the 57th IETF

Threat Analysis for NEMO

July 16, 2003

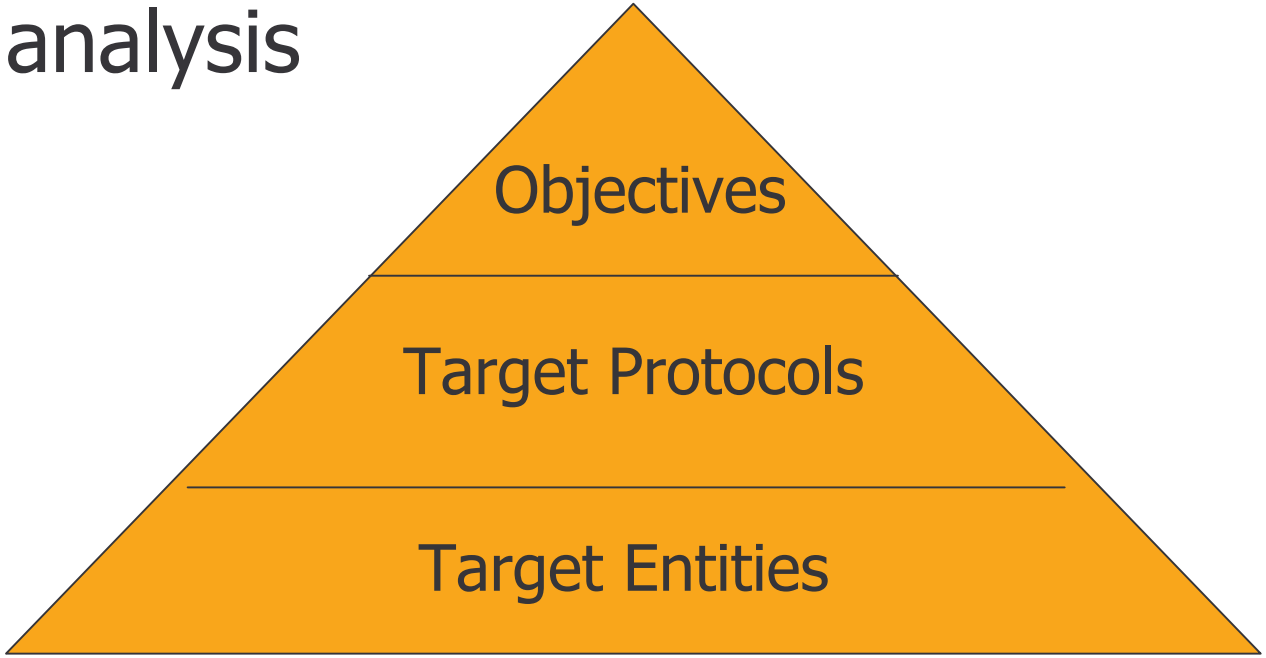
Souhwan Jung, Soongsil University, Korea
Felix S. Wu, UC Davis, USA
Hyungon Kim, Sungwon Sohn, ETRI, Korea
souhwanj@ssu.ac.kr

Outline

- Three-layer threat model
- Generic threats to NEMO
  - Threats to protocols/services
  - Threats to network entities
- Discussion: What are the threat issues specific to NEMO basic support draft?

Three-layer Threat Model

- draft-jung-nemo-threat-analysis-00
- Provides a generic approach for threat analysis



