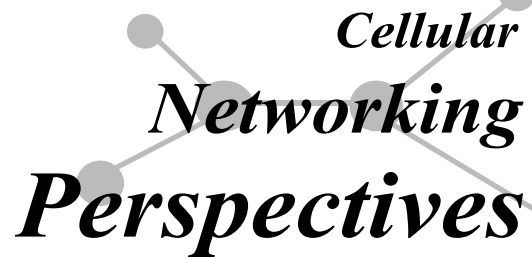


Wireless Security Perspectives



Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: wsp@cnp-wireless.com

Vol. 3, No. 9. October, 2001

Broadband wireless networks are showing up everywhere these days. At universities, airports, hotels, coffee shops, and corporate campuses all across the US, wireless local area networks, or WLANs, are aggressively being deployed. Some corporate users are discovering that wireless networks are simply cheaper and easier to install. Other users like the enhanced mobility and productivity gained by “cutting the wires” with WLANs. Still others like the flexibility and convenience WLANs offer for dynamically changing office environments or for travelling workforces. The corporations that are flocking to WLAN technology are helping the wireless industry experience a real boom. International Data Corporation (IDC) expects this tremendous growth to continue in the coming years. In fact, sales within the WLAN market are predicted to rocket to \$3.2 billion in 2005, from today’s \$1.5 billion market. Also, WECA (Wireless Ethernet Compatibility Alliance), the organization behind IEEE 802.11b WLAN technology – or “Wi-Fi” – has already noted that manufacturers are churning out products rapidly, and products prices are dropping drastically to fuel the growth.

While, the WLAN industry is indeed burgeoning, everything has not been positive. There have been several publicized attacks against the IEEE 802.11b WLAN technology. For example, researchers at UC Berkeley, University of Maryland and AT&T have all published papers on the security – or lack

of good security – of the standard. This month’s issue of *Wireless Security Perspectives* is an article by members of the RSA Security team who discuss one proposal the industry is considering, to address security inadequacies of the IEEE 802.11b WLAN standard.

Les Owens

Improving Wireless LAN Authentication

Håkan Andersson, Allen Forbes and Magnus Nyström

The IEEE 802.11b WLAN standard [1] is one of the dominant standards that specifies how to achieve wireless connectivity for fixed, portable, and moving stations in a local area. Any device that contains an 802.11b interface (e.g, laptop with network card) to the wireless medium is called a *station*. An entity that has station functionality and also gives associated stations access to a wired LAN (or the Internet) is called an *access point*. The basic architecture of 802.11b WLANs, with access points – or APs – and wireless stations, is depicted in Figure 1. Also, shown in the figure is the typical topology of connectivity from the WLAN to the Internet.

Today, common knowledge recognizes the inadequacy of the authentication mechanism – the process of verifying a claimed identity – defined by the IEEE 802.11b WLAN standard. For instance, since the access point is never

About Wireless Security Perspectives

Price

The basic subscription price for *Wireless Security Perspectives* is \$300 for one year (12 issues) for delivery by emailed PDF file or by first class mail within the US or Canada. International subscriptions are US\$350 per year. The basic subscription allows for distribution to up to 10 people within one organization. Contact us for license fees to allow more readers.

We provide discounts to educational institutions and small businesses (less than 10 employees).

Back issues are available individually, or in bulk at reduced prices.

Delivery is by first class mail or by email (Acrobat PDF file).

Complete pricing information for both publications is available at:

[www.cnp-wireless.com/
prices.html](http://www.cnp-wireless.com/prices.html)

To obtain a subscription, please contact us at:

cnpaccts@cnp-wireless.com

Next Issue Due...

November 15th, 2001.

