Wireless Network Security

UNIT 1

Introduction to Wireless

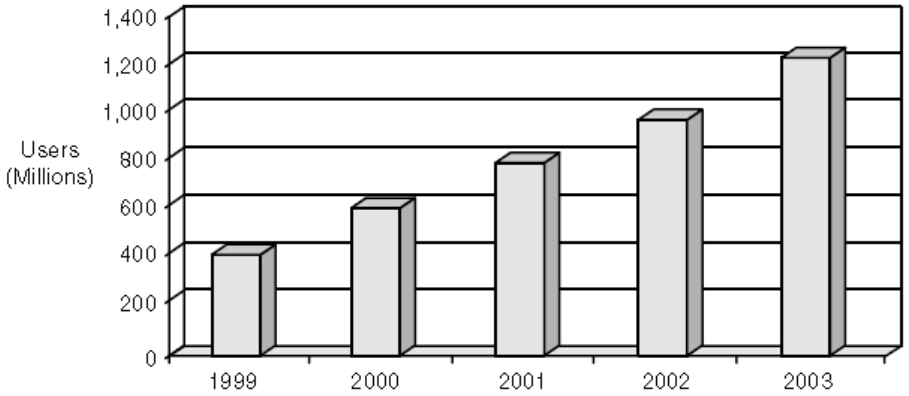
Guglielmo Marconi transmitted the first wireless radio signal through the Italian hillside in 1894, wireless technologies have transformed how people communicate and receive information.

As the twenty-first century unfolds, wireless technologies have become an increasingly important technology. Today's business and technology press are supplied with many terms and abbreviations including Code Division Multiple Access (CDMA), Global System for Mobile Communications (GSM), Time Division Multiple Access (TDMA), 802.11 Wireless Application Protocol (WAP), third generation (3G), General Packet Radio Service (GPRS), Bluetooth, and so on.

The complete number of new wireless technologies and services indicates that this is just the beginning of the wireless revolution. Wireless devices and services are projected to experience high growth rates in the future. By 2004, over 1 billion people worldwide are expected to carry a cellular phone, a 105 percent increase from 2000. (Figure 1-1)

Figure 1-1

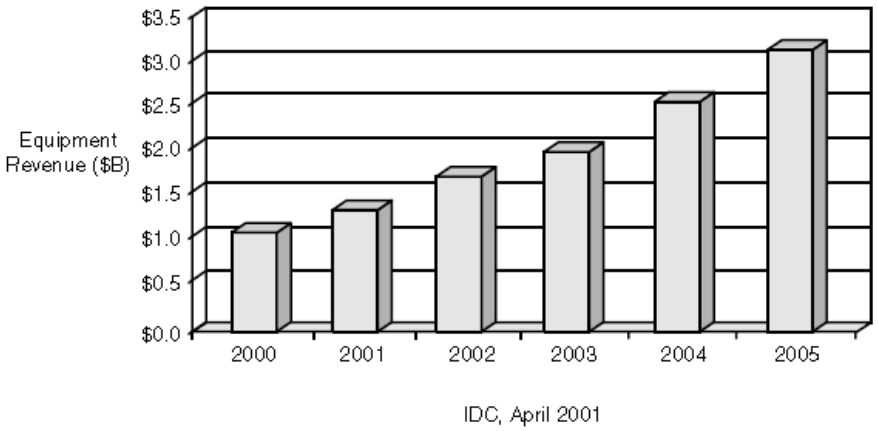
Worldwide wireless phone users



The market projections for other wireless technologies such as wireless local area networks (LANs) and Bluetooth are equally impressive. According to market researcher International Data Corporation (IDC), the wireless LAN equipment market grew 80 percent in 2000 and is expected to continue robust growth into the future as wireless networking is installed in airports, hotels, academic settings, and corporations. (Figure 1-2)

Figure 1-2

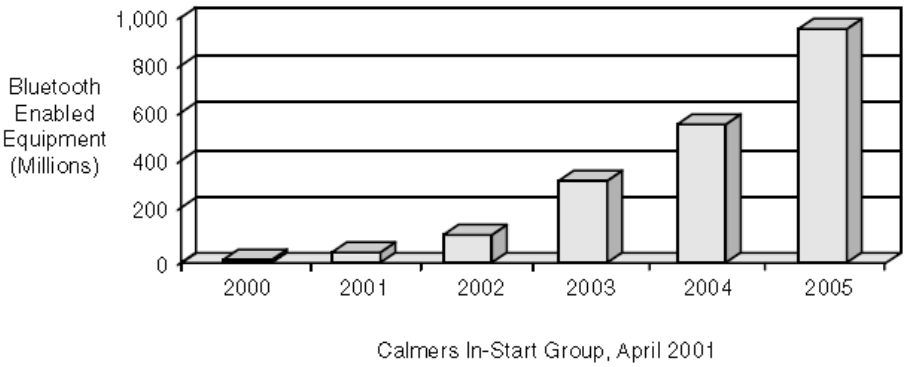
Wireless LAN market forecast, 2000 to 2005



The forecast for Bluetooth, a new short-range (less than 10m) wireless technology for interconnecting devices and peripherals like printers, personal digital assistants (PDAs), keyboards, and cell phones is impressive as well (see Figure 1-3). By 2005, nearly 1 billion Bluetooth-enabled devices will be shipping worldwide, according to Cahner's In-Stat Group. Collectively, this means that even with the astonishing advances in wireless technology over the last 20 years, further technological advances will still occur in the future.

Figure 1-3

Bluetooth market forecast, 2000 to 2005



History of Wireless Technologies

Wireless technology started in the late nineteenth century with the development of Marconi's wireless telegraphy. Patented in 1896 in England, this technology enabled the transmission of wireless radio waves across great distances. Following Marconi's success, American inventor Reginald Fessenden completed the first true radio broadcast in 1906 and the wireless revolution commenced in earnest.

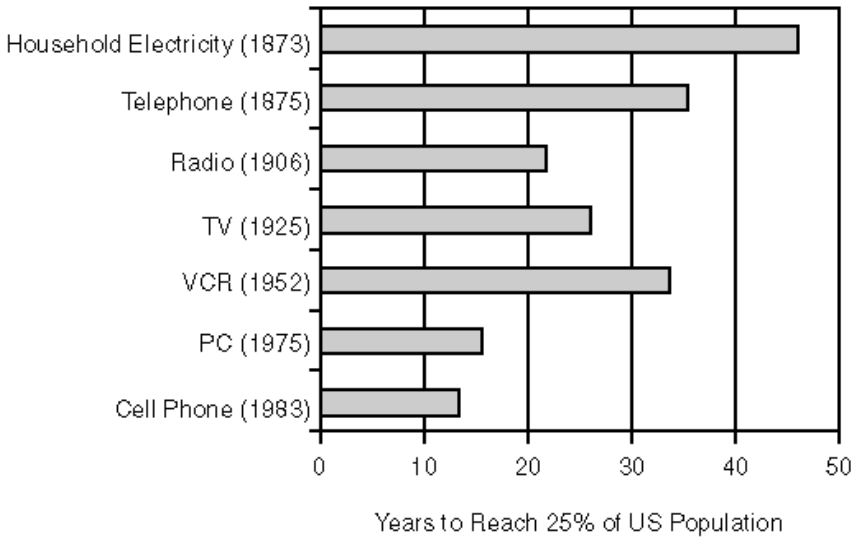
By the 1920s, companies such as General Electric (GE), AT&T, and the newly created Radio Corporation of America (RCA) were creating the first real wireless industry: the AM radio.

