Alcatel·Lucent

TECHNOLOGY WHITE PAPER

The Bell Labs Security Framework: Making the Case for End-to-End Wi-Fi Security

Wi-Fi technology has dramatically improved the flexibility and productivity of end users. At the same time, however, it has created serious security concerns for service providers and enterprise IT managers, risking exposure of critical data across a wide range of networks. What steps can you take to make sure that this critical data is protected?

This white paper explores the security implications of wireless LAN from the perspective of enabling service providers to prepare their enterprise customers' security in end-to-end network environments; and delivers the insights necessary to identify gaps and recommend potential solutions in the security of various Wi-Fi standards, such as 802.11i, WPA (Wi-Fi Protected Access) WPA 2, and WEP (Wired Equivalent Privacy). Additionally, this paper explores the Bell Labs Security Framework, the foundation for security architecture standards ITU-T X.805 and ISO/IEC 18028-2. This framework delivers a comprehensive methodology for assessing and upgrading end-to-end network security across the enterprise analyzing end-to-end security at each stage of a WLAN's lifecycle: design, planning, implementation, and maintenance.

Table of Contents

Wi-Fi networks can transform an enterprise, freeing end-users from ties to a desktop computing setup and allowing them to be far more productive. A truly mobile enterprise would have a significant business advantage with the flexibility to shift strategies and realign its mission with the market far faster than its competitors.

However, what's been missing from the vision of a mobile enterprise is a method to substantively evaluate the end-to-end security of Wi-Fi networks. There has been no truly satisfactory way to accurately appraise every security aspect of a Wi-Fi network and provide IT professionals with solutions that identify and correct Wi-Fi security shortfalls.

The Alcatel-Lucent Bell Labs Security Framework, which is the foundation for security architecture standards ITU-T X.805 and ISO/IEC 18028-2, offers a solution to this problem. The framework delivers a comprehensive methodology for assessing and upgrading end-to-end network security across the enterprise. Bell Labs is playing a big role in helping bring secure wireless connectivity to enterprises and government agencies with an understanding that to be truly effective, end-to-end security considerations must be evaluated and properly implemented at every stage of a network's lifecycle.

Admittedly, performing a comprehensive security evaluation is a complex undertaking. The Bell Labs Security Framework makes it possible to evaluate one of the most vulnerable aspects of a Wi-Fi infrastructure — the airlink. Furthermore, IT professionals can determine if data traveling across that link is adequately protected and, if not, what steps to take to assist in rectifying the situation.

Introduction

Despite the advantages that Wireless LANs (WLANs) bring to the enterprise, questions about wireless security have raised concern for companies considering its implementation.

In addition to the myriad vulnerabilities of conventional wired networks, wireless networks also have a host of other vulnerabilities associated with the use of radio communication and mobile clients. In fact, wireless LANs lack even the most basic protection against unauthorized access — a physical barrier. Packets are transmitted over the airlink, which makes it relatively easy to eavesdrop, intercept them, inject malicious payloads, or launch a DoS (Denial of Service) attack. Similarly, wired networks typically have some security measures in place, such as firewalls, IDS/IPS (intrusion detection/protection system), proxy servers, and content security systems to protect the end-user device (e.g. laptop) and the information. But, when a device such as a laptop computer, generally protected in a wired environment, moves to an unprotected wireless network, such as a public hotspot, the protections simply vanish.

As discussed later in this paper, most of the security vulnerabilities in Wi-Fi networks can be addressed with the available protocols and security mechanisms and a reasonably secure Wi-Fi network with an acceptable level of risk for most enterprises can be deployed. To achieve this, IT organizations need a mechanism that can analyze end-to-end security at each stage of a WLAN's lifecycle: design, planning, implementation, and maintenance. Now, a decade after WLAN technology first became generally available, they have exactly that — the Bell Labs Security Framework, which facilitates secure network design and comprehensive end-to-end security analysis.

