Security and Trust of Public Key Cryptography for HIP and HIP Multicast

Amir K.C, Aalto University, Helsinki, Finland
Harri Forsgren, University of Helsinki, Helsinki, Finland
Kaj Grahn, Arcada University of Applied Sciences, Helsinki, Finland
Timo Karvi, University of Helsinki, Helsinki, Finland
Göran Pulkkis, Arcada University of Applied Sciences, Helsinki, Finland

ABSTRACT

Host Identity Protocol (HIP) gives cryptographically verifiable identities to hosts. These identities are based on public key cryptography and consist of public and private keys. Public keys can be stored, together with corresponding IP addresses, in DNS servers. When entities are negotiating on a HIP connection, messages are signed with private keys and verified with public keys. Even if this system is quite secure, there is some vulnerability concerning the authenticity of public keys. The authors examine some possibilities to derive trust in public parameters. These are DNSSEC and public key certificates (PKI). Especially, the authors examine how to implement certificate handling and what is the time complexity of using and verifying certificates in the HIP Base Exchange. It turned out that certificates delayed the HIP Base Exchange only some milliseconds compared to the case where certificates are not used. In the latter part of our article the authors analyze four proposed HIP multicast models and how they could use certificates. There are differences in the models how many times the Base Exchange is performed and to what extent existing HIP specification standards must be modified.

Keywords: Certificates, HIP Base Exchange, Host Identity Protocol (HIP), Public Key Certificates (PKI), Public Key Cryptography

INTRODUCTION

Host Identity Protocol (HIP, specified in RFC 5201) was developed to give hosts cryptographically verifiable Host Identities (HIs) separate from their IP addresses. HIP provides a method to establish IPsec ESP Security Associations (SAs) and support for IP mobility.

The Base Exchange protocol creates a SA between communicating peers. Messages are digitally signed. Current HIP standard uses public key cryptography with RSA or DSA keys for signing. In order to be completely sure about signatures, verifiers should check the status of the used public keys. The current HIP standard does not require certificates to validate public keys, but in Base Exchange messages are reserved fields which can carry certificates.
We examine in this article some methods to derive trust in public key based HIs and in the binding between IP addresses and HIs. We give an overview on HIP and some background on its current security mechanisms. We examine two methods to achieve authenticated sessions, the use of DNSSEC (RFC 4033) and the use standard PKI certificates for HIs Base Exchange. Certificates offer more trust than DNSSEC. We examine alternative certificates implementations and modifications needed in current standards. We analyze security implications and measure computational costs. Finally, we describe four HIP multicast models (Kovácscházi & Vida, 2007; Jokela, 2009; Jokela, et al., 2010; Zhu & ATwood, 2006) and analyze their applicability in the context of certificates.

SURVEY OF HIP AND ITS SECURITY

In this section we give an overview of HIP and its security mechanisms. For more detailed surveys, see (Gurtov, 2008; Nikander et al., 2010).

Cryptographic Name Space and the Base Exchange

HIP adds a new name space to the TCP/IP protocol stack. Network hosts are identified HIs, which are public cryptographic keys. Therefore, peers authenticate directly by their HIs. HIP is backwards compatible, i.e. no changes to the network infrastructure or to applications are needed. In order to bind other names to HIs, Host Identity Tags (HITs) and mechanisms like DNSSEC, SPKI certificates, and X.509 certificates are available.

If an entity A wants to start a HIP connection with B, A first makes a DNS query to get B’s IP address and HI. In this query, A uses human-friendly host names. It is essential that A can trust the DNS response. If the response data is incorrect, then A could communicate with a malicious entity without noticing it.

There can be only one HIP SA between a pair of HITs. Multiple SAs between two hosts require several HITs per host. Therefore, a host may have several RSA or DSA public/private key pairs.

A HIP connection is negotiated by a Base Exchange protocol, see Figure 1. An initiator I starts the negotiation with a responder R. Messages R1, I2, R2 are signed (sig). R1 and I2 contain Diffie-Hellman parameters (DH(r), DH(i)), a puzzle (in R1), its solution (in I2), and a puzzle difficulty parameter K. R1 and I2 may contain certificates. Normally the signature in R1 can be calculated beforehand, because the signature does not contain HIT(i) or the checksum if a puzzle is used. After receiving R1, I calculates the Diffie-Hellman secret. R calculates the same secret after receiving I2. This secret is used in the hmac values in I2 and R2. The hmac value is checked before the signature is checked. The CERT parameter is optional. It is contained in the variable size part of the HIP packet. The maximum HIP packet length is 2040 bytes and the maximum parameter field length is 2008 bytes.

The standard also allows an opportunistic mode in which I starts Base Exchange without HIT(r) in I1 (it is set to zero). This mode creates security vulnerabilities and should be avoided in unsecure environments.

Security Mechanisms in HIP

In terms of security, confidentiality and authentication, HIP aims at the high-level goals of payload security, protocol security, and secure

*Figure 1. HIP base exchange*

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>I.</td>
<td>I → R: HIT(i), HIT(r)</td>
</tr>
<tr>
<td>R1</td>
<td>R → I: HIT(r), HIT(i), puzzle, DH(r), K(r), [CERT], sig</td>
</tr>
<tr>
<td>I2</td>
<td>I → R: HIT(i), HIT(r), solution, DH(i), K(i), [CERT], hmac, sig</td>
</tr>
<tr>
<td>R2</td>
<td>R → I: HIT(r), HIT(i), hmac, sig</td>
</tr>
</tbody>
</table>
Trust and Stability in Heterogeneous Multimedia Networks
www.igi-global.com/chapter/trust-stability-heterogeneous-multimedia-networks/40789?camid=4v1a