"Overnight, everyone had gone into broadcasting, newspapers, banks, public utilities, department stores, universities and colleges, cities and towns, pharmacies, creameries, and hospitals, among others."

By 1929, over 6 million radios were in use in the United States, providing consumers with a new mechanism for receiving content and information. In just over 20 years, radio technology had reached 25 percent of the population. At that time, it was the fastest adoption of any mass-market technology (Figure 1-4).

Figure 1-4

Comparative adoption of mass-market technologies



→ The 1970s—The First Wireless Networks

The first wireless phone systems appeared in the United States in the 1970s. Based on technology developed at AT&T's Bell Labs in the late 1940s, these systems were analog, operated in a limited frequency range, and could only handle a low volume of simultaneous calls. A key limitation of these systems was that they did not support communication continuity during movement from one cell to another.

Demand for mobile voice grew during the 1970s, requiring the development of methods to support more users in a single cell and mobility between cells.

The first system of this type to be installed was AT&T's Advanced Mobile Phone Service (AMPS), which was deployed in Chicago in 1979. Similar systems were installed in

Europe and Japan in the early 1980s. These systems are now referred to as first-generation networks.

The first-generation networks were hardly indicative of the future potential of wireless technology. Demand for mobile telephony started to outstrip available network bandwidth, leading to dropped connections. In 1981, the New York City system could only handle 24 simultaneous calls and the network operators limited the total subscriber base to only 700 users.

The limited capacity restricted mobile phone usage to an elite group of people. Plus, the early mobile handsets were large and heavy. Nevertheless, demand and interest in the mobile phone only increased. Network operators eagerly upgraded networks to meet the growing demand.

→The 1980s—Wireless Markets Start to Evolve

Following the success of the AMPS systems, pressure grew on the U.S. government to allocate additional radio spectrum for wireless communication. The Federal Communications Commission (FCC) was tasked to regulate the market, through licensing new radio spectrum. In the spring of 1981, the FCC announced its intention to allocate 40 MHz of spectrum in the major metropolitan markets in the United States. This was a significant step forward in capacity. This spectrum enabled 666 channels for cellular communication in each major metropolitan market. Compared to the 44 channels that had been previously allocated to cellular service, this was a quantum leap in capacity.4 The FCC's initial focus was on the largest cities in the United States, but ultimately, spectrum would be allocated for the top 300 metropolitan areas in the country.

To promote competition, the FCC awarded each market two licenses: one license to the local phone company and another license to a non-wireline company. Since the AT&T breakup was announced in the midst of the initial wireless spectrum auction in 1982, it was clear that a host of new players, not AT&T, would be creating the wireless voice market.

In 1983, the FCC began awarding spectrum licenses in the major markets.

In October 1983, Ameritech, one of the seven Baby Bells created by the AT&T breakup, launched the first commercial system in Chicago and quickly signed up 3,000 subscribers.

The European telecommunications market differed from the U.S. market in several key dimensions, which ultimately led to very different policies.

- **State-owned telephone monopolies**
  In most of Western Europe, state-owned telephone monopolies provided local and long-distance phone service. In United States, which was breaking up the AT&T phone monopoly and promoting a new wireless voice market without AT&T.
- **Geography**
  Western Europe is a much smaller area than the United States and has a much higher population density. This means that the physical cost of developing networks would be considerably less than in the United States.
- **Mobile population**
  The creation of the European Common Market encouraged the creation of Pan-European commerce and trading. Europeans traveled to other countries with much greater frequency than Americans.

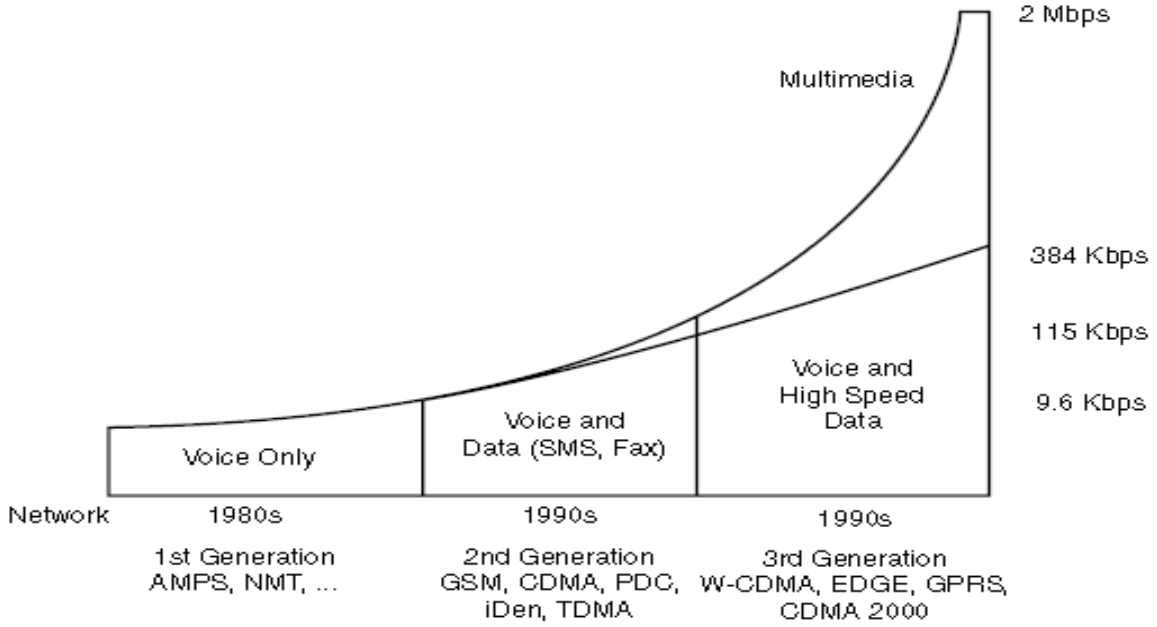
In 1982, the Conference of European Posts and Telecommunications Administrations (CEPT), which consisted of the telecommunications administrations of 26 nations. The CEPT made two important decisions.

