Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 18, 2013

S. Orr
A. Grieco
Cisco Systems, Inc.
D. Harkins
Aruba Networks
October 15, 2012

Cryptographic Security Characteristics of 802.11 Wireless LAN Access Systems
draft-orr-wlan-security-architectures-00

Abstract

This note identifies all of the places that cryptography is used in Wireless Local Area Network (WLAN) architectures, to simplify the task of selecting the protocols, algorithms, and key sizes needed to achieve a consistent security level across the entire architecture.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 18, 2013.

Copyright Notice

Table of Contents

1. Introduction

Wireless LAN Access Systems (WLAS) are complex systems that involve interworking many technology components defined by various standards bodies. To ensure that the entire system is secure against sophisticated, persistent, and well-funded adversaries, each component MUST use strong cryptography. However, the architectural-level cryptographic capabilities and relationships between the various protocols and security mechanisms provide by each of the WLAS architecture components have not been documented.

In this note, we define a series of architectures based on common wireless LAN standards; IEEE 802.11 [IEEE.802-11.2012], Control and Provisioning of Wireless Access Points [RFC5415], RADIUS [RFC2865], IEEE 802.1x [IEEE.802-1X.2010], and the Extensible Authentication Protocol [RFC5247]. Within each of these architectures, we describe the uses of cryptography and in doing so, we capture an overall understanding of the cryptographic security of the Wireless LAN Access Systems. This document can also serve as a framework for future specifications to define profiles that specify particular cryptographic algorithms at each area of the architecture creating detailed specifications for interoperability with well understood cryptographic security properties.

This document does not define new protocols, nor cryptographic algorithms.

2. Conventions Used In This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Architectures

3.1. Overview

The Wireless LAN Access System (WLAS) architectures discussed in this document describe host/user and network authentication, over the air security, as well as various methods for managing the backend processes to support that wireless LAN access system. These backend processes include both distributed as well as non-distributed infrastructures for doing access control, authentication and Radio-Frequency management.

3.2. Standalone WLAS

The Standalone WLAS consist of a Wireless Termination Point (WTP or Access Point) and a client. The client contains an IEEE 802.1x [IEEE.802-1X.2010] supplicant and the client side of an EAP method [RFC3748]. The WTP contains an IEEE 802.1x [IEEE.802-1X.2010] authenticator. An Authentication, Authorization and Accounting Service (AAA), which incorporates the server side of at least one EAP method [RFC3748], resides either on the WTP or as a stand-alone server. This architecture is commonly deployed in small scale environments such as consumer and commercial deployments, or in places where backend resources are not available to provide a more distributed architecture. If 802.1x authentication is not deployed then 802.11 SAE authentication SHOULD be used for secure authentication using a pre-shared key or password.

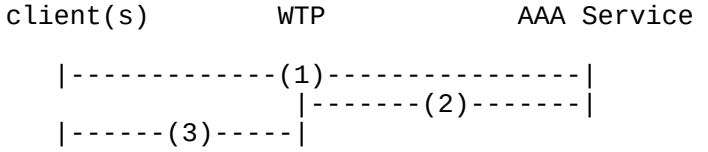

Figure 1: Standalone WLAS Architecture

Each of the lines in Figure 1 denotes communication that MUST be secured. The numbers are defined in (Section 3.4). This notation is used throughout this note.

3.3. Centralized WLAS

The Centralized WLAS is similar to the Standalone AP architecture with the addition of an Access Controller (AC) to manage the collection of WTP's. By moving the IEEE 802.1x [IEEE.802-1X.2010] authenticator off the WTPs and centralizing it on the Access Controller, this architecture allows for large scale deployments of

secure wireless infrastructure. As with Section 3.2 the AAA service can be incorporated on the AC or reside on a stand-alone server. This architecture supports [RFC5415] for control and provisioning of wireless access points (CAPWAP).

