

PART IV

I-ADD

Identify Targets and Roles

Chance favors the prepared mind.

—Louis Pasteur

NOW WE BEGIN TO APPLY OUR I-ADD security analysis process, described in Chapter 2, “Security Principles.” As you may recall, the I-ADD security analysis process consists of four phases:

- ◆ Identify targets and roles.
- ◆ Analyze known attacks, vulnerabilities, and theoretical attacks, generating mitigations and protections.
- ◆ Define a strategy for security, mindful of security/functionality/management trade-offs.
- ◆ Design security in from the start.

Identify Targets

The first step in the process is to identify the system’s high-level functional blocks. In Chapter 2, we identified six high-level functional blocks of a typical wireless system (see Figure 9.1). After the blocks are identified, an examination of each is performed to identify the resource or information targets within it that should be protected. After you break down the wireless system to its fundamental components and produce a list of targets, you examine these targets and generate a list of associated roles.

The Wireless Device

We begin our examination of each of these high-level blocks with the wireless device. At this highest level, the only obvious target is the device itself. A statement of the target at this level is something like the following:

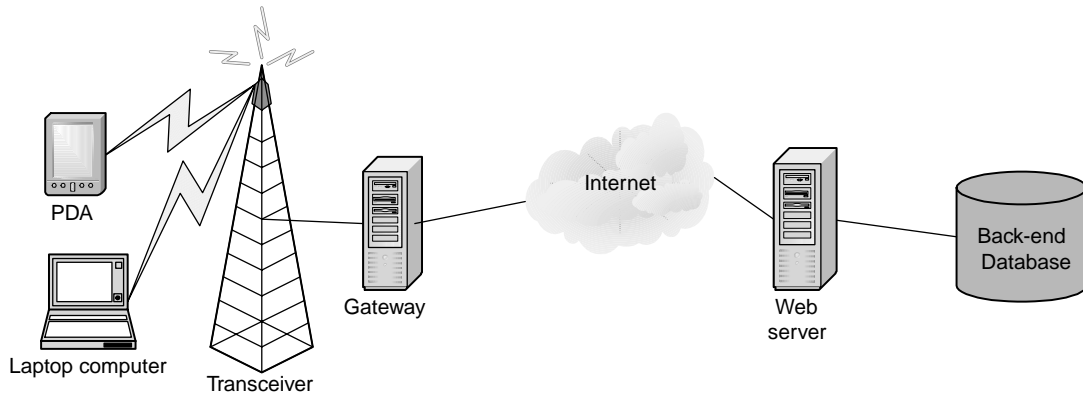


FIGURE 9.1 A typical high-level wireless system

Wireless Device

The wireless device itself

Although this may seem obvious, it is provided here to introduce a methodical and consistent method for identifying targets, or components of a system that need to be protected. This is as far as you can go at this level, so you repeat the process at the next lower functional level (see Figure 9.2).

There is no right or wrong way to determine how to break the functional blocks down to their next level. Experience and trial and error yield the best breakdown for any given system. A method or approach that works well for one system may not provide adequate results for another. Should you choose an alternative breakdown, such as that shown in Figure 9.3, you may encounter repeated functional blocks at lower levels. You may have functional blocks with certain branches that can no longer be broken down and other branches that continue for several levels, as shown in Figure 9.4.

This does not matter, as long as you examine all aspects of the functionality of the system component being analyzed. If our approach is followed, you cannot help but cover all aspects of the system. Figure 9.5 shows a possible breakdown of the multifunction phone depicted in Figure 9.4, but following the delineation started in Figure 9.2.

