Handover Security in Wireless and Mobile Networks

Yi Ding and Markku Kojo
[ yding, kojo ] @ cs.helsinki.fi

Department of Computer Science
University of Helsinki
WISEciti Project (2008 – 2010)
http://www.cs.helsinki.fi/group/wiseciti

Background and Motivation

- IP based heterogeneous wireless access environment
- Mobile devices with mobile Internet services
- Handover aims at: always-on connection, best possible performance and user experience

Merits

- Localized handovers with less latency
- Avoids frequent signaling across Internet
- Less key management overhead
- Fast authentication with re-authentication schemes

Challenges

- Security in handover: user confidential context, mutual authentication, key management
- Demanding requirements from real time applications
- Overhead from security implementations: latency, energy
- Seamless and Secure

Research Question

- How to best achieve a balance between security and performance in handover?

Proposal

- Local Administrative Domain (LAD)

Main Technique

- Secure Reachability: Proxy Mobile IP, IKEv2, IPSec

EAP based authentication: EAP-AKA', ERP

Current Work

- Security impact analysis
- Mobility requirements from security perspective
- Performance analysis of handover security in LAD
- Implementing handover security protocols in ns-2