Understanding

Server Certificate Validation

and 802.1X Update

Kevin Koster

Founder & Principal

Cloudpath Networks

Special Thanks To:

Robert Hopley, RSA

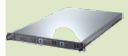
Chris Hessing, Cloudpath & OpenSEA

Alex Sharaz, University of Hull

Louis Searchwell, JANET

Damien Shaw, JANET

Cloudpath NETWORKS

	Wireless Threats	How To Mitigate	Open	WPA-PSK	WPA-Enterprise
	Unauthorized User or Device Accesses Network	User Authentication to Network Authentication via 802.1X is inherent in WPA/WPA2-Enterprise	✓ Captive Portal	✓ Captive Portal	✓ Built-in
	Wireless Snooper Intercepts User's Traffic	Over-The-Air Encryption For protecting data, WPA/WPA-2 Enterprise inherently uses per-user rotating keys.	✗	✓	✓
	User Provides Credentials to Imitation (Rogue) Access Point	Network Authentication to User PEAP/TTLS/TLS implement "server certificate validation" (SCV) to verify authentication is occurring with trusted RADIUS server.	✗	✗	✓

High-level PEAP/TTLS Authentication Flow

I'm "Outer Identity" & I want to authenticate

Here's my server cert. Give me your credentials.

I'm "Bob" and my password is "AllYours".

Thanks, welcome to the network.

Quick. Easy. Secure.

High-level PEAP/TTLS Authentication Flow

I'm "Outer Identity" & I want to authenticate

Here's my server cert. Give me your credentials.

I'm "Bob" and my password is "AllYours".

Should I give my credentials to this RADIUS server?

Quick. Easy. Secure.

Should I Trust the RADIUS Server?

Keep in mind:

No PHY layer validation of AP/Switch

- AP may or may not be legitimate

AP/Switch selects RADIUS server, not client

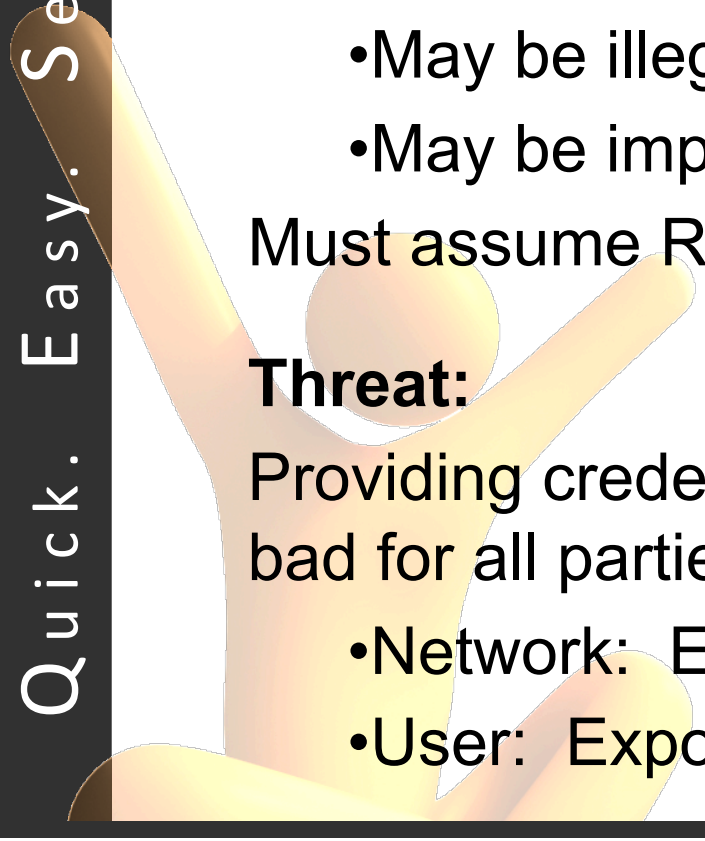
- May be illegitimate network
- May be improperly configured network

Must assume RADIUS server may be illegitimate

Threat:

