Host Identity Protocol for End-to-End Security in IoT

Huda Mulani[1], **Aruna Gawade**[2]

[1]Student, Computer Engineering Department, D. J. Sanghvi College of Engineering, Mumbai, India

[2]Professor, Computer Engineering Department, D. J. Sanghvi College of Engineering, Mumbai, India

Abstract: ***This document aims to provide secure authentication of hosts using Host Identity Protocol. The impact and occurrence of Denial of service attacks and Man in middle attacks are tried to overcome and minimized. Furthermore, the various limitations in the HIP protocol are addressed here. The packet loss, network congestion, replay attack, packet flooding and spoofing are major considerations of HIP protocol are aimed to overcome.***

Keywords: Internet of Things, IoT, Wireless Sensor Networks, Host Identity Protocol, Multihoming and Mobility, HIP Base Exchange, Man in Middle

1. Introduction

As the Internet becomes increasingly utilized by mobile users, who are bound to roam freely and attach to a variety of networks, host mobility becomes a key feature of the Next Generation Network (NGN) which is the All-IP based heterogeneous networks . Host mobility in the Internet introduces technical challenges, such as session continuity, host reachability, and security threats. A major issue is the duality problem of IP addresses in serving at the same time as both host identifier and locator in the Internet.Host Identity Protocol (HIP) is developed in Internet Engineering [1].

The HIP protocol is an end-to-end (e2e) security association establishment protocol that aims at integrating security, multihoming and mobility management. The cornerstone of HIP is the separation of nodes location and identifier by means of introducing a new namespace, named Host Identity (HI), for identifying nodes. The protocol defines a Base Exchange (BEX) to establish a Security Association (SA) together with a signaling exchange to update this association through UP-DATE messages[2].

The Host Identity Protocol (HIP) as the main building block for network-layer security in WSNs[3]. For identification of nodes, public keys are used by HIP. DOS attacks are eliminated by puzzle mechanism. Encryption is supported using IPsec protocol. A Diffie-Hellman key generation algorithms are approached for creating session key in between pair of nodes. Signature mechanism is adopted for authentication between peers. HIP security architecture is strengthen by integrating all of above mechanisms, thus creating WSN as a safer platform in a network.

The Host Identity Protocol (HIP) solves the semantic overloading of IP addresses by introducing a new name space, the Host Identity name space. Based on Rendezvous servers (RVS) and DNS Extension ,host mobility is supported by HIP. In addition, the performance in HIP is better than Mobile IPv6 [4].

End-to-end security along with mobility and multihoming is provided by The Host Identity Protocol . The innovative approach taken by HIP is the separation of the identifier currently used to define both the identity and the location of a host. Instead of relying only on the IP address of a host, the HIP protocol maintains the IP address specified in its network layer to refer to the location of a host, but it defines a new namespace for the identities of the host [5].

To represent this namespace, a public/private key infrastructure is used where a cryptographic hash is performed to the identity of the host (the private key of the pair) and a 128-bits Host Identity Tag (HIT) is created as a public key, and made available for its usage in the transport and application layers instead of the IP address as the identity of a host. This separation of identity/location, allows easy mapping of a host to different locations, hence allowing an easy implementation of mobility and multihoming, but it changes the TCP/IP protocol stack by adding the HIP layer between the IP layer and the TCP layer when the new namespace is created [5].

The secured end-to-end encrypted sessions created between hosts provides the communications using the Host Identity Protocol with an additional layer of security that the current TCP/IP stack lacks [5].

2. Host Identity Protocol

HIP is an end-to-end protocol which strengthens security against some attacks. In this section, we describe some basic architecture of HIP, which is important to a secure several types of attacks.

A. Locator/ID Split

In an ordinary Internet connection, an IP address performs two roles,they identify the host in network i.e a host ID is obtained and gives information as to where is the host located in the topology of a network. Because of this, it is difficult to cope with various requests flexibly. For instance, a mobile host may want to connect to an another network seamlessly. In such a scenario only the location of the host is changed irrespective of it's ID. Based on this Locator/ID

Split concept.The parameters used by HIP to determine ID are Host Identity and Host Identity Tag respectively. For determining locator and IP address is the parameter. In this paper, we adopt HIP with some reasons. That is, HIP hosts can authenticate each other with data connection encrypted. Additionally, we think HIP can be applied to secure ubiquitous networks without major changes to existing system [6].

B. Host Identity and Host Identity Tag

All HIP hosts have a pair of a public key and a secret key. These keys are unique, thus hosts are able to be authenticated. This public key is called Host Identity (HI), which is generated by the host itself with RSA algorithm. The length can be 512, 1048, or 2048 bits. The secret key is mainly used for electronic signature. Host Identity Tag (HIT) is designed the format of Overlay Routable Cryptographic . 128 bits is the length of Hash Identifiers.. HIT holds a special class of IPv6 address. Last 32 bits of HIT is called Local Scope Identifier (LSI), which is usually used in local network. HIT and HI of a host are stored in DNS. HIP uses these HI and HIT as the identifier of the host [6].