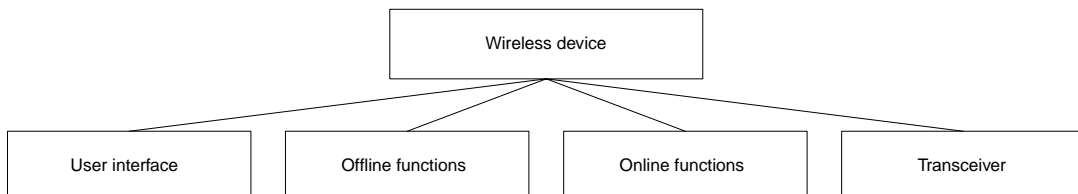


FIGURE 9.2 A wireless device broken down to the next functional level

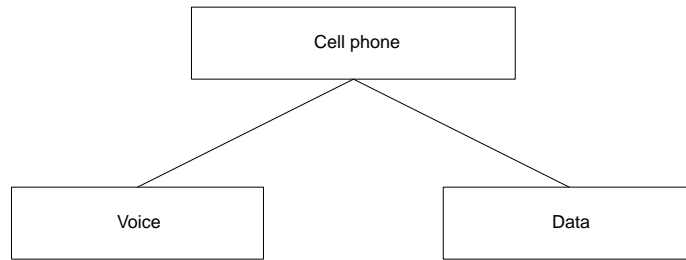


FIGURE 9.3 *An alternative breakdown of a multifunction phone*

We could debate whether auto dial is an offline or online function (it is assumed to be an online function for this example). The intent is not to break down an actual cell phone completely but to demonstrate that the same result can be reached with differing approaches. An actual cell phone can have many additional features and administrative functions, and the transceiver could be broken down to transmitter and receiver or to administrative/overhead transmissions and payload transmissions, and so on. The important thing to notice is that the same 10 branches of the breakdown tree are present in both Figure 9.4 and Figure 9.5. The ends of these branches are microphone/speaker, keypad/display, usage monitor, settings, contacts, e-mail read, e-mail compose, auto dial, speech, and transceiver. The choice of functional breakdown is left to your preference and the type of application or device being analyzed.