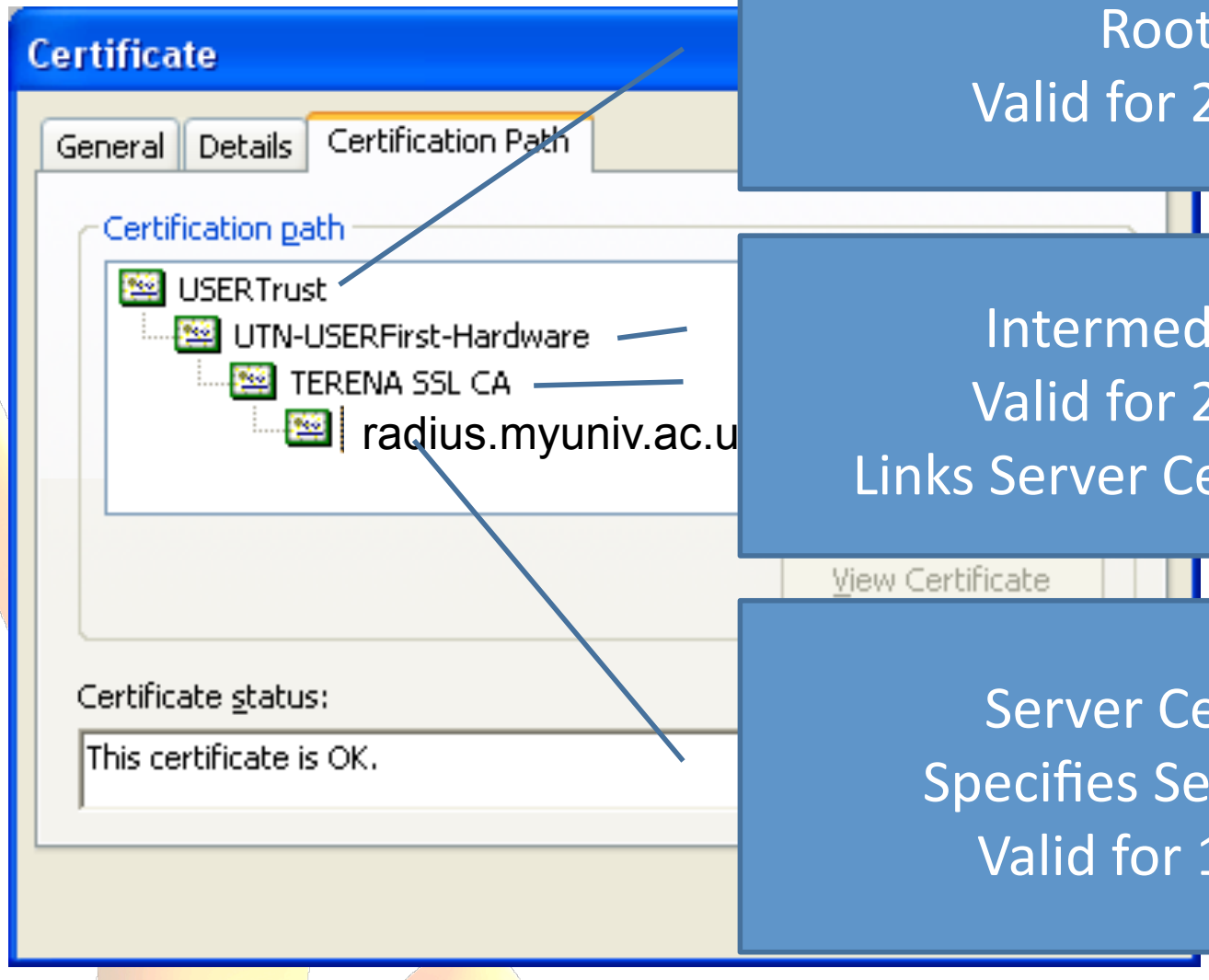
Providing credentials to illegitimate RADIUS server is bad for all parties.

- Network: Exposed to illegitimate access
- User: Exposed to network sniffing & manipulation



Quick. Easy. Secure.

Server Certificate Information



Root CA
Valid for 20+ Years

Intermediary CAs
Valid for 20+ Years
Links Server Cert to Root CA

Server Certificate
Specifies Server Name
Valid for 1-3 Years

Certificate Viewed in Windows CertMgr

Quick. Easy. Secure.

Should I Trust the RADIUS Server?

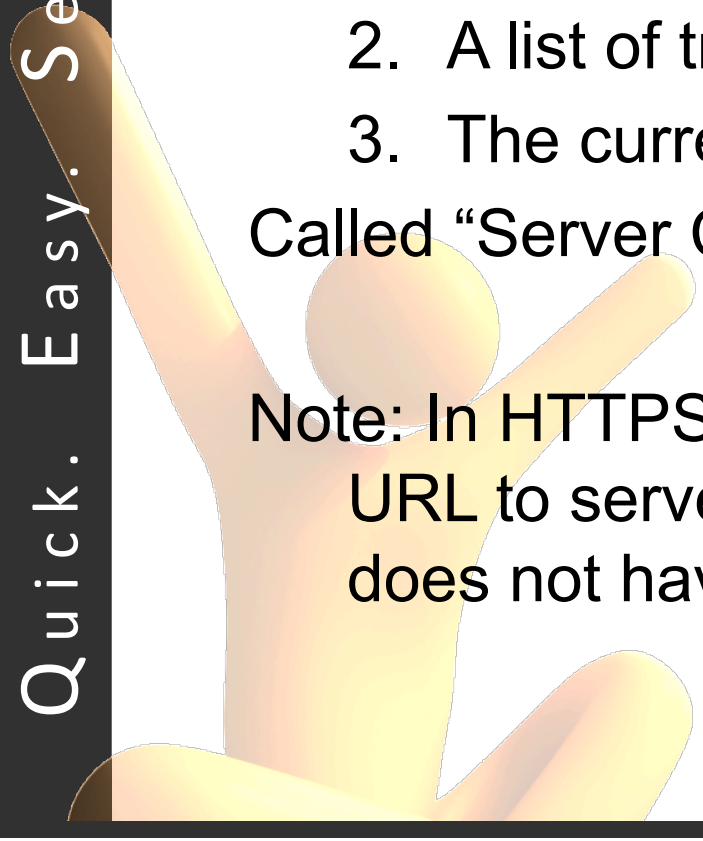
Establishing Trust:

Before passing credentials, client should validate RADIUS server's certificate against:

1. A list of trusted root CA(s).
2. A list of trusted common names (server names).
3. The current time.

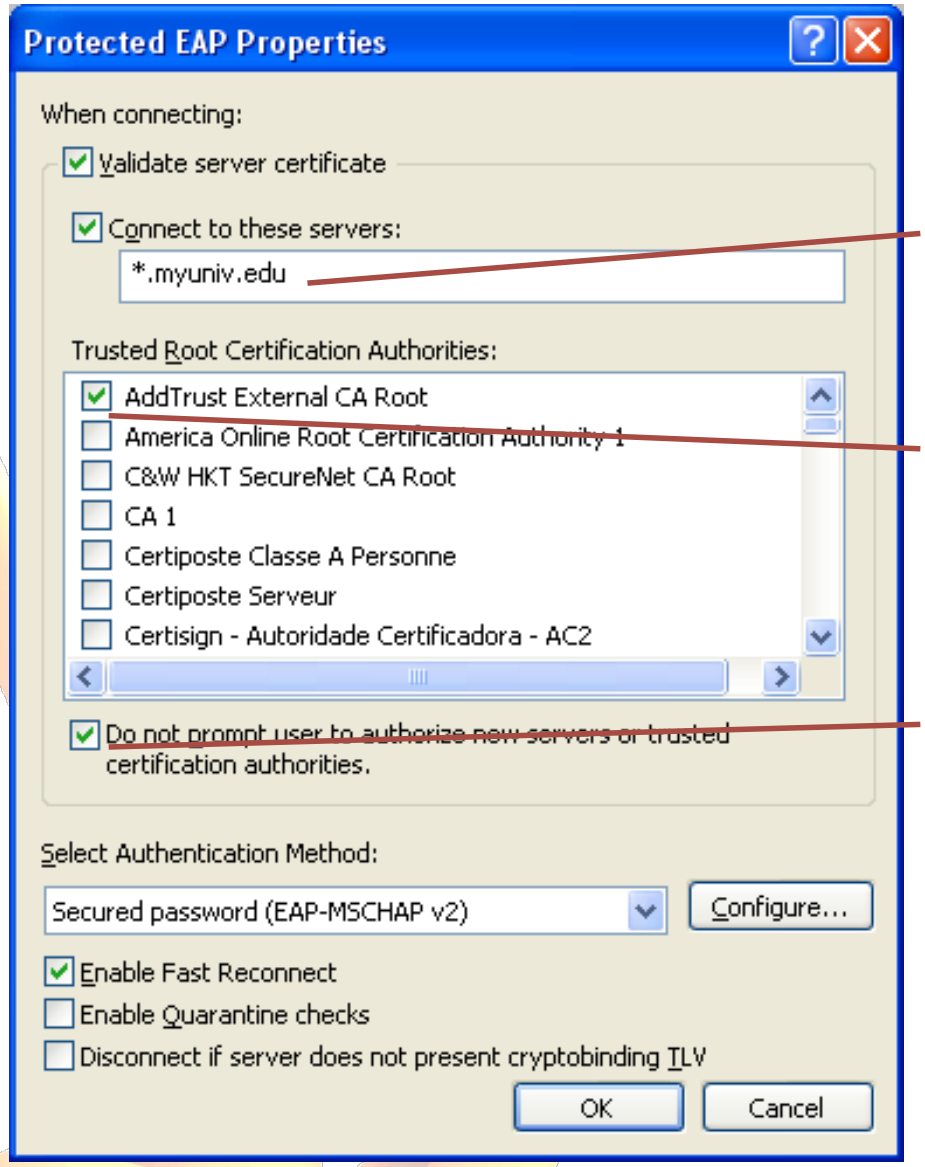
Called "Server Certificate Validation" (SCV)

Note: In HTTPS, trust is established by comparing URL to server name in server's certificate. 802.1X does not have a URL to base trust on.



Quick. Easy. Secure.

Windows Configuration



Verify that the server certificate is:

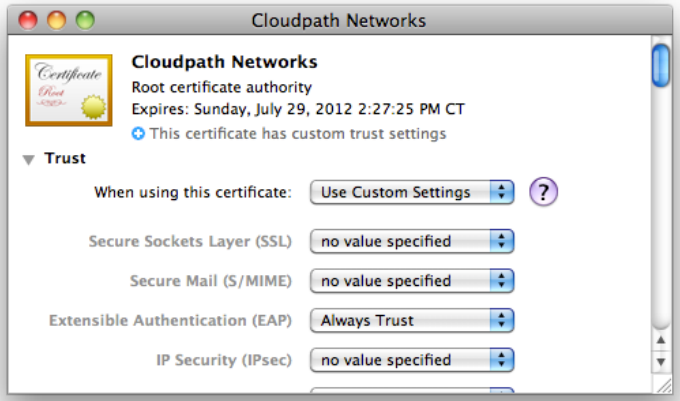
1. For any server in myuniv.edu domain (may be single name, list of names, or wildcard)
2. Signed by AddTrust External CA Root (if multiple by name, look at thumbprint by dbl-click).
3. If certificate is invalid, authentication will be refused if certificate is untrusted (don't ask user to interpret cert).

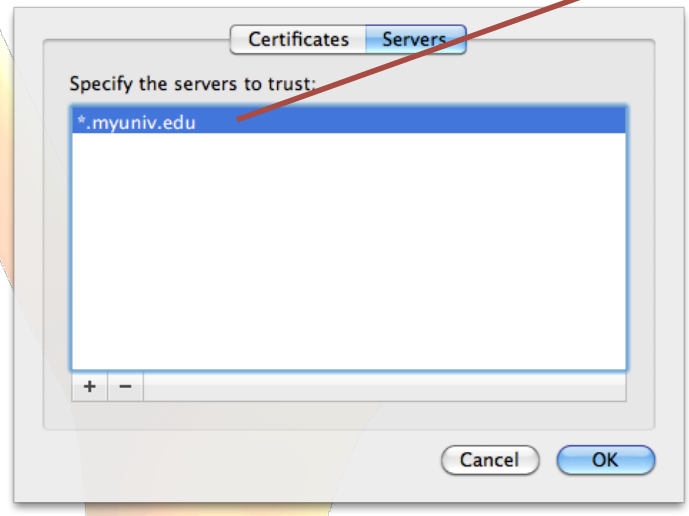
Wireless - Configured per SSID

Wired – Configured per NIC

Quick. Easy. Secure.

Mac OS X Configuration





Root CAs are marked “trusted” for EAP (802.1X) in Keychain.

Trusted Root CAs are generic, not tied to single SSID.

Snow Leopard & iPhone allow SSID to specify trusted server names.

