

## PART ONE

# Introduction to Wireless and Mobile Networks

© Rodolfo CiviDreamstime.com

**CHAPTER 1** The Evolution of Data Networks 3

**CHAPTER 2** The Evolution of Wired Networking to  
Wireless Networking 31

**CHAPTER 3** The Mobile Revolution XX

**CHAPTER 4** Security Threats Overview—  
Wired, Wireless, and Mobile XX



# The Evolution of Data Networks

ONE OF THE MOST PROFOUND CHANGES in network security over the past 10 to 15 years has been the untethering of network connectivity. The ability to log on to both the Internet and corporate networks without having to physically connect a computer to the network via an Ethernet cable has radically altered the culture and has greatly blurred the line between work life and personal life.

Although most people view the resulting changes as a net positive, both wireless and mobile networking have introduced significant security vulnerabilities to networking in general. These vulnerabilities, along with prevention and detection methods, are the focus of this text. Before jumping into the details of wireless and mobile network security, however, let's take a look at how these profound changes came about.

## Chapter 1 Topics

---

This chapter covers the following concepts and topics:

- How early forms of data communication worked
- How mobile phones evolved
- How computers went mobile
- How mobile and data networks converged
- What the impact of the bring your own device (BYOD) trend is
- What the basic tenets of network security are
- How cybercrime has evolved
- How wireless network security is achieved
- How Mobile IP security is achieved

## Chapter 1 Goals

---

When you complete this chapter, you will be able to:

- Describe the evolutionary history of networking
- Relate the three core principles of network security
- Describe the security concerns specific to wireless networking
- Describe the security concerns specific to mobile networking
- Relate the IT policies employed to ensure the security of wireless and mobile networks

## The Dawn of Data Communication

---

Data communication and networking have a long history going back to 1835, when Samuel Morse developed the first practical telegraph system. In 1844, Morse sent his first long-distance message, “What hath God wrought!” encoded in Morse code, from Washington, D.C., to Baltimore, Maryland. By 1850, more than 12,000 miles of telegraph lines traversed the country, run by more than 20 different commercial operators.

**Telegraphy**, as it was known, used start and stop signals of dots and dashes transmitted over copper wires. It was a one-way message protocol that evolved to support two and later even four channels. Telegraphy monopolized electronic communication until 1877, when the first telephone networks started to appear.

Despite reservations that telephones would be too technical for the common man, **telephony** was quickly adopted. Indeed the telephone system quickly usurped telegraphy in terms of traffic carried, revenue generated, and network coverage. Telephony, however, was limited to voice. Therefore, despite telegraphy losing out to the telephone as the popular means for interpersonal communications, it remained an effective medium for carrying digital data traffic.

In 1923, the first teletypewriter services came into being, serving the need for true and accurate communications. By 1930, AT&T had launched a high-speed telex service, the Teletypewriter Exchange Service (TWX). This was followed in 1935 by the introduction of rotary-dial telex services. All these telex, telegraph, and TWX networks existed independently, as separate and distinct entities from the **public switched telephone network (PSTN)**.

By the 1950s the PSTN had become ubiquitous and affordable, in large part due to broad interconnectivity, creating a network effect. The PSTN could interconnect telephones from anywhere in the community, the country, or even internationally over its network of exchanges. To accomplish this, a hierarchy of networks connected local exchange

## CHAPTER 1 | The Evolution of Data Networks

carriers (LECs) with regional, national, and international carriers via interexchange carriers (IXCs). It was this national and international reach that made the PSTN such an inviting medium when it became necessary to network large business-computer mainframes.

## Early Data Networks

By the late 1950s, there was a demand to network the growing number of business computers being deployed by large companies. These computers were large standalone machines that operated independently. IBM accomplished the first successful interface between two digital devices over the analog PSTN using acoustic couplers and telephone sets. These couplers operated over the PSTN at 300 bits per second (bps). At this point, voice networks and the burgeoning data network began to merge.

### NOTE

The **network effect** is a phenomenon in which a technology becomes more valuable as the number of users or units increases. A common example is the fax machine. The first fax machine was useless, but the second fax machine made the first one useful. As more were added, all fax machines had greater utility.

### FYI

Until the appearance of the personal computer (PC), computers were huge mainframes that often occupied an entire room. Access to these computers was achieved through a “dumb terminal,” which offered a simple text display (often called a *green screen* due to the green color of the font on the black screen), as shown in Figure 1-1. These displays had no computing power; rather, they were simple readout displays.



Courtesy of U.S. Department of Defense

**FIGURE 1-1**

A dumb terminal or green screen.

## 6 PART 1 | Introduction to Wireless and Mobile Networks

Another significant point in the history of data communications was the transmission of the first fax over the standard PSTN in 1962. This was possible due to the modulation of data into sound by devices called *modems*, which were attached to either end of the analog telephone lines. A **modem**, short for modulator/demodulator, was required to transfer digital communications over the analog PSTN for the several decades that followed. Modems convert digital data into an analog signal for transport over the wire. At the other end, the analog signal is demodulated to recover the original digital signal. Using modems, computers located anywhere there was a telephone line could communicate over the analog PSTN.

Soon, however, telephone companies saw the obvious benefits of digital technology and began upgrading their networks. Digital communication was accepted as technically superior to analog. Furthermore, digital technology had become both cheaper and more reliable, which made it suitable for transmitting voice communications.

Digital communications have the following advantages over analog:

- More efficient use of bandwidth
- Greater utilization
- Improved error rates (that is, fewer errors)
- Less susceptibility to noise and interference
- Increased throughput
- Support for additional services (such as caller ID, auto forwarding, and call waiting)

As telecom providers rolled out new digital networks, high-speed digital communication became a widely available service.

The innovation that enabled the technological leap in long-distance digital communication was **packet switching**, used in lieu of **circuit switching**. In circuit switching, a physical connection was made between two phones using a series of telephony switches, creating an electric circuit. While the circuit was in use, no other phones could use the wires connecting the two phones. This was very inefficient because conversations—even among chatty people—are in fact about 50 percent silence when you account for the pauses between words and between speakers. It was also very expensive, especially on long-distance calls, because the callers had to “rent” the exclusive use of the circuit.

There were also concerns with circuit switching regarding the resilience of the message path. Circuit switching restricted communications to a pre-provisioned point-to-point circuit for the duration of the call. Should any intermediary exchange along the message path fail, the circuit was lost and had to be re-provisioned. Ideally, the call would be automatically rerouted over a different path. However, that required multiple paths to any given destination and an awareness of alternative routes to the destination, which greatly increased the user cost.

In packet switching, the voice signal is first digitized and then chopped up into a series of packets. These contain the voice information along with the source and destination. The packets are then forwarded from the source to the destination. Taking advantage of the silent gaps, packets from multiple conversations can share the same circuit, making

## CHAPTER 1 | The Evolution of Data Networks

packet switching much more efficient. Additional efficiencies were created through the development of digital compression techniques so that today, many conversations exist on the same wires.

Packet switching is more resilient. Packets can take multiple paths from source to destination, so there is no dependence on a single circuit. Also, because each single packet is such a small fragment of the speech signal, many packets can be lost or dropped without noticeably affecting the quality of the call. With packet switching, if any one circuit or exchange fails, the packets are rerouted. Any dropped packets are simply ignored. As it turned out, packet switching was also key to modern data communication.

Not surprisingly, the military was very much involved in developing packet switching. Its interests lay in the possibilities of high-speed failover and resilient data communications under battlefield conditions. In these conditions, the communications link required an alternate path, which could be automatically determined should the primary communications link be lost. This initiative, formulated in 1963 by J.C.R. Licklider, led to the earliest idea for networking computers to communicate over a common data communication mesh.

