Chapter 2

Vulnerabilities in the Organization

Cyberspace is the infrastructure of the modern world, and Cybersecurity is the infrastructure of Cyberspace.

Introduction

Internet presence has become a prerequisite for the operation of any organization, whether it is a government agency, a business activity, or an academic institution. Every organization needs an *open door* to the public, with the ability to serve its constituency online and the capacity to securely hold data. The Internet presents unprecedented opportunities for practically every organization. However, along come unprecedented dangers that may lead to costly, often irreversible, damage.

Let us consider the cost of the *one penny intrusion*. The story goes that in a certain bank the online system was compromised, and one penny was removed from an account. Let us see how much that penny will cost the bank. Following the discovery of the account compromise, an emergency meeting of twenty executives was called which lasted for four hours. A decision was made to reconcile all of the bank's 250,000 accounts based on the previous day's records. This activity would require two full days of the bank's five member IT department. A public relations campaign was authorized, via several media, to hopefully offset any negative publicity. Undoubtedly, the cost of the *one penny intrusion* ended up as far more than the one penny loss.

Organizational operations are not physically performed and monitored anymore, but are done electronically via shared databases and via intranets, extranets, and the Internet. That is, we operate based on the perception of reality and not with reality itself. A bank manager looks at the screen to see the financial standing of the bank and does not count the bills and the coins that are in the hundreds of the bank's locations.

While the convenience, efficiency, and effectiveness provided by the information systems are of unprecedented magnitude, similarly are the accompanying dangers. As a result, it is imperative that organizational security measures must match the ever-increasing threats. In the case of a security breach in an information system, the most important security measure is the real-time detection, notification, and instant countermeasure.

A certain white paper states: "The business . . . needs to detect attacks or vulnerabilities instantaneously and provide effective solutions."* Therefore, incident detection is the cornerstone in any security plan—a plan that is supported by the design of a secure system that provides an incident analysis and a vulnerability repair procedure.

Common Organizational Vulnerabilities

In the definition of an organizational information system, each and every functional requirement needs to have an accompanying security component addressing external as well internal possible attacks. According to statistics, the most successful cyber attacks are of the *hybrid* nature. An insider, knowledgeable of a vulnerability, helps an outsider to successfully bypass the system security and access the organization's resources.

In information system design and implementation, besides the expected nominal performance, security functions need be added that will prevent the creation of vulnerabilities. Most vulnerabilities arise from one or more of the following:

Data Backup: Backing up data in intervals that are incompatible with systems operations speed. It is the CIO's decision whether data be backed up every hour, minute, second, or millisecond. The frequency of moving data from the soft backup storage to the hard archival media has to be carefully selected. Also, decisions need to be made as to the permanency of data and their accessing policy. Deletion of unnecessary data can be very important because

* Internet Security and Business, Part One, http://www.backupdirect.net/internet-security-and-business-part-one.

it may be under compliance regulations. The dependence of postintrusion analyses on backed-up data is absolute, because the access trail of archived data* can provide valuable information.

Operational Buffer Overflow: Every piece of data entry or entry request is temporarily stored in a buffer while being serviced. Easy software design calls for a fixed-size buffer of a guesstimated size. Whatever the size, the buffer may fill, making the particular function inoperable or inaccessible. Security-minded software design calls for a dynamic size buffer that may endlessly extend itself into the vast available disk storage. Attackers would overflow targeted buffers, usually resulting in data or code overwriting. It is possible that attackers may install malware that a *naive* buffer may pass for executable code with disastrous consequences.

Operational Speed Saturation: Endless and persistent requests, though simple, may exceed the computational limits of the system and virtually incapacitate external communications with bona fide users. Again, security-minded software design calls for provisions to ignore or block persistent requests of common origin.

Access Authorization and Authentication

Authorization codes and processes are often vulnerable for a variety of reasons. The most common are

- System allows the user endless password entry attempts. In this case, the attacker automates the attack, using a password generator that in a matter of time discovers the correct password.
- System does not allow the user many password entry attempts, and the user writes the password in possibly vulnerable places.
- System demands password change at frequent intervals, creating inconvenience to the user, and user makes minimal changes, with each change adding vulnerability.

Present authentication technologies include the following four *factors,* also illustrated in Figure 2.1a–d:

- Something the user knows (e.g., password, PIN)
- Something the user has (e.g., ATM card, smart card, USB device)
- Something the user is (e.g., biometric characteristic, such as a fingerprint) [1]

* Archived Data: Data that are not being used anymore at the operational level of the organization, but contain valuable information that may assist in postintrusion analyses.

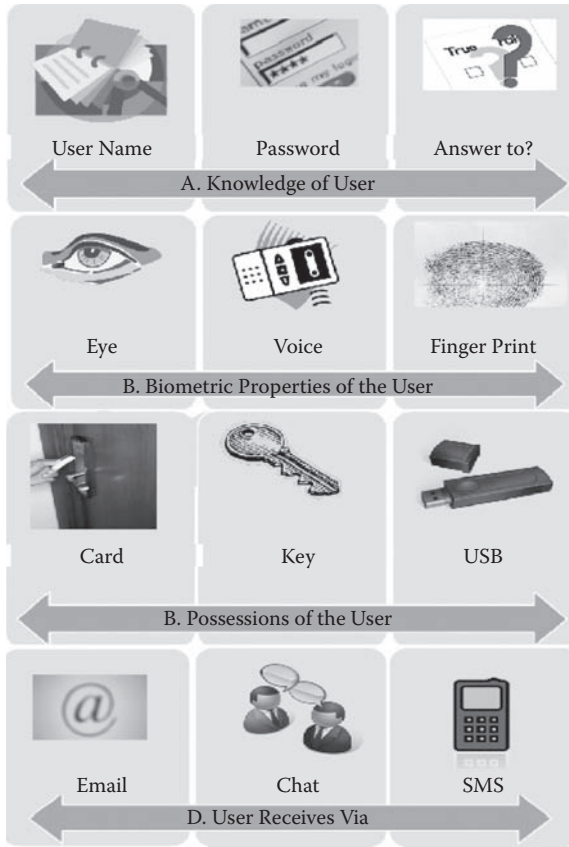

Figure 2.1 Authorization criteria.

