A CRC PRESS FREEBOOK

Cybersecurity: Intrusions, Vulnerabilities & Systems

NaSPA
Network and Systems Professionals Association

CRC Press
Taylor & Francis Group

TABLE OF CONTENTS

Introduction

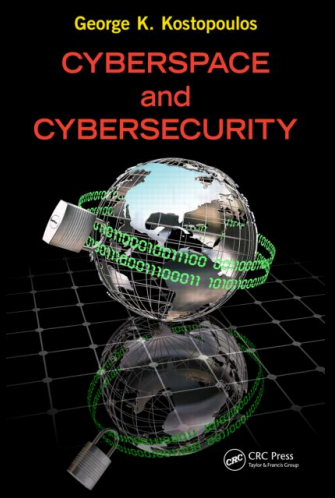
Chapter 1: Vulnerabilities in the Organization from *Cyberspace and Cybersecurity*

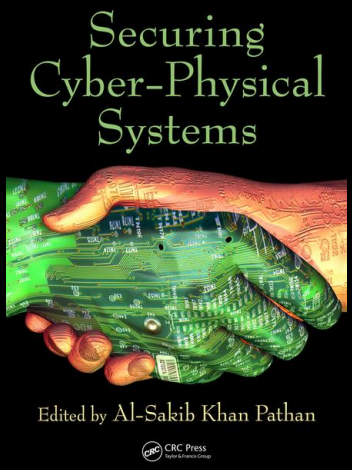
Chapter 2: Cybersecurity and the CIO from *Cyberspace and Cybersecurity*

Chapter 3: Cyberspace Intrusions from *Cyberspace and Cybersecurity*

Chapter 4: Securing Power Systems from *Securing Cyber-Physical Systems*

Learn the Traits a CIO Must Have to Address Cybersecurity Challenges!





Visit www.crcpress.com to browse our collection of books in Information Technology and Engineering-Electrical

SAVE 20% and receive **FREE Shipping**, simply enter code **JWR37** at time of checkout.

Introduction

About this FreeBook

Introduction by Leo A. Wrobel, President, Network and Systems Professionals Association.

Welcome to the world of FREE NaSPA Books! This is a new experiment for our membership. We hope it helps each of you find meaningful content from reputable, published experts on the topics that interest you most. The title of this first NaSPA FreeBook is *Cybersecurity: Intrusions, Vulnerabilities & Systems*. We chose this collection of relevant material based on a recent survey we conducted with our members. If you like this approach, let us know and we'll make it a regular feature. Email your comments and suggestions to president@naspa.com and watch for the next member survey.

You will find the following topics in this compendium:

Section 1 – Securing Power Systems

Security issues for the power industry are taking center stage as that industry relies more than ever on networking and automation protocols. The next generation of electrical grid incorporates significant advances in communications and control that closely couple cyber and physical systems. This enables new capabilities, but also exposes new vulnerabilities. If you are dependent on the power grid, and who isn't these days, you owe it to yourself to check out this Section.

Section 2 – Vulnerabilities in the Organization

An unclassified US government report has revealed that *"The great majority of past compromises have involved insider, cleared persons with authorized access who could circumvent physical security barrier, not outsiders breaking into secure areas."* This is why establishment of policies as to how

data should be entered, modified, read, or deleted, constitutes the backbone of data security in any enterprise. Learn the secrets here.

Section 3 – Cybersecurity and the CIO

One of the things I have loved most about NaSPA is watching the steady development of my peers in the industry. I have written for NaSPA since the late 1980's. That's a long time. Many of the NaSPA members I started off with 25 or 30 years ago have advanced into prestigious management positions. And as technology becomes more and more important to their organizations, their role changes from Technology Steward to Business Leader. His or her mission is no longer centered on the day-to-day operations, but rather on increasing the value of information technology to shareholders, stakeholders, and other constituents. If this describes you, you can find some very useful tips in this insightful Section.

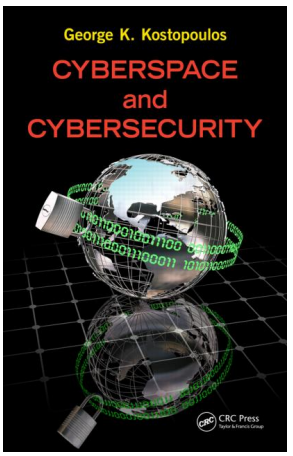
Section 4 – Cyberspace Intrusions

Information systems are defended by traffic analysis systems designed to detect and block intrusions. **Intrusion Detection and Prevention Systems** (IDPS). IDPSs implement rules established by the security administrator for protecting access or entry points. Based on these rules, the IDPS passes, blocks, delays, or diverts data traffic. IDPSs are broadly classified into four types of systems. Learn more about each of them in this Section.

Our very special thanks to longtime NaSPA supporter and sponsor CRC Press for this fine content. NaSPA members enjoy a 15% discount on ALL CRC Press books and products. Visit CRC Press at https://www.crcpress.com/ and learn more.

CHAPTER 1

Vulnerabilities in the Organization



Learn More:

Chapter 2

Vulnerabilities in the Organization

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

Introduction

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

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

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

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

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

Common Organizational Vulnerabilities

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

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

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

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

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

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

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

Access Authorization and Authentication

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

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

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

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

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

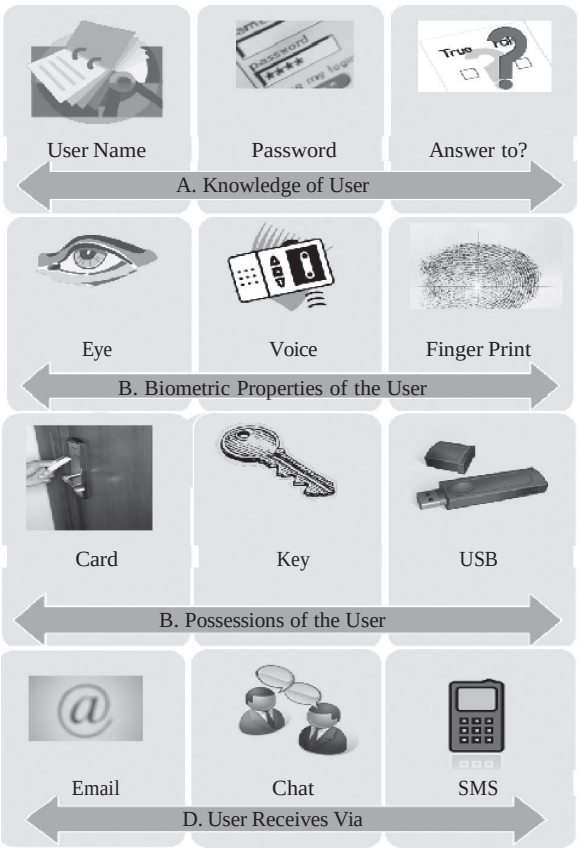


Figure 2.1 Authorization criteria.

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

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

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

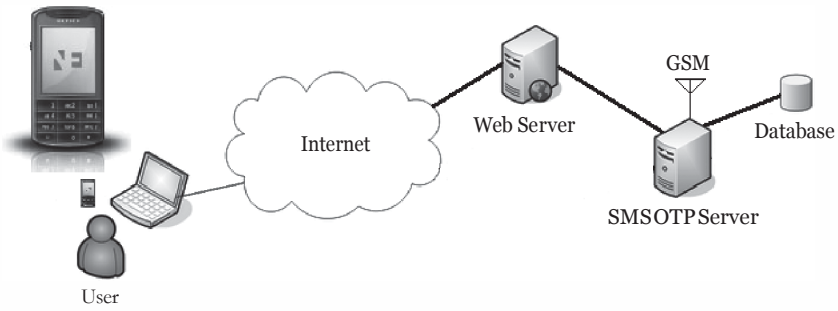


Figure 2.2 Authentication technology using an OTP delivered as an SMS to the user. (Courtesy of Nordic Edge, http://www.nordicedge.se.)

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

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

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

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

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

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

---

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

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

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

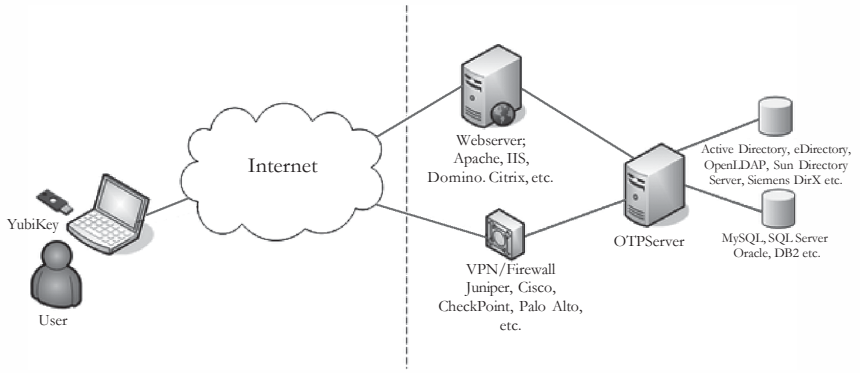


Figure 2.4 Authentication technology network using biometrics (fingerprint) and OTP. (Courtesy of Nordic Edge, http://www.nordicedge.se.)

Human Factors

An unclassified US government report has revealed that The great majority of past compromises have involved insider, cleared persons with authorized access who could circumvent physical security barrier, and not outsiders breaking into secure areas. Personnel, whose activities involve the Internet or other modes of data handling, constitute a critical organizational asset, which may turn into a weak link. Their activities may be writing code, programming databases, using a USB storage device, or merely sending emails. Each and every such activity needs to be per- formed in a security-minded way and in accordance to policies. Technology alone is not the answer.

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

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

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

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

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

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

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

Security Services

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

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

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

Table 2.1 Security Consultancy Services

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

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

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

External Technologies

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

This technology finds application in numerous industries, such as emergency response services, law enforcement, cargo security, nuclear materials transport, air- craft navigation, and critical time and synchronization standards for utilities, tele- communications, and computer networks.

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

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

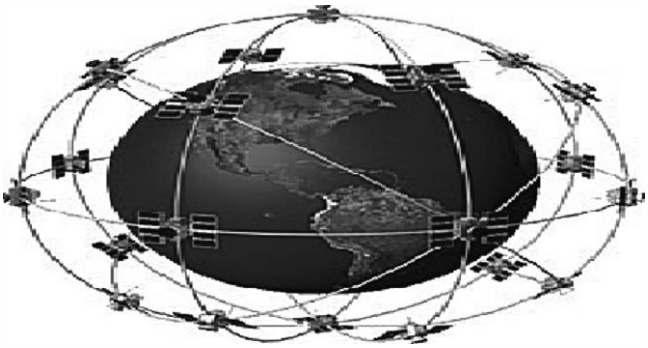


Figure 2.5 The GPS and its twenty-four satellite constellation.

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

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

Wireless Networks

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

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

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

Bluetooth

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

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

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

Figure 2.6 PAN employing BT technology.

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

Passive Vulnerabilities

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

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

Active Vulnerabilities

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

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

Precautions

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

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

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

Wireless Fidelity

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

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

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

---

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

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

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

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

Table 2.2 802.11 Wireless LAN Basic Characteristics

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

Wi-Fi Precautions at Home

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

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

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

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

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

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

point to broadcast its SSID identity to the world. Usually, this ID is entered manually, and only once, during laptop login and is remembered afterwards. **Four: Change Router's Access.** The router, located in the AP, is accessible via a name and a password. They are set at the initial installation, but can be reconfigured at any time. These two parameters should be changed at intervals. Also, the default fictitious local, intranet, IP address, which may have come as 192.168.1.1, can be changed to any other, as long as the numbers in the four fields range from 0 to 224, without leading zeros. Also, there is no need to keep the default router name. To the contrary, any change from the default values will contribute to a better security posture. Typically, the default values are the same for all access points of a given manufacturer and are usually known to intruders.

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

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

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

---

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

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

Wi-Fi Precautions at the Hotspot

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

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

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

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

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

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

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

---

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

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

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

Wi-Fi Precautions at the Enterprise

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

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

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

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

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

Worldwide Interoperability Microwave Access

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

WiMAX Features

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

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

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

---

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

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

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

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

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

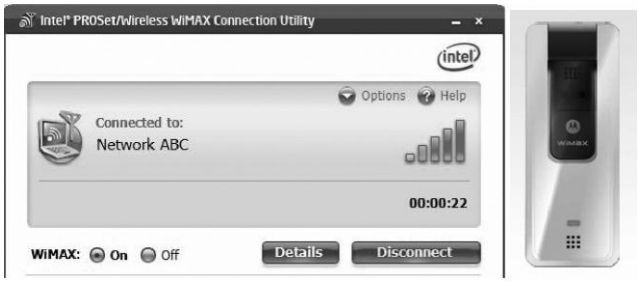


Figure 2.8 WiMAX control window and a USB WiMAX adapter. (From Intel, http://download.intel.com/support/wireless/wmax/5350_5150/S6/intelrproset wirelesswimax userguide.pdf.)

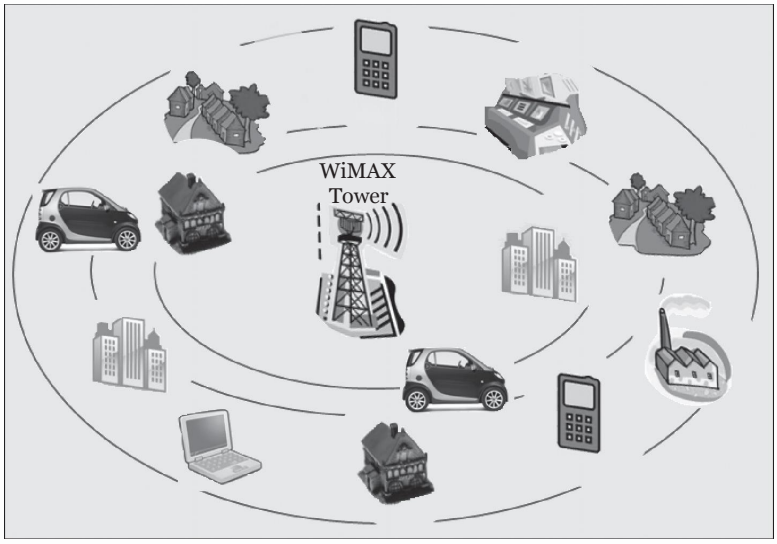


Figure 2.9 Typical WiMAX network where Internet access can be wirelessly provided to a metropolitan area.

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

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

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

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

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

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

Cloud Computing

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

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

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

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

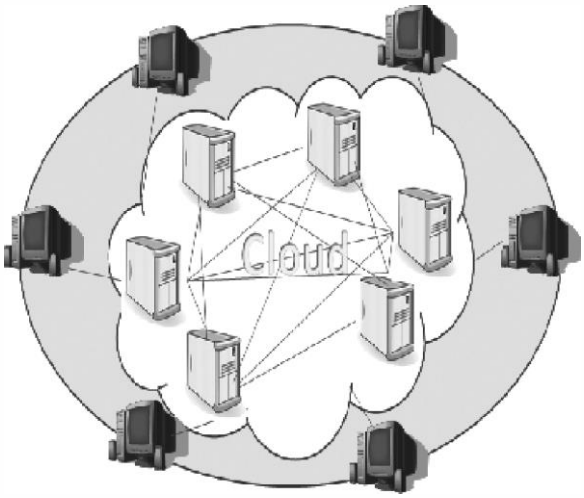


Figure 2.10 Cloud computing. The only user requirement is Internet access.

Table 2.3 Cloud Computing Option

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

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

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

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

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

Table 2.4 Cloud Computing—Advantages

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

Table 2.5 Cloud Computing—Disadvantages

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

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

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

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

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

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

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

Cybersecurity and the CIO

Chapter 5

Cybersecurity and the CIO

Cybersecurity is an integral part of any security concept, be it corporate or national.

Introduction

Over time, the position of the most critical person in an enterprise changes. Today, that most critical person is the Chief Information Officer (CIO). At the same level, above or below, or the same person is the Chief Technology Officer (CTO) and the Chief Information Security Officer (CISO) of the enterprise. For all practical purposes, we will consider the CIO as being an all *three-in-one*. Being all three, the CIO is expected to be the organization's visionary, advising on how to leverage technology to achieve the organization's aims. The CIO is responsible for every aspect of information within the enterprise. The CIO's role within the organization can be described as follows:

- Member of the senior administrative/management/planning team
- Manager of the technology and other information resources
- Responsible for IT planning
- Responsible for the development of new systems
- Responsible for policy development and implementation

The position of the CIO demands a certain spectrum in the personality, education, and experience of the person.

Cyberspace is a maze of infinite vulnerabilities, the existence of which is typically discovered by attackers at a cost, at least to the first victim. The role of the CIO is to be aware of all protection mechanisms and have the ability to devise more where needed. This can be hoped for if CIOs enter their tenure with extensive applicable experience and expertise and with the understanding that the position of the CIO is the most life-long learning job.

CIO: Personality

Let us meet the CIO and see what qualifications and career path have brought that person to this position. Figure 5.1 shows the personal and professional qualifications a CIO needs to have to successfully address the demands of the position.