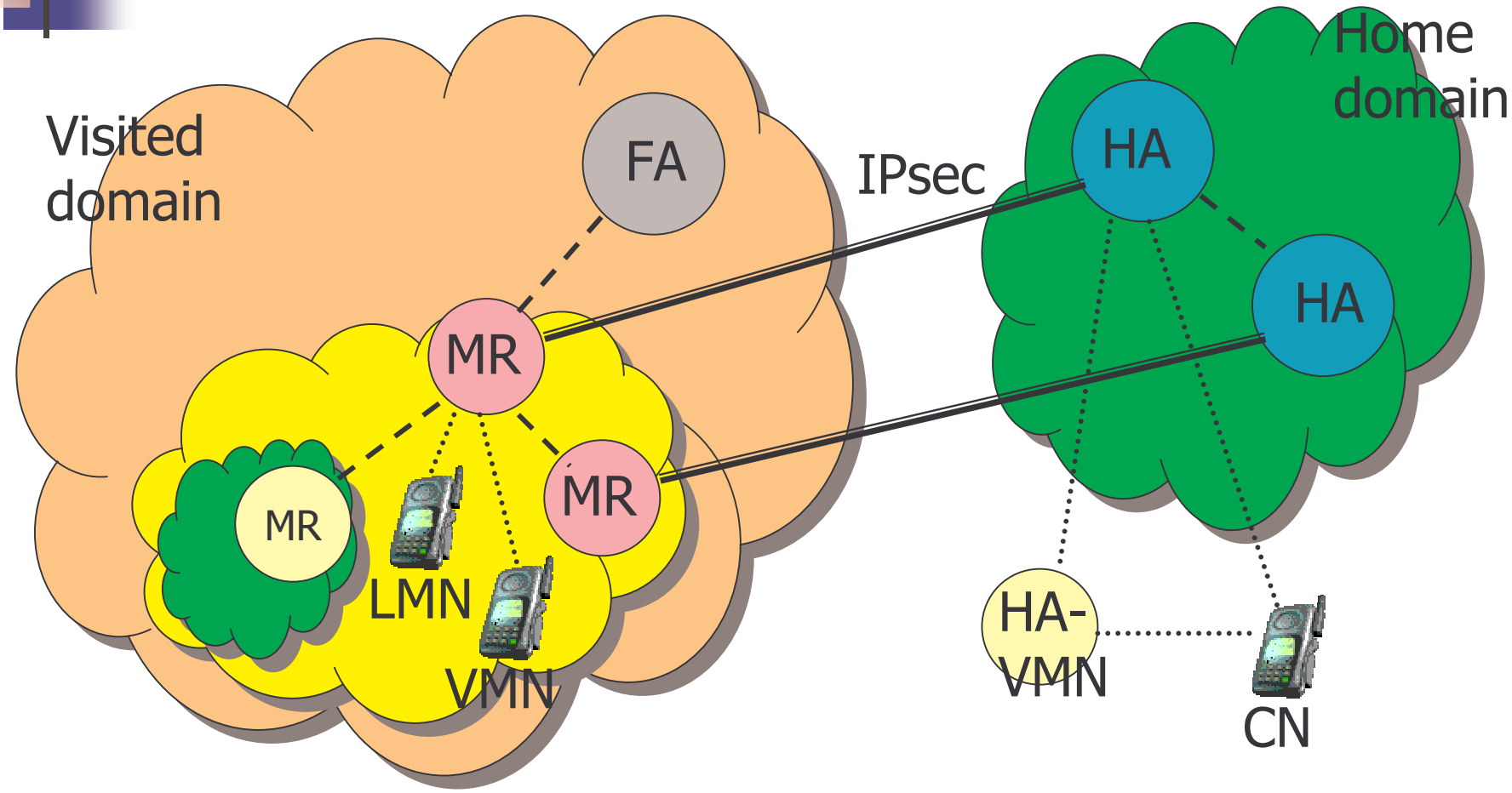
Threat Model

- Objectives: a limited number of goals of attacks in abstract level

  e.g. eavesdropping, impersonation, modification, unauthorized access of resources, repudiation etc.

- Target Protocols/Services
  - Messages in signaling and data paths
- Target Entities/Entry Points
  - network entities
  - MR, HA, FA, MNN, CN etc.

Example of NEMO Configuration



Generic Threats to NEMO

- Threats to signaling and data path
  - MR-FA, MR-HA, MR-MNN, MR-CN
- Threats to network entities
  - Compromise of MR or HA
- Other threats
  - DoS
  - Traffic analysis

Discussion

What are the threat issues specific to NEMO basic support draft?