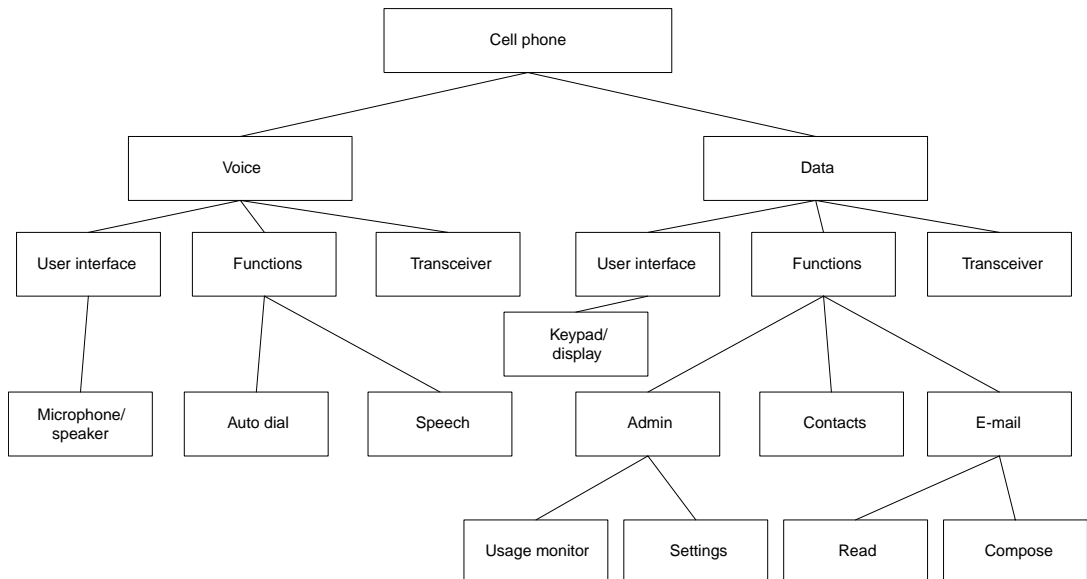


FIGURE 9.4 *A continued breakdown of a multifunction phone*

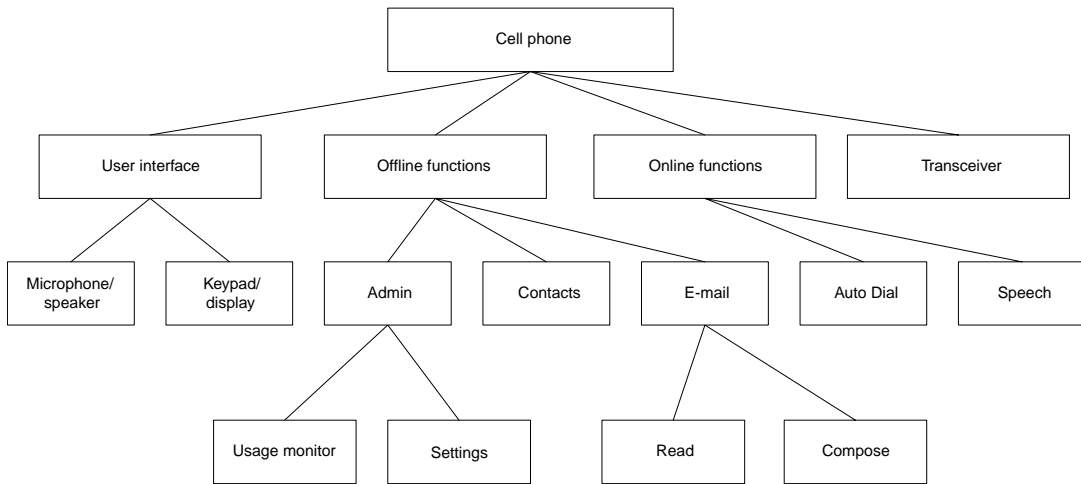


FIGURE 9.5 *An alternative breakdown of a multifunction phone*

Now that we have shown a breakdown for a typical multifunction cell phone, let's assume that the wireless device is a typical wireless PDA. This serves two purposes. First, you do not have to consider voice communications. Second, you will not jump ahead because you already know how the next level will be broken out. Figure 9.6 shows the wireless PDA broken down to the second functional level. Examining each functional block, you repeat the earlier process of identifying targets or components to protect.

The User Interface

Examining the user interface at this level, you consider the need to protect the display and keys from damage or inadvertent input while the device is being transported (after all, the whole point of wireless is to enable mobility). Now, you may be wondering, why are we concerned about damage to the display in a security book? Recall that one of the security principles discussed in Chapter 2 is Integrity. We assert that integrity applies not only to data but also to the system. Under this premise, the ability to access

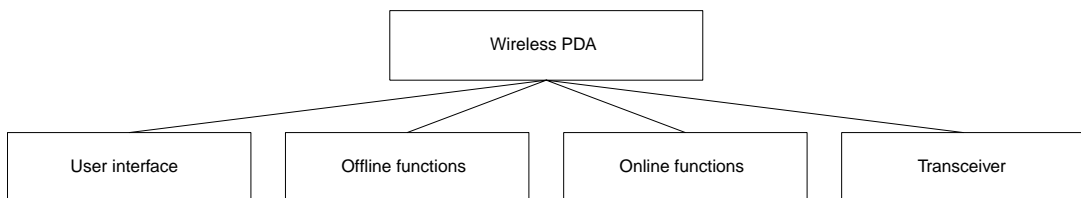


FIGURE 9.6 *A wireless PDA showing the second functional level*

data on demand is a security concern. Furthermore, if the screen becomes damaged, can you guarantee that the information you receive is accurate? It is not outside the realm of possibility for a user to misinterpret a letter because the confirmation code received contains an *O* instead of a *U* and the display is damaged where those pixels should be. Arguably, this would fall under the Development and Operational principle of Functionality or Utility. This is certainly true, but also recall that these principles are often related and interdependent. Your list now looks like this:

Wireless Device

The wireless device itself

User Interface

The physical interface

Access to the user interface

Offline Functions

In examining offline functions, several potential targets come to mind. Personal data—such as information in an address book or calendar files (names, addresses, phone numbers, or public and private keys)—stored on the PDA should be protected from unauthorized access. As m-commerce becomes more prevalent, PDAs will store bank account, brokerage, and credit card information that must be protected. Corporate or other nonpersonal information housed on the PDA should be protected. The list of data potentially stored on a PDA extends as far as the imagination (and device engineers) will allow. The point is that no one other than those who are authorized should have access to information stored on the PDA.