First, the CEPT decided to create a single European wireless technology standard and established a task force to define that standard. Second, the CEPT agreed to allocate wireless spectrum in the 900-MHz band in each country for use with this new wireless network.

By the late 1980s, the CEPT had developed the GSM standard, and mobile operators from 13 European countries signed a Memorandum of Understanding (MoU) that outlined the specifics of the GSM standard.

→The 1990s—Wireless Networks Mature

In 1991, the first commercial GSM networks began offering service, starting in Scandinavia. A year later, Australia became the first operator to offer GSM service outside Europe. GSM and the other network standards (TDMA, CDMA, and Personal Digital Communication [PDC]) are known as second-generation (2G) networks. See the following illustration:

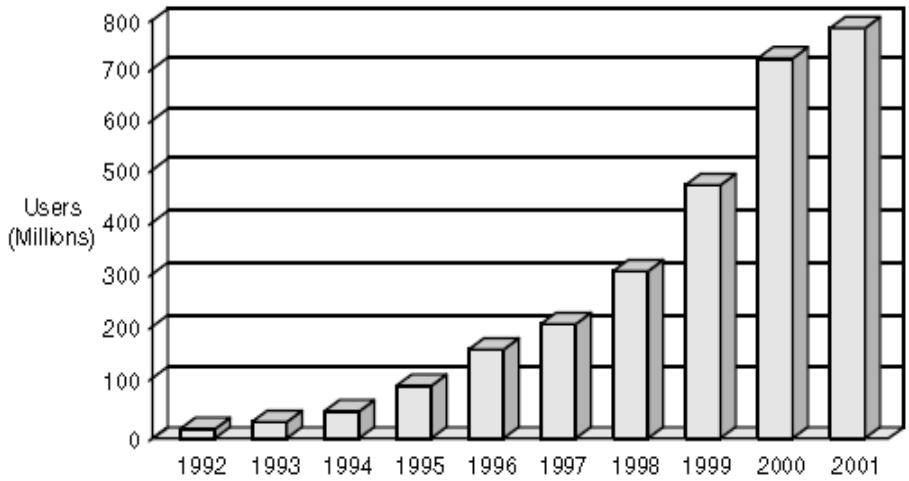


In 1992, the first international roaming agreement between two European carriers, Vodafone and Telecom Finland, was signed enabling transparent roaming between Vodafone and Telecom Finland's customers.

A steady increase in GSM subscribers in the mid-1990s, as shown in Figure 1-5.

Figure 1-5

GSM subscribers, 1993 to 2000



Despite the rapid move toward free market policies, the migration toward new technologies and services was still slow. In 1997, the average wait to install a new wired phone line in Poland was over 4 years and Poland had less than 13 fixed phone lines per 100 people compared to over 50 fixed lines per 100 people in the West.

Although the Polish government only licensed two GSM carriers in Poland (Era GSM and Plus GSM), these two carriers competed aggressively for subscribers. Table 1-1 shows the effects of the competition in just the first six months of GSM service being available in Poland. Initial services required purchase of a mobile phone ($300) and an activation fee ($300).Within six months, the activation fee had dropped to $1, phones were heavily discounted, and tens of thousands of users had signed up.

→The Mid-1990s—Other Wireless Networks Emerge

Beginning in the early 1990s, operators worked on improving these networks' functionality, adding features such as two-way paging and the ability to send alphanumeric messages. In striking parallels to the mobile voice market, the paging market quickly diverged into two competing standards: one for Europe (Ermes) and another for outside Europe (FLEX).

In 1992, the Baby Bells pooled resources to create a new packet-based wireless data network called Cellular Digital Packet Data (CDPD). The CDPD networks offered relatively high throughput (up to 19.2 Kbps) and were based on Transmission Control Protocol/Internet Protocol (TCP/IP), making compatibility with the Internet relatively straightforward.

By the end of the twentieth century, CDPD networks covered the 50 largest metropolitan areas in the United States and possessed over 10 million subscribers, mainly for uses such as transportation, messaging, and inventory control. The wireless LAN standard started in 1990 when the Institute of Electrical and Electronics Engineers (IEEE) started the 802.11 committee to define a wireless LAN standard. The standard was not finalized until 1997, but computer manufacturers such as Intel, 3Com, Cisco, and Lucent.

For near-range (less than 10m) wireless networks, the Bluetooth Special Interest Group (SIG) was founded in May 1998 by Ericsson, IBM, Intel, Nokia, and Toshiba. Taking its name from Harald Bluetooth, a Viking warrior from the tenth century, the Bluetooth SIG created a mechanism for enabling wireless devices to communicate with each other in a world without wires.

→The Late 1990s—The Wireless Internet Emerges

Another disruptive technology— the World Wide Web—exploded onto the scene. Initially commercialized by Netscape Communications Corp., the Web unleashed a consumer fervor never before witnessed in documented history.

Nokia, Ericsson, and Motorola to create the WAP Forum and commercialize the concept of accessing the Web from a mobile device. By the end of 1997, over 90 companies had joined the WAP Forum. The initial specification, WAP 1.0, was released in late 1997 and finally ratified in mid-1998.

In 1999, operators began slowly launching WAP services. They consisted of basic information services such as weather, news, and airline flight timetables. Users needed to purchase new handsets and pay an incremental monthly fee for service.

At the end of the year 2000, it was estimated that there were only 1 million wireless Internet users in the United States, which was less than 1 percent of the total wireless phone users in the nation. Bluetooth and 802.11 technologies suffered considerably. Bluetooth-enabled devices were few and far between and carried high prices, while some very public security flaws were exposed in the 802.11 specification.

Why the uptake of WAP, Bluetooth, and wireless LANs been slower than expected?

- **Economics**

  Wireless-Internet-capable cell phones are often quite expensive and require additional monthly service charges. With Bluetooth, the new chipsets are still quite expensive, leading to high prices for Bluetooth-enabled devices.

- **User experience**

  Content providers were also slow to optimize existing wired content for delivery over a wireless network. Customers tried these services, but quickly decided that the value and convenience was not worth the extra cost.

- **Security**

  Although the security requirements for wireless services like weather and sports scores are minimal, value-added services like stock trading, wireless access to corporate networks, and transactions require a much higher level of security than the current infrastructure could support.

The wireless Internet still faces some serious obstacles. For one, there are some significant physical differences between the client devices. As Table 1-2 indicates, the differences between a standard PC and a wireless- Internet-capable cell phone are dramatic.

Table 1-2 Hardware Differences Between PCs and Cell Phones

Category	PC	GSM Cell Phone
Processor speed	1 GHz	50 MHz
Memory	512MB	32KB
Storage	50GB	64KB
Battery life	3 hours	100+ hours standby
Display	15-inch Super XGA+	5-line monochrome
Operating system	Windows 2000 and XP, Linux	Proprietary operating system
Bandwidth capability	1 GBps	14.4 KBps

The wireless user interface is especially important. Because of the slow throughput of wireless networks, wired Internet content must be modified for wireless users. This means fewer graphics and simpler displays.