Issue 1. Threat to MR

Issue 2. Threat to HA

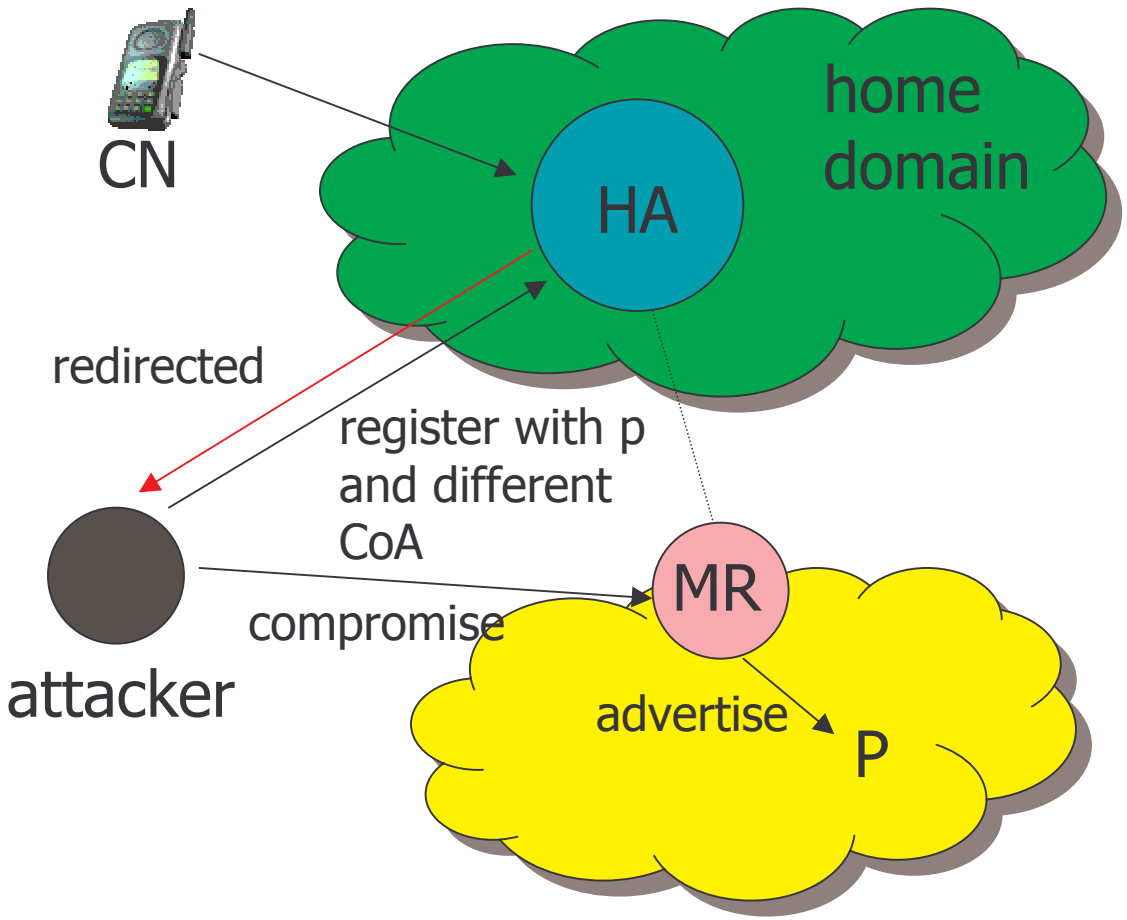
Issue 3. Threat related to multi-homing

Issue 4. Traffic analysis

Issue 1: Threat to MR

- MR is the most important entity in NEMO.
- IPsec that protects the signaling messages between MR and HA may not be enough.
- Compromise of MR can cause serious problems in NEMO operations.
- Correctness of BU is especially critical.
- Somebody (e.g. HA) needs to double-check whether MR is working correctly.

Example of Issue 1



Issue 2: Threat to HA

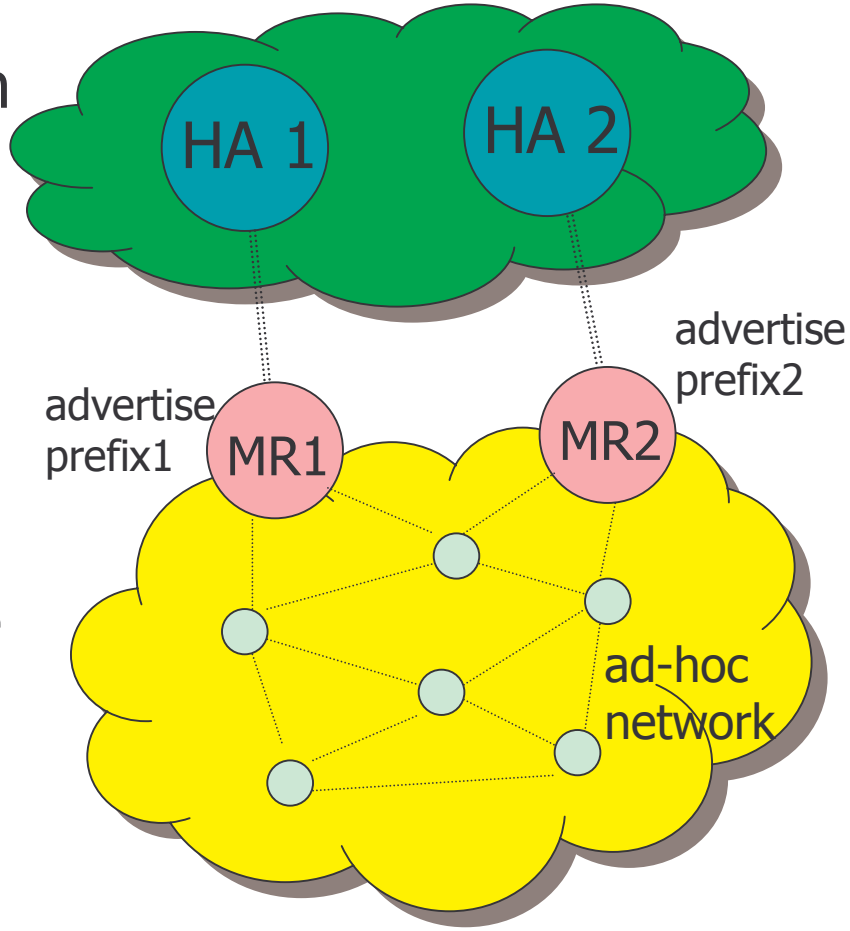
- Prefix table has prefix information of MRs, and is maintained in HA.
- Prefix table definitely should be protected by an authorization mechanism.
- Anybody who want to check and modify the prefix table needs to get authorization first.