The Bell Labs Security Framework was developed as an architectural framework for assessing and achieving end-to-end security for distributed applications. It provides the insight necessary to identify gaps and recommend potential solutions in the security of various Wi-Fi standards, such as 802.11i, WPA (Wi-Fi Protected Access) WPA 2, and WEP (Wired Equivalent Privacy).

Bell Labs Security Framework Overview

The Bell Labs Security Framework is a structured framework that drives the consideration of all possible threats and vulnerabilities that can jeopardize end-to-end network security. It fills a void in existing security standards by providing a holistic network security architecture that is applicable to end users, as well as the management and control/signaling infrastructures, services and applications.

It can be used for assessing, planning, managing and maintaining secure computer and communications networks and was designed to furnish a methodical, organized way of addressing five threats classes to networks:

- Destruction of information and/or other resources
- Corruption or modification of information
- Removal, theft, or loss of information and/or other resources
- Disclosure of information
- Interruption of services

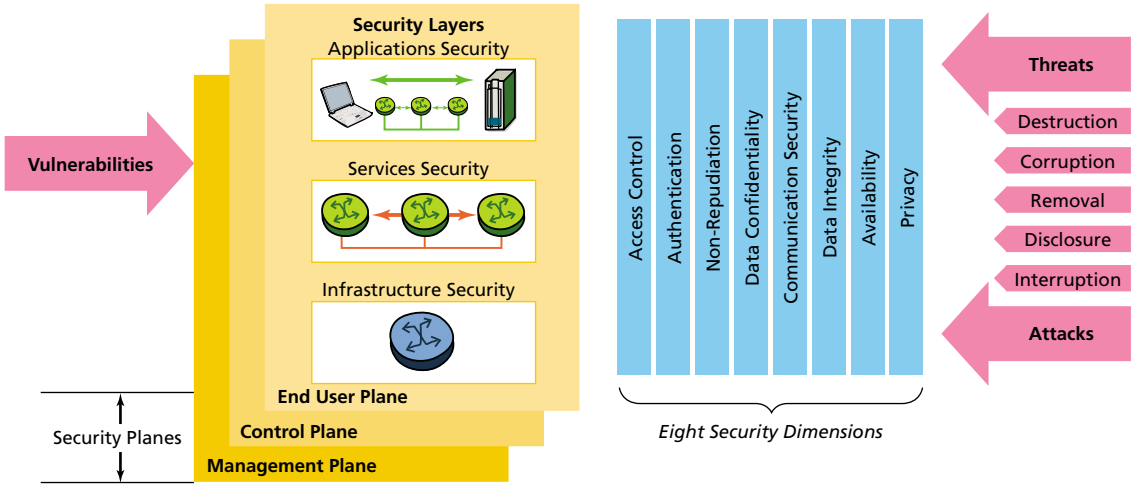
Assembling a Comprehensive Security Model

To ensure that each and every aspect of the network is covered from the security perspective, the Bell Labs Security Framework defines three layers, three planes, and eight dimensions that are used to determine if a network is vulnerable to any or all of the five threat classes listed above, and to pinpoint where such weaknesses exist (Figure 1).

The following definitions apply to the framework's layers, planes and dimensions:

- Security layers are a series of enablers for secure network solutions such as infrastructure, services and applications, each having different security vulnerabilities.
- Security planes represent the various types of network activity such as management, control and end-user.
- Security dimensions are a set of security measures to assist in countering attacks at each layer and plane.

Figure 1. The Bell Labs Security Framework



Security Layers

The Bell Labs Security Framework defines three discreet security layers as follows:

- *Infrastructure layer* – Includes the basic building blocks used to create the network, services, and applications. It comprises individual communication links and network elements, including underlying hardware and software such as access points, Wi-Fi access client.
- *Services layer* – Focuses on services that end-users receive from networks such as Wi-Fi access.
- *Applications layer* – Consists of network-based applications accessed by end-users. These applications are enabled by network services and are characterized by the end-user interacting with remote hardware or software in order to access information or perform a transaction e.g. e-mail, VPN, etc.