Online Functions

In examining online functions, the same offline concerns apply. The difference is that unauthorized access is obtained as the information transits the air or the wired network. In addition to data, the user's activity and usage patterns should not be available to unauthorized parties. This introduction of additional data to protect is not the whole picture, though. The user's location and movements are also in need of protection, with the incorporation of GPS technology into wireless devices. Finally, *spoofing* the user (the use of the device or a similar device by an unauthorized user pretending to be an authorized user) to obtain service or data should be disallowed.

The Transceiver

The transceiver should be protected from tampering by someone who has gained unauthorized access to the device. By way of example, the transceiver could be changed in such a way that it always accesses a different service provider's transceiver

or an attacker's transceiver. (Spoofing the device's service provider, vulnerabilities, and attacks are discussed in greater detail in Chapter 10, "Analyze Attacks and Vulnerabilities.") The attacker then communicates with the service provider, on the user's behalf, thereby giving the attacker the ability to monitor and control the user's activities.

Now, if you are imagining the intricacies that must fall into place for this to occur, you may immediately think that this is an awfully elaborate man-in-the-middle attack and not very likely to occur against the average wireless user. Although we concur, keep in mind that the goal of this phase is to identify targets for completeness, separate from any assessment of vulnerability or likelihood of realization. The task of prioritizing and making those kinds of trade-offs occurs during the I-ADD define phase. To be aware of the full set of risks associated with a given system, all possible attacks must be examined. Ruling out the least feasible ones is the secondary and simpler part.

Each functional block at this level is then broken down to the next functional level. We will not do so here because the discussion would become too dependent on the specifics of the PDA or application being used. Further, many of the preceding issues would simply be repeated for each of the lower-level blocks, particularly under the two *Functions* boxes. However, in analyzing a specific PDA or application for wireless use, this process should continue to the same depth as the functional design process to ensure that security issues are considered for these lower-level functional blocks as well.

Examining the targets list at this point yields the following:

Wireless Device

The wireless device itself

User Interface

The physical interface

Access to the user interface

Offline Functions

Personal data on the PDA

Corporate or third-party information

Online Functions

Personal data being sent

Corporate or third-party information being sent

User online activities, usage patterns

Location and movement

Access to network and online services

Transceiver

The transceiver itself

The Service Provider

The next functional block to examine is the transceiver of the service provider (refer to Figure 9.1). For the sake of brevity, we use the term *transceiver* here, although the component we are referring to is the service provider infrastructure, which provides wireless connectivity between the wireless device and the rest of the wired world. At this level, the transceiver needs to be physically protected. Logically, it needs to protect its services from unauthorized use. From the wireless side, the transceiver needs to ensure that users are authorized to use its services. From the wired side, the transceiver—or more appropriately, the service provider—needs to ensure that its services are accessed only by authorized entities and thereby obtains access to the wireless users.

As with the wireless device, when this level is complete, you break it down to the next functional level (see Figure 9.7).

The Transceiver

For our purposes, we do not need to drill further beyond the higher-level targets. If a functional block is identified, it should be listed and retained so that there will be no confusion about whether it was considered by others or during a review at some point in the future.

