Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 4, No. 1. January, 2002

Cryptography In the News

Security Silicon is Booming

It is now generally recognized that security has become a very important part of all forms of communications, including wireless communications. Last month brought a flurry of activity in the security processor market to capitalize on this belief. For instance, Silicon Valley security silicon vendor Hifn announced a multi-phase relationship aimed at integrating Hifn security cores into Samsung broadband products, such as always on DSL modems and cable routers. The Letter of Intent (LoI) between Hifn and Samsung indicates, first, the joint development of a reference board leading to full incorporation of Hifn security IP (intellectual property) into Samsung s chipsets. Similarly, another Silicon Valley player, Cavium Networks, announced a reference design partnership with the Applied Micro Circuits Corporation (AMCC).

Two other players in the security silicon, or security processor, market are Corrent, and NetOctave. These companies, too, are positioning themselves to improve the security of communications equipment such as cable modems, set-top boxes, home networking and two-way satellite products. The cryptographic capabilities of these devices are designed to perform concurrently with the communication processing to ensure high-performance.

The chipsets of these four security silicon companies support such protocols as IPSec (Internet Protocol Security), L2TP (Layer 2 Transport Protocol), and IKE (Internet Key Exchange). Cryptographic algorithms that are supported include ones such as DES, 3-DES RC4, and the new NIST algorithm, AES. Hashing algorithms for message integrity and authentication include SHA-1 and MD5. Some of the devices will include random number generation capabilities to support both symmetric and public key processing.

Pundits predict continued growing interest in the security silicon market. Estimates are that the market will grow to more than $800 Million CAGR (Compound Annual Growth Rate) by 2005.

For more information on the security silicon vendors, visit the following sites:

- Cavium Networks: www.cavium.com
- Corrent: www.corrent.com
- Hifn: www.hifn.com
- NetOctave: www.netoctave.com

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

To obtain a subscription, please contact us at:

cnpaccts@cnp-wireless.com

Next Issue Due

February 17th, 2002.

Future Topics

Privacy in Wireless • Radius forWireless • 3G Security • IPSecurity • Public Keys & Wireless • Security Issues inAd hoc Wireless Networks • 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**: cnpsales@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 and Illustrator: 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.

Financial Network Security
28th - 30th January 2002
Marriott East Side
New York, NY
www.it-telecomsolutions.com/IT-Telecom_home.htm

Internetworking VPNs
29th - 31st January 2002
Hyatt Regency on Capital Hill
Washington, DC
www.it-telecomsolutions.com/IT-Telecom_home.htm

2002 Network and Distributed System Security Symposium (NDSS 02)
6th - 8th February 2002
Catamaran Hotel
San Diego, CA
www.isoc.org/isoc/conferences/ndss/02

Internet World Wireless East 2002
20th - 22nd February 2002
Jacob Javits Center
New York, NY
www.internetworld.com/events/weast2002

Usenix BSDCon Conference
11th - 14th February 2002
Cathedral Hill Hotel
San Francisco, CA
www.usenix.org/events/bsdcon02

m-CommerceWorld 2002
12th - 14th February 2002
Olympia 2
London, UK
www.m-commerceworld.com

US Postal Service Securing Information in the Electronic Age Conference
20th - 22nd February 2002
USPS/NCED Conference Facilities
Norman, OK
www.conference-ok.com

Securing The Maginot Line of Wireless LANs

By David N. Juitt,
Chief Security Architect, Bluesocket, Inc.

Editor's Foreword

This month s issue of *Wireless Security Perspectives* is another article in our series on 802.11 (commonly referred to as W i-Fi) wireless LAN security. David Juitt of Bluesocket provides his perspective on the requirements for securing this increasingly popular protocol. In particular, Mr. Juitt introduces the 802.1x port-based network access control protocol that is gaining momentum, and he provides brief glimpses of several flavors of the EAP (Extensible Authentication Protocol) being developed. He also suggests the need for fine-grained control over wireless network resources through the use of role-based access control (RBAC). Readers who are already familiar with the 802.11 architecture, the security services provided by 802.11, and the fundamental problems with the 802.11 WEP cryptography may wish to skip to the section titled ***The 802.1x Standard***. For additional information and other perspectives, consult the October 2001 and November 2001 issues of *Wireless Security Perspectives.*

More Upcoming Events . . .

Information Security Policy for the Public Sector - Implementing a Government-wide Security Infrastructure
26th - 27th February 2002
Ottawa, ON
www.iqpc.com

Enterprise Wireless Forum Conference & Expo
29th April - 1st May 2002
Convention Center
Santa Clara, CA
www.imgevents.com

Instant Messaging Planet Conference and Expo — Spring 2002
7th - 8th March 2002
Omni Parker House
Boston, MA
seminars.internet.com/im/spring02/index.html

14th Annual Computer Security Incident Handling Conference
24th - 28th June 2002
Hilton
Waikoloa Village, HI
www.first.org/conference/2002/cfp.html

Note: This conference will not occur for several months, but it is provided now because there is a *Call for Papers* (and because it may take a few months to negotiate the trip to the Islands).

Introduction

The goals of this paper are to create an understanding of the issues inherent in Wireless Local Area Network (WLAN) security, and to propose an architecture that provides a trusted local wireless data environment.

