Secure DHCPv6 Mechanism for DHCPv6 Security and Privacy Protection

Lishan Li, Gang Ren, Ying Liu, and Jianping Wu

Abstract: With the rapid development of the Internet, the exhaustion of IPv4 address limited the development of the Internet for years. IPv6, as the core technology of the next generation Internet, has since been rapidly deployed around the world. As the widely deployed address configuration protocol, DHCPv6 is responsible for allocating globally unique IPv6 addresses to clients, which is the basis for all the network services. However, the initial design of the DHCPv6 protocol gave little consideration to the privacy and security issues, which has led to a proliferation of privacy and security accidents breaches in its real deployment. In this paper, to fundamentally solve a range of possible security and privacy issues, we propose a secure DHCPv6 mechanism, which adds authentication and encryption mechanisms into the original DHCPv6 protocol. Compared with other proposed security mechanisms for the DHCPv6, our method can achieve all-around protection for the DHCPv6 protocol with minimal change to the current protocol, easier deployment, and low computing cost.

Key words: DHCPv6; security; privacy; IETF; authentication; encryption

1 Introduction

With the rapid development of the Internet, the Internet Assigned Number Authority (IANA) exhausted all the IPv4 addresses in Feb 2011[1]. Yet, the new Internet technologies, such as IOT, bring with them a continuous demand for the allocation of IP addresses. Compared with the IPv4, IPv6[2] has a 128-bit address format that overcomes the issues of IPv4, which greatly expands the IP address space and which has been quickly deployed around the world.

For all the terminal equipments, the basis of the Internet connection is obtaining one globally unique address for routing. IPv6 address configuration protocols, including StateLess Address Auto-Configuration (SLAAC)[3] and Dynamic Host Configuration Protocol for IPv6 (DHCPv6)[4], allocate globally unique IPv6 addresses to clients. DHCPv6 allows the DHCPv6 server to flexibly allocate IPv6 addresses and manage the address state information for clients. Compared with the SLAAC protocol which uses stateless mode, DHCPv6 uses stateful mode that makes it easier to perform network management functions, such as trouble shooting and access control. In addition, even if a host obtains an IPv6 address via SLAAC, the DHCPv6 is also used to obtain other information relating to the local network infrastructure, such as the DNS server address. Currently, DHCPv6 is widely used and deployed throughout the real world. However, in the initial design process of the DHCPv6, no consideration was given to issues of security and privacy, which has led to many challenges in the current protocol.

With respect to security, clients are vulnerable to attacks by the rogue DHCPv6 server, which may lead to network connection failure over the wide area controlled by the original DHCPv6 server. With respect to privacy, the clear-text DHCPv6 messages exchange process may disclose privacy information of the client, such as their unique identity information. As the basic routing information, the IPv6 address can be
used to establish the relationship between the location and network activity information. By monitoring the address configuration process, the attacker can track the location and network activities of specific users. In London, the Renew company has implemented the location tracking and recolonization of the device operation system by collecting the unique identifier of clients, such as the client’s DHCP Unique IDentifier (DUID) in the DHCPv6 message\cite{5,6}.

The Internet Engineering Task Force (IETF) has for some years focused on the security and privacy issues of the DHCPv6. The Dynamic Host Configuration (DHCP) Working Group (WG) has issued many requests for comments (RFCs) and drafts in an effort to mitigate these issues\cite{7–9}. However, those proposed mechanisms have mainly focused on fixing discovered security and privacy issues and do not fundamentally address the generation of these issues mentioned. In addition, the proposed secure mechanisms give little consideration on the deployment issue, leading to deployment difficulties in the current network. As such, there is an urgent demand for the design of a new secure mechanism that fundamentally solves the existing security and privacy issues and is easily deployed in the current network.

In this paper, we propose a secure DHCPv6 mechanism that fundamentally solves the security and privacy issues in DHCPv6. In our proposed secure DHCPv6 mechanism, we have added the authentication and encryption mechanisms to the original DHCPv6 protocol. The authentication mechanism can protect the DHCPv6 from active attacks, whereas the encryption mechanism can be used to defend against passive attacks. Compared with other proposed secure mechanisms, the secure DHCPv6 mechanism we propose here can achieve all-around protection of the DHCPv6 configuration process, with minimal change to the original DHCPv6 protocol, easy deployment in the real world, and low computing cost on the equipments.