Issue 3: Threat related to multi-homing

- Right packets should be forwarded by MR or HA to the right destination.
- In case of multi-homing, data forwarding may not be correct as expected.

Example of Issue 3

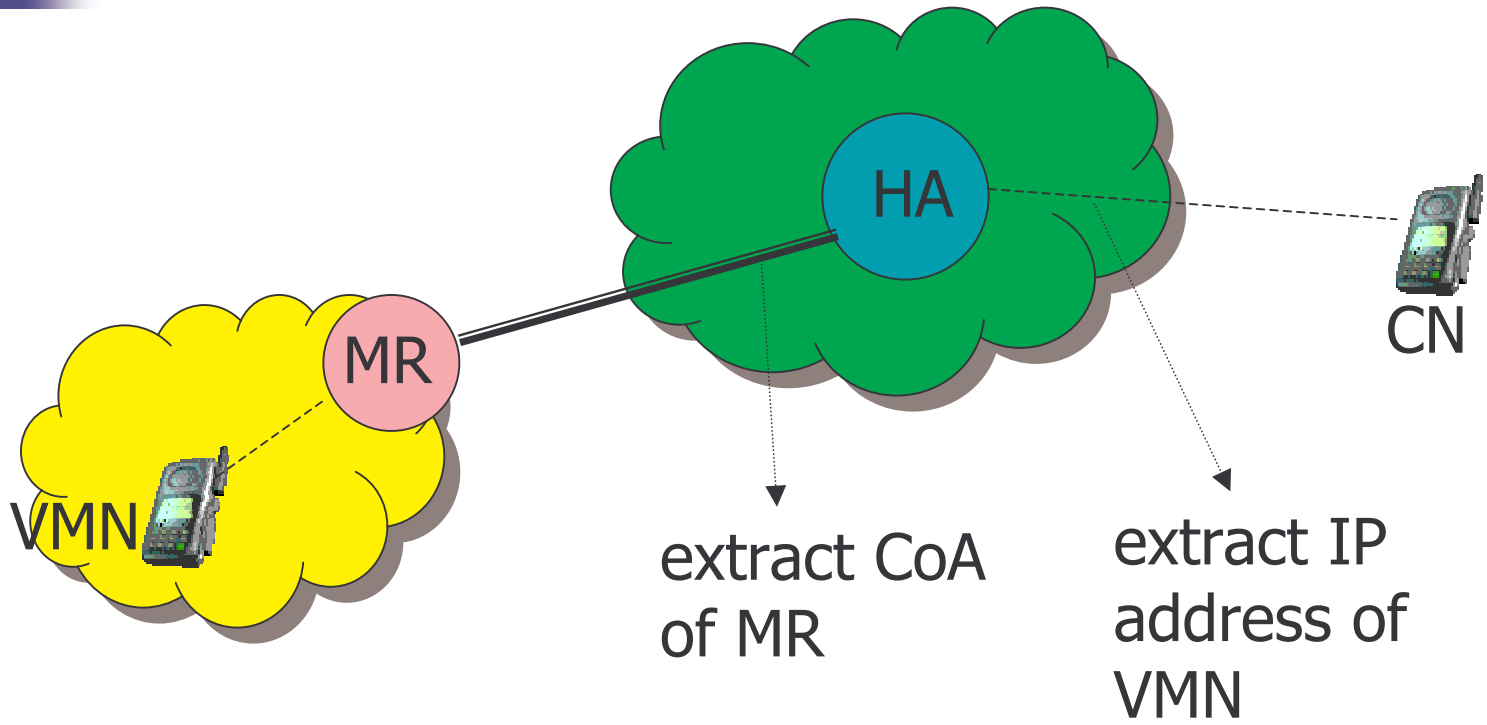
- Some nodes get configured with p1, and others are with p2.
- Packets are routed according to their destination addresses depending on the routing algorithms.
- Some packets out of p1 may be routed to MR2. Then they will be dropped at HA2.
- DoS attack may be possible.



Issue 4: Traffic Analysis

- All the traffic from mobile networks go through the bi-directional tunnel between MR and HA.
- Analysis of correlation between the amount of incoming and outgoing traffic of HA may induce the location information of VMN.

Example of Issue 4



- Location information of VMN may be extracted by traffic analysis.

More threat issues to discuss?

Thanks!