Trust and Ethics

One of the most highly trusted positions in an enterprise today is that of the CIO. The CIO is the bodyguard of the organization's information. The CIO must be self-confident and radiate trust and success. Trust is a personal characteristic, often subconsciously sensed, that makes a person welcome in any environment. Respect for self, others, the organization, and society is a cornerstone to trust. Self-confidence and radiation of success are acquired only through a sequence of prior successes, small and possibly big.

There is absolutely no substitute for consistently ethical behavior. There will be continuous pressures or *rewarding opportunities* to be unethical. Yet the CIO must stand above such temptations, take no risks, and in addition restrain the greed of others who suggest shortcuts to the straight line of ethics.

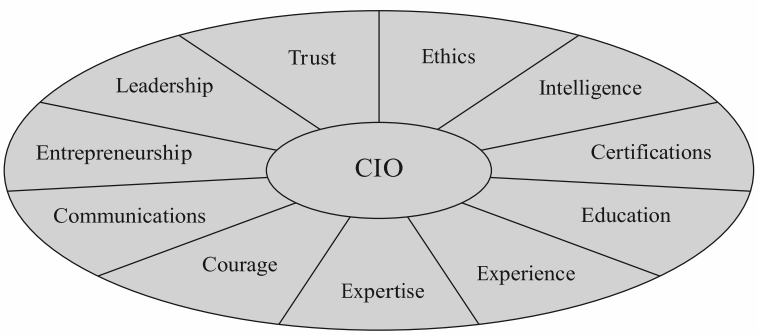


Figure 5.1 CIO personal and professional qualifications.

Communication and Intelligence

The CIO must be the organization's *great communicator*. This is the person who will have to persuade others for the acquisition of resources, where the word resources leave nothing outside. The CIO may need capital for a new technology or may need the loyalty and trust of colleagues in all directions of the hierarchy. Persuasion is needed for upward communications, and motivation and inspiration downward communications. In a modern organization, nothing is accomplished through *iron fists*. The CIO has to capture the mind and hearts of all within the enterprise, always remembering that "techie" language can be boring for the nontechies. Outside of the organization, the CIO joins relevant associations, attends fora, participates in conferences, and delivers seminars, thus acquiring visibility and most important polishing skills.

We cannot leave nature out of the CIO picture. Natural intelligence is the algorithm that converts observations to knowledge and knowledge to wisdom. Wisdom coupled with experience usually results in sound judgment. As the saying goes: smart people learn from their own mistakes, while wise people learn from the mistakes of others.

Leadership and Entrepreneurship

Some claim that a leader is born; others believe that a leader can be made. The CIO as a leader must be a level above the followers. This superiority, in the wholesome sense of the word, must be in personal qualities as well as in technical skills. The CIO as a leader, walking through the hallways of the enterprise, as the expression goes, must be viewed as a *guide-by-the-side* and not as a *sage-on-the-stage*.

For the CIO to be received in that manner, that person must be very humble and very knowledgeable and experienced. Everyone in an organization wants to see a friend in the person of the CIO. This is because the CIO is the great gatekeeper, granted with authority that hopefully matches the responsibility that has been placed on that person's shoulders. The CIO and the executives of the enterprise must realize the CIO is a strategic position that provides direction, and the CIO should not become entangled in low-level technical problems. However, the CIO must have the experience to provide direction for the solution of the problems.

The CIO is always looking for opportunities to enhance the organization's business posture, willing to take non-catastrophic risks. The CIO must be a visionary "who can challenge conventional wisdom," with a supervisory style that is well balanced between granting autonomy and applying controls.

Courage and Limitations

CIOs with the above qualifications must be able to foresee the viability of a proposed idea and must have the necessary courage—derived from job security and

upper management support—to be able to freely and objectively express their opinions.

Equally, the CIO should be able to drop a project that appears to be heading in the wrong direction. With unpredictable technology advances, good ideas may not be as good because new solutions make themselves available continuously. The CIOs, besides recognizing technological limitations, above all should recognize their own limitation, be it human or technical.

Becoming a successful CIO is like going up the stairs, it has to be done one step at a time. Once there, it is not a playground. Being a CIO is a mission and not a pleasant occupation. The CIO is an integral and most critical part of the enterprise. The CIO must have a *love affair* with technology. Millions of engineers, worldwide, are producing new technologies or new malware, and the CIO can never say, "I do not know." The CIO can only say, "At the moment I don't know, but in 48 hours I will have an educated opinion about it."

CIO: Education

University Degrees

The CIO must hold college degrees that indicate an information systems education. The degree(s) must bear the word computer or information, while the respective curriculum must include courses that started with the binary numbers and logic gates and ended with capstone courses that have delved with networks. The CIO is expected to have a technical graduate degree. Many universities now offer MBA degrees in information systems that best prepare CIO position candidates. Table 5.1 lists typical courses that are included in such degree programs.

Certifications

Besides the expected college education, the CIO must have certifications that show technological currency. Depending on the career path the CIO has followed within the information systems profession, current related certifications are expected to be held for such a position.

Table 5.2 presents a partial list of certifications in information systems offered by industry-leading organizations. While university degrees imply broad knowledge on a subject, certification confirms expertise in a particular technology sector.

CIO: Experience

The CIO must have reached the position *through the ranks*. Education alone will not do it. That is, the person must have served in the IT sector in a meaningful capacity

for a number of years. Possibly, the person started as a design engineer or as a programmer, then became an analyst, a few years later a first level supervisor, and

Table 5.1 Typical Courses in MBA in Information Systems

Managerial and Business	*Technical*
Information Technology Project Management	**Systems Integration**
Business Process Innovation	**Database Management Systems**
Supply Chain Management	**Enterprise Architecture**
Security and Privacy of Information	**Knowledge Management**
Management of Information Services	**Software Engineering**
Information Systems Strategy	**Systems Development**
Global Systems Sourcing	**Mobile Applications Development**
International Information Technology Issues	**Wireless Networks**
Software Requirements Management	**Human Computer Interfaces**
Software Quality Management	**Business Computer Forensics**
Business Telecommunications and Networks	**Incident Response Systems**
Information Systems Legal Framework	**Cybersecurity**

so on. Parallel to that, the CIO-to-be was enhancing the background with related courses, seminars, and hopefully acquired a few certificates on the way.

With about ten to fifteen years of experience, and feeling confident about the already acquired qualifications in IT, the CIO-to-be ventures into the market *trying the waters*. The rest of it is a matter of matching the acquired soft and hard skills to the presented opportunities.

On average, about twelve years from college may get one to the CIO position, depending on the size of the organization and if the experience and education cards are played right. While career planning, the CIO-to-be must remember that "recruiters are looking for—proven success stories—not people who have the potential to succeed."

CIO: Responsibilities

With time, IT evolved as an integral and indispensable participant in any organization, and the need for a central figure, the CIO, became apparent. In 1996, it reached the point where, in the United States, a federal law was passed that

Table 5.2 Information Systems Certificates

Organization	*Certificate*
(ISC)²	**Information Systems Security Architecture Professional, ISSAP** **Information Systems Security Engineering Professional, ISSEP** **Information Systems Security Management Professional, ISSMP** **Certified Information Systems Security Professional, CISSP** **Certified Secure Software Lifecycle Professional, CSSLP** **Certified Authorization Professional, CAP** **Systems Security Certified Practitioner, SSCP** **International Information Systems Security Certification Consortium** **http://www.isc2.org/default.aspx**
CISCO Network Security	**Cisco Certified Entry Networking Technician–Security, CCENT** **Cisco Certified Network Associate–Security, CCNA** **Cisco Certified Security Professional, CCSP** **Cisco Certified Network Professional–Security, CCNP** **Cisco Certified Internetwork Expert–Security, CCIE CISCO, IT Certification and Career Paths** **http://www.cisco.com/web/learning/le3/learning_career_certifications_and_learning_paths_home.html**
ISACA	**Certified Information Security, CISM** **Certified in the Governance of Enterprise IT Manager, CGEIT** **Certified in Risk and Information Systems Control, CRISC** **Certified Information Systems Auditor, CISA** **Information Systems Audit and Control Association, ISACA** **http://www.isaca.org**

UMUC Certificates	**Chief Information Officer** **Homeland Security and Information Assurance** **Homeland Security Management** **Information Assurance** **University of Maryland University College** **http://www.umuc.edu/programs/grad/certificates/**
NYU Certificate	**Information Systems Security Certificate New York University** **http://www.scps.nyu.edu/areas-of-study/information-technology/professional-certificates/information-systems-security.html**

Table 5.2 (CONTINUED) Information Systems Certificates

Organization	*Certificate*
GIAC	**Certified Incident Handler, GCIH** **Certified Intrusion Analyst, GCIA** **Penetration Tester, GPEN** **Certified Firewall Analyst, GCFW** **Certified Windows Security Administrator, GCWN** **Web Application Penetration Tester, GWAPT** **Assessing and Auditing Wireless, GAWN** **Certified UNIX Security Administrator, GCUX** **Information Security Fundamentals, GISF** **Certified Enterprise Defender, GCED** **Certified Forensic Analyst, GCFA** **Reverse Engineering Malware, GREM** **Certified Forensic Examiner, GCFE** **Management Security Leadership, GSLC** **Information Security Professional, GISP** **GIAC, Global Information Assurance Certification** **http://www.giac.org/**

even included the responsibilities of the CIO within the various departments of the government. The CIO responsibilities are partially listed in Table 5.3 and highlighted in Figure 5.2. It is difficult to prioritize them, so they are listed in alphabetical order.

It is apparent that the CIO's responsibilities cover the entire spectrum of the information systems within the organization. In effect, the CIO is the organization's *Minister of Defense*.

Other responsibilities not explicitly stated in the above act include the following.

Data Backup and Archiving

The CIO has to design the implementation of plans made by the organization's Data Administrator for the real-time backing-up of the operational data. With the introduction of the *cloud* as a possible backup destination, additional security concerns need to be addressed because of the ambiguity as to the exact physical location of data.

Culture of Security

The CIOs in their capacity as the organization's Chief Information Security Officers bear the responsibility of creating a corporate *culture of security* that will serve as

Table 5.3 CIO Responsibilities (Clinger–Cohen Act of 1996)

Acquisitions	**Performance and results-based management**
Architecture	**Policy**
Business continuity	**Process improvement**
Capital planning and investment	**Program management**
Customer relations	**Risk management**
Innovations	**Security**
Leadership management	**Strategic planning**
Operations	**Technology assessment**

Figure 5.2 CIO professional responsibilities.

a subconscious guide in everyone's actions. The basic elements of a *culture of security* are, on one hand, the awareness as to the existence of threats and of their potential harm to the organization and, on the other, the adherence to the security rules.

Creating a *culture of security* is not easy, because it creates inconvenience to many. However, through training programs it will be understood that security measures are a very small price to pay for not having security incidents of possibly catastrophic consequences. While the CIO's actual security staff may be small in size, the virtual staff should include each and every member of the organization.

Cyber Training

Considering that technology is endlessly evolving, training of the organization's IT staff will have to be on a continuous basis. The CIO will need to have a career path for each and every member of the IT department, and training will contribute in the realization of a *live* career path. Training may be in-house, external, face-to-face, or online. Certifications must be an integral part of the organization's training philosophy, as well as training by vendors wherever applicable.

Contingency Plans

The CIO, in cooperation with organization's department heads, designs contingency plans for as many adverse eventualities as practically possible.

The CIO has come through the ranks of the organization's operations track and may mistakenly believe that the position is still of the operational level. This is very wrong, and unfortunately many CIOs get lost in technical details. The CIO position is a strategic-level position, and the CIO must be free of the CIO's operations hat. To accomplish that CIOs must "clone" themselves. That is, similar to the ships where the *first officer* is running the ship and not the captain, the CIO needs to have a *first officer* who will handle all the operational IT aspects of the organization. This way, the CIO will be able to concentrate on the strategic role—keeping track of technological advancements, securing resources for the organizational IT needs, and making certain that the morale and trust in the IT cadre are high.

Liability

It is not uncommon for CIOs to carry liability insurance, especially if they are working as independent consultants. There are numerous companies that offer such coverage, often extending to coverages of $5M.

CIO: Information Security

There are numerous components to information security. Table 5.4 itemizes the most important ones, classifying them as *internal* and *external*.

Internal Information Security Components

Access Control—Electronic

Here, we have three questions: Who? What? How? Sometimes one more question is added: When? Today's database systems allow access control down to the cell of a spreadsheet. Programming security to that level might be tedious, but these are options technology offers and should be weighed relative to the importance of the protected data. Data access can also be time-locked. Data can be accessible during working hours or after being specifically enabled.

With biometrics still not mainstream access controls, the user name and passwords remain the prevalent access control mechanisms. The password vulnerability

Table 5.4 Components in Information Security

Internal	*External*
Access control–electronic	Access control
Access control–physical	Compliance
Cyber awareness and training	Legal framework
Business continuity	Telecommunications
Operations security	Cryptography
Networks security	Firewalls
Security policy	Malware
Internet use policy	Digital signatures
Intrusion detection systems	Digital certificates

can be eliminated with the use of *two-factor authentication.* This is a technology where, once the user name is entered, the server sends the user a one-time password (OTP) via a relatively secure medium, such as an email or an SMS to the user's mobile phone.

The second factor in authentication can be one of several options in addition to the above mentioned. It may be a biometric parameter—fingerprint or voice sample—or may be a device—wireless or USB—that via the login computer sends the server a recognizable and identifiable code.

Access Control—Physical

In an enterprise, it is often the case where access is granted for specific areas of the facilities. In such cases, combination locks or card swiping devices allow authorized access. In the former case, the drawback is possible loss or compromise of the entry code, while in the latter, the drawback is possible loss of the card itself. A practical solution to physical access can be mobile phone-controlled locks where only authorized phone numbers can unlock and provide access. Such technologies also record a timestamp of the interaction and save all unauthorized entry attempts.

Cyber Policies

One of the CIO's major responsibilities is to draft the organization's Information Security Policy. This policy itemizes the rules based on which information travels within the organization and from the organization to other outside ones.

Cyber Awareness and Training

Cyber awareness is "protecting your personal information . . . and . . . keeping your computer safe and secure." The CIO promotes cybersecurity awareness through in-house communications, such as occasional email-newsletters and seminars, emphasizing that cybersecurity is a collective intra-organizational task and mission. **Cyber Awareness** can be quantified with the following list of advices:

- Always have a reliable and self-updating antivirus software installed.
- Always use the latest versions of needed software, including the installed operating system.
- Install the patches as soon as they are made available.
- In a Wi-Fi environment, disable the SSID broadcast, and apply the WAP/WEP encryption. Where possible, program the access point to the MAC of the allowed computers (for more see Chapter 4).
- In social networking, understand all the security and privacy measures, and apply them to your maximum protection. Do not post sensitive information and non-complimentary photos.
- When sending sensitive information, encrypt it and send the recipient the passcode via a mutually agreed medium, such as an SMS, an email, or over the phone.
- Review the cookies options of your browser, and select the one that you feel comfortable based on your surfing needs. Even better, program your browser to prompt you before accepting cookies.
- Program your browser to automatically turn off after X minutes of inactivity and to delete temporary Internet files and possibly the history and the cookies, if appropriate.

Training

Cyber awareness training courses can be found at no cost and may include the following parts:

- *Intro to Cyber Safety,* covering security settings in the personal computer and mobile phone, browser protection settings, document encryption, and password selection.
- *Malware Attacks,* covering viruses and the way they infect computers and mobile devices, and protection through appropriate settings and with the use of antivirus software.
- *High-End Attacks,* covering distributed denial of service attacks and protective countermeasures.
- *Cybercrime,* covering the various schemes of crime in cyberspace and ways to possibly recognize such schemes.
- *Netiquette*, covering the socially and professionally accepted etiquette in interacting over the Internet. This will include chatting, social networking postings, and emails.

Business Continuity

The CIO is responsible for having in place a Business Continuity Plan that has the knowledge and approval of the organization's senior management. The plan is for the "prevention, mitigation, preparation, response, and recovery of the organization's normal activities from emergencies." Detailed information security standards are specified in various published standards.

To successfully address an emergency that will create discontinuity in the normal operations of the organization, the CIO will need to have performed, as a minimum, the following two tasks:

1. **Business Discontinuity Cause–Impact Analysis.** This is a study that assesses the consequences of a possible adverse situation that will force the organization to interrupt the delivery of expected products or services. In the context of information systems, the adverse situations may be related to intraorganizational operations or to interorganizational cooperation. Such as,
    a. ***Front Office.*** Website server shut down, where the causes may be under capacity to handle legitimate tasks, denial-of-service attack, malware attack, natural disaster, or personnel problem.
    b. ***Back Office.*** Database storage or computation crash, where, similarly, the causes may be undercapacity, malware, non-malware bug, malware attack, natural disaster, or personnel problem.
    c. **Failure in Dependency.** The organization adds value to a certain product or service, and the supplier has failed. For example, an online

education delivery organization is using a leased platform that experiences operational problems.

d. **Failure in Compliance.** Organization's operations are suspended until compliance is achieved. Losses of certain data may require notification of the government regulators before resumption of operations.