### The Internet Revolution

Licklider went on to head up the U.S. government's Advanced Research Projects Agency (ARPA) to research and develop computer networks. The results of the ARPA project were the design, creation, and development of the ARPANET. This was the first computer network based on packet switching.

The ARPANET project was the predecessor of the modern Internet. During the 1970s and 1980s, however, it was a noncommercial network developed and used by universities and research institutions. During this period, despite being little known and seldom used, the ARPANET project developed several key protocols—one of the most important being the **Transmission Control Protocol/Internet Protocol (TCP/IP)**. TCP/IP would become the protocol of the Internet in the early 1990s. However, the ARPANET project's continued development of packet switching had a more noticeable effect on data communications during the 1970s and 1980s.

The desire for more efficient digital (rather than analog) communication prompted the creation of the Integrated Services for Digital Network (ISDN), a set of communication standards that came on the scene in the late 1980s. ISDN supported simultaneous voice, video, and data. It was essentially a circuit-based telephone system that allowed access to packet-switched data networks. It could provide both 64 Kbps circuit-based increments for use by voice or data and packet-based service for data. ISDN was available to both business and residential users.

Other technologies, such as Frame Relay (FR) and Asynchronous Transfer Mode (ATM), became the standard methods of connecting business computers and networks over long distances. These *wide area networks (WANs)*, as they were known, were point-to-point or point-to-multipoint topologies, which enabled companies to connect networks and computers in cities and countries across the globe at high speeds and high throughput.

### LAN Technologies Vie for Supremacy

In the early 1990s, many LAN technologies vied for supremacy. Proprietary networking protocols such as DECnet, AppleTalk, and IBM's Token Ring were all prevalent. These proprietary protocols were not compatible, however. That is, LANs using different protocols could not be connected to each other. The challenge was to connect all these different operating systems and protocols into one heterogeneous network. By the early 1990s, a clear winner had emerged in the LAN technology war: the Ethernet protocol. It became the ubiquitous LAN network standard protocol across the globe. Nearly 30 years later, Ethernet is still the dominant LAN protocol.

### Advances in Personal Computers

Digital communications were not the only technology growing by leaps and bounds. Within businesses themselves, a revolution was occurring that spelled the end of the road for the huge mainframes and their dumb terminals.

The IBM personal computer (PC) was launched in the early 1980s. It immediately caught the attention of businesses and became popular for running standalone word-processing and accounting packages. But because most of the business data resided on the mainframe, both a PC and a mainframe terminal were required on the desktop. Not only was that inconvenient, there was no easy way to transfer information from the mainframe to the PC applications for local processing. The solution was to connect each PC to the mainframe by networking them over a local area network (LAN). This made the dumb terminal redundant.

### Mobile Phones and the Creation of the Other New Network

In the early 1980s, the first analog mobile phone system, called **Advanced Mobile Phone System (AMPS)**, became commercially available. AMPS was an immediate success despite its inherent security weaknesses—namely, it was unencrypted and vulnerable to eavesdropping. These failings were to be remedied in the second generation (2G) of mobile phone systems that emerged in the early 1990s.

The success of the first-generation (1G) mobile phones was only the beginning of a massive new market, as second-generation systems emerged to compete for supremacy. In response, the U.S. developed the **Code Division Multiple Access (CDMA) standard** and the Europeans established the **Global System for Mobile (GSM) standard**. Both these standards used digital transmission to rectify many of the 1G standard's failings. The adoption of the new 2G standards in both the U.S. and Europe was widespread, with major technological advances spurred as a result of the technologies' success. The size of the phones shrank as electronics and battery technology improved, and also because of denser cells



## CHAPTER 1 | The Evolution of Data Networks

(coverage areas) and more cell towers, which required less battery power. By the late 1990s, mobile phone subscriber rates reached a tipping point, transforming the mobile phone from a fashion statement into a commodity item.

It wasn't just about the technology and mobility, however. Mobile operators were determined to get a return on investment (ROI), and they pushed innovation in service and marketing to the limits. Prepaid mobile subscriptions became available and were instantly popular. But one protocol in particular would transform the mobile phone into a must-have device: **Short Message Service (SMS)**. SMS was a simple text-message format of less than 120 characters that was initially designed for use by network engineers to communicate with each other over a back channel. However, it soon proved to be a "killer app." SMS was adopted first by young people, who, much to the surprise of carriers and parents, used their phone almost exclusively for text communication rather than voice communication. Eventually, adults became regular users of SMS and "texting" became a standard method of quick, cheap, and easy communication.

Mobile telephony created advances in radio wireless technology that enabled the proliferation of 2G mobile networks. It was those same developments in radio technology, combined with the public's demonstrable desire for mobility, that transformed the modern data network. Suddenly, **wireless local area networks (WLANs)** became the hot topic in wireless mobility, and the possibilities seemed endless.

### Computers Go Mobile

Outside the enterprise workplace, mobile data communication was becoming commonplace. The availability of affordable, easy-to-configure WLAN routers conditioned Internet users to expect wireless connectivity. This was reinforced when local hotspots sprang up in shopping malls, cafés, restaurants, bars, airports, and even sports stadiums. Home users rushed to buy WLAN access points and routers, as this enabled them to create a WLAN for all devices to connect throughout the household. The fact that one could easily build a WLAN that covered the entire home without having to run or hide cables was a huge selling point. It reduced the effect of the WLAN's lack of performance compared to a wired connection.

In addition to performance issues, WLANs presented new security risks. It was perhaps not surprising, then, that when WLAN vendors tried to push into enterprise markets, information technology (IT) security and network managers were less than excited at the prospect of using them. In fact, most were very much against it. The problem was, users were to beginning demand access from anywhere in the office, especially in conference rooms. When IT managers said they would not support wireless connections, many people simply connected their own WLAN routers to an Ethernet port, creating their own rogue access points. This was a huge problem for IT, which rightly set harsh rules against it.

In the end, however, it was too much to fight. User demand simply overwhelmed IT departments' resolve. Consequently, after 2005, businesses gradually started to roll out WLANs in areas where temporary network connections were a convenience rather than a necessity. These areas—reception areas, meeting rooms, cafeterias, and recreational facilities—could be supplied by wireless access points. From a purely functional perspective, this proved to be an ideal use of the technology, as people using their portable devices in those areas would typically not require high throughput, anyway. Rather, they would more likely than not just be checking e-mails or using an instant message application.

On the horizon, though, an even more disruptive technology was rolling in: 3G Mobile IP broadband. This new technology promised to have an even larger footprint—one that could truly be described as “ubiquitous mobile access.”

## The Convergence of Mobile and Data Networks





Previously, data communications were performed over mobile networks with an extension to the 2G CDMA network using a wideband version of CDMA and other techniques. These technologies were simply expansions on the CDMA and GSM standards developed to enable low-bandwidth voice-over-circuit-switched paths. While they did allow data transfers, these technologies were barely sufficient for access to even low-resolution Web pages using Wireless Access Protocol (WAP) sites and text-based Web services. Not surprisingly, these didn't get much traction due to the restrictive data rates and the lack of suitably designed content.

Advancement came in the form of **General Packet Radio Service (GPRS)** or 2G+, a packet-based data service for mobile networks, which made steady improvements on mobile data rates. With improved data rates, the next iteration of GPRS, GPRS+, became the first feasible way to access the Internet over mobile networks.

The introduction of 3G, however, removed any doubt as to the ability of mobile networks to facilitate high-speed packet-switched Internet access. Its fast download speeds and connection rates made 3G an extremely convenient way to connect to the Internet. Suddenly, a technology that had appeared stalled after 10 years with little improvement found its market. The new 3G took off spectacularly with the advent of a new breed of smartphones. Full high-speed Internet access over mobile networks quickly became consumers' expectation.