- Something the user receives, e.g., one-time passwords (OTP) received via mobile telephony (such as short message service, SMS) or via the Internet (such as email or other personally accessible application)

"User names and passwords no longer provide adequate security [2]." A successful solution to the password problem has been the use of OTP [3], where the authorization server, via an alternate channel, sends the user an OTP each time the user needs to access the system. Such passwords can be valid for a short period of time, with the possible alternate channels being:

- Mobile telephony, where the authorization server sends the OTP to the user's cell phone via SMS or even machine spoken
- The Internet, where the authorization server sends the OTP to the user via chat, Skype, MSN, or as an email [3]

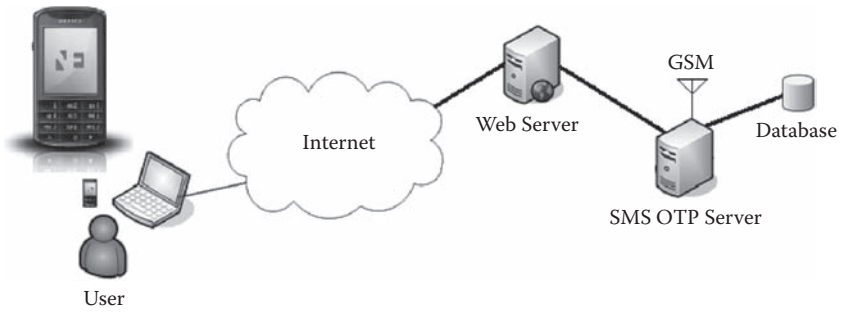

Figure 2.2 Authentication technology using an OTP delivered as an SMS to the user. (Courtesy of Nordic Edge, http://www.nordicedge.se.)

This solution falls in the category of the so-called *Two Factor Authentication* (TFA).* TFA implies the application of two authorization modes to best authenticate the user. The first factor is a conventional one, such as *user name* and *password,* and the second factor is an unconventional mode, such as the answer to a certain question or a biometric parameter, or a *parabiometric*† parameter.

The "two-factor authentication solution leverages an everyday tool—the [mobile] phone—[that is very close to the person] to secure [authentication for] account logins and transactions [2]." This type of authentication falls in the parabiometric category.

The participation of the mobile phone in the authentication process can be as simple as receiving an OTP or even speaking back a certain passphrase for voice print authentication. Furthermore, even if an attacker enters the correct user name and password, the authorized user will receive an immediate call informing them of the access. If the access is an intrusion attempt, the legitimate user "can immediately block the account and notify the company's fraud department, [that] can instantly take appropriate action [2]."

Multifactor (multimode) authentication procedures are on the rise and are being progressively deployed in high-security applications. An OTP example is illustrated in Figure 2.2, where the password is sent to the user via mobile telephony as an SMS.

An OTP can be combined with biometrics, as shown in Figure 2.3, where the fingerprint reading and an OTP is sent to the server for resource access.

A network illustrating the biometric OTP technology appears in Figure 2.4.

---

* Two Factor Authentication: Access is provided when two independent modes of secret parameters are presented to the access control authority.

† Parabiometric Parameter: A parameter that is closely identified with an individual, but it is not a physical property of that person. Examples are a user's mobile phone number, laptop's MAC address, or the IMEI of a mobile device used in the access authorization process.

Figure 2.3 Biometric fingerprint reading in USB form. (Courtesy of http://www.yubico.com.)

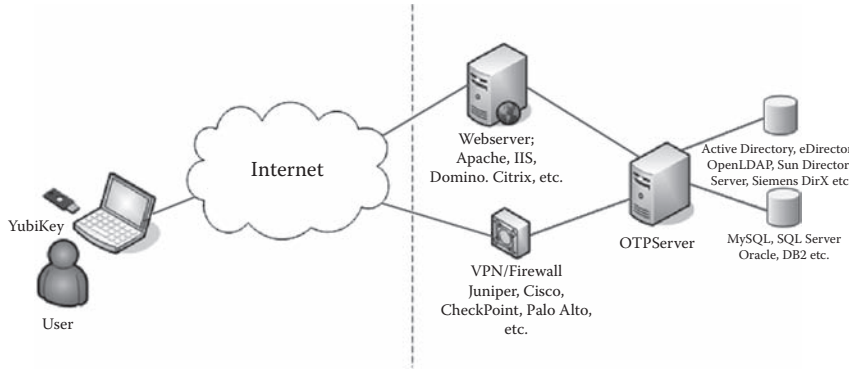

Figure 2.4 Authentication technology network using biometrics (fingerprint) and OTP. (Courtesy of Nordic Edge, http://www.nordicedge.se.)

Human Factors

An unclassified US government report has revealed that "The great majority of past compromises have involved insider, cleared persons with authorized access who could circumvent physical security barrier, [and] not outsiders breaking into secure areas [4]."

Personnel, whose activities involve the Internet or other modes of data handling, constitute a critical organizational asset, which may turn into a weak link. Their activities may be writing code, programming databases, using a USB storage device, or merely sending emails. Each and every such activity needs to be performed in a security-minded way and in accordance to policies. "Technology alone is not the answer [5]."

The establishment as well as the enforcement of policies, as to how organizational data are to be entered, modified, read, or deleted, constitutes the backbone of data security in any enterprise. Equally important is the audit trailing capability within the information system, so that data changes can be traced to their origin.* There are

* Audit Trail: Audit trail is the process that reveals the chronological sequence of actions that have resulted in the completion or attempt of a transaction or data change.

numerous ways of notifying data owners that their data is being accessed.* Depending on the criticality of the data, appropriate measures can be taken, ranging from receiving an email to receiving an SMS message on a mobile phone.

While technology can reasonably protect the electronic assets of an organization, it cannot, with the same ease, protect against insider threats.† Overwhelming statistics point out that most attacks on databases are internal or external with internal help. The expression goes: You cannot protect yourself from your bodyguard, your cook, or your doctor. It is difficult to set barriers between the organizational data and those who have a bona fide need to use them. Neither can an organization treat its members as potential criminals. However, security mechanisms need be in place so that no member in the organization can single-handedly cause major damage. Equally important is that no member in the organization can affect data access or changes without leaving a trace [6].

> Case studies and survey research indicate that there is a subset of information technology specialists who are especially vulnerable to emotional distress, disappointment, disgruntlement and consequent failures of judgment which can lead to an increased risk of damaging acts or vulnerability to recruitment or manipulation [6].

