Mobile IPv6 Route Optimization Enhancements: Revision of draft-irtf-mobopts-ro-enhancements

Christian Vogt, Jari Arkko
chvogt@tm.uka.de, jari.arkko@ericsson.com

Reviews, Major Discussion Items, Additions, Changes

63th Meeting of the Internet Engineering Task Force
Mobopts Research Group Session, August 2, 2005

Reviewers

Samita Chakrabarti

Francis Dupont

Thierry Ernst

Gerardo Giaretta

James Kempf

Rajeev Koodli

Gabriel Montenegro

Vidya Narayanan

Fan Zhao

Thank you, folks!

Role of Ingress Filtering

Note on ingress filtering as part of Introduction

- Clarifies position of the draft
- Acknowledges general benefits if ingress filtering
- Points out why it should not be relied upon (for the purpose of MIPv6)
- Emphasizes that opinions differ

Role of PKIs for Mobility

Clarification of the position taken

- Not necessarily a scalability issue (examples of CAs with millions of certificates), but…
- More "aggressive" application pattern:
  - Traditionally, few checks, only at beginning of session
  - With mobility, more frequent checks (causing overhead for CNs)
  - Checks may occur in middle of session (causing delay)
- Problems with CRLs
- Coordination of address assignment w/ certification is problematic
- Attractive attack target (esp. w/ many certificates)

Are Redirection-Based Flooding Attacks Irrelevant?

Statement on malicious redirection and flooding

- Typical flooding strategy is by malware,
  so why would the attacker use redirection?
- Because redirection…
  - …could be another tool for the attacker
  - …could be used in combination with classical flooding
  - …would be a "standardized" flooding tool ☹
- Trust relationships don't help:
  Nodes may become a redirecting zombie w/o malicious intents
- Reachability test required even for CGA-based CoAs;
  uniqueness property does not protect against network flooding

Additions to the Draft

Robustness objective

- In principle, RO could work w/o home agent

Network mobility

- Mobile router
- Correspondent router

Credit-Based Authorization

- New, more understandable text

Perspectives

- What we need are RO techniques which can be useful in many different scenarios, like…
  - Optimistic behavior
  - Proactive behavior
  - CGA-based security
  - Credit-Based Authorization

  What we don't need is limited-applicability RO techniques
- Always a trade-off btw. general applicability and efficiency benefits (e.g., end-to-end optimizations vs. infrastructure support)

Still to Do: Make the Draft More Concise

Remove section that don't attend to RO

- HMIPv6
- FMIPv6
- Processing improvements
- Delegation

Remove text already published elsewhere

- Disquisition of security threats