Future Topics

Wireless Packet Data Security • IP Security • Public Keys & Wireless • IP Mobility Security • Security Issues in Ad hoc Wireless Networks • Electronic Signatures in Wireless • Latest in Watermarking • Security for PDAs • Blackberry • SMS security

Wireless Security Perspectives (ISSN 1492-806X (print) and 1492-8078 (email)) is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cresc. NW, Calgary, Alberta T2N 3W1, Canada. **Phone:** 1-800-633-5514 (+1-403-274-4749) **Fax:** +1-403-289-6658 **Email:** cnp-sales@cnp-wireless.com **Web:** www.cnp-wireless.com/wsp.html. **Subscriptions:** \$300 for delivery in the USA or Canada, US\$350 elsewhere. **Payment:** accepted by cheque, bank transfer, American Express, Diners Club, MasterCard or Visa. **Delivery:** Email or 1st class mail. **Back Issues:** Available individually for \$35 in the US and Canada and US\$40 elsewhere, or in bulk at reduced rates. **Discounts:** Educational and small business discount: 25% off any order. **Copies:** Each subscriber is licensed to make up to 10 copies of each issue or back issue. Call for rates to allow more copies.

Technical Editor: Les Owens.
Article Sourcing: Betsy Harter.
Production: Doug Scofield.
Distribution: Debbie Brandelli.
Marketing: Muneerah Vasanji.
Accounts: Evelyn Goreham.
Publisher: David Crowe.

Upcoming Fraud and Security Events

The following are some upcoming conferences and security events that may be of interest to the wireless and network security practitioners.

SecureIT 2001

21-23 October, 2001
Westin Innisbrook Resort
Tampa, FL

www.securitsummit.com/index.htm

Meta / DCI 4th Summit on Wireless Computing

28-31 October, 2001
Marriott Copley
Boston, MA

www.dci.com/brochure/wirebos

Fall 2001 Biometrics Summit

29-31 October, 2001
Washington Court Hotel
Las Vegas, NV

www.aliconferences.com/conferences/biometrics_oct01.htm

Information Assurance Technical Framework Forum

30 October, 2001
Laurel, MD

www.iatf.net/next.cfm

Blackhat Briefings 2001

21-22 November, 2001
Golden Tulip Grand
Hotel Krasnapolsky
Amsterdam

www.blackhat.com/html/bh-europe-01/bh-europe-01-index.html

SANS Institute Cyber Defense Initiative - East

27 November - 3 December, 2001
Grand Hyatt Washington
Washington, DC

www.sans.org/CDIeast/glance.htm

Ensuring End-to-End Security for Wireless Networking

29-30 November, 2001
Washington Court Hotel
Washington, DC

www.iirusa.com/security/index.cfm

authenticated by the distribution system (see Figure 1), a number of potential security attacks are possible – such as Denial-of-Service via rogue access points. Also, the standard defines only one-way authentication between the stations and the APs. This asymmetric use of a “challenge-response” authentication, whereby only the wireless stations are validated, presents a whole host of security issues. Because of the recognition of the problems with the current security scheme, for more than a year now, engineers and security professionals have been working to improve the standard. In fact, Ron Rivest – the cryptographer behind the Rivest Cipher 4 (RC4) algorithm that forms the foundation for 802.11b security – has been collaborating on improvements. Mechanisms for mutual authentication and key negotiation, making use of the new IEEE 802.1x port-based network access control standard [2], are being considered..

The first mechanism to address 802.11b security is the Extensible Authentication Protocol (EAP) for mutual authentication in a roaming environment. A second mechanism suggests server authentication and the negotiation of a cryptographic session key using the EAP Transport Layer Security (TLS) protocol. Therefore, the user authenticates using an EAP mechanism that is integrity and privacy protected by TLS. In essence, an embedding of *EAP inside TLS* is specified. This article briefly describes these new techniques that provide security services for access points and stations within an IEEE 802.11b WLAN, but these mechanisms may also be applicable in the future for other wireless networks, such as Personal Area Network (PAN) access with Bluetooth wireless.

Wireless Network Business Drivers

The possibility of achieving high-speed network access in an untethered fashion opens up a wide range of interesting applications. For example, a company can provide wireless access to the local network and to the Internet by installing WLAN access points in strategic locations of a building. This network topology provides significant flexibility and convenience for employees, who can easily bring their laptops from the office to the conference room while still enjoying full network services. Additionally, it can be used in public access Internet places, such as airports and hotels, allowing travellers to check their email using their own laptops – without cumbersome wires and cabling. In the modern supermarket or stock room, where inventory control might be performed using a WLAN, items could be scanned using a special mobile data-collection device, and the information transferred to an access point connected to the corporate LAN. In this application, the concept of roaming is very important. There would probably be numerous access points installed in the building, each of them covering a small area. Special hand-over mechanisms would allow the employee performing the inventory to walk around without losing their connection.

