# Authenticated Wireless Roaming via Tunnels*

Mark Manulis

Cryptographic Protocols Group

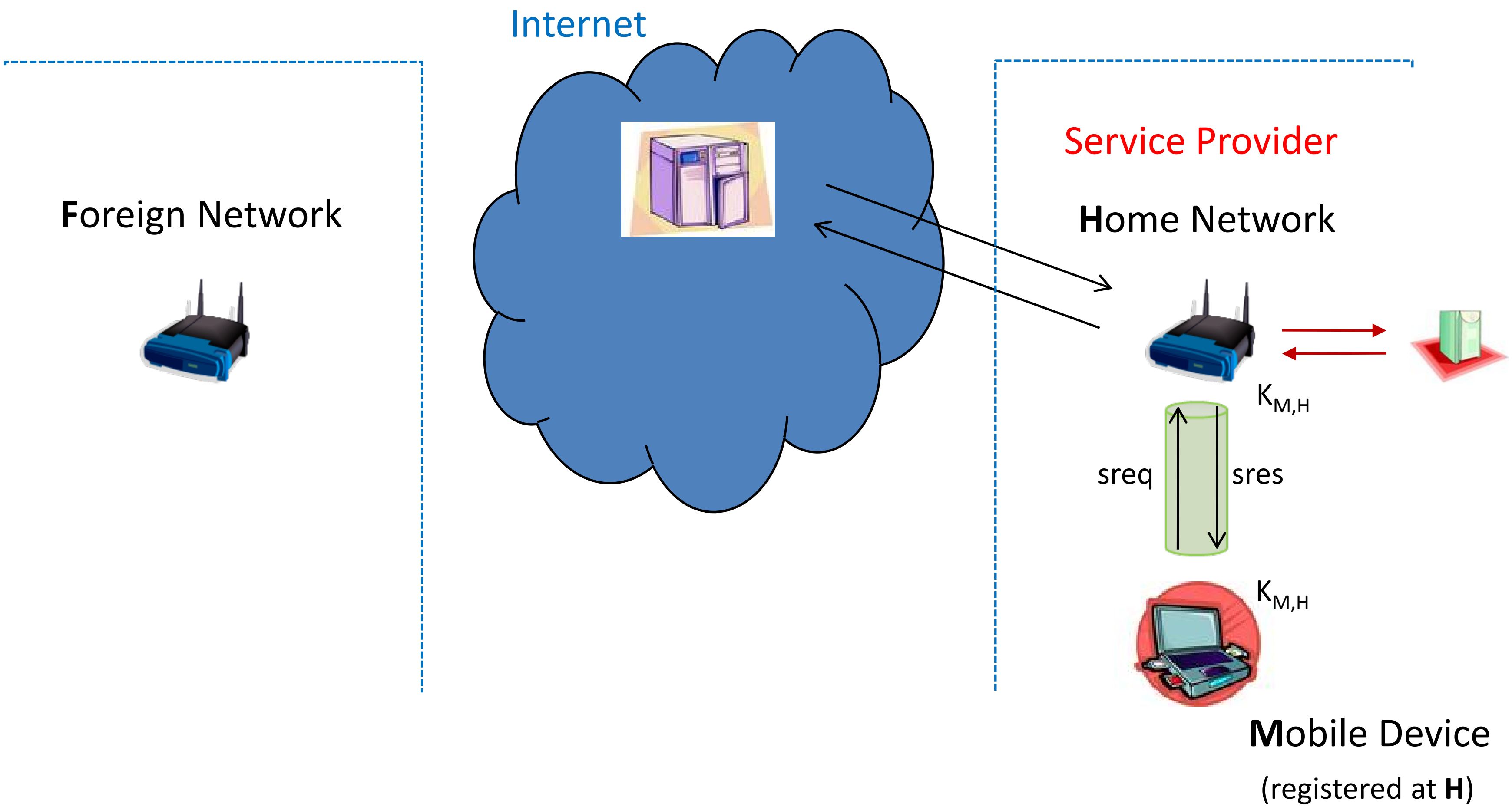
TU Darmstadt & CASED

[*] M. Manulis, D. Leroy, F. Koeune, O. Bonaventure, J.-J. Quisquater: *Authenticated Wireless Roaming via Tunnels: Making Mobile Guests Feel at Home.* ACM Symposium on Information, Computer, and Communication Security (ASIACCS'09), 10-12 March, Sydney, Australia