If untrusted server cert, will always prompt unless:

- AllowTrustException = false on iPhone
- Server name specified on Snow Leopard

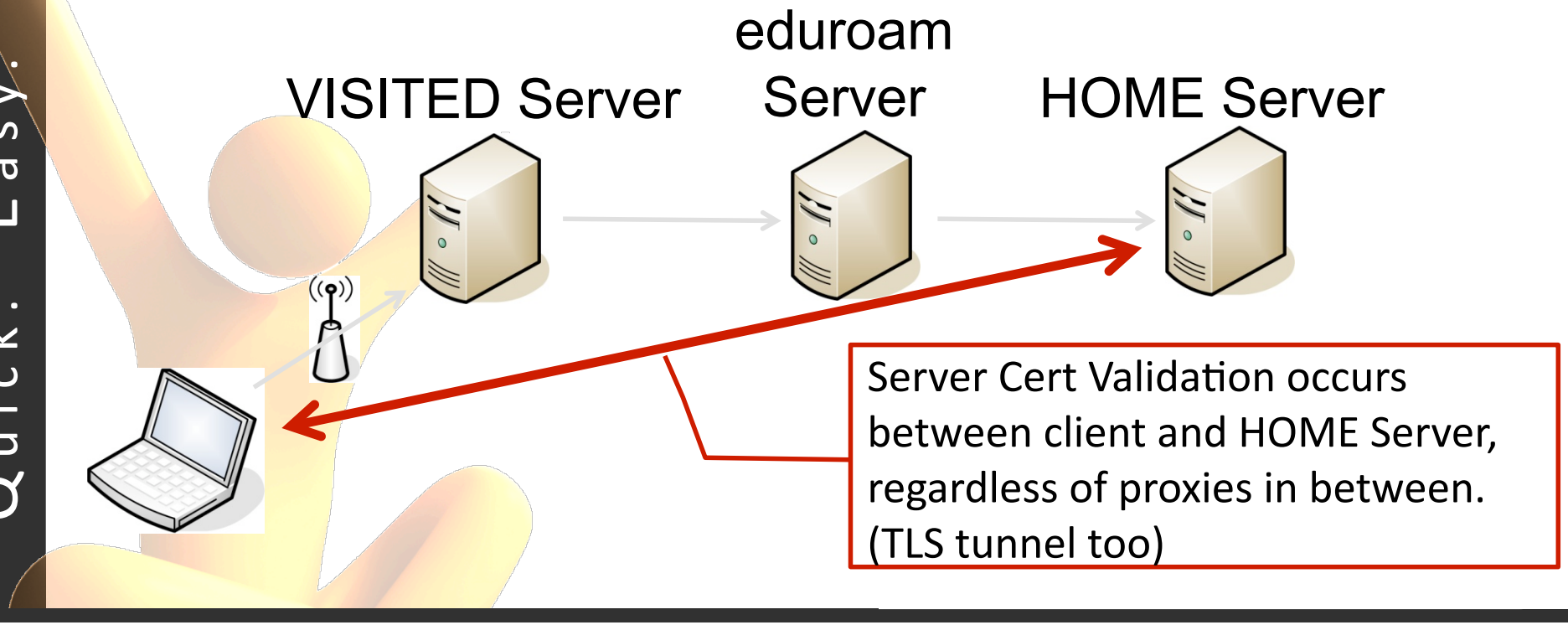
Quick. Easy. Secure.

Certificate–Related Threats	Detection
Certificate issued to “Hacker”, Signed by private “Hacker CA”.	Detectable because Root CA is not trusted.
Certificate issued to “Hacker” Signed by real “Verisign CA”.	Root CA is trusted, but detectable because server name is not trusted.
Certificate issued to “radius.myuniv.edu” Signed by private “Hacker CA”.	Detectable because Root CA is not trusted. If prompted, user is likely to improperly trust due to server name.
Certificate issued to “radius.myuniv.edu” Signed by hacker’s private CA named “Verisign CA”.	Detectable because Root CA is not trusted. If prompted, user (& IT staff) is likely to improperly trust.