Security Planes

The three security planes defined by the Framework correspond to the types of activities performed over the network — management, control, and end-user activity. Some systems might implement one or more planes as a separate network, such as dedicated network for the management functions. Wi-Fi deployments typically share the same network for all three functional activities (planes). That lack of separation means that security incursions on all three planes must be dealt with simultaneously.

Security Dimensions

The eight security dimensions apply to both the security layer and the security plane extending beyond the network to include applications and end users. Each dimension represents measures implemented to counter threats and potential attacks.

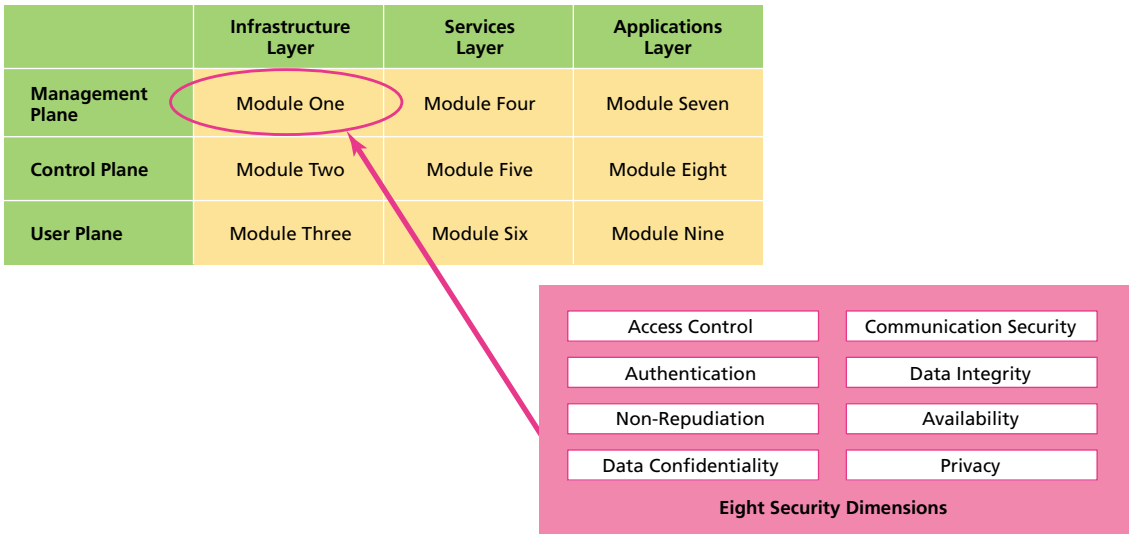
- *Access management or access control* protects against unauthorized use of network resources;
- *Authentication* confirms the identities of each entity using the network;
- *Non-repudiation* proves the origin of the data or identifies the cause of an event or action;
- *Data confidentiality* or *data security* ensures that data is not disclosed to unauthorized users;
- *Communication security* allows information to flow only between authorized endpoints;
- *Data integrity* ensures the accuracy of data so it cannot be modified, deleted, created or replicated without authorization, and also provides an indication of unauthorized attempts to change data;
- *Availability* ensures that there is no denial of authorized access to network elements, stored information, information flows, services and applications due to network-impacting events;
- *Privacy* provides for the protection of information that could be derived from the observation of network activities.

Modular Methodology

To ensure comprehensive coverage of the network being analyzed, every unique combination of security layer and security plane, each called a module (as shown in Figure 2), represents a unique perspective for consideration of the eight security dimensions. The security dimensions of different modules have different objectives and consequently comprise different comprehensive sets of security measures.

The basic methodology for analysis is to consider the threat model for each module and evaluate the effectiveness of security measures in each dimension.

