Handover Security in Local Administrative Domain

Yi Ding
Email: yi.ding@cs.helsinki.fi

Handover security is essential to the success of mobile services in forthcoming IP-based heterogeneous wireless access environment. In WISEciti project we study the impacts of securing handovers and seek to achieve a balance between security and performance of handover in local administrative domains.

Research background

- IP-based backbone Internet with multiple wireless access technologies: GSM, WiFi, WiMAX, UMTS, etc
- Mobility management protocols for wireless and mobile environment: Mobile IP, HIP, Proxy Mobile IP, SIP, etc
- Handover across different access networks: vertical/horizontal, intra/inter-system
- AAA architecture for Authentication, Authorization, and Accounting
- Key management with mobility consideration
- Long term end-to-end trust between user and home network

Challenges

- Security in handover: essential user context transfer, mutual authentication, and key distribution and derivation
- Demanding requirements from time sensitive applications: VoIP, real time video
- Overhead from security: transmission delay, packet loss.
- Signaling traffic across the Internet
- General requirements from mobility solutions: scalability, efficiency, manageability, and interoperability
- Balance between security and performance: Seamless & Secure

Research question

Is it feasible to achieve a balance between security and performance regarding to the handover?

Proposed solution

Handover security within a well defined Local Administrative Domain.

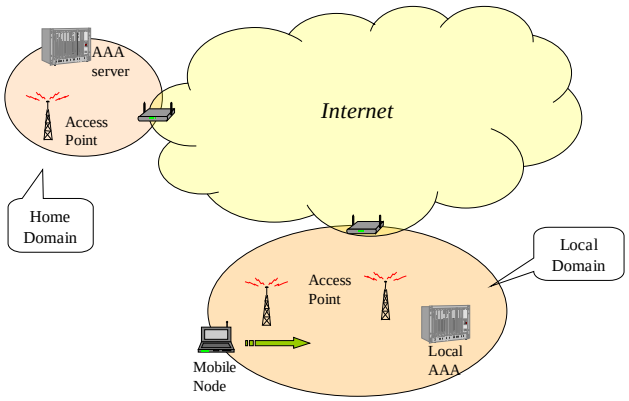

Figure 1: Localized Administrative Domain

Local Administrative Domain

An intranet, or a collection of networks, computers, and databases under a common administration. Computer entities operating under such administration may be assumed to share administratively created security associations. Optimization can be implemented in the domain to enhance the performance and security of the handover.

Benefits

- Avoid frequent signaling across the Internet
- Localized handover with less delay and loss
- Less key management overhead
- Possibility of fast re-authentication during a handover

Main technique

- Proxy Mobile IP: Mobile IP based, network initiated mobility support
- Extensible Authentication Protocol (EAP): authentication framework supporting multiple authentication methods
- EAP-AKA: key agreement for 3rd Generation authentication, with fast re-authentication
- Diameter: AAA protocol, carrying AAA related messages

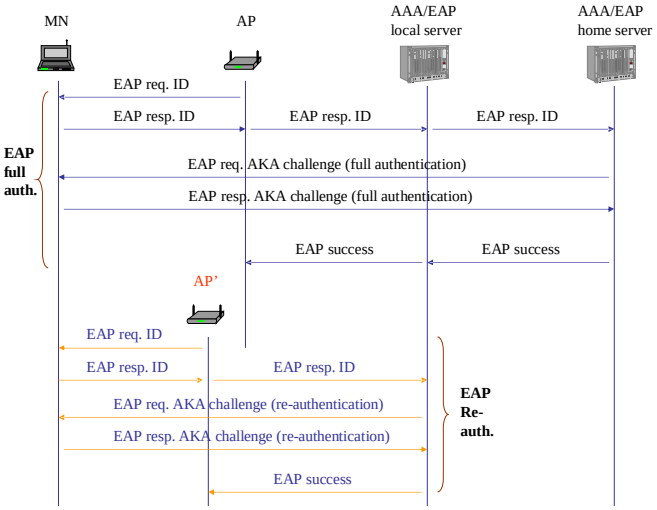

Figure 2: EAP-AKA authentication

Current work

- Analysis of handover security impacts
- Mobility requirements from the security point of view
- Implementing of an advanced simulation platform for EAP authentication with ns-2
- Performance analysis of handover security on TCP transmission
- Implementing Proxy Mobile IP for the advanced simulation platform

WISEciti – Wireless Community Services for Mobile Citizens (2008 – 2010)

http://www.cs.helsinki.fi/group/wiseciti/