GOVERNMENTS AND SECRECY

CHAPTER 17

723025.

ABOUT THIS CHAPTER

This chapter surveys government cybersecurity with a special focus on military-grade secrecy requirements. Although parts of this may apply to other national governments, this chapter focuses on policies and concepts specific to the U.S. government and often to the U.S. defense and intelligence communities. This chapter examines the following aspects of governments and secrecy:

- The secrecy problem as seen by governments and by the defense and intelligence communities
- Security classifications and clearances
- National cybersecurity policy issues and typical policy elements
- Communications security in the U.S. defense and intelligence communities
- Special data protection concerns, like media handling and transmission security
- Cybersecurity in critical applications

17.1 Secrecy in Government

Governments try to rely on commercial products for most tasks, including information technology. Many countries even rely on a number of commercial technologies for military applications, though nuclear-armed countries tend to spend more money on specialized equipment. In information technology, government secrecy requirements often lead to specialized products, technologies, and equipment.

Government secrecy in the United States evolved during the 20th century. Before World War I, the state department routinely published its communications with embassies and with other governments. Military secrets were few, because military advantage usually resided in physical superiority. When the U.S. Army or Navy went to battle, secrecy and surprise were important, but secrecy played little role in peacetime.

This changed in 1917. On the same day President Woodrow Wilson asked for a declaration of war, an Espionage Act was introduced to Congress. The law made it unlawful to disclose information about national defense. Even though espionage earlier had been handled through laws regarding treason, this established a different offense: a failure to keep a secret.

Following World War II and the development of the atomic bomb, government secrecy took on apocalyptic proportions. If a cold-war adversary could exploit a military secret to make a successful nuclear attack, then the target might be obliterated while the aggressor suffered little damage.

When we talk about risks and threat agents in the national arena, we often speak of ***adversaries***. The term refers to threat agents motivated by loyalty to a particular nation or cause who see our nation as a threat. Unlike threat agents associated with private or commercial risks, these agents often are willing to sacrifice their lives to achieve their objectives. Moreover, agents of national governments may have far greater resources behind them than those in private industry.

When we compare the risk of warfare or even nuclear annihilation with risks faced in private and commercial realms, we see why governments put more resources into secrecy. Commercial and private enterprises may be obliged to keep certain secrets, but disclosure doesn't obliterate a nation. Although a disclosed secret could destroy jobs and companies, and possibly lives, there is almost always a way to pay restitution for leaked secrets in the private and commercial sphere. We can't do that with secrets that risk a nation's existence.

This justification arose during the Cold War era and variants of it continue today. This has led to an elaborate bureaucracy for establishing, identifying, and managing secret information as well as an elaborate technical infrastructure to protect secrets. This has had a major impact on government information technology since computers evolved in the 1950s. Military and intelligence agencies also paid for most early computer developments in the United States, United Kingdom, and other countries.

Hostile Intelligence Services

Governments typically face a more sophisticated threat than private enterprises. Companies may, of course, have competitors who systematically try to steal proprietary secrets and confidential company information. However, both the competitors and the companies themselves must limit the effort they put into espionage. Companies thrive on profits and spying is an overhead expense.

A ***hostile intelligence service*** is a threat agent that collects sensitive information on behalf of a potential adversary. Traditionally, such services worked on behalf of nations. This is not always true; some may work on behalf of nonnational entities, like terrorist organizations or extremist political groups.

Hostile intelligence services may be very well funded when associated with large or wealthy nations. Both the United States and Russia deployed human agents and technical means, including satellites, submarines, and large-scale code breaking operations to penetrate the others' secrets. Both nations likewise spent large amounts of resources to protect their most critical secrets.

Classified Information

The concept of ***classified information*** refers to information explicitly protected by particular laws or regulations and marked to indicate its status. Although many

governments also have laws to protect private personal information and health care information, neither of these are considered classified. Typically, a government classifies information associated with national security or intelligence activities.

In countries with a culture of openness or free speech, classified information represents an exception in which disclosing information may be a criminal act. Nations justify such restrictions is necessary to discourage people from disclosing sensitive information. According to typical laws and regulations, information is classified when its disclosure might cause "serious" or "exceptionally grave" injury to the nation.

In the United States, the free speech guarantee of the Constitution's First Amendment poses a challenge to the secrecy needs of the defense and intelligence communities. Although federal laws and regulations make it possible to prosecute individuals for disclosing classified information, most criminal convictions are limited to those who release more sensitive, "Top Secret" information. There have been few civilian convictions for disclosing less-sensitive—but still classified—information.

17.1.1 The Challenge of Secrecy

Secrecy poses a challenge in two dimensions. First, disclosure is ruled by Transitive Trust; a secret remains secret only if *everyone* who knows it keeps it secret. Second, secrets are easy to leak. There are many ways for a physical fact to leak out, like a scientific formula or the attributes of a machine or weapon. A threat agent may discover the fact independently or accurately infer secret facts through observation and study.

In the 1980s, the novelist Tom Clancy spoke informally with many military experts, observed unclassified military activities, and read extensively about military topics. He had no access to classified information. Nonetheless, military officials claimed that some information appearing in his novels was in fact classified. Clancy says that such information is the product of combining unclassified facts to infer classified ones.

Clancy's experience illustrates the problem of ***aggregation and inference.*** If we collect a large amount of public information on a classified topic, the *aggregate* of information may contain classified information. We extract the classified information by *inferring* it from the visible facts.

Information rendered to paper or to bits often leaves evidence behind. In Section 7.4.3, we saw how difficult it was to totally erase data from a hard drive. Printed documents may leave telltale information inside the computer that operates the printer and in the printer itself. Photocopy machines may retain thousands of images of previously copied documents.

To keep a secret, we must consider the leakiness of information in general, plus we must take account of the carelessness and possible blunders of *everyone* who knows the secret. A typical strategy to protect secrets is to establish a comprehensive set of policies and procedures to manage and protect the secrets. The U.S. Defense Security Service has published a set of such procedures in their 140-page *National Industrial Security Program Operating Manual* or *NISPOM*.

The Discipline of Secrecy

Secrecy processes like those described in the *NISPOM* provide layered defenses to help individuals avoid disclosing secrets. In theory, everyone who handles the secrets uses a similar process, though this is not true in practice. The *NISPOM* describes procedures for private enterprises that handle classified government secrets, but government agencies and military commands make their own rules.

Secrecy procedures often rely on a collection of simple strategies. When we combine the strategies and apply them consistently, the secrets should remain safe. Basic strategies include:

- Secrets are secured by default. Under normal circumstances, keep classified documents locked up so that others can't retrieve them. There are security standards for how long it takes to break into a cabinet approved to store classified information. Always lock up classified documents in approved cabinets except when actually in use. Approved cabinets often resemble safes, complete with combination locks.
- Secrets are never left unattended. If the secret document isn't locked up, then it must remain under the direct physical control of someone authorized to have it. If the authorized person leaves the area, the classified document goes with the authorized person.
- Avoid identifying secrets as secrets. A nonclassified document should avoid referring to a classified document, because it indicates the existence of a secret. When carrying a classified document, hide the cover so that others can't tell it is a classified document.
- Secrets are revealed only in safe places. Discussions of classified information are restricted to rooms declared safe. Exclude cell phone, webcams, and other recording or transmission equipment from the area. Don't work on a classified document except in a closed area that excludes others who might eavesdrop or shoulder surf.
- Verify permissions before sharing. Always check with authorities before sharing classified information with others. Confirm that the intended recipient is both authorized to receive the information and has the appropriate Need to Know.

These five strategies are simple to enumerate. The specific procedures to implement them can become quite detailed. It can be difficult to follow all security procedures, day after day, year after year. People become lax or careless without further help. We address this with two familiar strategies:

1. Defense in Depth. Provide layers of protection; multiple opportunities to detect lapses in security and fix them before classified data actually leaks. For example, people who work with classified materials on a daily basis usually work in a closed area that only allows access to people allowed to share the secrets. If someone forgets to lock up a classified document, the document remains in the closed area, inaccessible to unauthorized people.
2. Security awareness. Everyone responsible for protecting secrets must participate in periodic briefings, retraining, or other security awareness activities to help ensure ongoing compliance with procedures.

Practical security procedures recognize the inevitability of human errors and take steps to reduce their risk. Childrens' diaries rarely remain secret because it is hard for anyone to systematically protect a secret, especially a child.

Secrecy and Information Systems

It is extremely difficult to control the spread of secrets—or of any type of information—in an information system. Secrecy seems to pose a simple problem; we use a few trustworthy processes to handle the data and we block access from everything else.

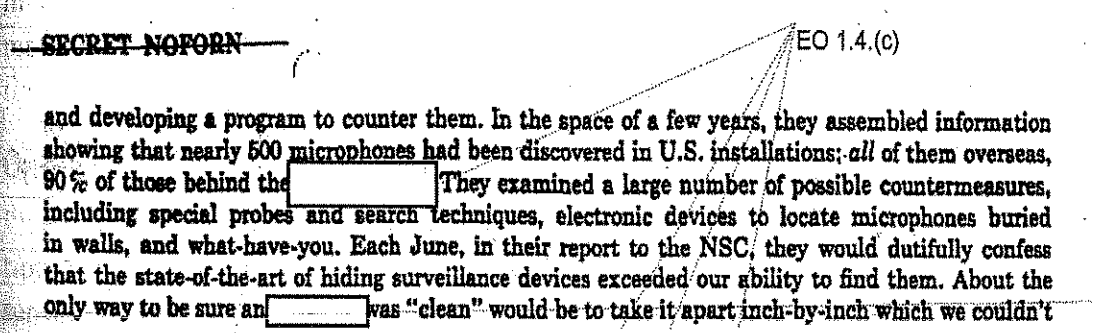
However, such a solution relies on a flawless operating system. We have no such operating system. It relies on flawless applications for constructing and modifying secret documents. Applications mustn't accidentally leave too-secret information in a less-secret document.

This is called the *redaction problem*; how can we remove sensitive information from a document and be confident that we removed *all* of the sensitive information? It is easy to redact a paper document; we simply blank out the information we want to remove (Figure 17.1). Blanking out doesn't always do what we expect in a word-processing program.