GI / HGI Workshop „Wireless Security 2009“, Bochum

CRYPTOGRAPHIC PROTOCOLS

# Wireless (IP) Roaming



Internet

**F**oreign Network

Service Provider

**H**ome Network

$K_{M,H}$

sreq

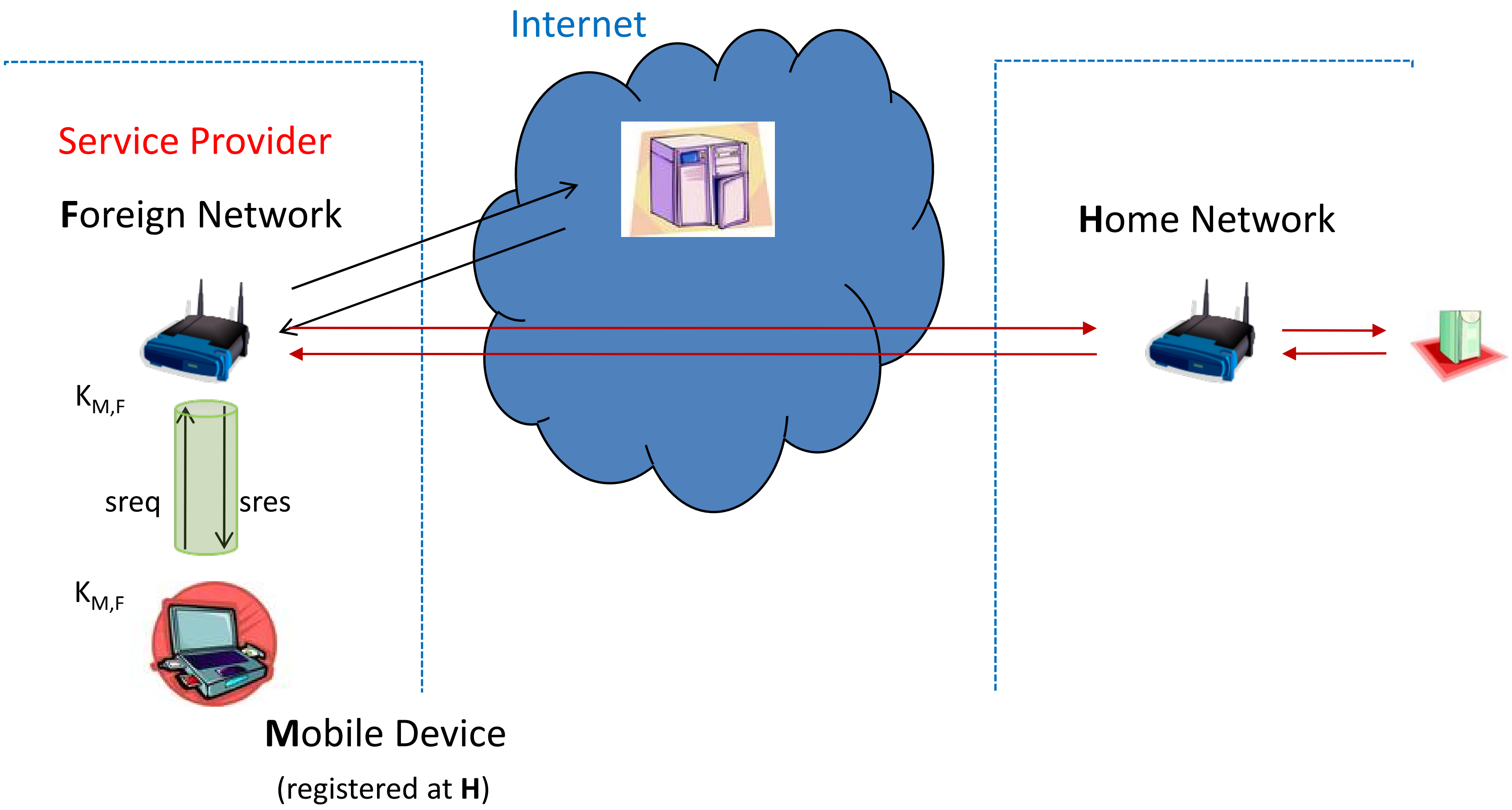
sres

$K_{M,H}$

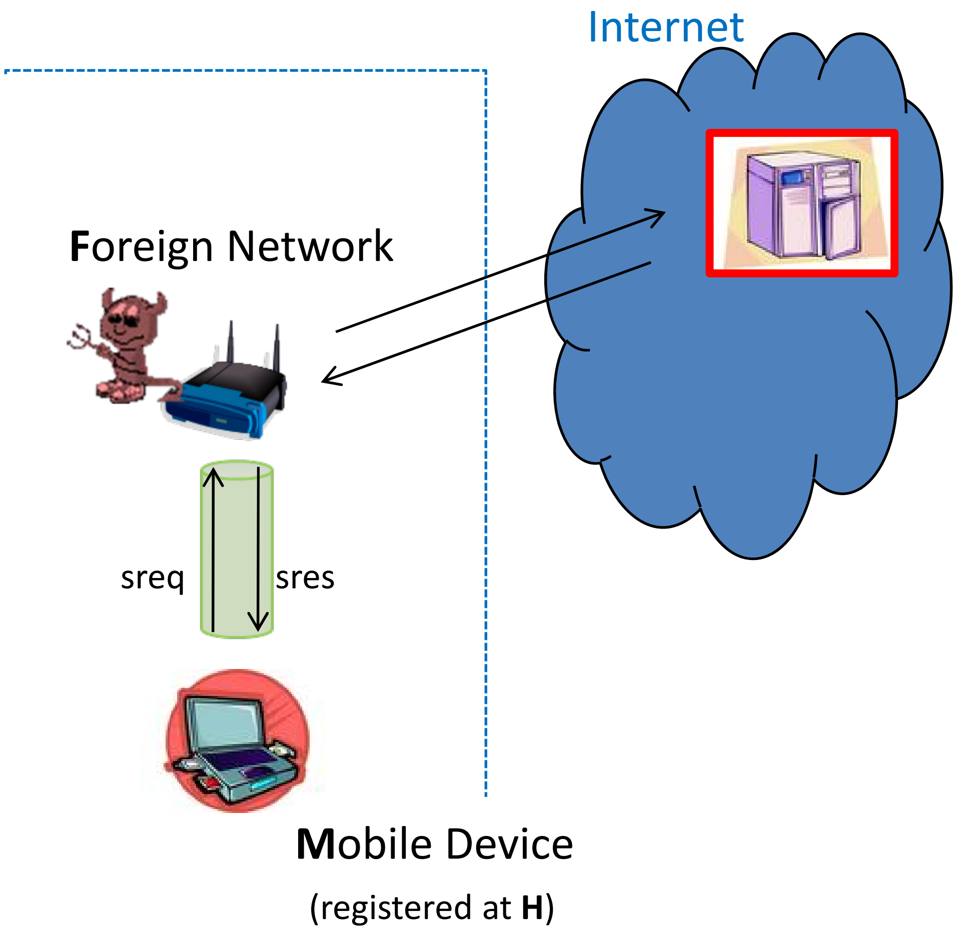
**M**obile Device

(registered at **H**)