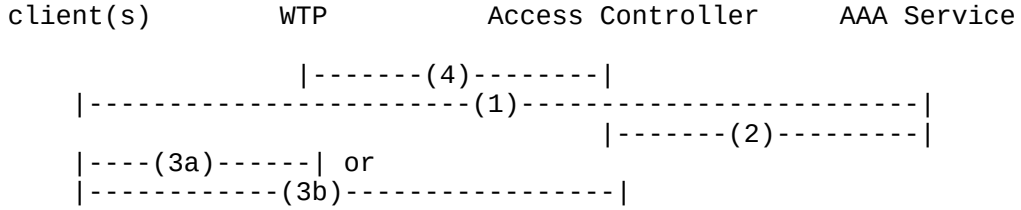

Figure 2: Centralized WLAS Architecture

3.4. Architectural Commonality

In each of the above architectures, there are necessary services that we will describe in more details in the sections below. (1) describes authentication and authorization communications that occurs between the client and the AAA service in the form of an EAP method. (2) describes additional communications that occurs in support of EAP, as well as distribution of other keying material via the AAA service. (3a) and (3b) describe the cryptographic security applied to [IEEE.802-11.2012] frames. In (3a), the frames are terminated on the WTP; in (3b) the frames are terminated on the AC. (4) Describes the authentication and cryptography security between the WTP and the access controller.

4. WTP to Access Controller Service Cryptographic Security

Specific to the Centralized WLAS Architecture is the establishment of a secure channel between the WTP and the AC. This command channel MUST be secured to insure both confidentiality and integrity of the communication between the AC and the WTP. The IETF has defined CAPWAP [RFC5415] to communicate between the WTP and the AC but there are other, proprietary, tunneling protocols to perform the same task. However, standards based security protocols such as DTLS, TLS or IPSEC MUST provide the authenticity and integrity assurance for securing any tunneling or encapsulation mechanism.

There are two channels between the WTP and AC that need security-- the command and control channel; and, the data channel. Through the command and control channel, the AC configures, queries and manages the WTP, and the WTP reports status and airtime monitoring information to the AC. Traffic sent between the client and the network behind the AC goes through the data channel.

[RFC5415] defines using DTLS [RFC6347]to protect the control and data channels. Other protocols such as IPSec [RFC4301] or TLS [RFC5246] can also be implemented to secure the control traffic in addition to the user data channel.

In order to establish secure connections between the WTP and AC credentials MUST be deployed on each device. The most obvious choice is an X.509 certificate which can be used to perform mutual authentication with DTLS [RFC6347], IPsec [RFC4301] or TLS [RFC5246].

5. Client to AAA Service Cryptographic Security

5.1. EAP Method

The [IEEE.802-11.2012]standard defines a Robust Security Network (RSN). An RSN can utilizes IEEE 802.1x [IEEE.802-1X.2010] and the Extensible Authentication Protocol [RFC3748], or it can use the SAE protocol in [IEEE.802-11.2012] to provide authentication and key management services between the client and WLAS. EAP Authentication occurs between the client and the AAA service which may reside within a component of the WLAS (WTP or AC) or as a standalone AAA Server. It is not the intent of this document to specify the type of transport for the authentication service (i.e RADIUS, Diameter [RFC3588] etc) or the specific communication channel between the Network Access Server (NAS) and the Authentication Service. Mutual-Authentication is achieved through the establishment of a secure channel for exchanging credentials between the client and the Authentication Server utilizing an EAP method which satisfies the requirements of [RFC4017]. The main output of the EAP process is the generation of the Master Session Key (MSK) and Extended Master Session Key (EMSK) known only to the Client (supplicant) and the AAA server that will be used to generate the keying material for the cipher suites. An in depth discussion on EAP Key management can be found in EAP Key Management Framework document [RFC5247].

5.2. Pre Shared Key, or Password, Method

When 802.1X is not used, a pre-shared key or password/passphrase can be used with the SAE protocol from [IEEE.802-11.2012] to perform the mutual authentication and key management functions required by an RSN. SAE employs a zero-knowledge proof protocol that allows the client and WTC/AC to prove knowledge of a shared secret (PSK or password or passphrase) without disclosing the secret. It is resistant to off-line dictionary attack. The result of the SAE protocol is a cryptographically strong PMK based on discrete logarithm cryptography.