A classic example occurred during the Iraq war; the U.S. military released a report about an incident at a checkpoint where civilians were killed. The original report contained a great deal of classified information; it was edited to hide the information and then released to the public. Unfortunately, the editor simply placed black boxes over the sensitive text. In fact, the text was still present in the document's released Adobe Acrobat file, *underneath* the black boxes.

Exposure and Quarantine

Many security experts see secret information as analogous to contagious diseases. Until medical science developed tests to distinguish healthy patients from those carrying such a disease, public health officials would place people in quarantine if they were simply *exposed* to an infected person. Boarding schools routinely shut down for several weeks if a student was diagnosed with an infectious disease. Everyone who came in contact with a sick student was placed in quarantine while sick students were treated. Those not in contact with sick students were sent home to avoid both the sick and the exposed.



Courtesy of the US National Security Agency. Accessed on August 19, 2011 at [http://www.nsa.gov/public_info/_files/cryptologic_histories/history_comsec.pdf]

Figure 17.1 Redacted NSA document.

Computer systems follow this "exposure and quarantine" model when handling highly sensitive information. If any data in a system is considered highly sensitive, then *all* data on the system is treated as being equally sensitive. If an operator produces a document containing no sensitive data, the operator must take special steps to export the nonsensitive data and nothing else.

Redaction technology is similar to disease testing of a century ago. We can't automatically and reliably ensure that we have removed every bit of sensitive information from a document. Our editing software may have some subtle feature or undocumented flaw that retains information in an unexpected place. Thus, if any classified information infects a document, we can't be positive that our editing has removed all of it.

17.1.2 Cybersecurity and Operations

Governments place a high value on protecting their most important secrets. Hostile governments may place an equally high value on finding that information. Strategies and actions unknown in the world of legitimate commerce are routine in international conflicts, even when countries aren't directly at war. These particularly apply to these situations:

- Intelligence and counterintelligence
- Information operations
- Operations security

The following subsections examine strategies and techniques applied in these challenging environments.

Intelligence and Counterintelligence

The intelligence community uses the whole gamut of "spy tradecraft" to collect information and to try to defeat adversary spies. Although it's customary to collect information about "adversary businesses" in the commercial world, many of these measures are too extreme or are even illegal in the commercial realm. They are routine in the national intelligence communities.

- Human-based intelligence gathering (HUMINT)—the use of human spies. In some cases, companies may take legal action against people who share their secrets with competitors.
- Covers—assuming a different name, position, or other personal trait to hide sensitive information, like a person's actual personal identity or actual job title or position. This is very common with intelligence agents. The CIA does this routinely with many staff members. Former CIA employees sometimes must provide cover information on a resume when job hunting. In the commercial world, a cover is "misrepresentation" and may be reason to fire the perpetrator.
- Technical surveillance countermeasures—using various techniques to defeat eavesdropping, bugs, wiretapping, or other surveillance techniques. Private and commercial enterprises might either perform illegal surveillance or take steps to defeat

it in extreme situations. Technical surveillance often violates the law; if a commercial adversary does it, the victim may pursue legal action against the perpetrator.

- Emergency destruction—the process of destroying information that risks falling into the hands of adversaries. Legitimate private and commercial enterprises rarely have information that is sensitive enough to justify emergency destruction.

Although some or all of these techniques occasionally may arise in private or commercial environments, it is the exception rather than the rule. Military and government agencies rely on them more often because they can't use the same types of financial inducements or legal threats to deter their adversaries.

Military Information Operations

Within the U.S. military, ***information operations*** are intended to influence or actually disrupt the decision making of adversaries. These operations rely on a variety of measures that are rarely used in private or commercial activities. These include:

- Electronic warfare—using the electromagnetic spectrum to jam, mislead, or attack an adversary. This may involve eavesdropping on adversary signals or on jamming them.
- Computer network operations—exploiting and attacking adversary computer networks on one side and defending our own networks from attack on the other.
- Military deception—specific actions taken to mislead an adversary in order to promote the success of a military operation. The deceptions intend to encourage particular actions or inactions on the part of the adversary.
- ***Operations security*** (OPSEC)—managing publicly visible aspects of military operations to prevent disclosure of sensitive information about the operations. We discuss this further later.
- Psychological operations—conveying selected elements of factual information to foreign audiences to influence their behavior. These operations may appeal to public emotions and motives to try to influence public opinion and the actions of governments and organizations.

Companies and other private organizations may use some of these techniques in a milder, legal form. Advertisements, public relations campaigns, and other activities to manage an enterprise's public image clearly have similar objectives to information operations. In general, most companies avoid actually violating laws or incurring legal risks.

Operations Security

OPSEC is a process for assessing publicly visible ("friendly") aspects of military operations from the point of view of adversaries to ensure that adversaries can't deduce sensitive information from its publicly visible actions. An OPSEC analysis may restrict public activities or lead to cover-and-deception activities.

A classic example arose during the first Gulf War. In late 1990, as the U.S. military approached the moment of their invasion of Iraqi-held Kuwait, a pizza delivery official

reported a sharp spike in nighttime delivery orders around Washington, D.C., and the Pentagon. A related legend claims that pizza orders also spiked prior to troop deployments in Grenada, Panama, and the Middle East and during the Kremlin coup in 1991.

OPSEC experts call these visible side effects of military operations "unclassified indicators." An effective OPSEC program eliminates such indicators. Sometimes we suppress indicators by keeping an operation as secret as possible until implementation. During the 1991 Gulf War, the air strike planning activity was kept secret from the command's Air Force headquarters staff until only a few hours before its execution; this was justified on OPSEC grounds.

Within the U.S. defense community, every major command has an OPSEC program officer who manages the program and coordinates its operation within the command. This includes assessing ongoing activities and operations from an OPSEC standpoint, making assessments of specific programs, and providing awareness and training to the command.

OPSEC planning arises in all operations planning in a military command. A military campaign targets particular strategic and operational objectives and OPSEC planning focuses on ensuring these objectives. The OPSEC planning process is similar to the risk management framework: (1) identifying critical resources (information, in this case), (2) assessing risks, (3) identifying policy goals, and (4) applying security measures. An "OPSEC assessment" applies the process intensively to a particular operation or activity. The assessment involves a multidisciplined team of experts and the results help assess the organization's OPSEC processes and procedures.

Given the central role that websites, email, and personal cell phones play in modern communications, cybersecurity has a significant impact on OPSEC. A careless individual easily may leak information that indicates an upcoming operation or other sensitive activity. In some cases, we prevent this through security training: If people remain aware of data sensitivity, they are less likely to release sensitive information by accident. In other cases, we can monitor websites and other communications to squelch disclosures after the fact.

Another cybersecurity aspect is in the choice of media for sharing sensitive information. Users may share OPSEC-sensitive unclassified information safely via restricted and specifically approved chat rooms or other discussion media. Users should never share data on external commercial sites, because the data could leak to adversaries, even if the site resides in a "friendly" country.

17.2 Classifications and Clearances

Security classification and clearance programs are a distinctive feature of military and government cybersecurity. The outline of a classification system evolved in Great Britain during the late 19th century. All allied powers adopted similar systems before or during World War I, including the United States.

A modern security classification system has four elements:

1. Classification—identifies a special category of information called "classified information" and identifies ***classification levels*** that indicate different degrees of risk of disclosure.
2. Protections—specific security measures that prevent physical access to classified information by unauthorized people.
3. Clearances—a process to establish permission to receive classified information in which we investigate individuals to assess their trustworthiness. A person must receive a ***security clearance*** to be granted access to classified information.
4. Penalties—significant administrative and legal penalties for mishandling or disclosing classified information.

Although commercial organizations occasionally implement similar programs to protect commercial secrets, they are rarely more than a poor imitation. Commercial organizations never need the level of secrecy or assurance demanded in the military and intelligence communities. Moreover, commercial enterprises can't apply the serious penalties a government or military service may establish.

Classification Levels

The "classification" part of classification systems assigns different levels to information. In the United States, we classify information into one of three levels. The classification reflects the degree of damage to national security that unauthorized disclosure could reasonably be expected to cause:

1. Confidential—"damage"
2. Secret—"serious damage"
3. Top Secret—"exceptionally grave damage"

Although we use the phrase classification level here, other publications often use different phrases to mean the same thing. These include, for example, security level, sensitivity level, security classification, sensitivity label, and classification label.

In principle, the classification decision is supposed to balance the risks of disclosure and the benefits of leaving the information unclassified. Classified information is costly to manage and inconvenient to distribute. Moreover, troubles may arise from failures to share information. The 9/11 Commission noted several cases in which unshared information helped prevent detection of the attacks on New York City and Washington, D.C., ahead of time.

Other Restrictions

Figure 17.1 displayed part of a declassified, formerly secret document. The legend "NOFORN" appears after the classification level. This is an acronym meaning "no foreign distribution." In other words, the material must not be shared with foreign nationals, even if they have a U.S.-approved secret clearance. Documents may contain a

variety of such restrictions. Some indicate that recipients first should receive a briefing on how to handle material with such markings. Other legends restrict the document to members of specific projects or programs or to a controlled list of authorized recipients. For example, some documents are "originator controlled" (abbreviated ORCON). In such cases, the document's originator has the sole authority to grant access to it. This often is applied to intelligence data that could disclose information about the source. The team that manages the intelligence source decides to release the data if the risk of losing their source is justified by the benefit of sharing the intelligence data.

When we establish special restrictions to a program's information, we also may require a special clearance procedure. Although the clearance procedure for Top Secret information is more-or-less standard across the U.S. government, access to special programs and certain types of intelligence may require a more elaborate investigation and clearance process. People often refer to such programs as being classified "above Top Secret."

Legal Basis for Classification

Although federal laws passed by Congress make it a criminal act to disclose national security information to adversaries, the classification system is entirely a presidential artifact. The security classification system was established through an executive order issued by the president. Executive orders provide the president with a way to specify how government departments should perform their legally mandated duties. As such, executive orders have the force of law.