2 Threat Model for DHCPv6

2.1 DHCPv6 protocol

The current DHCPv6 mechanism was standardized by the RFC3315\cite{4}, and then modified by 3315-bis\cite{10}. With the DHCPv6 mechanism, hosts are assigned IPv6 addresses and other configuration information relating to the local network infrastructure, such as a DNS server address, from the DHCPv6 server. The DHCPv6 server is responsible for the assignment of unified addresses and the management of lease information for all clients. However, the current protocol provides no security mechanism, and is therefore vulnerable to a range of security and privacy attacks. In the following section, we use the STRIDE threat model to analyze on the existing security and privacy issues and the possible attacks associated with the use of DHCPv6.

2.2 Security issues analysis

The goal of establishing a secure DHCPv6 is to ensure that clients are routinely assigned a globally unique and routable IPv6 address. In the message exchanges between a client and server, the DHCPv6 faces the following three types of attacks.

2.2.1 Rogue DHCPv6 server attack

Under the current DHCPv6 protocol, there is no authentication mechanism for a rogue server check. As showed in Fig. 1, attacker can forge as a DHCPv6 server to achieve the wrong IPv6 address and other information configuration on the host. The incorrect configured IPv6 address will then lead to network connection failure. The wrong DNS server configuration can cause the DNS spoofing attack and DNS resolution among other issues.

2.2.2 DHCPv6 message tampering attack

The current DHCPv6 mechanism provides no method for checking message integrity, which may lead to a man-in-the-middle attack, as illustrated in Fig. 2. If the attacker modifies the DHCPv6 message content, then the client will suffer the same attack result as it would be in a rogue DHCPv6 server attack.

Fig. 1 Rogue DHCPv6 server attack.

Fig. 2 DHCPv6 message tampering attack.
2.2.3 Denial-of-service attack for DHCPv6

Besides the lack of any server authentication method, the DHCPv6 also lacks any client authentication method. As illustrated in Fig. 3, numerous zombie hosts may cause Distributed Denial-of-Service (DDoS) attacks on the DHCPv6 server. DDoS attacks result in the huge waste of the server’s IPv6 address and CPU resources, which may lead to DHCPv6 server crashes and the failure to provide DHCPv6 service to all clients.

2.3 Privacy issues analysis

With respect to the privacy of the DHCPv6, here, we focus on the provision of DHCPv6 client privacy protection. As a public infrastructure, the privacy of the server and relay agent is less important. The most critical privacy information in the DHCPv6 message is the host’s DUID information, which uniquely identifies the specific host\[8, 11\]. The host’s DUID is computed based on the stable MAC address, which makes the host’s DUID stable and unique. However, currently, DHCPv6 messages are transmitted in clear-text and privacy information has no protection from passive attacks, such as pervasive monitoring\[12\]. The client’s DUID will disclose the host’s privacy information and can result in the following attacks.

2.3.1 Network activity tracking

The IPv6 address can be used to correlate the host’s network activities over the lifetime of the IPv6 address. By monitoring the DHCPv6 configuration process, the attacker can establish the relationship between the IPv6 address and the DUID of the specific host. In this way, the attacker can determine the corresponding relationship between the host’s DUID and network activities. However, the existence and use of stable DUID prolongs the correlation period of network activities on the order of years. Even if the host moves between different networks and the IPv6 address changes, the client’s DUID remains stable. Compared with other privacy information, such as cookies and application-layer user names, the lifetime of the host’s DUID is much longer.

2.3.2 Location tracking

Generally, as basic routing information for routing, the IPv6 address indicates the topological location of the host. By monitoring the DHCPv6 process, the attacker can also establish the relationship between the host’s DUID and location, which is similar to network activities tracking.

2.3.3 Address scanning

When the client reconnects to a network, based on the associated client DUID information, the server attempts to assign the same IPv6 address as that assigned when the client previously connected to this network. Although this method is beneficial to client with stable network connection, for the attacker, this situation greatly reduces the search space and makes it easy to scan for the specific host.