Figure 2. Modular form of Bell Labs Security Framework[1]



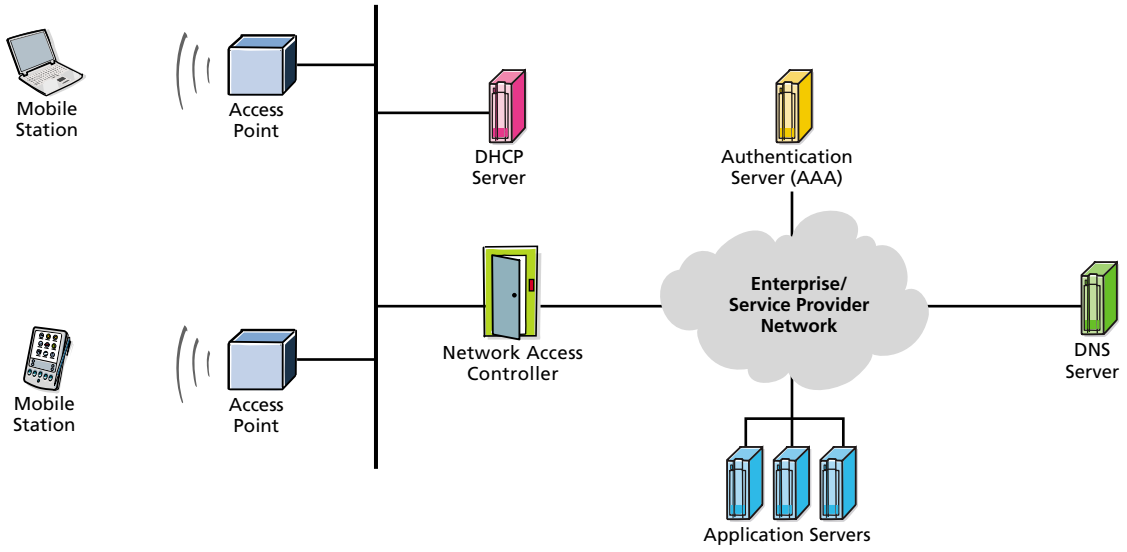
Using the Bell Labs Security Framework to Secure Wi-Fi Networks

The Bell Labs Security Framework can be effectively used for the analysis of Wi-Fi networks by assessing the security controls available in the network in each of the eight security dimensions across each intersection of the layers and planes (modules).

The Reference Architecture

The reference architecture for this assessment is based on a typical Wi-Fi network used by enterprises and hot spot service providers and includes a set of access points (AP), network access controller (NAC) and authentication server (AS) as shown in Figure 3.

Figure 3. The reference architecture



1 Modules 1-6 are included in the illustrative analysis in this paper.

The AP provides wireless access to laptops, PDAs (personal digital assistants), and other mobile stations. It also supplies these devices with information about the WLAN and responds to requests from them.

The main function of the Network Access Controller (NAC), commonly referred to as a "WLAN Gateway," is to perform or assist with user authentication and to control network access. The NAC will not permit access to the network behind it unless the mobile station has been successfully authenticated and authorized. The NAC may integrate other functions, including NAT (network address translation), DHCP (dynamic host configuration protocol) server, authentication server, and VPN server, etc.

The authentication server is critical to implementing advanced security standards such as 802.1x, WPA, and 802.11i/Robust Secure Network (RSN). It is responsible for user authentication and authorization and can optionally participate in the key management. The remaining components shown in the reference architecture are common to wireless and wired networks, and therefore are not discussed.

Scope of the Analysis

As indicated earlier, if the scope of the security analysis includes the end-to-end Wi-Fi network architecture and the entire framework is applied, vulnerabilities could be identified for every layer, plane and dimension. For the sake of simplicity, the scope of analysis in this paper is limited to wireless access only. All applications running on top of Wi-Fi access and other enabler services such as DNS, DHCP, AAA etc are excluded from the scope of the analysis.

