Fondation RESTENA
RedIRIS WiFi-Workshop
31 March 06

Security and Privacy Considerations in eduroam

Stefan Winter <stefan.winter@restena.lu>

Overview

- Security in wireless networks – general part
  - the early days: hidden SSIDs, MAC auth, WEP
  - Dynamic WEP, WPA and WPA2
  - “Enterprise Security”: adding IEEE 802.1X to the mix
- Security settings in eduroam
  - User authentication mandatory
  - Sensible use of 802.1X
  - client configuration
- Enhancing user privacy
  - minimising the disclosed information
- abuse tracking

Wireless security
The early days

- hidden SSIDs
  - do not broadcast network name (SSID) in beacons
  - everybody can see that a network is present, but need its name in order to associate
  - nice try, but: valid users send network name in the clear when associating → **sniffing attack possible!**
- MAC address authentication
  - in theory, every NIC has a unique, unchangeable MAC address
  - in practice:
    `ifconfig eth1 hw ether 00:00:DE:AD:BE:EF`

Wireless security
The early days (2)

- WEP
  - attempts to encrypt traffic
  - specification seriously flawed:
    - original key length too short (64-bit)
    - only part of those 64 bit are “secret” → 40 bit (5 characters) long user keys, 24 bit IV
    - mathematically weak crypto algorithm: depending on IV, parts of the “secret” key are deductible → **sniffing attack possible!**
    - key is static
  - various, unstandardized key lengths or workarounds

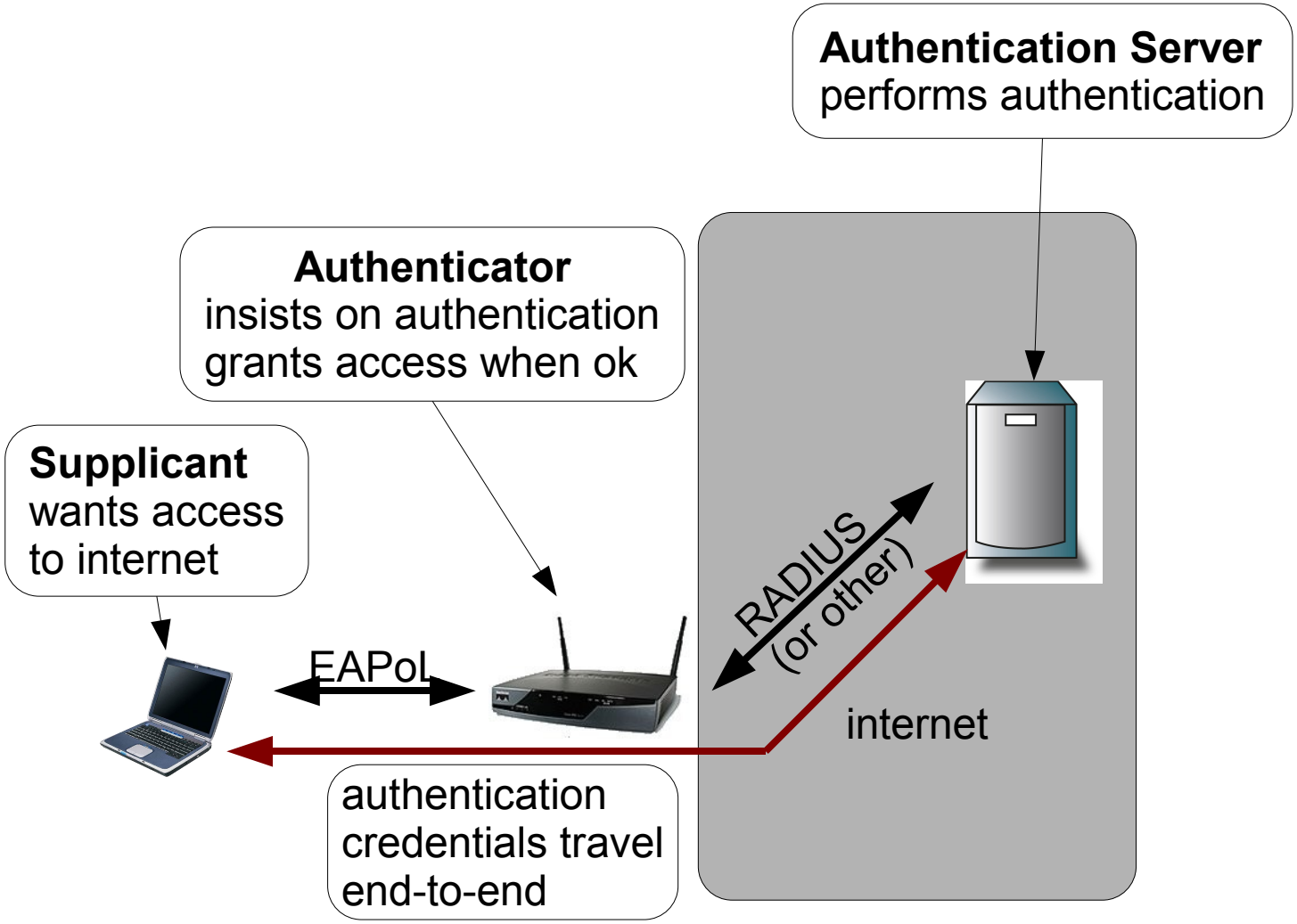
Wireless Security
Dynamic WEP, WPA, WPA2

