Enhanced Route Optimization for Mobile IPv6 (RFC 4866)

Thanh Minh Tu Tran
Internet Technologies
IEM2 – SS08 – HAW
Overview

- Introduction
- Objectives
- Enhanced Route Optimization
  - Protocol Design
  - Protocol Operation
  - Security Considerations
- What else?
- Questions
Introduction

- Home Address Test
- Care-of Address Test
- If using non-cryptographic method
  - Lightweight (adv.)
  - Handoff latency (disadv.)
  - Security (disadv.)
  - Signaling overhead (disadv.)

=> Need improvement !!!
Objectives

- Reducing handoff latency
  - How to do …?
- Increasing security
  - How to do …?
- Reducing signaling overhead
  - How to do …?

=> Enhanced Route Optimization
Enhanced Route Optimization Protocol Design

- Cryptographically generated Home Address
  - To prove ownership & reducing signaling overhead

- Non-cryptographic Care-of Address

- Semi-permanent security association
  - Using Home Keygen Token
  - Reducing handoff latency & signaling overhead

- Initial Home Address test
  - Preventing spoofing attack
Protocol Design

- Concurrent Care-of Address test
  - Increasing handoff efficiency

- Credit-based authorization
  - Preventing redirection-based flooding

- Parallel home & corresponding registration
  - Increasing handoff efficiency
Figure 1: Correspondent registration with authentication by a proof of the mobile node's knowledge of a permanent home keygen token; concurrent care-of address test.
Protocol Operations
Topic Overview

- Sending Binding Update Messages
- Receiving Binding Update Messages
- Sending Binding Acknowledgment Messages
- Receiving Binding Acknowledgment Messages
- Sending CGA Parameters
- Receiving CGA Parameters
- Sending Permanent Home Keygen Tokens
- Receiving Permanent Home Keygen Tokens
- Renewing Permanent Home Keygen Tokens
- Handling Payload Packets
- Credit Aging
- Simultaneous Movements
Security considerations
Home address ownership

- Prove the private key’s owner of the home address (public key)
- \texttt{CGA\_Generator(private\_key, CGA\_params) = public\_key = home\_add.}
- \texttt{Extension\_func(modifier, public\_key) = string\_with\_leading\_zeros} (encoded in the 3 bits RES)
- CGA use RSA public & private keys
Security considerations
Care-of Address Ownership

- Cryptographical generated Care-of Add.
- Not solve the problem totally
- Flooding packets could impact the whole network
  => Have less effectiveness on Flooding protection
  => Expensive computation
  => It is not used
Security considerations
Credit-Based Authorization

- Home keygen token – symmetrical cryptography
- Redirection-based flooding attack
- CN sends packets in UNVERIFIED state
- Non-amplified redirection-based flooding
- => Attacker has no interest

Figure 4: Handling outbound payload packets
Security considerations
IP Address ownership of C.N.

- CN sends CGA and signature parameter option and home keygen token
- MN use CN’s CGA & signature to calculate & compare the home keygen token
- In case CN has no CGA properties
  - Priority authentication
  - Obtaining certainty if IP add. is a CGA
What else?

- Security considerations
  - Time Shifting Attacks
  - Replay Attacks
  - Resource Exhaustion

- Option Formats and Status Codes
  - CGA Parameters Option
  - Signature Option
  - Permanent Home Keygen Token Option
  - Care-of Test Init Option
  - Care-of Test Option
  - CGA Parameters Request Option
  - Status Codes

- Protocol Constants and Configuration Variables
- IANA Considerations