The good news is that these limitations have been identified. The bad news is that the worldwide macroeconomic downturn in 2000 and 2001 exacerbated the problem as companies delayed or cancelled planned capital wireless investments or service offerings.

History of Wireless Security

As World War II commenced, the Allies and Axis powers increasingly relied on wireless radios to communicate with their geographically dispersed military forces. Even though signals were encrypted, they were still being intercepted. In some cases, the ability to intercept and decrypt wireless signals provided significant advantages.

Eavesdropping and Jamming

The eavesdropping fear consisted of two dimensions. One dimension was that curious citizens could listen in on random conversations. The second and more sinister dimension was that government agencies such as the CIA and FBI could intercept conversations at will in the name of law enforcement or national security.

In addition to eavesdropping, wireless signals can also be jammed. First in military applications, jamming technology enabled cellular networks to become inoperable in a limited geographic area by sending a high volume of radio signals. Besides jamming an individual phone, it is also possible to jam an individual cellular tower, thereby taking down an entire geographic area.

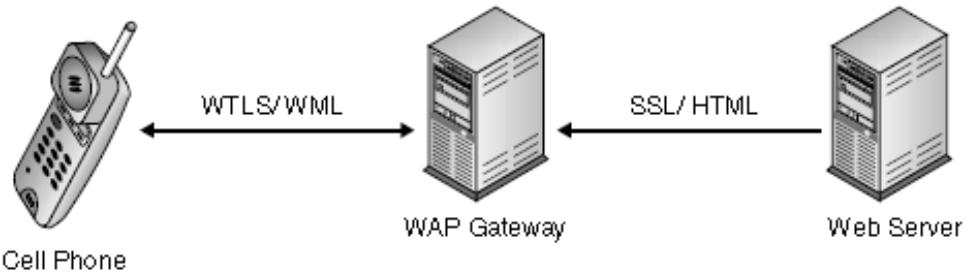
wireless networks are susceptible to the following possible breaches:

- Interception of law enforcement data on specialized mobile radio, private radio, or CDPD networks
- Interception of credit card authorizations over wireless networks
- Stealing of cellular airtime
- Interception of e-mail messages on wireless Internet connections
- Physical breach of security at unmanned base stations or other
- communications centers

The Wireless Internet—Wireless Security Moves into the Mainstream

With the introduction of the wireless Internet, security issues rose to the forefront. During the meteoric growth of the wired Internet, security and privacy issues were important issues. Vendors like Netscape and Microsoft supported Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption over Hypertext Transfer Protocol (HTTP) in web browsers and web servers.

The WAP Forum provided an SSL-like alternative called *Wireless Transport Layer Security* (WTLS). The WAP approach required two protocols: WTLS from the wireless handset to the WAP gateway and SSL from the WAP gateway to a web server on the Internet. During the protocol conversion from WTLS to SSL, data was unencrypted and reencrypted, leaving data temporarily in an unencrypted form. This so-called WAP Gap created a level of concern about wireless security that delayed consumer adoption. See the following illustration:



WTLS was designed specifically because the low-bandwidth and hardware limitations of cellular handsets made implementing wireless SSL technically challenging.

Wireless Value Chain

The wireless value chain can be divided into five different sectors. Some vendors operate in multiple sectors and some firms are almost 100 percent wireless focused, whereas others trace their roots to traditional wired networking products. Table 1-4 contrasts the different players in the wired and wireless worlds.

Table 1-4 Wired and Wireless Market Segments

	Wired	Wireless
Device vendors	Dell, Compaq, HP, Toshiba, NEC, IBM, and Apple	Nokia, Motorola, Ericsson, Siemens, Palm, Compaq, and Handspring
Network operators	AOL, AT&T, Prodigy, and Earthlink	Verizon, Vodafone, DoCoMo, and Sprint PCS
Hardware providers	Intel, Cisco, Lucent, Sun, IBM, and EMC	Texas Instruments, Ericsson, Alcatel, Siemens, and Cisco
Content providers	AOL, eBay, Amazon, Yahoo, and MSN	Yahoo, airlines, and Weather.com
Application providers	Microsoft, Oracle, SAP, Lotus, IBM, and BEA Systems	Openwave, iAnywhere, CellPoint, and Jinny

a) Device Vendors

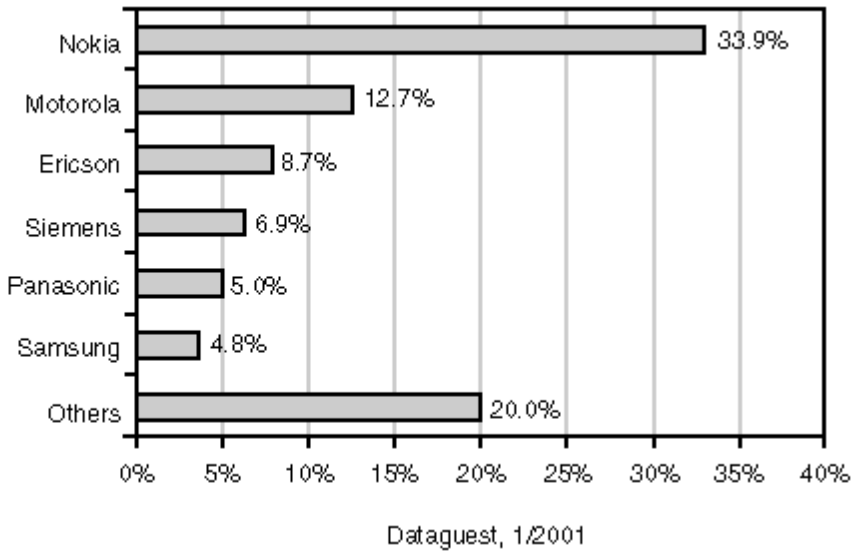
This sector is responsible for designing, manufacturing, selling, and marketing myriad wireless devices available to consumers worldwide. Voiceoriented devices (namely cell phones) compose the vast majority of this category, but there are also wireless data devices from Compaq, Palm, Handspring, and Research in Motion.

This sector experienced tremendous growth during the ramp-up of wireless services in the mid-1990s. Large volumes of new users enabled manufacturing economies of scale and more functional phones at very aggressive price points.

Within this sector, Finland-based Nokia remains the dominant player. As Figure 1-6 demonstrates, Nokia was the dominant worldwide market share leader in mobile handsets in 2000.