As of 2014, the classification system is defined by Executive Order 13526. The order is issued under the president's legal authority as commander-in-chief, because it regulates aspects of national security. The order defines the recognized classification levels, assigns responsibility for classifying information, establishes responsibilities for safeguarding the information, and sets standards for declassifying information.

Minimizing the Amount of Classified Information

It is easy to misuse security classifications. Once information is classified, the government may justifiably refuse to disclose it in court and, in some cases, to Congress. The U.S. Supreme Court has upheld the government's right to protect classified data even when it may be important evidence in a civil or criminal trial. To minimize abuse, classifiers may not classify information simply to hide embarrassment, waste, fraud, errors, or criminal conduct.

The amount of classified information has grown dramatically over time and it continues to grow. Most U.S. presidents have taken steps to stem the tide when they revise the classification system through a new executive order. These steps fall into three categories:

1. Limit the ability to classify information. In most cases, it is limited to a handful of agency heads, who may delegate it to officials in their agency. However, people who work with classified information may classify a new document that contains information already deemed classified. This is called "derivative classification."

2. Systematically downgrade classified information. Provide a mechanism by which older classified information automatically is downgraded to a lower level over time. Ideally, this eventually leads to the declassification of the oldest classified information, except in special cases.
3. Restrict or forbid reclassification. Occasionally a presidential administration will decide that previously unclassified or declassified data may indeed be sensitive after all; then a collection of formerly unclassified information suddenly sports classification labels. This may be forbidden by executive order, but it may be reversed by a subsequent order.

Most classified information in the United States becomes so through derivative classification. There aren't enough people granted direct classification authority by the president to create today's ever-growing mountain of classified information. Derivative classification often happens when someone creates a document based on an existing classified document. For example, Alice might be working for a defense contractor on a military cryptographic device. She needs to document how she solves an engineering problem, and the problem description is classified. Her document earns a derivative classification because it includes Alice's statement of the classified problem description.

Alice has solved a classified problem. Is the solution itself classified? If the solution description discloses nothing about the classified problem, then the solution might not be classified. Alice must consult the ***classification guide*** for her project. A government official who is personally authorized to classify information produces the guide for Alice's project. The guide lists different types of data the project might handle and specifies the classification of those types. For example, project design details, like Alice's problem solution, might be classified secret. Alice must therefore treat her solution as secret information. The classification guides themselves are often classified. Edward Snowden and others have leaked classification guides to the public.

17.2.1 Security Labeling

Anything containing classified information must carry a visible label indicating its classification level. This helps keep the materials safe by making them easy to spot by those responsible for their safety.

Classified devices or equipment likewise carry a label. The outside label indicates the most sensitive information contained therein. If a device contains a single item of Top Secret information, we label it Top Secret.

Classified documents always have standard, colored cover sheets that indicate their classification level. Document cover sheets and paper labels to apply to equipment or other items often use this color code:

- Top Secret—orange or gold
- Secret—red
- Confidential—blue

Document markings are quite elaborate. The DOD publishes a special manual explaining the details (DOD 5200.1-PH). Figure 17.2 shows an unclassified example of classified document markings.

The document's first page briefly explains who classified the document and how or when it will be declassified. This example was classified through derivative classification, and it identifies the document from which it derived its classification. The document's overall classification level appears at the top and bottom of the first page. If the document contains multiple pages, the overall level also appears at the top and bottom of the back page.

Every page of a classified document carries its classification level on its header and footer. The header and footer simply may repeat the overall classification level of the entire document. However, authors are encouraged to mark pages individually to reflect the highest classification level of information on that particular page. This makes it easier to lower a document's sensitivity by examining the headers to remove more-sensitive pages.

Classified documents also carry "portion markings." These are abbreviated classification levels prefixed to every paragraph. In Figure 17.2, the portion markings indicate that the first bullet is classified secret and its subbullet is unclassified. Portion markings are supposed to make redaction easier by distinguishing between more-classified and less-classified information, and by clearly indicating unclassified information.

SECRET

date

TO: USD(I)

FROM: DUSD(I&S)

SUBJECT: **(U)** Request for Data Concerning DoD Declassification Efforts

- **(S)** This is the portion marking for a classified primary bullet statement.
  - **(U)** This demonstrates that sub-bullets must also contain portion markings.
- **(C)** This is the portion marking for a classified primary bullet statement.

(U) RECOMMENDATION: Sign the Memorandum at right.

Signature Block

Classified By: **John Smith, DUSD(I&S)**
Derived From: **USD(I) Memorandum, dtd 20110205, same subject**
Declassify On: **20210205**

SECRET

Figure 17.2

Classified document markings—an unclassified example.

Sensitive but Unclassified

Governments have several mechanisms to restrict the flow of sensitive information. Laws to protect privacy and to protect health information, for example, establish federal restrictions on data distribution. However, this does not make private information classified information. The term "classified information" applies to specific categories of sensitive national security information. Not all sensitive data is classified.

When classification systems first evolved, they included the category "Restricted" or "For Official Use Only," abbreviated FOUO. Traditionally, this marking indicates information that should not be released to the public or to the press. The information is intended only for use within the issuing organization and should only be shared with others if there is a Need to Know.

However, FOUO information is *not* classified information. Recipients don't need a security clearance. Recipients only need a bona fide reason to receive the data. Individual organizations may establish their own rules for sharing and handling such information. Rules even may be contradictory between different organizations.

Contradictory rules and other regulatory obstacles cause the executive branch to periodically create a new and different general-purpose term for unclassified information that requires special handling. The term "Sensitive but Unclassified" was popular for many years. More recently, the phrase "Controlled Unclassified Information" has become popular.

Government rules also forbid the export of certain types of information. This usually applies to specialized technical data with obvious and immediate military application. Again, this information is not classified, even though the government restricts its distribution. Such documents usually carry a specific "Export Controlled" or "Export Restricted" marking.

Document authors sometimes format an unclassified document to look like a classified one. They place distribution restrictions in the header and footer, simulating a classification level. They even might include portion markings that abbreviate distribution restrictions, like FOUO, or "U.S. Only" to indicate an export restriction.

These stylistic tricks occasionally confuse people in the government and military community. When the press reports that a hacker retrieved "classified information" from a poorly secured website, the documents are usually restricted distribution documents formatted to look like classified documents. Sensitivity labels distinguish a classified document from others, but a claim of "leaked classified information" always attracts greater attention.

17.2.2 Security Clearances

A security clearance indicates that an individual is deemed trustworthy and may have access to classified information up to a particular classification level. We call these *hierarchical* levels because access to a higher level grants access to all lower levels. Figure 17.3 shows the arrangement graphically. The arrows indicate that information at a particular level may flow to people with appropriate clearances.

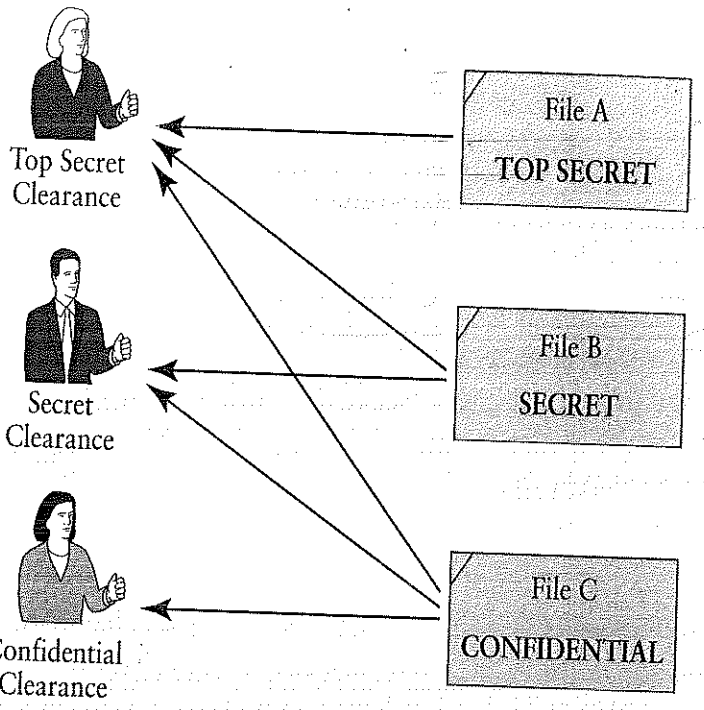


Figure 17.3

Access permissions for security clearances.

In Figure 17.3, Bob is in the middle with a Secret clearance. He may read Files B and C, because the Secret clearance allows him to read either Secret or Confidential documents. Tina at the bottom with a Confidential clearance can read only File C. Alice on top with a Top Secret clearance may read all three files. Despite clearances, though, any of them might be refused access to a document if they lack the Need to Know.

A government agency or military command issues someone a security clearance after investigating their background. The investigation begins with a detailed questionnaire that asks about the individual's previous addresses, jobs, education, legal problems, financial condition, family, and acquaintances. The investigation then evaluates the questionnaire and searches for any evidence that might call the individual's loyalty or trustworthiness into question.

Lower-level clearances require shorter and less-detailed investigations. Higher-level clearances require more detailed investigations. In the past, a private government contractor could perform its own investigation to issue an employee a Confidential clearance. Today, the government performs both Confidential and Secret investigations. Both involve a local and national check of law enforcement databases for criminal history and a credit check to assess financial stability. If a Secret clearance applicant needs access to a special program, then the investigation may be more thorough or include a personal interview.

All Top Secret clearances require a background investigation. A standard Top Secret investigation starts with a detailed questionnaire that reviews the applicant's personal history with a particular focus on the past 10 years. It also collects names of friends, neighbors, and family members who might be interviewed as part of the investigation.

An investigator interviews the applicant to discuss information on the application. Other investigators may interview friends, neighbors, and family. Like lower-level clearances, investigators also perform a criminal background and credit check.

For access to information beyond Top Secret, the investigation is even more thorough. The investigation may look more closely at relationships with foreign nationals for spying risks or at lifestyle details for blackmail or extortion risks. The investigation also may include a ***polygraph*** examination, also known as a lie detector test.

