIUS as authenticator**

• RADIUS can connect to all of them and more!

• All relevant clients (from classical desktop PC to modern smart phone) implement **supplicants**
Radius strengths

• RADIUS virtual servers: a strong tool for configuring flexible access – pointing at different user stores depending on where the request comes from, e.g. if it comes from the Guest AP VLAN/IP, I will ask the guest database, not my employee Active Directory
Radius strengths

- **RADIUS client configuration:** allow access and define *Shared Secret* on a per-client base -
  
  *Note: client here means the AP that is asking, not the end user!*

- Allows you to enable/disable flexibly, change dependent on time (e.g. Student Cafe access only after closing time of offices)
Strengths of approach

• No technology lock-in

• You may replace all parts of this chain by other products, as it’s all standard based
  – May use any commercial Radius product
  – May use any type of backend database or LDAP product
  – Low cost as well as expensive wireless systems can connect to it
Radius strengths

• Flexible front end:
  802.1x
  Captive Portals

• Lots of hardware offer RADIUS compatibility

• Can be mixed, for different user groups: e.g.
  – Captive portal for Cafe
  – Full 802.1x for Finance department
802.1x on client

- Works on all relevant clients
- One time setup
- Windows integration:
  You can configure 802.1x to use the existing user credentials – this means, you only log on to your PC/domain and do not have to enter any user info again
Wireless security – one possible architecture

- > LDAP
- > AD
- > MySQL
- > Text
- > other
Wireless security – one possible architecture
Hands-on Lab

We will work in this order

• Configure Access Points to use 802.1x
• Connect to existing Radius server
• Configure laptop clients, smart phones, etc
• If we have enough time:
  Install and configure our own Radius/LDAP server
Hands-on Lab: example network setup

University LAN

Main router/switch (e.g. a blue Linksys box)

10.1.1.1 Gateway for LAN
serving DHCP on 10.1.1.100 to 10.1.1.200
LAN 10.1.1.0/24 (need BIG SWITCH here)

AuthKit AP1 AP2 AP3 ...
10.1.1.2

The APs have eth interface: 10.1.1.2xy
with xy = number of group
Hands-on Lab: example network setup

University LAN

| Main router/switch (e.g. a blue Linksys box) |
| 10.1.1.1 Gateway for LAN |
| serving DHCP on 10.1.1.100 to 10.1.1.200 |
| LAN 10.1.1.0/24 (need BIG SWITCH here) |
|_________________________________________|
|_________________________________________|
|_________________________________________|
| AuthKit   AP1   AP2   AP3   ... |
| 10.1.1.2 |

APs will be configured to bridge, NOT route, so that we simulate a real Campus LAN with roaming capabilities within the subnet 10.1.1.0
Wireless security – one possible architecture

USIU University LAN

Main router/switch (currently: the blue box)

10.1.1.1 Core / Border Router

Auth Gateway AP1 AP2 AP3 ...

Diagram: Wireless network architecture with routers, switches, and access points labeled.