Figure 1-6

Worldwide wireless handset market share, 2000



b) Network Operators

The network operators are responsible for building, maintaining, and promoting wireless networks. Many network operators (such as Verizon and British Telecom) began as wired operators and used that position to expand into wireless services. Within the wireless value chain, they are the most powerful segment.

Table 1-5 lists some of the major mobile operators in the world, based on the number of subscribers.

Table 1-5

Major Global Wireless Operators

Operator	Markets Served	Subscribers as of 2001 (in millions)
Vodafone	United Kingdom, Germany, and Japan	96
China Mobile Telecom	China	89
T-Mobil	Germany	42
NTT DoCoMo	Japan	38
Verizon	United States	28
Telefonica	Spain and Latin America	25
Telecom Italia	Italy	22

Gradually, many markets opened the wireless sector to new entrants, creating more competition. This created additional problems for operators, particularly in the area of churn (customers leaving one operator to subscribe to another).

c) Hardware Providers

This sector is almost invisible to consumers, but it is a critical supplier to the network operators and handset vendors. These firms provide the hardware (chips and CPU) for the handset vendors as well as the network- switching infrastructure for connecting wireless networks. There is some overlap between the handset vendors and this segment. For instance, Ericsson, Siemens, and Alcatel are all major hardware providers in addition to being handset manufacturers. This sector is getting increasing focus because of the migration to faster wireless networks.

d) Content Providers

This sector is responsible for generating and distributing information that can be served up on a wireless device. Not surprisingly, many of the leading wired content providers like AOL, Yahoo, MSN, Amazon, and eBay all announced wireless versions of their content in 2000. In the wireless world, to a large extent the operators determined what content subscribers

could or could not view. If content provider X did not have a distribution agreement with network operator Y, network operator Y's subscribers could not view that content.
Despite these issues, the content providers still aggressively promoted wireless services. They were especially interested in location-based services. Newer networks and handsets could give content providers the location of a specific subscriber to within a city block, creating many new potential uses.

e) Application Providers

This sector is divided into two categories: traditional independent software vendors (ISVs) that have modified existing wired applications for wireless environments and software vendors that have developed exclusively for wireless environments. In 2000, all the major software vendors including Oracle, IBM, Microsoft, and SAP announced plans to make existing applications wireless ready. The same year saw the emergence of certain wireless pure-play vendors like Phone.com (now called Openwave), CellPoint, and Jinny Software. These vendors can coexist in wireless environments, particularly in scenarios where a wireless device needs to connect to a legacy application or database.

State of the Wireless Industry, 2001

It is necessary to review the current state of the wireless industry as of 2001. Table 1-6 gives a sense of the ubiquity of wireless technologies throughout the world.

Table 1-6
Key Wireless Indicators in 2000 (EMC World Cellular Database)

Indicator	Year End 2000
Monthly churn	2.56%
SMS messages sent per GSM subscriber per month	30
World's largest cellular market	USA (130 million subscribers)
World's fastest growing cellular market	Morocco (629% increase in subscribers versus 1999)
World's largest GSM market	China (73 million subscribers)
World's largest CDMA market	United States (55 million subscribers)
Highest penetrated market (percent of population with mobile phone)	Iceland (77.4%)

The following are the four geographic regions to be reviewed:

- North America
- Europe
- Japan
- Asia

a) North American Wireless Industry, 2001

There are now six dominant national brands (AT&T Wireless, Cingular, Nextel, Sprint PCS, Verizon, and Voice stream) that control 90 percent of the U.S. wireless subscribers. Where there were once all analog networks, there are now four different and incompatible digital network standards (CDMA, GSM, TDMA, and iDEN)—see Table 1-7.

Table 1-7
U.S. Network Operators

Carrier	Network Technology	Subscribers as of Dec. 2000 (in millions)[11]
AT&T Wireless	TDMA	16
Cingular	CDMA and GSM	21
Nextel	iDEN	8
Sprint PCS	CDMA	13
Verizon	CDMA	28
Voicestream	GSM	5

The North American market divides into two segments: consumer and enterprise. U.S. wireless carriers market wireless services in a variety of manners. For instance, Nextel focuses exclusively on the corporate market offering special handsets that enable Nextel users to communicate with each other like a walkie-talkie, instead of placing an actual call. Service plans are very similar. Users pay a nominal fee for a handset (sometimes it is free) and sign up for a certain "bucket" of monthly minutes. Because of the high cost of attracting a new customer, carriers need to retain subscribers for several months to break even. This is why operators are keen to offer new services (such as wireless data) that will increase customer satisfaction and retention.

In 2000, enterprises were extremely attracted to wireless data services because they viewed wireless data as an important strategic tool that could address three areas:

Improved productivity Enabling employees real-time access to enterprise information would allow for quicker information distribution and allow employees to obtain important business information faster than before.

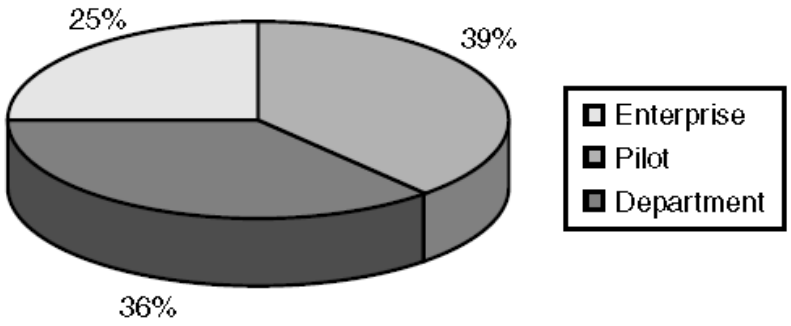
Improved customer service Wireless data services enabled mobile users to get immediate reports on customer relationships or issues and respond to those issues in a very fast manner, thereby improving customer satisfaction.

Competitive advantage As more companies adopted wireless technologies to maintain contact with customers, partners, suppliers, and employees, many companies realized that wireless connectivity was a necessity.

Enterprises were quick to move ahead with wireless plans. As Figure 1-7 indicates, many companies quickly moved from wireless pilots into production environments that went companywide. Security often emerged as a barrier to deployment, but in many cases, senior management put security issues aside in order to realize other business benefits like better productivity, customer service, and so on.

Figure 1-7

InformationWeek survey of enterprise wireless deployments, 2000



In order for these new wireless services to succeed in the United States, two things must happen:

_ ***Fix security.*** It is imperative that the security weaknesses in wireless LANs be addressed. If the wireless LANs cannot provide solutions immediately, organizations need to adopt a best-practices security policy to minimize risk, but still allow the technology to be deployed.

_ ***Develop compelling apps.*** American consumers can be a skeptical bunch, which is why new wireless technologies like Bluetooth and wireless LANs must have well-articulated benefits that consumers can understand

U.S. wireless voice industry faces three crucial issues:

→Mobile Party Pays

→Spectrum allocation

→Technology divergence

Mobile Party Pays In the United States, wireless phone users pay to place and receive calls on their handsets in what is called Mobile Party Pays. In every other region of the world, users only pay to place a call in what is called Calling Party Pays.