The CIO performs an analysis addressing the above possible business discontinuity causes, and many more, and develops a Business Recovery Plan.

2. **Business Recovery Plan.** This is a plan that has been designed by the office of the CIO, has been adopted by the organization's senior management, and is ready to be implemented should an emergency arise. The plan identifies, by name or by position title, the person who will lead the business recovery process, the responsibilities and the authorities of that person, as well as the line of command to be followed until the organization exits from the state of emergency.

CIO: The Changing Role

As technology becomes more of a critical cornerstone of any organization, the role of the CIO changes "From Technology Steward to Business Leader . . . In this new world of technology-enabled transformation, . . . CIOs play an increasingly important role." The mission of the CIO is no longer to oversee the day-to-day operations of the data processing department, but it is to help the organization's leaders use information and technology to increase the worth of the produced and delivered service to the stakeholders.

The real metric of organizational success is the benefit offered to the stakeholders relative to the available resources. Today, practically every organization leverages on information to maximize that benefit. The aim is to make the offered products or services more productive to the user, more responsive to the market needs, and above all more accessible to the targeted markets.

1. The CIO is a *revolutionary* with a transformation vision who wants the organization to use technological advances to reach new heights in accomplishments. They may be measurable in efficiency, delivered service, or profits. In this quest, the CIO will find technology as the faithful ally and the organizational culture and bureaucracy as the constant adversary.

To best serve their organizations, CIOs must be granted the necessary resources, visibility, and participation so that they are exposed to organizational problems and concerns in order to provide technology-based recommendations.

Cyberspace Intrusions

Chapter 7

Cyberspace Intrusions

Cybersecurity is measures that are embedded into an information system during its development process.

Introduction

Intrusion, in the context of information systems, is a violation of established rules as to data access, where the violation may pertain to either reading or modifying protected data. Information systems are defended by dedicated traffic analysis systems designed to detect and hopefully block intrusions. Such systems, made of hardware and/or software, are referred to as Intrusion Detection and Prevention Systems (IDPS, often pronounced "eye-deps"). Depending on the particular application, a system may be an IDS, that is, only Intrusion Detection System with no prevention capabilities, or may be an IDPS, sometimes still referred to as IDS, that has both capabilities, detection as well as prevention. IDPSs implement rules established by the security administrator applicable to protecting access or entry points. Based on these rules, the IDPS passes, blocks, delays, or diverts data traffic. The selected action cannot be at human speed, thus requiring an *expert system,* ideally with *artificial intelligence,* to decide at an electronic speed for the needed action.
IDPSs are broadly classified into four types of systems, namely,

- Network-Based
- Host-Based
- Network Behavior Analysis
- Wireless

Table 7.1 Basic Requirements in IDPS

1. Security Services	*3. Operational Considerations*
Monitoring	**Scalability**
Devices	**Reliability**
Functions	**Interoperability**
Capabilities	**Reconfiguration**
Detection	**Documentation**
Prevention	**Technical support**
Reporting	**Training**
2. Capacity	*4. Cost-Effectiveness*
Computational	**Initial Cost**
Storage	**Maintenance cost**

The IDPS requirements are a map of the organization's security policy toward intrusions. Table 7.1 lists the basic IDPS requirements.

The implementation of these requirements is based on the available technologies, as applied to the projected needs, with cost-effectiveness as the parameter. There is a wide variety of IDPS tools that can provide events monitoring and information system security, vis-à-vis known threats. The number one target of an intruder is the protection mechanism of the information system. Initially, through a variety of attacks, intruders try to determine the strengths and weaknesses of the IDPS in an effort to recognize the presence of vulnerabilities through which to enter the system and access, or damage, targeted resources. Such resources may be passwords lists, files of sensitive content, or access mechanisms.

IDPS Configuration

Generally speaking, any system is made of three major components: the *sensors,* where data are collected from the environment and are partially processed; the *processor* that makes decisions as a result of data evaluation and correlation; and the *actuators* that, driven by the processor, affect the environment. Similarly, in the case of the IDPS, there are sensors, processing software, and affected units or functions.

Figure 7.1 shows an information system monitored by an IDPS. Table 7.2 lists the functions of the major IDPS components.

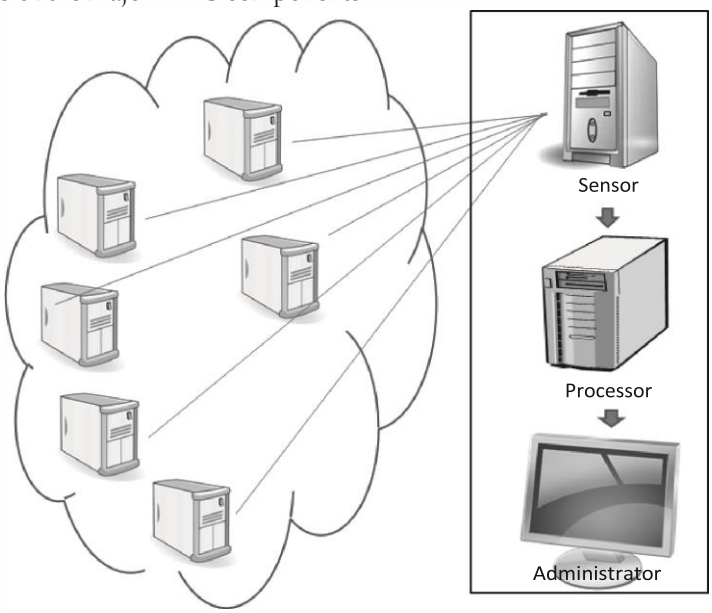


Figure 7.1 Information system monitored by an IDPS.

Table 7.2 Major Components in Intrusion Detection and Prevention Systems

Data Origin	*Data Processing*	*Controls Destination*
Sensors **Agents**	**Management server** **Evaluation algorithms** **Parameter database**	**Admin consoles** **Access authorization**

Sensors

The sensors are essential components in the intrusion detection process, with their function being to recognize the occurrence of potentially harmful events. The location of the sensors within the information system is critical and of paramount importance. Thus, before identifying sensor locations, the information system topology needs to be carefully decided. Such locations are points of entry into system functions or areas. Typical examples are enterprise interfaces to the outside world, such as connections to the Internet, either via LAN or WLAN, as well as remote access via modems. With organizations divided into departments, sensors

may also be placed at interdepartmental points of entry, monitoring access to valuable resources within a department.

Extranet interfaces are also critical. These are entry points where partners will access, and possibly modify if authorized, critical data in corporate databases. There have been cases where an intruder from network A enters corporate network B via the A–B extranet, and while in B, via the B–C extranet, accesses corporate network C, for which the intruder had no authorization. This clearly shows that organization B bears a liability vis-à-vis its extranet partners. Figure 7.2 illustrates this possible intrusion.

The intra-corporate network vulnerabilities should not be underestimated, and sensors must be placed at interdepartmental crossing points. Thus, corporate network to pology and the location of critical resources much be clearly known before sensors are placed. Equally important is for the sensors to be properly programmed as to what they will be "looking" for.

Placed in strategic locations, the sensors monitor traffic in accordance to certain criteria. That is, the sensors are looking for the occurrence of certain events, and they report to the agents. The agents are software that receive the observations of the sensors and pass judgment as to the possible threat posed by the event itself or in combination with other events. Agents have *artificial intelligence*, meaning that they make decisions based on criteria that may change based on varying circumstances. Furthermore, through an inter-agents secure communication, agents collectively monitor the entire enterprise network.

Sensor metrics can be as simple as counting the number of failed user name or password attempts. Based on that number, the agent decides as to the required action. A parameter that can statistically provide a piece of information is the time interval between the submission of the user's name and that of the password. This interval indicates the time it took the user to key in the password.

It is possible for the password webpage to have a short executable code that counts the time intervals between keyed characters. This is applicable to the user name entry or that of the password. The produced *keystroke dynamics* can

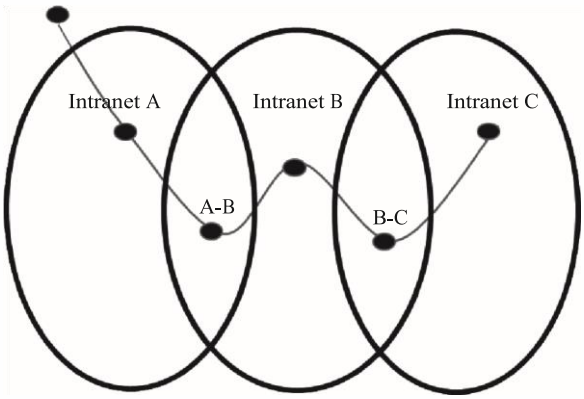


Figure 7.2 Intrusion from network A to network C via network B.

statistically provide a reasonably reliable semibiometric authentication mechanism, serving as a user's digital identification.

Sensors may be placed *in-line* with the flow of data serving as a firewall. Being inline, the sensor can block the suspicious traffic, thus preventing the realization of the attempted attack. Sensors may be on the side, *tapping* the flow of traffic and sending the collected data to the IDPS processor. Being on the side, the sensor passively observes the traffic without affecting the speed of the network. Of course, it may not block any suspicious traffic. Either way, the sensors' findings are forwarded to the IDPS processor, from where a blocking action can result. Figure 7.3 and Figure 7.4 illustrate IDPS topology with in-line and passive sensing examples, respectively.

Processor

The processor collects recorded activities provided by the sensors and agents and correlates them in the search for malware identification or abnormal situations. The performance has to be thoroughly tested—with the IDPS offline and online—with criteria continuously updated to reflect the latest in defense technologies, as well as in the always advancing malware capabilities.

Consoles

The processor delivers all findings to consoles, where administrators oversee the system performance. Sensing and processing parameters may be adjusted by the processor on a real-time basis or by administrator's actions.

IDPS Sensors Firewall

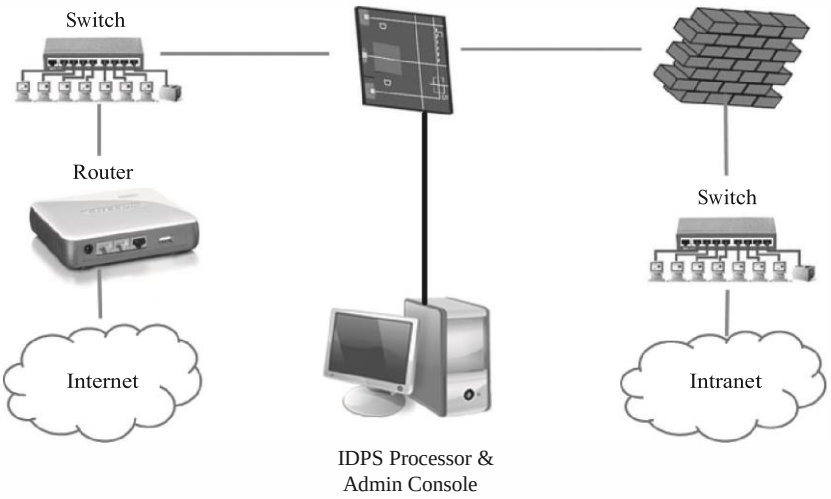


Figure 7.3 IDPS topology with in-line sensing.

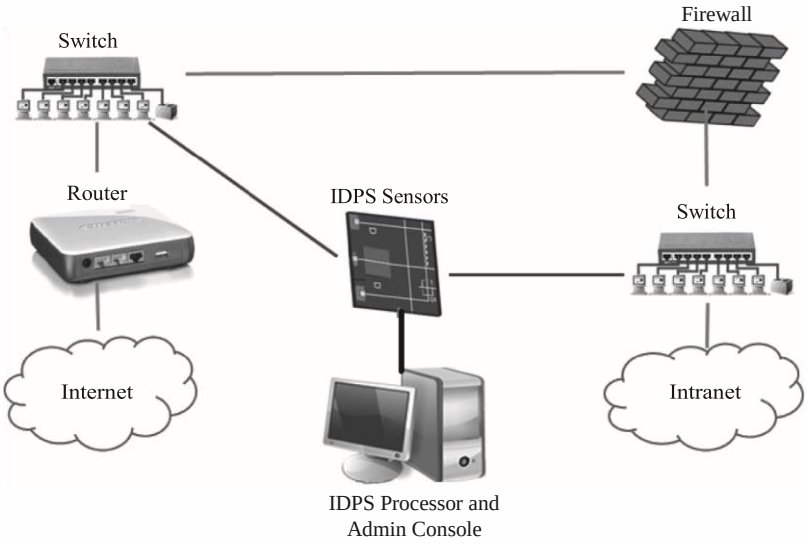


Figure 7.4 IDPS topology with passive sensing.

Network

The IDPS components—sensors, processor, and consoles—communicate with each other using its own network, separate from the production network, which is Web accessible. This way, the IDPS becomes immune to intrusion attacks, because it is physically or logically isolated from the Web.

IDPS Capabilities

The IDPS capabilities vary depending on the sophistication of the system. However, minimally, a Chief Information Officer (CIO) will use the IDPS to independently confirm the firewall's operation, assessing the expected filtering and alerting capability, and also to be notified of non-transactional activities, such as IP or port scanning, which, although not a threat, is the precursor of a possible pending intrusion attack. In the process of overseeing the assigned activity, IDPSs record related information and report to various authorities, as programmed.

Such releases may be *scheduled reports* issued at predetermined points in time, *exception reports* issued automatically because the occurrence of a special event took place, or *on-demand reports* where authorized destinations may receive custom reports. Furthermore, in the event of a recognized intrusion, the IDPS may collect and distribute peripheral information that may later help in the forensics investigation of the intrusion. The basic IDPS capabilities can be classified as

- Information Acquisition
- Information Logging
- Detection Techniques
- Prevention Actions

Information Acquisition

Information acquisition is done by the sensors, which provide the initial processing before forwarding the results to the IDPS processor.

Information Loggings

Events loggings, along with their classification, result in the collection of an extensive amount of data related to detected events. Table 7.3 lists data typically collected by the sensors and sent to the IDPS processor for analysis.

Detection Techniques

The intrusion detection techniques can be classified into three categories, respectively named

- Signature-based detection
- Anomaly-based detection
- Stateful protocol analysis

Table 7.3 Sensor Acquired Data

1. mestamp: Date and time. Often an IDPS may have its own time clocks to best maintain accurate records.

2. ddresses: Source and destination (IP, MAC, IMEI)
3. rt Numbers: Source and destination
4. rt Types: TCP, UDP, or ICMP types and codes
5. ayer Protocol: Network, transport, or application
6. Number: Connection or session
7. ating: Priority or importance for processor to consider
8. iolation: Type of violation or alert
9. ize: Number of bytes transmitted over the connection
10. redentials: User name, password, any special codes
11. load: Application-level data exchanged

In the **signature-based detection**, the IDPS has a database of parameters that indicate a known virus. For example, if a file named love.exe is known to be a virus, its presence will create an alert, and appropriate action will be taken by the IDPS. Also, if a packet's origin or destination has a blacklisted IP, Media Access Control (MAC), or International Mobile Equipment Identity (IMEI) address, again an alert will be created. Possibly, based on the IP address, an entire geographical region can be blacklisted, or a resource can be made unavailable during nonworking hours, for example.

In the case of signature-based detection, blacklists (hot lists) and whitelists are being used. Of course, signature-based detection is not possible on unknown threats. **Blacklists** contain the signatures of *discrete entities* that may be associated with intrusions. Such entities are hosts, port numbers, applications, file names or file extensions, or other quantifiable parameters that can be recognized in network communications. **Whitelists** contain the signatures of *discrete entities* that may raise an intrusion flag, while in reality they are known to be benign.

In the **anomaly-based detection**, the IDPS has a database of profiles that represent the "normal" network behavior. Should something appear to be out of the ordinary, a flag is raised. It is like the passport control at international crossings. If a person is blacklisted, or if something strange is noticed, an alert is raised. These profiles describe the expected behavior of applications, networks, hosts, or even individual users. The parameters of such profiles can be based on statistical information and may dynamically adjust themselves. That is, the use of artificial intelligence may allow these profiles to progressively change without creating an alert. Deviation from these profiles will sound an alarm, and the IDPS will take the

appropriate action. In the case of anomaly-based detection, a significant amount of fine-tuning is required. Tight thresholds will result in false alerts, while loose thresholds may fail to recognize malicious activity.

Denial-of-service (DoS) attacks can be recognized using artificial intelligence that monitors the rate of increase in network traffic. "If artificial intelligence is embedded in the Internet routers, the routers can, collectively, create an Internet SCADA able to detect and prevent potential DoS attacks." However, "anomalybased IDS are more prone to generating false positives due to the ever-changing nature of networks, applications and exploits." "The major benefit of anomalybased detection methods is that they can be very effective at detecting previously unknown threats."

In the **stateful protocol analysis**, models of protocol performance are developed and are used, serving as nominal references. In a way, this technique resembles that of the anomaly-based detection, but instead of statistically building up the models of normal operation, here vendor-provided profiles are being used. "When we perform stateful protocol analysis, we monitor and analyze all of the events within a connection or session" and then map the behavior to the available profiles. Though useful, this detection technique cannot detect attacks unless there is a violation of the expected behavior.