An alternative to SAE is the pre-shared KEY mode of [IEEE.802-11.2012] referred to by the Wi-Fi Alliance as Wi-Fi Protected Access Personal (WPA2-PSK). With WPA2-PSK, the pre-shared key repeatedly hashed to directly generate a 256-bit PMK. This technique should be avoided, though, as is susceptible to off-line dictionary attack and numerous attack tools to subvert WPA2-PSK exist on the Internet.

6. Authenticator to AAA Service Cryptographic Security

As stated in the previous section, the byproduct of EAP authentication is the generation of keying material to be used in the cryptographic process between the client and the WTP to secure the over the air communications. The AAA server generates the AAA key which will be forwarded directly to the WTP in a Standalone WLAS, and forwarded to the AC in a Centralized WLAS where they will generate the Pairwise Master Key (PMK) (bits 0-255 of the AAA key). The transmission of the AAA key needs to be protected between the AAA server and the WTP or the AAA server and the AC depending on which architecture is deployed. NIST has previously made recommendations on securely encrypting plain text keying material for transport over insecure media with AES Key Wrap [AES_Key_Wrap] as well as industry with the Advanced Encryption Standard Key Wrap Algorithm [RFC3394]. In addition to the transport of the keying material it is suggested that all AAA traffic between the Authenticator (WTP or AC) and the Authentication Service (AAA) be secured by standards based methods such as, but not limited to: IPSEC, TLS or DTLS.

7. Wireless Link Layer Cryptographic Security

Upon completion of an authentication protocol, such as SAE or [IEEE.802-1X.2010], the client and AC (or WTP) share a PMK. Since the PMK may be been disclosed by an external AAA server to the AC (or WTP) it is necessary to perform a key confirmation handshake. [IEEE.802-11.2012] defines the 4-way Handshake to prove possession of the PMK and to derive a transient session key, called the PTK, which is used to secure the wireless link layer. During the 4-way handshake, the WTP or AC also discloses a broadcast/multicast key, called the GTK, to use for the wireless media.

Wireless link layer communication is protected through the Advanced Encryption Standard Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). AES-CCMP is currently the preferred cryptographic algorithm for both unicast and multicast/ broadcast traffic. The client is the source and sink of a secure bi-directional data flow. The other end of that flow can be either the WTP or the AC, depending on whether it is a standalone WLAS (Section 3.2) or a centralized WLAS (Section 3.3), respectively.

8. Cryptographic profiles

In each of the above architectural areas, there are a number of different security protocols that serve various functions needed to build secure wireless LAN architectures. Each protocol has important choices to be made in context of this overall cryptographic security within that protocol and subsequently has significant impacts to the overall security parameters of the system. The security mechanisms are summarized in Table 1.

	Client	WTP	AC	AAA
Client		802.11	3rd Party; 802.1x Supplicant	EAP w/TLS
WTP	802.11		DTLS; IPSEC	TLS, DTLS, IPSec, AES KeyWrap (Standalone Architecture)
AC	3rd Party; 802.1x Supplicant	DTLS; IPSEC		TLS, DTLS, IPSec, AES KeyWrap
AAA	EAP w/TLS	TLS, DTLS, IPSec, AES KeyWrap (Standalone Architecture)	TLS, DTLS, IPSec, AES KeyWrap	

Table 1: Cryptographic Security Interactions

8.1. DTLS and TLS

TLS and DTLS are well studied and documented from a cryptographic strength perspective and there are a number of works that create profiles for TLS and DTLS and its use within systems of varying security requirements. Table 2 provides an example of the cryptographic functional requirements necessary to define a TLS CipherSuite and associated security of each. When profiling against this document, authors MUST define cryptographic algorithms for each function in Table 2

Function	Example Algorithms	Cryptographic Strength	Algorithm Reference	Cryptographic Strength Reference
Authentication	RSA 2048	112	[RFC3447]	NIST SP 800-57 [NIST800-57]
Key Exchange	ECC P256	128	[RFC4492]	NIST SP 800-57 [NIST800-57]
Payload Protection	AES 128 CBC	128	[FIPS.197.2001]	NIST SP 800-57 [NIST800-57]
Message Auth	HMAC-SHA - 1	128	[NIST.PUB.198A]	NIST SP 800-57 [NIST800-57]

Table 2: DTLS and TLS Cryptographic Security Algorithms

Throughout the Wireless LAN Access System, TLS and DTLS are used in a number of different places. Someone profiling wireless architectures might require alternative algorithm definitions for different uses of TLS/DTLS in the architecture. One example might be a place that describes using TLS or DTLS to protect the transport of an ephemeral key vs its use to protect a long lived secret. In this case, a profile might be willing to trade off less security of the cryptographic algorithms for the ephemeral key.

