Design of a Network Security Testing Environment

T. Andrew Yang (yang@cl.uh.edu)

1 Overview

The primary objective of designing a high-speed networking environment is to build a set of interconnected networks on which vulnerabilities of a corporate network can be analyzed and effectiveness of security mechanisms can be evaluated. A typical corporate network is composed of servers which provide services to users. Whether the services are data bases, computer applications, or web pages, they are resources critical to the successful operations of the corporation. Before deploying a control mechanism in a corporate network to guard against potential threats, the pros and cons of the mechanism must be evaluated. The networking environment that we propose to build will provide an environment for researchers to evaluate vulnerabilities and to test solutions.

The resources in a corporate network may be accessed by various users via a variety of access methods. Many existing networks are being upgraded from a 10/100 Mbps network (10/100Base-T) to a Gigabit high-speed network (1000Base-SX). This fact implies that new security threats may be introduced due to the increased speed, and existing security controls may not be able to properly address those threats. The proposed testing environment will allow researchers to evaluate network security products (hardware, software, and combination of both) in a realistic inter-networking system, which is composed of a high-speed networking lab, a wired remote LAN, a wireless LAN, and mobile devices connecting to mobile service. To prevent any potential negative impact that the testing environment may have on production networks, the testing environment will not be connected to any existing networks, such as the university campus network. Instead, a dedicated digital subscriber line (DSL) will provide Internet connectivity to the testing environment.

Before describing the configuration of a secure high-speed networking environment, I will first examine the various access paths through which resource in such a system may be accessed, and a set of *vulnerability points* (VPs) associated with the access paths. The design of a corporate network to address potential threats, represented by the VPs, will be presented later. The report is concluded with a listing of equipments to purchase and an overview of the installation plan.

2 Access to a High-Speed Corporate Network

Figure 1 shows how a high-speed network may be accessed by users via a variety of access paths. A user may access the network resources by using a computer that is part of the network, by using a computer that belongs to a remote network (such as one in another department), by using a local wireless device, by using an Internet connection from home, or by using a mobile device on the road. In order to identify potential threats to the security of a network, it is critical to understand the probable access paths to the network. The *vulnerability points* (VPs) of a network is related to how those access paths would be used.

2-A. Vulnerability Points

A *vulnerability point* represents a point in a network where an attack may be launched against the network. A set of VPs that are typical in a network system have been identified. The VPs are marked in Figure 1 as VPs from A through G.