There are two general reasons to refuse a clearance. First, an applicant may have a history or personal traits that place trustworthiness in doubt. For example, applicants may be refused a clearance if they participate in illegal activities (drugs or black-hat hacking, for example) or have a serious criminal record. The second reason for refusal is if the applicant lies to investigators or tries to mislead them. Such dishonesty raises strong questions about an applicant's trustworthiness.

17.2.3 Classification Levels in Practice

We protect classified data according to its sensitivity using Defense in Depth. Lower classification levels require less protection than higher levels. Higher classification calls for additional layers of security and for stronger measures.

To protect Confidential documents, we lock them up in a filing cabinet with an approved locking mechanism. We may also store Secret or Top Secret documents in a similar filing cabinet, but we must provide additional and stronger protections around the cabinet itself. More sensitive information may require a periodic guard patrol, an intrusion alarm, or both. If we use stronger storage containers and perimeter defenses, we reduce the need for guards. Access control systems to protect Secret information have less-stringent requirements than those to protect Top Secret information.

Working with Classified Information

When it comes time to work with classified documents, we must use a work area that excludes unauthorized people. If we work in an office, we typically post a sign on the door saying "Restricted Area; Do Not Enter," and we close the door. No one may enter the office unless they have the appropriate clearance.

Ideally, we have a storage container in the office to store our classified documents and other materials. Otherwise, we may need to carry our classified documents past uncleared people. If so, we cover them to hide any classification markings. We want to avoid indicating that we are carrying classified information.

If we have classified material outside of a container, we are essentially shackled to that material. We may not leave it unattended in our restricted area unless there is another authorized person present who will take responsibility for it when we leave. Otherwise, we either bring the classified material with us or we lock it up.

There are very stringent restrictions on working with classified information on computers. The entire computer is classified at the level of the most sensitive information it contains. We can't connect a computer to any network, unless the network is cleared

to handle information at the same level as the computer. We examine these issues further in Section 17.6.

Higher Levels Have Greater Restrictions

At first it may seem that things are easiest if we are cleared for Top Secret and higher and if we arrange everything so that we can handle and store Top Secret and higher information. In theory, this would grant us access to whatever information we need and allow us to produce whatever documents we want. In practice, this arrangement is expensive and highly restricting.

When we accept responsibility for protecting sensitive information, we take on a burden. We must take active steps to protect the information and those steps restrict what we may do. Moreover, the burdens—both restrictions on data handling and on our own behavior—become much heavier as the classification level increases.

The office in which we work on Top Secret information may have thick and comfortably soundproof walls, but it doesn't have windows. The door to our office suite is a vault door with a combination lock. We can't use a desktop computer to routinely produce unclassified documents if we also use it to create classified documents. Internet access is impossible or severely restricted if the computer handles *any* classified information. Friends and family can't drop in at work unless they have the right security clearances. Otherwise, the guard turns them away at the building's front entrance.

Moreover, there are government agencies ultimately responsible for the classified information and they often take special steps to reduce the risks posed by hostile intelligence services. They monitor our activities as much as is practical, keeping an eye on our offices and our homes. Some agencies may tap our phones to check for unauthorized contacts or other suspicious activities. People cleared for certain programs are even forbidden to travel overseas.

17.2.4 Compartments and Other Special Controls

Besides the hierarchical classification levels, we assign additional classifications to special types of information. This is how we classify information above Top Secret. The markings may belong to special programs or to intelligence data associated with particular sources or data collection methods. Here are some types of additional classified controls:

- ***Sensitive Compartmented Information*** (SCI)
- ***Special Access Program*** (SAP)
- ***Special Intelligence*** (SI)

First, we will examine these different categories, then we will look at how we interpret combinations of such markings.

Sensitive Compartmented Information

The word ***compartment*** refers to a well-known security strategy in the intelligence community. We protect secrets by breaking them up into separate sets and placing each in a separate compartment. We grant different people access to different compartments.

If someone in a compartment turns out to be a spy, we only lose the information from the spy's compartment.

If we look at this in terms of earlier concepts and strategies, compartments combine Least Privilege with Separation of Duty. We divide the information into independent elements that people can work on separately (Separation of Duty). We restrict people, even highly trusted and cleared people, to as few compartments as possible (Least Privilege).

SCI Clearances

Access to SCI is the province of the U.S. intelligence community; it establishes the standards and issues the clearances. Top Secret access to SCI often requires an extensive investigation and a polygraph examination. The requirements may be lower for some compartments or for compartments restricted to Secret information.

Clearance procedures become more stringent if the person needs access to multiple compartments. Some intelligence operatives may need access to only a single compartment. Others, like intelligence analysts, may take information from one or more compartments and process it to yield information assigned to a different compartment. Such people face much more stringent investigation and clearance requirements.

For example, people with clearance to a single compartment might not require a polygraph examination. To gain access to an additional compartment, the investigation might call for a "counterintelligence" polygraph examination that focuses on questions about risks of spying. Broader access might require a "full-scope" polygraph examination that probes the person's lifestyle for risks of extortion as well as spy risks.

Example of SCI Processing

Here is a fictional example of how to process intelligence data through a series of compartments. We assume that Bob, Alice, Tina, and Clark all work for an unnamed intelligence agency, spying on the south of Freedonia to develop information about the grape harvest. They all have Top Secret clearances, but they work on different things. Kevin works in the department of agriculture and has a clearance and a Need to Know about the Freedonian grape harvest. Table 17.1 identifies the different workers and their clearances.

TABLE 17.1 Fictional example of intelligence agency compartments

Who	Classification Level	Compartments	Duties
Bob	Top Secret	ARGUS, SAUVE	Analyze satellite photos
Alice	Top Secret	BISHOP, KRUG	Analyze HUMINT
Tina	Top Secret	SAUVE, KRUG, MALBEC	Merge satellite and HUMINT data
Clark	Top Secret	MALBEC	Sanitize MALBEC data, add public info
Kevin	Secret	MALBEC	Forecast world grape crop

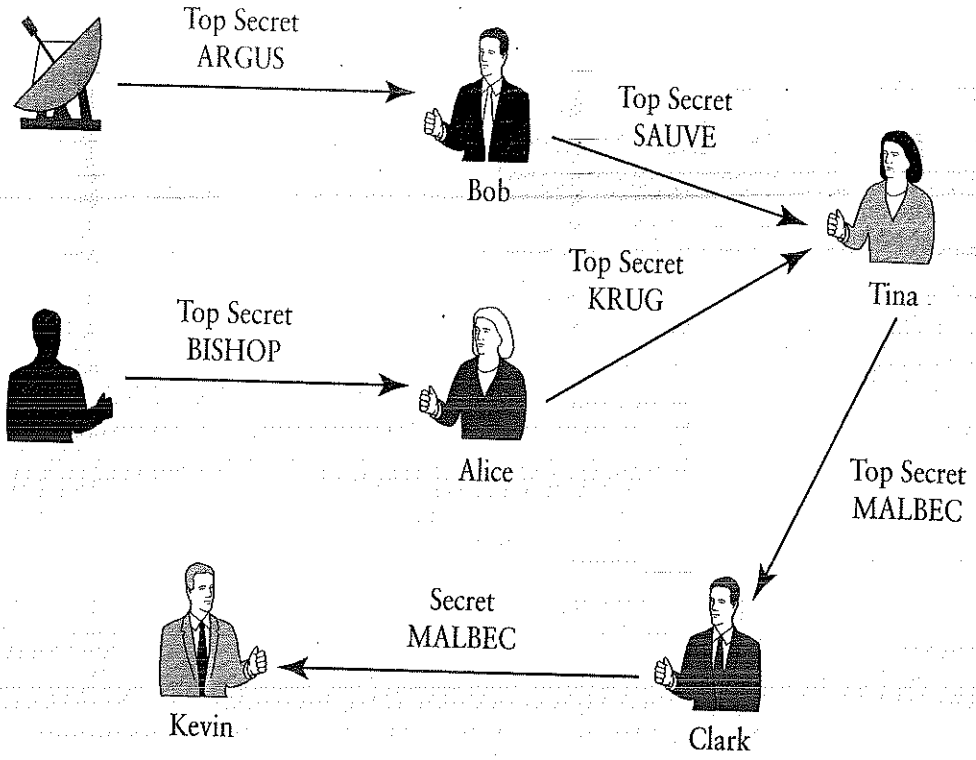


Figure 17.4

Using compartments to process data.

The agency assigns separate compartments to collect and process different types of intelligence data. As separate compartments process the data, they make it harder to identify the data's source. This allows the agency to release the data without disclosing exactly *how* they collected the data.

In this example, compartment names may have some relationship to the topic. In practice, the agency may choose the names totally at random, so that the name itself suggests nothing about the associated compartment. However, the compartment names *are* associated with information of particular types, so a spy could infer information by watching compartment names. Therefore, the agency usually classifies the compartment names themselves. Thus, we need the appropriate clearance before we even can look at a document's cover page to see to which compartment it belongs.

Figure 17.4 illustrates the flow of data between the different workers and their compartments. Bob and Alice both analyze raw intelligence data, but they work in different compartments. Bob takes raw satellite images of the south of Freedonia that belong in the ARGUS compartment. He analyzes and sanitizes the images to remove indications of the satellite image's real quality and to omit hints at how to hide information from the satellite, then he moves the result into the SAUVE compartment.

Alice takes intelligence from spies in the grape arbors (compartment BISHOP), analyzes it, and sanitizes it to hide the spies' identities, then she moves the result into the KRUG compartment. Tina takes the somewhat-sanitized data from SAUVE and KRUG,

further removes indications of its sources, and produces a combined result for the MALBEC compartment.

Clark is responsible for taking information classified Top Secret MALBEC and sanitizing it so he can hand it over to Kevin. He combines the MALBEC data with published information about the grape harvest. To reduce the information to Secret, he further disguises the actual information sources. Now he can release the data to Kevin, who has a Secret clearance, plus clearance to the MALBEC compartment.

No one on this project belongs to more than three compartments. Tina has the most access to information, but she doesn't have direct access to raw intelligence. Kevin needs to have a special clearance to look at intelligence data, but he only sees it after several layers of sanitization and abstraction. If he sells the information to his friend at the Freedonian embassy, the Freedonian can't quite identify the human agents or infer the quality of the satellite cameras.