The same way *level of vulnerability* is being assigned to software, processes, or procedures, it should also be assigned to personnel handling critical organizational data. This is a very sensitive matter that, if not administered with extreme professionalism, may lead to the creation of alienation within the organization.

The CIO, together with the HR head, bears the responsibility of assessing the presence and level of a potential vulnerability in each and every member of the organization who handles critical data. In that respect, all members of an organization need to receive specific training and security guidelines. For the federal sector, an explicit document is provided by the National Institute for Standards and Technology (NIST) [7]. The guidelines are meant for government agencies, but equally apply to the civilian sector, with the emphasis being on awareness of the possible adverse consequences should there be an information security compromise.

Security Services

Security services may be provided by in-house talent, by external data security organizations, or by a combination of the two. Either way, the in-house Chief

---

* Data Owner: The data owner is the entity that controls the access of certain data and is also responsible for the security of the data—integrity, confidentiality, and availability.

† Insider Threat: Insider threat is the potential risk that entrusted members of an organization will abuse their designated access to organizational data to the detriment of the organization.

Table 2.1 Security Consultancy Services

Security audit	Intrusion tests	Network monitoring
Security architecture	Performance tests	Data migration
Security design	Off-site data archiving	Resource acquisition
Antivirus service	Off-site data backup	Security training

Information Security Officer (CISO or CSO) is the ultimately responsible person and ultimate authority in the information system definition, design, and implementation and in subsequent operations and security management.

Significant benefits can be derived from the use of external security organizations with experience and expertise that exceed that of the internal talent. However, in principle, the organizational vulnerability will increase when external security consultants enter an organization. Table 2.1 lists most services typically offered by security consultancy organizations.

External Technologies

The concept of *Enterprise Information Architecture* often goes beyond data, databases, intranet, and cyberspace and includes external technologies and resources. One such case is the use of the Global Positioning System (GPS) offered and maintained by the US Department of Defense [8]. The GPS, a twenty-four satellite system, provides the location information in the form of longitude, latitude, altitude, direction, and time. Figure 2.5 illustrates the GPS and its twenty-four satellite constellation.

This technology finds application in numerous industries, "such as emergency response services, law enforcement, cargo security, nuclear materials transport, aircraft navigation, and critical time and synchronization standards for utilities, telecommunications, and computer networks [9]."

While the system is highly accurate and reliable, and free of vulnerabilities, the system's "GPS signals are not secure [9]." The radio reception of the provided data can be jammed by attackers and, even worse, can be *spoofed,* fabricated to mislead the user. Thus, erroneous data will mislead the user as to the exact location of the tracked asset.

Fortunately, there are certain countermeasures that, although they do not restore the correct signals, give an indication of foul play. In the case of signal jamming, the GPS receiver receives a relatively strong radio signal but produces no data, leading to the conclusion that the signal is being jammed. As for spoofing, one may confirm the data produced by the received signals through conventional means, for example, verifying the direction of travel using a compass or comparing

Figure 2.5 The GPS and its twenty-four satellite constellation.

the received time using a clock. Also, the spoofed signal will be stronger than the expected one, "1×10^{-16} watts [9]."

Therefore, although the GPS signals originate from a very credible source, awareness of possible hacking should be included in the organizational data security equation.

Wireless Networks

An organizational network and the associated assets are also threatened by vulnerabilities in the wireless internal or external communications. While the three standardized wireless technologies—Bluetooth, Wi-Fi, and WiMAX—do have secure communications features, vulnerabilities do exist and need to be known and properly addressed by the users. By virtue of being wireless and operating in the radio frequency (RF) spectrum, such networks are exposed to some threats that are difficult to defend against. These are

- **Eavesdropping.** The availability of traffic analyzers enables the reception and capture of exchanged data very easily. Subsequently, data, though encrypted, can be collected and possibly deciphered at a later time.
- **Noise injection.** This is the intermittent injection of RF noise bursts aiming at the corruption of normal communications.
- **Jamming.** A powerful RF source transmitting in the vicinity of the organization's units and in the spectra of operations can incapacitate the network. Of course, the source location can be easily identified unless the source is mobile.
- **Man-in-the-middle.** This is a case where an adversary with a similar wireless capability is posing as a legitimate base station, mobile station, or subscriber station.

The most commonly used standardized wireless networks are Bluetooth (BT), Wireless Fidelity (Wi-Fi), and Worldwide Interoperability Microwave Access (WiMAX).

Bluetooth

Bluetooth (BT) is the commercial name of a data communications protocol certified by the IEEE (Institute of Electrical and Electronics Engineers) and technically known as the IEEE 802.15.1—1Mbps WPAN (Wireless Personal Area Network) Protocol. The protocol's aim is to provide "standards for low-complexity and low-power consumption wireless connectivity [10]."

Despite the extensive security precautions that have been entered into the BT specifications, it appears that the BT operating system design has inadvertently left several vulnerabilities. However, the fact that most BT code is in firmware makes BT wireless technology resistant to "*malicious code* [11]." Figure 2.6 illustrates a BT WPAN, serving as a cable replacement for an up to 30-feet, 10-meter, range.

To be vulnerable to intrusion risks, a BT-equipped device—mobile phone or personal computer—must have its BT feature activated. That is, the device must be in the *Discoverable Mode*. Furthermore, in all BT communications—bona fide or malicious—the devices—victim and attacker—must be within a 10-meter proximity to each other for communication to take place. However, the availability of highly sensitive receivers makes BT eavesdropping possible from much longer distances. Vulnerabilities in the BT-equipped devices can be considered as passive or

Figure 2.6 PAN employing BT technology.

active. In the passive ones intruders spy or create inconvenience, while in the active ones intruders inflict casualties on the victim's device databases.

Passive Vulnerabilities

The presence of the targeted device can be recognized through pinging. Repeated pinging can render the BT features of the victim-device inoperable. While a BT-equipped device is communicating, an intruder may determine the device's address and use it to communicate with it, thus disabling it from properly communicating with other devices. Improvements in BT specifications would eventually eliminate the penetration of devices in the nondiscoverable mode.

The BT wireless technology operates in an unlicensed band where numerous other applications find it equally convenient to operate. The Wi-Fi wireless LAN technology is there, using the very same band, as do microwave ovens and many cordless phones. Consequently, BT-equipped equipment found within the radiation terrain of one such product may be unintentionally inoperable [12].