# Wireless (IP) Roaming



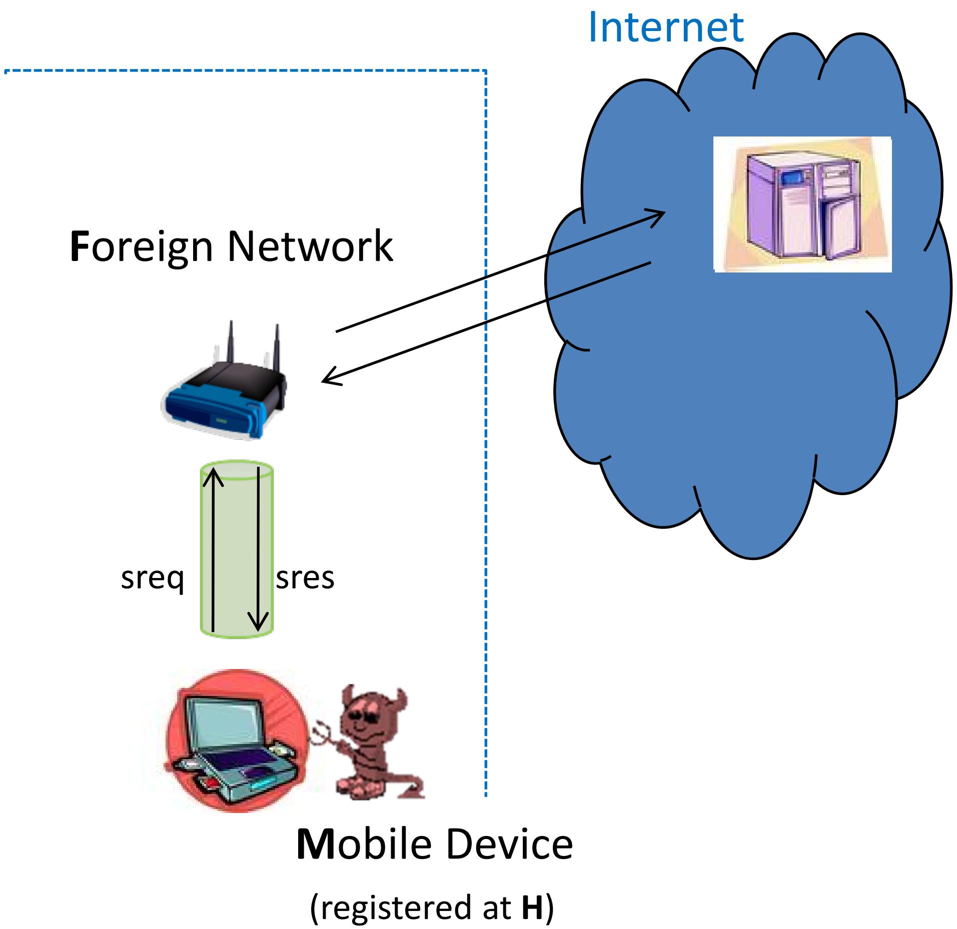
# Potential Security Risks 1



**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

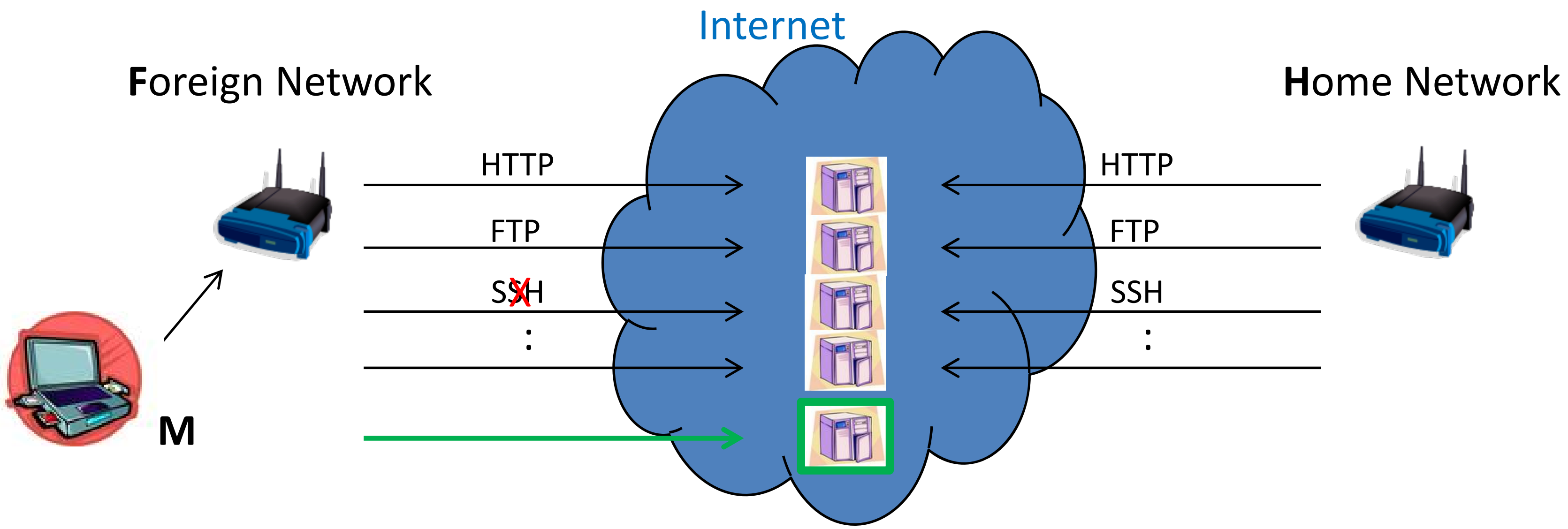
# Potential Security Risks 2



**Malicious M**

- 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

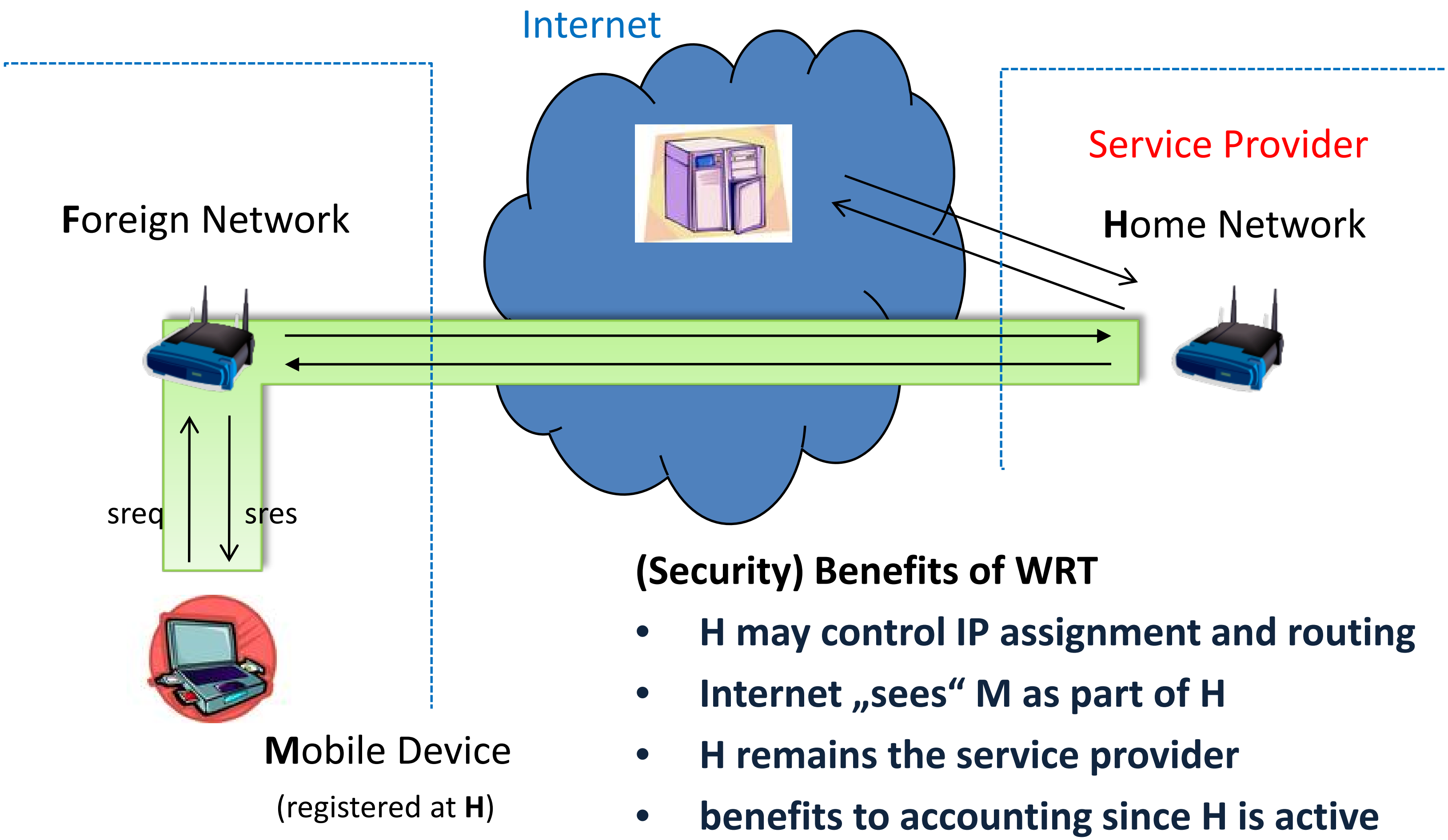


**Access to Services**

**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**

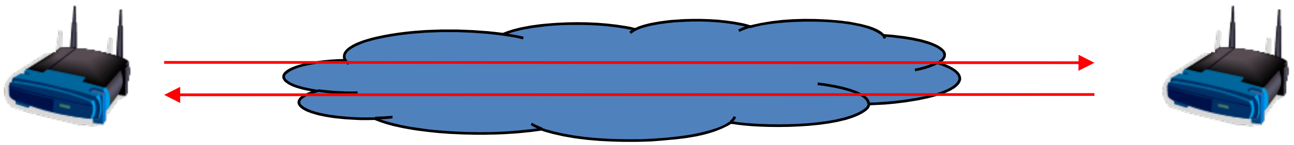