Prevention Actions

IDPSs, as their name implies, are expected, after detection, to actually prevent the attempted intrusion. This can be accomplished in a variety of ways, including

- Blocking the access to all services of the targeted resource (database, server, or application).
- Blocking all communications with users bearing a certain identifier, such as IP address, MAC address, user number, or other unique characteristic of a suspected attacker.
- Blocking further activity of the session of the network connection that created the incident.
- Blocking only the infected part of the transaction. This is applicable to an email attachment or to a toxic file that accompanies an HTML file.
- Blocking an attacker's request by altering the network's firewall criteria.

It is very possible that the IDPS may miss an attack, creating a false negative, or may block a bona fide user, creating a false positive. However, through extensive pre-deployment testing and fine-tuning, the IDPS can asymptotically approach perfection.

IDPS Management

Once an IDPS is acquired, its management is concerned with the implementation, operation, and maintenance of the system. Organizations refrain from in-house IDPS development for two reasons. One is that IDPS, to be powerful, must be very complex. The other is that IDPSs are readily available and are reconfigurable.

Implementation

The implementation of the acquired IDPS product has five steps.

- Step One: Identification of the product's features
- Step Two: Design of the architecture/topology where the product's features are mapped onto the intrusion detection and prevention requirements of the information system that is to be protected
- Step Three: Installation of the IDPS, which may be application-based or appliance-based software
- Step Four: Progressive testing of the IDPS
- Step Five: Activation of the system, with possible return to any of the steps

Step One: Features

There are numerous IDPSs available. Some are in the form of an application. That is, the IDPS is a software of minimal code making extensive use of routines or modules available in the host's operating system and is, of course, operating-system specific. Others are in appliance form. That is, the software is a self-sustained package with own routines, and it is independent of the operating system of the host.

Figure 7.5 shows the control console of an appliance-based IDPS.

Step Two: Architecture

The designed architecture will provide the topology of the applied IDPS, taking into account the monitoring locations and the level of the expected reliability. For increased reliability, sensor redundancy is deployed where multiple sensors monitor the same activity. The IDPS architecture is also concerned with the location of the other IDPS components, like the servers and the administration consoles. The IDPS will interface with the information system it protects in order to collect data and affect necessary actions. Table 7.4 lists the typical IDPS interfaces.

Step Three: Installation

Once the IDPS solution has been identified and the topology has been defined, the installation may proceed. Usually, appliance-based IDPSs are simpler to deploy. However, positioning of the sensors remains the most important parameter. Depending on the particular security application, sensors may be placed in front or behind firewalls, at critical subnets, at Web and email servers, and at critical databases.

Figure 7.5 Administration control console of an appliance-based IDPS. Enterasys Dragon Network IDS Appliance (Fast Ethernet).

Table 7.4 IDPS Interfaces with Information System

Data Collected from Tapped Sources to Be Analyzed	*Data Delivered in Response to Incidents*
• **Event management software**	• **Warnings to admin**
• **Login and email servers**	• **Warnings to emails**
• **Paging systems**	• **Automated emails**
• **Network routers and switches**	• **Incident's profile**
• **Firewalls**	• **Firewall reconfiguration**
Data Received from Network Management Software	*Commands Delivered to Prevent Attempted Compromise Incidents*
• **Patch update**	• **Processes terminations**
• **IDPS configuration update**	• **Attachment removal**
• **Admin console commands**	• **Access blocking**

Step Four: Testing

System testing and operator training should run parallel. Testing is a lengthy process during which detection and prevention criteria are adjusted to minimize false alarms. Operator training will be an ongoing activity, as new threats and software updates are being introduced.

Step Five: Activation

This is the final stage where the system goes into use. Practice has shown that when an IDPS is activated with all sensors active at once, a large number of false alarms overwhelm the operator. It is suggested that the activation of sensors takes place in a progressive manner, so that additional fine-tuning can be implemented. A phased IDPS deployment will best reveal hidden problems and maximize the successful defense of the information system. While in the activation phase, temporary, partial, or total system outages may become necessary for the logical and physical engagement of the IDPS with the production network.

Once in production, a continuous updating of the signatures database will be needed, as well as thresholds adjustments. Considering the importance of IDPS in the secure operation of the information system, it is suggested that administrators' credentials include a two-factor authentication, especially if remote access is used.

Operation

IDPS products are usually operated through a console that employs graphical user interface, with some offering command line interface, as well. Using the console, the administrator can perform a wide range of activities including

- Monitoring and analysis of IDPS data
- Configuration and updating of sensor and management server parameters, including the segmentation of the IDPS mission into sectors, thus facilitating operations and troubleshooting
- Setup of user accounts and of the authorization parameters, including specific privileges and sensors to be monitored
- Design and preparation of scheduled, on-demand, and exception reporting

The screen of a typical intelligent IDS console is illustrated in Figure 7.6. Through this, console operators can define, edit, store, and retrieve queries. Also, user-defined query filters and alert profiles can be created, and custom reports are prepared.

Maintenance

An IDPS needs to be maintained on a continuous basis. The expected maintenance is basically three parts—confirming proper operation, updating of the software, and training of the responsible personnel. Maintenance is an unavoidable task—performed online and offline—that will affect the expected continuity of service.

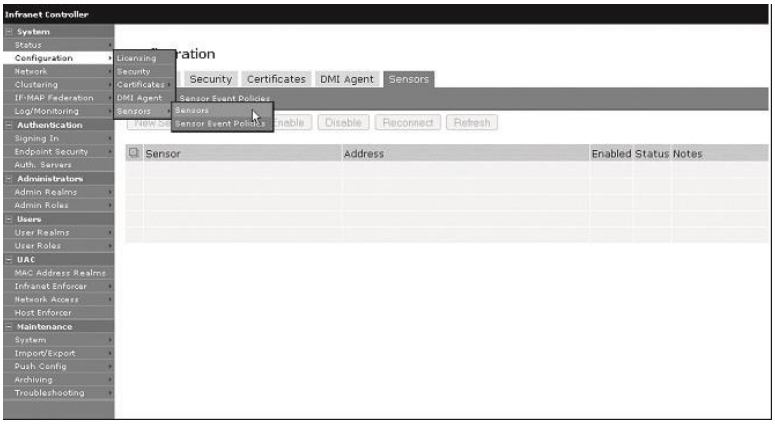


Figure 7.6 Administration console: configuring the connection to the IDPS appliance (partial view).

Confirming proper operation includes monitoring and testing. Testing can be periodic and may take place in an offline testing environment or while the system is in production—in online use.

Updating of the software includes updating of the threat signatures database; adjusting the threat levels; updating the vendor-provided software through the installation of patches; and reconfiguring the system as new requirements, technologies, and threats call for. After each updating a thorough test is needed. It is advisable that, before applying updates, their authenticity be confirmed through the available mechanisms. Typically, the checksums of the updating files computed by the administrator must match the one provided by the vendor. Also, backing up the old configurations is always a good idea.

Training of the responsible personnel on a continuous basis is an absolutely necessary task in order to develop skills for the best defense of the system. Training is typically in-house, after an initial vendor-provided one, to bring everybody up to speed. The product documentation is always an excellent source of information that operators can rely on, not to mention the expected product vendor support live chat availability.

The successful supervision and operation of an IDPS requires IT professionals with skills in information security and network administration, as well as system administration on which to build their ever-increasing *cybersecurity* expertise with the

focus on intrusion, detection, and prevention. Along this objective, joining the *users group* of the particular product is advisable, because this serves as a forum where problems and concerns are brought and, hopefully, solutions are found.

To focus on their core activities, many organizations outsource their information system security to firms dedicated to this field with extensive experience and expertise. Of course, outsourcing has to be evaluated vis-à-vis the organization's mission and constrains.

IDPS Classification

IDPS are classified into the following four general categories.

- *Host-Based,* which analyzes events inside a particular host (a computer) looking for activities that may imply intrusion
- *Network-Based,* which analyzes protocol activity within a particular network (devices or segments) looking for protocol abnormalities
- *Network Behavior,* which analyzes events that may reveal policy violations, presence of malware, or distributed denial of service
- *Wireless-Based,* which examines the wireless network traffic for suspicious activities

Host-Based IDPS

A host-based IDPS is an intrusion detection and prevention system concerned with a single host, that is, with a single computer—workstation or server (web, email, DNS, or other). This IDPS typically monitors the following six areas and activities:

- External wired interface
- Wireless (Wi-Fi and Bluetooth)
- Modem traffic
- File status (access, modification, and creation)
- System configuration (static or dynamic)
- Running processes (system as well as applications)

Observations in the above areas are compared against templates of expected performance and may cause detection alerts and/or prevention actions. Figure 7.7 illustrates a typical configuration of a host-based IDPS.

The host-based IDPS can be software-based, in which case it is installed inside the monitored host itself, or can be appliance-based, in which case it is a separate physical piece of hardware placed in-line between the monitored host and the path to the Internet or intranet.

In the application-based case, there are two approaches: one, where the agent monitors results of activities, and the other, where pieces of code (referred to as *shims*)

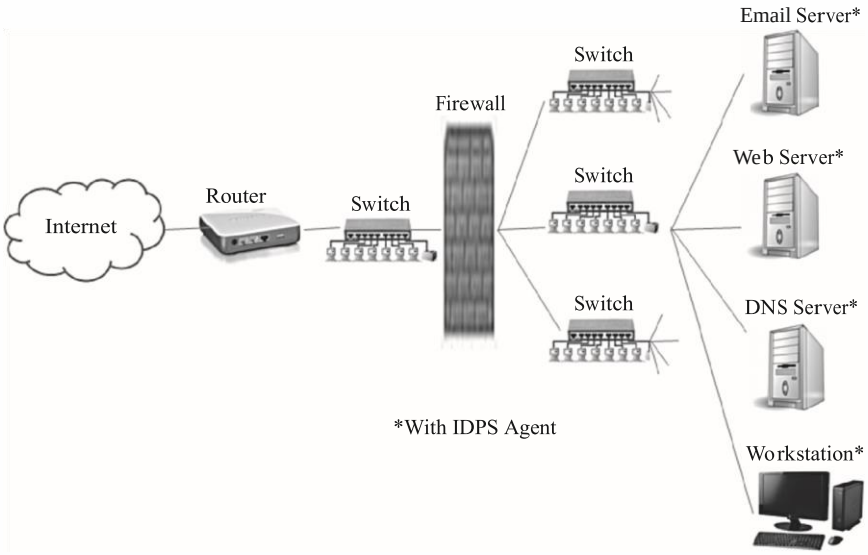


Figure 7.7 Typical configuration of a host-based IDPS. (From http://www. enterasys.com.)

are inserted in selected places, such as the OS, operating system code, application code, or protocols, serving as mini-firewalls able to detect and block undesired activity.

In the appliance-based case, the agent is physically outside of the host and does not have the possible microcontrol provided by the *shims*, but it is independent of the OS used. Recorded parameters of detected events include

- Type of event and its level of priority.
- The timestamp, based on assigned source. Most IDPS generate their own timestamp rather than copying one from an external source.
- Associated port and IP (Internet and intranet) addresses.
- File names and their paths (directories, subdirectories, etc.).
- Authorization/authentication credentials (user names).

The host-based IDPS examines codes for malware by executing them in a *sandbox* environment, that is, in an environment where the execution cannot harm other programs, nor can it use forbidden resources. In this supervised execution, the IDPS agent is on the lookout for

- Violations, such as venturing into unauthorized space
- Privilege escalation
- Buffer overflow, stack or heap
- Unauthorized library calls
- Sequences of instructions that may be either copying keystrokes or attempting to install rootkits

The host-based IDPS also checks for the integrity, properties, and access of files. Integrity is checked through checksum testing; if incorrect it indicates that the file content has been altered. Checksum is a residual, a leftover, a binary sequence produced after the passing of a file's content through a predetermined algorithm.

File properties are very important for the security and integrity of the file content. Properties include access privileges—read/write, file authorship, timestamps of access and modification, digital signature, and possibly other parameters depending on the type of file. File access control is the most critical security feature. The placement of a *shim* may detect policy violations and even implement security policies by blocking access.

A host-based IDPS, similarly to other systems, requires *tuning*. This has to take place at the initial activation as well as after the installation or replacement of selected protected files. Also, the whitelists and the blacklists need to be current to prevent false detections. Before deployment, any conflict with other protection systems must be resolved to avoid malfunctioning in both systems.

Because of their continuous vigilance, host-based IDPSs pose a load on the protected host, requiring significant processor time and space in memory and disc. Furthermore, between installation and deployment, extensive testing is required to ensure correct integration of the IDPS into the host. Such testing will have to take place offline, causing the host to be out of service during that period.

Network-Based IDPS

In network-based IDPS sensors can be either application-based or appliance-based and may monitor more than one device or segment in the network. For prevention measures to be applied, sensors must be installed *in-line*. *In-line* sensors must be of very high speed so that they do not create traffic congestion. Should handling of the traffic reach a near-saturation point, traffic has to let pass through unchecked, or low-priority traffic be dropped to reduce the load. When installed as *passive,* observations are only reported, without any ability to block detected events. *Passive* sensors forward the collected data to a *management server*, where they are analyzed and where prevention action may be initiated. Figure 7.3 and Figure 7.4 illustrate network-based IDPS. Network-based IDPSs with *in-line* sensors may intervene and prevent the attempted execution of an event, while network-based IDPSs with *passive* sensors serve as mere observers and reporters of events.

Network-based IDPSs analyze activities in the network, transport, and application layers, and the majority use all three detection techniques discussed earlier in this chapter, namely, s*ignature-based detection*, *anomaly-based detection,* and *stateful protocol analysis*.

The detection processes can be distributed to several sensors handled by an IDPS load-balancer. A network-based IDPS is basically an observer looking at the network traffic *passing by*. In that process, the IDPS is on the lookout for violations, as per prescribed criteria. The IDPS reports such violations to the respective IDPS management server, which may apply prevention measures.

The types of collected data include IP and MAC addresses of the communicating hosts, as well as their operating system type and version. Determination of the version leads to information about the existence of possible vulnerabilities that need to be protected. Other collected parameters are numbers of the used ports, applications and their versions, number of hops in the travel between two hosts, and other data that are normally included in communications protocols.

Network Behavior Analysis System

The Network Behavior Analysis (NBA) System, as its name implies, examines the behavior of a finite network, and it is usually appliance-based. The NBA passively observes numerous points and protocol activities in the network and creates a benchmark, which continuously updates itself and constitutes the "normal traffic behavior." NBA uses that model as a benchmark to detect deviations, as well as to recognize trends in the use of the various resources.

NBA is ideal in detecting DoS attacks or persistent attempts to break authorization codes. An NBA sensor can be deployed in either mode, *in-line* or *passive*.

In the *in-line* mode, NBA serves as a mini-firewall, blocking requests from suspicious hosts. In the *passive* mode, NBA collects data out of the tapped traffic flow—such as IP addresses of communicating hosts, protocols use, and active applications—and intervenes if necessary, terminating connections that support activities that cannot be trusted. Figure 7.8 illustrates the topology of an NBA intrusion detection system.

Wireless IDPS

The wireless IDPS monitors the performance of the wireless local area networks (WLANs). The de facto WLAN technology is the Wi-Fi, officially known as IEEE 802.11. This technology operates in spectra that are subdivided into channels, where communications continuously change channels. Therefore, a wireless IDPS

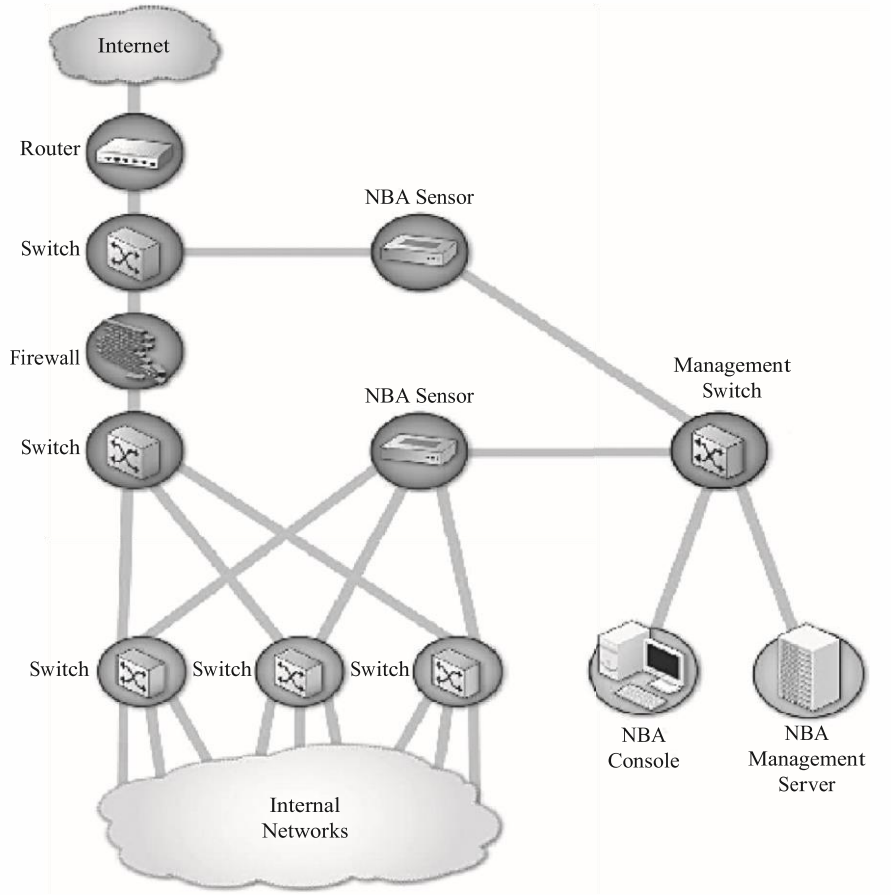


Figure 7.8 Topology of an NBA intrusion detection system. (From http://www.juniper.com.)

should have one sensor per channel to maximize its performance. If there is only one sensor, that sensor will need to hop from channel to channel, naturally missing traffic activity. Figure 7.9 illustrates the configuration of a WLAN IDPS.