Spectrum allocation An alternative to the spectrum issue is to design handsets, devices, switches, and other networking hardware that can more efficiently use the existing radio spectrum.

Technology Divergence While the government is not going to adopt a national standard like GSM, the different networks hurt the U.S. wireless market in four ways:

1. No global roaming
2. Supplier customization
3. Network compatibility
4. Network infrastructure

b) European Wireless Industry, 2001

Owing to Europe's much larger population, the European wireless market is considerably larger than North America's wireless market, as indicated in Table 1-9.

Table 1-9 European Wireless Market Metrics (www.gsmworld.com)

Metric	Value
Subscribers (as of Dec. 2000)	281,000,000
Direct carrier employees	470,000
Cumulative capital investment	$120,000,000
Annual year-2000 cellular service revenue	$215,000,000

In 2001 European operators enjoyed several benefits over operators in other regions:

→ **Stable universal network infrastructure** The GSM network was complete in Western Europe with over 110 GSM networks online.

→ **Relatively high cost of wired Internet access** The national phone monopolies continued to keep the cost of dial-up Internet access much higher than that in North America. This situation made the European market more attractive to the wireless Internet.

→ **Healthy nonvoice revenue stream** European operators were highly successful in marketing SMS in 2000, generating significant revenues, and reducing reliance on voice calls only.

→ **Protected incumbent carriers'** European operators still enjoyed a relatively protected local market. Although many state phone monopolies had been partially privatized in the 1980s, these same players were still the dominant telecommunications players in 2001.

Despite the optimism, Europe still faces some significant challenges in 2001:

→ **3G debt loads** European operators do not suffer from a spectrum shortage, but the development of 3G networks in Europe has come at a staggering cost because of the high license fees paid to governments for the right to build 3G networks.

→ **Subscriber saturation point** The tremendous success of GSM has resulted in many Western European countries reaching adoption rates between 60 and 70 percent. At this saturation rate, there are not many remaining eligible new subscribers.

→ **Regulation** In some regions, governments are conducting 3G spectrum auctions via so-called beauty contests in which spectrum is not allocated based on the highest bidder, but based on some qualitative measures that the government determines.

c) Japanese Wireless Industry, 2001

The Japanese market exploded into the mainstream in the late 1990s. The phenomenon was the i-mode wireless data service offered by NTT DoCoMo. DoCoMo (Do is the Japanese word for everywhere) is a subsidiary of Japanese phone monopoly Nippon Telegraph and Telephone (NTT). DoCoMo started offering traditional wireless voice in 1992 and quickly became Japan's leading mobile operator with over 35 million subscribers.

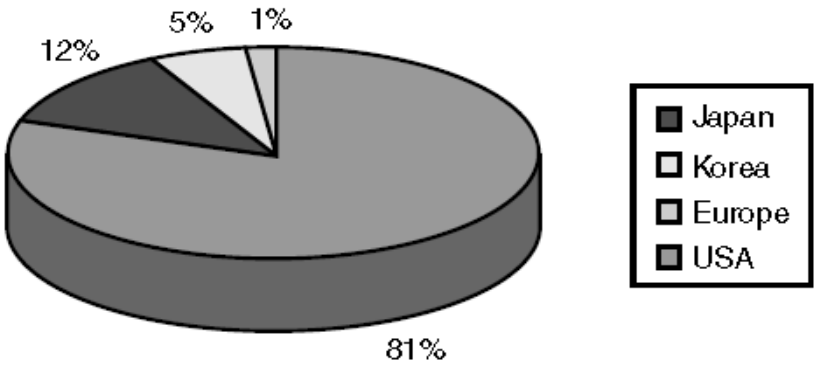
In August 1999, DoCoMo launched i-mode, a wireless Internet service.

i-mode offered three distinct technology advantages:
→Service was a packet-switching network, not circuit-based network ("based" meaning that the service was always on).
→It was compatible with existing cellular networks infrastructure—no additional investment was needed.
→Service did not require significant modifications to existing wired web content.

Within 18 months, over 20 million subscribers had signed up to the service and over 30,000 i-mode-specific content sites were available. To put it into perspective, it took AOL nearly 15 years to achieve the same number of wired Internet subscribers. i-mode's success dwarfed that of any other region, as Figure 1-9 demonstrates.

Figure 1-9

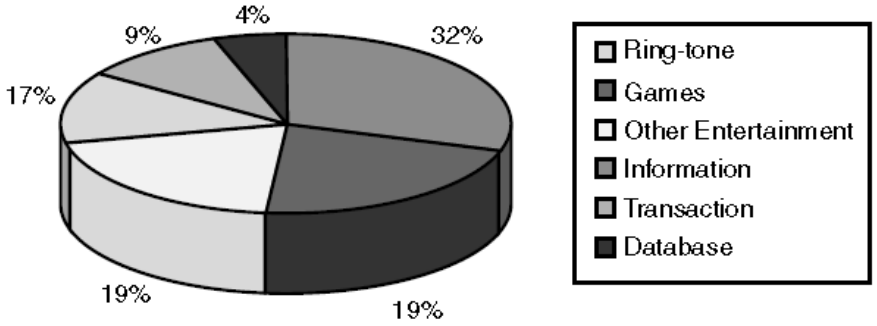
Geographic distribution of wireless Internet users



Economically, i-mode users paid an incremental $3 per month for i-mode service plus 0.3 yen for each packet of data transmitted. All the monthly rates and fees are presented on the subscriber's monthly voice bill. Popular content included downloads of ring tones, Pokémon characters, and games. i-mode's usage is displayed in Figure 1-10.

Figure 1-10

i-mode content by category



Moving ahead, DoCoMo has already started the first trial of a 3G network and plans to launch the 3G service in 2002, well ahead of any other operator in the world. In fact, DoCoMo's success is helping keep the wireless Internet alive in the economic downturn of 2001 by serving as a positive proof point for this technology.

So why has i-mode been much more successful than any other wireless Internet efforts? The following are some of the factors:
→ High cost of fixed Internet access
→ Cultural
→ Close collaboration with Japanese suppliers
→ Dominant incumbent phone monopoly

d) Asian Wireless Industry, 2001

Asia's wireless industry varies from country to country. In countries with high standards of living like Singapore and Taiwan, wireless usage equals that of many Western European nations.

The country that attracts the most attention as a future wireless market is China. Owing to its 1.2 billion people, wireless vendors are very eager to participate in the Chinese market. China is already the second largest wireless market.

Table 1-10 summarizes the key statistics for the Chinese wireless market.