Although this arrangement makes the secrets safer, it also makes sharing more difficult between different parts of the government. The intelligence agency wants to keep its assets safe, so it filters high-priority secrets through a sanitization process like this. Lower-priority information may never be analyzed and thus never be shared. Other government agencies, like Homeland Security, have public safety obligations that may be compromised if a potential terrorist threat goes undetected because information was not shared.

In any case, when Kevin gets caught for stealing secrets, he's in serious trouble. Moreover, if they used defense satellites to collect the grape harvest information, then the disclosure places defense intelligence assets at risk. Even though it is hard to prosecute a case of disclosing classified information in some cases, the law explicitly forbids disclosing intelligence data that supports national defense. The disclosure could make the defense satellites less effective, even after the layers of sanitization.

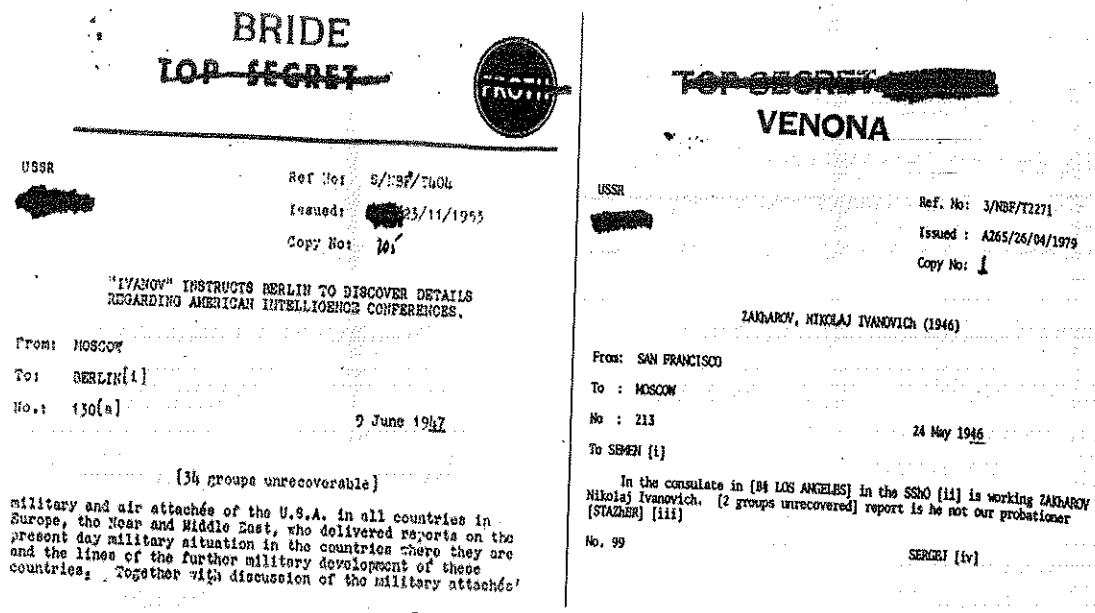
Special Access Programs

A special access program is one whose data is released only to individuals specifically cleared by the program's own security office. This includes people working directly on the program, either in the DOD or in the contractors who perform the work. The DOD establishes a SAP when the project relies heavily on secrecy for its success.

Stealth aircraft provide examples of special access programs. The DOD established separate SAPs to develop particular prototypes and for operational aircraft. Each aircraft has a variety of secret properties associated with how it evades detection. The SAP may grant access when individuals on related projects need access to project details.

Many SAPs, including early stealth aircraft, began as *black programs*. The DOD won't officially acknowledge the existence of a black program. When a black program becomes public, as in the unveiling of stealth aircraft in the late 1980s, the program remains a SAP, but the DOD acknowledges its existence.

When the DOD creates a SAP, especially for a black program, it often creates two different security identifiers for its information: a classified identifier called a ***code word***



BRIDE
TOP SECRET
FROTH

USSR
[redacted]
Ref No: S/NSF/T404
Issued: [redacted]23/11/1953
Copy No: 101

"IVANOV" INSTRUCTS BERLIN TO DISCOVER DETAILS REGARDING AMERICAN INTELLIGENCE CONFERENCES.

From: MOSCOW
To: BERLIN[i]
No.: 130[a]
9 June 1947

[34 groups unrecoverable]
military and air attachés of the U.S.A. in all countries in Europe, the Near and Middle East, who delivered reports on the present day military situation in the countries where they are and the lines of the further military development of these countries. Together with discussion of the military attachés'

TOP SECRET [redacted]
VENONA

USSR
[redacted]
Ref. No: 3/NSF/T2271
Issued : A265/26/04/1979
Copy No: 1

ZAKHAROV, NIKOLAJ IVANOVICh (1946)

From: SAN FRANCISCO
To : MOSCOW
No : 213
24 May 1946
To SIMEN [i]

In the consulate in [84 LOS ANGELES] in the SShO [ii] is working ZAKHAROV Nikolaj Ivanovich. [2 groups unrecovered] report is he not our probationer [STAZHER] [iii]

No. 99
SERGEJ [iv]

Courtesy of the US National Security Agency

Figure 17.5

Declassified intercepts from the NSA's VENONA project.

and an unclassified identifier. The classified code word is used within the project. The unclassified identifier usually is constructed from a pair of words, like HAVE BLUE, the name applied to a prototype of the F-117 stealth fighter. The unclassified identifier may be used to identify the project in published budgets or on documents released to people not cleared for code word materials.

Special Intelligence

Special Intelligence refers to information about communications security (COMSEC) or communications intelligence (COMINT). These clearances are the province of the NSA. Although they have requirements similar to SCI clearances, the NSA enforces its own, specific requirements.

As with SCI, the agency assigns code words to different types of intelligence or other sensitive information. This tradition dates back at least to World War II. Figure 17.5 shows two decoded messages intercepted from Soviet spy traffic in the 1940s.

Both intercepts originally were classified Top Secret. The left-hand intercept originally was assigned the code word FROTH and later assigned BRIDE. The right-hand intercept also was given two code words, one being VENONA. The other code word was blacked out before the intercept was declassified, suggesting that the other code word was still being used.

There could be several reasons for reassigning a document from one code word to another or for assigning it two separate code words. In the case of FROTH and BRIDE, the intercept apparently started out with the FROTH code word and was changed to BRIDE. In this case, the renaming may have been a response to the Kim Philby incident noted in Section 8.2. Perhaps the NSA replaced the FROTH keyword after Philby fell under suspicion in the 1950s.

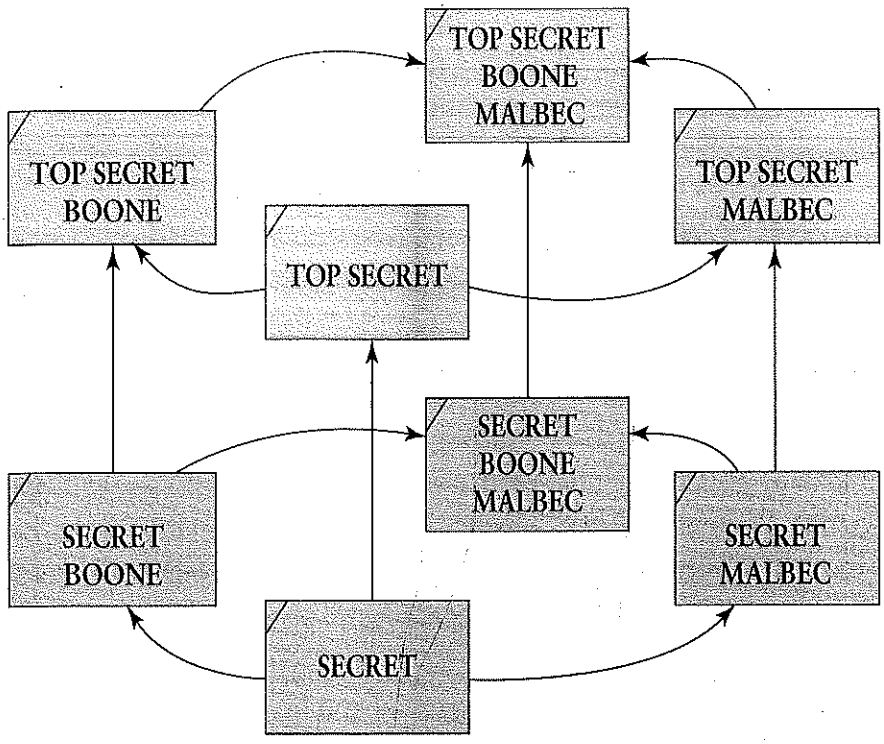


Figure 17.6

A lattice showing compartment clearances.

Enforcing Access to Levels and Compartments

A compartment, code word, or SAP identifier indicates that recipients must be cleared for a specific type of information to receive a document so marked. This works the same as other distribution restrictions: to receive the document we must fulfill all of its restrictions.

Figure 17.6 shows how this works. The diagram yields a structure called a *lattice* that shows how the different levels and compartments relate to one another. Computer-based systems that enforce access restrictions on classified information often use a lattice to implement the protections.

For example, Kevin's Secret clearance and his MALBEC clearance allow him to see Secret MALBEC data, but without a Top Secret clearance he can't look at Top Secret MALBEC data. If Kevin also is cleared for the BOONE compartment, then he can read Secret BOONE documents as well. Because he is cleared for both, he also can look at compilations of both that carry a Secret BOONE MALBEC label.

If we have the clearance to read a particular document in the figure, we also can read all documents that point to it and all documents pointing to those documents. For example, Kevin can read the Secret BOONE MALBEC document, so he can read all of the Secret documents in the diagram, even those without a compartment name. If we can read Top Secret documents, then we also can read Secret documents. However, if we don't have any compartment clearances, we can't read any compartmented documents, not even the Secret ones.

The same rules apply, regardless of whether we are talking about compartments, SI or SAP code words, or about other distribution restrictions. The hierarchical classification levels apply according to individual security clearances. To read a specific document, we must be authorized for *every* compartment, code word, or other restriction it carries.