# Wireless Roaming via Tunnels



**(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

# On Expected Increase of Latencies



one additional communication round *per each* service request

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

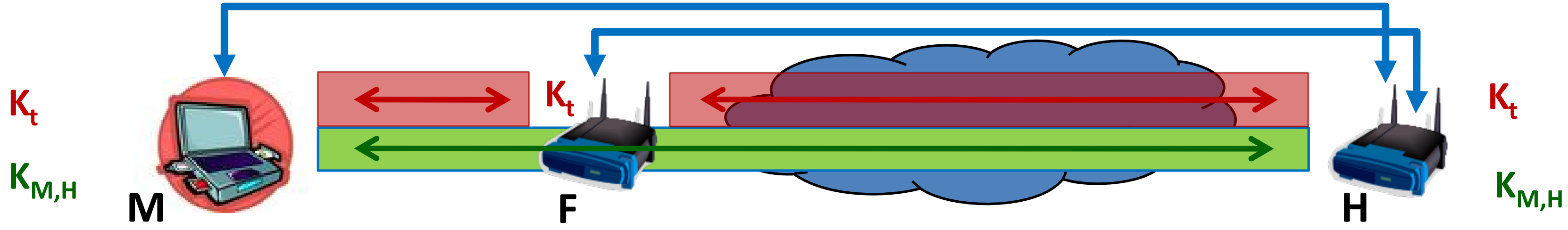
H must authenticate F as a „good“ network to be accessed by M