Mobile operators keen to leverage their products launched 3G wireless access points and routers for remote sites where no wired or radio backhaul existed. Laptops became truly mobile, thanks to the use of 3G **subscriber identification modules (SIMs)** for access anywhere, anytime. This newfound mobility brought a new product to the market: lightweight netbooks designed specifically for Internet access over 3G.

After 3G technology came Long Term Evolution (LTE), which offers an all-IP mobile network. This 4G technology is currently the predominate mobile offering. Figure 1-2 shows the generations of mobile technologies.

 <p><b>1G</b> <b>1st Generation Wireless Network</b></p> <ul style="list-style-type: none"> <li>• Basic voice using analog technology</li> </ul> <p><b>2.4 kbps</b></p>	 <p><b>2G</b> <b>2nd Generation Wireless Network</b></p> <ul style="list-style-type: none"> <li>• Voice using digital technology; very basic data transfer</li> </ul> <p><b>64 kbps</b></p>	 <p><b>3G</b> <b>3rd Generation Wireless Network</b></p> <ul style="list-style-type: none"> <li>• Digital voice and mobile broadband</li> </ul> <p><b>2,000 kbps</b></p>	 <p><b>4G</b> <b>4th Generation Wireless Network</b></p> <ul style="list-style-type: none"> <li>• Voice and IP-based protocols for data transfers 10 times faster than 3G—LTE</li> </ul> <p><b>100,00 kbps</b></p>
--	--	---	---

**FIGURE 1-2**

Advances in successive generations of mobile technologies led to major leaps in voice quality and networking speeds.

Mobile telecom operators were not alone. Other wireless technologies, such as satellite and WiMAX, were making an impact. These provided high-speed Internet connections over a wide metropolitan area or even an entire continent.

By the turn of the decade, security professionals' worst fears were coming to pass. Mobile IP wireless technology had finally come of age and was accepted, not only as an access medium inside the network, but as a method for remote access from anywhere across a wide variety of devices and access types. Worse from a security standpoint, in 2012 Mobile IP became a business strategy after users demanded that IT support their mobile data devices. Despite IT's well-founded security concerns, the business benefits—along with overwhelming demand to use one's own personal device rather than one assigned from IT—led to the birth of the bring your own device (BYOD) phenomenon. BYOD caused a major shift in IT policy.

#### NOTE

Satellite technology uses low-altitude satellites that relay information from terrestrial stations. Download rates are not bad, but data uploads can be very slow and consume a great deal of power. The advantage of satellite technology is that it can be used almost anywhere. **Worldwide Interoperability for Microwave Access (WiMAX)** is a method of providing wireless broadband access for voice and data.

## Business Challenges Addressed by Wireless Networking

Wireless networking addresses several challenges thanks to its inherent ability to allow network access without the hindrance of cables. The most obvious benefit is that areas considered for WLAN deployment do not require a cable run to each desk or print station.

This is a major savings in time and effort. Moving cables and activating sockets is a considerable burden in any installation, office move, or reshuffle. With WLAN, there is no

need to worry about cabling. You can put desks and network printers wherever you want. There is also a significant cost savings, particularly in new installations where the savings on Ethernet cables alone can be substantial.

### NOTE

A Wi-Fi device is generally any device based on the IEEE 802.11 standard. But the term is often used to describe any WLAN-capable device (most of which are 802.11 compatible). The terms Wi-Fi and WLAN are often used interchangeably. The Institute of Electrical and Electronics Engineers (IEEE) develops global standards for a wide range of technologies. The 802 standard pertains to local area networks and the .11 extensions define standards for WLAN.

Other important benefits respond to some less obvious business challenges. These benefits relate to the WLAN's ability to provide network access over a large area, which allows freedom of movement and unrestricted access to all areas within coverage. The challenge is to cover the whole workplace in such a way that users can roam from one area to another without dropping a signal or losing a session. This is very similar to the way mobile phone users can roam from one cell coverage area to another with a seamless radio handover of the call. The goal of IP mobility is to provide the ability to roam while maintaining network access anywhere on the premises and on any WLAN- (commonly referred to as **Wi-Fi**) enabled device.

The benefit of this mobility is more obvious in some industries than in others. For example, in the retail sector, wireless-enabled tablets or smartphones allow shop-floor assistants to move about the store assisting customers while retaining an active mobile data and Internet connection. This gives them immediate access to stock information, prices, and all the relevant data they require anywhere in the store, greatly improving both efficiency and customer satisfaction.

Logistics is another example. In logistics, mobility makes stocktaking in large warehouses far easier, as workers have data entry and stock lists at their fingertips on tablets or smartphones. This ability to provide a data access connection anywhere, whether temporarily or permanently, makes Wi-Fi the perfect solution to data access and connectivity needs.

Moreover, WLAN and wireless access make communications more effective and provide workers with greater access to network resources while outside the office. Wi-Fi hotspots are commonplace. Combined with mobile phone technology such as 3G and the like, access is available practically anywhere, and for a wide range of devices from laptops to tablets to smartphones. Now employees can access and respond to e-mail or use network resources 24 hours a day, 7 days a week, without having to go into the workplace. This may not be great for employees' work/life balance, but it's a big win for business productivity.

Along with productivity and efficiency improvements, wireless access makes possible improved collaboration, impromptu data sharing, and brainstorming sessions within informal groups. Typically, this would have required finding a suitable meeting room or free desk with the required number of network ports. (This alone might normally be enough to stall the initiative!) However, with WLAN technology, team members can simply find a free table nearby or in the cafeteria and use their laptop wireless connections.

Additionally, comprehensive Wi-Fi coverage in the workplace has made Voice over Internet Protocol (VoIP) a more efficient communication tool. Users are no longer restricted to a wired IP desk phone or fixed computer VoIP soft phone. With Wi-Fi access, an administrator can configure a user's smartphone as a VoIP internal extension phone. The **IP private branch exchange (IP PBX)** software can then track it as the user roams around the workplace. That way, the user will never miss an important call, whether internal or external. When the user steps outside the WLAN's boundaries, the IP PBX can automatically redirect calls to the user's mobile (cell) phone number.

These are some of the more obvious ways that WLANs remove barriers to effective communication, impromptu collaboration, and brainstorming sessions. This makes communication and innovation more efficient and effective within the workplace.

Certain aspects of WLANs that were once seen as security issues—namely the access control and authentication techniques found on all WLAN controllers (discussed later in this chapter)—have been robustly addressed and are now the envy of any fixed network administrator. By moving access control and configuration from the wireless access points to a central controller, vendors have given administrators much greater control over smaller pieces when creating, implementing, and administering access and authentication policy. The result is that as the technology has matured, elements of wireless networking that network administrators once considered major drawbacks have become strengths.

## IP Mobility

The number of mobile wireless devices is projected to surpass the number of fixed devices sometime in 2015 or 2016. The growth and adoption rates of smartphones and tablets have created huge demand on mobile operator data networks, with data traffic rates growing upward of 115 percent compounded per year since 2011. The public's and business's adoption of smartphones and tablets has been so fast that manufacturers of fixed PCs and desktop computers are seeing slumps in their sales for the first time since the PC market emerged in the 1980s.

The shift toward wireless mobile devices has presented businesses with many opportunities and challenges—most notably, the challenge of how to make best use of new mobile wireless technologies. After all, networks have been designed and secured with static devices in mind. When LANs were designed, it was assumed that employees would be at a desk within a department. The network was segmented accordingly via subnets to accommodate physically present numbers of employees and allow for future growth. The emergence of WLAN technology was used to address any unexpected growth. However, the growth in the number of IP-capable wireless devices means that employees are now far more mobile and can work from anywhere in the network or even from outside the network—at home or at a client's site.