This is an appropriate time to state something that may or may not be obvious. A common target across all functional elements is physical protection. Having physical access to a device or resource makes an attacker's job much easier. Hence, perimeter security fencing, the presence of armed guards, as well as locks and alarms on buildings contribute greatly to overall security in wired systems. With wireless systems, this fundamental aspect of security goes right out the window. Wireless systems eliminate the need for legitimate and illegitimate users to have physical access to the network. Put another way, unless you encase the wireless system in an RF shielded enclosure, an attacker is going to be able to identify the network, and no number of armed guards around the tower is going to prevent her from attempting to access the system

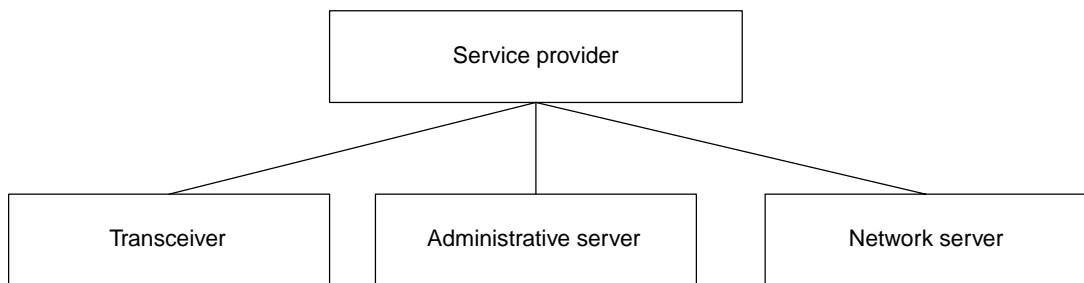


FIGURE 9.7 A second-level breakdown of the transceiver

if that is her intent. This doesn't mean that you should just pack up your bags and head home. Quite the contrary, you need to acknowledge this fact and design systems that are secure in spite of this big plus in the attacker's column.

The Administrative Server

Two additional targets become apparent when examining this functional block. First is user-specific data, which must be protected from unauthorized disclosure. Second is corporate proprietary data or resources, which must be protected from unauthorized disclosure. We will not break the service provider down to additional functional levels. For our purposes, this is sufficient. However, we do want to point out that the administrative server can be broken down to several additional levels, depending on the service provider architecture. Potential lower-level functional blocks would be authentication functions, billing functions, fraud detection functions, and performance monitoring functions.

The Network Server

This functional block is likely to have corporate proprietary data or resources that must be protected from unauthorized disclosure. As with the administrative server functional block, we will not break this functional block down any further because it quickly becomes provider-specific.

This completes the service provider functional block, and the targets list now looks like this:

Wireless Device

The wireless device itself

User Interface

The physical interface

Access to the user interface

Offline Functions

Personal data on the PDA

Corporate or third-party information

Online Functions

Personal data being sent

Corporate or third-party information being sent

User online activities, usage patterns, location and movement

Access to network and online services

Transceiver

The transceiver itself

Transceiver (Service Provider)

The transceiver itself
The transceiver services
Access to its subscribers

*Transceiver**Administrative Server*

User-specific data
Corporate proprietary data and resources

Network Server

Corporate proprietary data and resources

The identify phase is then continued to the next functional block of Figure 9.1, the gateway. The gateway's role is discussed in Chapter 1, "Wireless Technologies." Although the term *gateway* is most associated with cellular phones, its function of converting standard Web pages to the format used by wireless devices is common. These gateways can be co-located with the Web servers or with the wireless service providers.

The Gateway

Examining the high-level functional block, you can readily identify several targets. The gateway must be physically protected from loss or theft. User-specific data must be protected from unauthorized disclosure. The user's data must be protected from unauthorized disclosure. Corporate proprietary data and resources must be protected from unauthorized disclosure. Third-party data must be protected from unauthorized disclosure as it transits the gateway. The integrity of the data processed by the gateway must be maintained.

