Narendar Shankar
Univ of Maryland

William Arbaugh
Univ of Maryland

Kan Zhang
Hewlett-Packard Labs

Wireless Key Management using DHCP
draft-ietf-dhc-key-management-00.txt

Status of this memo

Abstract

This document defines a new DHCP option which is passed from the DHCP Server to the DHCP Client to configure the WEP key on a client's wireless card.

In wireless LAN's it is important to encrypt data at the link layer, because of the potential for eavesdropping. This is done in current wireless networks using WEP which has a number of well known flaws- some of which are mitigated through the use of effective key management. For a wireless LAN, DHCP provides an excellent mechanism for implementing wireless key management as it is transparent to the users.

1. Introduction.

DHCP [1] transports protocol stack configuration parameters from centrally administered servers to TCP/IP hosts. Among those parameters are an IP address. DHCP servers can be configured to dynamically allocate addresses from a pool of addresses, eliminating a manual step in configuration of TCP/IP hosts.

A wireless LAN consists of wireless clients(called STA's) which communicate with the wired backbone by means of wireless access points(called AP's). The AP acts a bridge between the wireless and the wired networks. Nodes of a wireless LAN normally use DHCP services to obtain IP addresses, and key management is an easy extension. We propose the use of a new DHCP option which supports wireless key management

1.1 Threat Model

Organizations are rapidly deploying wireless infrastructures based on the IEEE 802.11 standard. Unfortunately, this standard provides only limited and weak support for confidentiality through the wired equivalent privacy (WEP) [2][3]. Furthermore, the standards committee for 802.11 left many of the difficult security issues such as key management and a robust authentication mechanism as open problems. As a result, many of the organizations deploying wireless networks use either a permanent fixed key or no encryption what so ever.

1.2 Use of DHCP for wireless key management.

Many new schemes which have been proposed to address the authentication, confidentiality and key management for IEEE 802.11. The IEEE 802.11 task group on security proposes a change in the 802.11 standard to use the recent 802.1X standard as a means for key managment. However, this cannot solve the problem for the current installed base. We propose the use of a new DHCP option for wireless key management.

The advantages of using DHCP as a "transport" for wireless keys are

1.2.1 DHCP leases provide an excellent mechanism for implementing cryptographic key periods. When a DHCP client renews its lease with the DHCP server, it also obtains the current wireless key as a part of the lease. The time for renewal of the lease can be appropriately set by the enterprise.

1.2.2 The use of DHCP for wireless key management is very inexpensive and more importantly it interoperates with the huge existing installed base.

1.3 Design goals

These are the goals that were used in the development of the authentication protocol, listed in order of importance:

1. Provide a good key management system for wireless LAN's using the DHCP services of the wired LAN's

2. Work with the existing infrastructure

3. Limit complexity (complexity breeds design and implementation errors).

1.4 DHCP Terminology

This document uses the following terms:

- "DHCP client"

  A DHCP client or "client" is an Internet host using DHCP to obtain configuration parameters such as a network address.

- "DHCP server"

  A DHCP server or "server" is an Internet host that returns configuration parameters to DHCP clients.

1.5 Wireless LAN terminology

This document uses the following terms

- "Wireless Station/Wireless client(STA)"

  A node/client with a wireless interface .

- "Wireless Access Point(AP)"

  An access point mediates communication between wireless nodes which can't directly communicate with each other. The AP acts like a link layer bridge.

- "Wired Equivalent privacy(WEP)"

  WEP is a the standard for ensuring confidentiality of data (link layer data) specified by the IEEE802.11b standard

- "Shared Key and window of keys"

  WEP uses a shared key for all nodes which wish to communicate with each other. Link layer traffic is encrypted and decrypted with this key. A window of four keys is used as a back up when keys become invalid or unusable. In other words the access point and the clients have a window of keys on their wireless cards and use one of the keys on the card for communication.

- Authentication key

  This is a relatively long lived "WEP" (link layer) key used by the STA for authentication purposes. It is denoted by 'A'.

- "Current link layer key"

  This is the current key being used for link layer communication. It is denoted by 'K' o "Next link layer key"

This is the next link layer key to be used. It is denoted by 'K_n'

2. Basic protocol

The wireless network consists of STA's trying to connect to a wired network using the AP. The DHCP server is in the wired part of the network. All link layer traffic is encrypted using the "Current Key"- 'K' (the current link layer key). Wireless traffic from the STA's is encrypted using 'K'. The AP decrypts the wireless traffic (because it too has 'K') and forwards the traffic to the wired network.

The idea to mitigate current WEP flaws is to keep changing the current key 'K'. At the same time valid STA's of the network, who leave the network must be able to obtain the new current key (if it has changed) when they rejoin the network. This is accomplished by a "double door" entry mechanism where the STA authenticates itself into the network using a "link layer authentication key" (another WEP key) called 'A'. The frequency of use of 'A' is small when compared to 'K' and is hence considered to be a key with a longer lifetime. Both the AP and the STA's have a window of four WEP keys. They can listen on any of the four keys but can transmit only on one key.