Active Vulnerabilities

Via BT communication, an intruder may take full control of victim-device commands—namely, the AT Commands that control the mobile phone—without, in any way, attracting the attention of the victim-device owner. In this vulnerability, intruders can use the victim-device as if it were in the palm of their hand. Data can be altered, calls and messages can be sent and received, the Internet can be accessed, and even conversations can be listened to via the intruder's phone [13].

With specialized software, intruders not only may access all data in a victim-device, but they may even read the phone's unique hardware identification, the so-called International Mobile Equipment Identity (IMEI) [14].

Precautions

In the BT protocol specifications, a variety of security mechanisms have been embedded. However, in addition to establishing security policies, enterprises may also deploy BT software that scan the environment and monitor the BT band to

- Identify the various types of active BT devices
- Provide all retrievable attributes of the identified devices (class, name, and manufacturer)
- Provide connection information (pairing)
- Identify available services (fax, printer)

The level of the risk associated with the use of the BT wireless technology is directly related more to the specific application and less to the inherent BT architecture. Taking into account the numerous limitations under which BT technology operates—low RF power, distance, bandwidth—no highly sensitive or critical application will turn to the BT for support. For what it offers, namely, cable replacement, and for as long as basic precautions are adhered to, the BT wireless technology will be as secure as was intended to be, namely, for minimal-security intra-office applications [15].

Wireless Fidelity

Wireless Fidelity (Wi-Fi) is the commercial name of a data communications protocol certified by the IEEE, technically known as the IEEE 802.11—Multi-Rate DSSS* [16]. Wi-Fi is the wireless equivalent of IEEE 802.3 wired Ethernet protocol [17].

Major technology developers and OEM companies have formed the Wireless Ethernet Compatibility Alliance (WECA) to support certification of Wi-Fi equipment. WECA was established by the industry's network and microchip giants including 3Com, Cisco, Sony, Intel, Motorola, Nokia, and Toshiba, and it is now serving as a Wi-Fi equipment clearinghouse with a present membership of over 250 manufacturers [18]. The 802.11 protocol provides a universal wireless LAN (WLAN) infrastructure standard, through which interoperability among "Wi-Fi certified products" is guaranteed [19]. Prior to the establishment of the WLAN standard, and for decades, the WLAN applications stagnated because each major telecommunications manufacturer had its own designs. With the establishment of the Wi-Fi standard, WLANs became a standard intranet facility.

Wi-Fi security features were originally established by the WEP,† followed by the WPA,‡ and are currently defined by the WPA2,§ with the next generation of access protection covered by 802.11w.

---

* DSSS (Direct Sequence Spread Spectrum): This is a telecommunications modulation technique where the original signal is multiplied by a *known noise* to cover the entire given bandwidth, and it is then transmitted. At the destination, a counterpart demodulation technique retrieves the original signal.

† WEP (Wired Equivalent Privacy) is a Wi-Fi optional encryption standard. When activated, WEP encrypts the data that are wirelessly communicated. WEP provides a 40- or 64-bit encryption key based on which secure communication takes place between a radio NIC and its respective access point. NIC: Network Interface Card connects a computer to a network wired or wirelessly.

‡ WPA (Wi-Fi Protected Access): This is a 128-bit key WEP.

§ WPA2 (802.11i) (Wi-Fi Protected Access 2) is a 128-bit key WEP, which has provisions for PKI authentication.

Table 2.2 802.11 Wireless LAN Basic Characteristics [20, 21]

IEEE WLAN Standard	*Over-the-Air Data Rate*	*Media Access Control Layer Data Rate*	*Operating Frequency*
802.11b	11 Mbps	5 Mbps	2.4 GHz
802.11g	54 Mbps	25 Mbps	2.4 GHz
802.11a	54 Mbps	25 Mbps	5 GHz
802.11n	200–540 Mbps	100–200 Mbps	2.4 GHz or 5 GHz

There are presently three versions of the Wi-Fi standard, namely, the 802.11a, 802.11b, and 802.11g. Versions "a" and "g" offer a data rate of 54 Mbps, using a 5 GHz and a 2.4 GHz band, respectively. Version "b," the oldest standard, has an 11 Mbps data rate operating at a 2.4 GHz band [20]. Being unlicensed, the 5.0 GHz band is a very busy one. However, application of the 802.11h standard, which supports Dynamic Frequency Selection and Transmit Power Control, ensures "coexistence between Wi-Fi and other types of radio frequency devices" such as the BT [21].

The next Wi-Fi version is the 802.11n. The "n" standard not only quadruples the data throughput, bringing it to the 200–600 Mbps range, but is also backward compatible with legacy versions "a," "b," and "g." The "n" version capitalizes on the availability of a sufficient bandwidth, and through "multiple antennas, [and] cleverer encoding . . . [aims] to achieve raw data rates up to 600 Mbps [22]." Table 2.2 displays the basic specifications of the four 802.11 versions [21, 22].

In a wireless Wi-Fi system, excluding the software, there are two physical components: the access point (AP),* and the wireless interface unit, which is an insertable card, an embedded circuit, or a USB device. The system's central component is the AP, which interfaces the "wireless" world with the wired one—referred to as the infrastructure.

Thus, the AP, on one side, communicates with the organization's network, the so called *infrastructure*, and on the other side, communicates with its wireless clients and serves as a router meeting the networking needs of the wireless stations, as shown in Figure 2.7. The AP provides shared LAN/Internet access using Network Address Translation (NAT).

In a nonprotected Wi-Fi environment, a *wardriver* (WD)† can use a victim's bandwidth to access whatever is accessible. As a minimum, the WD can access the Internet or the victim's intranet, and as a maximum, the WD can access all files in the victim's computer and penetrate into any other place that is accessible by the

* AP (Access Point) interfaces the wired network infrastructure to the wireless one. Contains radio interface, logic and router.

† WD (Wardriver) is an intruder who drives by Wi-Fi areas with a laptop trying to access the Internet for free and/or to snoop on Wi-Fi clients' sensitive data.