Table 3 shows the places in the wireless architectures described in Section 3 that TLS or DTLS can be used

Location in Architecture	Protocol	Used to Protect
WTP To Access Controller Service (Section 4)	CAPWAP using DTLS	Management, session keys, user traffic
Client to AAA Service (Section 5)	EAP method using TLS	session keys, authentication
Authenticator to AAA Service (Section 6)	DTLS/TLS, IPSec	Confidentiality and Authenticity of Radius traffic (wrapped session keys)

Table 3: DTLS and TLS Architectural Usage

8.2. X.509 Certificates

The security level provided by algorithm and key length choice for X.509 Certificates is well studied solely in context of the certificates itself. Table 4 lists the types of cryptographic security functions used within X.509 Certificates and provides examples for each. Any profile of Wireless LAN Architecture MUST include definitions for each cryptographic security function used within X.509 certificates.

Function	Example Algorithms	Cryptographic Strength	Algorithm Reference	Cryptographic Strength Reference
Signature Algorithm	RSA with 2048 bit public keys	112	[RFC3447]	NIST SP 800-57 [NIST800-57]
Public Key Algorithm	RSA 2048	112	[RFC3447]	NIST SP 800-57 [NIST800-57]
Hash Function	SHA256	128	[FIPS-180-3]	NIST SP 800-57 [NIST800-57]

Table 4: X.509 Certificate Cryptographic Security Functions

Throughout the Wireless LAN Access System, X.509 certificates are used in a number of different places. Table 5 shows the places in the wireless architectures described in Section 3 that X.509 Certificates are potentially used

Location in Architecture	Protocol	Used to Protect
WTP To Access Controller Service (Section 4)	DTLS used within CAPWAP; IPSec	Authenticity of Management, session keys, user traffic
Client to AAA Service (Section 5)	TLS (Example EAP Method)	Authenticity of session keys, authentication
Authenticator to AAA Service (Section 6)	DTLS, TLS or IPSec	Authenticity of AAA traffic (wrapped session keys)

Table 5: X.509 Architectural Usage

8.3. Link Layer Encryption

Link Layer encryption for Wireless LAN Access Systems is well defined by the IEEE 802.11-2012 standard Future 802.11 standards need to address link layer encryption as an integral part of the standard. Current 802.11 standards require the implementation of 128 bit key length.

Function	Example Algorithms	Cryptographic Strength	Algorithm Reference	Cryptographic Strength Reference
802.1x 4 Way Handshake	AES Key Wrap with HMAC-SHA1 - 128	128	[IEEE.802-11.2 0 12]	NIST SP 800-57 [NIST800-5 7]

Message Authentication	HMAC-SHA-1	128	[NIST.PUB.198A]	NIST SP 800-57 [NIST800-57]
Pseudo-Random Function	HMAC-SHA-1	128	[NIST.PUB.198A]	NIST SP 800-57 [NIST800-57]
802.11 Management Frame Encryption	AES-CCMP	128	[FIPS.197.2001]	NIST SP 800-57 [NIST800-57]
802.11 Payload Encryption	AES-CCMP	128	[FIPS.197.2001]	NIST SP 800-57 [NIST800-57]

Table 6: Link Layer Security Algorithms

As a minimum, link layer encryption needs to be used in wireless architectures as indicated in Table 7 to protect the data in transit. When profiling against this document, authors MUST define cryptographic algorithms for each function described in Table 7. In addition to over the air link layer encryption, there are other places where related, but different link layer encryption (i.e. 802.1ae) could be leveraged within the wireless architecture. Link layer encryption in these alternative places MAY be profiled for use in the overall cryptographic integrity of the system but are not covered here.