Unauthenticated users in these networks can have debilitating effects on the business through unauthorized access to sensitive corporate information, theft-of-services, fraudulent use of subscriber Internet access, and theft of goods and services by altering company data such as inventory information. Companies need a robust means of authenticating the users of 802.11b networks, which should be designed to mitigate these business risks. In the subsequent paragraphs, we describe 802.11b WLAN connectivity, security issues and a new security proposal.

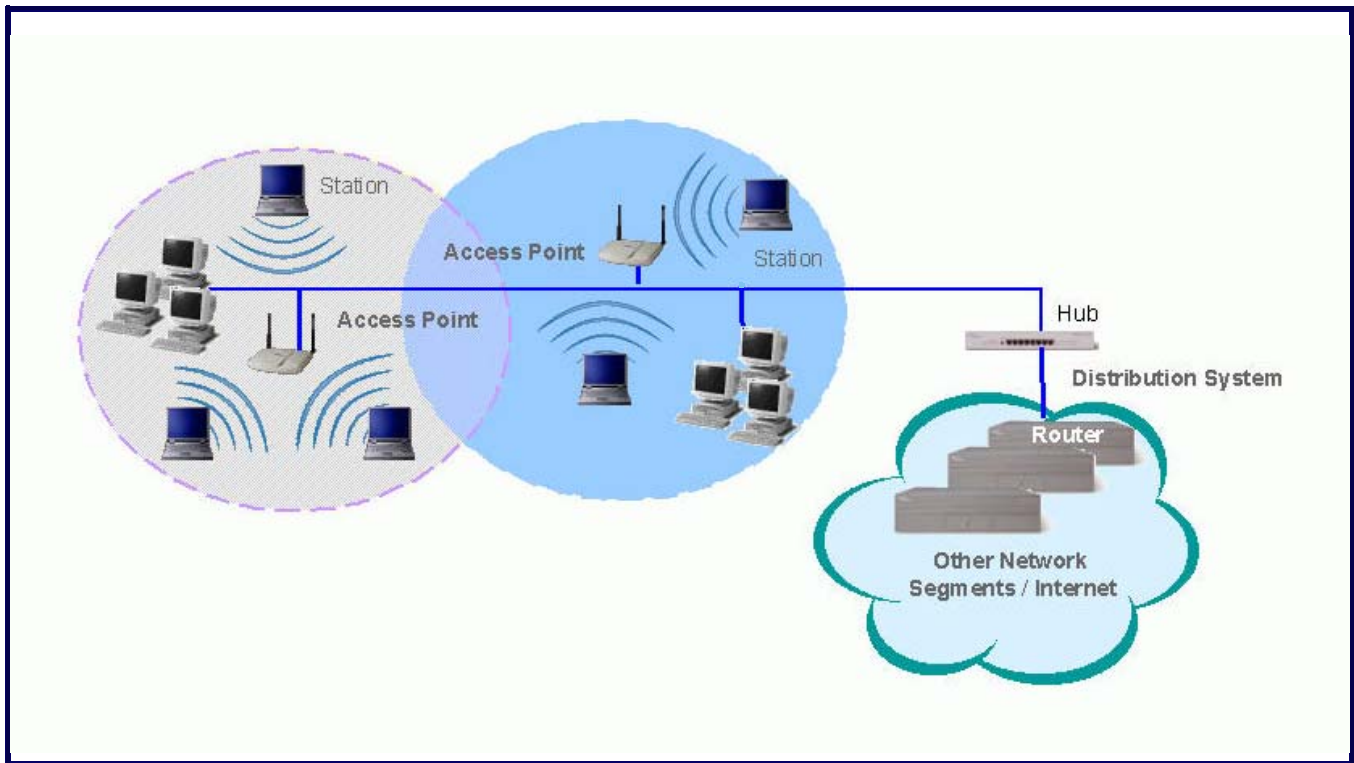
Another Upcoming Event

Privacy By Design 2001

3-5 December, 2001
Fairmont The Queen Elizabeth
Hotel
Montreal, Canada

privacy.zeroknowledge.com/privacybydesign2001

Figure 1: Typical 802.11b Wireless LAN Architecture



WLAN Connection Establishment

When establishing an 802.11b WLAN connection between a station and an access point, the entire process can be partitioned into three basic phases:

1. Probe
2. Authentication
3. Association

Probe Phase

A wireless station may locate an access point by active or passive scanning. In active scanning, the station sends a probe request, and the access points that detect this message send a probe response back to the station. The station then uses this information to determine which access point to address in the sequel. In passive scanning, the station simply listens for signals that are periodically transmitted by each access point, and it makes its choice based on that information.

Authentication Phase

When a suitable access point has been selected, the authentication phase begins. The IEEE 802.11b standard defines an authentication mechanism that is based on the knowledge of a pre-installed shared key. The authentication makes use of the WEP (“Wired Equivalent Privacy”) mechanism. The access point sends a random challenge parameter that the station must encrypt and return. If the access point computes the same response based on the shared key, validation is successful, and the station may proceed with the association phase.

Association Phase

After station identity validation, the station proceeds to send an association request to the access point. Given approval, the access point adds the station to its association table. During the association process, the current position of the station is distributed to the system. A station may be associated with no more than one access point, but an access point may, of course, be associated with several stations at one time.

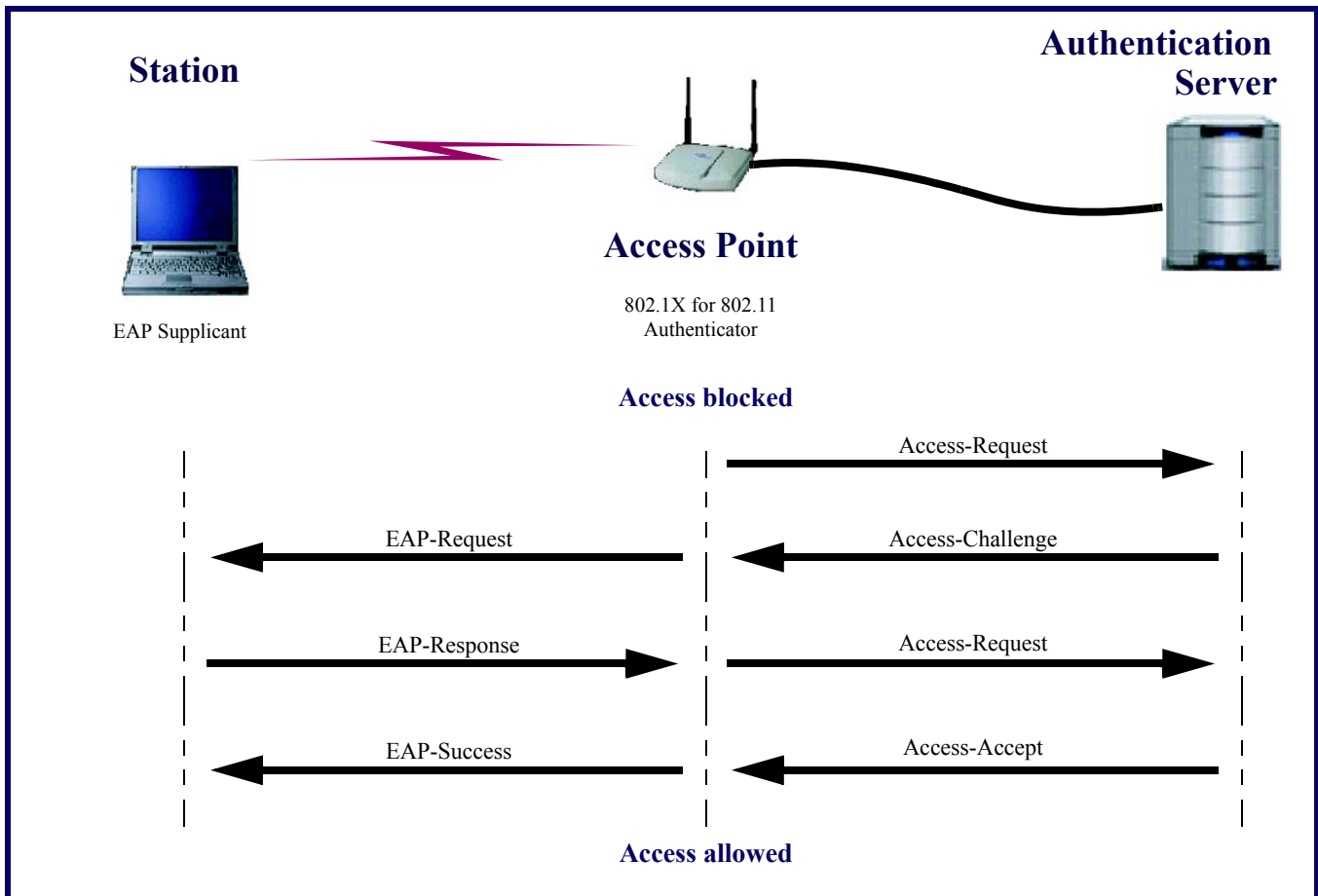
Security Issues in WLANs

Not unlike the challenges faced during first generation cellular communications, WLANs also have significant vulnerabilities and business limitations. In both cases, follow-on standards work, and adhoc solutions have and will solve many of the current weaknesses.

Privacy and Integrity

In the IEEE 802.11b standard, an encryption mechanism called WEP is defined to protect WLAN traffic. Unfortunately, a number of security problems have been identified with this mechanism (refer to references [3] & [4]). As an example, it is possible for an attacker to retrieve the secret key used in a session by simply monitoring encrypted packets sent over the air. Unfortunately, because of the design of other security parameters, increasing the key size will not help against these attacks. At present, an IEEE 802.11b Working Group is developing alternative solutions to provide privacy. A secondary goal of this work is to reach a solution with minimal impact on existing hardware.