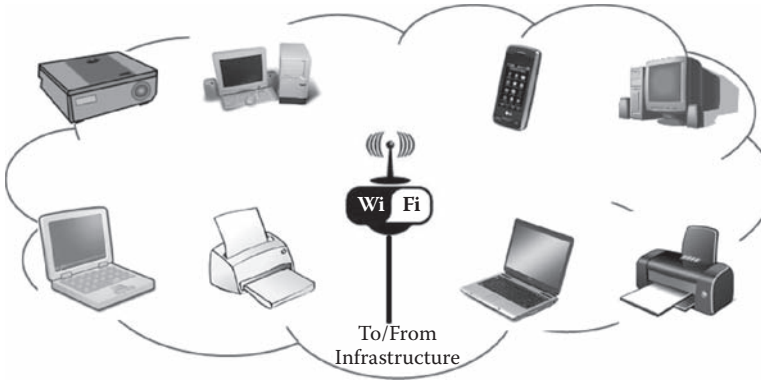

Figure 2.7 A typical WLAN network where diverse types of equipment communicate with each other and with the infrastructure, all via Wi-Fi.

victim's computer. In other words, in a nonprotected Wi-Fi environment, a WD can take full control of the victim's computer.

Worth mentioning is that any visit to the Internet by the WD will bear the victim's router identity, which may implicate the victim beyond easy proof of Wi-Fi hijacking. There are numerous cases of Wi-Fi hijacking covered in the media, most too sad to mention.

Wi-Fi Precautions at Home

Below is a list of precautionary measures that must be followed while using Wi-Fi in a home environment.

One: Turn Off the IBSS* Mode. In this mode the mobile unit is open to communication without any restriction. Hackers may link and silently access sensitive information. Such risks can be eliminated if the IBSS is disabled. Also, turn off the Wi-Fi access connection as soon as it is not needed anymore.

Two: Turn On the Infrastructure Mode. The infrastructure mode enables Wi-Fi clients to access resources on the other side of the access point (printers, servers, etc.).

Three: Turn Off SSID† Broadcasting. Since in the home environment one does not anticipate unexpected Wi-Fi devices, it is not necessary for the access

* IBSS (Independent Basic Service Set) mode, commonly known as ad-hoc mode. In this mode, Wi-Fi clients can connect to each other directly without the need for an access point. This can be useful in a secure environment, like a conference room, where participants can set up an "ad-hoc" network to communicate with each other.

† SSID (Service Set Identification): This is the Wi-Fi network identifier—a secret key—established by the network's administrator. The SSID is included in the header of all communicated packets.

point to broadcast its SSID identity to the world. Usually, this ID is entered manually, and only once, during laptop login and is remembered afterwards.

Four: Change Router's Access. The router, located in the AP, is accessible via a name and a password. They are set at the initial installation, but can be reconfigured at any time. These two parameters should be changed at intervals. Also, the default fictitious local, intranet, IP address, which may have come as 192.168.1.1, can be changed to any other, as long as the numbers in the four fields range from 0 to 224, without leading zeros. Also, "there is no need to keep the default router name." To the contrary, any change from the default values will contribute to a better security posture. Typically, the default values are the same for all access points of a given manufacturer and are usually known to intruders [23].

Five: Turn On the Encryption. The Wi-Fi specification includes the so-called Wired Equivalent Protection (WEP). The encryption algorithm comes in 40 and 64 bits. A later version, the WPA2, comes in 128 bits. Each time a mobile unit logs on to a Wi-Fi access point, the unit's login name and password can be easily captured by a "sniffer." One way to prevent that is to use PKI,* where each side knows the other side's public key, and a "passkey" can be established under encryption without exposing any non-encrypted information. The latest version of the Wi-Fi security protocol, WPA2, does provide PKI. It needs to be pointed out that the encryption *dissolves* once the data reach their destination. That is, WPA2 is for the air-transit only. Furthermore, "the underlying [encryption] algorithm is flawed and subject to relatively easy cracking." There are even websites that provide the steps to crack a WEP [24].

Six: Turn On the MAC† Address Filtering. Usually, Wi-Fi access points contain a gateway that has Media Access Control (MAC) filtering capabilities. One may allow the filter to pass traffic only from devices of known MAC addresses. These devices may be in the infrastructure (that is, on the wired side of the access point), they may be printers or other computers, or they may be in the wireless space—the Wi-Fi card of the laptop, a Wi-Fi PDA, and the like. If in a wireless network, the SSID is known, then "without MAC address filtering, any wireless client can join [25]." However, this will not deter the advanced hacker who knows how to capture packets and extract the SSID and MAC addresses from them.

Seven: Scout the Airwaves. Using specialized software, like the packet sniffer freeware *Ethereal,* one must frequently scout the airwaves for unexpected Wi-Fi access points or Wi-Fi clients. Such tools, like the *Ethereal*, can capture data "off-the-wire from live network connections . . . can read captured files . . . decompress them on the fly . . . [and can currently dissect] . . . 759 protocols [26]."

---

* PKI (Public Key Infrastructure): An encryption scheme based on digital certificates.

† MAC (Media Access Control) is the 32-bit address of a unit's Network Interface Card (NIC). An intelligent access point allows access to clients of authorized MAC addresses.

Wi-Fi Precautions at the Hotspot

For the convenience of clients, public hotspots do not use any of the possible security features of the Wi-Fi (WEP or WPA encryption) or networking (MAC filtering). To facilitate clients' connections, Wi-Fi access points actually broadcast their SSID. In a hotspot, clients start by turning on their Wi-Fi option, connect to the access point, submit a valid credit card number, and the link is established. For a mobile unit to communicate with the access point, knowledge of the SSID of the access point is necessary.

For a Wi-Fi client to be hacked it is not necessary that the mobile unit be in communication with any access point. The mere fact that the Wi-Fi feature is on is sufficient to establish vulnerability. Wi-Fi clients in, either public or corporate, hotspots need to take several precautions to maximize the defense of their sensitive information from intruders. Below are some precautions that need be taken while at a hotspot.

One: Hotspot Legitimacy. Hackers often set up a fake access point in the vicinity of a legitimate public hotspot and attempt to lure connection seekers. Through such connections, hackers would capture sensitive information (user names, passwords, credit card numbers, etc.), making subsequent illegal use. Wi-Fi clients need to absolutely ascertain that the hotspot they attempt to connect to is a legitimate one. Usually, the facility associated with the hotspot service (waiting rooms, coffee shops, etc.) would have appropriate signs posted. There are several websites that list known legitimate hotspots worldwide [27].