F and M are not aware of each other and rely on the authorization made by H

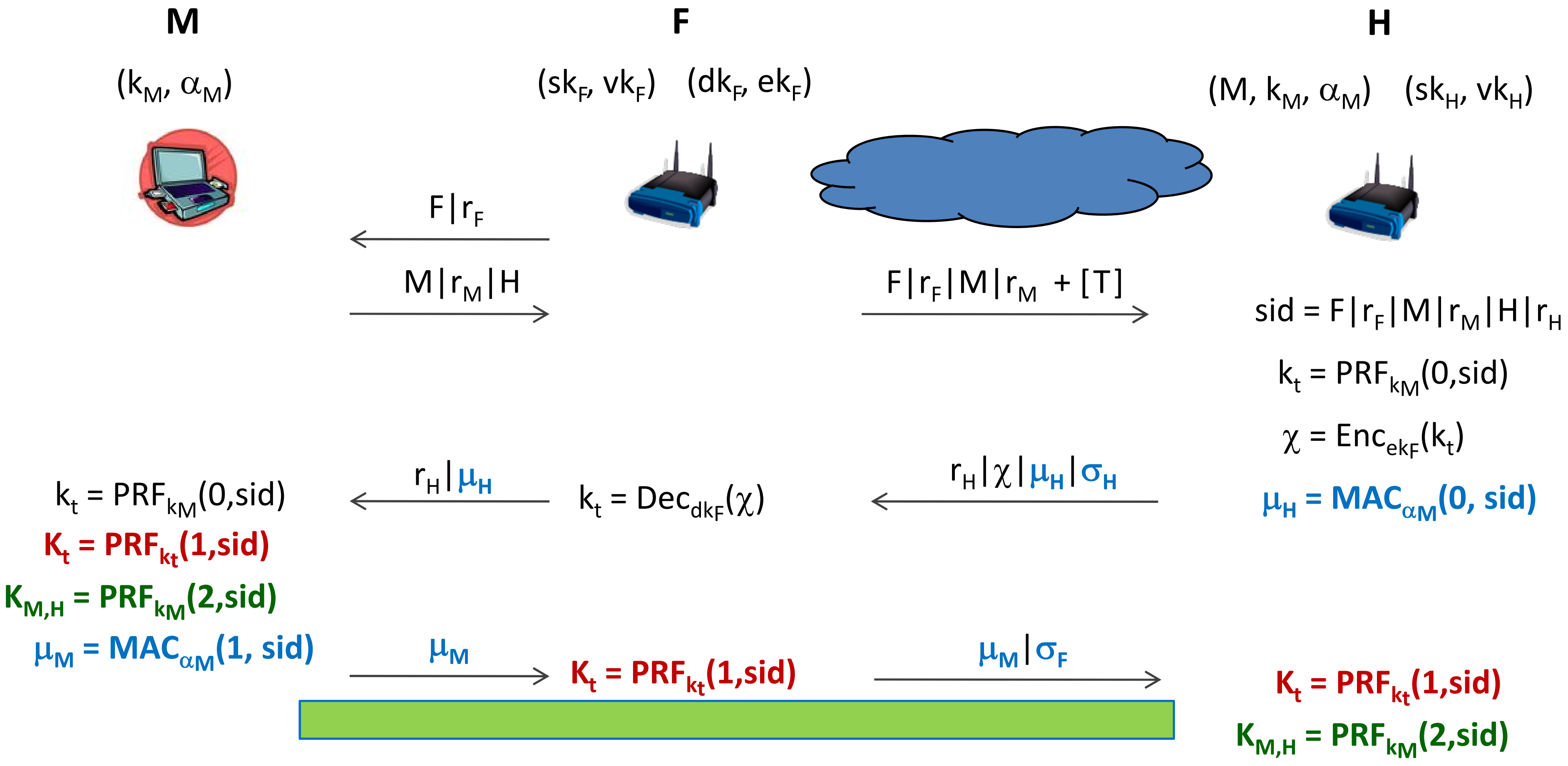
## Key Establishment

end-to-end tunnel protection → $K_{M,H}$ (end-to-end key)

protection of communication between M, H, and F → $K_t$ (tunnel key)