Table 1-10 Chinese Wireless Market Metrics (Courtesy of *South China Post* and *Business Weekly*)

Metric	Value
Subscribers (as of Dec. 2000)	85,300,000
Cumulative capital investment	$60,000,000
Annual year-2000 cellular service revenue	$16,000,000

Qualcomm had successfully convinced South Korea to choose CDMA over GSM in 1996, and Qualcomm was eager to duplicate its success in China. Senior U.S. government officials were engaged in lobbying the Chinese delegation and Qualcomm's stock soared 2,600 percent in 1999 as investors anticipated a major CDMA win in China.

Wireless Threats

The Uncontrolled Terrain

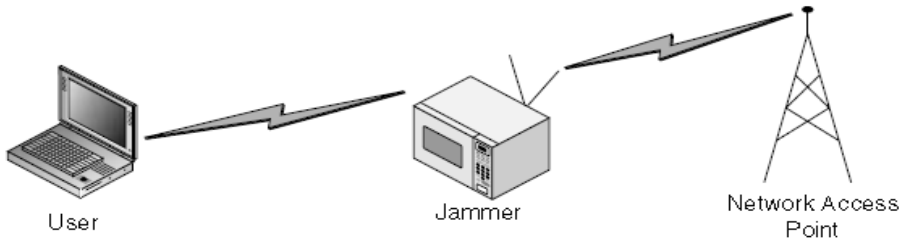
The major difference between wired and wireless networks is the anonymous, uncontrolled coverage areas between the end points of the network. In wide area cellular networks, the wireless medium cannot be controlled at all. Current wireless networking technology offers little to control the coverage area. This enables attackers in the immediate vicinity of a wireless network to perform a number of attacks that are not found in traditional wired networks.

Communications Jamming

Jamming occurs when an intentional or unintentional interference over powers the sender or receiver of a communications link, thereby effectively rendering the communications link useless. An attacker can apply jamming in several ways.

→ **Denial of Service (DoS) Jamming** Jamming the entire network can cause a denial of service (DoS) attack. The entire area, including both base stations and clients, is flooded with interference so that no stations can communicate with each other as shown in Figure 2-2.

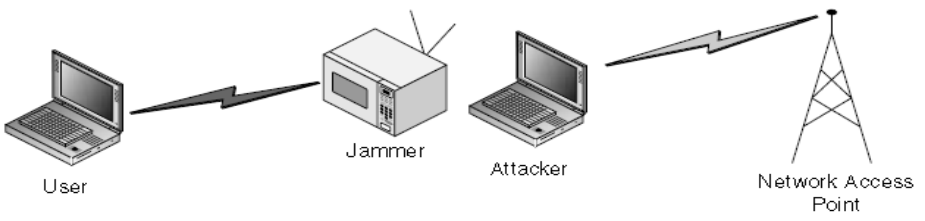
Figure 2-2 Jamming attack on wireless communications



This attack shuts down all communications in a given area. This type of attack can require a significant amount of power if applied to a broad area. DoS attacks on wireless networks may be difficult to prevent and stop.

→ **Client Jamming** Jamming a client station provides an opportunity for a rogue client to take over or impersonate the jammed client as shown in Figure 2-3. Jamming also can be used to DoS the client so that it loses connectivity and cannot access the application.

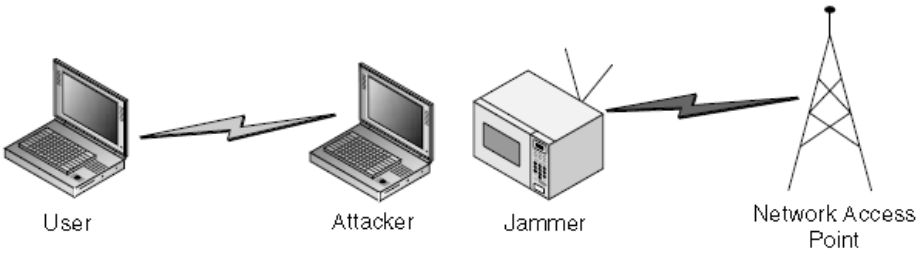
Figure 2-3 Jamming attack against client to hijack communications



→**Base Station Jamming** Jamming a base station provides an opportunity for a rogue base station to stand in for the legitimate base station as shown in Figure 2-4. The jamming can also deprive clients of service or a telecom company from revenue.

Figure 2-4

Jamming attack against access point to hijack communications



Therefore, many devices such as cordless phones, baby monitors, and microwave ovens may interfere with wireless networking and effectively jam the wireless communications.

Injection and Modification of Data

Injection attacks occur when an attacker adds data to an existing connection in order to hijack the connection or maliciously send data or commands. An attacker can manipulate control messages and data streams by inserting packets or commands to a base station and vice versa. Inserting control messages on a valid control channel can result in the disassociation or disconnection of users from the network.

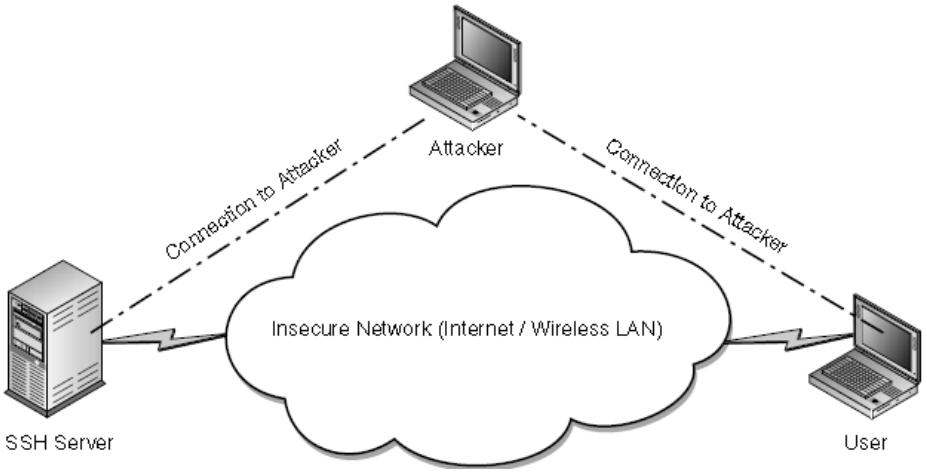
Injection attacks can be used for DoS. An attacker can also flood the network access point with connect messages, tricking the network access point into exceeding a maximum limit, thereby denying authorized users access to the network.

Man-in-the-Middle (MITM) Attacks

When a victim initiates a connection, the attacker will intercept the connection, and then complete the connection to the intended resource and proxy all communications to the resource as shown in Figure 2-5. The attacker is now in a position to inject data, modify communications, or eavesdrop on a session that would normally be difficult to decode, such as encrypted sessions.