Two: File Encryption. Files including emails should be encrypted prior to transmission. There are numerous encryption options using dedicated software or using features embedded in applications such as word processors and email clients. One may install an encryption application that "automatically encrypts all . . . inbound and outbound Internet traffic [28]."

Three: File Sharing. While in a hotspot, keep the file sharing option off to prevent unwanted file transfer.

Four: Turn the VPN* on. This way, intercepted data are rendered useless because of encryption.

Five: Firewall Use. A hotspot, most probably, uses a single static IP address to possibly serve 200 clients. That is, all clients are in the same subnet, making

* VPN (Virtual Private Network) is a security concept using IPSec.
IPSec (Internet Protocol Security): This protocol provides encrypted tunneling with header and payload encryption and transport with payload encryption only. It also provides advanced authentication features.
Tunneling: Tunneling is a security concept where data are first encapsulated in a private protocol (such as IPSec) and afterwards are encapsulated again in a public protocol for transportation via any standard networks (Internet, intranet, etc.).

it easier for a client-intruder to snoop on other clients. That problem can be minimized with the use of a "personal firewall." One may purchase a firewall or may use the one provided by the Windows XP. Through the firewall one may restrict traffic and block or permit "communications that might . . . be dangerous [29]."

Six: Rules of Thumb. Regardless if one is accessing the outside world wired or wirelessly, certain additional precautions also apply: use of the latest antivirus software, use of the most updated version of the operating system, use of Web-based secure (https) email, individual password protection for sensitive files, and last but not least have a computer password mechanism that locks the computer if there is no keyboard or mouse activity for x minutes.

Wi-Fi Precautions at the Enterprise

Corporate Wi-Fi security demands a much more serious tackling of the Wi-Fi vulnerabilities. For such cases advanced protocols and VPNs are in order. In the enterprise environment the Wi-Fi security precautions may include all the above described, as well as the ones below.

One: Perimetric Fencing. Solutions are currently available where positioning of RF sensors can geometrically determine if a client is within the authorized physical area. Such technologies, which need onsite *terrain training* and *fine tuning*, have offered 100% security in testing. Using perimetric fencing, "Wi-Fi environments can be protected in a 3-D air space [to an accuracy of] . . . about 5 feet [30]."

Two: Advanced Authentication. Rather than relying on the nominal security features of the Wi-Fi, an enterprise may use advanced authorization/authentication protocols, such as DIAMETER.*

Wi-Fi has by now become a cornerstone technology in local wireless communications. Its major vulnerabilities—session hijacking, man-in-the-middle, and denial-of-service—are being continuously mitigated through advances in security technologies and through increased security awareness on the users' side. With the increase in the effective data rates to exceed 200 Mbps, there will be plenty of bandwidth for advanced encryption techniques and for sophisticated authorization/authentication protocols. It is expected that security standard 802.11w, with the *per packet encryption key* and additional powerful features, will significantly enhance Wi-Fi security and will reduce successful intruder attacks [31].

* DIAMETER is an advanced communications protocol providing increased wireless security. It is the successor of the RADIUS (Remote Authentication Dial In User Service) protocol.

Worldwide Interoperability Microwave Access

The Worldwide Interoperability Microwave Access (WiMAX) is the IEEE Wireless Networking Standard 802.16 and was released in 2004. Its specifications are continuously enhanced with amendments that aim at making it a viable wireless replacement of cable, ADSL*, and T1† wired technologies. WiMAX serving as fixed or mobile LAN‡ or Metropolitan Area Networks (MAN) uses licensed and unlicensed frequency bands for high- and low-power transmissions, respectively, to provide Broadband Wireless Access (BWA).

WiMAX Features

The unlicensed bands in the 2–10 GHz spectrum limit the range to that of the Wi-Fi, which is about 10 to 50 meters, where transmitted power is usually limited to 200 mW. The licensed bands in the 10–66 GHz line-of-sight spectrum, where transmitted power can reach 20 watts, can offer a radius range of 50 km from a single base station. Furthermore, the standard WiMAX data rate is 70 Mb/s. Figure 2.8 shows a WiMAX control window and a USB WiMAX adapter.

Several laptop vendors offer "WiMAX ready" units [32], and WiMAX USB adapters are available, as well [33]. WiMAX technology is also being utilized for long-distance point-to-point connections via repeaters using directional antennas. WiMAX features include

- Roaming—offers client mobility (802.16e)
- Forward error correction—uses fault-tolerance algorithms
- Adaptive modulation—trades range for bandwidth
- User and device authentication
- Confidentiality of transmitted data messages
- High data throughput—reaches 75 Mb/s
- Triple-DES§ encryption—for authentication and transmission
- AAS¶ —uses advanced antenna techniques (802.16e)

---

* ADSL (Asymmetric Digital Subscriber Line) is a wired telephony technology where a data channel is frequency multiplexed with the regular voice communications, and it is demultiplexed at the user's site using a splitter that provides a voice outlet to be connected to a standard telephone and a data outlet to be connected to a data terminal. The first facilitates traditional telephony, while the latter usually provides Internet access.

† T1 is a wired telecommunications standard indicating a data speed of 1.544 Mb/s (1,544,000 bits per second).

‡ LAN (Local (intra-building) Area Networks): MAN (Metropolitan (intra-city) Area Networks).

§ DES (Data Encryption Standard): This is an encryption cipher believed to be breakable through bruteforce. Triple application makes code breaking impractical with today's computational power.

¶ AAS (Advanced Antenna Systems) are smart antenna technologies that enhance gain, directivity, and data throughput.

Figure 2.8 WiMAX control window and a USB WiMAX adapter. (From Intel, http://download.intel.com/support/wireless/wmax/5350_5150/S6/intelrproset wirelesswimax userguide.pdf.)