The Problem

The current state of security in most wireless LANs is no more than a Maginot Line, which proved useless during the latter part of WWII (a more detailed explanation of Maginot is in [1]). The security mechanisms thought to protect these networks need to be updated to provide more than just an illusion of security. Undue trust has been placed on the present industry standard mechanisms purported to protect our proprietary resources from access via wireless hacking.

In February 2001, the Wireless Ethernet Compatibility Alliance (WECA)

www.weca.net

issued a statement in response to the first of many successful attacks against Wired Equivalent Protocol (WEP), the privacy and authentication mechanisms built into 802.11 wireless LANs:

> A team of researchers at [the] University of California at Berkeley correctly reported [4]: A sophisticated methodology could be potentially used to compromise security of the Wired Equivalent Privacy (WEP) mechanism of Wi-Fi (IEEE 802.11b standard) wireless LAN products.

A series of papers from Intel, the Department of Computer Science at the University of

Maryland, and the Computer Science Department of the Weizmann Institute in conjunction with Cisco pointed out numerous flaws in the WEP standard. This research seriously stalled the advancement of interoperable security solutions for wireless LANs. The Cisco/Weizmann paper delivered its most devastating blow to WEP by describing a passive attack (i.e. one in which the attacker merely listens to data passing over the network) that can be used to recover a WEP key. Adam Stubblefield, John Ioannidis, and Aviel D. Rubin then demonstrated that 128-bit keys could easily be recovered using the FMS Attack.

Wireless LANs

An IEEE 802.11 wireless LAN consists of a set of 2.4 GHz radio transceivers. This includes clients (e.g. PCs, printers or PDAs) and access points (base stations). Access points act as bridges, transporting 802.11 wireless traffic between clients and to an 803.2 ("Ethernet") wired LAN. A typical 802.11 wireless LAN is shown in Figure 1 of our October 2001 issue of *Wireless Security Perspectives*. It shows a configuration of access points, clients and a hub – connected to the Internet via Ethernet.

Security issues

When data is transmitted over an untrusted medium, such as radio frequency, safeguards should be in place and effectively managed. In the case of wireless LANs, the fundamental trust model is significantly more challenging than in wired LANs, because the medium cannot provide rudimentary protection mechanisms. Wireless LANs allow casual eavesdropping purely because they use a public broadcast system for the communications medium, rather than a wire which constrains all communications.

For a wireless LAN security system to be effective, it needs to provide the following capabilities:

- **Access Control:** Authenticating users and authorizing them to access particular resources, while denying access to unauthorized users;
- **Link Privacy and Integrity:** Preventing unauthorized users from reading, introducing or altering data transmitted over the network;
- **Protection from Denial of Service:** Ensuring that one user, or a small group of users, cannot take up all of the bandwidth available on an access point, and thus deny access to other legitimate users.

The following sections describe how the 802.11 standard performs access control, and how it attempts to ensure privacy and integrity. Denial of service is not addressed at all in the current 802.11 standard.

Initial 802.11 Security Approaches

Authentication

Each node in a standard 802.11 network uses a network name (referred to as the Service Set IDentifier, or SSID). Before associating with a particular access point (AP), users can be required to enter the access point's SSID, together with a password. Unfortunately, the SSID is regularly broadcast by the AP, and can easily be detected. Moreover, the password is sent in plaintext, and an unlimited number of access attempts is allowed. These weaken the use of an SSID as an authentication mechanism.

The Medium Access Control (MAC) address of the 802.11 card may also be used for authentication and authorization. The MAC address is a unique 48-bit serial number allocated to each Ethernet device. Although it is not part of the 802.11 standard, many vendors allow the use of access control lists. Lists of authorized MAC addresses can be stored inside each AP. Only client devices with a MAC address appearing in an AP's access control list are allowed to connect to it. The problem with this approach is that an attacker can easily "sniff" the MAC addresses of clients connected to an AP, since they are not encrypted – they are sent in plaintext like SSIDs. Most 802.11 client devices allow the MAC address to be changed via software, so once in possession of a valid MAC address, the attacker can easily masquerade as a legitimate user. This is very similar to cloning that occurs when the ESN (Electronic Serial Number) of a cellular phone is modified.

Wired Equivalent Privacy (WEP)

In addition to the measures described above, the 802.11 standard defines a combined access control, data privacy and data integrity system called Wired Equivalent Privacy (WEP).

WEP Access control

WEP can be configured on a 802.11 network so a user cannot gain access without the correct key. This symmetric encryption key ranges from 40 to 128 bits. Generally, it is physically typed into each device and then stored for future use. Since the same key is used on each mobile device, if one key is compromised (e.g. a notebook computer is stolen), then all the remaining devices need to have their keys changed. WEP does not currently provide this key management function (automatic and scalable key changes for uncompromised devices).