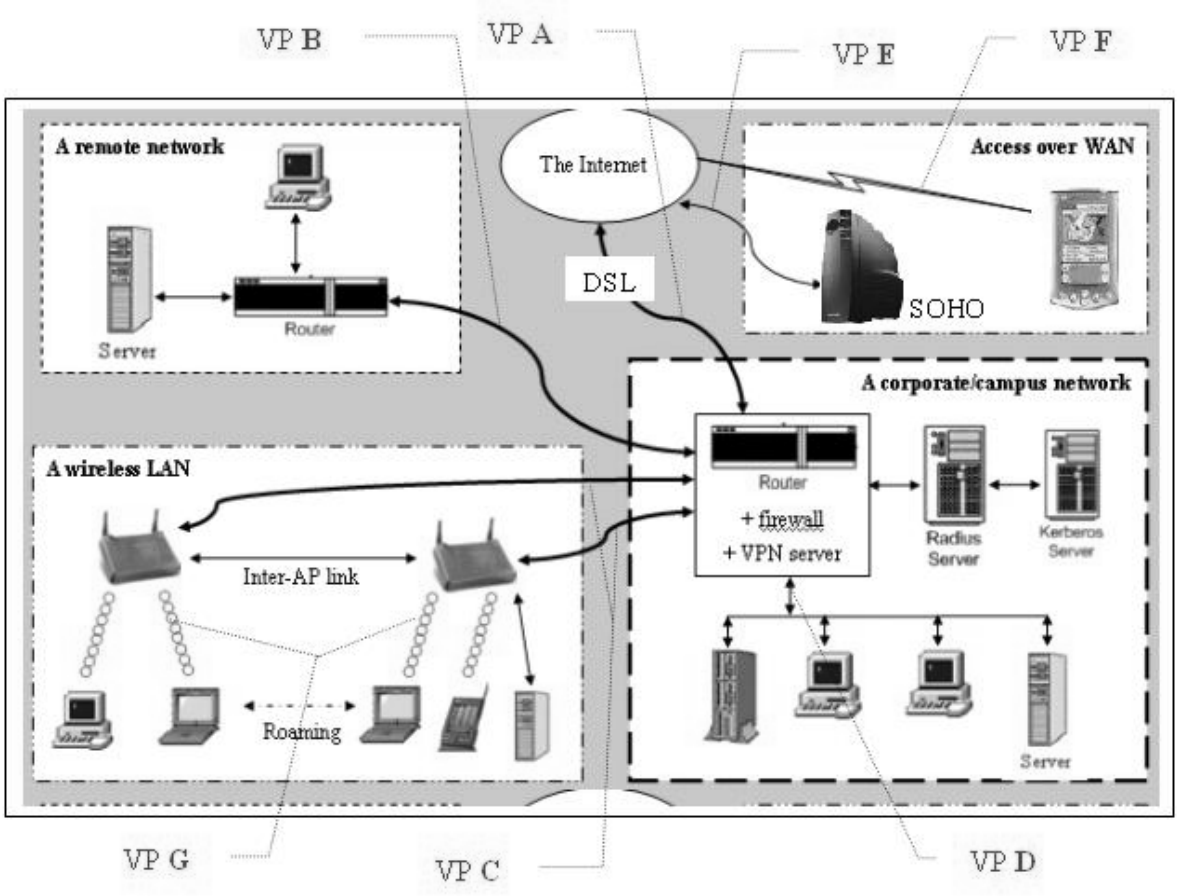

Figure 1. A High-Speed Networking Environment

Some of the VPs (A, B, C, D) correspond to direct attacks at the corporate network. The others are indirect attacks at small offices or home offices (E), at wireless mobile networks (F), or at wireless LANs (G). An indirect attack may eventually become a threat to the corporate network. An attacker, for example, may take over a telecommuter's identification by attacking his/her home office and then use the exposed user information to access the corporate network. A drive-by hacker, as another example, may connect to an insecure wireless access point and then gain access to the corporate network via the access point.

- VP-A represents attacks coming from a public network, such as the Internet. Employees may use a dialup line, a subscribed ISP service, or a mobile device/service to access the corporate network from the public network.

- VP-B represents attacks launched from a remote network, which may be a network in another department of the same corporation.

- VP-C represents attacks from a wireless LAN. Special authentications such as LEAP and RADIUS are required to guarantee the wireless LAN to be safe.

- VP-D represents attacks that may be launched from within the corporate network. This type of attacks include deliberate attacks by employees as well as involuntary attacks which may be launched by, for example, an ignorant employee opening an email with a subject line that says "I love u".

- VP-E represents attacks targeted at small offices or home offices (SOHO), where an employee uses a dial-up line or cable modem to connect to the corporate network.

- VP-F is the type of attacks taking advantage of a mobile network, in which data are transmitted through the air. Mobile networking plays a significant role in the realization of *pervasive computing*, which would allow users to have access to network resource from anywhere at any time using small devices such as a cellular phone or a PDA. The growing use of mobile services, however, implies increasing attacks associated with mobile networks.

- VP-G is similar to F in the sense that data in a wireless local area network (WLAN) also travel in the air. Communications occur between a wireless client and an access point, which serves as a bridge between the client and the backend network. Recent news stories have revealed the vulnerability of the IEEE 802.11b protocol, which is the network protocol built into WLAN cards. The encryption method used in the 802.11b protocol is the WEP (Wired Equivalency Protocol), which is vulnerable to attacks, unless other methods (such as LEAP and RADIUS) are integrated to achieve a secure solution.

