Using tunnels and three party authentication to improve roaming security

Damien LEROY

UCLouvain - Belgium
IP Networking Lab - http://inl.info.ucl.ac.be

BELNET Security Conference - April 30th, 2009
Content

(I) Introduction to WiFi Roaming

(II) Remote authentication: risks for the visited network

(III) Security risks for the mobile user

(IV) Solutions based on VPN

(V) ALAWN project
(I) Introduction to WiFi Roaming

(II) Remote authentication: risks for the visited network

(III) Security risks for the mobile user

(IV) Solutions based on VPN

(V) ALAWN project
"WiFi Roaming"
Scenario 1: Open WiFi Access

Internet

H

F
Scenario 1: Open WiFi Access
Scenario 1: Open WiFi Access

Internet

ILLEGAL ACTIVITIES
Scenario 1: Open WiFi Access
Scenario 3: Remote authentication

Internet

H

user: smith@H-Network
passwd: in H

F

D. Leroy
UCL Belgium, Apr 2009

Security of WiFi Roaming
BSC 2009
Scenario 3: Remote authentication

Internet

user: smith@H-Network
passwd: * in H
Content

(I) Introduction to WiFi Roaming

(II) Remote authentication: risks for the visited network

(III) Security risks for the mobile user

(IV) Solutions based on VPN

(V) ALAWN project
Authenticated Wireless Roaming via Tunnels:
Making Mobile Guests Feel at Home

M. Manulis, D. Leroy, F.K., O.B., J.J.Q.
UCL Belgium, March 2009

The Eduroam Project

M. Manulis, D. Leroy, F.K., O.B., J.J.Q.
UCL Belgium, March 2009

Authenticated Wireless Roaming via Tunnels:
Making Mobile Guests Feel at Home
Authentication within Eduroam

Stockholms universitet

Internet

Swedish Authority

Belgian Authority

IEEE802.1X

TTLS+PAP

user: Beck@SU.se
Roaming with Eduroam

Stockholms universitet

Internet

user: Beck@SU.se
Roaming with Eduroam

Stockholms universitet

Internet

http://www.swedbank.se/

user: Beck@SU.se

UCL
Roaming with Eduroam

Stockholms universitet

Internet

user: Beck@SU.se

D. Leroy
UCL Belgium, Apr 2009

Security of WiFi Roaming
BSC 2009
User abuse: Access to illegal data

Stockholms universitet

Internet

Auth. server

user: Beck@SU.se

ILLEGAL ACTIVITIES

Auth. server

User abuse: Access to illegal data

Stockholms universitet

Internet

Auth. server

user: Beck@SU.se

ILLEGAL ACTIVITIES

Auth. server
User abuse: Access to illegal data
User abuse: Attack on the Internet

Stockholms universitet

Internet

SPAM

SU
user: Beck@SU.se

Auth. server

UCL
How do spam filters work?

Score each mail based on:

- **Content**: “viagra”, “diploma”, “free videos”, ...
- **“Packaging”**: Large images, lots of receivers, ...
- **Well known spam-sender** (often attacked hosts)
  Based on shared databases
How do spam filters work?

Score each mail based on:

- **Content**:
  - "viagra", "diploma", "free videos", ...

- **"Packaging"**:
  - Large images, lots of receivers, ...

- **Well known spam-sender (often attacked hosts)**
  - Based on shared databases

**high score -> mark as spam**
How do spam filters work?

Score each mail based on:

- **Content**:
  “viagra”, “diploma”, “free videos”, ...

- **“Packaging”**:
  Large images, lots of receivers, ...

- **Well known spam-sender (often attacked hosts)**

  Based on shared databases

**high score -> mark as spam**
How do spam filters work?

How are these databases built up?

- Based on previous “mass spam” activities
- Based on IP addresses of senders
- Open databases
User abuse: Attack on the Internet
User abuse: Attack on the Internet

In PYZOR database:
add 130.104.*.* (=UCL)

User: Beck@SU.se
User abuse: Attack on the Internet

Stockholms universitet

Internet

PYZOR database:

... 130.104.*.* (=UCL)

...
Access control based on IP

- Some services (e.g., website) have their access control based on source IP.
  - Digital libraries
  - Intranet
  - ...