WEP Link privacy

The 802.11 standard outlines the use of WEP as the encryption algorithm used to ensure privacy in a wireless LAN. The WEP encryption algorithm is based on RC4, developed in 1987 by Ron Rivest for RSA Data Security, Inc. The IEEE 802.11 group chose RC4 for WEP because it was cheap to license and easy to implement in software or hardware, thus allowing the vendors who made up the group to bring products to market quickly at affordable prices. Moreover, RC4 was freely exportable from the US, providing the key length was limited to 40 bits. RC4 is regarded as a reasonable encryption system for its time, but it can no longer be described as state-of-the-art. RC4 is a rudimentary stream cipher, and it must be implemented in an appropriate manner.

Link and data integrity

The standard way of ensuring integrity is to append some form of message authentication code to each block of data before it is transmitted. In WEP, the transmitting device generates a 32-bit cyclic redundancy code (CRC-32) checksum by performing a polynomial calculation on each frame

of data being sent. The checksum is appended to the data frame. The receiving device performs the same polynomial calculation on the data, and if the answer matches the checksum it has received, the data is assumed to be uncorrupted. This approach is fairly basic and simple to implement.

WEP s fatal flaws

The reason Wired Equivalent Privacy (WEP) failed was due to the attempt to use the RC4 stream cipher for both the authentication and the privacy functions. Even though RC4 is a perfectly good encryption algorithm, it was not applied correctly. RC4 explicitly warns never to use the same key material twice – no matter what the payload – since it is simply an XOR stream cipher.

The fatal flaw is the 24-bit initialization vector (IV), which is transmitted in the clear in every packet. Two straightforward changes (using a longer IV and using a secure hash algorithm, instead of CRC-32, for integrity) might have avoided the weakness in the privacy portion of the implementation.

The generation of the key schedule for RC4 involves appending the IV to the WEP shared key. In high traffic wireless environments, many packets are dropped, requiring a resend. Every resend of a packet is supposed to change the IV (which only has a 2^{24} keyspace), but often that is not the case. Walker's study[4] claims that two packets will have a 99% probability of a key space collision after only 2^{12} frames. If true, this translates to less than 5 seconds in a loaded 11 Mbps network; every few seconds there will be more than one packet transmitted using the same (IV, WEP) key pair. Obviously the problem will be exacerbated in 802.11a when bandwidth rises to a 54 Mbps maximum.

The attack involves collecting a significant amount of traffic, their associated plaintext fields (IP addresses and sequence numbers, for instance) and IVs. Every time there is an IV reuse, more information is available to do the cryptanalysis. Since we know some of the information in the packet (the plaintext), we get to generate a table that maps out the XORing material. This is basically a master decryption table. Demonstrations show that this table can be created in a matter of hours. Although the WECA believes this security attack is quite difficult, in reality, determined adversaries can be quite successful with it.

Because of the WEP design error involving the IV, 40-bit WEP keys provide very little protection. 128-bit keys are not much better, since the attack simply requires collection of more traffic to complete the decryption table.

The 802.1x Standard

Since 2000, IEEE has been aware of the security implications and implementation headaches of the WEP symmetric key approach. In June 2001, the new IEEE 802.1x standard, which specifies “a general method for the provision of port-based network access control,” was approved. The IEEE 802.1x standard enables authentication and key management for Local Area Networks.

802.1x is not an encryption algorithm, but it can be used to derive authentication and encryption keys for use with any cipher, as well as traditional key management functions. These capabilities fill in the pieces that were missing from the original 802.11 security solution.

IEEE 802.1x integrates well with standards for authentication, authorization and accounting (AAA), including RADIUS and LDAP. It fits in well with legacy AAA infrastructure. The general topology for 802.1x is shown in Figure 1.

The protocol itself is not a single authentication method; rather it utilizes Extensible Authentication Protocol (EAP) as its authentication framework. EAP typically runs directly over the link layer without requiring any services from IP (Internet Protocol), and therefore it includes its own support for in-order delivery and re-transmission.