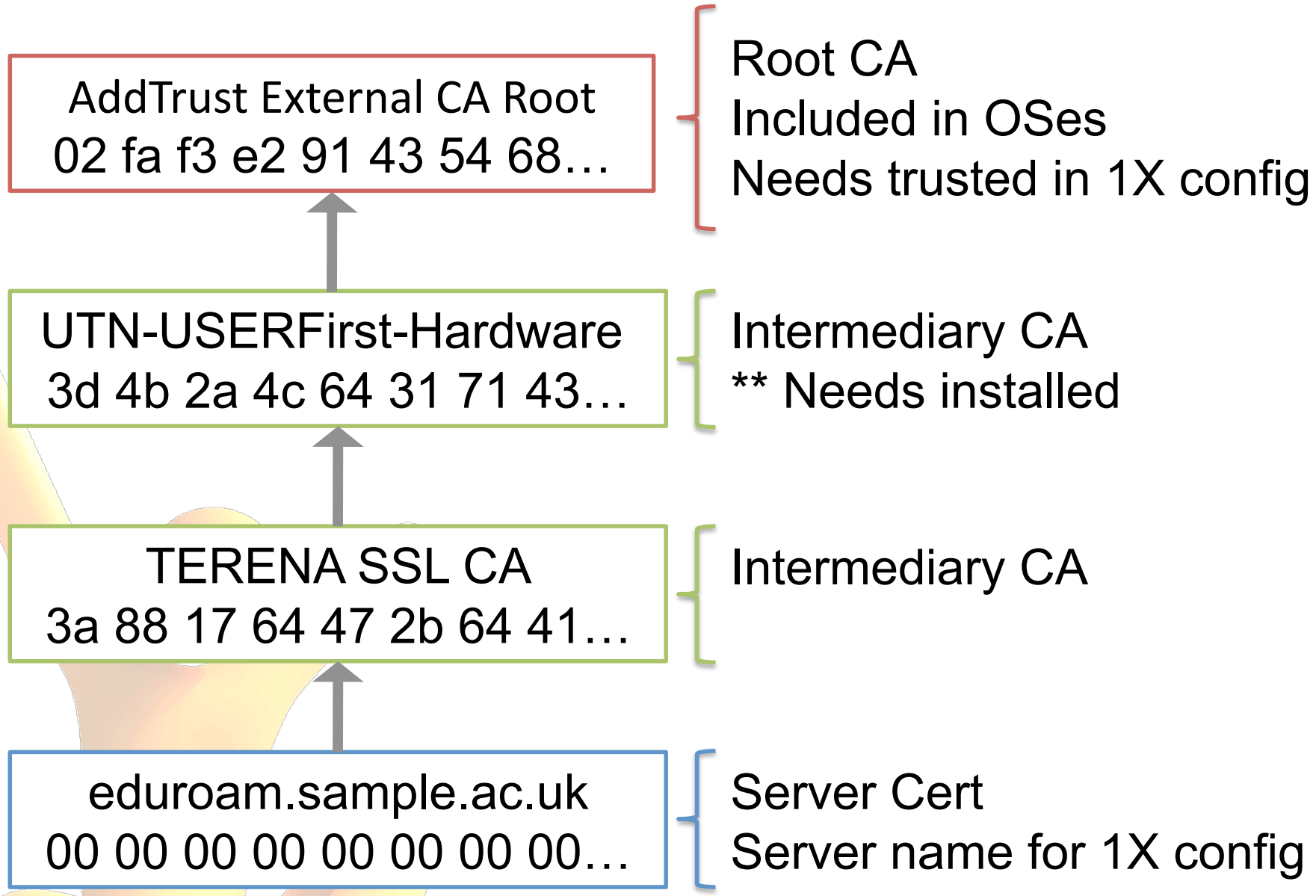
eduroam & Server Cert Validation

Quick. Easy. Secure.

- eduroam uses RADIUS proxy protocols.
- Server certificate exchange occurs between client and HOME RADIUS server.
- Fully-specified server certificate validation is critical within eduroam.



New JANET CA Structure



Quick. Easy. Secure.

JANET CA Chaining Confusion

Quick. Easy. Secure.

AddTrust External CA Root
02 fa f3 e2 91 43 54 68…

UTN-USERFirst-Hardware
04 83 ed 33 99 ac 36 08…

UTN-USERFirst-Hardware
3d 4b 2a 4c 64 31 71 43…

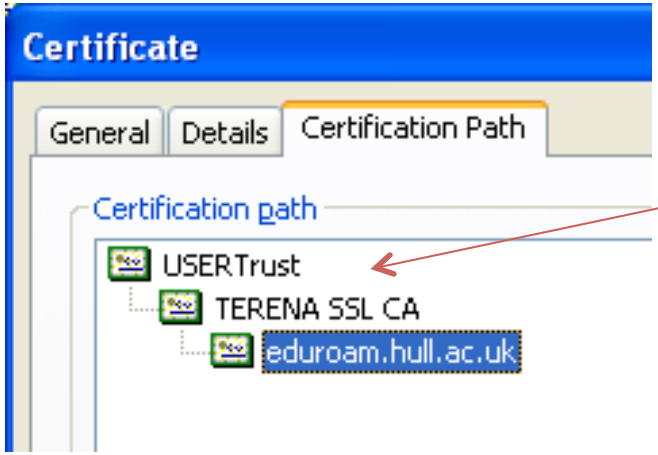
By Default, The OS Will **INCORRECTLY** Chain To The Old UTN-USERFirst-Hardware.
(Tested on Windows & Mac)

TERENA SSL CA
3a 88 17 64 47 2b 64 41…

eduroam.sample.ac.uk
00 00 00 00 00 00 00 00…

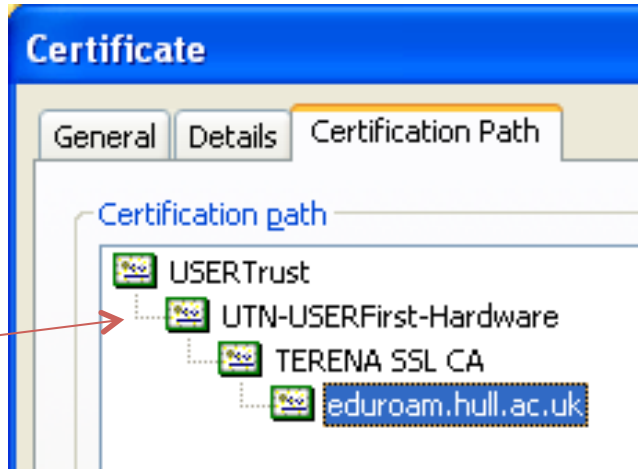
Chains incorrectly when old Root CA is installed but not the new Intermediate CA.

JANET CA Chaining Confusion



Wrong.

Correct.



Why OS Confusion:

The two UTN-USERFirst-Hardware certs are copies:

- Old one is unsigned, therefore Root CA.
- New one is signed, therefore Intermediary CA.

To Resolve:

- Install the new UTN-USERFirst-Hardware (3d 4b 2a…) certificate as an Intermediate CA.
- Do not need to delete the old UTN-USERFirst-Hardware certificate.

Quick. Easy. Secure.

Recent OS Changes

Windows 7 includes PEAP “Identity Privacy”

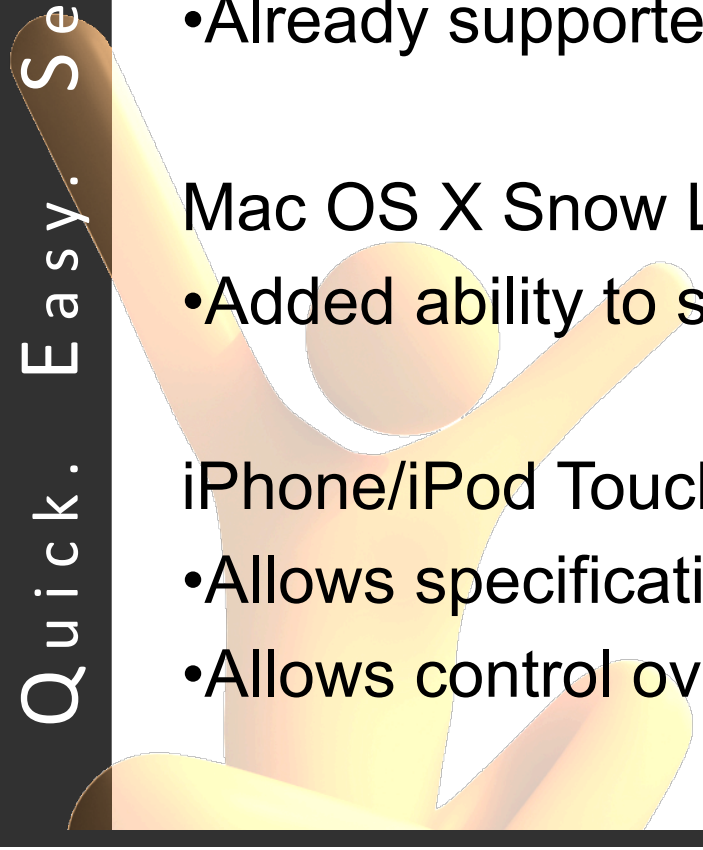
- Allows control over outer identity (similar to TTLS)
- Most common use is “anonymous”
- Already supported for PEAP on Mac OS X