The gateway can be broken down to additional functional levels, but we will not do so here. By now, the process should be clear, so we do not want to belabor the point. Likewise, we will not break down the remaining high-level functional blocks listed in Figure 9.1. The following is the complete target list:

Wireless Device

The wireless device itself

User Interface

The physical interface
Access to the user interface

Offline Functions

Personal data on the PDA
Corporate or third-party information

Online Functions

Personal data being sent

Corporate or third-party information being sent

User online activities, usage patterns, location and movement

Access to network and online services

Transceiver

The transceiver itself

Service Provider

The transceiver itself

The transceiver services

Access to its subscribers

Transceiver

Administrative Server

User-specific data

Corporate proprietary data and resources

Network Server

User data

Corporate proprietary data and resources

Gateway

The physical gateway

User-specific data

User data

Corporate proprietary data and resources

Third-party data transiting the gateway

Web Server

The physical Web server

User-specific data

User data on the Web server

Corporate proprietary data and resources on the Web server

Aggregate commercial data stored on the Web server

User or corporate data in transit

Backend System

The physical backend system

User-specific data on the backend system

User data on the backend system
Corporate proprietary data and resources on the backend system
Aggregate commercial data stored on the backend system

Identify Roles

The second step in the I-ADD process is to identify the roles associated with the system. Let's review what we mean by *roles*. A role is simply an individual or group of individuals who plays a role in either protecting or exploiting a target. As we proceed through the process of identifying roles, this should become clear. At this point, the easiest way to proceed is to go through the targets list and identify the roles associated with each target. We will not explain these roles in detail here. As you read through the list, try to identify why each role is listed where it is. We discuss the roles in more detail in the section "Vulnerabilities and Theoretical Attacks" in Chapter 10.

Malicious Users

You will soon notice the ever-present malicious user. The term *malicious* is used liberally. What we are referring to is an individual or group who has the knowledge, skills, or access to compromise a system's security. *Malicious user* is a generic category encompassing a variety of roles that deserve additional discussion. A malicious user can be any of the following.

Organized Crime (Financial Motivation)

These malicious users are capable, motivated, well organized, and well funded. They are intent on operations such as cloning cell phones or other wireless devices and stealing money, goods, and services. Organized crime is the most capable category of attackers. Their ability stems from having the resources available to obtain the necessary hardware, software, and knowledge to mount sophisticated attacks quickly if the potential financial benefits justify the effort.

Hackers (Nonfinancial Motivation)

These malicious users are also capable, motivated, and well organized and may be well funded. Although hacker interest in wireless systems may initially be sparked by the financial or proprietary information the system protects, their attacks are generally focused on achieving notoriety. Attacks that can be expected of hackers include small-scale and wide-scale disruption of operations and the collection and release of sensitive information.

Malicious Programmers (Financial or Brand Damage)

These malicious users vary in their technical ability and are usually highly motivated by personal greed, grievance, or grudge. They are usually not well organized but may possess significant knowledge of the wireless system and access to internal processes. Malicious programmers can originate from various sources: a disgruntled employee at a wireless manufacturer; an application programming contractor; operations and support personnel; a knowledgeable programmer who feels wronged by someone associated with the manufacture, distribution, or management of a wireless system or device; a programmer who feels wronged by an individual or a company using wireless systems or devices.

Also in this group we consider attackers with nonmalicious intent whose actions can incur security issues, either inadvertently or because of an interest in improving the system's security. The information and vulnerabilities generated by nonmalicious attackers are capitalized on by malicious attackers if not immediately addressed by the affected wireless component or system.

Academics and Security Researchers

These attackers are capable, motivated, well organized, and often well funded. Academics and security researchers can analyze the security of a wireless component or system from an intellectual standpoint to determine how the system is designed or whether and how potential vulnerabilities have been addressed. They look at both the theoretical and practical implementation of the system, focusing primarily on issues in their area of expertise for the purposes of advancing the field, or their standing in the field. Although this group does not have malicious intent, malicious attackers can use their findings before mitigation or corrections are in place. This group is more likely to inform the vendor when a vulnerability is detected, before publishing their results, although this is not guaranteed.

Inexperienced Programmers and Designers

Although they do not fit most standard definitions of a malicious user, inexperienced programmers and designers can inadvertently create security issues and are considered malicious for this analysis. These inexperienced personnel are motivated to perform a specific task to support a wireless system, but they do not possess the skill or experience necessary to execute the task properly. The mistakes and oversights made by these personnel affect the operation of wireless components and can adversely affect the security of the wireless system. Other attackers exploit the vulnerabilities generated by inexperienced personnel.