17.3 National Policy Issues

In the United States, national policy for telecom and information systems is coordinated by the Committee for National Security Systems (CNSS). The committee traces its roots back to an executive order issued by the president in 1953. Until 2001, the committee was called the National Security Telecommunications and Information Systems Security Committee (NSTISSC). This committee also establishes federal standards for cybersecurity training.

To provide an overview of national policy issues, we organize them into the following areas:

- Legal elements
- Personnel roles and responsibilities
- Distinctive threats, vulnerabilities, and countermeasures
- Planning and management

We have covered many of these areas already and will cover others later in this chapter. The next few paragraphs summarize the first three areas listed. The next subsection reviews major facets of national security policy. The final subsections review national planning and management processes for security-critical information systems.

Legal Elements

We encountered legal elements earlier in this chapter with a brief review of the executive order concept and its role in establishing the system for classifying information. We reviewed other legal elements in earlier chapters, including cybersecurity legislation and standards in Section 4.6.2 and the overview of legal systems in Section 5.1. Federal agencies face additional requirements intended to reduce the risks of fraud, waste, and abuse by government employees. Although evidence collection and preservation often follow standards similar to private industry if a security incident leads to prosecution, there may be different requirements for applying military or administrative sanctions.

Moreover, the investigative process may vary from one agency to another. Some agencies have an inspector general with broad investigative powers. Others may incorporate investigations and audits into routine operations. In some cases, separate agencies like special prosecutors or the Government Accountability Office (GAO) may have the authority to investigate.

Federal Information Security Management Act

The third part ("Title III") of the 2002 E-Government Act is called the Federal Information Security Management Act (FISMA). The act requires executive branch

agencies, including the DOD, to take the following steps to ensure the security of information and systems:

- Plan for security
- Assign security responsibility to appropriate officials in the agency
- Review information system security controls periodically
- Explicitly authorize information systems to operate *before* they go into production and periodically reassess and reauthorize existing systems

FISMA follows a series of legislative acts that promote a risk-based approach to government cybersecurity. In other words, government cybersecurity must follow a continuous improvement process, like the one studied in this textbook.

NIST Standards and Guidance for FISMA

Since FISMA was passed, civilian, defense, and intelligence agencies have adopted policies to implement a standard, risk-based approach to information systems security. The approach is based on the six-step risk management framework (RMF) introduced in Chapter 1. NIST has documented the process in federal standards (FIPS documents) and recommendations (NIST-SP documents). These include:

- FIPS 199: Standards for categorizing the sensitivity of information systems in terms of loss of confidentiality, integrity, and availability.
- FIPS 200: Summary of minimum information system security requirements in terms of 17 general areas. Specifies SP 800-53 as the source of security controls to implement the requirements based on system sensitivity (as defined in FIPS 199).
- NIST SP 800-30: Risk assessment process for information systems, introduced in Section 1.5.2.
- NIST SP 800-37: Establishes the six-step RMF for information systems security.
- NIST SP 800-53: Provides a strategy for selecting security controls within the six-step framework described in SP 800-37.

Personnel Roles and Responsibilities

U.S. laws and regulations establish executive roles and responsibilities for government agencies and military commands. Agency managers establish specific policies and procedures to implement national requirements and standards. NIST SP 800-37 provides a framework for cybersecurity roles, responsibilities, and accountability.

In general, roles and responsibilities in federal agencies are similar to those described for private and commercial organizations in Section 13.2.3. In terms of cybersecurity planning and management, federal agencies follow more specific policies and procedures described in later subsections. An agency director or military commander must decide personally whether a system with critical security elements is secure enough to be deployed. This decision is based on a careful analysis of the system design and on extensive testing of its security properties.

Another significant difference between private enterprises and federal agencies is that the federal agencies often have more significant responsibilities for protecting secret information. We examined these in Section 17.1. In terms of personnel, agencies may require individuals to manage OPSEC, cybersecurity, and cryptographic resources, depending on the nature of their operations. Agency employees also may be personally accountable for agency information. This typically requires agencies to provide procedures and systems to associate employee actions with access or modification of important or sensitive federal data.

Distinctive Threats, Vulnerabilities, and Countermeasures

In general, government agencies face the same cybersecurity issues—and apply the same remedies—as other large enterprises and institutions. However, two major differences arise. First, legal elements make the agencies accountable in ways unfamiliar to private organizations. Second, federal agencies often have secrecy obligations far beyond those faced by private organizations or even by local and state governments. We must adjust our security objectives and requirements to include these concerns when we address security in the federal context. Secrecy concerns in particular may lead to particular types of security controls and countermeasures, including the following:

- Communications security, discussed in Section 17.4
- Data protection, discussed in Section 17.5
- Information assurance, discussed in Section 17.6

17.3.1 Facets of National System Security

To support system security in compliance with national standards, it is important to recognize certain essential areas of interest. These include physical security, communications security, cybersecurity, and security procedures. The following sections summarize facets that are particularly relevant to national system security. Appropriate security controls for these elements are enumerated in NIST SP 800-53.

Physical Security

Within physical security, the following topics require particular attention in national system security:

- Protection of areas. Physical areas are protected not only to prevent loss of equipment and information within those areas, but also to provide basic TEMPEST protection (Section 17.5.2).
- Protection of equipment. This involves both the physical protection of information against theft, but also to keep proper control of security-critical equipment to ensure its integrity (Section 17.4.2).

- Protection of magnetic media. Physical protection ensures the integrity of magnetic media; Section 17.5 discusses particular media handling issues for sensitive information.
- Backup of data and files. This provides multiple physical copies of critical information, both for copies in physically separate locations and copies for immediate local recovery.

Communications Security

Within communications security, the following topics require particular attention in national system security:

- Protection of data communications. These problems are addressed through physical security and through cryptosystems. We examine cryptosystems further in Section 17.4 and physical security in Section 17.5.
- Protection of voice communications. Although this originally focused on classic analog voice systems, modern voice systems often are hosted atop digital communications backbones. Nonetheless, there remain national standards for analog voice systems deployed within critical federal and defense sites. Moreover, the CNSS has published NSTISSP-101 as a national policy on protecting voice communication. CNSS also has published numerous standards that apply specifically to telephone systems.
- Application of crypto systems. This is addressed further in Section 17.4.
- Protection of keying material. National policies to protect keying material are managed and administered by the NSA. Section 17.4.1 discusses these in detail.
- Transmission security countermeasures. These are measures intended to hide significant patterns in transmission behavior so as to minimize the information disclosed by patterns of crypto-protected communications traffic. This is discussed further in Section 17.4.3.

Cybersecurity

Within cybersecurity, the following topics require particular attention in national system security:

- IT security. These are called *automated information systems* (AIS) in older policy documents.
- Protection of files. In most cases, government applications rely on the conventional measures studied in earlier chapters. In some cases, these are augmented by special measures to protect critical secrets from disclosure (Section 17.6).
- Protection against malicious logic. These are conventional security measures, though in some cases the systems avoid Internet connections, which may affect the nature of the threat. Different agencies and environments may publish specific guidance on antivirus measures and others to resist malicious logic.
- Protection of passwords. Agencies publish their own policies on password management.

Life-Cycle Procedures

National security systems must comply with specific policies for life-cycle procedures. The RMF in NIST SP 800-37 incorporates these into a security process adopted government-wide.

- Policies for acquisition, enterprise architecture, and risk management are discussed in the next section.
- Approval for operation. Critical defense systems must follow national policies outlining a specific approval process. These correspond to RMF steps 4 (assess) and 5 (authorize).
- Reporting security violations. Government agencies establish specific policies and procedures to monitor security activities and to address procedure violations. CNSS has published a recommendation on incident management, CNSS-048-07, a policy on information spills, CNSSP-18, and a list of frequently asked questions on incidents and spills, CNSS-079-07.

17.3.2 Security Planning

Security planning is implemented through life-cycle management, plus two additional concerns: budgeting and training. Security system budgeting poses a challenge, particularly in the federal arena. On the one hand, budgeting may follow a conventional cycle when developing or maintaining IT systems in a conventional manner. On the other hand, new threats and vulnerabilities may arise unexpectedly, and new countermeasures may impose unexpected expenses. These must be addressed in agency policies and procedures.

As noted earlier in the section, FISMA legislation is promoting a government-wide transition to standard processes for cybersecurity management. These are illustrated in NIST SP 800-37 and 800-53.

System Life-Cycle Management

System life-cycle management involves acquisition, architecture, approval to operate, and risk management. Here are specific CNSS policies that address these areas:

- Acquisition policy. The CNSS has published a policy on system acquisition, CNSS-11, that addresses issues in using commercial technologies for cybersecurity in applications that were restricted to government-specific technology under older regulations and standards.
- Enterprise architecture. The CNSS publishes a specific policy on enterprise architecture: CNSSP-21.
- Risk management. The CNSS publishes a specific policy on risk management, CNSSP-22, that implements NIST's RMF.

Government standards organizations also have published guidance for selecting and applying security controls. These documents present a process to identify security measures to apply according to the system's purpose and sensitivity:

- Recommended information system security controls: NIST SP 800-53.
- Federal standard for cybersecurity controls: FIPS-200.
- Controls for national security systems: CNSSI-1253.

The process of validating a system's security properties and approving it for operation are addressed through ***certification and accreditation*** or C&A. The certification process is addressed by RMF step 4. It analyzes the system design and tests the implementation to verify the operation of security controls. The accreditation is addressed by RMF step 5. It is a formal acceptance by agency management of the risks inherent in operating the system.

Security System Training

The NSA and the U.S. Department of Homeland Security have developed a program to recognize degree-granting colleges and universities that offer comprehensive training in cybersecurity. The program has established curriculum standards for two-year, four-year, and graduate level degree programs. This program replaced a series of CNSS and the National Security Telecommunications and Information Systems Security Instruction (NSTISSI) training standards, including NSTISSI 4011.

Institutions that offer degree programs in cybersecurity may submit their curricula for evaluation and certification. The applicant provides an overview of the curriculum and indicates how the different elements cover the requirements for training individuals in one or more of the listed roles.

