Rafiqul Islam: Enhanced Security in Mobile IP Communication

Jukka Valkonen

1.3.2006

Agenda

1. Introduction
2. Background
3. Proposed Solution
4. Analysis

Introduction

- Master of Science Thesis
- Year 2005
- Royal Institute of Technology (KTH)
- Study based, no actual implementation
- Some important aspects omitted

Goal

"The chief goal of this masters thesis is to provide a trusted solution to provide security to Mobile IP using IP Security protocol suit"

IPSec

- Authentication and/or encryption at IP level
- Authentication Header (AH)
  - Integrity
  - Authentication
- Encapsulation Security Payload (ESP)
  - Same functionality as with AH
  - Also Confidentiality

IPSec (2)

- Security Association (SA)
- Security Parameter Index (SPI)
- Transport Mode
- Tunnel Mode
  - IP-within-IP

Mobile IP

- Mobility for IP
- Same IP, different networks
- Mobile Node, Correspondent Node, Home Agent, Foreign Agent
- Care-of address
- Tunneling

Mobile IP, problems

- Triangular Routing
- Ingress Filtering

Security Requirements

- Same connectivity and safety as in home network
- Attacks against home and foreign nework should be protected

Previous solutions

- IPSec in different parts of the network
- Sec MIP
  - IPSec tunnel between Mobile Node and Home Agent
  - All data transported through Home Agent
- Use of IPSec
  - IPSec tunnel between MN-HA, HA-FA and FA-MN
  - All data transported through Home Agent
  - MN-HA not needed

Solution

- Security Border Gateway (SBG)
  - Firewall with IPSec processing capability
- Correspondent Agent
- Mobile node doesn’t necessarily have to have IPSec processing capability (*)
- SBGs act as agents
- IPSec tunnels between HA-FA, CA-FA, FA-MN (*), HA-CA

Future Work

- In practice? (Simulator...)
- Handovers
- Certificate distribution

Analysis

- Works on paper, but...
- Contribution was quite small
- Discussions of results were very short
- Many carelessness errors

Thank You!

Questions?