# AWRT Protocol (basic version)



**M**

$(k_M, \alpha_M)$

**F**

$(sk_F, vk_F)$ $(dk_F, ek_F)$

**H**

$(M, k_M, \alpha_M)$ $(sk_H, vk_H)$

$F|r_F$

$M|r_M|H$

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

$sid = F|r_F|M|r_M|H|r_H$

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

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

$\mu_H = MAC_{\alpha M}(0, sid)$

$r_H|\chi|\mu_H|\sigma_H$

$k_t = Dec_{dkF}(\chi)$

$r_H|\mu_H$

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

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

$K_{M,H} = PRF_{kM}(2,sid)$

$\mu_M = MAC_{\alpha M}(1, sid)$

$\mu_M$

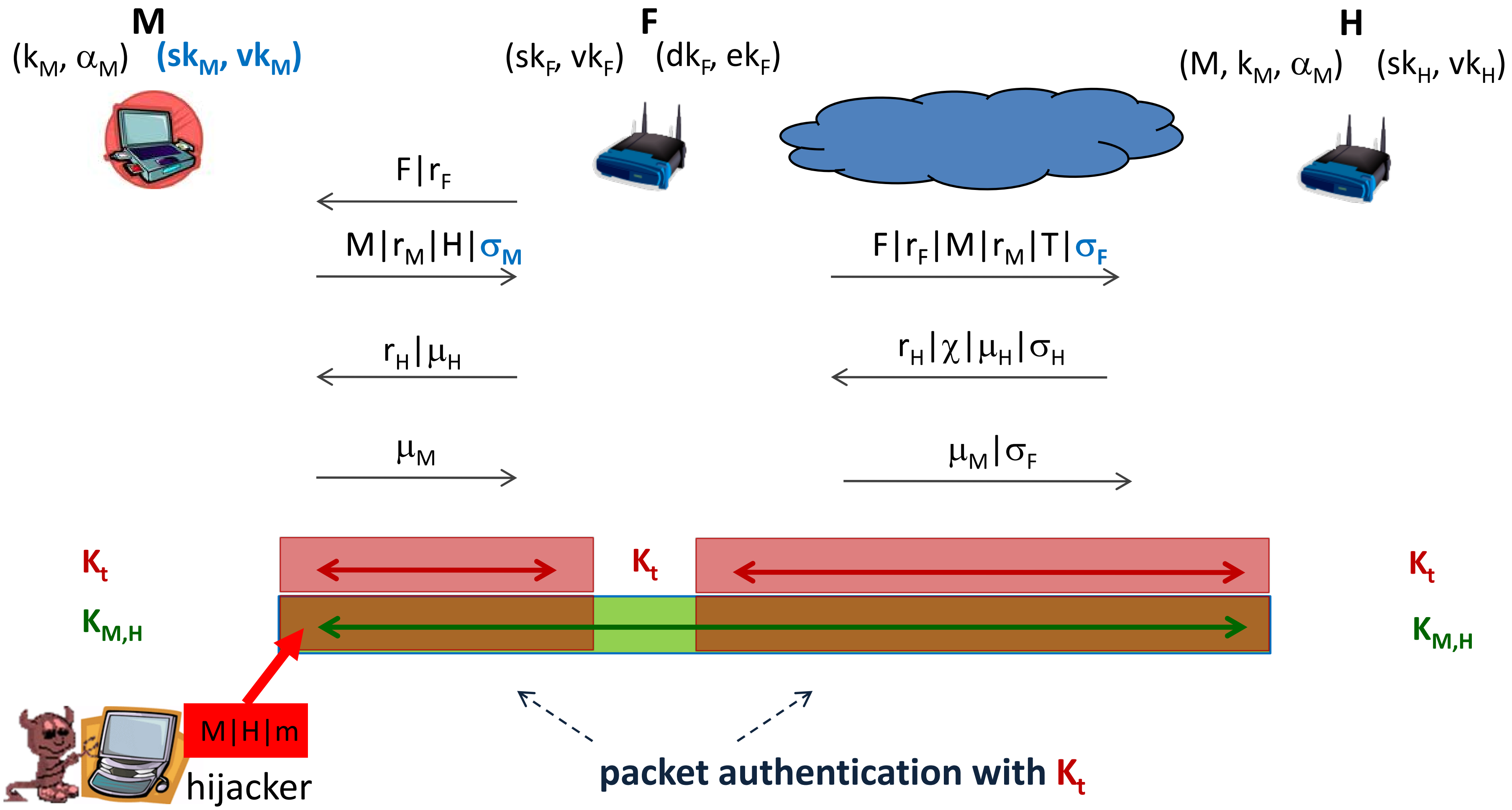
$K_t = PRF_{kt}(1,sid)$

$\mu_M|\sigma_F$

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

$K_{M,H} = PRF_{kM}(2,sid)$

# Resistance to DoS & Hijacking Attacks



**M**

$(k_M, \alpha_M)$ $(sk_M, vk_M)$