2-B. Classification of Use Cases

Access Context / User status	**Within the local network**	**From a remote (wired) network**	**From a local wireless network**	**Over the Internet**	**Over a wide-area mobile network**
Employees	a. Local internal users k. Internal hackers	b. Remote internal users k. Internal hackers	c. Local wireless users k. Internal hackers	d. Tele-commuters k. Internal hackers	e. Mobile users k. Internal hackers
Non-employees (ordinary users or hackers)	h. Physical security threat	h. Physical security threat	i. Drive-by hackers	f. External users j. External hackers	g. Mobile external users j. External hackers

Table 1. Users versus Access Contexts

At the highest level, users can be classified into employees and non-employees. The problem with this type of classification is that it does not take into account the fact that employees may become hackers while non-employees may have legitimate uses of network resources (such as Web surfing or anonymous ftp). Alternatively and more practically, users may be classified into legitimate and illegitimate users. Legitimacy is determined by the user's status (employees or non-employees[1]) and the context in which the access occurs. There exist a set of five access contexts: (i) within the local network, (ii) from a remote wired network, (iii) from a local wireless network, (iv) over the Internet, and (v) over a mobile network. The "intersection" of user status and access contexts results in seven legitimate use cases and four illegitimate use cases, which are listed in Table 1 and to be explained below. Illegitimate cases are underlined in the table.

- **Legitimate Use Cases**

Case a. Local internal users are users of computers belonging to the local corporate network.

Case b. Remote internal users are employees who access the network from a wired remote network. An example is an employee belonging to department A accessing department B's local network from department A.

Case c. Local wireless users are users who access the network resources via a wireless LAN client device, which is a computer or a PDA with a WLAN adapter that supports IEEE 802.11b or 802.11a protocols. A WLAN access point provides a wireless client connection to a backend network. The typically range of coverage of an access point is between 100 ft (indoor use) and 300 ft. Special security controls are required to guarantee secure communications between wireless devices and the wireless access points and between the wireless access point and the backend network.

Case d. Telecommuters represent the group of employees who access the corporate network from a remote location, whether a home office or a remote branch office. The access paths in general pass through a public network such as the Internet. The unique security concern facing this group of users is how to guarantee secure transmissions across a public network, without exposing sensitive information along the way.

Case e. Mobile users are users who access the corporate network by using a mobile device, such as a cellular phone or a PDA with a mobile PC card. Wireless WAN provides mobile Internet services, which allow users to access the Internet from virtually anywhere. The coverage of a mobile service is national or even global. The speed of current mobile wireless communication (2G or 2.5G) is only close to that of a 56Kbps dial-up modem, but the new 3G (Third Generation) mobile technologies, such as CDMA 2000, promise mobile speeds of 384 kbps and up to 2 Mbps in a fixed or stationary wireless environment.

[1] Alternatively, instead of a two level classification, user status can be further refined by considering levels of security clearance, such as those adopted in military facilities. At the operating system level, user authorizations are in general managed via the use of *access control list (ACL)*, which works together with user authentication and system security policy to grant a user certain access privileges to a system resource.

Case f. External users are non-employees who access the corporation's resources, such as a web site or FTP site, via the Internet.

Case g. Mobile external users are non-employees who use a mobile device to gain access to network services provided by the corporation.

- **Illegitimate Use Cases**

Case h. The two instances of case *h* represent physical security threats when unauthorized external users are present inside the facility to use a local computer.

Case i. Another form of physical security threat may appear in the form of wireless access. An external user may use a wi-fi (WLAN) device to access an insecure access point, through which access to the internal networks may be obtained.

Case j represents the situation when a hacker attacks the network via the Internet.

Case k represents the "ultimate" security threat to a corporate network. An employee may become a hacker, who would launch attacks from within the network. Being an employee, an *internal hacker* has convenient access to the internal network, whether locally, remotely, or via the Internet. An employee may become an *involuntary hacker* when he opens an email attachment that contains a virus or downloads an infected file from a web site. It was reported by several sources, including the draft of *National Strategy to Secure Cyberspace* recently announced by the White House, about 70% of security breaches are attributable to internal users[2].

3 Configuration of a Network Security Testing Environment

A high-level configuration of the network security testing environment is illustrated in Figure 1. Figure 2 shows possible configuration of a protected corporate network. The incoming traffic to the network passes through the router, which directs traffic to either a DMZ (Demilitarized Zone) or to the firewall. DMZ usually consists of computer servers that need to be directly accessible from the world outside the corporate net, such as a corporate web server or an anonymous FTP site offered as services to the public. All other traffic must first be filtered by a firewall, which protects the rest of the network from potential attacks.