The illustrative results shown in this paper are our assessment of the security for the typical WLAN architecture (Figure 3,) assuming no additional security controls are deployed in the network. The assessed degree of effectiveness of the security measures included in the Wi-Fi standards, across each security dimension against the framework's threat model is open to some variation depending on the exact network environment and the perception of threats.

Wi-Fi Threat Model

Every type of Wi-Fi attack could pose one or more threats, depending on intent and approach. Table 1 maps some popular Wi-Fi attacks to the threat model adopted by the Bell Labs Security Framework.

Table 1. Mapping of major Wi-Fi attacks to Bell Labs Security Framework threats

Bell Labs Security Framework-Defined Threat	Methods of Attack
Destruction of information and/or other resources	AP Intrusion
Corruption or modification of information	WEP key cracking, man-in-middle
Theft, removal, or loss of information and/or other resources	AP Intrusion, WEP key cracking, man in middle, MAC address spoofing, rogue devices, war driving, Layer 3 hijacking, ad-hoc networks
Disclosure of information	AP Intrusion, WEP key cracking, man in middle, MAC address spoofing, rogue devices, war driving, Layer 3 hijacking, ad-hoc networks
Interruption of service	RF jamming, data flooding, Layer 2 hijacking, fake AP, spoofed de-authenticate frame, FATA-Jack DoS

Wi-Fi Layers

The infrastructure layer of Wi-Fi networks consists of all components of the network, cables, interconnections and transmissions media (coverage space) e.g. access points, mobile stations, Wi-Fi gateway and servers hosting associated services like RADIUS, DNS, etc.

The service layer in the case of Wi-Fi networks is composed of wireless LAN access services and other services enabling wireless access e.g. authentication, authorization, accounting (AAA), key management services etc.

User applications running over the Wi-Fi network defines the application layer and is excluded from the scope of this analysis.

Wi-Fi Planes

Wi-Fi security standards do not address the management plane activities for the Wi-Fi networks.

Signaling and controls associated with 802.11 including RTS/CTS, fragment bursting, DRS (Dynamic Rate Shifting), DCF (Distributed Coordination Function), PCF (Point Coordination Function), PSP (Power Save Polling) defines the control plane.

The interaction of end-users with Wi-Fi networks including the transmission of data constitutes the end-user plane.

Applying Security Dimensions

In the following sections, we will assess the effectiveness or the adequacy[2] WPA2 and 802.11i have similar of the controls available in each of the eight dimensions for all applicable security features, however, WPA2 can modules in an attempt to determine the relative strengths and weaknesses interoperate with the less secure WPA , of 802.11i, WPA2[2], WPA and WEP security standards. therefore the weaknesses of WPA have a reflection on WPA2 in this analysis.

We have performed the analysis for all eight dimensions and the summary results are tabulated in Table 7, but individual details are shown only for sample dimensions in context of Wi-Fi standards. The qualitative results for each dimension are tabulated using following legends:

Access Control

Original 802.11 specifications, including WEP, had no built-in access control mechanism thus larger Wi-Fi deployments used a WLAN gateway for service level access control. Based on this assumption, access control for the Wi-Fi service to the end-users has been rated as partially adequate.

802.1x is the end-user access control mechanism for Wi-Fi service for 802.11i, WPA, and WPA2.

Table 2. Wi-Fi Security standards coverage for Access Control Dimension

Access Control Security Dimension								
Security Planes	**Security Layers**							
	Infrastructure				**Services**			
	802.11i	WPA2	WPA	WEP	802.11i	WPA2	WPA	WEP
End-User	✓	✓	✓	X	✓	✓	✓	P
Control	✓	X	X	X	✓	✓	✓	X
Management	X	X	X	X	X	X	X	X

✓	Satisfactory Compliance
P	Partial Compliance
X	Not addressed by the standard

2 WPA2 and 802.11i have similar security features, however, WPA2 can interoperate with the less secure WPA, therefore the weaknesses of WPA have a reflection on WPA2 in this analysis.