C. Base Exchange

In HIP, endpoints perform a key exchange at the beginning of a session, called Base Exchange. It is a 4-way handshake process, consisting of packets called packets. An Initiatorsends an I1 packet, and a Responder send a R1 packet as a reply. Then the initiator send an I2 packet, and the responder send a R2 packet. In this sequence, Base Exchange distributes Diffie-Hellman keys (DH keys)and authenticates the hosts. HIP Association is encapsulated by IPsec ESP mode using this key exchanged with DH keys, hence data are encrypted between endpoints. When HIP hosts want to terminate their session, HIP hosts send HIP Closing packets. Packets are encrypted excepts Base Exchange packets and HIP Closing packets [6].

End-to-end security is a mandatory security pattern for the protection of communications in the Internet. It can be ensured at different levels of TCP/IP model: application, transport or network layer. In the IoT scenario, end-to-end security is even more important, as the information being exchanged is generally sensitive and enough private. Recent research works have intensively investigated this issue, by trying to find adaptation techniques allowing the extension of existent secure protocols in the classical Internet, to WSNs while considering their severe constraints (limited energy, low memory and computational power)[7].

3. Related Work

If the same DH key pair is used by the Responder for multiple handshakes, there might be possibilities for small subgroups attacks that must be avoided.

DH key does not provide any information about the identities of both parties. As a result it is exploitable to impersonation attack.It is vulnerable to a clogging attack as it is computationally intensive[8].In such a situation an opponent requests a high number of keys. Major time and resources are unnecessarily invested in modular exponentiation. The victim is deprived of real work. It is vulnerable to Man in Middle attack where in the communication between legitimate A and B is impersonated with A by a third party intruder C. This end up creating network traffic as both A and B negotiates with C. Moreover, replay attack cannot be prevented by DH key.

A problem may be detected with an incoming packet while dealing with HIP implementation. The identity of the sender of the packet may not be determined or it does not have any existing HIP association with the sender of the packet. Also network-based protocols involve the packet encapsulation and tunneling, and those are required more bandwidths and packet processing overheads [9]. Hence a feasible solution needs to be proposed.

A HIP packet can be received that has an unrecognized version number.

If an I2 packet with invalid puzzle solution is received by a HIP implementation, the behavior depends on the underlying version of IP. This aspect of IP behavior with respect to I2 packet needs a solution.

A congestion of the network and DOS attacks might occur by sending multiple I1 packets in parallel. The same I1 packet may be sent to more than one of the Responder's address. The implementation must not send the same i1 packet to multiple addresses upon timeout.

The storm or bulk processing of Incoming I1 packets to a HIP association may occur during a DOS attack that results in an I1 packet flood.
Spoofing of I1 packet can result in an attack on the system by an R1.

A malformed I1 packet may be received by an implementation. This may lead to denial of service threat.

A re transmission in the UPDATE message in a HIP association may give rise to a replay attack.

A kind of DOS attack arises due to floods of forged I2 packets. The attacker here, can send packets with spoofed IP source address. This packet is sent with either an invalid HIP signature or invalid encrypted HIP payload. The Responder may discover that the I2 packets cannot be completely processed. The forged I2 packets needs to be defended as a security consideration.

The major root cause of the DOS attack is the forging of the packets. The HIP should refrain from attackers flooding the forged packets.

A DOS attack may also result on account of a asynchronization between Initiator and the Responder when the Initiator is solving the state puzzles.

HIP is subject to Man in Middle attacks. Without a third party authentication it becomes difficult to defend a Man in Middle attack. HIP needs to provide protection from the resulting Man in Middle attacks.

4. Proposed System

The DH public key needs to be validated by the Responder initially as and when it receives the I2 messages in order to attack the small subgroup attacks in multiple handshakes. In case the validation fails, the DH key must not be generated by the Responder and the HIP BEX must silently be aborted.

When a HIP implementation detects a problem with an incoming packet, it may respond with an ICMP packet. Such replies must be rate limited.

For an unrecognized HIP version number, the HIP implementation should respond, rate-limited, with an ICMP packet, with the Pointer pointing to the version /RES, byte in HIP header.

For an invalid puzzle solution, if IPv6 is used, the HIP implementation should respond with an ICMP packet with the pointer pointing to the beginning of puzzle solution in the SOLUTION payload in the HIP message. Important improvement to PMIPv6 for inter-technology handover and multihoming, as it provides multiple interfaces for multihomed MNs by overcoming the virtual interface. The solution for HIP-PMIPv6 scheme for intra-technology handover has been implemented in a real test-bed[10].

In case IPv4 is used, the HIP may respond with an ICMP packet. This packet copies enough bytes form the I2 message so that the SOLUTION parameter is incorporated into the ICMP message.

To avoid sending multiple I1 packets in parallel the I1 packets should not be send to more than one destination address. These constraints are placed to avoid potential DOS attacks and congestion of the network.

To avoid and I1 packet flood, the storm of received I1 packets should be handled by the HIP implementation such that it discards those packets that arrive within a small time delta carrying common content with them.