Figure 1: Conceptual View of 802.1x Port-based Network Access Control

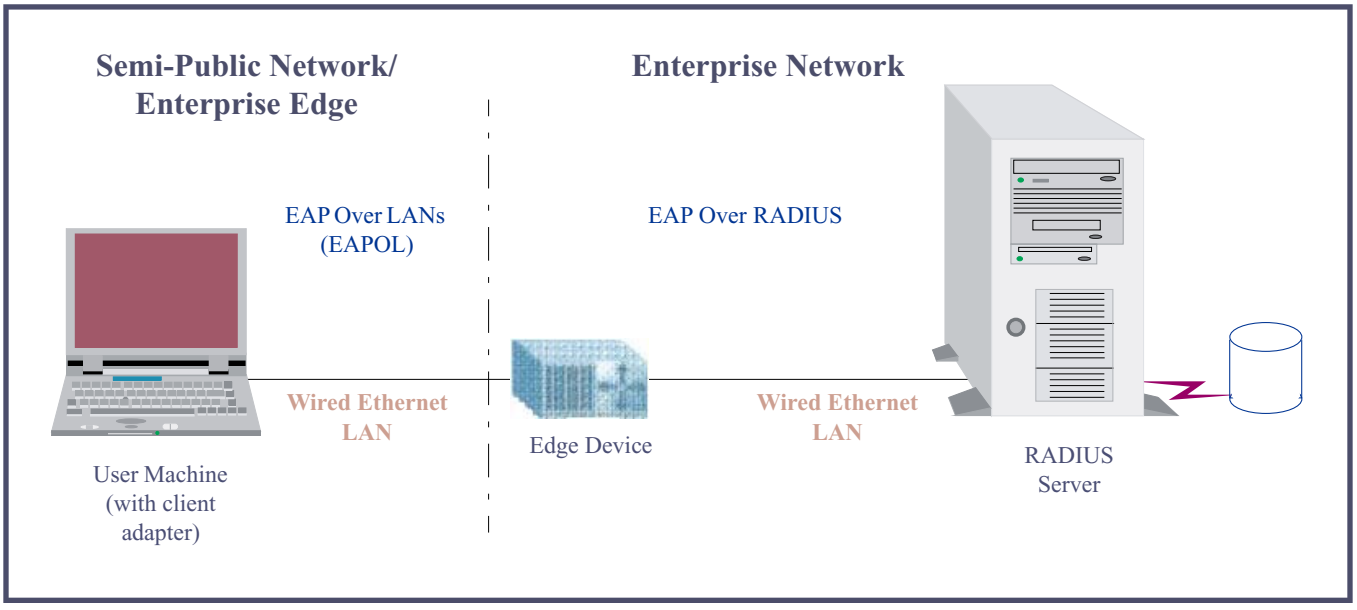
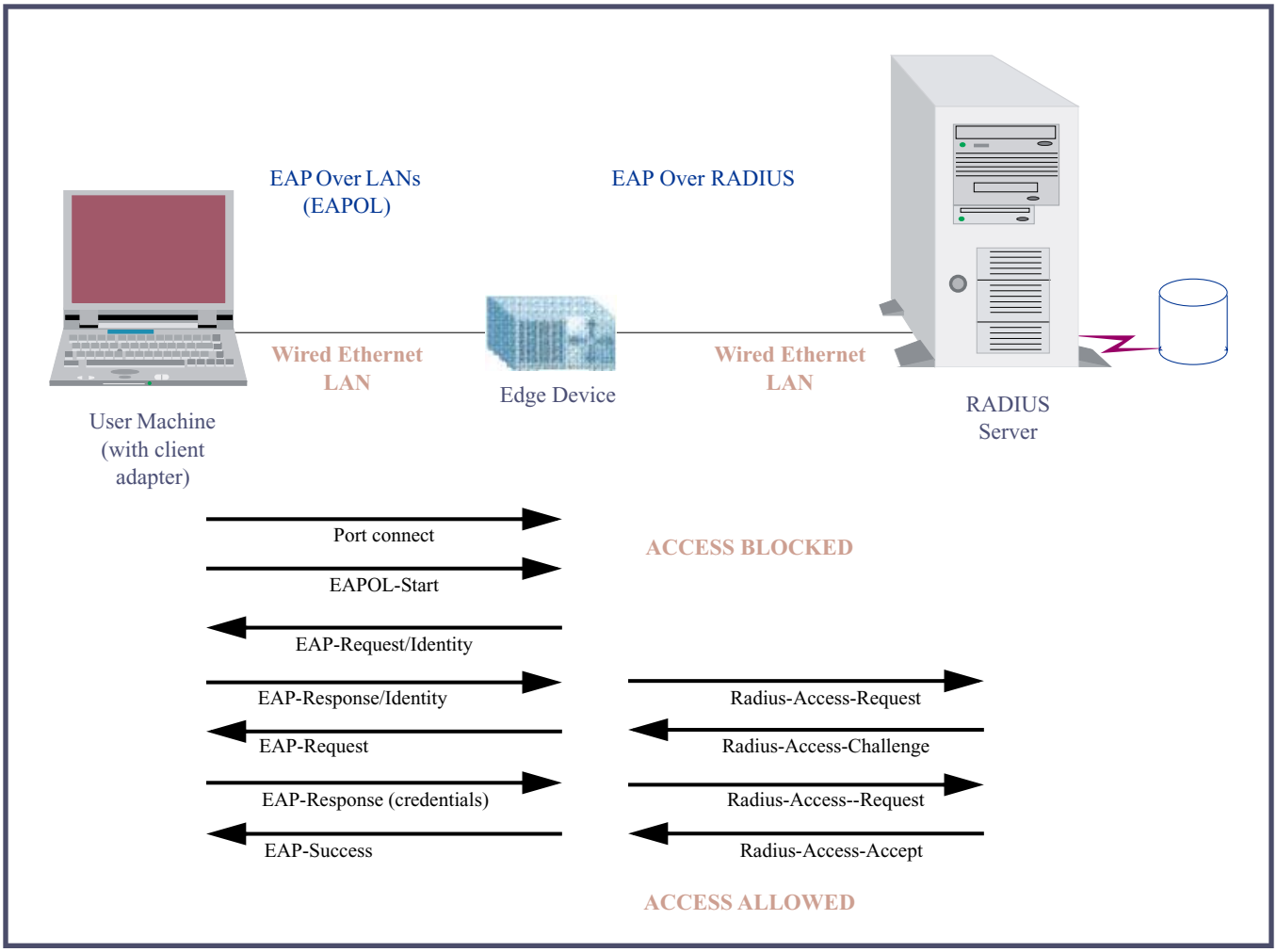


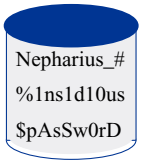
Figure 2: General 802.1x Protocol



Credentials Used in Authentication Solutions

Credentials are defined as data that is transferred or presented either to establish a chained identity or the authorizations of a system entity.