Authentication

802.11i, WPA2, and WPA use 802.1x/EAP for authentication. In contrast, WEP employs either "open" or "shared secret" authentication, which uses the same static key used for encryption. Thus, WEP authentication is rated "partial." Authentication in other standards could also receive the same rating if a weak EAP protocol like MD5 is selected for 802.1x.

Authentication of control information across access points and other network elements (to support roaming) is only addressed in 802.11i. APs supporting other standards normally use proprietary mechanisms to exchange this information while roaming and validating the security of such implementations is out of the scope.

Table 3. Wi-Fi security standards coverage for Authentication Dimension

Authentication Control Security Dimension								
Security Planes	**Security Layers**							
	Infrastructure				**Services**			
	802.11i	WPA2	WPA	WEP	802.11i	WPA2	WPA	WEP
End-User	✓	✓	✓	P	✓	✓	✓	P
Control	✓	X	X	X	✓	✓	✓	X
Management	X	X	X	X	X	X	X	X

✓	Satisfactory Compliance
P	Partial Compliance
X	Not addressed by the standard

Data Confidentiality

WEP employs RC4 encryption for end-user data, but the implementation is very weak (24-bit initialization vector). WPA also uses RC4, but implements a 48-bit initialization vector and other strong-security mechanisms. 802.11i and WPA2 support AES (Advanced Encryption Standards), which offers the strongest encryption.

Since WEP does not define how control information is stored in network elements, some Windows-based mobile stations store the WEP key in the registry, which can be read remotely unless precautions are taken. Similarly, some Wi-Fi card manufacturers store the WEP key in firmware — if the card is lost or not disposed of properly, this can constitute a security risk.

The other standards support key management features that automatically generate critical keys, rather than manually. Additionally, WPA and WPA2 have the option of using Pre-shared Secrets Keys (PSK).

These standards only define the wireless interface. End-user data may appear unencrypted on the Ethernet ports, depending on the network architecture or the status of port mirroring.

Table 4. Wi-Fi Security standards coverage for Data Confidentiality Dimension

Data Confidentiality Security Dimension								
Security Planes	**Security Layers**							
	Infrastructure				**Services**			
	802.11i	WPA2	WPA	WEP	802.11i	WPA2	WPA	WEP
End-User	P	P	P	X	P	P	P	X
Control	✓	P	P	X	✓	P	P	X
Management	X	X	X	X	X	X	X	X

✓	Satisfactory Compliance
P	Partial Compliance
X	Not addressed by the standard

Data Integrity

WEP is relatively weak when it comes to protecting the integrity of end-user data because it both uses CRC32 (cyclic redundancy check 32) as its integrity check vector (ICV) and concatenates the predictable ICV to the wireless frame, making it easier to insert malicious frames. WEP doesn't protect the integrity of control (header) data.

WPA uses 'Michael' with key mixing both for end-user data and header to deliver stronger integrity protection. 802.11i employs CBC-MAC both for data and header integrity protection.

Table 5. Wi-Fi security standards coverage for Data Integrity Dimension

Data Integrity Security Dimension								
Security Planes	**Security Layers**							
	Infrastructure				**Services**			
	802.11i	WPA2	WPA	WEP	802.11i	WPA2	WPA	WEP
End-User	✓	✓	✓	P	✓	✓	✓	P
Control	✓	✓	✓	X	✓	✓	✓	X
Management	X	X	X	X	X	X	X	X

✓	Satisfactory Compliance
P	Partial Compliance
X	Not addressed by the standard

Availability

DoS attacks like RF Jamming, data flooding, and Layer 2 session hijacking, are all attack against availability. None of the Wi-Fi security standards can prevent attacks on the physical layer simply because they operate on Layer 2 and above. Similarly, none of the standards can deal with an AP failure.