Wireless IDPSs can be stand-alone or embedded in the wireless access point (AP), from where they monitor the network's activities. Although the Wi-Fi technology provides for data security via its Wired Equivalent Privacy (WEP), its encryption strength is considered weak and breakable, and additional measures are needed. Even if an organization has no wireless network in operation, a wireless IDPS could be deployed to explore the airwaves and make certain that no unauthorized AP is connected to the organization's network. As a minimum, a Wi-Fi finder should be used to confirm that no unauthorized AP is connected in the organization's LAN. Figure 7.10 displays a typical Wi-Fi finder.

If an organization indeed has operational WLANs, "Solutions are currently available where positioning of RF sensors, can geometrically determine if a client is within the authorized physical area. Such technologies, which need onsite terrain training and fine tuning, have offered 100% security in testing."

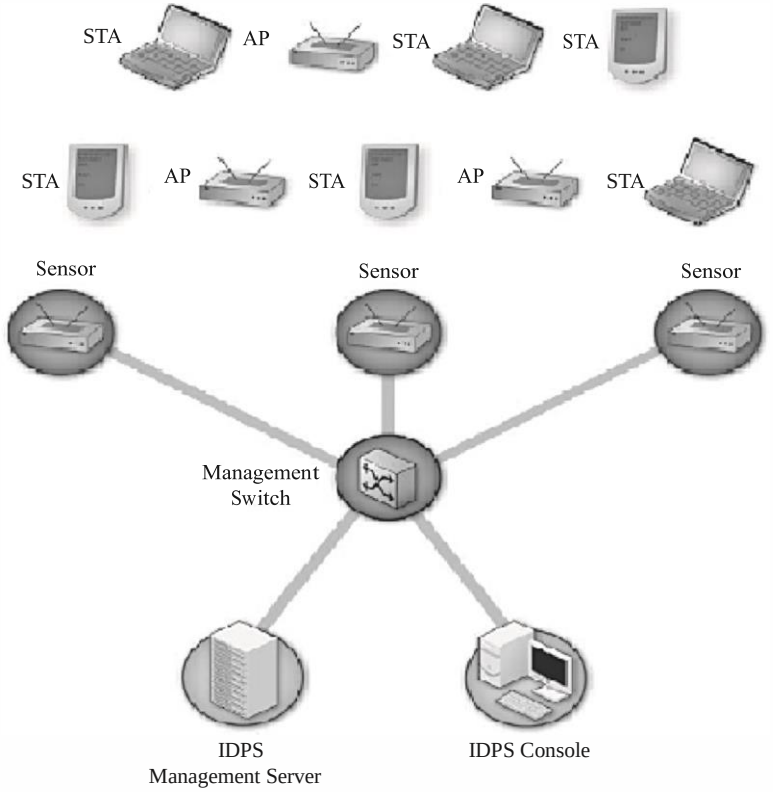


Figure 7.9 Typical configuration of a WLAN IDPS.

Figure 7.10 Typical Wi-Fi finder.

The deployment of the sensors needs to take into account various factors, including the following:

- Range of the sensors and the building floor plan
- Topology of the organization's wireless APs
- Topology of the organization's wired network
- Cost of the IDPS versus the worth of the protected data
- The physical security of the devices
- The IDPS technologies to be used

The detected events are assessed relative to criteria similar to those of the other three IDPS types described above. The expected capabilities of the wireless IDPS include the following:

- Recognition of the presence of all wireless device—APs or stations.
- Determination of the physical location of any wireless device—APs or stations. Finding the physical location is through triangulation, which will require that several sensors be deployed.
- Recognition of policy violations.
- Ability to execute prevention action while still in detection mode. This is accomplished using two independent RF modules, one listening all the time, while the other transmits information on events.
- Detection of the presence of
  - Man-in-the-middle attacks
  - DoS attacks
- Wireless network scanners used by wardrivers (Wardrivers are persons who drive around streets to locate a wireless network to use or to attack.) Recorded parameters of detected events include the following:

- Identification of the MAC or IMEI number of the wireless unit suspected in the event.
- Number of channel over which event took place.
- Intranet address assigned to wireless unit by the AP. This address typically is 192.168.1.xx, where xx is the number assigned to the unit.
- Timestamp, based on assigned source. Most IDPSs generate their own timestamp rather than copying one from an external source.
- Type of event and level of priority, as classified by the IDPS.
- Sensor number, should a multisensor IDPS be used.
- Type of applied countermeasure. Typically, termination of connection and prevention of new connection to the suspected unit.

Pre-deployment of a wireless IDPS requires initialization, where the parameters of legitimate units are entered and fine-tuning is performed to make certain that the protected terrain is properly covered.

IDPS Comparison

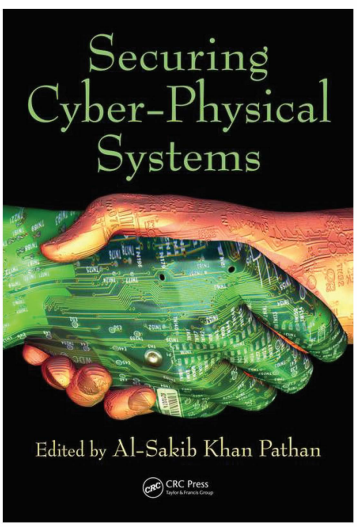
Each of the previous IDPS solutions has a unique purpose and, to a certain extent, a unique design. Table 7.5 summarizes their main characteristics.

Table 7.5 Major Types of IDPS—A Comparison

Type	*Protected Domain*	*Examined Activities*	*Focus*
Host-Based	**A single host workstation or server**	**Operating system Applications Network traffic**	**Examines all activities including traffic flow and files properties.**
Network-Based	**Subnets and networked hosts**	**Layers: network, transport, and application**	**Focuses on whitelist/blacklist detections. Analyzes protocols.**
Network Behavior Analysis (NBA)	**Subnets and networked hosts**	**Layers: network, transport, and application**	**Focuses on anomalous behavior recognition. Recognizes DoS attacks.**
Wireless	**Wireless networks and hosts**	**Protocol activities and access authorization**	**Focuses on hosts security and on traffic authorization.**

CHAPTER 4

Securing Power Systems



Learn More:

Chapter 1

Securing Power Systems

Martin Saint and Timothy X. Brown
University of Colorado and Carnegie Mellon University

Juan Hoyos
University of Colorado and Empresas Públicas de Medellín

Contents

1.1 Power System Overview 2
1.1.1 The Power System as Critical Infrastructure 3
1.1.2 Generation 4
1.1.3 Transmission 4
1.1.4 Distribution 5
1.1.5 Load 6
1.2 New Capabilities and Challenges for Modern Control Systems 6
1.2.1 Objectives 7
1.2.2 Performance 8
1.2.3 Culture 8
1.2.4 Cyber-Physical Coupling 8
1.2.5 Distributed Systems 8
1.2.6 Design Lifetime 8
1.2.7 Regulation and Standards 9
1.2.8 Risk Management 9
1.3 IEC 61850 Standard 9
1.3.1 Background 9
1.3.2 Overview of the Standard 11
1.3.3 Example IEC 61850 Functionality 12
1.3.4 Challenges and Vulnerabilities 13
1.3.4.1 Complexity 14
1.3.4.2 Cyber-Physical Security for IEC 61850 14
1.3.4.3 The Problem of Encryption and Message Authentication versus Latency 15
1.3.4.4 Other Issues 16

1.4 IEC 61850 Attack Vectors, Consequences, and Mitigation 17
1.4.1 Attack Vectors and Techniques 17
1.4.2 Attack Consequences 17
1.4.3 Mitigating Attacks 18
1.5 Exploiting IEC 61850 via GOOSE 18
1.5.1 Normal GOOSE Function 19
1.5.2 Building a Practical Cyberattack 20
1.5.2.1 Technical Details 20
1.5.2.2 Building the Script 21
1.5.2.3 The Results of the Attack 21
1.6 Conclusion 23
Acknowledgment 23
Author Biographies 23
References 24

Abstract: Security issues for the power industry have become increasingly relevant as it relies more than ever on networking and automation protocols. The next generation of electrical grid incorporates significant advances in communications and control that closely couple cyber and physical systems. This enables new capabilities, but also exposes new vulnerabilities. While modern control networks share many elements in common with traditional information technology networks, they must be designed, managed, and secured with different goals in mind. The IEC 61850 standard for power automation has been widely adopted, and the design concepts are being incorporated throughout the generation, transmission, and distribution areas of the power industry. The success of IEC 61850 for substation automation has led to adaptations developed for other applications such as hydroelectric plants, wind turbines, distribution feeders, and high-voltage switch gear. This chapter describes the IEC 61850 architecture and potential threats, existing security protections, and some remaining vulnerabilities. Challenges to implementing security for IEC 61850 are described. An example IEC 61850 exploit is implemented on real equipment to demonstrate what might be necessary for a successful attack capable of creating a widespread interruption in power generation and distribution. Mitigations for some current vulnerabilities are offered, and areas which require further solutions are highlighted.

Keywords: Cyber-physical security; GOOSE message; IEC 61850; Substation security; Critical infrastructure.

1.1 Power System Overview

Electricity is a key energy sector in modern society. Electricity is provided through a power system consisting of interconnected generation, transmission, distribution, and end-user load components. The electrical grid has been called the most important engineering achievement of the twentieth century, and the transmission and distribution system is the largest machine ever made. However, it still uses technologies that have changed little in the last hundred years and are poised for a revolution in their physical, organizational, and conceptual structure. What began as a physical system governed by electromechanical controls is rapidly evolving to become a complex cyber-physical system that relies on the integration of sophisticated control and communication networks. At the same time, there is a new focus on the critical nature of key infrastructure that affects the function of society and the need to identify

vulnerabilities and improve critical infrastructure security. The increasingly interdependent nature of infrastructure is also being recognized; for instance, telecommunications depend on electric power, and control of the electric grid depends increasingly upon telecommunications, creating the possibility for a negative feedback loop following a disturbance in either.

Electricity is a major industry in which service providers retail power that is provided by operator companies at prices that are set by a combination of markets and regulatory oversight. The electric power industry is a $385 billion (2013) industry in the United States and tops $1882 billion (2012) worldwide. Failures such as outages and voltage fluctuations lead to significant economic losses and impact societal health and safety. Reports written for the U.S. Department of Energy (DoE) by LaCommare and Eto in 2004 and 2006 place the cost of power outages at approximately $80 billion annually in the United States. They note, however, that there are significant gaps in the amount and quality of outage information gathered. They performed sensitivity analysis, which indicated costs could range from less than $30 billion to over $130 billion annually. Other work by Clemmensen et al. in 1999 estimates losses of $26 billion per year, Swaminathan and Sen in 1999 estimate $150 billion per year, and the Electric Power Research Institute in 2001 reports an estimate of $119 billion per year. Even these comprehensive studies have their limits: LaCommare and Eto state that an extended power outage may have social impacts such as emergency response or public health costs, or the costs of inconvenience and anxiety, none of which are accounted for. Studies often do not take into account the effects of power quality disturbances, only outages.

1.1.1 The Power System as Critical Infrastructure

Critical infrastructure protection is becoming an increasingly important topic internationally, and particularly after the events of September 11, 2001 in the United States. Federal laws mandate that any virtual or physical assets whose incapacity or destruction would have a debilitating impact on security, national economics, or national public health or safety must be considered critical infrastructure [9]. The Department of Homeland Security defines a total of 18 sectors* for the United States, and each sector is assigned to a specific government agency, which is responsible for identifying risks and promoting rules or standards to protect its assigned critical infrastructure.

For energy-related critical infrastructure, the U.S. DoE has been assigned to identify and promote best practices and methodologies for protection and continuity of energy services. The DoE has designated the North American Electric Reliability Corporation (NERC) as the organization responsible for assuring security of the power grid and elevating awareness and understanding of threats and vulnerabilities to utility assets, systems, and networks. In May 2006, NERC released a set of Critical Infrastructure Protection (CIP) Cyber Security Standards, CIP-002 through CIP009, applicable to users, owners, and operators of the power grid. The CIP standards are designed to minimize the risk of possible cyberattacks using the communications

infrastructure, as well as potential physical attacks, either of which could compromise the integrity of the grid.

There are other organizations, such as the British Standards Institute (BSI), the U.S. National Institute of Standards and Technology (NIST), and the International Society of Automation

* The full list includes agriculture and food, banking and finance, chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, government facilities, healthcare and public health, information technology, national monuments and icons, nuclear reactors and materials and waste, postal and shipping, transportation systems, and water.

(ISA), that are working on internationally applicable standards for cybersecurity for automation processes.

The rest of this section describes the key generation, transmission, distribution, and load components of the electrical grid system. A basic overview of the system is helpful for understanding how it is evolving, why there is a need for sophisticated communications and control, and where specific vulnerabilities exist.

1.1.2 Generation

Common generators are driven by hydro, wind, oil, or nuclear power and work on the principle of electromagnetic induction. When a conductor moves in relation to a magnetic field, voltage is induced in the conductor. Power plant generators are three phase, or constructed with three terminals, each producing power that is 120° out of phase with the others. This permits constant instantaneous power from the generator and reduces the overall size of conductors required for transmission. In North America, alternating current (AC) generators operate at 60 Hz, and in much of the rest of the world at 50 Hz. It is important that all generators connected to a common system be able to coordinate their output so that the sine waveforms produced are as nearly synchronous as possible.

Classic generators convert mechanical energy to electrical energy. The rotating shaft of the generator is driven by a prime mover, such as a steam turbine, or directly through hydropower. Most generation is thermally driven, which means that a fuel such as coal or natural gas is burned to produce steam, which drives a turbine. In the case of nuclear plants, it is the heat from the fission reaction that is used to create the steam for the turbine.

As it is impractical to store large quantities of electricity, at any instant the quantity of electricity generated must match the quantity demanded by the load. This leads to three types of generating plants: baseload, load-following, and peaking. Baseload generation, such as is provided by coal-fired and nuclear plants, is economical to operate but cannot be quickly modulated. It is used to meet the level of relatively constant loads that are determined to historically exist on a power system. Load-following units, such as combined-cycle gas turbine-driven generation, have the ability

to run for long periods of time, but may be turned off and can vary their output more readily than baseload units. Peaking plants, such as gas turbine, may be started, stopped, and regulated quickly. They are normally only used when electricity demand is near its peak. The electricity generated from these plants is relatively expensive, as they may use more expensive fuels, and building the plants involves high fixed costs, even though they may be idle most of the time.

Environmental concerns, difficulty obtaining permits and approvals, and high cost all serve as impediments to constructing new traditional generation facilities. At the same time, increasing demand and aging infrastructure pose a threat to reliability and adequate capacity in the electric sector. Advances in sensing, communications, and control hold the promise of reducing and shifting demand, improving efficiency, enabling the incorporation of alternative generation, and providing for better monitoring and maintenance.

1.1.3 Transmission

Unlike the first generating stations, as power plants grew they began to be located outside of the population centers they served, necessitating the long-distance transmission of power to the local distribution networks. The transmission system is composed of transmission substations and transformers to boost the voltage from the level at which it can be safely generated to levels high enough to be efficient for long-distance transmission. It is also composed of high-voltage transmission lines, commonly between 138 and 765 kV, and shares distribution substations containing transformers that reduce the transmission voltages back down to distribution levels. Substations also contain related equipment, such as switchgear or circuit breakers, which are used to protect the system and disconnect parts of the network for maintenance. Measurement, metering, control, and communications equipment are also housed in substations and at points along the transmission network, allowing parameters such as voltage, current, and power quality to be remotely monitored and some equipment to be remotely controlled.

The amount of power that can be transmitted over a given conductor is limited by a number of factors, including the conductor's material, size, length, and distance from other conductors and potential ground elements. Transmission loads are also governed by *thermal limits*, *stability limits*, and *voltage limits*. *Thermal limits* are primarily a function of heating of the conductors due to resistance in the conductor material, leading to excessive power loss and sag in the line. While not the primary constraint, transmission thermal limits are affected by ambient temperature, and are part of the concept of *dynamic rating*, which permits the maximum carrying capacity of the line to be adjusted for factors such as ambient temperature and the amount of time the line has been heavily loaded. The *stability limit* refers to the difficulty of keeping remote generators in synchronism with each other, particularly as feedback is required due to ever-varying loads on each generator. *Voltage limits* affect power transmission because impedance in the transmission line causes a drop in voltage over its length, and for practical reasons, electrical systems generally do not permit a drop to less than 95% of the design voltage.