Location in Architecture	Protocol	Used to Protect
Client to WTP (Section 7)	AES-CCMP, AES Key Wrap, HMAC-SHA-1	802.1x 4-way handshake (stand alone configuration), 802.11 unicast/multicast data frames and Management Frame protection using the Integrity Group Temporal Key (IGTK)

Client to AC	AES-CCMP, AES Key Wrap, HMAC-SHA-1	802.1x 4-way handshake and optional configuration where 802.11 unicast/multicast data frames and Management Frame protection using the Integrity Group Temporal Key (IGTK)encryption is performed on the AC

Table 7: Link Layer Encryption Architectural Uses

8.4. AAA

It is strongly suggested that traffic between the WTP/AC and the AAA service be secured to provide confidentiality and integrity of the user/device being authenticated as well as the key data used for the encryption process. The use of the well documented cryptographic protocols IPSEC (Section 8.5), TLS or DTLS (Section 8.1) can be used to protect traffic between the WTP/AC and the AAA service. When profiling against this document, authors MUST define the cryptographic algorithms for each function in listed in Table 8

Location in Architecture	Protocol	Used to Protect
Authenticator to AAA (Section 6)	TLS/DTLS or IPSec	Used to secure all authentication traffic between the Authenticator (WTP or AC) and the AAA service
Authenticator to AAA (Section 6)	AES Key Wrap [AES_Key_Wrap]	Used to encrypt only the key data between the Authenticator (WTP or AC) and the AAA services
Client to AAA (Section 5)	EAP	Used to perform authentication between Client and AAA server

Table 8: AAA Security Architectural Uses

8.5. IPSEC

IPSEC is well studied and documented from a cryptographic strength perspective and there are a number of works that create profiles for IPSEC and its use within systems of varying security requirements. Table 9 provides an example of the cryptographic functional

requirements necessary to define an IPSEC CipherSuite and associated security of each. When profiling against this document, authors MUST define cryptographic algorithms for each function in Table 9

Function	Example Algorithms	Cryptographic Strength	Algorithm Reference	Cryptographic Strength Reference
IKE Authentication	RSA 2048	112	[RFC3447]	NIST SP 800-57 [NIST800-57]
IKE Pseudo-random Function	HMAC-SHA-256	256	[RFC4868]	NIST SP 800-57 [NIST800-57]
IKE Diffie-Hellman group	Group 14	112	[RFC3526]	NIST SP 800-57 [NIST800-57]
IKE Hash	SHA-256	128	[FIPS-180-3]	NIST SP 800-57 [NIST800-57]
IKE Encryption	AES 128 CBC	128	[FIPS.197.2000 1]	NIST SP 800-57 [NIST800-57]
ESP Encryption	AES-CBC	128	[FIPS.197.2000 1]	NIST SP 800-57 [NIST800-57]
ESP Integrity	HMAC-SHA1	128	[FIPS-180-3]	[NIST.PUB.198A]

Table 9: IPSEC Cryptographic Security Algorithms

IPSec in many cases has been superseded by other protocols for security within the Wireless LAN Access System. However, IPSEC could play a role and Table 10 describes places in the WLAN Access System Architecture (Section 3) where it can be utilized.

Location in Architecture	Protocol	Used to Protect
WTP To Access Controller Service (Section 4)	IPSec	Authenticity of Management, session keys, user traffic
Authenticator to AAA Service (Section 6)	IPSec	Authenticity and Confidentiality of AAA traffic (wrapped session keys)

Table 10: IPSEC Architectural Usage

9. Security Considerations

The cryptographic security level of a complex system is limited to that of the weakest component in the system. The use of 128-bit block ciphers with 128-bit keys is now common, but in many systems, the security is limited by other factors, such as public keys with a strength of just 80 bits, or keys that are manually configured. A typical security protocol uses multiple cryptographic algorithms to achieve different security goals: encryption to provide confidentiality, data authentication to protect the integrity of data, key derivation to provide the keys for those algorithms, key establishment to determine shared keys, and digital signatures to authenticate the entity on the other end of the wire. In order to provide a high security level, a protocol needs to use algorithms and parameters that consistently meet that security goal. Wireless systems use multiple security protocols, thus requiring consistency across multiple protocols. To achieve consistency, one must first understand all of the cryptographic components in a wireless system. This note makes that process easier, by cataloging the components that appear in typical wireless architectures.