Mapping Roles to Targets

Wireless Device

The wireless device itself

Device manufacturer

User

Malicious user

User Interface

The physical interface

Device manufacturer

User

Environment

Access to the user interface

Device manufacturer

Application (app) developer

User

Environment

Offline Functions

Personal data on the PDA

Device manufacturer

Device support personnel

App developer

App support personnel

User

Malicious device support personnel

Malicious app developer

Malicious app support personnel

Malicious user

Corporate or third-party information

Device manufacturer

Device support personnel

App developer

App support personnel

User

Malicious device support personnel

- Malicious app developer
- Malicious app support personnel
- Malicious user

Online Functions

Personal data being sent

- Device manufacturer
- Wireless service provider (WSP)
- WSP operations, maintenance, and support personnel (OMS personnel)
- App developer
- App support personnel
- User
- Malicious WSP
- Malicious device support personnel
- Malicious WSP OMS personnel
- Malicious app developer
- Malicious app support personnel
- Malicious user

Corporate or third-party information being sent

- Device manufacturer
- WSP
- WSP OMS personnel
- App developer
- App support personnel
- User
- Malicious WSP
- Malicious device support personnel
- Malicious WSP OMS personnel
- Malicious app developer
- Malicious app support personnel
- Malicious user

User online activities, usage patterns, location and movement

- Device manufacturer
- WSP
- WSP OMS personnel
- App developer
- App support personnel
- User

Malicious WSP
 Malicious device support personnel
 Malicious WSP OMS personnel
 Malicious app developer
 Malicious app support personnel
 Malicious user

Access to network and online services

Device manufacturer
 WSP
 WSP OMS personnel
 App developer
 User
 Malicious device support personnel
 Malicious WSP OMS personnel
 Malicious app developer
 Malicious user

Transceiver

The transceiver itself

Device manufacturer
 Device OMS personnel
 User
 Malicious device OMS personnel
 Malicious user

Service Provider

The transceiver itself

WSP
 WSP OMS personnel
 Malicious OMS personnel
 Malicious user

The transceiver services

WSP
 WSP OMS personnel
 Malicious OMS personnel
 Malicious user

Access to its subscribers

WSP

- WSP OMS personnel
- Corporate/private servers
- Corporate/private server OMS personnel
- Content providers
- App developer
- App support personnel
- User
- Malicious WSP OMS personnel
- Malicious corporate/private servers
- Malicious corporate/private server OMS personnel
- Malicious content providers
- Malicious app developer
- Malicious app support personnel
- Malicious user

Transceiver

Administrative Server

- User-specific data
 - WSP
 - WSP OMS personnel
 - App developer
 - App support personnel
 - Malicious WSP OMS personnel
 - Malicious app developer
 - Malicious app support personnel
 - Malicious user
- Corporate proprietary data and resources
 - WSP
 - WSP OMS personnel
 - App developer
 - App support personnel
 - Malicious WSP OMS personnel
 - Malicious app developer
 - Malicious app support personnel
 - Malicious user

Network Server

- User data
 - WSP

WSP OMS personnel
App developer
App support personnel
Malicious WSP OMS personnel
Malicious app developer
Malicious app support personnel
Malicious user

Corporate proprietary data and resources

WSP
WSP OMS personnel
App developer
App support personnel
Malicious WSP OMS personnel
Malicious app developer
Malicious app support personnel
Malicious user

Gateway

The physical gateway

Gateway manufacturer
OMS personnel
App developer
App support personnel
Malicious OMS personnel
Malicious app developer
Malicious app support personnel
Malicious user

User-specific data

Gateway manufacturer
OMS personnel
App developer
App support personnel
Malicious OMS personnel
Malicious app developer
Malicious app support personnel
Malicious user

