

Security Review of the Light-Weight Access Point Protocol draft-ohara-capwap-lwapp-02

T. Charles Clancy

clancy@cs.umd.edu

Laboratory for Telecommunication Sciences
Department of Defense*

Department of Computer Science
University of Maryland, College Park

May 12, 2005

Abstract

This document introduces the LWAPP protocol and provides an analysis of its security features. In particular, the public-key authentication, preshared-key authentication, and packet-level encryption are examined. Also, the security ramifications introduced by the IEEE 802.11 binding are reviewed. Lastly, recommendations on changes to the protocol are presented.

Overall, LWAPP is “secure”. However, given access to the wired network, there are opportunities for denial of service attacks against the public-key authentication algorithm. None of the attacks presented in this document result in the compromise of keying material for active sessions, or the ability to steal service.

1 Introduction

The Light-Weight Access Point Protocol (LWAPP) [1] offers a solution to the Control and Provisioning of Wireless Access Points (CAPWAP) problem [2]. Traditional access points are replaced by Wireless Termination Points (WTP) that essentially act as thin access points (APs). A collection of WTPs are governed by an Access Controller (AC). LWAPP defines the protocol between WTPs and ACs.

LWAPP includes three areas related to security. The first is its authentication protocol between a WTP and an AC. Both a public-key mode and a preshared-key mode are supported. Section 2 discusses these protocols in more detail and provides a security evaluation. The next area is packet level encryption, which is accomplished using AES-CCM, described in section 3. The LWAPP draft defines an 802.11 [4] binding, which is the third area. The interaction between LWAPP and 802.11 security is discussed in section 4. Lastly, section 5 provides recommendations to increase LWAPP’s overall security.

*The opinions expressed in this document are solely those of the author, and do not represent a formal evaluation or endorsement by the Department of Defense or US Federal Government.

2 Authentication

LWAPP defines two authentication protocols. The first is a public-key approach where the WTP and AC each have a certificate signed by a trusted certificate authority. These certificates are used to perform authentication and key distribution. The second is a preshared-key approach where a shared key is used to derive various authentication and session keys, which are subsequently validated.

In the next sections, the following notation will be used:

- $CERT_X$: Certificate of party X , containing PUB/X
- $E_K(Z)$: Encryption of message Z with key K
- $KDF_K(Z)$: PRNG keyed with K using entropy Z used for key generation
- MAC_X : L2 MAC address of party X
- $MIC_K(Z)$: Message Integrity Code generated over message Z with key K
- N_X : Nonce generated by X
- $\text{not}(Z)$: Boolean NOT of binary value Z
- PUB/X : Public key of party X
- PRV/X : Private key of party X
- PSK : Preshared Key between the WTP and AC
- $S_K(Z)$: Digital signature of message Z with key K
- SID : Session ID, randomly generated by the WTP

Each protocol will be evaluated in the following areas: mutual authentication, replay protection, key derivation, and session independence.

2.1 Public-Key Authentication

LWAPP public-key authentication can be abstracted as the following algorithm.

$$\begin{array}{c}
 \begin{array}{cc}
 \text{WTP} & \text{AC} \\
 \hline
 CERT_W, SID & \Rightarrow \\
 & \Leftarrow CERT_A, E_{PUB/W}(K) \\
 & \quad S_{PRV/A}(SID, E_{PUB/W}(K)) \\
 & \text{encryption key} = K
 \end{array}
 \end{array}$$

The WTP selects a random SID and sends it along with its certificate to the AC. After validation, the server replies with its own certificate, a session key encrypted with the WTPs public key, and a signature validating the message came from the server.

The LWAPP draft claims this protocol achieves mutual authentication; however, it only achieves *implicit* mutual authentication. The WTP is never *explicitly* authenticated by the AC. Lack of explicit mutual authentication can lead to several types of denial of service attacks. One example of an overloading DoS is where many spoofed clients could all simultaneously authenticate, overloading an AC. Another DoS attack involves a single client authenticating using an already-authenticated WTP certificate. This spoofed authentication session creates new session keys that the real WTP does not know, rendering it unable to communicate with the AC.

With only one round trip, replay protection is not possible. Obviously the first packet of any conversation can be replayed, however it is typically validated later by a packet that cannot be replayed. This replay problem is what facilitates the DoS attacks described above. Also, the AC is only weakly authenticated. The Join-Response can be replayed if an earlier transaction used the same *SID*. Since the *SID* is only 32 bits long, this space is fairly small from a cryptographic standpoint.

With respect to key derivation, the protocol uses entropy from only the AC and pushes the key to the WTP. This could lead to attacks if the AC's random number generator is compromised.

The LWAPP draft says that the WTP must validate the AC certificate, however the validation requirements should be more specific. In particular, there is nothing to prevent a second compromised WTP with a valid certificate from impersonating an AC. Certificates used by ACs should have an extended key usage field authorizing them for use as LWAPP ACs, or WTPs should have some other mechanism for authorizing ACs.

2.2 Preshared-Key Authentication

The preshared-key mode of authentication for LWAPP works by validating the successful decryption of various nonces encrypted with keys derived from the original PSK. Upon completion, both parties have independently derived a joint session key. The algorithm is described below.