Passwords



Certificates

Tokens

Although EAP was originally developed for use with PPP (Point-to-Point Protocol), it has been extended for use on IEEE 802 links using the encapsulation described within IEEE 802.1X. While this provides a flexible environment, it introduces a new interoperability challenge. Since the introduction of the 802.1x specification, as illustrated generically in Figure 2, several competing alternatives have evolved as solutions fitting into the EAP framework.

These competing solutions vary widely, mainly falling into three broad categories of authentication credentials: Passwords, Certificates and Tokens.

Password-based EAP Proposals

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco-based standard that was one of the first implementations viable for use in a wireless environment.

EAP-SKE (Shared Key Exchange) supports efficient mutual authentication. It is targeted to support roaming across multiple-network-provider networks

EAP-SRP is a mechanism for EAP, based on the Secure Remote Password (SRP) [RFC2945] protocol.

Certificate-based EAP Proposals

EAP-TLS. In EAP-TLS, a Transport Layer Security handshake is used to mutually authenticate a client and server. This method is very similar to the mutual authentication that takes place in a standard SSL (Secure Sockets Layer) connection. EAP-TLS is a protocol requiring public-key cryptographic certificates on both sides of the wireless connection.

EAP-TTLS is an EAP protocol that extends EAP-TLS. Tunneled-TLS extends the authentication negotiation by

using the secure connection established by the TLS handshake to exchange additional information between client and server. EAP-TTLS differs from EAP-TLS, in that it is a protocol requiring public-key certificates only on the network side of the connection. It relies on legacy systems such as RADIUS for the authentication of wireless clients accessing the wireless network. This protocol will be featured in an upcoming issue of *Wireless Security Perspectives*.

PEAP (Protected Extensible Authentication Protocol) provides a mechanism for mutual authentication and session key generation in a roaming environment. The server authentication and the negotiation of the session key is done using the PPP EAP Transport Layer Security (TLS) Authentication Protocol. The user authenticates using a PPP EAP mechanism, with integrity and privacy protected by TLS. In essence, a wrapping of EAP inside TLS inside EAP is specified. For more details of PEAP, interested readers should view the September issue of *Wireless Security Perspectives*.

EAP-MAKE (Mutual Authentication Protocol). In EAP-MAKE, authentication is provided through a mechanism derived from the Diffie-Hellman scheme, and it is possible to derive and check a common symmetric key for the purpose of privacy. Scalability is provided by the underlying support of legacy PKI systems.

Token-based EAP Proposals

EAP-AKA is an EAP mechanism for authentication and session key distribution using the UMTS AKA authentication mechanism. AKA is based on pair-wise symmetric keys, and it runs in a UMTS Subscriber Identity Module, or SIM – a simple smart-card device. AKA also provides backward compatibility to GSM authentication, making it possible to use EAP AKA for authenticating both GSM and UMTS subscribers.

EAP-SIM is an EAP mechanism for authentication and session key distribution using the GSM Subscriber Identity Module (SIM).

Additionally, **EAP-GSS** is an EAP mechanism for support of multiple authentication methods, including public key, smart cards, Kerberos, One Time Passwords, and others.

Is the problem intractable?

Wireless Networks

One reason for multiple solutions is the emerging realization that wireless LANs are completely different environments from wired. The initial approach for providing wireless LAN security was to create the equivalent of wired privacy. That is a necessary element, but not a full solution.

Link layer security is designed to provide a protection mechanism from one point to another. The basic assumption is that all data on the link is considered to have been "created equal" – there is no inherent difference in any of the transmitted data. When used in a wireless LAN, link layer (Level 2) security only provides the ability to make coarse-grained – binary ON or OFF – decisions regarding access to the network.

At lower protocol layers (below IP), a wireless LAN is much more a traditional client/server environment than it is a link extension of a wired LAN. Wireless networks require the ability to identify accurately the source of the data, followed by a decision of whether that traffic belongs on that link. Therefore, none of the data can be treated from a bulk perspective.

The need for a unified approach

Traditional infrastructure solutions for providing authentication, authorization, service control and security management in a wireless local area network have required the configuration and integration of several different network components. With each of these components, there is often a different user interface. This can lead to a high degree of complexity, along with the risk of misconfiguration when deploying a wireless data solution. Some capabilities, such as centralized management of keys, might not even be provided.

This complexity creates a risk. An end user may not care as much about security as his/her employer does. If the security system is too hard to use, then the user may attempt to circumvent it, perhaps by simply ignoring security instructions. Hence, making the security as transparent as possible is a key design goal.

The need for key management

One of the fatal flaws in WEP can be traced to the lack of an automatic and scalable key management mechanism. Early work – by the IEEE 802.11 Task Group I – had proposed Kerberos as a solution.