2.3.4 Device-specific property exploitation

The DUID is generated via the MAC address. Like the MAC address, the host identifier may reveal the host’s specific property information, such as the network interface card vendor, operation system, and so on. In addition, some information contained in the DHCPv6 options, such as Vendor Class option, also reveals this type of privacy information. Attacker can utilize the device’s specific property information to quickly identify the specific weakness of a target.

2.4 Threat model of DHCPv6

Based on the above security and privacy analysis, here, we use the STRIDE threat model to summarize the DHCPv6 threat model as shown in Table 1.

3 Related Works

RFC3315\[4\] defines a DHCPv6 message authentication mechanism for a message integrity check. This authentication mechanism is based on the symmetric key shared by the client and server. However, it provides no any key distribution mechanism. For key deployment, operators can set up a key database for both servers and clients from which the client obtains the same key prior to running the DHCPv6. However, this manual key distribution conflicts with the goal of minimizing the manual configuration for each host. Consequently, this mechanism has never been deployed.
Anonymity profile for DHCP clients, which were standardized in RFC7844\cite{9}, explains how to generate randomized DUID information to minimize disclosure of the privacy information. In the current DHCPv6 protocol, this stable identifier information is useful for both the network administrator and host. For the network administrator, knowledge of the host’s identifier facilitates some network management functions, such as trouble shooting and access control. For the host, this identifier can be used to achieve the same IPv6 address assignment when the network connection is re-established. Randomized DUID cannot perform the above functions, nor can they protect other newly defined options that may contain private information.

The privacy consideration for DHCPv6, which is standardized in RFC7824\cite{8}, presents an analysis of privacy issues and the possible caused attacks in current DHCPv6 protocol. However, no solutions are presented in the document.

4 Secure DHCPv6 Mechanism Design

Based on the above threat model analysis, a secure DHCPv6 mechanism must satisfy the following four requirements: server authentication, message integrity check, server availability, and information privacy protection. In this paper, we propose a secure DHCPv6 mechanism, in which we add the authentication and encryption mechanisms into the current DHCPv6 protocol. The authentication mechanism meets the following three requirements: server authentication, message integrity check, and server availability. The encryption mechanism protects the privacy information in DHCPv6 communication from passive attacks.

4.1 Secure DHCPv6 configuration process

Figure 4 details the message exchange procedure of the secure DHCPv6 mechanism. Briefly, the secure DHCPv6 mechanism requests the server’s certificate information via an anonymous information-request exchange. Upon receiving the server’s reply, the client checks the server’s identity information. Through the above information-request and reply messages exchange, the client achieves server authentication while not revealing any private information.

The authentication process has three parts: certificate check, signature check, and increasing-number check. For the certificate check, it is assumed that the client/server has been pre-configured a trusted certificates list. In this way, a certificate is authenticated if it finds a match in the trusted certificates list. The signature is used for the DHCPv6 message integrity check, and the increasing-number is used for the replay attack defense. In Sections 4.2 and 4.3 below, we explain in detail the methods used in the signature and increasing-number checks.

Once the client chooses to communicate with the selected server, it uses an Encrypted-Query message to encapsulate its communications to the DHCP server. Client authentication is established via the first Encrypted-Query message from the client to the server. As shown in Fig. 4, the first encrypted message is the Solicit message, which includes the client’s information, which is checked by the server according to the above described methods.
The Encrypted-Query message includes three options, as shown in Fig. 5: Encrypted-Message option, Server Identifier option, and Encrypted-Key-Tag option. The Encrypted-Message option carries the content of the encrypted DHCPv6 message using the server’s public key. Via the Server Identifier option, the server can determine whether it is the target server, and thus paying no extra cost to decrypt the message. The Encryption-Key-Tag option is used to identify the public/private key pair used for decryption when the server receives an Encrypted-Query message. The client and the server share a common encryption-key-tag calculation algorithm. In this way, the client and server can establish the same corresponding relationship between the encryption-key-tag and the public key. In Section 4.4, we explain the encryption-key-tag algorithm in detail. After client authentication, the server responds to the client with an Encrypted-Response message, which contains only the Encrypted-Message option. The format of the Encrypted-Response message is the same as that in the Encrypted-Query message. Using the client’s public key, the Encrypted-Message option carries the content of the encrypted DHCPv6 message.