Figure 2-5

MITM attack



Rogue Client

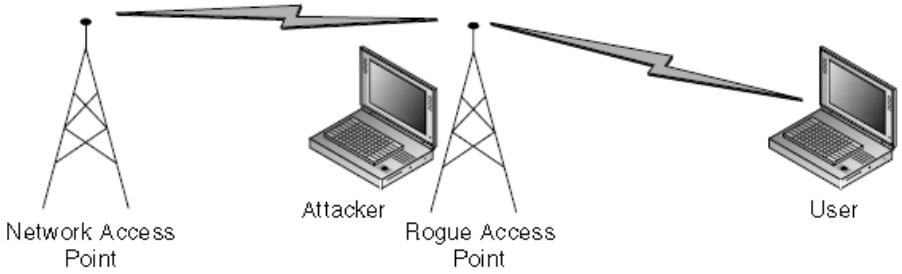
After studying a client in the field, an attacker may choose to mimic or clone the client's identity and attempt to gain access to the network and advertised services. The attacker may also be so bold as to steal an access device to attempt to gain access to the network. Securing all wireless devices may be very difficult, for convenience and mobility dictate that most wireless devices are very small. A common wireless security mechanism was supposed to use layer 2 access controls to limit access to resources. This mechanism proved a failure when it was used by cellular phone companies to limit access to phone numbers by using an Electronic Serial Number (ESN). Then the failure was repeated by the 802.11 wireless LAN standard with Media Access Controls (MACs) that can be easily circumvented by a skilled attacker.

Rogue Network Access Points

An adept attacker can set up a rouge access point to impersonate a network resource. Clients may unknowingly connect to this false access point and divulge sensitive credentials such as authentication credentials. This type of attack can be used in conjunction with directive jamming to block the ears of the legitimate network access point as shown in Figure 2-6.

Figure 2-6

Rogue access point



Users with access to the wired network may also install rouge access points, unknowingly opening up the network to attacks. Users may install a wireless access point seeking the convenience of wireless without knowing the security concerns. Attackers can easily connect to these access points and have the same access that a wired user would have.

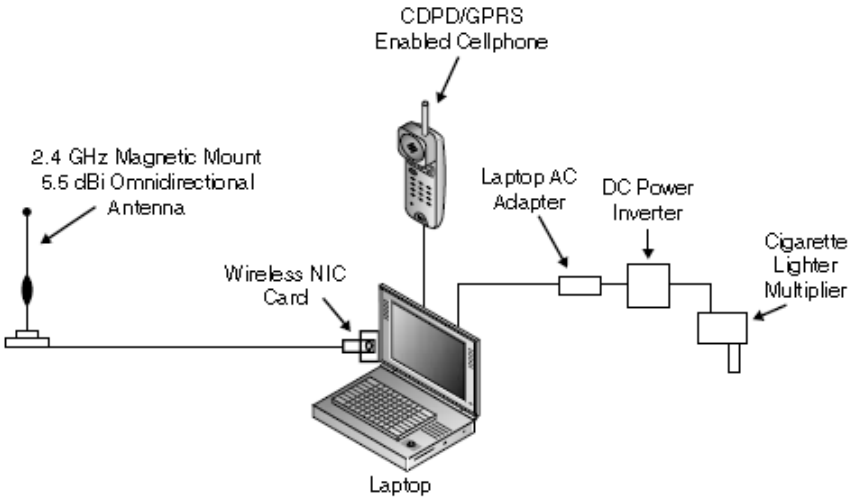
Attacker Equipment

The equipment used by the casual attacker can minimally consist of a wireless network interface. This can either be a wireless Ethernet network interface card (NIC), a General Packet Radio Service (GPRS), or a Cellular Digital Packet Data (CDPD) cellular telephony handset connected to a laptop either as a Personal Computer Memory Card International Association (PCMCIA) card or through some communications link.

Cellular network attackers will generally use a configuration as depicted in Figure 2-7 because the network coverage is understood and generally covers a large area.

Figure 2-7

Attacker hardware configuration



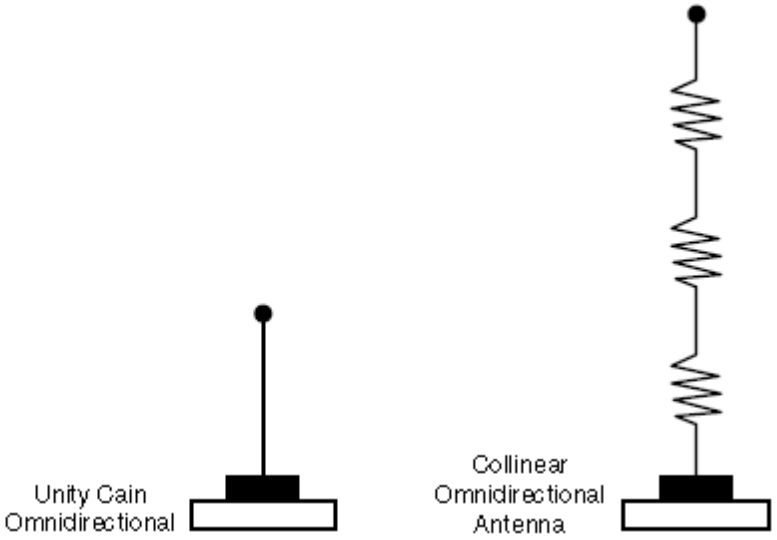
The basic network discovery setup consists of a laptop, a GPS unit, an antenna, an amplifier, and a wireless Ethernet NIC. In order to perform long-duration sweeps, extra power can be obtained by using an inverter for converting 12V DC into 120V AC to power the laptop or any other equipment one may be using.

The three most common antenna types are the
omnidirectional antenna,
the yagi, and
the parabolic.

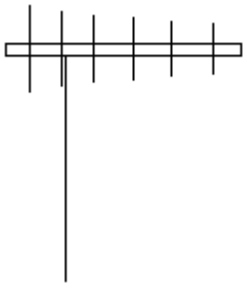
The omnidirectional antenna has a beam width of 360 degrees and is usually deployed to survey or jam a wide area

Figure 2-8

Common omnidirectional antenna



The yagi antenna has special properties that focus the electromagnetic radiation from a driven element into a directed pattern. A yagi antenna, shown below, typically exhibits a beam width of 10 to 20 degrees and a gain of 10 to 18dBi. The yagi is usually deployed when one cannot gain direct access to the coverage area using an omnidirectional antenna. A typical yagi antenna has a gain of 10 to 18 dBi.



The parabolic antenna, shown below, has the narrowest beam width of all, typically between 4 and 10 degrees. The parabolic antenna is generally deployed when concealment is of concern and great distances are to be covered. The parabolic antenna is difficult to use due to the narrow beam width, but this characteristic can be used to determine location. This antenna can also be used to support jamming functions as well as very precise attacks, perhaps to avoid detection systems.