Shorter transmission lines are usually constrained by the thermal limit and longer lines by the stability limit. Voltage limits may also constrain longer lines, although it is possible to install equipment that helps to boost or regulate voltage.

Transmission networks are typically connected in a grid or mesh topology, rather than point-to-point or hub-and-spoke. This creates redundancy and allows electricity to take multiple routes, bypassing generation and transmission resources which may be accidentally or intentionally taken off-line. As electricity follows the path of least resistance, affected by phase, amplitude, and impedance, it is difficult to predict the exact circuit it will follow between varying generation and loads when there is more than one possible route. Small changes in voltage and impedance may be made to influence the power path and hence the load on individual lines, but a great deal of state information and computation is required to monitor and control the system to prevent transmission line overloads. Increasingly, the U.S. electrical grid faces the issue of *congestion*, whereby loads cannot be matched to the most economical remote generation due to the lack of capacity and potential for overloads in the transmission system. Congestion, lack of incentive, and the difficulty of obtaining rights-of-way and permits to build new transmission lines present a significant threat to critical energy infrastructure.

Developments of new conductor materials that support high temperatures and have low sag are coming in the next decade to boost the capacity of existing transmission corridors, avoiding the environmental issues related to the construction of new lines. Until new conductors are viable in the market, utilities have taken the path of optimizing their existing infrastructure using existing technology. Current technologies include flexible AC transmission systems (FACTS), synchrophasors, Volt/VAR regulation/optimization, grid-scale energy storage, and installing utility-scale smart solar inverters. All of these techniques require high interdependence between telecommunication, control, and power system operation.

1.1.4 Distribution

Distribution networks begin at the distribution substation, which typically steps power down from transmission voltages to the 4–35 kV range. The substation may contain equipment similar to that found in transmission substations, although currently they are often less automated, providing an opportunity for improvement. Like transmission lines, distribution is three phase, although the conductors may be split near the load to serve individual neighborhoods. Residential and small commercial loads in the United States are typically served at 120 and 240 V, requiring another small transformer near the point of consumption. Distribution networks are often arranged in a radial topology, although ring and mesh are not uncommon. Even with ring and mesh configurations, a disconnect is usually left open so that the networks are operated as point-to-point connections with the ability to close the disconnect and failover to another route if necessary. While power flows have historically been from substation to load, this is changing with the introduction of distributed generation and microgrids, which will require more sophisticated monitoring and control.

.

1.1.5 Load

While it is an important element of the electric system, beyond the meter the grid becomes the domain of the consumer more than the regulator or the utilities. While this domain is generally not considered part of regulated critical infrastructure, if the goal is to deliver end-to-end reliable electricity, this link in the chain cannot be ignored. As "smart" buildings, homes, and systems become interconnected with the electrical grid, the potential for disruption of the grid increases, even if consumer systems are not directly interconnected with utility control and communications architecture.

Electrical loads are the reason the electrical grid exists, and they have important engineering implications for the way the grid functions. A charging plug-in electric vehicle (PEV) may draw as much power as an entire house, so the appearance of several within a neighborhood may easily exceed the original design for the neighborhood's distribution system unless they can be monitored and controlled. It is also important to monitor the load on the total system, both to plan for peak demand and to meet instantaneous requirements.

The type of load also has important implications for the way the grid functions, based upon its so-called impedance. In an AC system, voltage and current are sinusoidal, and both reverse their polarity at the same time if the load is strictly resistive, resulting in the transfer of only *real power* If the load has capacitance and inductance elements, then voltage and current are out of phase and some current flows back to the source during each cycle. This *reactive power* does no useful work, but conductors, transformers, and generators must be sized to carry the total current and dissipate the heat generated.

Baseboard heaters and incandescent light bulbs are examples of purely resistive loads, which only consume real power. Many loads, such as motors, are a combination of resistive and inductive impedance, which effectively draws reactive power. The number of motors connected to the grid means that it is heavily skewed toward needing generators to supply both real and reactive power. It is possible to connect capacitor banks, which produce reactive power, to cancel inductive loads and reduce the demands on generation and transport, but this introduces the need for monitoring and control of power quality in the system.

1.2 New Capabilities and Challenges for Modern Control Systems

The requirements of the future smart grid communications infrastructure will create significant new challenges for control system cyber-physical security. High-speed, two-way communication will create more attack possibilities. The expansion of the network and more monitoring and control points will also increase the attack surface, as will the addition of customer interfaces. The interconnection of networks will present a greater number of vulnerabilities, particularly if communications use public data

networks. The use of wireless devices and protocols will open new avenues for access, presenting challenges because the wireless spectrum cannot be physically secured. The control system trend is toward open software and protocols, but this also makes the source code and necessary knowledge to exploit these systems readily available. In addition to the increase in vulnerability, expanding the scope of systems and interconnection also increases the potential scale of any damage should a system be compromised.

As electric grid industrial control systems (ICSs) evolve, they are taking on many of the characteristics of enterprise information technology (IT) systems, such as running common enterprise operating systems like Microsoft Windows and Linux on personal computer-like architecture and the use of protocols such as the transmission control protocol and the Internet protocol (TCP/IP) using physical infrastructure such as Ethernet or public communication networks. While IT systems pose their own ever-evolving security challenges, the environment and methods by which these challenges are addressed is more mature than for modern ICSs, and there is a need to develop a different approach to ICS security.

Although ICSs are starting to share some similar components and architectures, such as hardware, operating systems, and protocols, they are fundamentally different from enterprise IT systems. Some of the reasons for this are considered next, and additional differences are detailed in several documents from the National Institute of Standards and Technology.

1.2.1 Objectives

Information systems, including control systems, have three broad security goals:

Confidentiality. "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information".

A loss of confidentiality is the unauthorized disclosure of information.

Integrity. "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity".

A loss of integrity is the unauthorized modification or destruction of information.

Availability. "Ensuring timely and reliable access to and use of information".

A loss of availability is the disruption of access to or use of information or an information system.

ICSs manage processes that are integral to the functioning of critical national infrastructure, life safety, and the orderly functions of society. In ICSs, availability is the most critical metric, while IT systems prioritize confidentiality and integrity. As

.

ICSs monitor continuous processes, they are not tolerant of interruptions, and any upgrades or maintenance must be tested and planned in advance to insure availability and continued reliability.

1.2.2 Performance

Peterson and Davie state that the two principal metrics of networking are throughput and delay. ICSs are real time and may be sensitive to delay and jitter or require deterministic protocols. Though many applications do not require high sustained throughput, data burst rates can be very high in order to reduce packet latency in support of real-time control.

1.2.3 Culture

ICSs are often managed by control engineers, not IT specialists, and while control engineers may not have the same level of familiarity with modern IT infrastructure, they are more aware of the impact of communications and control on overall power system performance. A commitment to system reliability and availability may necessitate a compromise in other common IT objectives; for instance, rapid access to the control system by different operators in the event of an emergency may be more critical than strict access control or conformance to the principle of least privilege.

1.2.4 Cyber-Physical Coupling

ICSs typically control physical processes, and cyber-physical systems highlight the intersection of physical processes, computation, and communications. Unlike, for instance, embedded systems, where the focus is primarily on computation, cyber-physical systems recognize the important role of interaction with the physical world.

Security issues also have cyber-physical coupling. We focus here on cyberoriginated attacks that have physical consequences, so-called cyber-physical (CP) threats, rather than cyber-cyber (CC), physical-cyber (PC), or physical-physical (PP) threats. CC threats include attacks on power system information management systems via network and other cyberavenues. CC attacks are addressed through traditional cybersecurity measures. PC threats include physical destruction of cyberassets or their supporting cabling and power supplies. These threats require proper physical security around cyberequipment. Further, we are more interested in attacks that impact the physical power grid. PP threats include causing physical faults in one part of the network, such as overloads, demand spikes, or loss of synchronization, that propagate to other parts of the power grid. These threats tend to lie within traditional grid stability and control systems. Here, we focus on CP attacks that cross the cyber to physical domain.

1.2.5 Distributed Systems

ICSs are often widely distributed, although they have centralized servers similar to IT systems. Unlike IT systems, which may only include a few types of distributed clients,

.

ICSs often have a much greater variety of complex devices and systems at the edge of the network. It may also be difficult to physically access these systems for maintenance or troubleshooting, whereas IT systems tend to be more centralized and accessible.

1.2.6 Design Lifetime

Components in IT systems are often replaced on 3–5-year life cycles. ICSs may be expected to have a service life of 10–15 years. This impacts everything from multivendor support to available computational resources and capabilities. It is also often necessary to couple modern ICSs with legacy devices and protocols, which may have few security features or options.

1.2.7 Regulation and Standards

The electrical system is in many respects a natural monopoly in each local area. Due to economies of scope and scale, it is more efficient to build a single large power generation plant than two side-by-side competitors. Historically, with large coal, hydro, or nuclear generation plants, it made more sense to build a single transmission and distribution network than to provide multiple sets of wires between the producers and consumers of power. Because of their monopoly position and critical infrastructure status, these entities must be, and are, regulated. Most utilities are covered by a variety of regulations, which range from federal to local and govern all areas of the utility, from rates to reliability. Organizations such as the Institute of Electrical and Electronics Engineers (IEEE), NIST, and the International Society of Automation (ISA) all publish recommendations and standards that relate to the electric grid. Standards cover equipment specifications, safety, communications protocols, cybersecurity, and other topics that vary widely in their scope and focus. While standards are not in themselves regulations, they may be incorporated "by reference" such that compliance with the standard becomes a required part of the regulation.

1.2.8 Risk Management

Risk mitigation includes four categories of alternatives:

Retain. Accepting the chance of loss from a risk.
Avoid. Eliminating the vulnerability or consequence.
Reduce. Taking steps to reduce the impact of a threat acting on a vulnerability.
Transfer. Sharing some or all of the exposure or consequence.

Maintenance activities such as patch management are common in IT systems and may even be automated. Since it is not possible to patch or reboot a control element without advance testing and planning, the process is much more expensive and involved for ICSs. Security managers may need to retain risk for a period of time and

.

balance the cost of avoidance or reduction against the potential impact of compromise or failure.

1.3 IEC 61850 Standard

1.3.1 Background

The International Electrotechnical Commission (IEC) standard 61850 was originally conceived for substation automation. It has been adopted by the industry, and its success in substation automation has led to adaptations developed for other applications such as hydroelectric plants, wind turbines, distribution feeders, and high-voltage switchgear. Table 1.1 lists some of these adaptations and shows both the depth of industry interest in this protocol and the need to understand the security implications of the IEC 61850 methodology. The operational benefits for utilities that have moved to IEC 61850 for substation automation are providing a visible incentive to innovate and create solutions outside of substation boundaries. The new target of utilities is to use modern

Table 1.1 Extensions to the IEC 61850 Protocol to Domains beyond Isolated Substation Automation

IEC 61850-7-410	**Hydroelectric power plants—communication for monitoring and control**
IEC 61850-7-420	**Communications systems for Distributed Energy Resources (DER)— logical nodes**
IEC 61850-90-1	**Use of IEC 61850 for the communication between substations**
IEC 61850-90-2	**Use of IEC 61850 for the communication between control centres and substations**
IEC 61850-90-3	**Using IEC 61850 for condition monitoring**
IEC 61850-90-4	**IEC 61850—network engineering guidelines**
IEC 61850-90-5	**Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118**
IEC 61850-90-6	**Use of IEC 61850 for distribution feeder automation system**
IEC 61850-90-7	**Object models for photovoltaic, storage and other DER inverters**
IEC 61850-90-8	**Object models for electrical transportation (E-Mobility)**
IEC 61850-90-9	**Object models for batteries**
IEC 61850-90-10	**Object models for scheduling**
IEC 61400-25	**Application of the IEC 61850 methodology for wind turbines**
IEC 62271-3	**Communications for monitoring and control of high-voltage switchgear**

telecommunications technologies such as long-term evolution (LTE), Worldwide Interoperability for Microwave Access (WiMAX), and spread spectrum in conjunction with IEC 61850 to create applications with benefits similar to those seen in substations. Applications such as distribution automation, microgrids, distributed generation, smart metering, wide area protections schemes, and synchrophasors are all possibilities.

The IEC 61850 design concepts are being incorporated throughout the generation, transmission, and distribution areas of the power industry and may even see adoption in the consumer/ load component, as there is a proposal for hybrid PEV charging based on the standard. While not necessarily well known outside of the electric industry, the impact in this sector is similar to the introduction of the local area network (LAN) for corporate networks in the 1980s. Similar benefits and challenges may be ascribed to other automation networks in a variety of critical infrastructure and industrial automation applications. For the remainder of the chapter, IEC 61850 is

discussed in the context of the original substation automation application, but it is applicable to any of its derivatives.

For more than 20 years, almost all communication between devices inside and outside of power substations has been implemented using copper wires and legacy communication protocols such as MODBUS, DNP 3.0, and IEC 60870-5-101/104. There were many disadvantages to this approach, including long implementation schedules, the high cost of copper wiring, relatively few parameters available for monitoring, proprietary implementations, lack of interoperability, and the need for substantial ongoing maintenance. Ethernet (IEEE 802.3)-based systems have overcome some of these problems by applying the same LAN solutions that have worked for more than 25 years in the IT industry, but a solution that addressed more than networking alone was needed. In response to these trends, disparate legacy protocols are being replaced by the more structured suite of protocols defined by the IEC 61850 standard.

Electric substations perform a number of different functions, including transforming voltage up or down, and in some cases monitoring voltage, via *transformers*. The substation can also switch electricity to different distribution circuits via *switches* or *disconnects* and provide overload or overcurrent protection via *circuit breakers*. In modern substations, this equipment is connected to microprocessor-based controllers called intelligent electronic devices (IEDs), which receive data from the power equipment and other sensors. They are also capable of issuing control commands, such as opening a circuit breaker. These devices are networked to perform protection, monitoring, automation, metering, and control of the substation.

1.3.2 Overview of the Standard

The first version of IEC 61850 was released in 2005 with several broad goals. These included the desire to design a single complete standard for configuring, monitoring, reporting, storing, and communicating the equipment and related data in a substation. The standard also aimed to permit interoperability of equipment from different manufacturers. Data for configuration of all of the equipment in the substation can be stored in the substation configuration language (SCL). Physical devices such as circuit breakers are mapped to logical devices with specifically defined functions, data types, and attributes, such as their states and permitted functions.

In addition to a data model, IEC 61850 defined a communications model for methods and performance requirements related to data exchange. IEC 61850 was designed to run on top of a standard Ethernet LAN, usually implemented with ruggedized switches and routers. Cabling could be standard copper wire, but is almost always fiber optic to avoid electromagnetic interference, to prevent unplanned power conductors, and to permit high throughput should it be required. IEC 61850 defines two communication busses or LANs in the substation, a process bus and a station bus, although new trends can support one physical network with two logical networks. The process bus sends raw power system information such as status, voltage, or current

from switchyard devices such as transformers to the IEDs, where the data is processed into reported measurements or logical decisions and actions. The process bus is very sensitive to delay, so it has high bandwidth to reduce packet insertion delay and eliminate any congestion-based losses which would incur retransmission delays. Due to its importance, the process bus often has redundant components to ensure high availability. The station bus connects all of the IEDs, switches, and other networked equipment to each other and to a router for external communications with the utility control center or any other entity that needs data from the substation. The station bus is used for less sensitive data compared with the process bus, but still uses high bandwidth and redundant and reliable networks to ensure proper substation operation.

A number of different communication protocols are defined by IEC 61850. They can be classified into three different groups: machine-to-machine (M2M), client-server, and configuration protocols. The M2M protocols are based on the Generic Substation Event (GSE), which is a peer-to-peer layer 2 protocol that multicasts events to multiple devices, typically IED to IEDs. The GSE protocol is further subdivided into Generic Substation State Events (GSSE) and Generic Object Oriented Substation Events (GOOSE). In GSSE, only status events can be transferred, and practically speaking it is seldom used, as the industry standardizes on GOOSE messages. Any data set, such as status or values, may be sent via GOOSE. The IEC 61850 standard specifies that certain GOOSE messages must be sent and received within 4 ms, which equates to roughly the time of one-quarter of a wavelength in a power system operating at 60 Hz, and is considered critical for actions such as tripping protection devices. To minimize the network and device processing time, GOOSE was designed to operate at layer 2 and not layer 3, minimizing the processing time associated with the upper layers of the Open Systems Interconnection (OSI) model.

Messages are sent via GOOSE as a publish-subscribe model, in which the publishing device sends to a class of subscribers without regard for their unique identity and without knowledge of whether or not the message was successfully received. For speed and reliability, GOOSE data is embedded directly in Ethernet packets and sent over a virtual LAN (VLAN) with IEEE 802.1Q priority tagging. Messages are also automatically retransmitted at varying intervals and automatically tagged as a new or retransmitted message. Sampled measured values (SMV) messages are similar to GOOSE messages, but optimized for interchanging sensitive analog data, such as measurements from current and voltage transformers.