4.2 Increasing-number check method

For the increasing-number check, the client/server keeps a local record of the serial number and then checks whether the receiving serial number being received in the DHCPv6 message is higher than the locally stored serial number. The timestamp is one general choice for use in the increasing number mechanism.

The timestamp mechanism is based on the assumption that the client and server have roughly synchronized clocks. In general, it is difficult to strictly achieve time synchronization of the client and server. So, we have added the following parameters for timestamp check: the timestamp \( \Delta \) for the time difference between the client and server; the fuzz factor, which compares the last and current timestamps; and the clock drift parameter, which accounts for clocks that are not strictly accurate. As the default values of the above three parameters, we have allowed timestamp delta value of 300 seconds (5 minutes), an allowed fuzz factor of 1 second, and an allowed clock drift of 0.01 second.

To explain these rules more clearly, we developed the following definitions: \( RC_{new} \) indicates the timestamp contained in the received DHCPv6 message, and \( LC_{new} \) indicates the local timestamp in the receiver. \( RC_{last} \) indicates the timestamp contained in the last received and accepted DHCPv6 message. \( LC_{last} \) indicates the local timestamp when the last accepted DHCPv6 message was received. According to whether or not a timestamp is received for the first time, the receiver will check the timestamp using different rules. For the first case that the timestamp is received for the first time, the received timestamp passes the check if it meets the condition of Eq. (1).

\[
- \Delta < (RC_{new} - LC_{new}) < + \Delta
\]  

For another case in which the timestamp has been received in the past, the received timestamp passes the check if it meets the conditions of Eqs. (2) and (3):

\[
RC_{new} > RC_{last}
\]

\[
LC_{new} + fuzz > LC_{last} + (RC_{new} - RC_{last}) \times (1 - drift) - fuzz
\]

If the timestamp check is passed, the values of \( RC_{new} \) and \( LC_{new} \) in the caches are replaced by the values of \( RC_{last} \) and \( LC_{new} \), respectively.

4.3 Signature check method

The client or the server can support various algorithms simultaneously, which causes the challenge of how to ensure that the same hash and signature algorithm are used for the client and the server. The core technology of the signature check is an algorithm negotiation mechanism between the client and the server.

To realize this algorithm negotiation mechanism, the hash and signature algorithms used must be identified in the signature option. So, we added the Hash Algorithm id (HA-id) and Signature Algorithm id (SA-id) fields in the signature option, as shown in Fig. 6. During the negotiation process, there is one case in which the receiver does not support the identified algorithms of...
the sender. To solve this issue, we define mandatory algorithms, such as SHA-256 as the hash mandatory hash algorithms and RSA as the mandatory signature algorithm. If the negotiation fails, then these two peers can use the same mandatory hash and signature algorithms for the signature generation and check.

4.4 Encryption-key-tag calculation method

Typically, the DHCPv6 server has multiple local certificates, which correspond to multiple private/public key pairs. The DHCPv6 server may communicate simultaneously with different clients using different public keys. So, the key technology requirement for the server is the identification of the corresponding private key for encryption when receiving an Encrypted-Query message. To solve this problem, the client and server share one common encryption-key-tag calculation algorithm. In this way, the client and server can establish the same corresponding relationship between the encryption key tag and the public key. Algorithm 1 details the encryption-key-tag calculation algorithm. The input of this algorithm is the data relating to the public key, which is 32 bits or larger, and the output is the 16-bit encryption key tag.

5 Secure DHCPv6 Deployment

5.1 Secure DHCPv6 deployment method

Prior to the DHCPv6 configuration process, the client cannot connect to the Internet, which will cause difficulties in the authentication process if using the traditional certificate path validation method described in RFC5280[13]. So, the key technology requirement for a secure DHCPv6 is to address deployment issues, such as how to validate the received certificate offline. The current authentication mechanism relies on the operator’s manual operation, which restricts the wide deployment of the secure DHCPv6. To realize a wide deployment, we apply opportunistic security[14] in the proposed secure DHCPv6, which allows message encryption even if mutual authentication is not available.