[2] 'Approximately 70 percent of all cyber attacks on enterprise systems are believed to be perpetrated by trusted "insiders".' – Page 21, *The National Strategy to Secure Cyberspace (Draft for comment)*, September 2002. Available at http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf.

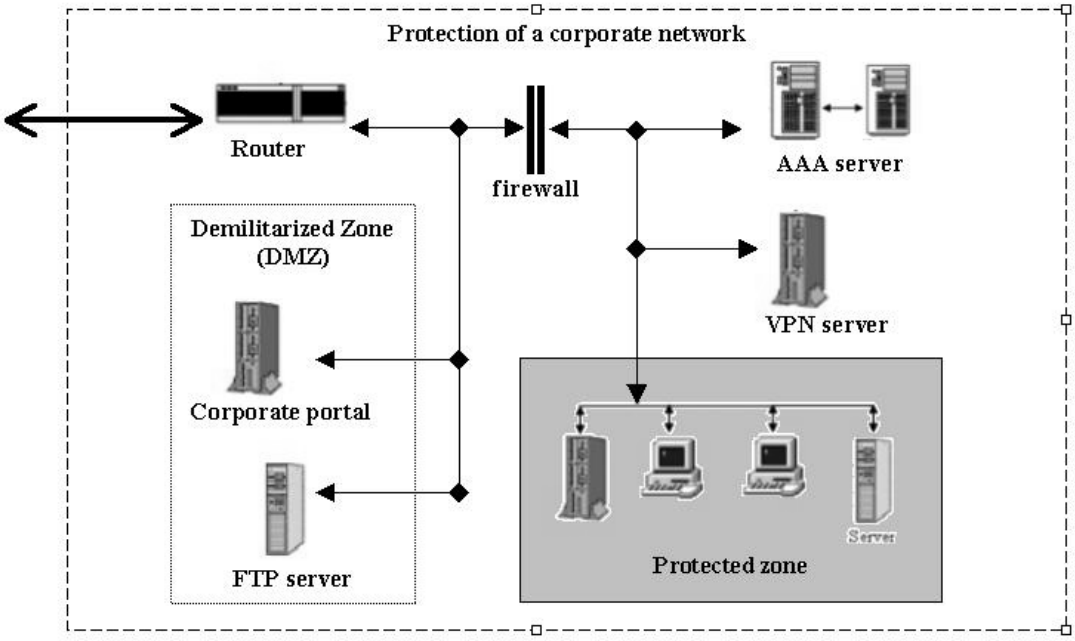

Figure 2. Configuration of a protected corporate network

In order to provide controls guarding the vulnerability points against attacks, the significance and potential impacts of the following technology need to be carefully examined.

- **AAA** (Authentication, Authorization and Accounting) server: An AAA server, such as Interlink Network's RAD-Series Server and Cisco's Access Control Server (ACS), implements the *Remote Authentication Dial In User Service* (RADIUS) protocol (see [RFC2865]) to authenticate a remote user trying to access a corporate network.

- **VPN** (*Virtual Private Network*) server**:** A VPN server works with a user's VPN client to establish a *tunnel* between the user and the backend network. The tunnel provides encrypted two-way communication through a publicly accessible networking environment, such as the Internet or a wireless local area network. VPN is considered as the *de facto* method for providing remote users secure access to the corporate intranet.

  VPN technology is usually used together with one or several VPN-related protocols, such as IP Security data encryption (*IPSec*, see [RFC2401]), *Point-to-Point Tunneling Protocol (PPTP), Virtual Private Dialup Network (VPDN), Layer 2 Tunneling Protocol (L2TP), PPP over Ethernet (PPPoE),* or *Multiprotocol Label Switching (MPLS).* Introduction to these technologies are available at [Cisco VPN].