User data

Gateway manufacturer

- OMS personnel
- App developer
- App support personnel
- Malicious OMS personnel
- Malicious app developer
- Malicious app support personnel
- Malicious user

Corporate proprietary data and resources

- Gateway manufacturer
- OMS personnel
- App developer
- App support personnel
- Malicious OMS personnel
- Malicious app developer
- Malicious app support personnel
- Malicious user

Third-party data transiting the gateway

- Gateway manufacturer
- OMS personnel
- App developer
- App support personnel
- Malicious OMS personnel
- Malicious app developer
- Malicious app support personnel
- Malicious user

Web Server

The physical Web server

- Web server manufacturer
- Web server OMS personnel
- Content providers
- App developer
- App support personnel
- Malicious Web server OMS personnel
- Malicious content providers
- Malicious app developer
- Malicious app support personnel
- Malicious user

User-specific data

- Web server manufacturer
- Web server OMS personnel
- Content providers
- App developer
- App support personnel
- Malicious Web server OMS personnel
- Malicious content providers
- Malicious app developer
- Malicious app support personnel
- Malicious user

User data on the Web server

- Web server manufacturer
- Web server OMS personnel
- Content providers
- App developer
- App support personnel
- Malicious Web server OMS personnel
- Malicious content providers
- Malicious app developer
- Malicious app support personnel
- Malicious user

Corporate proprietary data and resources on the Web server

- Web server manufacturer
- Web server OMS personnel
- Content providers
- App developer
- App support personnel
- Malicious Web server OMS personnel
- Malicious content providers
- Malicious app developer
- Malicious app support personnel
- Malicious user

Aggregate commercial data stored on the Web server

- Web server manufacturer
- Web server OMS personnel
- Content providers

- App developer
- App support personnel
- Malicious Web server OMS personnel
- Malicious content providers
- Malicious app developer
- Malicious app support personnel
- Malicious user

User or corporate data in transit

- Web server manufacturer
- Web server OMS personnel
- Content providers
- App developer
- App support personnel
- User
- Malicious Web server OMS personnel
- Malicious content providers
- Malicious app developer
- Malicious app support personnel
- Malicious user

Backend System

The physical backend system

- Backend system manufacturer
- Backend system OMS personnel
- App developer
- App support personnel
- Malicious backend system OMS personnel
- Malicious app developer
- Malicious app support personnel
- Malicious user

User-specific data on the backend system

- Backend system manufacturer
- Backend system OMS personnel
- App developer
- App support personnel
- Malicious backend system OMS personnel
- Malicious app developer

Malicious app support personnel
 Malicious user
 User data on the backend system
 Backend system manufacturer
 Backend system OMS personnel
 App developer
 App support personnel
 Malicious backend system OMS personnel
 Malicious app developer
 Malicious app support personnel
 Malicious user
 Corporate proprietary data and resources on the backend system
 Backend system manufacturer
 Backend system OMS personnel
 App developer
 App support personnel
 Malicious backend system OMS personnel
 Malicious app developer
 Malicious app support personnel
 Malicious user
 Aggregate commercial data stored on the backend system
 Backend system manufacturer
 Backend system OMS personnel
 App developer
 App support personnel
 Malicious backend system OMS personnel
 Malicious app developer
 Malicious app support personnel
 Malicious user

As you can see, this can quickly become a long list. Now that we have concluded the identification of the roles, it is worth discussing two observations that will assist you in performing future role identification. First, in general, whenever people are involved in protecting a target, they almost always are also listed in the malicious section against that target. We are not saying that the same people will be involved, but that the *category* of people or that group's *level of access* can be used maliciously.

This concludes the I-ADD identify phase. You break down the system into functional blocks and then examine each block to determine which resources or data

(targets) require protection at that level. The blocks are then examined to see whether they should be further broken down to lower-level functional blocks, where the process is repeated until you reach the lowest-level functional blocks practical for the type of analysis or design you are conducting. After identifying the targets, you determine the roles that affect the targets. With the roles and targets identified, you are ready to move to the I-ADD analyze phase.