**F**

$(sk_F, vk_F)$ $(dk_F, ek_F)$

**H**

$(M, k_M, \alpha_M)$ $(sk_H, vk_H)$

$F|r_F$

$M|r_M|H|\sigma_M$

$r_H|\mu_H$

$\mu_M$

$F|r_F|M|r_M|T|\sigma_F$

$r_H|\chi|\mu_H|\sigma_H$

$\mu_M|\sigma_F$

$K_t$ $K_t$ $K_t$

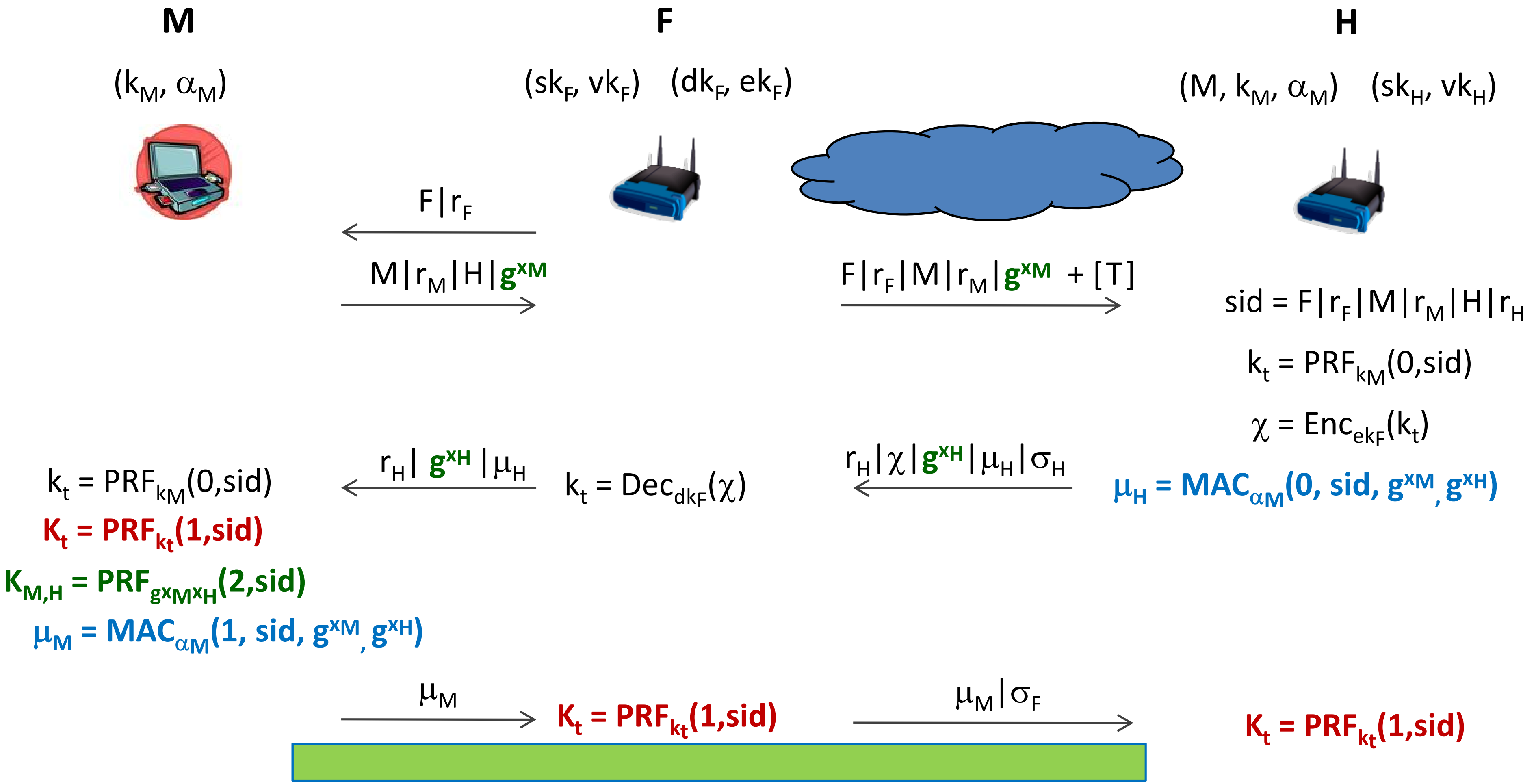
$K_{M,H}$ $K_{M,H}$

$M|H|m$

hijacker

**packet authentication with $K_t$**

# Forward Secrecy for $K_{M,H}$



**M**

$(k_M, \alpha_M)$

**F**

$(sk_F, vk_F)$ $(dk_F, ek_F)$

**H**

$(M, k_M, \alpha_M)$ $(sk_H, vk_H)$

$\xleftarrow{F|r_F}$

$\xrightarrow{M|r_M|H|g^{xM}}$

$\xrightarrow{F|r_F|M|r_M|g^{xM} + [T]}$

$sid = F|r_F|M|r_M|H|r_H$

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

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

$\mu_H = MAC_{\alpha M}(0, sid, g^{xM}, g^{xH})$

$\xleftarrow{r_H|\chi|g^{xH}|\mu_H|\sigma_H}$