Figure 2: Authentication Phase



Authentication

The authentication mechanisms defined in the standard are not satisfactory either, unfortunately. A station must prove its identity in order to get access to the WLAN. There is no provision, however, for an access point to prove its identity to the station, which exposes the networks to malicious access points that attempt to participate in the communication.

In the mid-1990's, deployment of cryptography-based authentication gave cellular carriers the ability to serve their legitimate customers and limit access by criminals. Today, both enterprise and public access authentication in the WLAN environment can meet similar goals. Additionally, a fraud-resistant means of authentication can be leveraged in public access roaming agreements while mitigating the incumbent risk to revenue.

Higher-Layer Authentication – the Basics

The IEEE 802.1x standard [2] specifies a general method for the provision of port-based network access control. A port is simply an attachment point to the LAN infrastructure – for example, a LAN edge switch or hub. The specification describes the architectural framework within which the authentication takes place, and it establishes the requirements for a higher-level authentication protocol between the station and the access point. The 802.1x work is now being leveraged by the 802.11b wireless LAN working group. Figure 2 introduces the 802.1x terminology as applied to an 802.11b WLAN implementation.

The Extensible Authentication Protocol (EAP), per reference [5], is a general authentication protocol defined in IETF (Internet Engineering Task Force) standards. In a WLAN context, the

access point sends one or more requests to the station and the station sends a response in reply to each request. The access point ends the authentication phase with a success or failure message. The IEEE 802.1x standard provides a framework that makes it possible to send EAP packets between IEEE 802.11b entities. Here, a back-end server is connected to the access point. This server actually communicates directly with the station during the authentication. The access point does not perform any calculations during the authentication phase; it transparently relays packets back and forth between the station and the server. In a roaming environment, the station may connect to several access points during a session. Hence, all the access points are assumed to be connected to the same back-end authentication server.