Table 6. Wi-Fi security standards coverage for Availability Dimension

Availability Security Dimension								
Security Planes	**Security Layers**							
	Infrastructure				**Services**			
	802.11i	WPA2	WPA	WEP	802.11i	WPA2	WPA	WEP
End-User	P	P	P	X	P	P	P	X
Control	P	P	P	X	P	P	P	X
Management	X	X	X	X	X	X	X	X

✓	Satisfactory Compliance
P	Partial Compliance
X	Not addressed by the standard

Analysis Summary

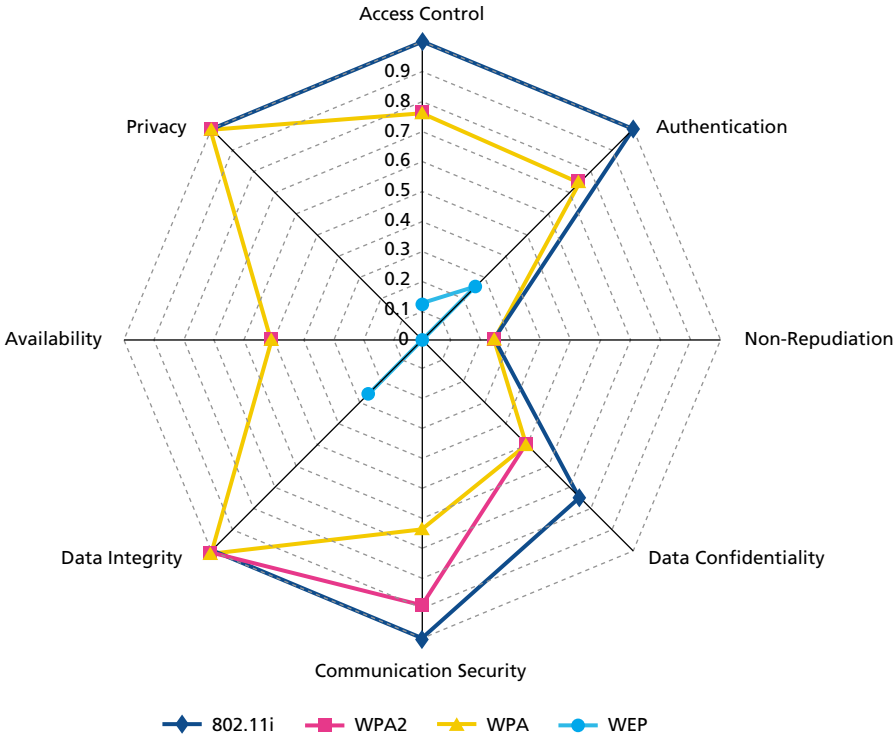
The foregoing assessments demonstrate how Bell Labs Security Framework can be used to evaluate the security of Wi-Fi security standards. Armed with this information, enterprise IT managers can determine where security is less than adequate, which protocols are most vulnerable, and which do the best job. The next step is to bring security up to specification across the entire Wi-Fi network. Results in Table 7 illustrate relative security scores of the four Wi-Fi standards derived from the rigorous application of Bell Labs Security Framework for security assessment.

Table 7. Relative security score for Wi-Fi standards[3]

WiFi Protocol Standards Security Comparison and Comprehensiveness per Bell Labs Security Framework			
WiFi Standards	**Covered**	**Partially Covered**	**Not Covered**
802.11i	22	8	0
WPA2	17	11	2
WPA	15	13	2
WEP	0	5	25

3 The table includes the assessment for all the eight dimensions, though the individual details are shown only sample Dimensions in the paper.

Figure 4. Relative security provided in each Dimension by Wi-Fi standards



The data shown is generated by Bell Laboratories security technology

Assigning a weighted value that reflects how successfully the standard addressed each dimension as shown in Figure 4, can create a more accurate picture of the security provided by these Wi-Fi standards and identifies the areas where the supplementary security measures are required to achieve the desired security posture. It quickly becomes evident that WEP is the least secure standard not adequately addressing many of the dimensions. In fact, the Bell Labs Security Framework analysis reveals that WEP security is inadequate for the enterprise or for service provider networks.