Mac OS X Snow Leopard (10.6)

- Added ability to specify trusted server name(s) per SSID

iPhone/iPod Touch

- Allows specification of trusted server name(s) per SSID.
- Allows control over prompting when cert is incorrect.



Quick. Easy. Secure.

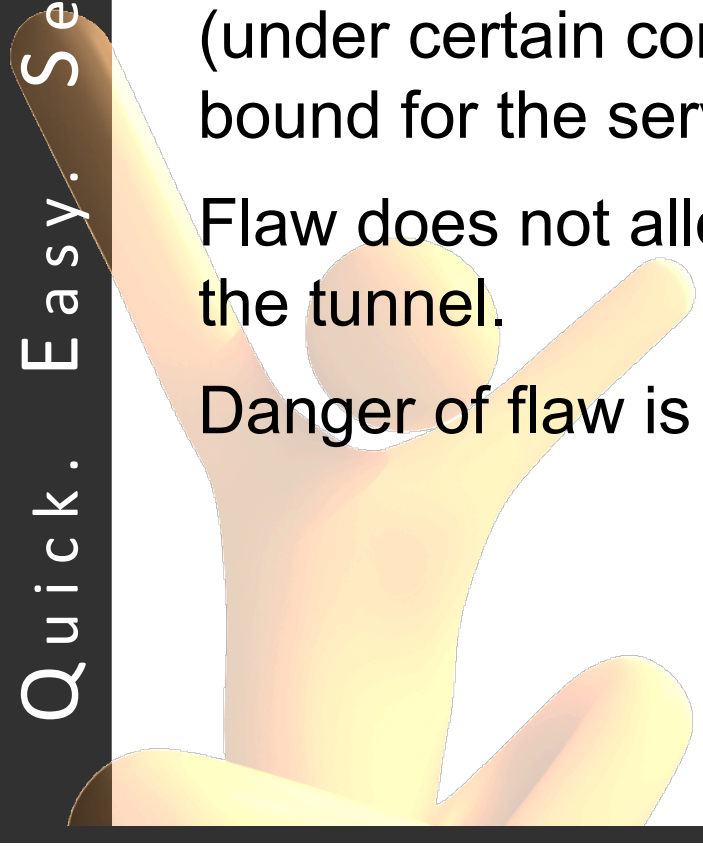
TLS Vulnerability & 802.1X

In late 2009, a fundamental flaw in the TLS standard was discovered.

Flaw is related to renegotiation and allows a hacker (under certain conditions) to inject data into the tunnel bound for the server.

Flaw does not allow hacker to see communication within the tunnel.

Danger of flaw is dependent on application using TLS.

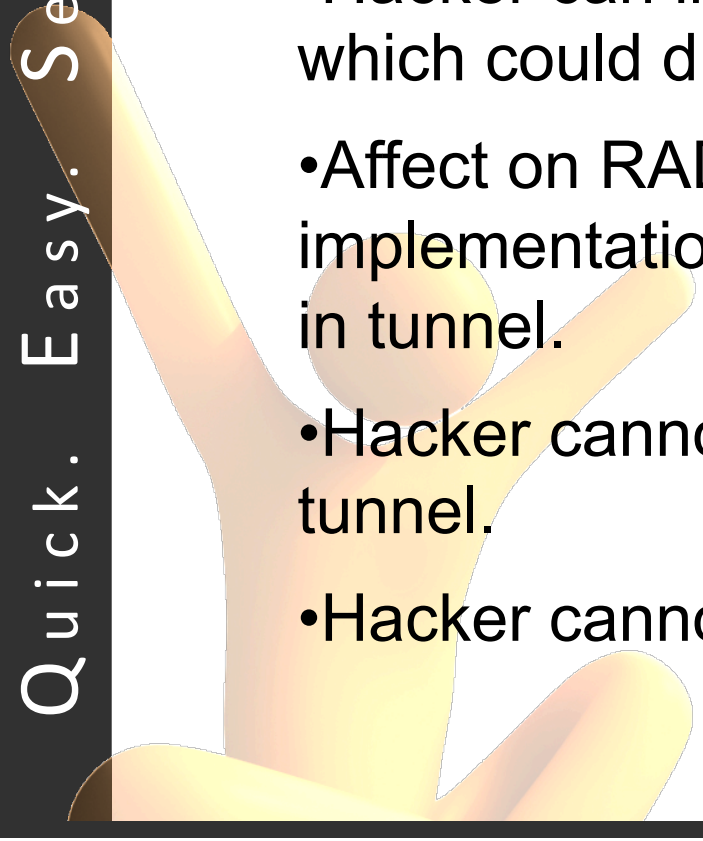


Quick. Easy. Secure.