- **LEAP:** *Lightweight Extensible Authentication Protocol* is Cisco's extension to the *Extensible Authentication Protocol* (EAP, see [RFC2284]). Many wireless LAN adapters support EAP and LEAP, in addition to *WEP (Wired Equivalent Privacy*), which is the encryption method built in to the IEEE 802.11b and 802.11a protocols. LEAP ensures mutual authentication between a wireless client and a back end RADIUS server. Communication between the access point and the RADIUS server is via a secure channel. This eliminates "man-in-the-middle attacks" by rogue access points (see [Cisco Aironet]).

- **EAPOL:** *Extensible Authentication Protocol (EAP) over LANs* (EAPOL) is defined in IEEE 802.1x standard (see [IEEE 2000]). EAPOL is an extension of EAP. In addition to encapsulating EAP packets transmitted between a wireless client and an access point, the 802.1X standard also defines EAPOL messages that convey the shared key information critical for wireless security. See [Goransson 2002] for an introduction to the protocol and its application toward wireless security.

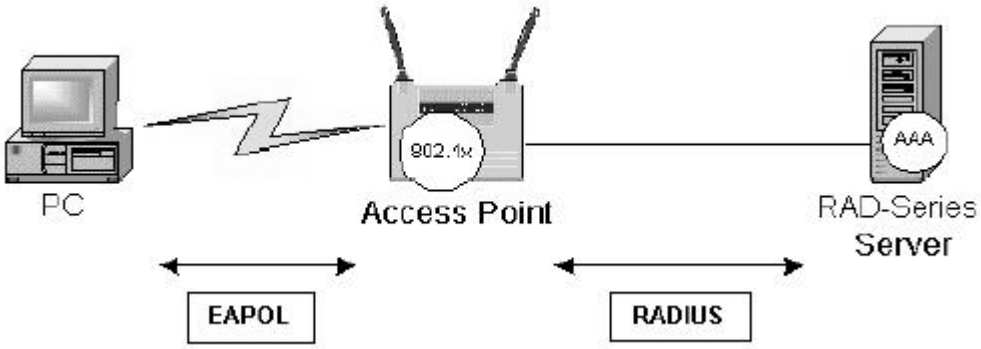

Figure 3. Two-level User Authentication in a WLAN

(from http://www.interlinknetworks.com/images/resource/wireless_lan_security.PDF)

The two-level authentication role played by a wireless access point is illustrated in Figure 3, which was originally published at Interlink Networks' web site as part of a white paper.

For more information regarding the protocols and their application to wireless security, please refer to [IEEE 2000], [Goransson 2002], [RFC2284], [RFC2865], and [Interlink RAD].

4 Purchasing and Installation of Equipments

4-A. The corporate network

	Qty	Alternatives and estimated cost	Installation location(s)
1. AAA server (for user authentication, authorization, and accounting)	1	• Cisco Access Control Server (ACS) 3.0 for Windows 2000 and NT: $6,000 (before academic discount) • Interlink Networks RAD-E for Linux: $5,400 (after academic discount) • LeapPoint AiroPoint 3600 Security Server (a hardware solution; supports up to 200 users): $3,500	D155
2. Firewall (for filtering	1	• Cisco Secure PIX Firewall 506: ~ $2,000.	D155

incoming packets)		$2,000. • SonicWALL PRO: See the VPN section.	
3. A VPN server (for remote access to corporate applications)	1	• Cisco VPN 3005 Concentrator, for unlimited users, $4,000. • Microsoft Advanced Server, for 25 users, $3,999 list; Server, for 5 users, $999. • NetMAX VPN Server: $499 • Novell Inc. For 10 users, $400 list. • RedCreek Ravlin 5300 & 3300 With Node Manager: 5300, $4,000 list; 3300, $1,500; RedCreek Node Manager, $1,000 (client licenses for 100 users, $2,000). • SonicWall Pro-VX, for 50 users, $4,995 list; XPRS2, for unlimited users, $1,795.	D155
4. Upgrades of the 10/100Mbps Ethernet cards to Gigabit cards (for computers in D155)	10 (?)	• Cisco gigabit network adapters: ~2,000 ($200 X 10) • Linksys EG1064 64-Bit Instant Gigabit Network Adapter: $92 (Amazon.com price)	D155
5. A new Gigabit router for D155	1	• Cisco router: ~ $3,000 (?)	D155 (or D118)
6. Two new PCs to install the server software listed in items 1, 2, and 3 above	2	• $3,000 ($1,500 X 2) • Alternatively the server software may be installed on the existing computers in D155	D155
7. Intrusion detection software (IDS)	1	• ?	
8. DSL subscription to provide		• ~ $300 per month	