- WEP disaster led to further development
  - dynamic WEP: an external source provides keying material on a regular basis, AP and client change their (still weak) keys accordingly
  - WPA: redesign crypto algorithm to avoid IV problem (WPA is no real standard: snapshot of what later became WPA2)
    - WPA-TKIP:
      - longer IV, makes password sniffing harder
      - password used as seed to create per-packet unique keys
      - replay protection
    - WPA-CCMP (aka WPA-AES):
      - AES as cryptographic algorithm

Wireless Security
Dynamic WEP, WPA, WPA2 (2)

- WPA2
  - mandate better key management and key exchange
  - aka. RSN (“robust security network”)
- WPA/WPA2 offer two operation modes
  - “Personal” - pre-shared key
  - “Enterprise” - combined with an external authentication source, i.e. IEEE 802.1X (see next slides)
- older hardware not WPA/WPA2 capable

Wireless Security
IEEE 802.1X



Wireless Security
IEEE 802.1X - EAP

- EAP (Extensible Authentication Protocol) is a container protocol that can carry arbitrary authentication payloads
- Supplicant can encapsulate his desired protocol in EAP and send the authentication data to the authenticator
- communication is on layer 2
- authentication payload travels through to authentication server – depending on the payload, opaque to authenticator

Wireless Security
IEEE 802.1X – after first hop

- authenticator can talk at layer 3 (IP)
- encapsulates EAP data in a higher-layer protocol and transports to authentication server
- authentication server evaluates EAP payload
  - either performs auth himself, sending back a yes/no answer to authenticator
  - or delegates auth decision to another authentication server (as in the case of eduroam: delegation by realm)
- protocols for encapsulating EAP payload:
  TACACS+ (obsolete), RADIUS (de-facto standard), Diameter (yet-to-come), RADSec (extended RADIUS)

Wireless Security
What EAP payload type?

- No clear text pass on the wire! → forget EAP-PAP
- Trust no one! → only methods with mutual authentication; forget EAP-MD5
- Protocols with mutual, certificate-based authentication are:
  - EAP-TLS (requires both server and user certificates)
  - EAP-TTLS (server authenticates via cert, user sends credentials within TLS tunnel)
  - EAP-PEAP (like EAP-TTLS, with encrypted tunnel payload)

IEEE 802.1X
Enterprise Security - Benefits

- all network users are known (and traceable if they do nasty things)
- different service levels depending on user type possible: dynamic VLAN assignment
- no shared key floating around
- re-keying in arbitrary intervals
- secure roaming possible

Wireless Security
Commercial roaming

- Commercial roaming: “Web redirect”
  - unsecured WLAN, you get an IP w/o authentication
  - access to internet blocked by ACL until user authenticates at a web site
  - on first access: redirected to authentication web site; enters his credentials
  - afterwards, ACL allows access for user's IP
- drawback 1: connection not secured, IP data is broadcasted in clear text
- drawback 2: user forced to enter credentials on a untrusted web site

Wireless Security
VPN over untrusted WLANs

- Point of view: don't care about this complicated WLAN security stuff, create an open network
- only allow VPN traffic, which takes care of encryption and authentication
- works, but: how to do roaming?
  - all users connect to your VPN, get authenticated via RADIUS hierarchy backend: drawback: user needs to enter credentials on a remote (untrusted?) site
  - open VPN ports for roaming partner's VPN boxes (drawback: poor scalability)
  - open VPN ports for world (drawback: NREN AUP?)

eduroam
Choice of technology

- as seen, a mixed bag of technologies to choose
- quite a lot of them are a no-go for roaming:
  - hidden SSIDs: this is a semi-public service after all
  - MAC authentication: no seamless roaming
  - static WEP: no seamless roaming
  - WPA/WPA2 “Personal”: no seamless roaming
- and some suffer of drawbacks
  - web redirect: spoofing risk, credentials to untrusted
  - VPN: doesn't scale to European level / breaks AUP

eduroam
Remaining options

- Encryption
  - dynamic WEP with IEEE 802.1X
  - WPA/WPA2 Enterprise (also IEEE 802.1X)