TLS Vulnerability & 802.1X

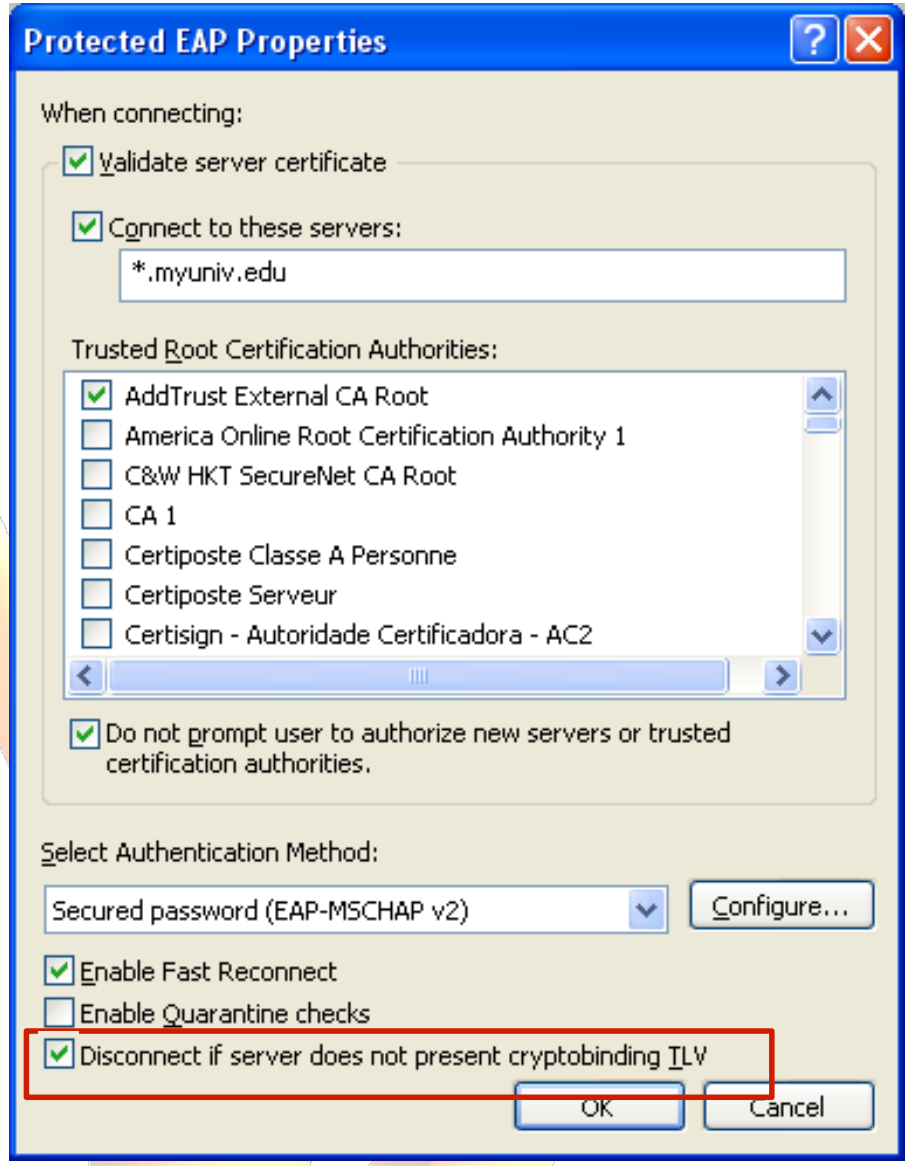
Potential Affect On 802.1X:

- PEAP & TTLS use TLS internally.
- Hacker can inject data into tunnel bound for server, which could disrupt authentication
- Affect on RADIUS server depends on implementation's ability to handle unexpected packets in tunnel.
- Hacker cannot see or modify authentication data in tunnel.
- Hacker cannot inject packets bound for client.



Quick. Easy. Secure.

Crypto Binding

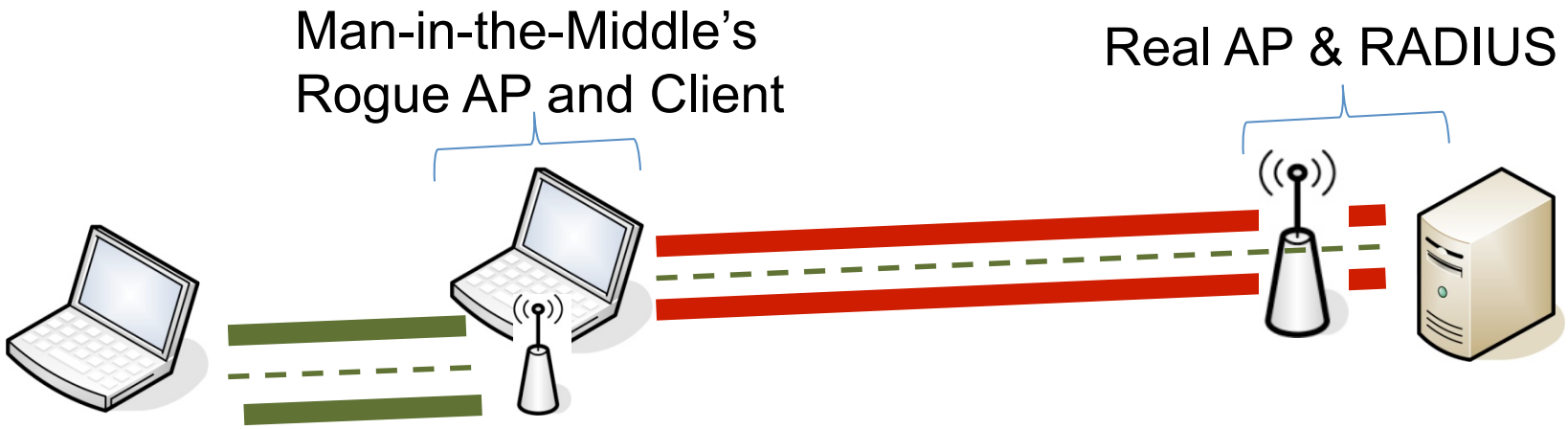


What is it?