CNSS also publishes a glossary of standard terms used in information assurance: CNSSI-4009.

17.4 Communications Security

The phrase ***communications security*** (COMSEC) refers to cryptography within the U.S. government and refers particularly to cryptosystems to protect critical government secrets. The CNSS has published the following policies on communications security and cryptography for national security systems:

- Safeguarding COMSEC materials: CNSSP-1
- Granting access to classified crypto information: CNSSP-3
- Wireless networking: CNSSP-17
- IPsec encryption: CNSSP-19
- Public key infrastructure: CNSSP-25
- Voice communications security: NSTISSP-101

The CNSS also has published the following instructions on communications security and cryptography:

- Public key infrastructure and X.509 certificates: CNSSI-1300
- Security doctrine for FORTEZZA crypto cards: CNSSI-3028
- COMSEC utility program: CNSSI-4007
- Voice-over IP guidelines: CNSSI-5000
- Voice-over IP telephone program: CNSSI-5001
- National COMSEC instruction: NACSI-6002

Although the rules have expanded recently to accept a broader range of civilian systems, the NSA retains authority to assess and approve cryptosystems that protect classified information. The NSA has developed a reputation for setting high standards for cryptographic safety. Some may argue that the standards are too high, but the standards arise from unfortunate experiences in the past.

In the 1950s, researchers determined that poorly designed crypto equipment often transmitted a faint signal that echoed its plaintext. Thus, when the device generated its ciphertext signal, a sensitive receiver could retrieve the plaintext. Cryptanalysis wasn't even necessary. The CIA found out that the Soviet military command in East Germany used such a device. Moreover, the Soviet signal cables ran in an underground tunnel near the Berlin Wall. The CIA promptly dug a secret tunnel under the wall and tapped into the cables.

This attack exploited vulnerabilities in crypto hardware. Today, we often refer to such exploits as ***side channel attacks***. To help prevent such problems with U.S. devices, the NSA insists on special design and analysis techniques.

A variant of this risk arises from "compromising emanations," a set of problems whose study remained highly classified for several years. Assigned the code word ***TEMPEST***, these problems allowed spies to listen to teletypes across the street from a locked communications room or watch the same image displayed on a television tube hundreds of feet away. The problems have proven extremely difficult to eliminate entirely, but many techniques minimize the risks. We examine this problem further in Section 17.5.2.

Although TEMPEST places the plaintext data at risk, we must recognize that the mere flow of traffic may disclose a great deal of information about classified activities. Even without decrypting message traffic, a careful analyst can detect patterns of data flowing between different recipients and associate the amounts and direction of flow with different types of activities. This is the ***transmission security***, or TRANSEC, problem. We discuss this later in this section.

Key Leakage through Spying

Another risk has arisen from leaked keying materials, particularly via spies. In 1976, federal agents arrested a highly cleared employee of a defense contractor for selling secrets to the Soviets. As described in Robert Lindsey's book *The Falcon and the Snowman* and the 1985 film, Christopher Boyce collected expired encryption keys used to protect Top Secret intelligence traffic. He then sold them to Soviet agents through a high school friend.

Both U.S. and Soviet security experts agree that the Walker spy ring, exposed in 1985, was a far more significant leak. Starting in 1967, John A. Walker, then a Navy warrant officer and communications specialist, started selling U.S. crypto materials to the Soviets. When a change of duty removed his access to crypto materials, he recruited others to collect the material for him. Ultimately his spy ring included his brother, his son, and a third naval officer.

Since then, the DOD claims to have spent billions of dollars replacing crypto equipment and revising key management procedures to help prevent a similar leak. Traditional crypto keys were used and then destroyed; a Walker or Boyce could simply pocket the key material and claim it was destroyed. Revised procedures require strict accountability and two-person control for Top Secret keying material.

The following subsections review technical and procedural strategies for ***high-assurance*** cryptography. The term *assurance* in cybersecurity reflects to refer to the degree of confidence we have in the system's operation. A high-assurance system meets the most stringent standards for protecting information in a critical application. High-assurance cryptography relies on two elements: high-quality equipment and an effective key-management process. We examine each of these in the following subsections.

17.4.1 Cryptographic Technology

The NSA and NIST share responsibility for establishing cryptographic standards to protect U.S. government traffic. The government typically places products and technologies in four categories:

1. Type 1—approved by the NSA for protecting classified and other highly sensitive national security information. The NSA takes responsibility for producing and distributing Type 1 keys. Most Type 1 algorithms are classified. AES is the only unclassified Type 1 algorithm.
2. Type 2—approved by the NSA for protecting unclassified but sensitive government information. The NSA produces and distributes keys for Type 2 applications. The NSA produced a Type 2 algorithm named SKIPJACK in the 1990s.
3. Type 3—commercial products using NIST-approved algorithms and evaluated under an approved process, like FIPS-140 (see Section 7.4.4). DES was a Type 3 algorithm until NIST decertified it.
4. Type 4—commercial products using other, possibly proprietary algorithms. These are not certified by NIST.

Traditionally, the NSA used their own, proprietary cryptographic algorithms and techniques in Type 1 systems. This provided a degree of Security Through Obscurity to protect the data, because the NSA routinely classified the algorithms it developed. This changed recently; newer systems may use AES to protect classified information.

Classic Type 1 Crypto Technology

In practice, Type 1 cryptography involves more than choosing the correct algorithm. The NSA requires Type 1 products to meet certain design constraints. To receive Type 1

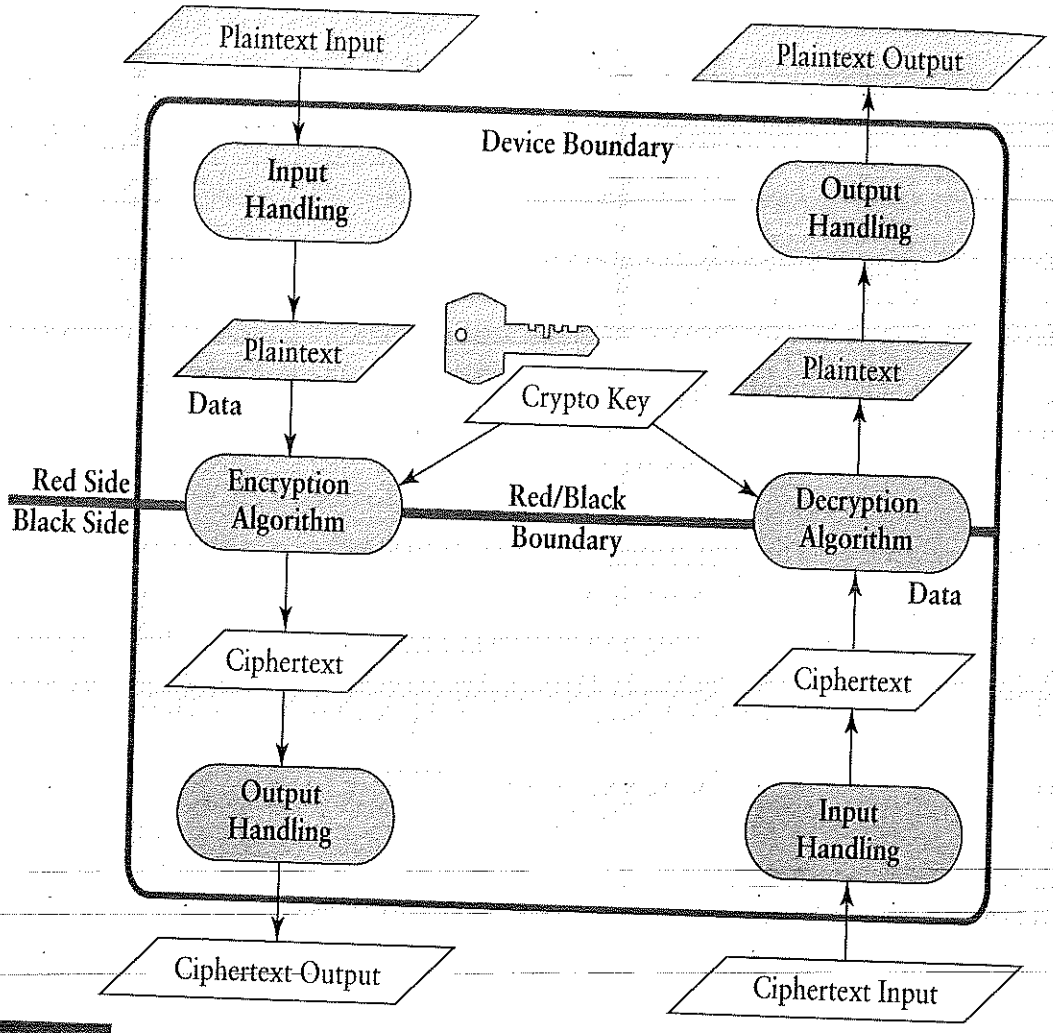


Figure 17.7

Red/black separation in a crypto device.

approval, a product also endures a rigorous analysis and review process to ensure correct operation.

Some Type 1 requirements ensure that the device always accurately displays its status to the operator, so the operator can tell if the crypto is disabled or not or has keys installed or not. Other requirements and analyses seek to minimize the risk of plaintext data leaking through poor design choices or through equipment failures.

A common feature of Type 1 products is ***red/black separation*** (Figure 17.7). The device's design draws a firm boundary between parts of the device that handle plaintext ("red") data and parts that handle ciphertext ("black") data.

The separation helps ensure that plaintext signals aren't transmitted along with the ciphertext. The device isolates the actual encryption and decryption from all other processing.

Type 1 devices also go through a ***security fault analysis***. This process searches for simple failures that might disable the encryption or allow plaintext to leak out with the ciphertext.

Example: Two military sites were communicating via teletypes using the Vernam cipher with one-time keys. This particular site had two teletypes: one for typing outbound messages and the other for printing inbound messages. One of the operators noticed that a perfect, plaintext copy of the outbound messages was being typed out on the inbound teletype. At first he assumed that another operator had rewired it to print an extra copy of outbound messages. In fact, a relay at the far station had failed, making it echo back the inbound message in plaintext on the return connection.