- The mobile user will have access to these services! (more complex filtering could be added)
## Summary

<table>
<thead>
<tr>
<th></th>
<th>Open WiFi</th>
<th>Temp. cred.</th>
<th>Remote auth.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User authentication</td>
<td>✗</td>
<td>🚨</td>
<td>✓</td>
</tr>
<tr>
<td>Administrative cost</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Ease of use (for user)</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Blacklisting based on IP</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Access based on IP</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Attack on the infrastruct.</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>
Content

(I) Introduction to WiFi Roaming

(II) Remote authentication: risks for the visited network

(III) Security risks for the mobile user

(IV) Solutions based on VPN

(V) ALAWN project
Stealing credentials

Internet

3rd party Authority

IEEE802.1X TTLS+PAP

user: hisname@hisnet.com
Pharming

A diagram showing the concept of Pharming, where a user (U) is directed to a malicious website (F) through a seemingly legitimate website (H) in the Internet.
Sniffing

Internet

H

F

RADIUS server

SU

SU

D. Leroy
UCL Belgium, Apr 2009

Security of WiFi Roaming
BSC 2009
Fake Access Point

Internet

SSID: EDUROAM

user: Beck@SU.se

IEEE802.1X
TTLS+PAP

RADIUS server

RADIUS server

H

F
Fake Access Point

Internet

SSID: EDUROAM

user: Beck@SU.se

IEEE802.1X
TTLS+PAP
Fake Access Point

It is able to:
- steal cred.
- do pharming
- sniff traffic

SSID: EDUROAM

user: Beck@SU.se

IEEE 802.1X TTLS+PAP
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>User authentication</td>
<td>✗</td>
<td>!</td>
<td>✓</td>
</tr>
<tr>
<td>Administrative cost for F</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Ease of use (for user)</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Blacklisting based on IP</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Access based on IP</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Attack on the infrastruct.</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>F malicious</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Fake access point</td>
<td>✗</td>
<td>✗</td>
<td>!</td>
</tr>
</tbody>
</table>
Content

(I) Introduction to WiFi Roaming
(II) Remote authentication: risks for the visited network
(III) Security risks for the mobile user
(IV) Solutions based on VPN
(V) ALAWN project
For the user: via username/pwd (or certificate)

For the home network: via certificate or no auth (cert must be distributed!)

D. Leroy
UCL Belgium, Apr 2009
For the user: via username/pwd (or certificate)

For the home network: via certificate or no auth (cert must be distributed!)

D. Leroy
UCL Belgium, Apr 2009
VPN

Internet

Stockholms universitet

VPN server

http://www.swedbank.se/

D. Leroy
UCL Belgium, Apr 2009
VPN

Stockholms universitet

VPN server

http://www.swedbank.se/

Internet

http://www.swedbank.se/

UCL

D. Leroy
UCL Belgium, Apr 2009

Security of WiFi Roaming
BSC 2009
VPN, a solution for previous issues?

Yes because:

- The requests are sent with the IP address of the home network
- If M sends spam over the Internet, only his home network is blamed
- It protects the user from a malicious visited network
Yes but:

- **Only authentication between H and M:**
  - F does not authenticate / know M and H
  - M does not always check H auth (F can do pharming)

- **On user’s demand**
  - If M wants to meet some security goals
  - F cannot force M to create VPN to H
### VPN, a solution for previous issues?

The previous table, updated

<table>
<thead>
<tr>
<th></th>
<th>Remote auth.</th>
<th>VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>User authentication (by F)</td>
<td>✅</td>
<td>✗</td>
</tr>
<tr>
<td>Administrative cost for F</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Ease of use (for user)</td>
<td>✅</td>
<td>!</td>
</tr>
<tr>
<td>Blacklisting based on IP</td>
<td>✗</td>
<td>✅</td>
</tr>
<tr>
<td>Access based on IP</td>
<td>✗</td>
<td>✅</td>
</tr>
<tr>
<td>Attack on the infrastruct.</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>F malicious</td>
<td>✗</td>
<td>✅</td>
</tr>
<tr>
<td>Fake access point</td>
<td>!</td>
<td>✅</td>
</tr>
</tbody>
</table>
Combining IEEE802.1X and VPN

How ?