### NOTE

A *private branch exchange (PBX)* is a switch used to connect internal phones in an enterprise to the PSTN. An IP PBX is a PBX that allows the use of VoIP over the PSTN.

This has proved to be very productive for business and has created tremendous improvements in employee efficiencies and communications. Laptops, smartphones, and tablets can be used in any location where there is a WLAN or 3G network connection. These devices can also roam around the workplace LAN, connecting to the WLAN wherever there is a signal. If the WLAN is one single subnet, users can maintain application and Web browser sessions.

The ability to roam and maintain an IP session is fundamental to true IP mobility. Ideally, the wireless device must not only be usable in any location, it should also be usable when in transit between locations and even between IP and mobile networks. This presents a significant problem: When moving from one network or subnet to another, the device will require a change of IP address. However, if the IP address of the mobile device changes, all its current sessions will be lost, and applications will hang and crash.

What is required is a method to allow the seamless transfer of an IP address from one network to another without losing IP sessions. Only then will there be true mobility with roaming using IP wireless devices. This is termed *IP mobility*. The International Engineering Task Force (IETF) uses the term **Mobile IP** to describe its standard communications protocol for addressing this problem. It does so preserving existing sessions as a device moves to a network with a different IP address space. Because this function is performed at the Network Layer of the Open Systems Interconnection (OSI) Reference Model rather than at the Physical Layer, a device can span different types of wireless and wired networks while maintaining connections and application sessions.

Another goal for the Mobile IP standard is for a device to be able to cross not just network boundaries, but technologies as well. Ideally, the device should transparently connect to any technology it can support including wired, wireless, and 3G/WiMAX networks.

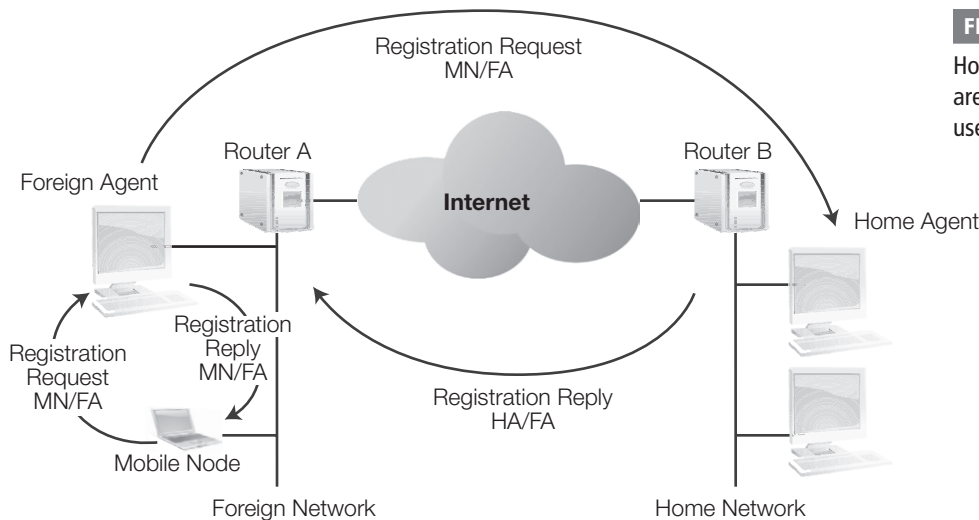
In a nutshell, with IP mobility, any compatible device that communicates at the Network Layer can roam from a fixed Ethernet to a wireless Ethernet to a mobile (cell) network without any loss of session and only a noticeable change in the access speeds, if that. There is no need to restart or reboot the OS, as the Network Layer handles it all seamlessly.

Mobile IP handles the change of IP address and maintains current sessions by using certain Mobile IP client stack specific components. These are as follows:

- **Mobile node (MN)**—A *mobile node* is a device (it could be anything) that changes its point of attachment from one subnet or network to another. It does its own move detection and must determine not just the change in access type, if any, but also the change in the subnet.
- **Home address**—The *home address* refers to the mobile node's home IP address, which is where it is registered with the home agent. The address can be static or dynamically assigned when registering with the home agent.

- **Home agent (HA)**—The *home agent* is a router capable of processing and tracking mobile routing IP updates, tracking mobile node registrations, and forwarding traffic to mobile nodes on visited networks through IP tunnels.
- **Care-of-address (CoA)**—The *care-of-address* is the new IP address the mobile node has been assigned by the visited network. The mobile node informs the home agent of the care-of-address when registering its movement.
- **Foreign agent (FA)**—The *foreign agent* stores all information about mobile nodes that are visiting its network. It advertises care-of-addresses and routing services to the mobile node while it is visiting its network. If there is no foreign agent present on a network, then the mobile node itself must handle getting a local address and advertising it.

Mobile IP enables a wireless device to traverse different network types—fixed, wireless, and cellular—while maintaining session and application status. It provides for transparent handover and supports different access types and IP subnets through the use of IP tunnels from the home network to visited networks. This not only enables wireless devices to work on different networks, but it allows them to be seamlessly accommodated without any drop in service. This is true IP mobility. It facilitates real roaming of wireless devices in which the device reconfigures itself automatically and registers with another network type and IP address while the user works without any interruption. Figure 1-3 shows how Mobile IP sessions are maintained as the user moves around.

**FIGURE 1-3**

How Mobile IP sessions are maintained as the user moves around.

## The Impact of Bring Your Own Device

One of the biggest influences on wireless and mobile security is the **bring your own device (BYOD)** trend that has swept through many businesses in the past few years. Although the idea that an employee would use a personally owned device to access work-related systems, files, and applications was once unthinkable, it is now not only normal—it has become the expectation. This section takes a look back at this evolution in IT policy.

### Common Operating Environment

#### NOTE

The Y2K concern was not without justification. As it turned out, it was over-hyped. Nonetheless, in hindsight, a lot of good came out of the effort to prepare for the event.

In the years leading up to the new millennium, IT departments around the globe were facing the threat of impending doom from the Millennium bug. The Year 2000 (Y2K) threat, as it was known, was not a virus or Trojan attack, but an inherent weakness in the way programmers in the past had coded the date format for years as a two-digit number. The fear was that older programs would crash when the two-digit date format rolled over from 99 to 00 because the system would think it was the year 1900 instead of the year 2000. To ensure Y2K compliance, and to facilitate efficient and standard validation, IT departments implemented what some called Draconian measures known as the **Common Operating Environment (COE)**.

COE was all about the control IT had over any technology used within a business. With COE, IT stipulated a common desktop PC policy; a common, stripped-down, and locked OS; and a select menu of authorized applications. The benefits to the business—or rather to IT—were quantifiable and undeniable. They included the following:

- Much lower support costs
- Improved help desk and IT support
- Thoroughly tested applications working on a common platform
- Fewer major virus contaminations
- Reduction of compatibility issues with OS versions, security and OS patches, and device drivers
- Higher user satisfaction due to preconfigured network printers, home drives, and network configurations

Due to its undeniable success, even after the Y2K threat had passed, the COE model remained. But fast-forward a decade and a half to 2014, and things had gone full circle. Control had been wrested from IT and security departments and placed back into the hands of users. BYOD, which arose seemingly from nowhere, had been embraced by CEOs and CIOs alike, much to the chagrin of the IT and security departments. How did this curious turnaround happen?



**CHAPTER 1** | The Evolution of Data Networks

BYOD is certainly a curiosity, as it flies in the face of everything known about creating and managing efficient and secure networks. COE advocates argue that BYOD is especially bad, given COE's success over the years. But it turns out that COE had a few downsides as well.