$k_t = Dec_{dkF}(\chi)$

$\xleftarrow{r_H| g^{xH} |\mu_H}$

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

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

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

$\mu_M = MAC_{\alpha M}(1, sid, g^{xM}, g^{xH})$

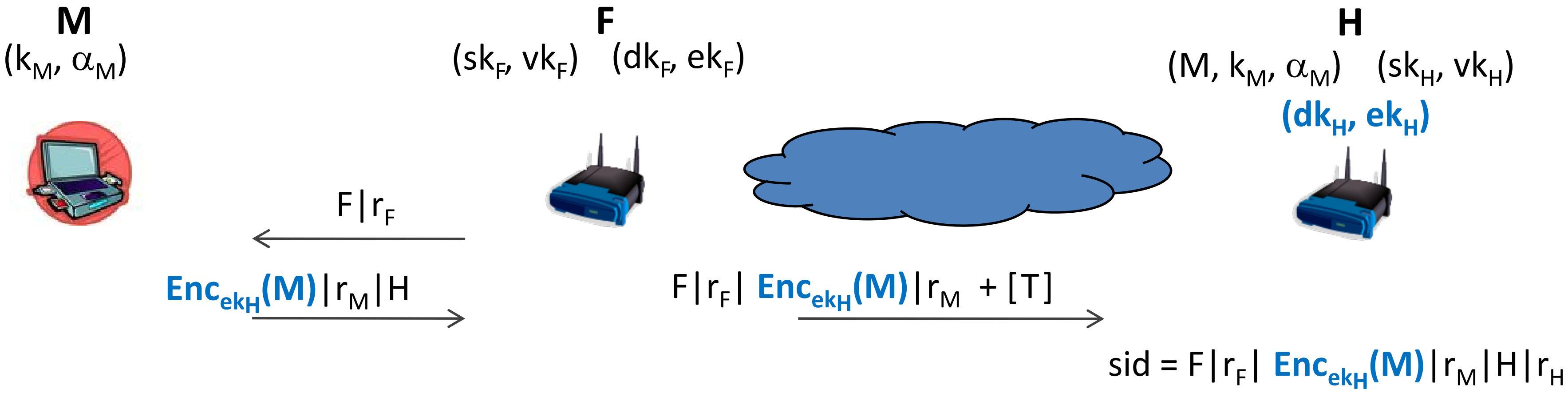
$\xrightarrow{\mu_M}$

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

$\xrightarrow{\mu_M|\sigma_F}$

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

# Unlinkability of Roaming Sessions



**M**

$(k_M, \alpha_M)$

**F**

$(sk_F, vk_F)$ $(dk_F, ek_F)$

**H**

$(M, k_M, \alpha_M)$ $(sk_H, vk_H)$

$\mathbf{(dk_H, ek_H)}$

$F|r_F$

$\mathbf{Enc_{ek_H}(M)}|r_M|H$

$F|r_F|\,\mathbf{Enc_{ek_H}(M)}|r_M\ + [T]$

sid = $F|r_F|\,\mathbf{Enc_{ek_H}(M)}|r_M|H|r_H$

# Summary & Conclusion

**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