- Firewall of F blocks everything
- User connects with his credentials for IEEE802.1X
- F opens the VPN port as destination port, only from this user, and to its home network (inferred from IEEE802.1X)
Combining IEEE802.1X and VPN

Using both IEEE802.1X and VPN to reach security goals is possible. But:

- Need both infrastructures
- Once the user is authenticated, how the tunnel is forced to H?
  - Filtering based on IEEE8021.X decision?
- Two init phases can take some time (few seconds) to succeed
Content

(I) Introduction to WiFi Roaming
(II) Remote authentication: risks for the visited network
(III) Security risks for the mobile user
(IV) Solutions based on VPN
(V) ALAWN project
The ALAWN project

Some words about the project

- A Walloon Region project
- In collaboration with:
  - CRID (Research Centre on IT and Law - FUNDP - Namur)
  - Crypto Group - UCL
  - IP Networking Lab - UCL
The proposal - Step 1

Stockholms universitet

Internet

3-party crypto authentication & key exchange
The proposal - Step 2

Stockholms universitet

Internet

RADIUS server

RADIUS server

RADIUS server

D. Leroy
UCL Belgium, Apr 2009

Security of WiFi Roaming
BSC 2009
The proposal - Step 2
The proposal

[Diagram showing WiFi roaming between Stockholms universitet and UCL with RADIUS server involved]
Remote Auth. and Key Exchange (RAKE)

Goals for the protocol

- Authentication between M, H and F
- Key exchange
- (Negotiation of session parameters)
Security Goals

Authentication
Security Goals

Authentication

- H must authenticate M as one of the registered mobile devices
- M must authenticate H as its home network
Security Goals

Authentication

- H must authenticate M as one of the registered mobile devices
- M must authenticate H as its home network
- F must authenticate H as a roaming partner
- H must authenticate F as a roaming partner
Security Goals

Authentication

- H must authenticate M as one of the registered mobile devices
- M must authenticate H as its home network
- F must authenticate H as a roaming partner
- H must authenticate F as a roaming partner
- F trusts H to correctly authenticate M
- M trusts H to correctly authenticate F
Security Goals

Key establishment

- Protection of communication between M, H and F
  - $K_T$ (tunnel key)
- End-to-end protection
  - $K_{M,H}$ (end-to-end key)
What are the keys used for?

$K_T$, the key shared between H-F-M

- To infer the key used for "wireless" communication
- To negotiate connection parameters (when it stops, accounting, mobility, ...)

What are the keys used for? 

$K_{M,H}$, the key shared between H and M

- For fully-encrypting the communication between M and H
- To negotiate connection parameters that should not be known/modified by F, shared between H and M
RAKE protocol

Additional constraints

- RTT should be as low as possible
- The mobile device should not do “hard computation”
The protocol in itself (simplified)

\[ M | r_M | H \]

\[ F | r_F | M | r_M \]

\[ \text{sid} = F | r_F | M | r_M | H | r_H \]

\[ k_t = \text{PRF}_{k_M}(0, \text{sid}) \]

\[ X = \text{Enc}_{e_kF}(k_t) \]

\[ \mu_H = \text{MAC}_{\alpha_M}(0, \text{sid}) \]

\[ r_H | X | \mu_H | \sigma_H(*) \]

\[ k_t = \text{Dec}_{d_kF}(X) \]

\[ k_t = \text{PRF}_{k_M}(0, \text{sid}) \]

\[ K_T = \text{PRF}_{k_t}(1, \text{sid}) \]

\[ K_{M,H} = \text{PRF}_{k_M}(2, \text{sid}) \]

\[ \mu_M, \sigma_F(*) \]

\[ \mu_M = \text{MAC}_{\alpha_M}(1, \text{sid}) \]

D. Leroy
UCL Belgium, Apr 2009

Security of WiFi Roaming
BSC 2009
The protocol in itself

- A full security model has been defined
- Protocol has been proved
- For the ones interested in details:

RAKE protocol

Additional constraints, results

- RTT should be as low as possible
- The mobile device should not do “hard computation”
The proposal

Stockholms universitet

Internet

D. Leroy
UCL Belgium, Apr 2009

Security of WiFi Roaming
BSC 2009
The proposal

Stockholms universitet

Internet

RADIUS server

RADIUS server

SU

SU

UCL

D. Leroy
UCL Belgium, Apr 2009

Security of WiFi Roaming
BSC 2009
Why using a tunnel?

- Tunnel from F to H is not encrypted, it is only used to permit M to send packet to his home network.
- Technical interests have been shown at the beginning of the presentation.
- We showed with CRID that it also has legal advantages:

Technical choices

- The RAKE protocol:
  - Extending IEEE802.1X (EAP)

- The tunnel:
  - Use a L2TP tunnel

- Encryption between H and M:
  - Optional
  - Using IPSec (ESP)
Extending 802.1X for RAKE

- IEEE802.1X is now widely used
- It uses EAP (the Extensible Authentication Protocol) for authentication
- EAP can be easily extended
Extending 802.1X for RAKE

How does IEEE802.1X work?