If secure DHCPv6 is deployed based on opportunistic security, two main types of scenarios can occur. The first is the enterprise network, where the stable clients and servers are pre-configured trusted server certificate lists, so the DHCPv6 configuration process is authenticated and encrypted. The other scenario is the coffee shop, where roaming clients cannot be pre-configured trusted certificates lists[15], so the DHCPv6 configuration process is not authenticated but encrypted. Although without an authentication mechanism, these clients can not be protected from the active attacks of a rogue server, the encryption mechanism can protect clients from the disclosure of privacy information, which is safer than the clear-text configuration.

5.2 Secure DHCPv6 system design

The Internet Systems Consortium (ISC) DHCPv6 system[16] is an open source software for DHCPv6 client and server implementation, which is widely used in the current enterprise grade DHCP implementation. The proposed secure DHCPv6 mechanism is also based on the ISC DHCP system[17]. Recently, the ISC has developed an authentication mechanism and will complete their development of an encryption mechanism soon. For authentication, the following functions have been added: timestamp check, signature check, and public key check. Because the current certificate contains only the public key information, we have replaced the certificate check with a public key check. To perform the above functions, we have added a signature option, timestamp option, and public key option in the DHCPv6 protocol. Via the authentication mechanism, we can ensure that the DHCPv6 server/client can not impersonate another. A secure DHCPv6 client is realized based on the Ubuntu 15.04 32 bits Virtual Machine with bridged Ethernet (MAC address: 00:0c:29:40:3b:88). The secure DHCPv6 server is realized on the iMac host with 10.10.3 version OS. The secure DHCPv6 server and client are all pre-configured with certificates and a trusted certificates list for public key validation. In the
IETF93 meeting, the DHC WG organized a hackathon to test the proposed secure DHCPv6\cite{18}. Based on the result of the hackathon check, no problem was identified in the proposed authentication mechanism. Figure 7 shows the run results for the client side, and Fig. 8 shows those for the server side.

5.3 Standardization in IETF

To date, the proposed secure DHCPv6\cite{19} mechanism has been submitted to the IETF DHC WG and been approved as a WG draft. This draft mainly focuses on a description of the messages exchange process. Compared with the draft, this paper adds specific implementation detail, including the timestamp check algorithm, and adds the secure DHCPv6 prototype implementation test to confirm its performance in the real world.

6 Comparison with Other Mechanisms

As described in Section 3, the DHC WG has proposed two secure mechanisms for the DHCPv6: a message authentication mechanism in RFC3315 and an anonymity profile mechanism in RFC7844. To evaluate and compare all the proposed security mechanisms, we consider the following four parameters: defense capability, impact on the current protocol, deployment difficulty, and cost. Table 2 shows our comparison of these four aspects for the proposed security mechanisms for the DHCPv6.

6.1 Defense capability

Based on the summarized threat model results in Section 2.4, the design of the secure mechanisms for the DHCPv6 must meet four requirements (see Table 1). The message authentication mechanism can meet the requirements 1, 2, 4, and anonymity profile mechanism meets the requirement 3. Via the authentication and encryption mechanism, the secure DHCPv6 mechanism can meet all four requirements and fundamentally solve the security and privacy issues of the DHCPv6.

6.2 Impact on the current protocol

The DHCPv6 protocol is currently widely used in the Internet. As such, the design of the new secure mechanism must minimize the changes to the current DHCPv6 protocol. The proposed message authentication mechanism simply adds an authentication option for message integrity check. The anonymity profile mechanism changes the DUID generation method on the client side. For the secure DHCPv6, the server authentication process is added prior to the implementation of the standard DHCPv6 configuration process. However, the server authentication process is completed through the traditional Information-request and Reply messages exchange, without introducing any newly defined message exchanges.
Table 2: Comparison of the secure mechanisms for DHCPv6.