- **It irritated employees**—With COE, employees could not customize their desktop and use their own wallpaper and screensaver. They had to make do with the uniform company logo. This might seem like a trivial point, and initially it was treated as such. But it wasn't. The removal of the basic freedom to customize their own workspace, even to the point of arranging their desktop icons, had a serious negative psychological effect on employees. Not surprisingly, they took it to be a demonstration of a lack of trust and confidence in their ability, which affected their motivation and goodwill. This was especially the case with knowledge workers such as engineers, who often saw themselves as more technically savvy than IT personnel.
- **It caused anger and resentment toward IT**—Even though IT did not devise the strategy, employees blamed IT for implementing this corporate tactic. This resentment came about in part because employees perceived IT as having upset the natural order. In any traditional bureaucratic business, there is a natural hierarchy. Profit-producing departments, known as line departments, trump service and support departments. Line departments bring in the money and are indispensable to the business model, while support departments are there for one reason only: to assist the line departments. By implementing a COE policy, IT was seen as usurping the natural order, which created resentment, even (if not particularly) among senior line managers.
- **It stifled productivity**—Yes, IT and help desk performance improvement went through the roof. But other departments, especially line departments, soon found their performance heading in the other direction. Why? Because forcing line employees such as engineers, developers, designers, and sales executives to use only authorized applications on authorized desktop hardware prevented them from working the way they wanted to work. Previously, they used whatever application they were happiest with to do their own individual tasks. Engineers had specialized programs they had taken from university—sometimes even based on Microsoft's old Disk Operating System (DOS)—that they used on a daily basis. The same was true of developers, designers, and sales teams. COE restricted the way the most productive and important staff went about their daily tasks. As a result, it was ultimately considered by those outside IT to be a failure.

The counterpoint to this is that users often did dumb things that put the network at risk, such as downloading unstable programs or screensavers with viruses. Also, when users' custom configurations stopped working, they called on IT to fix them, even if they were not officially supported. Repeat this with 1,000 users, and you end up with an impossible support requirement.

In the final analysis, COE was a much-needed and overall positive innovation for IT and for business. Most opponents of COE are similar to fast drivers who ignore speed limits because they “know how to drive fast.” The problem with this, however, is that many people do not know how to drive fast, and the rules are there to keep everyone safe. As the saying goes, an ounce of prevention is worth a pound of cure. COE is that ounce of prevention.

## BYOD: An IT Perspective and Policy

BYOD is the polar opposite of COE. It has revolutionized the way individuals work by allowing them to manage their own work methods. By allowing employees to use the tools they feel best suited to the task—their personal high-tech devices—BYOD removes the burden of training and encourages collaboration and innovation.

In addition, many business-supported programs, including software for sales-force management and expense management, now have apps that run on user devices. This reinforces the use of these devices in the workplace. For that reason alone, BYOD will stimulate motivation, innovation, and creativity within the workplace.

You might think of BYOD as the consumerizing of IT, in which employees are empowered to select and use whatever personal hardware or software they believe best fits the job. But it's not about having the right to choose your own hardware and software and then having IT supply it. Rather, BYOD is about employees using their own *personal* devices, with the understanding that when they leave the firm, the device and most of its contents (such as contacts) leaves with them. Proponents of BYOD suggest that this ownership yields cost savings for the business—in particular, for the IT budget. Opponents counter that those savings are minimal at best, and are counteracted by the extra spending required to support and secure these new devices.

### Support Issues

On the support side, it is true that this escalation in costs does occur. IT and help-desk performance are directly related to the variety of hardware and software under those departments' care. So having an unrestricted variety of devices will have a serious effect on IT and help-desk performance. For example, it might take just a few seconds to configure a COE device for company e-mail. Not so with some new unknown smartphone.

### Security Issues

The security side is of greater concern. How can employees' devices be secured? And more importantly, how can IT be responsible for the company's data, yet have no control over the devices that join the network? Finally, what is the line between acceptable and unacceptable usage? For example, it's clear that visiting adult Web sites, many of which are known to be sources of malware, is against company policy on a company device. This is a clear line. But where is the line for a user visiting such a site at home on his or her own time, with a device that he or she owns, but that he or she also uses for work?

**CHAPTER 1** | The Evolution of Data Networks

The common BYOD solution is to have employees agree to configure their devices to meet an acceptable security level before they may join the network. This requires, of course, a BYOD policy and acceptable usage policy. Fortunately, many employees claim to be willing to sign on to such policies.

But these devices are not just connecting to the network. They are transportable. That is, they pass outside the boundaries of the business every day and into the domain of a personal-use device. Almost certainly, these devices have company data stored in them. And therein lies another issue: What access should these devices have on the company network if they are active on non-company networks on a daily basis? A common argument is to give employees the same access they would have on their desktop. From a security standpoint, however, that's not acceptable. There's a big difference between a desktop PC and a smartphone or tablet. Employees don't pack up the central processing unit (CPU) each night and take it home with them.

On a similar note, there is the worry about leakage of company data from these devices. If people leave the company or lose their phones, the assumption is that the IT department can completely wipe the phone remotely. But is that going to be acceptable to the owner? Even if the owner *does* support such a policy, it's highly unlikely he or she would report a missing phone in a prompt manner, as IT is likely to wipe the phone—which likely includes all manner of personal data, such as family photos and contacts—before the owner has given up hope of finding it.

Proponents counter these arguments by pointing toward mobile application management (MAM) and mobile device management (MDM) solutions that have recently come to market. As the names suggest, these solutions allow IT managers to place restrictions on either the workplace applications (MAM) or on the device itself (MDM) to ensure that user behaviors do not compromise company access or security. These applications do a good job if the device's owner agrees to IT basically locking it down. But how often will that be the case?

**BYOD: The Employee's and Employer's Perspective**

From an employee's point of view, what's the advantage of the BYOD approach? After all, few employees would be willing to submit their car for company use free of charge—let alone allow the company to make changes that affect the vehicle's functionality. How is a device like a smartphone or tablet any different? Yet, many employees do seem willing to submit their devices to reasonable security measures.

On the other hand, what's the benefit of BYOD for employers? As mentioned, BYOD does result in improved employee job satisfaction and morale. Many argue that BYOD also increases productivity. But is that really the case? Or does it just represent a blurring of the boundaries between work and personal hours? Employees might view being able to receive and reply to work e-mails at all hours of the day as an invasion rather than an improvement in productivity. (Of course, this is a two-way street. Managers who send e-mails outside of normal business hours and expect a reply can't really take issue with employees who occasionally take time out of their day to catch up on Facebook.)

### A Third Option: Corporate Owned, Personally Enabled (COPE)

Some people say that the popularity of BYOD among employers has to do with perceived savings in capital expenditures and operational expenditures. That is, because employees provide their own devices, the company doesn't have to—thereby saving money. (Of course, some companies reimburse employees for their devices, thereby nullifying this advantage.) But there's a risk. What if an employee fails to pay for his or her service, and is disconnected? In such a scenario, who is responsible for the interruption in the employee's communication and productivity?

Fortunately, there's a third option: **corporate owned, personally enabled (COPE)**. In this model, the company buys the device and pays for all the operational charges associated with it, but the employee is free to use the device for personal business. To many, this makes more sense for these reasons:

- The company can often purchase devices at a far cheaper price per unit.
- By the company's taking responsibility for the maintenance and operational costs, there is no doubt who owns the device and who is responsible for service.
- The company has the freedom to place whatever security restrictions it feels are necessary without conflicts of interest. This freedom facilitates the adoption of MAM and MDM within the network, thereby securing the company's data and information both technically and legally.

At the same time, COPE offers all the positives for the employee. Employees get the device they want, the company pays for the service, and employees can use the device for personal business. The only drawback is that it isn't theirs to swap, sell, or trade for the latest model (which could be a stumbling block for users who want to have the latest and greatest gadget).

