Authenticated Wireless Roaming via Tunnels*

Mark Manulis
Cryptographic Protocols Group
TU Darmstadt & CASED

Wireless (IP) Roaming

Foreign Network

Internet

Service Provider

Home Network

Mobile Device
(registered at H)

sreq

sres

KM,H

KM,H

KM,H

Wireless (IP) Roaming
Wireless (IP) Roaming

Service Provider
Foreign Network

Internet

Home Network

Mobile Device
(registered at H)

K_{M,F}
sreq
sres

K_{M,F}
Potential Security Risks 1

Malicious F

- easy DNS manipulations, e.g. pharming attacks
- F may claim higher costs since H has no control over the amount of service provided by F

Foreign Network

Internet

Malicious F

Mobile Device

(registered at H)

sreq sres
Potential Security Risks 2

- risks for the infrastructure of F which treats M as its own device (based on the IP membership)
- F could be blamed for the illegal activities of M on the Internet
Service Availability

Access to Services

F may not provide the same set of services as H does

M may try to access some value-added services (e.g. subscriptions to digital libraries) based on the IP membership in F
Wireless Roaming via Tunnels

(Security) Benefits of WRT
- H may control IP assignment and routing
- Internet "sees" M as part of H
- H remains the service provider
- benefits to accounting since H is active

GI / HGI Workshop „Wireless Security 2009“, Bochum
20.03.2009 | MARK MANULIS | www.manulis.eu
On Expected Increase of Latencies

some findings on the Round Trip Time in wireless IP networks

City 30-60 ms for residential hosts / 3-4 ms for well-connected hosts [LP03]

Country <150 ms [LP03]

Continent <250 ms for residential [DHGS07] and well-connected [AKSJ03] hosts

ITU-T recommendations: one-way latency < 400ms may be acceptable (e.g. VoIP)
Security Goals

Authentication
H must authenticate M as one of the registered mobile devices
M must authenticate H as its service provider
F must authenticate H as a roaming contract partner
H must authenticate F as a „good“ network to be accessed by M
F and M are not aware of each other and rely on the authorization made by H

Key Establishment
end-to-end tunnel protection \( \rightarrow K_{M,H} \) (end-to-end key)
protection of communication between M, H, and F \( \rightarrow K_t \) (tunnel key)
AWRT Protocol (basic version)

\[ M \]
\[ (k_M, \alpha_M) \]

\[ F \]
\[ (sk_F, vk_F) \]
\[ (dk_F, ek_F) \]

\[ H \]
\[ (M, k_M, \alpha_M) \]
\[ (sk_H, vk_H) \]

\[ k_t = \text{PRF}_{k_M}(0, \text{sid}) \]
\[ K_t = \text{PRF}_{k_t}(1, \text{sid}) \]
\[ K_{M,H} = \text{PRF}_{k_M}(2, \text{sid}) \]
\[ \mu_M = \text{MAC}_{\alpha_M}(1, \text{sid}) \]

\[ r_H | \mu_H \]
\[ \mu_M \rightarrow K_t = \text{PRF}_{k_t}(1, \text{sid}) \]

\[ r_t = \text{Dec}_{dk_F}(\chi) \]
\[ r_H | \chi | \mu_H | \sigma_H \]

\[ F|r_F|M|r_M + [T] \]

\[ \text{sid} = F|r_F|M|r_M|H|r_H \]
\[ k_t = \text{PRF}_{k_M}(0, \text{sid}) \]
\[ \chi = \text{Enc}_{ek_F}(k_t) \]
\[ \mu_H = \text{MAC}_{\alpha_M}(0, \text{sid}) \]

\[ k_t = \text{PRF}_{k_t}(1, \text{sid}) \]
\[ K_{M,H} = \text{PRF}_{k_M}(2, \text{sid}) \]
Resistance to DoS & Hijacking Attacks

\[ M \quad (k_M, \alpha_M) \quad (sk_M, vk_M) \]

\[ F \quad (sk_F, vk_F) \quad (dk_F, ek_F) \]

\[ H \quad (M, k_M, \alpha_M) \quad (sk_H, vk_H) \]

\[ M|r_M|H|\sigma_M \]

\[ r_H|\mu_H \]

\[ \mu_M \]

\[ F|r_F|M|r_M|T|\sigma_F \]

\[ r_H|\chi|\mu_H|\sigma_H \]

\[ \mu_M|\sigma_F \]

\[ K_t \]

\[ K_{M,H} \]

\[ M|H|m \]

hijacker

packet authentication with \( K_t \)

GI / HGI Workshop „Wireless Security 2009“, Bochum
20.03.2009 | MARK MANULIS | www.manulis.eu
Forward Secrecy for $K_{M,H}$

$M$:
- $(k_M, \alpha_M)$

$F$:
- $(sk_F, vk_F)$
- $(dk_F, ek_F)$

$H$:
- $(M, k_M, \alpha_M)$
- $(sk_H, vk_H)$

$F \rarrow r_F$

$M \arrow r_M \arrow H \arrow g^{x_M}$

$sid = F \arrow r_F \arrow M \arrow r_M \arrow H \arrow r_H$

$k_t = PRF_{k_M}(0, sid)$

$K_t = PRF_{k_t}(1, sid)$

$K_{M,H} = PRF_{g^{x_M}H}(2, sid)$

$\mu_M = MAC_{\alpha_M}(1, sid, g^{x_M}, g^{x_H})$

$\mu_H = MAC_{\alpha_M}(0, sid, g^{x_M}, g^{x_H})$

$\chi = Enc_{ek_F}(k_t)$

$\mu_H \arrow \sigma_F$

$K_t = PRF_{k_t}(1, sid)$
Unlinkability of Roaming Sessions

\[ \text{Unlinkability of Roaming Sessions} \]

\[ M \quad (k_M, \alpha_M) \]

\[ F \quad (sk_F, vk_F) \]

\[ H \quad (M, k_M, \alpha_M) \quad (sk_H, vk_H) \]

\[ (dk_F, ek_F) \]

\[ (dk_H, ek_H) \]

\[ \text{sid} = F | r_F | \text{Enc}_{ek_H}(M) | r_M | H | r_H \]

\[ H \quad (M, k_M, \alpha_M) \quad (sk_H, vk_H) \]

\[ (dk_H, ek_H) \]

\[ \text{Unlinkability of Roaming Sessions} \]

\[ M \quad (k_M, \alpha_M) \]

\[ F \quad (sk_F, vk_F) \]

\[ H \quad (M, k_M, \alpha_M) \quad (sk_H, vk_H) \]

\[ (dk_F, ek_F) \]

\[ (dk_H, ek_H) \]

\[ \text{sid} = F | r_F | \text{Enc}_{ek_H}(M) | r_M | H | r_H \]
in this talk

the concept of wireless roaming via tunnels (WRT)
(security) advantages of WRT over traditional wireless roaming approaches
authentication and key establishment goals
AWRT protocol

in the paper (full version at http://eprint.iacr.org/2008/382)
formal model – extension of Bellare-Rogaway model towards WRT
security analysis of AWRT
some ideas on practical realization based on currently available standards
forward secrecy + unlinkability of roaming sessions
handling of the reimbursement of F’s costs in commercial scenarios