It is also important to note that not all secrets are equal. A secret which gives you access to data for a short period of time might be considered less important than one that exposes data for a longer period of time. Depending on the system being built and associated security constraints, the value of the secret being protected can inform appropriate choices for the cryptographic strength over sub components of a wireless architecture.

Finally, this note is intended to encourage the use of consistent cryptographic strengths of confidentiality, integrity and authenticity within the entire wireless LAN architecture. While profiles of this document might justify inconsistent algorithm strength choices, the profiles need to use cryptography throughout the architecture to provide end-to-end security.

9.1. Algorithm Choices

The choices of the algorithms to use in this document are left to the profile authors discretion. However, it must be clear that profiles need to avoid the use of known broken cryptographic algorithms (i.e. WEP, TKIP, etc).

10. IANA Considerations

None

11. Acknowledgements

The authors would like to acknowledge David McGrew, Nancy Cam-Winget and Carlos Pignataro for their constructive comments on this document.

12. References

12.1. Normative References

[IEEE.802-11.2012]
"IEEE Standard for Information technology--
Telecommunications and information exchange between
systems-- Local and metropolitan area networks-- Specific
requirements Part 11: Wireless LAN Medium Access Control
(MAC) and Physical Layer (PHY) Specifications",
March 2012, <http://standards.ieee.org/getieee802/
download/802.11-2012.pdf>.

[IEEE.802-1X.2010]
"IEEE Standard for Local and metropolitan area networks -
Port-Based Network Access Control", 2010, <http://
standards.ieee.org/getieee802/download/802.1X-2010.pdf>.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson,
"Remote Authentication Dial In User Service (RADIUS)",
RFC 2865, June 2000.

[RFC5415] Calhoun, P., Montemurro, M., and D. Stanley, "Control And
Provisioning of Wireless Access Points (CAPWAP) Protocol
Specification", RFC 5415, March 2009.

12.2. Informative References

[AES_Key_Wrap]
"", <http://csrc.nist.gov/groups/ST/toolkit/documents/kms/
key-wrap.pdf>.

[FIPS-180-3]
FIPS Publication 180-3, "Secured Hash Standard",
FIPS 180-3, October 2008.

[FIPS.197.2001]
National Institute of Standards and Technology, "Advanced
Encryption Standard (AES)", FIPS PUB 197, November 2001, <
http://csrc.nist.gov/publications/fips/fips197/
fips-197.pdf>.

[NIST.PUB.198A]
National Institute of Standards and Technology, "The
Keyed-Hash Message Authentication Code (HMAC)", FIPS PUB
198A, March 2002, <http://csrc.nist.gov/publications/fips/
fips198/fips-198a.pdf>.

[NIST800-57] Barker, E., Barker, W., Burr, W., Polk, W., and M. Smid, "Recommendations for Key Management", NIST SP 800-57, March 2007.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3394] Schaad, J. and R. Housley, "Advanced Encryption Standard (AES) Key Wrap Algorithm", RFC 3394, September 2002.

[RFC3447] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003.

[RFC3526] Kivinen, T. and M. Kojo, "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)", RFC 3526, May 2003.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC4017] Stanley, D., Walker, J., and B. Aboba, "Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs", RFC 4017, March 2005.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4492] Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)", RFC 4492, May 2006.

[RFC4868] Kelly, S. and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", RFC 4868, May 2007.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5247] Aboba, B., Simon, D., and P. Eronen, "Extensible Authentication Protocol (EAP) Key Management Framework", RFC 5247, August 2008.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer

Security Version 1.2", RFC 6347, January 2012.

Authors' Addresses

Stephen M. Orr
Cisco Systems, Inc.
1 Paragon Drive
Suite 275
Montvale, NJ 07645
US

Email: sorr@cisco.com

Anthony H. Grieco
Cisco Systems, Inc.
7025 Kit Creek Road
RTP, NC 27709
US

Email: agrieco@cisco.com

Dan Harkins
Aruba Networks
1322 Crossman ave
Sunnyvale, CA 94089
US

Email: dharkins@arubanetworks.com