Both the BYOD and COPE models blur the increasingly fluid boundaries between work and play, between business and personal use, but that is a price that both parties appear willing to accept. Indeed, younger workers in particular seem perfectly happy to merge the two.

The popular consensus is that allowing employees to use their own devices, laptops, smartphones, and tablets at work—whether purchased by the employee or by the company—is sound policy, despite legitimate security concerns. If the happiness and productivity of the workforce is the primary goal, then proponents of BYOD and COPE may well be correct.

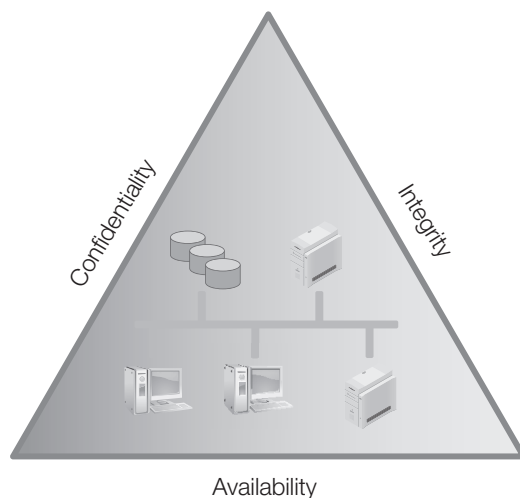
Others see it differently, however, as the IT and security departments are undeniably responsible for safeguarding the network and the company's data. For the IT department, securing the company's valuable information is paramount. As such, many IT professionals consider the potential for security breaches with the BYOD and COPE models to be an unacceptable risk.

Mostly it comes down to what the company determines is acceptable risk. In a technology or service company, the added productivity and employee satisfaction may carry the argument. In a financial services company, where a security breach could have a devastating impact on future revenues (not to mention result in regulatory fines), security concerns far outweigh employee preference.

## The Basic Tenets of Network Security

One of the core principles of network and data security is the **C-I-A triad**. Figure 1-4 illustrates the C-I-A triad. C-I-A stands for the following:

- **Confidentiality**—Confidentiality involves maintaining the privacy of information so that only those who are authorized to access the information are able do so. Confidentiality is most often achieved through encryption and cryptography, which protect data when it is stored or when it is transmitted across the network. Common methods of providing confidentiality over the Internet are Hypertext Transfer Protocol Secure (HTTPS), which encrypts data between secure browsers and secure Web sites, and Secure Sockets Layer (SSL), which uses 128-bit encryption between a safe HTTPS Web site and a safe browser. These techniques are frequently used in online banking and e-commerce.
- **Integrity**—Integrity is concerned with the accuracy of the data—that is, ensuring data remains unchanged or is not tampered with. Maintaining integrity involves using techniques such as mathematical message-digest (or hashing) algorithms to verify data integrity. This message-digest guarantees that if the identifier or message-digest is the same before and after transmission, then the document has not been tampered with. Correspondingly, if the message-digest differs, even if by only one bit, then the integrity of the document is in question.
- **Availability**—Availability involves ensuring that data will be available only to authorized viewers. It can also relate to services, in that a network service, such as e-mail, will be available when required. Availability is provided for through security measures such as firewalls or high-availability network designs for redundancy and fault tolerance. Typical attacks on availability are denial of service (DoS) attacks and brute-force password hack attempts (to gain access to data or configuration files).



**FIGURE 1-4**

The C-I-A triad illustrates the self-reinforcing components of confidentiality, integrity, and availability.

C-I-A (sometimes referred to as A-I-C) applies across all levels of security. If any element of the triad can be compromised, this could lead to serious consequences up to and including a security breach.

Network security is predominantly focused on vulnerabilities and attacks on network protocols. There are other components to network security, however. These can include dealing with vulnerabilities in servers, operating systems, and applications. These security issues must be considered in their own right as part of a holistic network security viewpoint.

Traditionally, network security has taken a layered approach:

- Web servers, which are exposed to the Internet, are positioned in a “demilitarized zone” (DMZ) of sorts, or a low-security area. After all, the Web servers must be available on the Internet if they are to be accessed. The idea is to place the Web servers behind an Internet-facing firewall that has only the required service ports open, such as HTTP 80 and SSL 443. This restricts traffic to only that which is necessary. In addition, a host-based intrusion prevention agent is often on the Web server.
- Application servers, which need to interface with Web servers, are kept behind a layer of inner firewalls. This protects the company from any threats from the DMZ. Again, only the necessary ports are opened to allow authorized communication between the Web servers and the application servers within.
- Inside the firewalls, on the company network, servers, databases, and desktop machines are segregated into isolated subnets, which are separated by routers. Access lists are often applied to the router interfaces to restrict traffic into and out of each subnet.
- Within each subnet, the individual hosts are connected through LAN switches, which are OSI Layer 2 intelligent devices. Unused ports on switches are shut down. This prevents someone from plugging an unauthorized computer into the network switch to gain access to the network. Typically, administrators restrict physical access to switches by placing them in locked cabinets.
- The operating system and Web applications are “hardened” with software updates, security patches, and appropriate settings to address any known vulnerabilities.

This design reveals one obvious inconvenience, however: How do you cater to guests or temporary workers? This has been a problem. The cabled Ethernet ports determine where people can be located. It’s not convenient to go looking for a network technician to configure and activate a port for a visitor.

A common way this is addressed today is with virtual local area networks (VLANs). A VLAN is a logical segmentation of a physical LAN that allows for flexible configuration and access rules to be applied to individual devices. VLANs provide another layer of security with network segmentation but don’t compromise a layered approach.

The alternative has been to use radio access points to connect a guest's laptop to the network. However, these WLAN devices have been considered inherently insecure—although they *could* be placed in an Internet-only partition of the network. Then they could at least be segregated from the corporate LAN. In most cases, this is just what businesses do—they simply provide a direct connection to the Internet that is separate from the corporate networks.

## The Evolution of Cybercrime

**Cybercrime**, which refers to a wide range of illegal activities performed on a network, has existed since the earliest forms of electronic technology came on the scene. The first cybercriminals were **hackers** who emerged in the 1960s. Unlike the anarchists, cyberthieves, and terrorists of today, these “mischievous trespassers” were often educated technologists who investigated and researched the PSTN telephone network. These hobbyists spent countless hours re-engineering the audible signals used by the telephony system to switch calls.

Eventually, they discovered that they could re-create the exact tone to send through the handset, which gave them access to the international exchange—free of charge. Although some people viewed these types of activities as victimless crimes, the people committing these acts were undoubtedly stealing a service from the provider. Many justified their actions as taking a stance against a monopoly supplier who they believed offered an overpriced and substandard service. But their real incentive was simply to be the first to use their technology skills to circumvent a service provider's security. In fact, most early security breaches were done solely for the purpose of establishing a reputation among other hackers—essentially, for bragging rights.

Eventually, however, bragging rights were not enough. Soon hackers began sharing the steps they took to compromise a system so they could be repeated. This culture of sharing greatly accelerated the acquisition of hacking skills by new hackers and the community as a whole. This attitude persists even today—so much so that the hacker community is far more efficient at information dissemination than most IT teams in large corporations.

In the United States, cybercrime was legally recognized as a federal criminal offense in 1986. The following year, the U.S. government formed the Computer Emergency Readiness Team (CERT) to counter the rise in cybercrime. The ensuing years saw a spate of criminal activity that resulted in the first known—though perhaps accidental—release of a computer worm, which brought the ARPANET to its knees. Far more scandalous was the first successful cyber bank robbery, in which the Bank of Chicago was robbed of nearly \$70 million dollars through a fraudulent computer transaction.