The “Protected EAP” Proposal

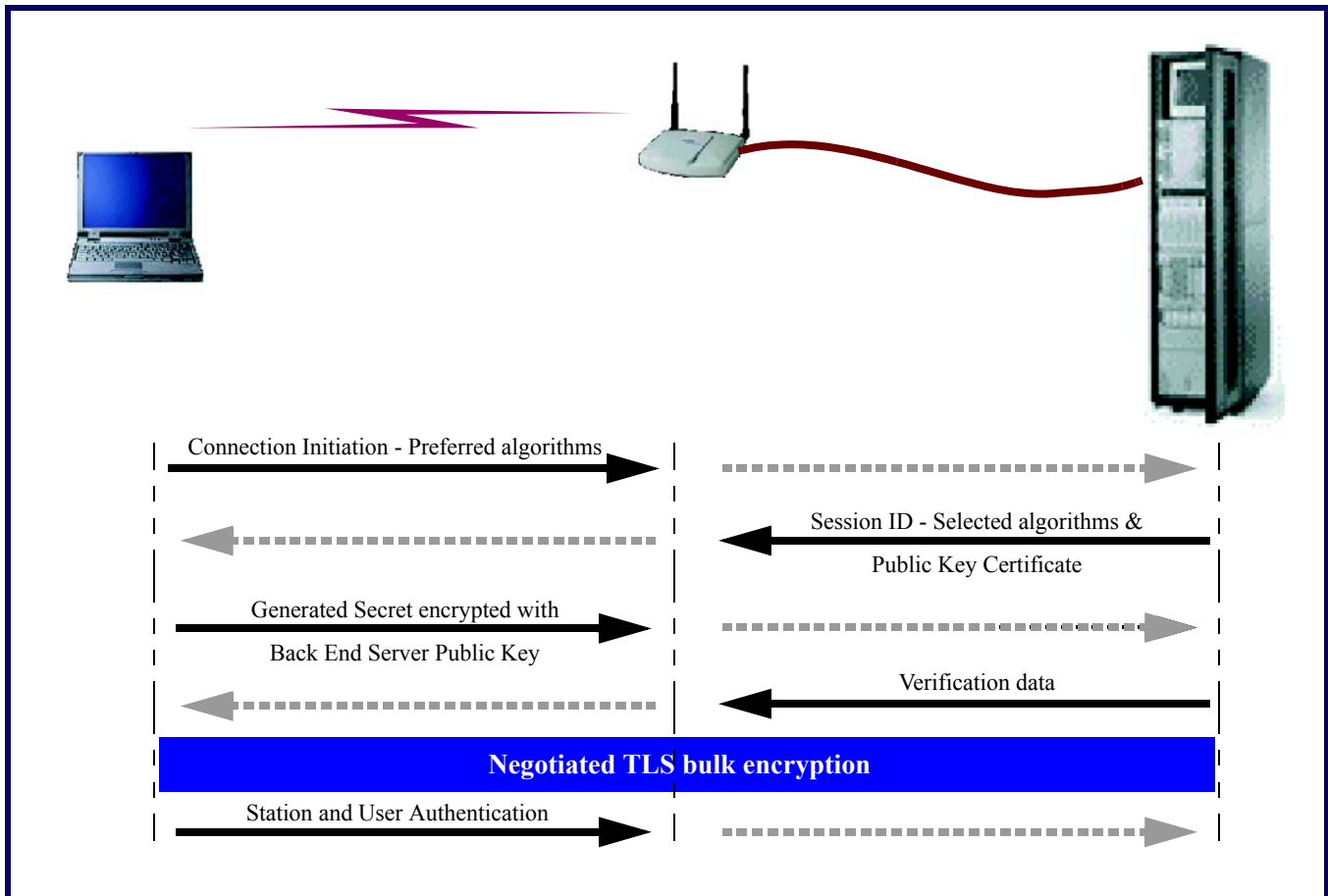
With the basic EAP method of higher-level protocol authentication introduced in the previous section, we can now introduce the EAP method for WLAN entities to provide the following: Strong authentication of the access point to the user; strong authentication of the user of the station to the access point; and session key negotiation. The method has been proposed to the IETF by RSA, working together with Cisco and Microsoft [6]. This draft is quite general,

and has 802.1x applications beyond 802.11b WLANs.