To resist an R1 attack on the system by the spoofed I1 packet, an R1 packet sender must adopt a rate-limit mechanism for R1 packets to be sent to an address.

On receiving a malformed I1 packet, the HIP association should not respond with a NOTIFY message. The NOTIFY message can give a potential DOS threat. Thus handling of malformed messages may be done by responding with ICMP message.

The packet is treated as a re transmission if the Update ID corresponds to an UPDATE that has recently been processed. For this reason it is needed that a host caches UPDATE packets sent with ACKs to avoid the cost of generating a new ACK packet so as to respond to a replayed UPDATE. The UPDATE ID must be recorded in the received SEQ parameter for replay protection.

A reflection attack can occur when the R1 packet is considerably larger than the I1 packet. In such a reflection attack, the attacker could spoof the IP address of a victim or the attacker could flood the Responder with I1 messages.

The flooding attack could all together get amplified due to large difference in packet sizes. In order to avoid such reflection attack the Responder should limit the sending of R1 packets in general.

HIP is subject to a DOS attack on the restart of a state after a reboot of one of the peers. In this situation, a restarting host would send an I1 packet to the peers and in response the host would generate R1 packet even if it were in established state.

To avoid the DOS attack in this scenario, the R1 packet would be received unexpectedly by the spoofed host and would be dropped.

The defence against the flooding of forged I2 packets leading to DOS attack, is that the Responder would discard any I2 packets after N bad I2 packets with the same puzzle solution. The Responder could increase the value of #K when the attacker would launch a new attack.

To detect the major root cause of the DOS attack, the Responder keeps a list of solutions from malformed packets. The state of malformed packets is kept as a record by the Responder. This record or state is supposed to be maintained until the R1 counter is increased. The solutions in packets that are forged to pass the checksum and puzzle are put into the blacklist. Also, every time a new list entry is created, a valid puzzle is required. The attackers will be needed to solve the puzzle first when they intend to the flood the blacklist. This would possibly defend the HIP against DOS attack.

The asynchronization leading to DOS attack can be solved if the R1 generation counter is a monotonically increasing counter designed to defend against this attack.

To provide protection from a Man in Middle attack, HIP needs to incorporate certain approaches.

The Initiator can validate the R1 HIP packet if the Responder’s HI is retrieved from a signed DNS zone, or some other secure means, or through a certificate.

To verify that the HI indeed can be trusted, the Responder can retrieve the HI if the Initiator’s HI is in the secure DNS zone, or has a trusted certificate.

5. Conclusion

In this paper, we have presented the challenges and limitations occurring in the Host Identity Protocol. End to end security is vital over communications in Internet Of Things. Host Identity Protocol is aimed to establish secure communications between sender and destination. Security considerations in Host Identity Protocol are exposed and it’s corresponding solutions are proposed in this paper. Major challenges in Host Identity Protocol such as Puzzle mechanism, HIP replay protection, Packet processing, HIP fragmentation, Handling of malformed messages etc are addressed along with overcoming them. The various attacks on HIP protocol such as Denial of Service attack and Man in Middle attacks are studied. This paper also specifies defence against above mentioned attacks. Security considerations in Internet of Things Platform is a major concern of this paper.

References

[1] Muhana Muslam, H.Anthony Chan, Neco Venture, "Host Identity Protocol Extension Supporting Localized Mobility Management", IEEE conference publications, 2011.

[2] Nerea Toledo, Jean Marie Bonnin, "Host Identity Protocol Based NEMO Solution: An evaluation of the signalling overhead", 2011 IEEE 73rd.

[3] Andrey Khurri, Dmitriy Kupstov, Andrei Gurtov, " On application of Host Identity Protocols in WSN networks", IEEE MASS 2010.

[4] Bo Hu, Tao Yuan, Shanzi Chan, " LHIP: A localized mobility management extension for HIP", 6th International Conference on WiCOM, 2010.

[5] Arraez Leonardo, Hakima Chaouchi, "HIP Proactive Mobility Management Experimentation", 6th Advanced International Conference on AICT, 2010.

[6] Akihirio Takahashi, Tomotaka Maeda, Yasau Okabe, " Design and implementation of a secure public wireless internet service model using host identity protocol", 12th International Conference Symposium, IEEE, 2012.

[7] Somia Sahraoni, Azeddine Bilami, " Compressed and distributed host identity protocol for end to end security in IoT ", 2014 International Conference on NGNS.

[8] Nan Li, " Research on Diffie Hellman key exchange protocol", 2nd International Conference on ICCET, 2010.

[9] Chan-Haeng Lee, Seong-Mun Kim, "A network based host identifier locator separating protocol in software defined networks", 17th International Conference on Ubiquitous and Future Networks, 2015.

[10] Guiliana Lapichino, Christian Bonnet, " Host Identity Protocol and Proxy Mobile IPv6: A secure global and localized mobility management scheme for multihomed mobile node", Global Telecommunications Conference, 2009.