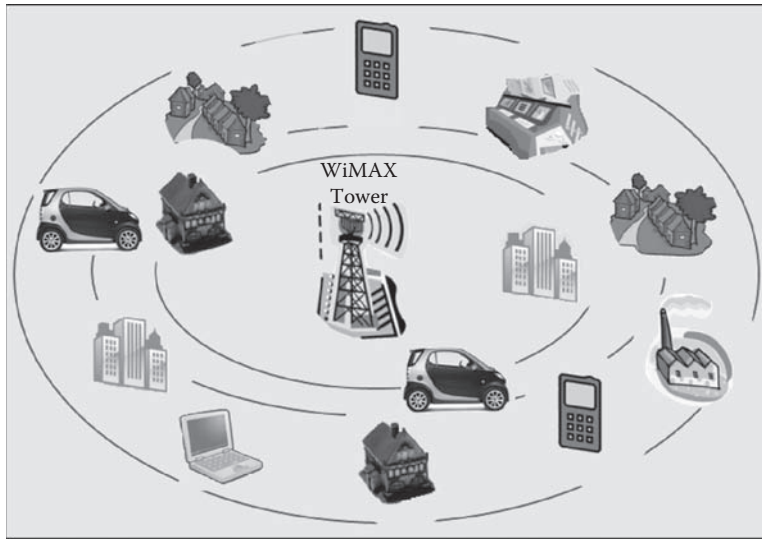

Figure 2.9 Typical WiMAX network where Internet access can be wirelessly provided to a metropolitan area.

- Speeds up to 1 Gbps and 100 Mbps for fixed and mobile operations, respectively (802.16m)

Figure 2.9 illustrates a possible WiMAX environment where Internet service is provided in a 50-km radius to the entire population. In this scenario, Internet is provided to a single user with a mobile phone, a laptop, or a desktop, as well as to multi-user organizations such as office buildings, residential compounds, or industrial parks.

Contrary to WiMAX products and services vendors, researchers allege that there are several vulnerabilities in the WiMAX technology. With the 802.16e specifications

in place, most of the alleged vulnerabilities have been removed. However, the following vulnerabilities remain, as pointed out in a NIST report [34].

- End-to-end (i.e., device-to-device) security is not possible without applying additional security controls not specified by the IEEE standards.
- Data SAs (Security Associations) cannot be applied to management messages, which are never encrypted.*
- Lack of mutual authentication may allow a rogue BS (Base Station) to impersonate a legitimate BS, thereby rendering the SS/MS (Subscriber Station/Mobile Station) unable to verify the authenticity of protocol messages received from the BS.

Therefore, for the confidentiality of management messages, WiMAX users need to improvise their own security scheme. In this case, the Diffie–Hellman Key Agreement Standard, which is often used in cases where confidential communications need to start without any prior keys exchanged, can also be used. A list of countermeasures that can reduce risks in wireless networks are described in documents prepared by the NIST† [34, 35, 36, 37, 38].

Cloud Computing

The increasingly low cost of computer and telecommunications hardware coupled with the standardization of software has resulted in *cloud computing*. The term *cloud computing* refers to a new concept in the acquisition of computing power as a service. This service is provided out of pooled resources, where the user has no knowledge of the physical origin of such service. Figure 2.10 illustrates the concept of cloud computing where users need only Internet access.

Providers of such services may even share resources, creating a service that can be paralleled to the distribution of electrical power. In this context, computing power includes software, virtual hardware, data storage, and data access. In a way, it is similar to the concept of time-sharing of the 1970s, but it is much more powerful and accessible via the Internet, rather than via telephone modems. Today, with cloud computing an organization needs no computer center, because all computational needs are realized and provided as a service via the Internet. Cloud computing falls in the four basic definitions listed in Table 2.3.

---

* SA (Security Association): This term refers to parameters used to provide secure communication between two or more entities. Such parameters include special identifiers and encryption keys, types, and ciphers.

† NIST (National Institute of Standards and Technology) is a US government agency responsible for providing the country with standards and guidelines in technology and science issues.

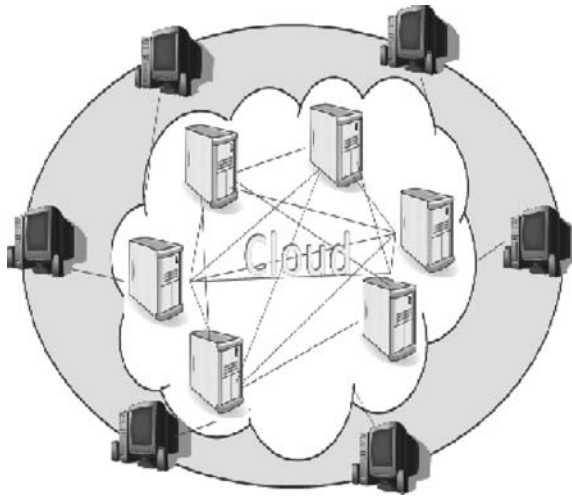

Figure 2.10 Cloud computing. The only user requirement is Internet access.

Table 2.3 Cloud Computing Option

Public Cloud	A commercial center of vast computing resources that are provided to the public on-demand basis in a metered fashion.
Private Cloud	A privately owned center of shared computing resources that are provided to the community's members on-demand basis in a metered fashion. The security and privacy measures are customized to the owners' needs.
Community Cloud	A community-owned center of vast computing resources that are provided to the community's members on-demand basis in a metered fashion. The security and privacy measures are customized to the community' needs.
Hybrid Cloud	A combination of the above options.

Cloud computing providers offer *Infrastructure*, *Platform,* and *Software* as a *Service* (abbreviated as IaaS, PaaS, and SaaS, respectively). Users subscribe to such services and configure their own virtual computer center with servers and databases as if they were to purchase physical equipment for that purpose. In such an operating mode, an organization may reconfigure and scale the computational needs at any time and be charged on a pay-per-use basis. The motto of this new industry is "buy exactly the capacity you need, when you need it, by the hour or by monthly subscription [39]."

Users' applications and data, delivered through shared data centers, may reside in geographically diverse locations and may even change locations transparently to the user. Yet, everything is Web accessible via the same logical addresses. With screen sharing as well as application sharing now possible on the cloud, cloud computing has become even more attractive for over-the-Web interactions. Cloud computing has been receiving increasing support as a practical solution to building a corporate data center all in a virtualized manner and without allocating physical space. Table 2.4 provides a list of the most acclaimed advantages of cloud computing.

There is no doubt that cloud computing is a very strong irreversible trend, but along with it come security and privacy challenges that translate into vulnerabilities which need to be carefully weighed before walking into this rose garden.

