CERT Parameter

draft-varjonen-hip-cert-00

Varjonen, Samu and Heer, Tobias

71st IETF - Philadelphia, PA, USA

March 13, 2008

Agenda

- What and why?
- CERT Parameter
- Groups, counts and IDs
- Certificate types
- SPKI example
- Considerations

What ...

- Host Identity Protocol uses Public/Private key pair as host identity

- These keys can and are used to sign information

- This draft defines a parameter that is used to transmit these digital signatures

- There exists articles and research that describe systems that use certificates and HIP in different ways.

… and …

- PISA: P2P Wi-Fi Internet Sharing Architecture
  - Home router issues an access token to MNs so that MNs can access the network from other access routers in the system
- “Hop of trust”
  - Initiator finds common friend (Responder->Bob->Initiator)
  - Initiator adds the certificate (Bob->Initiator) to I2
- HIPernet
  - Uses delegation/authorization certs to create trusted virtual domains in untrusted grid environments
- Non-repudiable service usage with host identities
  - Uses BEX packets to transport service certificates

... why?

- There has already been one CERT parameter
- It was left out of the standardization work
- But now there is more people using HIP and certificates together
- So we need a unified way to transmit certificates in HIP packets

CERT Parameter (1/3)

- We do not specify any semantics for the certificates
- CERT parameter can be used in I1, R1, I2, R2 and UPDATE messages
- CERT parameter can be inside HIP SIGNATURE and is non-critical
- Type number for the parameter is 768
- Length in octets, excluding Type, Length, and Padding

CERT Parameter (2/3)

- Group ID groups multiple related CERT parameters
- Total certificate count of certificates that are sent, possibly in several consecutive HIP control packets.
- The sequence number (Cert ID) for the certificate
- Type of the certificate
- If necessary, padding to make the TLV a multiple of 8 bytes.

CERT Parameter (3/3)

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Type              |             Length           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Cert group   |  Cert count   |    Cert ID    |   Cert type   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Certificate                          /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                               |            Padding           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Groups, counts and IDs

- Each HIP packet can contain multiple CERT parameters
- If certificates form sequences, the Cert group and count fields have to be used
- Certificates not belonging to a group have unique cert group value inside one HIP association and cert count as one
- Certificates with same group value are considered to belong to a same logical group and count informs about the number of certificates belonging to this group
- Groups can be divided over multiple sequential packets
- Cert ID must start from one and it identifies the certificates place in the sequence

Certificate types

- Certificate type defines which type of certificate is in case
- SPKI is type number 1
- X.509.v3 is type number 2
- All implementations MUST support SPKI
- New types can be defined if there is need for other types of certificates

SPKI example

```
(cert
        (issuer (hash hit 2001:14:fd64:ca3b:9ef2:8374:ec80:4f20))
        (subject (hash hit 2001:13:724d:f3c0:6ff0:33c2:15d8:5f50))
        (tag <capability-name_1> (arg <arg_1>)
        ...
        (tag <capability-name_n> (arg <arg_n>)
        (propagate)
        (online crl http://www.infrahip.net/crl)
        (not before 1/1/2008)
        (not after 12/31/2008)
)
```

Considerations

- For IANA the type is already 768 (from draft-ietf-hip-base-10)
- Cert types defined in draft-varjonen-hip-cert-00
- Cert Group and IDs managed locally by peers
- Using CERT parameter in I1 may lead to denial-of-service situations
- When using groups, sending of IDs in wrong order or skipping some IDs can cause “fragmentation” problems
- Size of the certificates can be a problem
- Do we support IKE hash or URL techniques

References

- [1] Authorising HIP enabled communication, Seppo Heikkinen, Proceedings of The 10th International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS07). San Diego, USA. Jul 2007
- [2] Non-repudiable service usage with host identities Seppo Heikkinen, Proceedings of The Second International Conference on Internet Monitoring and Protection (ICIMP07). Santa Clara, USA. Jul 2007
- [3] HIPernet: A Decentralized Security Infrastructure for Large Scale Grid Environments, Laganier, J. and Vicat-Blanc Primet, P, International Conference on Grid Computing, Proceedings of the 6th IEEE/ACM International Workshop on Grid Computing, Pages 140-147, 2005
- [4] PISA: P2P Wi-Fi Internet Sharing Architecture, Tobias Heer and Shaohui Li, and Klaus Wehrle, Seventh IEEE International Conference on Peer-to-Peer Computing, P2P 2007

The end

Thanks!
Questions?
Suggestions?