The access point listens on both 'K' and 'A'. The STA's who are a part of the network have 'K' and 'A'. The valid STA's who do not have 'K'(they had left the network and are now rejoining) can authenticate themselves using 'A'. After the STA's have authenticated themselves they obtain the current link layer key 'K'.

Apart from rejoining the network, regular timed key management takes place for all STA's currently in the network. In other words the current key 'K' keeps changing frequently. We use DHCP as a "transport mechanism" for gettng the new link layer key 'K_n'.

The basic idea is as follows:

1. When the client/STA joins/rejoins the network, it is assigned an IP address and is given the current link layer key 'K'. The IP address is leased for a particular time period. This time period is set by organizational policy. Apart from this the STA is also given the next link layer WEP key K_n. The reason for doing this is explained in the timing section.

2. All the clients in the network who have the current key renew their IP address (NOTE: the address does not need to change) depending on the lease time and in the process also get the new link layer key K_n.

2.1 Protocol for a client /STA rejoining the network

Like it had been mentioned before, the STA does not have the current link layer key 'K' but has the link layer authentication key 'A'. Given below is the protocol for the client to rejoin the network and get the current link layer key 'K'.

```
   <---Wireless LAN---------------------><--------Wired LAN------->

   DHCPDISCOVER(with Wireless re-key and authentication option set)
   STA ---------------------------------> AP------------->DHCP SERVER
                                          (Listens on 'A','K')


                       DHCPOFFER
    STA <--------------------AP<-------------------------------DHCP SERVER
                        Authentication Information
                                                          ASK AP TO CHANGE TO
'A'


                      DHCPREQUEST
    STA ---------------------------------> AP------------->DHCP SERVER
                        Authentication Information


                      DHCPACK
    STA <--------------------AP<-------------------------------DHCP SERVER
           Encrypted (Current Link layer key 'K' +
           Next  Link layer key 'K_n')
```

1. In the initial phase the STA sends a DHCPDISCOVER message with the wireless re-key option set and the DHCP authentication option set. The STA transmits the message encrypted with the link layer Authentication (WEP) Key 'A'. The AP can listen on 'A' and 'K' and hence forwards the request to the DHCP server on the wired LAN.

2. The DHCP server sends a DHCPOFFER message including the authentication information in accordance with the DHCP authentication protocol[5]. It must also be noted that the AP's transmission key MUST changed to 'A' before transmission and back to K afterwards. The protocol for changing the AP's key is beyond the scope of this document. The duration for the change from 'K' to 'A' can be aproximately set to the average period of time for an exchange starting from DHCPDISCOVER to DHCPACK

3. Then the STA transmits a DHCPREQUEST message, with the

authentication information.The authentication information is again in accordance with [5].

4. The DHCP server sends back a DHCPACK message and also its authentication informtion and also the Current Link layer key 'K' "in an encrypted format". The WEP key MUST sent in an encrypted format. The encryption can be done with a shared key or any authentication mechanism between the client and server as defined by [5]. Also the DHCP server sends the next link layer key K_n(encrypted). The reason and the details are explained in the timing section.

2.2 Phase for renewing allocated IP address when lease expires

```
<---Wireless LAN---------------------><--------Wired LAN------->

                                  DHCPREQUEST
STA ---------------------------------> AP------------->DHCP SERVER
                    Authentication Message


                                  DHCPACK
STA <--------------------AP<-------------------------------DHCP SERVER
        ENCRYPTED Next current Link Layer key K_n
```

When the lease expires the DHCP client contacts the DHCP server and tries to renew its IP address. When the IP address is renewed, the WEP key is also renewed.

This phase is very similar to the initial phase, but for the fact that the AP can transmit in 'K'(current key) because the client already has the current key 'K'. Again here the New WEP key K_n MUST be sent in an encrypted format, and both the client and the DHCP server MUST use the authentication option.

3. Delayed key installation for better key management.

The straight forward key management protocol has two problems:

1. If all the clients renew the keys at the same time then the server becomes overloaded.

2. If all the clients renew their keys at different times, then inconsistency problems are introduced and the server might have to listen on multiple keys for prolonged periods. We introduce a new idea of timed key management. All clients contact the server at different times.

For the first stage(client joins the network/rejoins the network), assume that the client contacts the server at time t1 (actual time or real world time) and assume the lease period is T seconds. When the client joins the network, it needs the current link layer immediately. Also as mentioned before, the client obtains the next link layer session key. The reason for doing so is that during every key renewal the client gets the next link layer key, but initially the client does not even have the current link layer key. Hence it has to be given both the keys. An example is given below.

At time t1 K is the current link layer key. The client contacts the server again at time t1+T (i.e t1+ time of lease). Since the client joins in the middle of a lease period, at some absolut time t2 (t1 < t2< t1+T), a new key K_n will be installed on all cards (t2 is termed the "key installation time" and t1+T, t1+2T are all termed as "key renewal times"). This means that from t2 to t1+T this client cannot communicate with the rest of the network.