Kerberos has its own problems. It is an extremely complex solution that depends on trusted (physically secure) online servers with time stamps for replay detection – which requires time synchronization between all access points and mobiles, and a physically secure clock. As a result, Kerberos does not lend itself well to being implemented in access points (costing approximately $250) left in unprotected locations.

A comprehensive security architecture for Wireless LANs

Wireless LANs need to provide the following security controls:

- Access control
- Secure tunneling
- Detection of fake access points
- Detection of rogue access points
- Roaming
- Prevention of denial of service

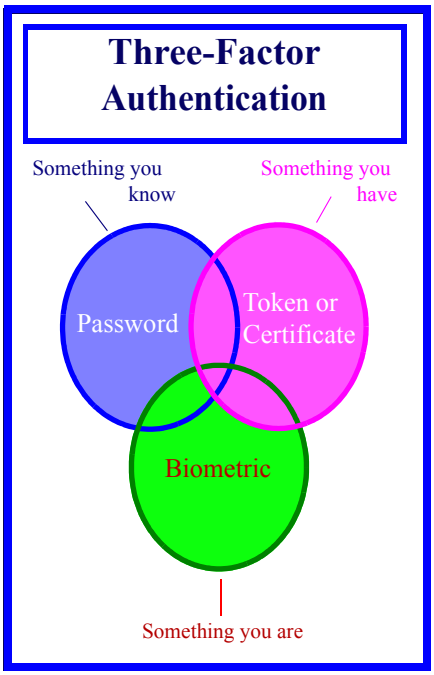
These security controls are described briefly below.

Access Control

Authentication is the ability to identify the end-user requesting a service. Authentication techniques have matured over many years of evolution of remote access systems.

Authentication works best when performed at the user level, not at the machine level. Ideally, the security architecture will support three-factor authentication (see below) corresponding to the value and nature of the information needing protection.

Strength of authentication is related to the use of multiple factors of information. For many years, security practitioners have recognized that ideal authentication includes verification according to: "something you know"; "something you have"; and "something you are" (physiological or physical characteristic).



Authorization is the process of determining whether an authenticated user has the appropriate privilege to access a requested resource. Together, authentication and authorization are commonly referred to as "access control".

One of the most challenging problems in managing large networked systems is the complexity of security administration. Today, security administration is costly and prone to error because administrators usually specify access control lists for each user on the system, individually. Role based access control (RBAC) is a technology that is attracting increasing attention, particularly for commercial applications, because of its potential for reducing the complexity and cost of security administration in large networked applications.

With RBAC, security is managed at a level closely corresponding to the organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role.

Security administration with RBAC consists of determining the operations that must be executed by persons in particular jobs, and assigning employees to the proper roles. Complexities introduced by mutually exclusive roles or role hierarchies are handled by the RBAC software, making security administration easier. The Bluesocket security solution, providing the above described RBAC capability, is shown conceptually in Figure 3.

Secure Tunneling

Protocols such as IPSec (Internet Protocol Security) and PPTP (Point-to-Point Tunneling Protocol) need to be used to provide richness of key management and encryption algorithm negotiations. Native compression capabilities in these protocols can also provide increased performance in the wireless environment. Table 1 shows typical performance for various security techniques.

Table 1: Throughput Measurements in Wireless Networks

Privacy mechanism	Data transfer rate	Bandwidth
None	5.8 MB	4.7 MB
64-bit WEP encryption	4.6 MB	3.7 MB
IPSec	7.0 MB	5.6 MB

Detection of Fake Access Points

Wireless LANs must prevent intruders from connecting their own access points to the network, with the intention of capturing users' passwords and mounting a "man in the middle attack."

Detection of Rogue Access Points

Wireless LANs must prevent users from installing unauthorized access points which, through poor configuration or design, could act as "back doors" providing unprotected access to the corporate network.

Roaming

Portability is another fundamental difference between wired and wireless networks. To provide user transparency and to meet user expectations, Wireless LANs must provide seamless, authenticated mobile handoffs anywhere in the enterprise.

Prevention of Denial of Service

Due to the potential bandwidth bottlenecks introduced by wireless network architectures, it is of paramount importance to ensure that one user (or a small group of users) cannot take up all of the bandwidth available on an access point, which would subsequently deny access and acceptable network performance levels to other legitimate users. Also, Wireless LANs should provide some mechanism to detect malicious attempts to jam access points with bogus traffic, resulting in degraded or shunted network performance.

To Probe Further

For additional information on the Bluesocket RBAC-based security solution, visit the Bluesocket web-site at:

www.bluesocket.com

or contact the author at:

djuitt@bluesocket.com

For additional information on the Extensible Authentication Protocol (EAP), the various referenced Requests for Comments (RFCs), or the various EAP-based protocols for securing 802.11, visit the Internet Engineering Task Force (IETF) web-site:

www.ietf.org

Also, the 802.1x specification may be obtained from the IEEE at:

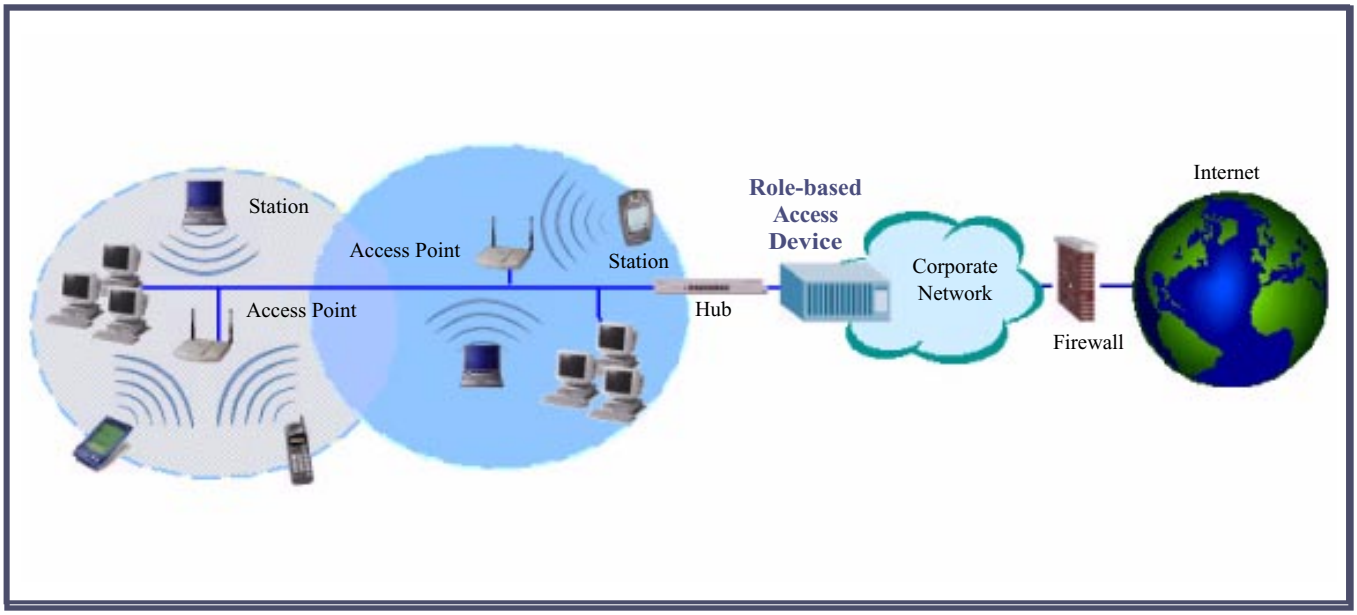
www.ieee.org

References

[1] The Maginot Line was named after Andre Maginot (1877 -1932), French Minister of War, who proposed a line of defense along France's border with Germany. Believed to be impregnable, the barrier proved to be of little use when Germans attacked through Belgium in 1940.

[2] Wireless Ethernet Compatibility Alliance, 802.11b Wired Equivalent Privacy (WEP) Security, February 19, 2001

Figure 3: Typical 802.11 Wireless LAN Topology with RBAC Security Device



[3] Intercepting Mobile Communications: The Insecurity of 802.11, N. Borisov, I. Goldberg, D. Wagner

[4] Unsafe at any key size; An analysis of the WEP encapsulation, J. Walker

[5] csrc.nist.gov/rbac

Fraud And Security Patent News

The US Patent and Trademark Office (USPTO) recently granted the following 12 fraud and security patents. These may be of interest to some of our wireless security practitioners. For each patent we include the patent number, the invention title, a brief description, the inventor(s), and the assignee (owner). For select patents, we provide additional information pertaining to the assignee, such as URL, background information and ways to contact them. All of these patents were granted in either December 2001 or January 2002.

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, since they include patent claims, specifications, illustrations and detailed descriptions. The references cited or other references included in the patent are an excellent source of background information regarding wireless systems and wireless security.

Search using the patent number at the USPTO website:

www.uspto.gov

US Patent: 6,330,140

Method and system for validating subscriber identities in a communications network

This patent specifies a method and system for cryptographically validating cellular wireless subscribers in an insecure IS-41 cellular environment that does not have (or support) the standardized Telecommunications Industry Association s CAVE-based authentication.

Issued: January 8, 2002

Inventor: Leslie D. Owens et. al.

Assignee: Iridium, LLC

Iridium.com

Note: This is the URL for the new Iridium: Iridium Satellite Solutions. The original went bankrupt in 2000.

The Iridium Satellite System is a provider of global mobile satellite voice and data solutions with complete coverage of the Earth (including oceans, airways and Polar regions). Through a constellation of 66 low-earth orbiting (LEO) satellites operated by Boeing, Iridium delivers essential communications services to and from remote areas where terrestrial communications are not available. The service is ideally suited for industrial applications such as heavy construction, defense/military, emergency services, maritime, mining, forestry, oil and gas and aviation. Iridium currently provides services to the United States Department of Defense. They launched commercial service in March 2001.

US Patent: 6,337,899

Speaker verification for authorizing updates to user subscription service received by internet service provider (ISP) using an intelligent peripheral (IP) in an advanced intelligent network

This patent specifies a method for controlling subscription services provided by an ISP that includes prompting for a voice response and authenticating a user's voice response pattern using an Automated Intelligent Network (AIN) telephone system and an intelligent peripheral subsystem connected to at least one central office switching system.