"The security challenges cloud computing presents, however, are formidable, especially for public clouds whose infrastructure and computational resources are

Table 2.4 Cloud Computing—Advantages

1. Reconfiguration	Users can redesign their computational infrastructure at the click of a mouse, selecting and removing resources (servers, storage, applications, networks, and services) as the need arises.
2. API support	Application Programming Interface is possible for cloud software interaction with machines or humans.
3. Reduced cost	Cloud computing reduces barriers-to-entry by facilitating the creation of organizational data centers out of metered resources through a pay-as-you-need business model.
4. Reduced skills	Necessary skills to set up and maintain a virtualized data center in a cloud are far less demanding than those of maintaining a physical one.
5. Connectivity	Cloud connectivity services include Internet as well as mobile phone access.
6. Reliability	Use of multiple redundant sites can secure business continuity and disaster recovery.
7. Scalability	Cloud computing provides on-demand scalability in a self-service mode allowing system reconfiguration for an increased or decreased size or use of resources.
8. Security	Security features are provided, normally too expensive for individual users to afford.
9. Maintenance	Cloud computing providers install the latest in software versions and antimalware protection.

Table 2.5 Cloud Computing—Disadvantages

■ System complexity	■ Cloud computing platforms, especially the public ones, because of their size and increased functionality, are open to errors and vulnerabilities.
■ Multi-tenancy	■ Concerns are that in a multi-tenant environment of shared resources, lack of strong compartmentalization may result in security or privacy issues.
■ Internet vs. intranet	■ Cloud computing is Web accessible and by definition less secure than an isolated organizational intranet.
■ Personnel	■ Personnel of public cloud computing may not have the required level of security clearance.
■ Forensics	■ In a cloud environment, depending on the level of internal auditing, it may not be possible to link performed services with associated hardware. Furthermore, past strings of computer- and human-generated activities can be difficult to trace and document to a court-acceptable level and can be impossible to duplicate.
■ Cloud policies	■ Cloud computing providers' security and privacy policies and practices may or may not comply with those of demanding private or government tenants.
■ Account hijacking	■ While examples are not available, strong concern exists in the possibility of credentials hacking and subsequent website compromise.
■ Service outage	■ There are numerous examples where causes beyond the control of the cloud providers have resulted in outages of several hours at the least expected times. This is an issue that can be well worded in a service agreement, but lightning will not read it before striking.
■ Incident response	■ Such an event will require a coordinated effort of the service subscriber and service provider in the formidable task of audit trailing that may involve the prior use of shared hardware.

owned by an outside party that sells those services to the general public [40]." The above statement, coming from a very authoritative body like the NIST, can make CIOs and CSOs stop in their tracks. There is a strong concern that the outsourced custody of the physical storage of sensitive organizational data constitutes in itself a major vulnerability.

To many, and by definition, cloud computing is a nonsecure environment. But to a growing number, cloud computing is the way to go and is here to stay. As for security and privacy, additional measures can be taken to bring this new mode to par with the traditional in-house data centers, in that respect.

Before embarking to transitioning into cloud computing, verifiable assurances must be obtained that organizational security and privacy requirements are fully satisfied. Cloud computing providers often offer nonnegotiable service agreements. However, this is not absolute, and negotiated ones can be obtained.

It has to be emphasized that the cloud computing system does include the client software and their access software and devices, and security and privacy policies must be safeguarded on this side as well.

Whenever necessary, a cloud computing provider should be able to demonstrate the effectiveness of the offered services, especially those related to security and privacy. Often, third-party auditors are brought in to attest as to the validity of the claimed services. Cloud computing falls in the general category of outsourcing, with all associated risks. Therefore, a thorough risk analysis is called for before engaging in any such agreements. The major perceived disadvantages in subscribing to a cloud computing environment are listed in Table 2.5.

While "the transition to an outsourced, public cloud computing environment is in many ways an exercise in risk management [40]," cloud computing, now in its infancy, will eventually become the mainstream data center hosting due to its cost-effectiveness that will be improving over time.

Exercises

1. Access and review the National Training Standard for Designated Approving Authority (DAA) document located at http://staff.washington.edu/dittrich/center/docs/nstissi_4012.pdf. Summarize it in a twelve-slide electronic presentation.
2. Access and review the *Authentication in an Internet Banking Environment* of the Federal Financial Institutions Examination Council located at http://www.ffiec.gov/pdf/authentication_guidance.pdf. Summarize it in a six-slide electronic presentation.
3. Visit the website www.NordicEdge.se, familiarize yourself with the One-Time-Password technology, and experience it though the Download Two Factor Authentication Trial option at http://nordicedge.com/products/one-time password-server/download/.

4. Access and review the Wireless LAN Security Today and Tomorrow document located at http://www.itsec.gov.cn/docs/20090507163620550203.pdf. Summarize it in an eight-slide electronic presentation.
5. Visit the website http://www.outofblue.net. Understand the presented technology, and express your thoughts as to any vulnerabilities on the side of the clients as well as on that of the server.
6. Visit the websites of Wi-Fi hardware vendors. Understand the technology, and design a WLAN service that will provide Internet access to a three-floor square office building of 30 m on each side. Determine the topology of the APs.
7. Visit the websites of WiMAX hardware vendors. Understand the technology, and design a service that will provide Internet access to a 50-km radius rather flat area.
8. Access and review the following two documents on cloud computing, located at
   - http://www.us-cert.gov/reading_room/USCERT-CloudComputing Huth Cebula.pdf
   - http://res.sys-con.com/download/1288112960/Cloud_101-WhitePaper.pdf

   Prepare a twelve-slide electronic presentation with the same title.
9. Visit the website of a Cloud Computing provider, subscribe in a free trial option, and build a multiserver and multistorage infrastructure. Describe and document your gained knowledge and experience.
10. Access and review the following three documents, and prepare a twelve-slide electronic presentation with the title Cloud Computing Vulnerabilities.
    - Seven Deadly Threats and Vulnerabilities in Cloud Computing, http://www.ijaest.iserp.org/archieves/15-Jul-15-31-11/Vol-No.9-Issue-No.1/16.IJAEST-Vol-No-9-Issue-No-1-Seven-Deadly-Threats-and-Vulnerabilities-in-Cloud-Computing-087-090.pdf
    - Cross-VM *Vulnerabilities* in *Cloud Computing,* http://rump2009.cr.yp.to/8d9cebc9ad358331fcde611bf45f735d.pdf
    - Top Threats *Cloud Computing* V1.0, *https://cloudsecurityalliance.org/top-threats/csathreats.v1.0.pdf*