Wireless Roaming using 3-Party Authentication & Tunnels

Damien LEROY\textsuperscript{1}, Mark MANULIS\textsuperscript{2}, Olivier BONAVENTURE\textsuperscript{1}

\textsuperscript{1}UCLouvain (Be), \textsuperscript{2}TU Darmstadt & CASED (De)

U-Net '09 - December 1st, 2009
Let’s consider basic WiFi sharing
Let’s consider basic WiFi sharing
Let’s consider basic WiFi sharing.
There are lots of risks in sharing one’s WiFi connection

Risk 1: Legal issues because of visitor’s behaviors
There are lots of risks in sharing one’s WiFi connection

Risk 2: Issues with ISP for misbehavior
There are lots of risks in sharing one’s WiFi connection

Risk 3: Attack on John’s network
There are lots of risks in sharing one’s WiFi connection

Risk 4: Resource consumption
There are risks in connecting to a shared network

Risk 5: Man-in-the-Middle attacks

- Sniffing
- Pharming
- Even if AP trusted (AP/SSID spoofing)
The main 5 risks in WiFi sharing

- legal issues
- ISP issues
- attack on visited network
- resource consumption
- MITM
Structure of the Presentation

Review of existing solutions

Our proposal

Implementation & Deployment
Software-based WiFi sharing

WEP/WPA keys shared by users on the service website

Specific software must be used

When connecting to a WiFi, the software knows the WEP/WPA key to use
Software-based WiFi sharing: Issues

Visitors are connected on the same SSID as the AP’s owner

SSID<->key mapping is stored on clients (!!!)

Easy to set up a fake AP to obtain keys
Software-based WiFi sharing: ... risks are still there

- legal issues
  - but user could be identified
- ISP issues
- attack on visited network
- resource consumption
- MITM
  - + keys can be known
  - risky if linked to other passwd
Hardware-based WiFi sharing

Have to buy the FON AP

One private SSID (encrypted),
One public (open + web-auth)

Access to FON users & paying users
Hardware-based WiFi sharing: issues

- Visitors’ traffic can be sniffed
- 15 free minutes for anybody
- Easy to set up a fake AP to stealing FON credentials
Hardware-based WiFi sharing: ... some risks are still there

- legal issues
- ISP issues
- attack on visited network
- resource consumption
- MITM
Wisher/Wifi.com & FON are not really satisfying...

Mainly on the following topics:

- liability (against ISP and law)
- possibility of MITM attack from the visited network
- easy to place a fake AP
Structure of the Presentation

Review of existing solutions

Our proposal

Implementation & Deployment
Remaining issues can be solve, but we need another solution

Liability (against ISP and law)
- visitors and users from the visited network must not be mixed on the Internet

Possibility of MITM attack from the visited network
- data sent by the visitors should be encrypted

Easy to place a fake AP
- AP should be authenticated
We think we should involve ISPs
Enhanced Wireless Roaming Security using 3-Party Authentication and Tunnels
Damien Leroy, M. Manulis, O. Bonaventure - IP Networking Lab - UCLouvain (be)
Enhanced Wireless Roaming Security using 3-Party Authentication and Tunnels
Damien Leroy, M. Manulis, O. Bonaventure - IP Networking Lab - UCLouvain (be)
Enhanced Wireless Roaming Security using 3-Party Authentication and Tunnels

Damien Leroy, M. Manulis, O. Bonaventure - IP Networking Lab - UCLouvain (be)
Enhanced Wireless Roaming Security using 3-Party Authentication and Tunnels

Damien Leroy, M. Manulis, O. Bonaventure - IP Networking Lab - UCLouvain (be)
Enhanced Wireless Roaming Security using 3-Party Authentication and Tunnels

Damien Leroy, M. Manulis, O. Bonaventure - IP Networking Lab - UCLouvain (be)

Key derivation

- Bob ↔ Green
- Green ↔ BT&T AP

Authentication

EAP-RAKE on RADIUS

John

Bob

BT&T
Enhanced Wireless Roaming Security using 3-Party Authentication and Tunnels

Damien Leroy, M. Manulis, O. Bonaventure - IP Networking Lab - UCLouvain (be)
Enhanced Wireless Roaming Security using 3-Party Authentication and Tunnels
Damien Leroy, M. Manulis, O. Bonaventure - IP Networking Lab - UCLouvain (be)
EAP-RAKE solves main security issues

- legal issues
- ISP issues
- attack on visited network
- resource consumption
- MITM
A look at the authentication protocol: EAP-RAKE

Crypto part has been proved in [Man09]
Tunnels between entities using standards

Tunneling between the AP and the home network
- Using L2TP (or AH tunnel)
- The tunnel is authenticated (e.g., with IPsec/AH)

Encryption
- Kept optional (should be turned off in some cases)
Structure of the Presentation

Review of existing solutions

Our proposal

Implementation & Deployment
A prototype of the authentication protocol has been implemented

As a new EAP method, in hostap implementation

- hostap is an open-source project
- (our implementation not yet)
- client (mobile) works on Linux, MacOS, Win (?)
- server (AP) works on Linux (and so on OpenWRT)
Results of first measurements: EAP-RAKE is lighter than PEAP

Processing time for authentication (in msec)

- Mobile (P4 2.6GHz): 0.125ms
- Access Point (ASUS 500GP, 266MHz): Blue - EAP-RAKE, Red - EAP-PEAP using MSCHAPv2
- Home Network (Dual-E2180, 2GHz):
Assembly of tunnels mechanisms has also been made

Using L2TP requires a PPP concentrator (no OpenSource solution existing)

- Using pure IPsec solutions is possible (tunnel mode)

Tunnel encryption/authentication uses AH mechanism (openswan)

It works ! And seems to fit to networks’ reality
It was not fair to compare our solution $\geq$ FON

- Security is stronger in our solution
- But (computing) cost is higher in our case
- But involving ISPs is a HUGE issue
  - even if in our case, ISPs do not increase their security risks (incentive)

What are we willing to do for stronger security?
Would a more secure mechanism push more people the share their WiFi?

Lots of people stops sharing their WiFi access after reading / experiencing issues with malicious (or stupid) visitors.

If there was no more risk in sharing, could we observe more sharing?
QUESTIONS ?
Some backup slides
Enhanced Wireless Roaming Security using 3-Party Authentication and Tunnels

Damien Leroy, M. Manulis, O. Bonaventure - IP Networking Lab - UCLouvain (be)
Our solution requires widespread adoption

Could rely on communities (as FON, Whisher, ...)

ISPs could decide to add EAP-RAKE to set-top boxes (home routers) they control
  ▸ but they must be >1 ISP participating
Scalability issues could appear

Cost of the authentication protocol evaluated

Cost of the authenticated tunnel (and encryption) has not been evaluated (yet)

- For home network, should load balance (or distribute servers in data centers around the world)
- For AP,
  - either limiting number of simultaneous clients,
  - or only tunneling (without AH) to a proxy-server that makes the job