- Authentication
  - only EAP methods with mutual authentication
  - proper client configuration to ensure mutual trust
  - secure RADIUS backend as best as we can (or even move on to something better than RADIUS)

eduroam
Mutual authentication

- Identity providers set up a RADIUS Server that identifies itself with certificate
- The choice of accepted EAP payload types is in principle the IdP's own choice ...
- ... but the remote organisation may decide to block authentication attempts that use an insecure protocol
- EAP-TTLS, EAP-TLS, EAP-PEAP are always on the safe side

eduroam
Server certificate validation

- more difficult than in browser case
  - in browser, user explicitly enters the server name
  - in 802.1X he enters his user name
  - therefore, automatic checking CN=input not possible
- higher certificate requirements
  - in typical browser case, “any trusted root CA” is sufficient
  - in 802.1X, you want to connect to exactly one server from exactly one CA
- proper client configuration is essential to prevent spoofing

eduroam
Risks in certificate validation

- Case 1: User doesn't validate cert at all
  → will send credentials to any server, incl. bad guys
- Case 2: any trusted root CA
  → will send credentials to any server with a valid cert, possibly to a bad guy who registered badguy.com at VeriSign
- Case 3: only CA that issues the server cert
  → close to ideal, but: if that CA is a “public” CA like VeriSign, he could still end up at badguy.com
- Case 4: only that CA, plus explicit server name
  → ideal, credentials will only go to the right server

eduroam
Proper client configuration

- CA only for eduroam servers: case 3 secure
- How to get towards case 4?
  - educate users?
  - audit user settings?
  - provide pre-configured client program
- an “eduroam client”: way to go!
  - SecureW2 is an open source EAP-TTLS client and has pre-configuring options
  - Intel PROset Wireless can load “profiles”
  - developing an own codebase for eduroam client is currently discussed in JRA5

eduroam
RADIUS hierarchy

- RADIUS is a rather old protocol with some peculiarities
  - UDP transport
  - client-server communication relies on static IP addresses and a shared secret
  - only very few parts of auth packet are encrypted
- anyway, it is the state-of-the-art protocol
- circumvent weak encryption by using secure EAP payloads (that use TLS, and don't need to rely on RADIUS security)

eduroam
move on to a new protocol?

- Diameter: designated successor of RADIUS
  - uses TCP or SCTP
  - peer validation with TLS certificates
  - avoids the hierarchy traffic aggregation by dynamic server discovery
  - lots of nice other features
  - but: no suitable implementations yet
- intermediate solution: RADSec
  - still transports RADIUS packets, but over TCP/SCTP and validates peers with TLS certificates
  - i.e.: full RADIUS packet encryption, reliable transport

eduroam (-ng) RADSec

- implementation of the RADSec extensions was provided by OSC (“Radiator”)
- test hierarchy was set up to test functionality
- result: things mostly worked as expected (some minor bugs, quickly fixed)
- an extra step was tried as well: dynamic peer discovery with DNS NAPTR records
  - nice idea, but: without DNSSEC no secure method to validate server identity
  - implementation way too buggy for real use

eduroam
user privacy

- in RADIUS: most attributes traverse the network unencrypted
- intermediate IP hops can read some data
  - supplicant's MAC address
  - EAP outer user name
  - current location (at least coarsely)
  - VSAs
- if authenticator sends accounting tickets, more
  - complete session data (time, amount of data transferred), associated with outer EAP identity
- sending real user name in outer EAP bad idea

eduroam (-ng)
Changes with RADSec

- TLS encryption between RADIUS hops
  - intermediate IP hops don't see data
  - still, the involved RADIUS servers do
- not entire hierarchy can speak RADSec
  - no authenticators do; communication between authenticator and first RADSec server is open
  - eduroam participants currently not obliged to use RADSec → unencrypted plain RADIUS in between possible
- (pre-)configure clients to use anonymous outer identity

eduroam abuse handling

- when using 802.1X, you need a means of correlating MAC and IP
  - 802.1X authenticates (and binds user name to) MAC address
  - abuse is happening on IP level
  - so, to track people MAC <-> IP binding is important
- mainly two options
  - log DHCP to find out which MAC got which IP (good, not perfect: user may change his IP manually)
  - ARP sniffing: also picks up a changed address

eduroam abuse handling (2)

- don't rely on EAP outer identity
  - person may have used anonymous outer identity, or worse: a valid outer EAP identity belonging to someone else
  - but inner EAP identity is TLS-encrypted and not visible to visited institution
- solution: ask IdP, he has info about inner identity
  - needs synchronised time source for logs
  - users can be sure no one is tracking them “just for fun” – admins need a good reason when calling home for user info

Links and References

- 802.11 Wireless Networks, 2nd Edition
  (O'Reilly)
- RADSec Whitepaper
  http://www.open.com.au./radiator/radsec-whitepaper.pdf
- SecureW2
  http://www.securew2.com./
- GN2 JRA5 Deliverables
  http://www.geant2.net./server/show/nav.778
  (DJ5.x.y; coming soon: policy document DJ5.1.3-2)
- TERENA TF-Mobility Website
  http://www.terena.nl./activities/tf-mobility/

The end

Thank you!