The client-server protocols are based on the manufacturing message specification (MMS). MMS is used to communicate between equipment such as remote terminal units (RTU) or data concentrators and IEDs. The MMS works under a client-server architecture in which the client (RTU) requests information from a server (IED) that has the field data. MMS uses the complete TCP/IP protocol stack, including IP addresses and all the control fields, unlike the GOOSE protocol, which uses layer 2 media access control (MAC) addresses to deliver its packets. It is useful to think of GOOSE as operating in a horizontal fashion between devices across the substation

and MMS messages traveling vertically between a sensor or actuator and a specific control element.

The configuration protocols define the interchange between engineering configuration tools and IEC 61850 substation components. The configuration is defined in the SCL, which is based on a structured XML file with specific elements that help represent the power grid systems.

1.3.3 Example IEC 61850 Functionality

A full description of IEC 61850 is beyond the scope of this chapter; however, an example of its functionality is provided in this section to better appreciate the operation of the protocol and the correspondence to physical hardware and network devices. A key element of the protocol is SMV and GOOSE messaging. The example below shows how the protocol behaves in a protection scenario. A hardware device in IEC 61850 may house one or more *logical devices*. A logical device is composed of one or more predefined *logical nodes*. For instance, a protection relay logical device could be composed of the logical nodes instantaneous overcurrent protection (predefined in IEC 61850 and denoted PIOC) and similarly protection trip condition (PTRC). The PIOC subscribes to SMV messages published on the process bus by devices such as a current transformer in the switchyard and reports when some overcurrent situation arises. From the IEC 61850 perspective, a PIOC is a data object, with predefined fields which have one or more attributes. The PTRC decides when the data in the PIOC warrants tripping the relay. A trip results in a GOOSE message being published to other logical devices, which may reside in the same hardware device, in the same equipment bay, or perhaps in a different bay or substation. For the purposes of this example, let the different logical devices be in different bays. Although there are no explicit commands defined in a GOOSE message, a state change of a Boolean value that represents a virtual trip is effectively a command for other devices. A circuit breaker (XCBR) will have been configured to subscribe to this relay. It receives the GOOSE message and physically trips a switch in the switchyard, possibly via a GOOSE message on the process bus. The trip open event is reported via a GOOSE message, to which the PTRC subscribes so that it can verify that the logical command has been physically carried out. This same message may also be subscribed to by an auto recloser (RREC). The recloser notes the circuit breaker tripping open, and after a waiting period, commands the circuit breaker to close. If the overcurrent fault has cleared, normal operation will continue (Figure 1.1).

1.3.4 Challenges and Vulnerabilities

The IEC 61850 standard uses abstraction of power elements, functions, services, and communication protocols to provide better device interoperability and simpler commissioning. While the foregoing description is brief, the standard itself and a number of other resources provide exhaustive detail, and so are not reproduced here. While IEC 61850 is a forward-thinking standard, not all future requirements were

predicted, and the remainder of this section details some of the challenges we have experienced in the lab and the field.

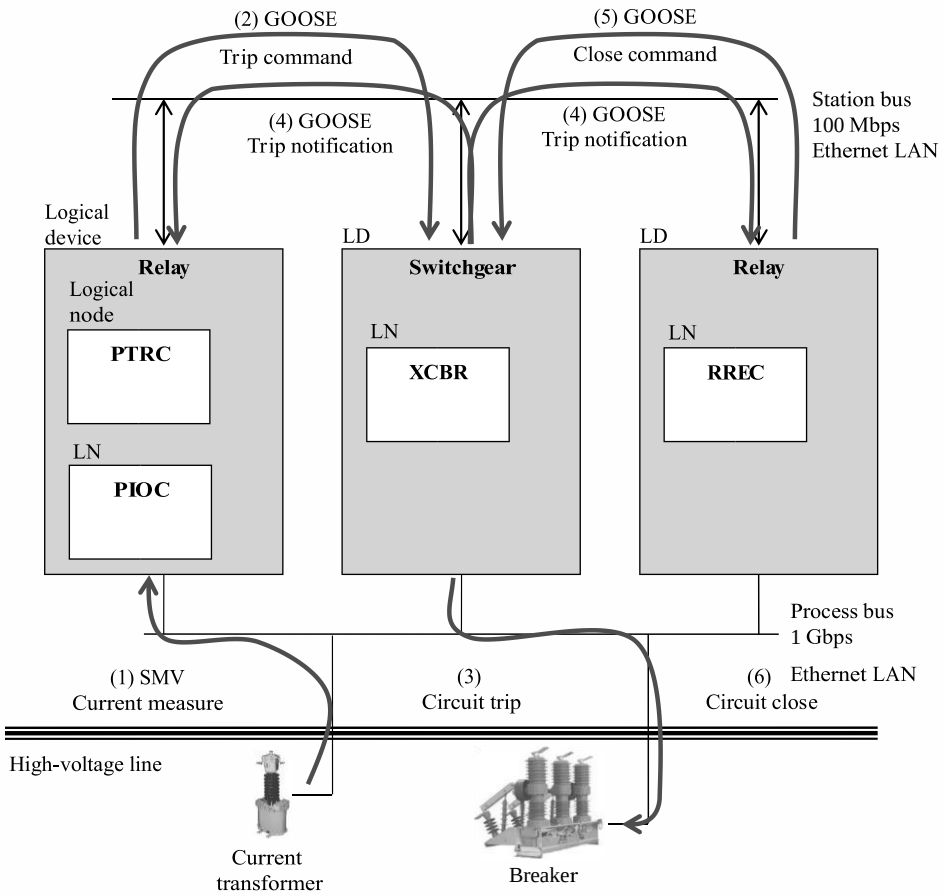


Figure 1.1 IEC 61850 Example: Steps (1) to (6) in a current overload condition.

1.3.4.1 Complexity

One downside of the move from legacy communications to IEC 61850 is the increased technical complexity, a situation which has operational and human consequences. While IEC 61850 is simpler than previous solutions that used dedicated wires between every device and its controller, nevertheless, as the demand for more electricity and new technologies on the grid increases, more and more IEDs are being integrated into the substations. As a result, the substation computer networks are ever more complex and more difficult to manage. Utilities may lack the right operational technology (OT) or IT engineers to support the new infrastructure, creating a reliance on outside

consultants or requiring significant internal training. For at least a period of time, utilities may not fully understand or fully control their own networks.

The engineers configuring the computer network today are power engineers whose specialization is working with the electrical half of the electric grid, not the computer network half. They may lack the training to properly configure computer network devices such as switches and routers, which may result in minimal attention to computer network security or even skipping security configurations altogether.

The IEDs, devices that read information about the substation, have to be physically connected. The process of connecting each IED with every other IED requires significant cable management skills to prevent the network of cables from becoming a tangled web of poorly marked wiring. Adding an IED to a substation means adding more cables and making sure that each existing IED is correctly connected to the new device. This can be a time-consuming and error-prone process, and errors can have significant consequences. In legacy networks, troubleshooting communication problems might include tracking cables. Tracking a GOOSE message requires understanding the configuration file of a communication device, understanding the interface commands specific to a given switch manufacturer, and being able to do an abstraction of the network. This is a demanding task, which requires network specialists or power engineers with a significant background in data networks.

With new networks come new vulnerabilities and the need for additional security measures. Switches require configuration for VLANs, port security, multicast filtering, and other tasks which increase complexity and the possibility of misconfiguration. While IEC 61850 permits interoperability between devices, it does not require that all devices are configured the same way. Ethernet switches from different manufacturers, for instance, may each have their own interface command language. Configuration and maintenance of IEC 61850 networks is a significant challenge for even experienced engineers due to their complexity. Care must be taken to prevent manual configuration errors, as these errors can have real consequences. We have first-hand knowledge of a simple switch misconfiguration leading to a city-wide blackout that lasted several hours. Time and attention spent on complex and unfamiliar tasks is time not spent on operational or security measures.

1.3.4.2 Cyber-Physical Security for IEC 61850

In the early days of IEC 61850, there were no recommendations for security on the layer 2 multicast GOOSE and SMV messages. The vulnerability was considered to be low, because the messages were running in a confined network inside a substation protected by the physical network isolation. This is not true today, when contractors get inside substations and have to perform maintenance connected to the data network or when new applications are running GOOSE messages outside substations for wide-area transmission protection schemes and distribution automation schemes. Further, substations have become more connected to external networks and often employ wireless networks, with the potential to expose their IEC 61850 network to outside attackers.

In 2007, the same technical committee that developed IEC 61850, the IEC Technical Committee 57 (TC57) in the Working Group 15 (WG15), released the IEC 62351 standard to provide security to a number of TC57 protocols, including IEC 61850 GOOSE messages. The objectives of IEC 62351 are authentication of data transfers through digital signatures, intrusion detection, and prevention of eavesdropping and spoofing. This provides security enhancements for MMS, GOOSE messages, and SMV messages. Part 6 of the IEC 62351 standard covers data and communication security for IEC 61850 peer-to-peer profiles, Part 3 defines the communication network and system message authentication profiles including TCP/IP, and Part 4 specifies the mechanism of strong authentication to be used with MMS profiles. These definitions provide manufacturers and integrators with the tools necessary to implement security for IEC 61850 and the GOOSE stack. Although IEC62351 addresses many security issues, problems remain.

1.3.4.3 The Problem of Encryption and Message Authentication versus Latency

Latency is one of the primary barriers to implementing security for peer-to-peer communications between IEDs. IEC 61850-5 specifies a 4 ms maximum delay for class P1 type 1A GOOSE messages related to breaker trip functions. As a result, encryption or other security measures that increase delay or latency are avoided.

The IEC 62351 standard defines a mechanism that requires low computational power to authenticate data when adding a digital signature. The digital signature is created via mathematical techniques to validate the authenticity of a digital message using asymmetrical cryptography. This kind of scheme uses public and private keys to authenticate the message. The public key is shared with everyone to decrypt a hash of the message, while the private key is kept private by the publisher to sign the message. In the IEC 62351 standard, Part 6 states: "for applications using GOOSE and IEC 61850-9-2 and requiring 4 ms response times, multicast configurations and low CPU overhead, encryption is not recommended". Nevertheless, the standard does not say anything about authentication and its limitations. Based on the ambiguity of authentication or encryption requirements, some manufacturers do not implement any security in their IEDs, arguing that any security mechanism will increase the processing time, decreasing the speed of action against a fault.

At present, it is difficult to reconcile the needs for security and low latency. One study conducted by Cambridge University and ABB in 2010 showed that processing (encoding and decoding) digital signatures required intense central processing unit (CPU) consumption. Therefore, 32-bit Intel and ARM cores are generally incapable of computing and verifying a digital signature using the Rivest, Shamir and Adleman (RSA) algorithm with 1024-bit keys within 4 ms. The time for a digital signature to be generated at the sender and verified at the receiver is shown in Table 1.2, as well as other similar algorithms such as the Digital Signature Algorithm (DSA), the Elliptic Curve DSA (ECSDA), and the Boneh, Lynn, Shacham (BLS) scheme. Although RSA

is the fastest (8.3 ms), this is not good enough to comply with the 4 ms time constraint. In a 2011 report, NIST qualified the RSA 1024-bits keys as acceptable through 2011, deprecated from 2011 through 2013, and disallowed after 2013. After 2013, it is recommended to use 2048-bit keys, which will make the 4 ms time restriction even more difficult to meet.

Table 1.2 Time to Generate and Verify a Digital Signature on a 1.0 GHz Pentium III Processor for Different Schemes

Algorithm	*Generation Time (ms)*	*Verification Time (ms)*	*Bandwidth (bits)*
RSA	*7.9*	*0.4*	*1024*
DSA	*4.1*	*4.9*	*320*
ECDSA F_{2160}	*5.7*	*7.2*	*320*
ECDSA F_p	*4.0*	*5.2*	*320*
BLS F_{397}	*3.5*	*23.0*	*170*

Source: **D. Dolezilek and L. Hussey, Requirements or recommendations? Sorting out NERC CIP, NIST, and DOE cybersecurity, in 64th Annual Conf. for Protective Relay Engineers, 2011. With permission.**

The CPUs embedded in the IEDs have restrictions due to power dissipation. The IEDs are fanless, since they are commonly installed in closed cases to avoid environmental issues such as dust, water, or insects. Thus, many embedded processors are slower than the 1.0 GHz processor used in this table, and processing times will be even longer. New technologies such as multiple cores may enable faster computation within the same heat dissipation budget; however, there are many IEDs already installed with slower CPUs.

Currently, neither the IEC 62351 recommendation nor proprietary manufacturer solutions have been implemented extensively to improve the security of GOOSE messages. In November 2011, Siemens published a patent to implement a new method of group key generation and management for the GOOSE model that could help to address the need for low-latency security. Meanwhile, there is little clarity on how to implement security for fast GOOSE messages without degrading the actual performance of the IEDs.

1.3.4.4 Other Issues

The rapid advance of technology and the lengthy standardization process can create gaps in needs, capabilities, or security that go unaddressed for a period of time. The IEC 61850 standard was originally designed for intra-substation communication on a LAN, and some of the protocols involve layer 2 multicasts that are not easily routable between different networks without compromising the integrity of the substation

automation architecture and security. An amended standard, IEC 61850 90-1, was released to allow inter-substation communication, and IEC 61850-90-5 defines routable GOOSE and SMV protocols, but this took
time.

A current issue is the lack of security within the substation network once a machine is physically connected. It has been shown that once connected, without authentication, a machine can inject traffic indicating the occurrence of a substation event, the results of which could be as severe as the substation going off-line or initiating a cascading failure. While physical security at substations is relatively good, at least in the United States, many operate remotely and without staff. Controlling physical access is also not always straightforward, as power systems, substations, and equipment may be owned, installed, and maintained by a federation of partners or contractors.

While the transition from analog to digital data acquisition allows the power industry to innovate with new communications technologies and protocols such as IEC 61850, it also poses new cyber-physical security problems that can affect the stability and reliability of the power grid. In the following section, we discuss IEC 61850 based attacks.

1.4 IEC 61850 Attack Vectors, Consequences, and Mitigation

1.4.1 Attack Vectors and Techniques

An attack is defined by the motivation, vectors, and techniques. For this work, we assumed a motivated attacker and focus on the attack vectors and techniques. The attack vector is a path or means by which an attacker gains access to a computer or network in order to achieve their ultimate goal. Attack vectors enable exploitation of system vulnerabilities, including human elements. Access to the network could be obtained via installation of malware on the computers of maintenance operators, engineers, or manufacturer support teams who access a GOOSE network and are unknowingly carrying the malware. A similar attack vector was used to allow the Stuxnet worm to gain access for an attack on Siemens industrial software and equipment in 2010.

An attack vector can come from malicious persons among cleaning crews or substation personnel who have access to the IEC 61850 network. Another attack vector is through manufacturing facilities of producers of IEC 61850 IED equipment or other network equipment. Such equipment can be infected with malware at the time of manufacture and installed directly in a substation, bypassing physical protection and providing the malware with a host. The attacks that we describe can be hosted on even simple devices.

There are several layer 2 attack techniques that could be applied to GOOSE messages, since the underlying IEC 61850 network is Ethernet. Attacks on Ethernet include: address resolution protocol (ARP) attacks, MAC flooding attacks, spanning-tree attacks, multicast brute-force attacks, VLAN trunking protocol attacks, private VLAN attacks, identity theft, VLAN hopping attacks, MAC spoofing, and double-encapsulated 802.1Q/Nested VLAN attacks. An attack could be created using a variety of techniques described above, and the structure of protocols in the OSI model are such that the upper layers in the model could be unaware that layer 2 has been compromised.

1.4.2 Attack Consequences

There are several consequences if a layer 2 attack is executed in a substation. The main purpose of the GOOSE message is to carry vital information (alarms, status, and control) between devices. Any alteration of these values could create an automation breakdown, causing a circuit breaker to miss an operation, bypassing interlocks, or causing physical damages in field devices such as power transformers or circuit breakers. If the attack compromises a bus bar or differential protection, more than one distribution or transmission circuit could be affected, and as a result, one part of a city or an entire region would suffer an outage. If the same attack involved transmission or generation circuits, the outage could trigger cascading failures and become sufficiently large to affect complete cities or states.

As a specific example, the Palo Verde Nuclear Generating Station (PVNGS) and California ISO use GOOSE messaging between their substations to create a remedial action scheme (RAS) on the Salt River Project. The GOOSE messages are implemented in a flat Ethernet ring and carry analog and digital values to control the load at both sides. Measured changes in generation levels on one side of the system must affect load balance on the other side of the system over 150 miles away in less than 1 s. A GOOSE attack that appears to changes the values of generation levels could produce voltage dips, frequency excursions, and cascading problems throughout the Western Electricity Coordinating Council (WECC) region.

Recall also that the IEC 61850 architecture has been applied to hydroelectric plants, wind turbines, distribution feeders, and high-voltage switchgear (see Table 1.1). Thus, these domains are also vulnerable to the kinds of attacks described here.