Issued: January 8, 2002

Inventor: Tommy Alcendor et. al.

Assignee: International Business Machines Corporation (Armonk, NY)

US Patent: 6,337,854

Method of securing communication between two mobiles and associated transmitter

This patent describes a method of transmitting an initial message between two radio communication stations (perhaps mobile), in which a first radio communication station inserts a time supplied by a clock in the initial message to form an outgoing message, and transmits the outgoing message and the successive times supplied by the clock to the second radio communication station.

Issued: January 8, 2002

Inventors: Helene Palpini and Fran Simon

Assignee: Alcatel (Paris, FR)

US Patent: 6,337,634

Radio frequency data communications device

This patent specifies a radio frequency identification device comprising an integrated circuit (preferably a monolithic single die) including a receiver, a transmitter, and a microprocessor that has a much greater range than other devices because of the transponder characteristics.

Issued: January 8, 2002

Inventor: James E. O Toole

Assignee: Micron Technology, Inc. (Boise, ID)

US Patent: 6,337,621

Security and emergency communication service coordination system and notification control method therefore

This patent specifies a security apparatus that upon detecting an abnormal condition occurring in a vehicle, issues an alarm and an emergency communication service apparatus that communicates with a response center, and which receives services from the response center during an emergency, being connected so that information can be transmitted and received between them.

Issued: January 8, 2002

Inventor: Takayuki Ogino

Assignee: Alpine electronics, Inc.

US Patent: 6,336,187

Storage system with data-dependent security

This patent specifies a host-independent storage facility that selectively provides data-dependent security by initially storing a security key in association with a storage region, where that key must be presented by any host seeking access to the region.

Issued: January 1, 2002

Inventors: Robert Kern and Mark Sovik

Assignee: International Business Machines Corp. (Armonk, NY)

US Patent: 6,336,186

Cryptographic system and methodology for creating and managing crypto policy on certificate servers

This patent specifies a cryptosystem that has a Certificate (Key) Server for storing and maintaining certificate or key information in a certificate database based on a set of policy constraints which are set for one's particular site (e.g., company).

Issued: January 1, 2002

Inventor: Marc Dyksterhouse et al

Assignee: Networks Associates Technology, Inc. (Santa Clara, CA)

US Patent: 6,336,142

Methods and apparatus for downloading data between an information processing device and an external device via a wireless communication technique

This patent specifies an information processing apparatus and a method for controlling that apparatus, which enables the smooth transfer of data (such as processed results obtained from execution of an application program, an HTML file acquired from a Web server in accordance with the TCP/IP protocol or the like) to an external PDA device by using an infrared communication function.

Issued: January 1, 2002

Inventors: Naotaka Kato and Yoshihisa Kanada

Assignee: International Business Machines Corp. (Armonk, NY)

US Patent: 6,336,971

Country to country call intercept process

This patent specifies a call intercept process (CIP) for calling card calls originating from an international country and terminating at an international high fraud country whereby a call is first screened against a database to determine if the country is considered high fraud potential and the call is routed to a first level operator in order to verify the billing account information of the caller as an authorized user.

Issued: January 1, 2002

Inventors: Arthur Springer and Dean Marchand

Assignee: MCI WorldCom, Inc. (Jackson, MS)

US Patent: 6,334,190

System for the manipulation of secure data

This patent specifies a system for the manipulation of secure data which includes electronics or software (or both) that are designed to operate within a specific clock speed range (a clock frequency limiter in the clock signal line).

Issued: December 25, 2001

Inventors: Kia Silverbrook and Simon Walmsley

Assignee: Silverbrook Research Pty Ltd. (Balmain, AU)

US Patent: 6,334,185

Method and apparatus for centralized encryption key calculation

This patent specifies a system and method for encrypting transmissions between a set of communication nodes and a mobile station, wherein the algorithm for generating an encryption key resides within the first communications node and the other nodes obtain keys from the first node through a PMAP interface interconnecting the nodes.

Issued: December 25, 2001

Inventors: Rolf Hansson and Hans-Olaf Sundell

Assignee: Telefonaktiebolaget LM Ericsson (publ) (Stockholm, SE)

US Patent: 6,334,146

System and method for remotely accessing data

This patent specifies a computer system and network to allow secure, network-based connectivity in support of multi-enterprise collaboration activities.

Issued: December 25, 2001

Inventor: Abhay Parasnis

Assignee: i2 Technologies US, Inc. (Dallas, TX)

Contact:
One i2 Place
11701 Luna Road
Dallas, Texas 75234 USA

Phone: (800) 800-3288
Fax: (214) 860-6060

i2 provides supply chain management solutions.

US Patent: 6,334,056

Secure gateway processing for handheld device markup language (HDML)

This patent specifies a method for secure access from a limited access data network (intranet) to handheld electronic devices which include the functionality to process alphanumeric information and process information received in handheld device markup language (HDML); the approach uses a proxy server for the necessary security services and has functionality to convert information received from the applications into HDML, so that it may be processed by the handheld device.

Issued: December 25, 2001

Inventors: Wayne Holmes and David Olander

Assignee: Qwest Communications Int'l., Inc. (Denver, CO)

Further Patent Information

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