HELSINKI
INSTITUTE FOR
INFORMATION
TECHNOLOGY

Status report on HIP-CERT

HIP and Strong User Authentication

Samu Varjonen

74th IETF - San Francisco, CA, USA

HIPRG, Monday March 23

Status report on HIP-CERT

- draft-ietf-spki-cert-structure-06.txt
  - Gives detailed structure of certificates that satisfy the theory RFC.
  - Discussions with Carl Ellison on the future of the structures draft
  - There will be new version, hopefully before Stockholm IETF

- Should X.509.v3 be the default choice of certificate?
  - Wide industry support
  - SPKI is not that widely used

- Any comments on the draft?

Agenda for HIP-SRP

- Motivation
- Secure Remote Password protocol
  - Negotiation
- Usage in Base Exchange
  - End-to-End
  - End-to-Middlebox
- SRP related parameters
- Obstacles

Motivation

- HIP is about identifying the host

- Identifying the user is also important

- Possible use cases:
  - Organizations and mobile employees
  - On-path service providers, for example middlebox offering forwarding service

- By adding user authentication for the tunnel creation:
  - We can ACL based on used HIT and password verifier
  - Or we can require HIP and use password verifiers for ACL

Secure Remote Password (SRP) protocol

- SRP allows a user to authenticate himself to a server.
  - Resistant to dictionary attacks mounted by an eavesdropper
  - Does not require a trusted third party.
- Upon initialization of SRP:
  - User gives a username and a password
  - SRP implementation takes a random salt
  - Verifier is calculated from these values and stored on the server
- SRP negotiation creates large private key shared between participants
- Evidence of knowing the username is calculated by using the key
- Details in RFC 2945

SRP negotiation

```
  Initiator                                       Responder
                   Username, Public value
              --------------------------------->
                     Salt, Public value
              <---------------------------------
Calculate the
evidence
                          Evidence
              --------------------------------->
                                                   Verify evidence
                                                   Calculate the
                                                   evidence
                         [Evidence]
              <---------------------------------
[Verify evidence]
```

SRP related Parameters

- The SRP_CV parameter is used to convey the users' username and the public value of the client to the server. SRP_CV parameter is used in I1 control packet.
- The SRP_SV parameter is used to convey the group and server values to the client. SRP_SV is used in R1 control packet.
- SRP_E parameter is used to convey the evidence between peers. If this parameter is in I2 it is the clients evidence and if this parameter is in R2 it is the server's evidence.
- *_M parameters are unsigned and used with middleboxes and to preserve the possibility for R1 pre-creation

Usage in Base Exchange

```
   Initiator                              Responder
               I1: SRP_CV
              -------------------------------->
                                               select precomputed R1
               R1: puzzle, SRP_SV, key, sig
              <--------------------------------
check sig                                      remain stateless
solve puzzle
               I2: solution, SRP_E, {key}, sig
              -------------------------------->
calculate                                      check puzzle
session key                                    check sig
               R2: sig, [SRP_E]
              <-------------------------------
                                               calculate session key
check sig                                      Verify evidence (M)
[Verify evidence (M)]
```

SRP and middlebox

```
Initiator               Middlebox                        Responder

                   .-----------------.
 I1, SRP_CV_M      |                 | I1, SRP_CV_M
-----------------> |                 |---------------------------->
                   |                 |
 R1, + SRP_SV_M    | Add SRP_SV_M    | R1
<----------------- |                 |<----------------------------
                   |                 |
 I2, + SRP_E_M     | Verify SRP_E_M  | I2, SRP_E_M
-----------------> | Let I2 through  |---------------------------->
                   |                 |
 R2                |                 | R2
<----------------- |                 |<-----------------------------
                   '-----------------'
```

Obstacles

- IPsec tunnels are created between hosts
- This allows one user to open a tunnel and another user on the same initiator to use the same tunnel
- Main use case is mobile equipment with one user
- Tunnels can be bound to flows, Simultaneous Multi-Access extension to the Host Identity Protocol: draft-pierrel-hip-sima-00
- Other solutions for binding tunnels to users/processes/applications exist

Thanks

If there is any interest for the topic, this draft could be generalized to “User Authentication in HIP”

Questions? Comments?