- Prevents Asokan Attacks, an attack on all tunneled protocols.
- Binds inner and outer tunnel together in PEAP & TTLS.
- Must be supported by RADIUS server.
- If binding is broken by man-in-the-middle, authentication will be blocked similar to server cert validation.

Quick. Easy. Secure.

Asokan Attack & Crypto Binding



- Outer tunnel is recreated between hacker & real network.
- Pass-through inner tunnel allows server certificate validation to pass for client.

What's Protected by Crypto Binding?

Protects network by preventing network access by man-in-the-middle.

Protects user by preventing machine from connecting to man-in-the-middle's rogue access point.

Quick. Easy. Secure.

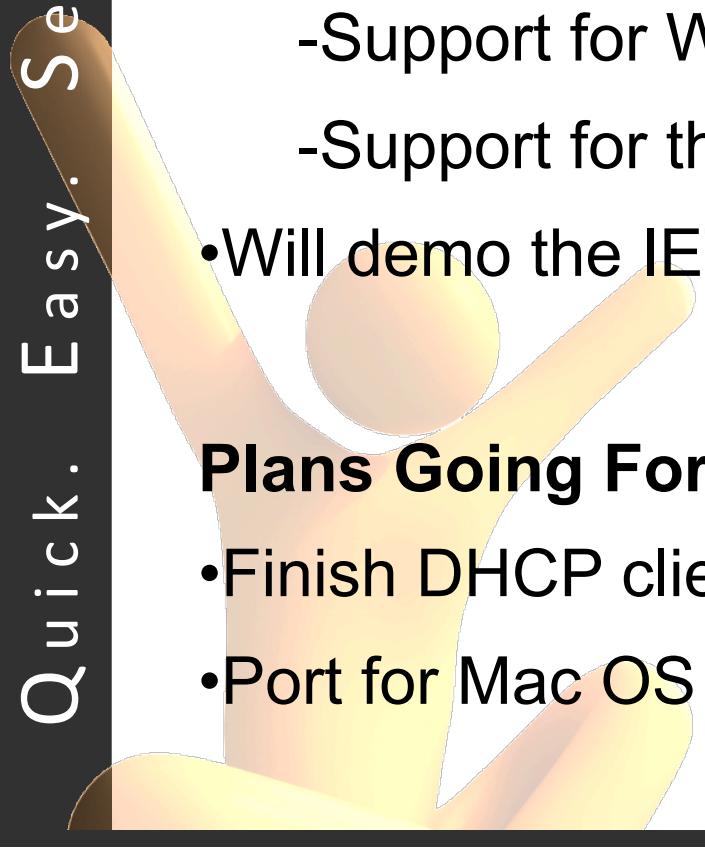
OpenSEA (XSupplicant)

Status:

- Two new development volunteers.
- Work underway on:
  - -Support for Windows Vista and 7 (x86 and x64)
  - -Support for the IETF NEA protocols.
- Will demo the IETF NEA operation at Interop Las Vegas

Plans Going Forward:

- Finish DHCP client integration on Linux versions.
- Port for Mac OS X



Quick. Easy. Secure.

802.1X-2010

Approved by IEEE but not yet published.

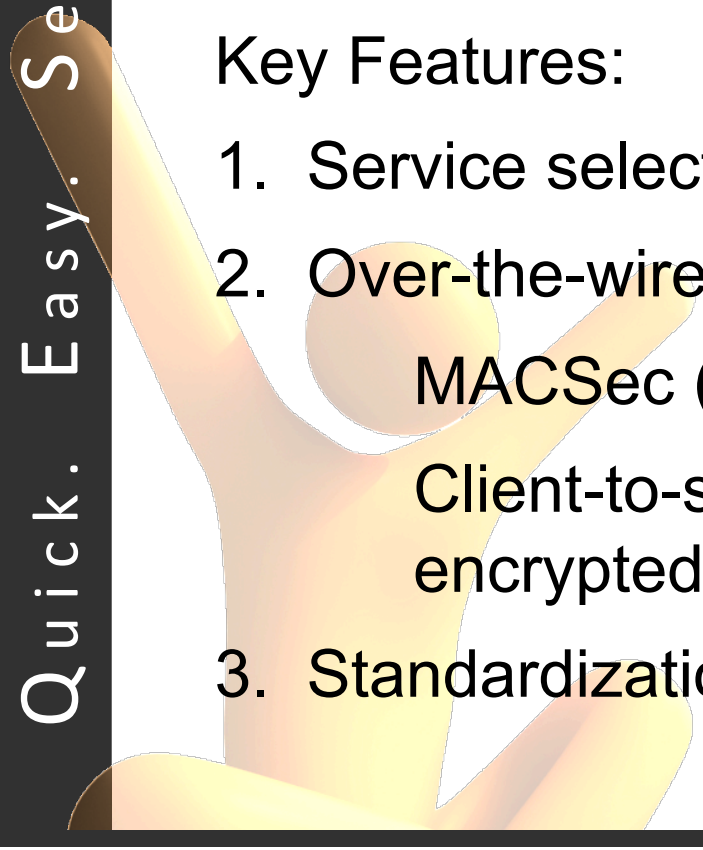
Brings “wireless features” to wired networks.

Key Features:

1. Service selection for wired ports
2. Over-the-wire encryption

   MACSec (IEEE 802.1AE)

   Client-to-switch, switch-to-switch, switch-to-router encrypted links.
3. Standardization of multi-auth.



Quick. Easy. Secure.

Understanding

Server Certificate Validation

and 802.1X Update

Kevin Koster

Founder & Principal

Cloudpath Networks

Special Thanks To:

Robert Hopley, RSA

Chris Hessing, Cloudpath & OpenSEA

Alex Sharaz, University of Hull

Louis Searchwell, JANET

Damien Shaw, JANET

Cloudpath NETWORKS