Hierarchical Host Identity Tag Verification

Dmitriy Kuptsov, Boris Nechaev
Helsinki Institute for Information Technology
Aalto University

IETF 80, Prague, Czech Republic
29.03.2011
Motivation and goals

Motivation

- Off-load Host Identity Tag (HIT) verification to trusted third party (TTP)
- No certificates
- Efficient HIT revocation
- Simple stateless routers (security gateways)
- Only symmetric cryptographic primitives

Goals

- Security gateways can:
  - Can recognize domain authority from Hierarchical HIT (HHIT)
  - Send HIP packet to domain authority for authentication
- Domain authority can:
  - Verify if it serves HHIT and it is valid
  - Authenticate the sender
Design

- Flat identifier comprises: trusted third party identifier (32 bits) and host identifier (96 bits)
- Hosts negotiate a secret with their domain authorities (out-of-band)
- Security gateways implement 3 simple rules:
  - Forward I1 packet without verification
  - Forward R1, I2 and R2 packets form “untrusted port” to “trusted port”
  - Forward R1, I2 and R2 packets from “trusted port” to destination
- Domain authority authenticate the clients:
  - Challenge-response-based authentication
    - Similar to “End-Host Authentication for HIP Middleboxes” by Heer et al.
- Clients should solve all advertised challenges
Implemented prototype

1. a) Lookup secret for A's HHit
   b) Store nonce \{Key=(A's HHit || B's HHit), value = nonce\} 
2. If 1. success send R1 with challenge ENC\{nonce || Hash(R1), secret A\} 
3. A solves the challenge and responds ENC\{nonce + 1 || Hash(I2), secret A\} 
4. Verify the challenge and if OK send to B
Performance issues

- Simulated storm of \textit{l1} packets with \texttt{exp(lambda=1)}, \texttt{exp(lambda=10)}
- Loss: %3 - %10
- Almost all losses caused by DHT
Conclusions

Pros:
- Stateless security gateways
- Efficient HIT revocation
- No certificates
- Symmetric primitives only

Cons:
- DHT increases delay and loss considerably
Thank you!
Questions?