The TLS (Transport Layer Security) handshake protocol, per reference [7], is used to authenticate the back-end server to the user. TLS is an improvement to and slight variant of the well-known, ubiquitously used Secure Sockets Layer (SSL) protocol. Note, from the viewpoint of the user of the station, it is the access point that is being authenticated. As shown in Figure 3, the message flows for the TLS security processes are:

- First, the station notifies the access point that a new connection should be initiated, and it sends a list of preferred cryptographic algorithms.
- The back-end server responds with a new Session ID, a list of selected cryptographic algorithms and a public key certificate.
- The station then generates a secret key, encrypts it using the public key obtained from the server, and sends the result.
- Finally, the server in its last message proves its ability to retrieve the secret.

Figure 3: Transport Layer Security Phase



At this stage, both station and server may generate any amount of new key material to be used for subsequent “bulk” encryption of user traffic. TLS also provides a secure link over which authentication of the user now can be established, by simply tunnelling – securely transporting – another EAP mechanism. The user authenticates using any suitable EAP

mechanism: a user name and password or even better, a user name and a one-time pass code provided by a hand-held token. The authentication information is transferred to the back-end server over the secure TLS link. In some instances, the back-end server may need to communicate with another server to get this information validated. With the

approach described here, the messages sent by the station during user authentication are not transmitted in the clear. This point is particularly important in a wireless environment, where passive eavesdropping is a serious threat.

An important aspect to consider is the case of roaming users. For instance,

when a station is transiting between two access points during an active session, in order to obtain a seamless transition, the connection re-establishment mechanism provided by the TLS handshake protocol is used. Note that the new access point is assumed to use the same back-end server as the previous one, hence the previously negotiated secrets are still available. The station sends the Session ID of the old TLS connection, and the cryptographic algorithms negotiated earlier are sent also. If the Session ID is still valid, then the handshake is finished promptly. Otherwise a new Session ID is presented to the station by the server, and full authentication takes place again. Both the station and the server must know the old secrets in order to successfully complete the protocol. The time of validity of the Session ID is application dependent. In some environments, it may be desirable to have the server notify the station that the Session ID is about to expire. However, no mechanism is defined to handle this situation.

There are many compelling business cases driving WLAN deployments. However, corporate auditors and information security personnel are becoming concerned about embracing 802.11b deployments, because it will expose the enterprise network. Further, financial institutions are unable to guarantee client confidentiality when negotiating transactions. Finally, public access providers need to interoperate to facilitate roaming, single billing, and compliance to law enforcement requirements.

RSA Security invites interested persons to comment on the full draft. Several technical gatherings are planned to discuss this concept further. Please write to wireless@rsasecurity.com for additional details.

References

- [1]. 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, IEEE Std. 802.11, 1999.
- [2]. IEEE Standards for Local and Metropolitan Area Networks: Port-based Network Access Control, IEEE Draft 802.1X/D11, March 2001.
- [3]. Borisov, N., Goldberg, I., and D. Wagner, “Intercepting Mobile Communications: The Insecurity of 802.11”, in Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MCAN), Rome, Italy, 2001. Available from www.isaac.cs.berkeley.edu/isaac/mobicom.pdf.
- [4]. Fluhrer, S., Mantin, I., and A. Shamir, “Weaknesses in the Key Scheduling Algorithm of RC4”, in Proceedings of the 8th annual workshop on Selected Areas of Cryptography (SAC), Toronto, Canada, 2001. Available from www.wisdom.weizmann.ac.il/~itsik/RC4/rc4.html.
- [5]. Blunk, L., and J. Vollbrecht, “PPP Extensible Authentication Protocol (EAP)”, IETF RFC 2284, March 1998. Available from ietf.org/rfc/rfc2284.txt.
- [6]. Andersson, H., S. Josefsson, G. Zorn, and B. Aboba, “Protected Extensible Authentication Protocol (PEAP)”, IETF Work in progress, October 2001. Available from ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-xx.txt.
- [7]. Dierks, T., and C. Allen, “The TLS Protocol Version 1.0”, IETF RFC 2246, January 1999. Available from ietf.org/rfc/rfc2246.txt.

About the Authors

Håkan Andersson received his Ph.D. in Mathematical Statistics in 1994 from Stockholm University, Sweden. He is now working as a senior research engineer at RSA Laboratories, a section within RSA Security.