1.4.3 Mitigating Attacks

Although some attack vectors could be reduced using physical security, there are others that are more difficult to control because they use trusted personnel or equipment. Some traditional IT techniques to prevent Ethernet layer 2 attacks could be applied to protect GOOSE messages. These practices include, but are not limited to: setting a dedicated VLAN ID for all trunk ports, disabling unused ports and putting them in an unused VLAN, using a VLAN other than the default (VLAN 1), setting all ports to nontrunking, creating an access or prefix list based on user/device credentials, and

avoiding the use of shared Ethernet such as WLANs or hubs. All of these techniques are well documented and known by IT staff.

Using the measures indicated provides some degree of protection against intrusion originating from outside of the organization. For trusted employees or compromised equipment with valid credentials inside the facility, most of the traditional IT techniques would be ineffective. Additional security measures would, therefore, be required. To prevent insider attacks, it is necessary that end devices have security algorithms implemented to encrypt packets or have a digital signature added so that they cannot be monitored by the attacker and authenticated, permitting spoofed packets to be sent. As noted previously, legacy and low-capability IEDs cannot support these cryptographic algorithms.

Solutions such as adding an external security module to network interfaces in each IED add expense and additional failure modes. These devices could be added just to the switches and some key equipment in the Ethernet to provide some limited protection. An alternative approach could use switches and routers that understand the IEC 61850 protocol and inspect GOOSE message content. In this approach, the network could discard or generate alarms when it detects logically inconsistent messages (such as packets with the same MAC address coming from different ports on a switch or messages not consistent with the IEC 61850 configuration).

Software-defined networking (SDN) is a recent innovation to address network complexity and vendor-specific protocols. SDN decouples the proprietary software running on each network device from the hardware that is responsible for forwarding the traffic according to the rules determined by the software on the network devices. With SDN, an open interface (currently led by the OpenFlow standard) abstracts the network from the applications by exposing the forwarding table as the interface to manage the devices. A centralized, logical server (or collection of servers) runs software (which can come from a variety of sources) that has a network-wide view and can monitor and configure the forwarding table. As it is an open standard, the software works across a variety of hardware, and likewise, the hardware can work across a variety of software. As a result, a more consistent environment can be presented for configuration and management of the network supporting IEC 61850.

1.5 Exploiting IEC 61850 via GOOSE

This section demonstrates how to create computer malware that can capture, alter, and reinject GOOSE messages into the network. By taking advantage of existing security holes in the GOOSE messaging protocol, we show how a malware could be used to significantly disrupt the power grid and highlight the need to apply security measures in this area.

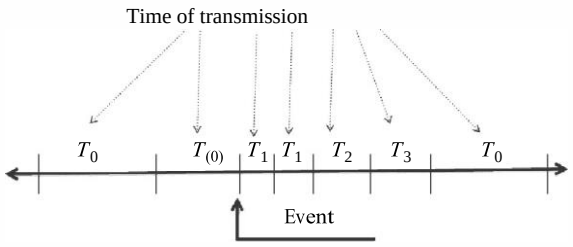
.

1.5.1 Normal GOOSE Function

The main objective of GOOSE messaging is to provide a fast and reliable mechanism for the exchange of data between two or more IEDs over IEEE 802.3 networks. To exchange these datagrams, IEC 61850-8-1 describes a type of communication based on a publish-subscribe model, in which one IED (the publisher) creates a message that is delivered to a group of destination IEDs (the subscribers) simultaneously in a single transmission from the source. GOOSE messages are periodically sent through the network. When there is no change in data set values, the retransmission time between messages is T_0 (see Figure 1.2).

If an event occurs, a message is generated immediately. After the first event message, the publisher retransmits (T_1, T_2, …, T_N) with a variable time separation between messages that is not defined by the standard, but is typically implemented following an exponential back-off until it reaches the stable retransmission time T_0. If T_0 is exceeded, the subscriber could declare a problem in the communication link or in the GOOSE message [35].

The GOOSE datagram has twelve fields that define the protocol data unit (PDU). The first two fields, *preamble* and *start* of frame, are equal to the first two fields of an Ethernet frame. The *destination* corresponds to an Ethernet MAC multicast address. IEC 61850 has been assigned Ethernet addresses that start with the three first octets (01-0C-CD). The fourth octet could be 01 for GOOSE, 02 for GSSE, or 04 for multicast SMV. The last two octets of the six are used as individual addresses for each GOOSE message. The *source address* is a unicast MAC address. The *VLAN priority tagging* is IEEE 802.1Q. The *Ether-type* of a GOOSE message is 88-B8. The *Application ID* is 00. The *length* indicates the total number of bytes in the frame less eight bytes. The *Reserved1* and *Reserved2* fields are reserved for future standardized applications and are set to 0 by default. The last two fields are the *Application PDU (APDU) length* and finally the *frame checksum sequence* [35]. The APDU has ten fields, described here. *DatSet* is a string that describes the name of the data set. *GoID* is the IED sender identifier. *T* is the "time stamp" at which the attribute *StNum* was incremented. *StNum* is the *state number*, a counter that increments each time



T_0 Retransmission in stable conditions (no events for long time)
$T_{(0)}$ Retransmission in stable conditions may be shorter by event T_1 Shortest retransmission time after the event

T_2 T_3 Retransmission time until achieving the stable condition time

Figure 1.2 GOOSE transmission. (From IEC 61850-8, Communication networks and systems in substations: Specific communication service mapping [SCSM]. International Electrotechnical Commission, 2008. With permission.)

a GOOSE message has been sent with any change in the values of the data set. The *SqNum* is the *sequence number*, containing an incremental counter for each time a GOOSE message has been sent. The *Test* field indicates whether or not the message is a test. *TimeAllowedToLive* is the time that the receiver has to wait for the next message. *ConfRev* is the *configuration revision*, a count of the number of times that the configuration of the data set has been changed. *NumDatSetEntries* is the *number of data set entries*, the number of elements that comprise this specific data set.

1.5.2 Building a Practical Cyberattack

1.5.2.1 Technical Details

The following attack was implemented in the Digital Energy Laboratory at the University of Colorado, Boulder as an ethical demonstration of a security vulnerability, with details of the equipment and scripts intentionally omitted. A similar attack could move from the lab to the field in a matter of days.

Our attack uses a GOOSE exploit via spoofing, whereby an intruder publishes false layer 2 packets, and devices on the receiving side mistakenly believe they are receiving valid (true) packets sent by a trusted or secured entity. This attack is possible due to the unencrypted and unauthenticated nature of GOOSE messages, because of the latency issues on IED devices previously detailed.

A practical GOOSE message spoof attack can be divided into four steps. First, monitor packets on the physical ports looking for GOOSE messages based on Ether-type identification. Second, decode the GOOSE message using Abstract Syntax Notation One (ASN1) and Basic Encoding Rules (BER) [36]. Third, change the values inside each data set, keeping the sequence for the different counters and timers. Fourth, encode the packet using BER and send the packet through a physical port, cloning the source MAC address. The schematic in Figure 1.3 shows how the attacker has opportunities between valid messages to insert the spoofed messages with incorrect data.

There are several programs that can be used to do this: Scapy, Yersinia, Macof, TCPDump, Cain & Abel, EtterCap, and Wireshark are a few. This attack was created using Scapy in conjunction with Python scripts. Scapy is also a Python program that enables the user to sniff, dissect, forge, and send network packets. These capabilities allow the construction of tools that can probe, scan, or attack Ethernet networks.

To prove the vulnerability of the GOOSE networks, our attack script uses the network configuration shown in Figure 1.4, which represents a typical substation

automation architecture. In addition, new scenarios were created, such as GOOSE messaging between substations using

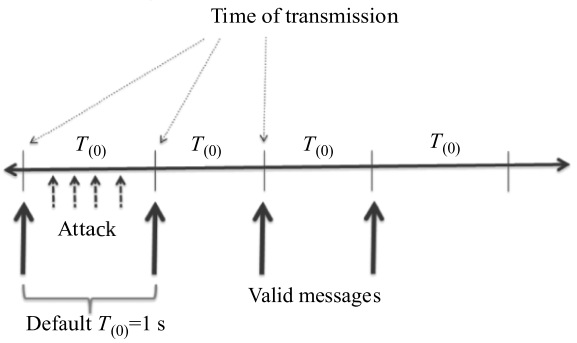


Figure 1.3 GOOSE attack schematic.

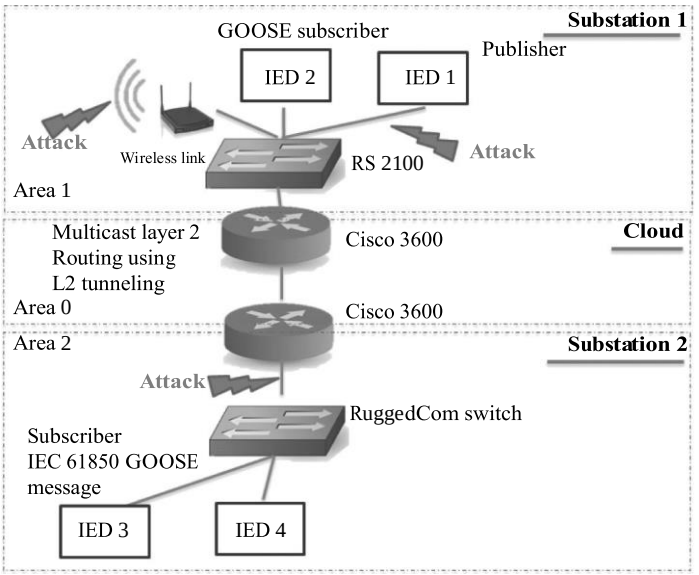


Figure 1.4 Network diagram.

Layer 2 tunneling and wireless communications inside the substation. The lightning bolts in Figure 1.4 represent the attack points. The attack was successful in all scenarios, and we describe one in detail below.

The hardware used for the test included two Cisco 3600 routers, one RuggedCom 2100 switch, one RuggedCom RS900, one Linksys wireless router, and four IEDs. The script ran on a MacBook Air 1.5 GHz Intel core i5 within a virtual machine running Xubuntu OS.

1.5.2.2 Building the Script

The first step to carry out the attack is to identify GOOSE messages in the network. After using Scapy to monitor all physical ports and capture the raw packets, the code parses the Ethernet frames looking for the specific GOOSE Ether-type, which in this case is 0x88B8. Second, it is necessary to decode the GOOSE message using the definition of ASN1 described in the IEC 618508-1. After decoding, the script looks for three specific fields: stNum, sqNum, and the Boolean values inside the data sets. For any Boolean value inside the data set, if the value is true the code overwrites a false, and vice versa. The last part of the code generates the spoofed messages and sends them through the network with the same source and destination MAC address as the valid user. To show that the attack can be successful, we implemented the above steps on the laptop described above.

1.5.2.3 The Results of the Attack

Figure 1.5 shows a Wireshark capture, where the topmost and the bottommost arrows are the true messages. The four middle arrows, events 194 to 197, are the spoofed messages. Looking at the time stamp of the packets 193 and 195, the time to generate spoofed GOOSE messages is less than 1 ms. This means that in a default GOOSE configuration, where the messages are sent at 1 s

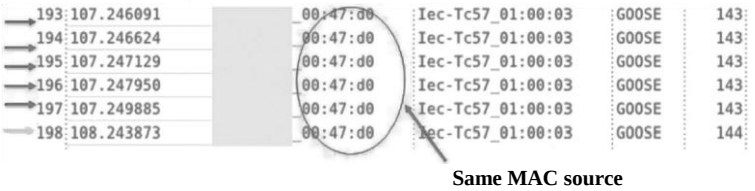


Figure 1.5 Wireshark capture showing spoofed GOOSE messages.

intervals during steady state, the attack could inject hundreds of false GOOSE messages before the next valid datagram reaches the IED.

The process of modifying data is illustrated in Figure 1.6, which shows the variable values in three successive GOOSE messages measured by the laptop at the RuggedCom 2100 in Figure 1.4. The leftmost message is a valid message. The attacker created the next message in the middle, which shows the change of stNum, and that resets the SqNum in the cloned packet. The rightmost message is the next valid message. This keeps the old number sequence, meaning that it is actually out of sequence. We note that the equipment did not generate any error or warning that the messages were out of sequence.

The attacker does not directly know the high-level meaning of this GOOSE message (e.g., that this is a command from a circuit-breaker controller to a circuit breaker). However, he can decode the message to find and change the data values. In Figure 1.6, the attacker changes the Boolean data value from False to True. To verify

this has an effect, Figure 1.7 shows the sequence event recorder (SER) on the IED. The SER monitors the physical outputs and generates a time stamp of output events.

Event 4 (number on the left) shows the times when the valid message instructed the IED to de-assert output 101. After 5 ms, a spoofed message is processed at the IED, asserting the output and generating event 3. Another 995 ms later, the next true message arrives, generating event 2, which again de-asserts the output. In this case, the effect of this action is to cause the IED to trip the relay, which in a real substation could control a circuit breaker or switch. Thus, through spoofed messages we were able to cause actual IEC 61850 equipment that might reside

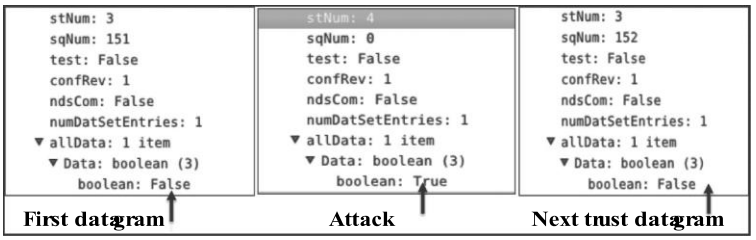


Figure 1.6 GOOSE exploit.

4	06/13/12	18:24:09.637	OUT101	Deasserted
3	06/13/12	18:24:09.642	OUT101	Asserted
2	06/13/12	18:24:10.637	OUT101	Deasserted

Figure 1.7 IED output status.

in a substation to change its state, with the potential to cause outages and other problems as described in Section 1.4.2.

There are many variants on this type of attack. For instance, a single GOOSE frame with a very high sequence number can be multicast to a subscriber. Once processed, any legitimate GOOSE message with a sequence number equal to or less than the spoofed message will not be processed by the subscriber.

1.6 Conclusion

Electric power systems pose unique challenges for cyber-physical security, and adverse events carry significant consequences due to the scale and importance of the industry. In this chapter we provided insight into the structure and function of the electric grid, the evolution of communications and control, and some of the challenges related to this evolution. We provide an introduction to the modern IEC 61850 grid automation standard, and discuss some of the issues and vulnerabilities which require further work. We demonstrated that a simple attack enables malware to control IEC 61850-enabled electrical equipment. This control has the potential to cause outages that range from a single feeder to cascading failure. While there is currently no clear definition of how to

.

implement security for GOOSE messages, utilities and power companies must find ways to implement cyber-physical measures to prevent this kind of attack. We describe several techniques for improving security, as it is of vital importance that network switches and routers be configured to permit only trusted traffic and users inside the substation network.

Lack of clarity in the standards concerning security for IEC 61850 layer 2 messages with current technology opens the door for new research. This includes a search for security measures and development of standards that could be backward compatible, allowing thousands of IEDs to be made capable of running GOOSE securely.

Acknowledgment

This work was supported by U.S. Department of Energy grant DE-OE00436.

Author Biographies

Martin Saint is currently a visiting scholar at Carnegie Mellon University in Rwanda. His background includes network and telecommunications engineering, creating and managing facilities and infrastructure for data center and telecommunications clients, work in emergency planning and response, and corporate business management. He currently teaches and researches in the areas of complex networks, wireless networks, and cyber-physical systems. Martin holds an MS in telecommunications and is a PhD student in the Interdisciplinary Telecommunications Program at the University of Colorado. He has studied with the U.S. Federal Emergency Management Agency's Emergency Management Institute, the International Centre for Theoretical Physics in Italy, and Idaho National Laboratory, home to the U.S. Department of Homeland Security's Control System Security Program and the Industrial Control Systems Cyber Emergency Response Team. He is a member of the Department of Homeland Security Industrial Control Systems Joint Working Group.

Juan Hoyos has a decade of experience in advanced computer network communications, specializing in substation communications engineering and automation. He was most recently a lead hardware engineer at Empresas Públicas de Medellín (EPM), Colombia's largest utility, which provides electricity, gas, water, and telecommunications services. EPM's energy strategic business unit (SBU) provides over 4 million customers with over 3000 MW of capacity. Mr. Hoyos holds an MS in telecommunications (with a specialization in energy communication networks) from the University of Colorado at Boulder and a BS in electronics engineering from Universidad Pontificia Bolivariana, and is a certified project management specialist.

Timothy X. Brown is a professor in electrical, computer, and energy engineering in the Interdisciplinary Telecommunications Program at the University of Colorado,

.

Boulder. He received his BS in physics from Pennsylvania State University and his PhD in electrical engineering from California Institute of Technology in 1990. His research interests include adaptive network control, machine learning, and wireless communication systems. His research funding includes National Science Foundation (NSF), Federal Aviation Administration, Department of Energy, and industry. He is a recipient of the NSF CAREER Award and the Global Wireless Education Consortium Wireless Educator of the Year Award. Since 2013, he has been a visiting professor in electrical and computer engineering at Carnegie Mellon University's campus in Rwanda.