In contrast, 802.11i is demonstrably more secure than prior versions, delivering good coverage for all security dimensions. Still, there is room for improvement, particularly when it comes to availability and non-repudiation. WPA2, meanwhile, offers marginally less security partially due to accommodating the need to interoperate with its less secure predecessor considering that security is only as good as the weakest link.

Recommendations

It is apparent that relatively secure Wi-Fi networks can be designed, implemented, and maintained using either 802.11i or WPA2. Simply implementing these standards, however, will not ensure end-to-end security for WLANs. In fact, it could leave major security gaps for availability and non-repudiation.

What's more, neither of these Wi-Fi security standards addresses the management plane. Thus, additional security would have to be incorporated in the design, planning, and operation of these networks. For example, redundant access points and pre-authenticated roaming are needed to ensure high availability. The architecture and configuration selected for the wireless network must account for these shortfalls. In addition, wireless networks are part of larger wired network and end-to-end security must address the security of the associated wired network as well.

Centrally managed thin access points that can communicate with one another help secure information related to roaming clients and will improve the availability by dynamically adjusting the RF power level. Operational security measures such as site surveillance, as well as planning the Wi-Fi RF coverage area, can also improve availability by reducing the risk of attacks like RF jamming.

Applying the Bell Labs Security Framework at each stage of the network lifecycle can ensure that all aspects of the network are evaluated for all applicable threats to achieve an end-to-end secure Wi-Fi network.

Keep in mind that the scope of this paper addressed only the security assessment for the Wi-Fi airlink. However, the use of Bell Labs Security Framework could be extended to design and evaluate the security of your entire network, which is clearly a demanding task even with the requisite on -site staff resources. An undertaking such as this requires skill and expertise both in Bell Labs Security Framework and the networking domain. Alcatel-Lucent is the partner who is ready to help you leverage the Bell Labs Security Framework and ensure that your networks are designed, deployed and managed with the highest standards of security.

For More Information

Sources

International Telecommunications Union, Telecommunications Standardization Sector, "Security Architecture for Systems Providing End-to-End Communications," Rec. BELL LABS SECURITY FRAMEWORK, 2003, http://www.itu.int

International Telecommunications Union, Telecommunications Standardization Sector, "Security in Telecommunications and Information Technology," pg 1, December 2003, http://www.itu.int

International Telecommunications Union, Telecommunications Standardization Sector, "Security Architecture for Open Systems Interconnection (OSI) for CCITT Applications," Rec. X.800, 1991, http://www.itu.int

ANSI/IEEE Std 802.11, 1999 Edition (R2003) – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

IEEE Std 802.11i 2004 – Amendment 6: Medium Access Control (MAC) Security Enhancements.

Wi-Fi Protected Access An overview
http://www.Wi-Fi.com/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf

Department of Defense Directive number 8100.2 - Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG);
http://www.dtic.mil/whs/directives/corres/html2/d81002x.htm

NIST SP800-48: Wireless Network Security – 802.11, Bluetooth and Handheld Devices;
http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

About the Authors

Ashok Gupta

Technology and Applications Research Group of Bell Labs. He has over twenty years of diverse experience in the field of enterprise IT Infrastructure, security, wireless, content delivery and MIS applications with various research organizations. His current areas of interest are end-point policy enforcement, and security of mobile devices and wireless networks. Some of the certifications he holds are CISSP, CWSP, PMP and CWNA.

Theresa Buthmann

Theresa Buthmann is the director of Wireless Solutions for Alcatel-Lucent Services. She leads the development of robust wireless solutions that balance the gains of productivity with concerns around security, quality of service, and cost. Buthmann applies the knowledge gained from holding several diverse positions within AT&T and Lucent Technologies in the CFO, marketing, and business development organizations to enable multiple facets of the wireless solutions business across many technologies including optical transport, VoIP, Wi-Fi, in-building optimization, and mobile IP.