Allen Forbes develops the RSA Security business around newer and emerging means of authentication, authorization, and wireless security technologies. Allen has held several key security management

positions in the financial and wireless carrier industries.

aforbes@rsasecurity.com

Magnus Nyström is a Technical Director at RSA Engineering, focusing on aspects of wireless security. In 1999, he became RSA Laboratories Europe's first manager.

Fraud And Security Patent News

The US Patent and Trademark Office (USPTO) recently granted the following eight fraud and security patents. The patent number, invention title, inventor, and assignee (owner) are provided. All of these patents were granted in October, 2001.

These may be of interest to some of our wireless security practitioners. With the listing below, one can see who is doing what in the world of inventions. Moreover, it is often instructive to read issued patents, the references cited or other references included in the patent. For select patents provided below, we provide the URL, contact information, and some information about the assignee.

For a complete analysis of the applicability, efficacy and merit of the patents below, contact the editors of *Wireless Security Perspectives*.

US Patent: 6,301,484

Issued: 9 October

Method and apparatus for remote activation of wireless device features using short message services (SMS)

Inventors: John Rogers and Eric Levken

Assignee: QUALCOMM Inc. (San Diego, CA)

US Patent: 6,301,472

Issued: 9 October

Portable Telephone System

Inventor: Jiro Nakasu et. al.

Assignee: Mitsubishi Denki Kabushiki Kaisha (Tokyo, JP)

US Patent: 6,300,863

Issued: 9 October

Method and apparatus to monitor and locate an electronic device using a secured intelligent agent via a global network

Inventor: Christian Cotichini et. al.

Assignee: Absolute Software Corporation (Vancouver, Canada)

www.absolute.com

Contact:

Absolute Software Corporation
Suite 304, 1212 West Broadway
Vancouver, BC
Canada V6H 3V1
Telephone: (604) 730-9851 or
toll-free at (800) 220-0733

About: Absolute Software provides managed services for computer security and tracking. Over 1500 customers, including Fortune 1000 companies, government agencies, small and medium businesses, and educational institutions, rely on these services every day to securely track and manage remote, mobile and desktop PCs. Absolute's software-driven Computrace® technology platform powers both the company's PC tracking and loss control service Computrace-Plus, and its asset tracking and inventory management service AbsoluteTrack.

US Patent: 6,298,442

Issued: 2 October

Secure modular exponentiation with leak minimization for smartcards and other cryptosystems

Inventors: Paul Kocher and Joshua Jaffe

Assignee: Cryptography Research, Inc. (San Francisco, CA)

www.cryptography.com

Contact:

Cryptography Research, Inc.
607 Market Street, 5th Floor
San Francisco, CA 94105
Telephone: (415)397-0123

About: Cryptography Research, Inc. provides technology and services to companies that build and use cryptography products. Cryptography Research has a strong technical focus in many areas of cryptosystem research. Cryptography Research assists consulting clients and partners in identifying, developing, and implementing appropriate, cost-effective security solutions.

US Patent: 6,298,383

Issued: 2 October

Integration of authentication authorization and accounting services and proxy service

Inventor: Andrew Gutman et. al.

Assignee: Cisco Technology, Inc. (San Jose, CA)

US Patent: 6,298,250

Issued: 2 October

Wireless prepaid telephone system with extended capability

Inventor: Byard Nilsson

Assignees: Kimberly Engen and Bettina Thompson

US Patent: 6,298,153

Issued: 2 October

Digital signature method and information communication system and apparatus using such method

Inventor: Kazuomi Oishi

Assignee: Canon Kabushiki Kaisha (Tokyo, JP)

US Patent: 6,298,137

Issued: 2 October

Ring-based public key cryptosystem method

Inventor: Jeffrey Hoffstein

Assignee: NTRU Cryptosystems, Inc. (Burlington, MA)

To review the specification and claims of these patents visit the US Patent and Trademark Office web-site at www.uspto.gov. To obtain a complete copy of these patents, contact the US Patent and Trademark Office, at the address or telephone numbers below:

General Information Services
Division
U.S. Patent and Trademark Office
Crystal Plaza 3, Room 2C02
Washington, DC 20231
800-786-9199 or 703-308-4357