	WTP	AC
	$\{J1, J2\} = \mathbf{KDF}_{PSK}(SID, MAC_W, MAC_A)$	
	$SID, \mathbf{E}_{J1}(N_W) \Rightarrow$	
		$\{J1, J2\} = \mathbf{KDF}_{PSK}(SID, MAC_W, MAC_A)$ $\{K, L\} = \mathbf{KDF}_{J2}(N_W, N_A, MAC_W, MAC_A)$ $M = \mathbf{E}_{J1}(\mathbf{not}(N_W), N_A)$
		$\Leftarrow M, \mathbf{MIC}_L(M)$
	$\{K, L\} = \mathbf{KDF}_{J2}(N_W, N_A, MAC_W, MAC_A)$	
	$\mathbf{E}_{J1}(N_W), \mathbf{MIC}_L(\mathbf{E}_{J1}(N_W)) \Rightarrow$	
		$\Leftarrow SID, \mathbf{MIC}_L(SID)$
	encryption key = K	

With respect to the evaluation criteria, the PSK authentication protocol satisfies them all. Mutual authentication is achieved by validation of the PSK-MIC fields in the final acknowledgement messages. Replay attacks are only possible on the first Join-Request packet, however without knowledge of the PSK, an attacker cannot forge the second Join-Request. Neither of the Join-Responses are replayable. This technique derives strong keys and provides session independence. It does not provide forward secrecy, but that is not a protocol requirement.

3 Packet-Level Encryption

Control packets in LWAPP are encrypted using AES-CCM with an IV seeded by the Session ID (*SID*) used in the initial authentication. The IV is not included in the packets, but rather each participant keeps a counter indicating the current IV.

This approach to the IV could lead to desynchronization attacks if there are any flaws in the WTP or AC state machines. Yet, this approach is good in that it doesn't allow either party to easily select their IV. However, note that since the client has complete control over the Session ID selection, it allows the client to consequently have control over the IV space.

4 IEEE 802.11 Binding

The LWAPP 802.11 binding supports both standard 802.11 WEP for privacy and authentication, along with the more recent amendment 802.11i [5] and RSN security.

First it should be noted that any network employing WEP (in conjunction with LWAPP or not) is insecure, due to the various insecurities of WEP [3]. Consequently this evaluation will only examine using LWAPP in conjunction with 802.11i RSN.

The biggest area of concern the handoff process. During an authentication, either EAP or a preshared-key is used to compute the pairwise master key (PMK). This key is then used in the 802.11 four-way handshake to derive session keys. In LWAPP this conversation happens between the wireless client and the AC. When a client roams from one WTP to another, LWAPP sends the link-layer encryption keys derived during the initial four-way handshake to the new WTP in the Add-Mobile request.

Without additional requirements on implementation state machines, there are two potential attacks here. The first is a denial of service attack where a client simply spoofs the association frames for an already authenticated client. If improperly implemented, the AC could send a Delete-Mobile request to the WTP to which the valid client is connected and Add-Mobile requests to the WTP to which the spoofed client is connected. The valid client loses connectivity. This is more serious than other L2 802.11 denial of service attacks because it can be carried out against any WTP.

The second attack involves a compromised WTP. Session keys should only be live between a client and a WTP. When a client roams to a new WTP it should have new packet-level encryption keys. However, in LWAPP draft does not specify that keys must be rederived.¹

5 Recommendations

The public-key protocol as-is is practically secure, but not cryptographically secure. It will prevent unauthorized clients from easily gaining access to the network; however, it is susceptible to various denial of service and replay attacks. The preshared-key protocol as-is is cryptographically secure.

To follow are alterations to LWAPP to enhance security. Changes that are *recommended* will prevent attacks currently mountable against LWAPP. Changes that are *suggested* will help prevent future attacks if the cryptographic primitives employed by LWAPP are weakened.

¹It should be noted that these attacks are not possible in the current Cisco LWAPP implementation, as handoffs are authenticated and rekeys occur upon roaming. These issues should, however, be addressed in the LWAPP draft.

At a minimum, it is recommended that the following changes be made to the LWAPP public-key authentication protocol:

- Add an additional round-trip to perform explicit key validation.
- Increase the size of the SID to 128 bits to prevent replay attacks, or add an additional nonce.
- Require AC certificates to contain an extended key usage authorizing them to provide AC services.

The following changes are suggested to the packet-level encryption:

- Secure derivation of the initialization vector, at least by the AC, but preferably by both the AC and WTP.

Additionally, the following suggested changes to the public-key protocol serve to mitigate future attacks:

- Perform key derivation based on exchanged entropy, rather than having the AC push a key to the WTP.

The following suggested changes to the 802.11 binding will increase overall security when LWAPP is used in conjunction with IEEE 802.11:

- Normatively RECOMMEND that LWAPP not be used with 802.11 WEP.
- Add text stating that handoffs must be authenticated, for example by requiring a successful 802.11 rekey before moving a session from one WTP to another.

In conclusion, this security evaluation was conducted from a protocol perspective, assuming the security of the underlying cryptographic primitives. If the security of any of the employed primitives are severely weakened, then the protocol security of LWAPP will need to be reevaluated.

References

- [1] P. Calhoun, B. O'Hara, S. Kelly, R. Suri, M. Williams, S. Hares, and N. Cam Winget, *Light weight access point protocol*, Internet Draft, I-D.ohara-capwap-lwapp-02, 2005.
- [2] B. O'Hara, P. Calhoun, and J. Kempf, *Configuration and provisioning for wireless access points (CAPWAP) problem statement*, RFC 3990, 2005.
- [3] N. Petroni and W. Arbaugh, *The dangers of mitigating security design flaws: A wireless case study*, January 2003.
- [4] IEEE Computer Society, *Wireless LAN medium access control and physical layer specifications*, IEEE Standard 802.11, 1999.
- [5] ———, *Wireless LAN medium access control and physical layer specifications amendment 6: Medium access control security enhancements*, IEEE Standard 802.11i, 2004.