As the Internet became more prevalent, criminals shifted their focus to the common person, who was far less likely to be security conscious than corporations or government organizations. The mass sending of marketing e-mails, called **spam**, became prevalent. Spam was quickly followed by **phishing**, in which cybercriminals tricked unsuspecting users into revealing personal data such as account passwords by sending fake e-mails from what appeared to be legitimate companies. In the 1990s, **viruses** (malicious programs) and **worms** (malicious self-replicating software), spread via e-mail and Web sites, caused mass contagion and gave the public a taste of what was to come.

Over time, the definition of hacking changed. Hacking is no longer about proving one's skill. Now, hacking is simply running a script for illicit profit or ill intent. Unlike in the past, when hackers attacked worthy opponents—businesses that were of equal strength—hackers now distribute tools that enable those with little skill or knowledge, called **script kiddies**, to do significant damage. These days, there's a veritable army of these attackers infiltrating organizations on a daily basis.

## Wireless Network Security

### NOTE

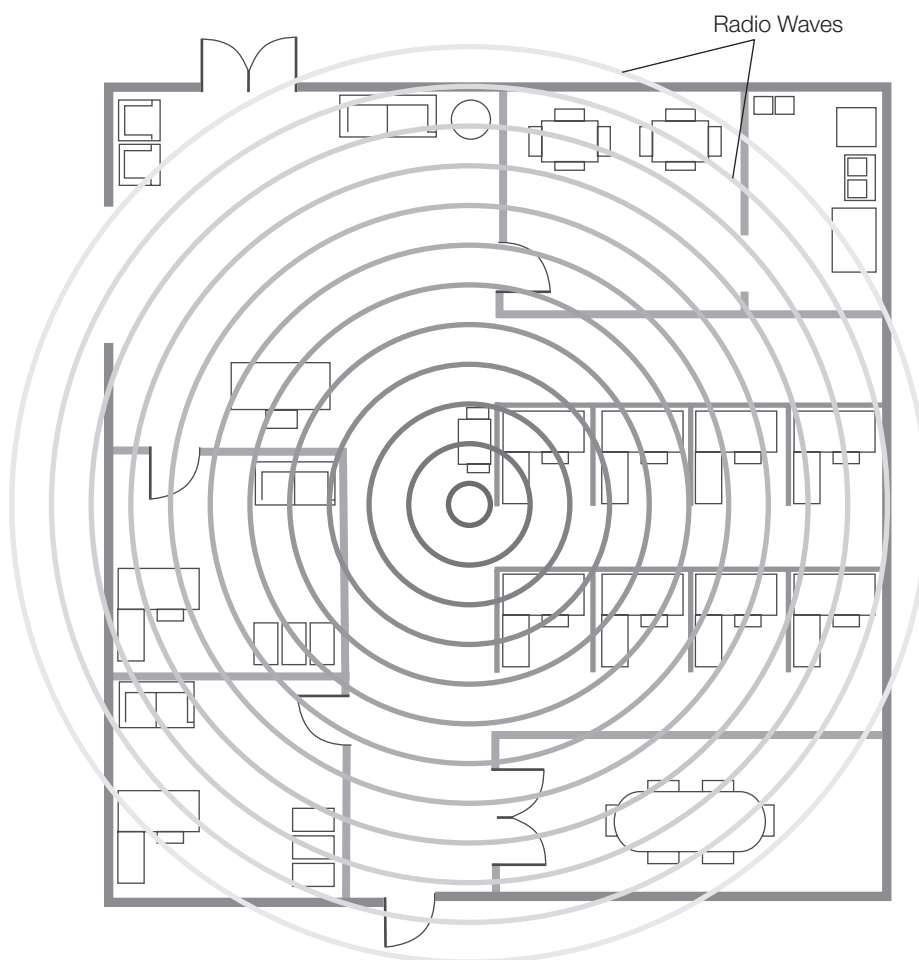
For an attacker, being able to hide one's identity is paramount. This is why they use The Onion Router (TOR) and other tools to disguise their source location IP address. However, with an unsecured WLAN, an attacker can simply connect, safe in the knowledge it won't be his or her door that gets knocked down during a pre-dawn raid.

Historically, WLAN technology has been viewed by security professionals as convenient but inherently insecure. This is because early WLAN implementations, often found in small office/home office (SOHO) environments, were typically installed by technicians who were not knowledgeable about radio technology or security. The result was unauthorized users poaching the network—that is, using its bandwidth without permission. Worse, some users would gain unauthorized access to the data on the network, even injecting or forging data.

Of particular concern was the use of omnidirectional antennas with wireless networks. With such an antenna, the wireless access point broadcasts to anyone in the vicinity who has a receiver, whether they are authorized to access the network or not. As shown in Figure 1-5, this area can and often does extend beyond the physical walls of an office or building. This puts the network at risk. Another risk with wireless networks is intruders using directional antennas to eavesdrop on the network, even from quite some distance away.

With these problems in mind, the IEEE set out to develop a security standard as part of the 802.11 standard. The goal was for WLANs to be considered as secure as their wired equivalents, allowing confidentiality, integrity, and availability. Unfortunately, early attempts to secure WLANs proved to be flawed.



**FIGURE 1-5**

Omnidirectional coverage areas can extend beyond an office's walls.

One problem was the way in which devices were authenticated. (Authentication was necessary to prevent intruders from masquerading as a valid device on the network.)

Another problem pertained to the inherent weakness in the security algorithm used in the 802.11 standard, called **Wired Equivalent Privacy (WEP)**. With WEP, each device shared a common key for authentication and encryption, which used a challenge/response mechanism. An eavesdropper, however, could intercept the challenge and response. Although the response was encrypted, the challenge was not. The attacker could simply capture and replay the response to successfully respond to a challenge and in doing so could gain access to the network. Exploiting WEP's weakness, hackers stole 94,000,000 credit card numbers from the TJX Companies' corporate network between 2005 and 2007.

In response to WEP's inherent weaknesses, the Wi-Fi Alliance introduced **Wi-Fi Protected Access (WPA)**. Unlike WEP, which used a 64- or 128-bit key, WPA used a 256-bit key, which is much more difficult to break. In addition, WPA featured integrity checks, which ensured that the message had not been tampered with en route to or from the access point. Unfortunately, even these advances were not enough, as WPA was proved to be breakable. However, WPA served as the interim replacement for WEP until **Wi-Fi Protected Access 2 (WPA2)** was developed as the permanent replacement.

#### NOTE

Encryption and strict access control can secure most networks from unauthorized use. If an authorized device falls into the hands of an attacker, however—for example, if a laptop is lost or stolen—then the attacker has all the information and configuration needed to beat the encryption and even the strictest access control.

Today, the security of wireless networks is not the issue it once was. Many of the broken security mechanisms have been replaced or updated. The three tenets of security—confidentiality, integrity, and availability—have been addressed through robust encryption algorithms using the WPA2 security protocol, which can also cooperate with business authentication services such as Radius to control network access.

From a security standpoint, it also helps to limit the broadcast range of the network to the boundaries of the property. This may mean scaling back the transmission power—although many users seem averse to this, preferring to boost the power to the maximum to increase range and improve performance. This can be counterproductive, however. Not only can it interfere with other WLANs on the same radio channel, it greatly increases the network's footprint, making it more desirable for an attacker.

### Lingering Security Issues

Although there have been considerable advances in WLAN security, network and security managers still cast a suspicious eye over anything wireless. And to be fair, wireless networks do give cybercriminals additional opportunities.

Because WLAN technology is so simple it's almost plug and play, it has become popular among homeowners and hobbyists, many of whom are not aware of how or why such networks should be secured. Indeed, the public appears to be more concerned with getting the most powerful WLAN for performance rather than security. As a result, many WLANs are essentially wide open, giving cybercriminals the next best thing to physical access to people's computers. People might as well leave their front doors wide open!