<table>
<thead>
<tr>
<th>Article</th>
<th>Key technology</th>
<th>Defense capability</th>
<th>Impact on the current protocol</th>
<th>Deployment difficulty</th>
<th>Computing cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC7844</td>
<td>Randomized DUID generation method on the client side</td>
<td>3</td>
<td>Replace the before stable DUID generation method</td>
<td>Hard</td>
<td>No extra cost</td>
</tr>
<tr>
<td>RFC3315</td>
<td>Message authentication based on symmetric key</td>
<td>1, 2, 4</td>
<td>Add Authentication option</td>
<td>Hard</td>
<td>Small cost</td>
</tr>
<tr>
<td>Secure DHCPv6</td>
<td>Authentication and encryption based on asymmetric keys</td>
<td>1, 2, 3, 4</td>
<td>Add server authentication before normal process</td>
<td>Easy</td>
<td>Small cost</td>
</tr>
</tbody>
</table>

6.3 Deployment difficulty

The reason that the proposed secure mechanisms have not yet been deployed in the real world is due to the deployment difficulty. The deployment of the message authentication mechanism is hard because of the lack of a symmetric key distribution mechanism. The anonymity profile relies on the MAC address randomization mechanism, which is difficult to be standardized and deployed. The proposed secure DHCPv6 mechanism introduces opportunistic security to facilitate wide deployment.

6.4 Computing cost

The anonymity profile introduces no computing cost to the client/server. The introduction of the cryptography technology will cause the computing cost on the client and server. However, there are only a few DHCPv6 message exchanges, so the associated computing cost on the client/server will be low.

7 Conclusion and Future Work

Currently, as the widely used address configuration protocol, the DHCPv6 is the basis of all Internet services for the host. However, the initial design of the DHCPv6 does not adequately consider security and privacy issues. In this paper, we propose a secure DHCPv6 mechanism, which adds the authentication and encryption mechanisms into the current DHCPv6 protocol. Through the authentication mechanism, the client can be protected from active attacks, including spoofing, tampering, and denial of service. The encryption mechanism helps the client to defend against the disclosure of privacy information. Compared with other secure mechanisms for the DHCPv6, the proposed secure DHCPv6 mechanism achieves all-around protection with the minimal change to the current protocol, easier deployment, and low computing cost.

However, some mechanisms, such as SAVI[20], rely on the monitoring of the DHCPv6 process[21]. The encryption mechanism in the proposed secure DHCPv6 will impede the DHCPv6 monitoring procedure, which makes them incompatible. The IETF has discussed this problem, which may be the focus of future work[22].

In addition, some new IPv6 address generation schemes have been proposed[23], such as NIDTAG[24], which will change the DHCPv6 configuration process. The proposed secure DHCPv6 can also be utilized to achieve all-around protection for these newly proposed mechanisms. The combination of the changed DHCPv6 configuration process and secure DHCPv6 may also be addressed in future work.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (Nos. 61772307 and 61402257) and Tsinghua University Self-determined Project (No. 2014z21051).

References


Lishan Li is a PhD candidate at Tsinghua University, China. Her research interests include DHCP, security, and NFV. She received the BS degree in computer science from the University of Science and Technology Beijing.

Ying Liu received the MS degree in computer science and the PhD degree in applied mathematics from Xidian University, China in 1998 and 2001, respectively. She is currently an associate professor at Tsinghua University, China. Her major research interests include network architecture design, next architecture, and routing algorithm and protocol.

Gang Ren received the PhD degree in computer system architecture from Tsinghua University, China in 2009. He is currently an assistant professor at Tsinghua University, China. His major research interests include network architecture design, next generation Internet architecture, and network security.

Jianping Wu received the BS, MS, and PhD degrees from Tsinghua University, China. His research interests include next-generation Internet, IPv6 deployment and technologies, and Internet protocol design and engineering. He is currently a full professor in Tsinghua University, vice chairman of the information committee, and director of the Information Office, Dean of the CS Department and Director of the Network Research Center, Dean of Institute for Network Sciences and Cyberspace, and Director of Information Technology Center, Tsinghua University. He is director of Network Center and Technic Committee of China Education and Research Network CERNET, director of the National Engineering Laboratory for Next Generation Internet, a member of Advisory Committee of National Information Infrastructure for Secretariat of State Council of China, and vice president of Internet Society of China (ISC). He is an IEEE Fellow and was also the Chairman of Asia Pacific Advanced Network from 2007 to 2011. He received the Jonathan B. Postel Award from the Internet Society in 2010.