- EAP start
- EAP-request identity
- PORT BLOCKED
- physical layer connection
Extending 802.1X for RAKE

How does IEEE802.1X work?

physical layer connection

EAP start

EAP-request

identity

EAP-response

identity: dleroy

PORT BLOCKED

(in RADIUS packet)

EAP-response

identity: dleroy
Extending 802.1X for RAKE

How does IEEE802.1X work?

- Physical layer connection
- EAP start
- EAP-response
- EAP response: dleroy (in RADIUS packet)
- (in RADIUS packet)
- EAP response: dleroy
- EAP requests/responses following the EAP method

D. Leroy
UCL Belgium, Apr 2009
How does IEEE802.1X work?

1. Physical layer connection
2. EAP start
3. EAP-request identity
4. EAP-response identity: dleroy (in RADIUS packet)
5. EAP-success
6. PORT OPEN

EAP requests/responses following the EAP method:
- EAP start
- EAP-request identity
- EAP-response identity: dleroy
- EAP-success
- PORT OPEN
Extending 802.1X for RAKE

How does IEEE802.1X work?

- Physical layer connection
- EAP start
- EAP-request
  - identity
- EAP-response
  - identity: dleroy
- (in RADIUS packet)
  - EAP-response
  - identity: dleroy
- EAP requests/responses following the EAP method
- EAP-success

Ethernet or WiFi (keys derived from previous negotiations)
Extending 802.1X for RAKE

We have implemented it

- In “Host AP” project (hostapd & wpa_supplicant)
- An open-source implementation
- *hostapd* works with most Linux & BSD drivers
- *wpa_supplicant* works with most Linux, BSD & Windows drivers
In next months, we would like to test it in real situations

With `hostap`:

- On laptop and mobile devices
- On access point (on OpenWRT OS)
- On basic Linux server

If you want to test the protocol in your network in a few months... please ask us
Tunnel between F and H

Stockholms universitet

Internet

UCL
Tunnel between F and H

Stockholms universitet

Internet

UCL
Tunnel between F and H

A L2TP tunnel

- The AP acts as layer 2 bridge

Advantages:

- Even the IP address is allocated by H
- Do not have to rely on F technical config (e.g., IPv4/v6)
- Less security risks for F
- Transparent for M (the host and the user)
On Expected Increase of Latencies

- For each request, a RTT “H-F” is added
  - **City**: 30-60ms for residential hosts (3-4ms for well-connected hosts) [LP03]
  - **Country (USA)**: <150ms [LP03]
  - **Intercontinental**: <250ms for 90% residential [DHGS07]

- ITU-T recommendations: one-way latency <400ms may be acceptable (e.g., VoIP)
Encryption between M and H

Stockholms universitet

Internet

D. Leroy
UCL Belgium, Apr 2009
Encryption between M and H

- Kept optional (negotiated)
- Using $K_{M,H}$ (only known by M and H)
- Encryption method negotiated
  - more suitable: IPSec ESP in tunnel mode
## Comparison with previous solutions

<table>
<thead>
<tr>
<th></th>
<th>Remote auth.</th>
<th>VPN</th>
<th>RAKE</th>
</tr>
</thead>
<tbody>
<tr>
<td>User authentication (by F)</td>
<td>✔️</td>
<td><img src="image" alt="X" /></td>
<td>✔️</td>
</tr>
<tr>
<td>Administrative cost for F</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Ease of use (for user)</td>
<td>✔️</td>
<td>![!]</td>
<td>✔️</td>
</tr>
<tr>
<td>Blacklisting based on IP</td>
<td><img src="image" alt="X" /></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Access based on IP</td>
<td><img src="image" alt="X" /></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Attack on the infrastruct.</td>
<td><img src="image" alt="X" /></td>
<td><img src="image" alt="X" /></td>
<td>✔️</td>
</tr>
<tr>
<td>F malicious</td>
<td><img src="image" alt="X" /></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Fake access point</td>
<td>![!]</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
Summary on our proposal

Constraints

✓ The tunnel increases the latency for some destinations
✓ The partnership has to be decided earlier
✓ Need (light) modifications of host, AP or the egress router, and authentication server.
Summary on our proposal

Advantages

✓ If the user sends spam, the user’s home network is blamed (and blacklisted), not the visited network

✓ Visited network does not care about the user activities

✓ Traffic can be encrypted
Summary on our proposal

Advantages

✓ Tunnel is initiated (and forced) by F and H, not by the user
✓ H does verify F authentication (>< TTLS)
✓ Same services as “at home”
Questions ?

Damien Leroy
damien.leroy@uclouvain.be

ip networking lab
http://inl.info.ucl.ac.be