This has spawned, among other things, a behavior called **wardriving**. An evolution of the old *wardialing* techniques used by **phreakers**, people who exploit bugs to locate computer networks on the PSTN, wardriving is the act of driving around looking for unsecured WLAN access points due to simple curiosity or in an attempt to gather information for a later attack. WLAN technology has given criminals easy access to networks they can use to engage in activities that range from poaching bandwidth, to accessing data, to launching nefarious campaigns without fear of repercussions.

## Mobile IP Security

Until the latter part of the first decade of the 21st century, mobile phones were predominantly voice only. Yes, people could use them to send text messages and download ringtones and wallpapers, but that was about it. There was only limited support for data—and at rates and throughput that were prohibitive.

The advent of 3G networks made high-quality Internet access from a mobile device a reality. Such was the rush for mobile Internet communications that data traffic now supersedes voice traffic on telecom providers' networks. With data networking as the new cash cow, telecom providers have focused their strategy on delivering high-speed data transport and services.

Unlike previous devices, however, these new 3G devices could not be locked down. Now the owners of these devices could download applications that used any nearby WLAN to send and receive data, bypassing the telecom operators' expensive data plans. Providing free WLAN access became a great cheap marketing tool; WLAN hotspots have since sprung up in shopping malls and leisure areas across the country.

Unfortunately, cybercriminals were not far behind. They found a vast array of new victims congregated in these areas—particularly teenagers. These kids quickly discovered the joy of instant messaging and other communications over a free WLAN infrastructure, thereby becoming easy targets.

This was mostly because phone manufacturers made instant and easy access a higher priority than basic security. As such, smartphones and tablets were enabled for Bluetooth discovery out-of-the-box. The criminal element rejoiced, as they now had direct access to these devices, which they could surreptitiously use to make voice calls, send data, listen to or transfer calls, gain Internet access, and even transfer money. The full menu of Bluetooth attacks was at the attacker's fingertips, including *bluesnarfing* (in which an attacker gains access to the contacts and data stored on the phone and redirects incoming calls) and *bluejacking* (in which an attacker sends unsolicited messages to other Bluetooth devices). These types of attacks were common on 2G mobile devices with Bluetooth in 2002 and 2003.

Today, mobile phones are no longer shipped with Bluetooth enabled in discovery mode. In addition, security has been hardened to prevent unauthorized connections and remote access to the phone's features. Confidence is such that smartphones are trusted for use in e-banking, e-commerce, and e-mail. Despite these improvements in securing wireless mobile devices and the underlying radio networks, however, there is no room for complacency. Cybercriminals, who have become adept at intercepting signals over unencrypted wireless networks, are never far behind.



## CHAPTER SUMMARY

Data communication and networking have a long history, starting first with telegraphy followed by telephony. Data networks came about in the 1950s to respond to a growing demand in business to network computers together and allow for remote access. This was achieved by the use of modems. The advent of digital technology, which was cheaper and more reliable than its analog counterpart, enabled telephone companies to upgrade their networks. This innovation allowed for the development of packet switching, which enabled multiple transmissions to share a single circuit. Other developments—specifically, the creation of ARPANET and the Internet, the invention and widespread adoption of PCs, and the invention and adoption of mobile phones and computers—prompted further advances in data communication and network technology.

Initially, networks were wired. But with advancements in mobile telephony came the development of the wireless local area network (WLAN), which could be accessed by mobile users. Wireless networking addressed several challenges, but also posed security concerns, particularly with regard to access control and authentication techniques.

The rise in the use of mobile devices such as smartphones and tablets has fueled demand for wireless networks. It has likewise presented businesses with many opportunities and challenges. Mobility has become a way of life, with smartphones and tablets part of the fabric of modern society. For the generation born in the Internet era, to be denied this mobility is unthinkable. But business is struggling to deal with the inherent tension between security and accessibility. BYOD and COPE are current business strategies that strive to balance the old guard's determination to secure networks at all cost and the new thinking that puts accessibility, productivity, and mobility at the forefront.

Regardless of which approach is taken, network security has three aims: confidentiality, integrity, and accessibility. The goal is to prevent cybercriminals from unauthorized access to systems and data. The fact is, for as long as there have been communication networks, there have been people who have attempted to exploit them for their own prideful, political, or economic gain. Early attempts to secure wireless networks were unsuccessful, but many of the broken security mechanisms have since been replaced or updated. Today, encryption and strict access control can secure most networks.

**KEY CONCEPTS AND TERMS**

Advanced Mobile Phone System (AMPS)	IP private branch exchange (IP PBX)	Transmission Control Protocol/Internet Protocol (TCP/IP)
Bring your own device (BYOD)	Mobile IP	Viruses
C-I-A triad	Modem	Wardriving
Circuit switching	Network effect	Wi-Fi
Code Division Multiple Access (CDMA) standard	Packet switching	Wi-Fi Protected Access (WPA)
Common Operating Environment (COE)	Phishing	Wi-Fi Protected Access 2 (WPA2)
Corporate owned, personally enabled (COPE)	Phreakers	Wireless Equivalent Privacy (WEP)
Cybercrime	Public switched telephone network (PSTN)	Wireless local area network (WLAN)
General Packet Radio Service (GPRS)	Script kiddies	Worldwide Interoperability for Microwave Access (WiMAX)
Global System for Mobile (GSM) standard	Short Message Service (SMS)	Worms
Hackers	Spam	
	Subscriber identification module (SIM)	
	Telegraphy	
	Telephony	

**CHAPTER 1 ASSESSMENT**

- Digital communication offers which of the following advantages?
  - More efficient use of bandwidth
  - Greater utilization
  - Improved error rates
  - Less susceptibility to noise and interference
  - All of the above
- ARPANET was the predecessor of the modern Internet.
  - True
  - False
- What was the first mobile generation to support Internet access?
  - 1G
  - 2G
  - 2G+
  - 3G
  - 4G
- Wireless networking was initially supported by IT departments because of the productivity gains it provided.
  - True
  - False

**30**      **PART 1** | Introduction to Wireless and Mobile Networks

- 5.** Mobile IP solves which important problem?
  - A. Battery life
  - B. Wireless connections to the Internet
  - C. Access to app stores
  - D. The ability to maintain an IP session while moving
  
- 6.** Which of the following is *not* a requirement for successful mobility?
  - A. Location discovery
  - B. Move detection
  - C. Update signaling
  - D. Omnidirectional antennas
  - E. Path establishment
  
- 7.** COE provides which of the following benefits?
  - A. Lower support costs
  - B. Improved help desk support
  - C. Reduction of OS compatibility issues
  - D. Reduced security incidents
  - E. All of the above
  
- 8.** BYOD and COE policies and aims are not aligned with each other.
  - A. True
  - B. False
  
- 9.** In network security, C-I-A stands for which of the following?
  - A. Confidentiality, integrity, availability
  - B. Central Intelligence Agency
  - C. Control, intelligence, and access
  - D. Confidentiality, intercept, awareness
  
- 10.** Wireless networking's security issues are primarily the result of which of the following?
  - A. Slower access
  - B. Ability to receive and inject data via remote means
  - C. Lack of IT control
  - D. IT policy configuration
  
- 11.** Hackers are motivated primarily by which of the following?
  - A. Social status
  - B. Political aims
  - C. Financial gain
  - D. All of the above
  
- 12.** Wardrivers use unsecured wireless networks to do which of the following?
  - A. Launch viruses
  - B. Source spam
  - C. Initiate DOS attacks
  - D. Visit illegal Web sites
  - E. All of the above