Internet connection to the test bed (without going through the UHCL campus network)			
Estimated subtotal:		**$20,000 (Cisco approach) + monthly DSL subscription**	

Table 2. Set-up of the corporate network test bed

4-B. The wireless local network

	Qty	Alternatives and estimated cost	Installation location(s)
1. A wireless access point that support both 802.11b and 802.11a protocols.	2	• Cisco 350 AP: ~ $600 • The access point will form a wireless LAN with the existing AP in D155. The wireless LAN may contain wired connection to local servers. The wireless LAN connects to the router of the corporate net through possibly an Ethernet cable.	D128
2. A laptop with a wi-fi adapter (802.11a)	1	• Dell Inspiron: ~ $2,500 • The laptop will be used to serve as a roaming client. The same laptop, when equipped with a mobile network adapter (see C.1 below), may be used as a mobile client, which access the network via a mobile wide-area communication network.	
3. Blue Socket wireless network switch	1	• ~ $6,000 • The switch provides bandwidth control and interface with a RADIUS server for user authentication.	D128 or D155

Estimated subtotal:	• **$9,100 (with blue socket switch)** • **$3,100 (without blue socket switch)**

Table 3. Set-up of the wireless network test bed

4-C. The mobile network

	Qty	Alternatives and estimated cost
1. A mobile network PC card	1	• Sierra Aircard 550: ~ $1,250 • The mobile card is to be used with the laptop listed in B.2 to allow access to WWAN.
2. Subscription to mobile service	annual	• Go.America: ~ $550 • Sprint PCS: ~ $550
Estimated subtotal:		**$1,800**

Table 4. Set-up of the mobile network test bed

The total estimated cost for setting up the network security testing environment is $24,900 without Blue Socket switch, or $30,900 with Blue Socket switch.

5 Acknowledgement

The author would like to thank those who have contributed information and their comments to this report. Murtaza Doctor has provided most of the quoted prices in the tables.

6 References

[Cisco Aironet] *Cisco Aironet Security Solution Provides Dynamic WEP to Address Researchers' Concerns*. A Cisco white paper. Available at http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1281_pp.htm.

[Cisco VPN] *Which VPN Solution is Right for You?* A Cisco white paper. Available at http://www.cisco.com/warp/public/707/which_vpn.html.

[Goransson 2002] Paul Goransson. *"802.1X provides user authentication"*. *Network World*. 03/25/02. Available at http://www.nwfusion.com/news/tech/2002/0325tech.html.

[IEEE 2000] *IEEE 802.11 Security and 802.1X*. By Dan Simon, Bernard Aboba, and Tim Moore. March 2000. Available at http://www.ieee802.org/1/mirror/8021/docs2000/8021xSecurity.PDF.

[Interlink RAD] *Wireless LAN Security using Interlink Networks RADSeries AAA Server and Cisco EAP-LEAP*. A white paper by Interlink Networks. Available at http://www.interlinknetworks.com/images/resource/wireless_lan_security.PDF.

[RFC2284] *PPP Extensible Authentication Protocol (EAP).* Part of the Internet Standard. By L. Blunk, and J. Vollbrecht. March 1998. Available at ftp://ftp.isi.edu/in-notes/rfc2284.txt.

[RFC2401] *Security Architecture for the Internet Protocol (IPSec).* By S. Kent, and R. Atkinson. Nov. 1998. Available at ftp://ftp.isi.edu/in-notes/rfc2401.txt.

[RFC2865] *Remote Authentication Dial In User Service (RADIUS).* By C. Rigney, S. Willens, A. Rubens, and W. Simpson. June 2000. Available at ftp://ftp.isi.edu/in-notes/rfc2865.txt.