Thus when the client joins the network initially it must be given both the curernt key K and the next link layer key K_n (note that both are link layer keys). Also the client must be given the directive -"Install the key K on the card immediately and use (install on card) the key K_n after t2 - t1 seconds"

Now in the next stage, the client already has the current key and it only gets the next link layer key K_n . Assume that the client contacts the server at time t1+T(end of the lease), it obtains the key K_n to be used at time t2+T and the directive "Install key K_n after t2+T-(t1+T) = t2-t1 seconds"

Thus the client keeps contacting the server at times(renewal phase) t1 + T, t1 + 2T, t1 + 3T etc., but actual use/installation of the key takes place at times t2, t2 + T, t2 + 2T, t2 + 3T etc.

4. Format of wireless authentication option.

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Code    |     Length     |Length of encapsulation            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |Time to install next key    (t2)                                         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | Encrypted current WEP Key (with appropriate encapsulation)  |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | Encrypted next WEP Key (with appropriate encapsulation)     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

o Code field is TBD

- o Length field specifies the length of the option o The DHCP authentication option MUST be set if the wireless re-key option is set.

o Length of encapsulation filed MUST be set to the size of the encapsulation method used to encapsulate the encrypted current wireless key(explained next).

o Encrypted current and next key MAY be of variable length but MUST be encapusulated with the PKCS#7 [6] standard which gives enough information about the algorithm and the encryption parameters

o Time to install next key- It is the time in seconds between acquiring the next WEP Key and the time when it is to be installed on the card. The length MUST be set to 32 bits.

5. DHCP client behaviour

o Client MUST use the DHCP authentication option.

o Client MUST set the wireless rekey option in the DHCPDISCOVER message if it wishes to rejoin the network(because it does not have the current link layer key).

o Client MUST set the "Time to install next key" field to be all 1's(0xffffffff) if it is joining/ rejoining the network. This is required because the server must be able to distinguish that the client requires the wireless key immediately.

o Client MUST set the wireless rekey option in the DHCPREQUEST message if it wishes to renew the current wireless key. Once again it must be remembered that there might be a time difference between getting the key and installing it on the card.

o If the Encrypted current WEP key field is set(not all zeroes), the client MUST install current WEP key(after decryption) on the card immediately

o Client MUST install the Next WEP key (after decrypting it) on the card only after a time which is equal to "time to install next key". It may be noted that "Time to install next key" MAY be zero.

o The protocol for updating the key on the Wireless card on the STA is beyond the scope of this paper.

6. DHCP server behaviour

o Server MUST use the DHCP authentication option.

o Server MUST ignore the wireless re-key option if the DHCP authentication option is not set.

o Server MUST set "Encrypted Current WEP key" field if the client is trying to rejoin the network. This can be identified if the client

sets the "Time to install next key" to be 0xffffffff. If the client hasnt set the "Time to install next key" (client is not rejoinng network but just renewing current key) field, the server MUST set the "Encrypted Current key" to be all 0's

o Server MUST set the "Encrypted next WEP key" (with the encrypted next WEP key)

o The server MUST set "Time to install next key" to be the difference in time between issuing the next key and the time when the client must install it.

o Server MUST encrypt the current WEP key before sending it to the client.

o Server MUST encrypt the next WEP key before sending it to the client.

o Server MUST send the encrypted WEP key only in the DHCPACK message.

o The protocol for updating and changing the key on the Access Point is beyond the scope of this paper as the protocol for the DHCP server to obtain the current and next keys from a key server. It is to be discussed in a separate paper.

6. References

[1] Droms, R., "Dynamic Host Configuration Protocol", RFC-2131, March 1997.

[2] J. Walker," Unsafe at any key size: an analysis of the WEP encapsulation," Tech. Rep. 03628E, IEEE 802.11 committee, March 2000. http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip.

[3] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11." http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.

[4] W. Arbaugh, N. Shankar, Y.C Justin Wan,"Your 802.11 wireless network has no clothes". http://www.cs.umd.edu/~waa/wireless.pdf

[5] R. Droms, W. Arbaugh. "Authentication for DHCP messages", RFC-3118, June 2001

[6] B. Kaliski. "PKCS #7: Cryptographic Message Syntax Version 1.5", RFC-2315, March 1998

7. Security Considerations

This document describes a key management option for use in wireless networks.

7.1 Protocol vulnerabilities

The fact that the AP is listening on 'A' allows unauthenticated clients to send unauthorized packets onto the network. Organizations are strongly advised to implement layer 2 and 3 packet filtering between the wireless and wired networks in conjunction with this option

7.2 Protocol limitations

This protocol assumes the existence of an authentication server and a key server.

8. Acknowledgements

The authors would like to thank Y.C.(Justin) Wan for working with us on an initial implementation of this protocol.

9. Authors Addresses

Narendar Shankar
Department of Computer Science
University of Maryland
A.V. Williams Building
College Park, MD 20742

Email: narendar@cs.umd.edu

William A. Arbaugh
Department of Computer Science
University of Maryland
A.V. Williams Building
College Park, MD 20742

Email: waa@cs.umd.edu

Kan Zhang
Hewlett-Packard Labs
1501 Page Mill Road
Palo Alto, CA 94304

Email: kan_zhang@hp.com