Fault analysis originated with mechanical and electromechanical crypto devices and evolved to address modern systems. While red/black separation tries to keep red and black data separate, the fault analysis ensures that a simple failure doesn't produce an unintended data path between red and black.

All Type 1 devices provide a simple and reliable way to ***zeroize*** the device. When we zeroize the device, we erase all of its working encryption keys. The design, analysis, and testing process ensures that the zeroize operation works reliably and that simple hardware failures won't interfere with it.

17.4.2 Crypto Security Procedures

The best crypto technology in the world is easily undermined if threat agents capture the keys used or subvert the crypto equipment. The NSA has established a set of policies and procedures to protect against such risks. These revolve around *COMSEC **materials***, a term that applies to both Type 1 crypto hardware and its keys.

If a site or organization needs Type 1 crypto protection, it manages the equipment and keys through a "COMSEC account." This account keeps track of each device and every key assigned to the organization. The organization assigns a specific person the job of *COMSEC **custodian***. This custodian has the following duties:

- Identify and keep an inventory of all COMSEC material.
- Provide access to COMSEC material for people who are authorized to access it.
- Ensure that COMSEC material is protected or that it is in the custody of people who may be trusted to protect it.
- Handle the destruction of COMSEC material and provide appropriate documentation of destruction.
- Report all COMSEC incidents to specifically identified authorities, both within the organization and at higher levels in the U.S. government.

In general, an organization handles COMSEC material the same way it handles comparably classified materials. Access is restricted to people specifically authorized to handle and use it. COMSEC materials are protected at all times or they are under the direct physical control of someone authorized to carry them. COMSEC materials never leave a secure site unless they are carefully wrapped and shipped via a highly trusted courier or service. These procedures apply both to equipment and to keys.

Two-Person Integrity

Top Secret keying materials require ***two-person integrity*** (TPI) controls. This is a form of Separation of Duty that requires two authorized people to take part in critical operations.

Photographed by Dr. Richard Smith at the Titan Missile Museum

Figure 17.8

Missile launch control is a no lone zone.

The Boyce and Walker incidents dramatically illustrated the risk of leaking Top Secret keying materials; TPI reduces those risks by having two separate people take part in all activities involving Top Secret crypto keys. In practice, sites assign people to teams to perform TPI operations. Each team member signs a log when they perform an action involving a Top Secret key.

The U.S. military also applies this concept to nuclear weapons. Traditionally called the "two-man rule," military doctrine does not allow anyone, regardless of clearance, to be alone with a nuclear weapon. Sites that contain or control nuclear weapons identify such an area as a ***no lone zone***. No one may enter a no lone zone alone; all workers enter such zones in pairs or in larger groups. Figure 17.8 shows a no lone zone warning sign from a Titan missile launch control center.

Controlled Cryptographic Items

A ***controlled cryptographic item*** (CCI) is a piece of COMSEC equipment tracked through a COMSEC account. We must ensure the safety and integrity of every CCI. This requires continuous physical protection during shipment and deployment. In most cases, we may install a CCI inside a cleared facility.

A CCI is not necessarily a classified device, especially when it contains no working crypto keys. Older devices are classified because they physically implement a classified encryption algorithm in discrete electronic circuits. If a hostile intelligence service steals one, its scientists might be able to reverse-engineer the algorithm.

Modern devices often implement crypto algorithms in software. We can design such devices to store algorithms in an encrypted form. If we don't load the appropriate decryption keys, an attacker can't recover the algorithms. When we prepare such a device for shipment, we remove the algorithm decryption keys.

Modern devices also have antitamper features. These include internal sensors and other checks to detect attempts to tamper with the device's internal circuits. The simplest antitamper mechanisms are physical seals attached to a device's covers. If attackers try to remove a cover, they break the seal, which indicates the tampering. Some devices also have antitamper sensors that may cause the device to zeroize itself.

The COMSEC custodian must inspect the CCI inventory periodically. The custodian must locate each device, check its antitamper indicators, and verify that it resides within an adequately protected location. The custodian must report any tampering with CCIs or any missing equipment.

Key Management Processes

Type 1 crypto keys may be distributed in either paper or electronic form. Older systems and procedures use paper keys. Newer systems use electronic keys as much as possible. The earliest form of electronic keying was over-the-air rekeying (OTAR). Several Type 1 devices incorporate OTAR, which wraps a new traffic key in a key-encrypting key using a device-specific protocol. More recently, electronic keys may be distributed on electronic storage media or distributed across networks using the Electronic Key Management System (EKMS).

The Walker spy ring flourished when crypto keys were produced and distributed exclusively on paper and entrusted to lone individuals. Digital keys were distributed on punched tape or punched cards. To load a key into a device, the operator connected a paper tape reader to the "key fill" connection and read the tape. A spy easily could copy crypto keys punched on paper by reproducing the pattern of holes in a photograph or photocopy or even by hand.

Since then, the NSA has developed policies and procedures to prevent a repetition of the Walker spy ring. The first major change was to require TPI for all Top Secret keys. The other major change is to minimize and even eliminate paper keys wherever possible. However, existing devices and procedures are hard to eliminate overnight. Paper-based key management will persist as long as end users still rely on older crypto technologies.

Data Transfer Device

As a first step to eliminate keys on paper, the NSA deployed the Data Transfer Device, or DTD. This device uses the same connection as a paper tape reader. Instead of using paper tape, the DTD stores keys internally and transmits them to individual devices by command. Unlike paper tape, the DTD keeps a record every time it transmits a key. This provides better records of a key's distribution and use.

Electronic Key Management System

The NSA established the EKMS to distribute and manage Type 1 crypto keys electronically. EKMS has a central facility at NSA that oversees the system and that establishes certain special-purpose keys used in other parts of the system. Every major site with a COMSEC account has a local management device (LMD) that communicates with the central facility to create and manage keys for local users. The LMD loads keys directly

into a transfer device as needed. From there, the COMSEC custodian or authorized clerk may load keys from the transfer device into individual COMSEC devices.

The LMD and the DTD handle these general kinds of keys:

- **Seed key**—a nonsecret key used to generate other keys using unpublished NSA algorithms.
- **Operational key**—a secret key used by a device for crypto operations. Seed keys must be converted into operational keys.
- **Black key**—a "benign" key or one wrapped by a KEK so that it may be handled with less risk of leaking.

Older Type 1 crypto equipment uses operational keys exclusively. In some cases, these devices may support key update or OTAR to periodically replace the working traffic keys. Otherwise, the operators must manually replace the operational key periodically. In some cases, the device stores an internal KEK, which supports the loading of a new operational key in black form. To use seed keys, a device must incorporate the crypto protocols necessary to convert a seed key into an operational key. The seed key and black key procedures reduce key distribution risks because operators don't need to protect those keys from disclosure.

17.4.3 Transmission Security

Transmission security, also called TRANSEC, arose as a communications security issue from two sources:

1. **Traffic analysis.** Even if we encrypt all traffic, attackers can learn a lot simply by observing communications patterns. They can identify military units and force structure by watching the message flow and infer the tempo of operations from the amount of traffic. This is a confidentiality problem.
2. ***Jamming.*** Attackers can seriously disrupt operations if they block messages from commanders or from surveillance systems that detect and report targets. This is an availability problem.

Some TRANSEC techniques are clearly extensions of the cryptography we already use. Others are extensions of ***electronic warfare*** (EW) techniques used in sophisticated weapons platforms. In all cases, the techniques help ensure confidentiality and availability. The most effective general-purpose technique is ***spread spectrum***, which also may appear in commercial communications systems and products.

Electronic Warfare

To understand the jamming problem, we must take a brief look at the EW environment. Modern defenses rely heavily on radar to detect incoming attacks. A typical modern radar system transmits a microwave radio signal. If the signal bounces off an object (like an airplane or ship), the radar antenna detects the reflected signal and uses it to locate the object in space. The Doppler effect also allows the radar to compute the object's relative motion.

Radars give us important information during military operations, but they also pose a risk. Anyone can easily detect the radar signals, because they are very strong. The signals also clearly point back at the radar's location.

EW begins with detection; we use specially designed receivers to detect transmissions from radar or communications equipment belonging to opposing forces. In either case, a good EW receiver will detect the transmission and the direction to its transmitter. If the transmitter is within missile range, an attacker can easily fire a missile that homes in on the transmitter. The EW receiver also may identify the types of equipment the opposition forces use. Different weapons incorporate particular electronic packages and the electronic signals often are distinctive.

Another part of EW tries to prevent detection of military units by screening them from radar or other sensors. This often involves active jamming or deception of the opponent's radar. In jamming, we transmit a signal that garbles the signal bounced back to the radar. Instead of seeing a clean radar signal that indicates the target's direction, distance, and speed, the opponent sees a noisy bar that indicates the general direction of the jammer itself. A more sophisticated jammer might actually adjust the radar signal so that it indicates a target that's not really there or hide the target entirely.

EW also may attack communications. If we identify frequencies being used by opposing forces, we can transmit noise on those frequencies. If the noise signal is powerful enough, it will drown out the opposition's communications traffic. This poses a serious problem to modern military forces. Most forces use surveillance aircraft to locate and identify targets. If we jam our attackers' communications, they can't direct their aircraft at military targets.

To counter an EW attack, we try to avoid jamming by masking our transmitters from the opposition. There are several techniques to achieve this:

- Low power transmissions. Keep the transmitted signals so low that opponents can't detect them and target them for jamming.
- Burst transmissions. Avoid two-way radio transmissions and rely instead on brief, highly compressed messages. Transmit each message in a very brief burst that is hard to detect and jam before the transmission ends.
- Directional transmissions. Use either directional radio transmissions or optical techniques, like a directed laser, to minimize the likelihood of interception, detection, and jamming. These often are restricted to line-of-sight transmissions.
- Spread spectrum transmissions. Disperse the transmission across a range of frequencies to make it harder to detect. We also may mix noise in with the transmission to make it harder to distinguish the communication traffic from random noise.

Different systems make use of these different techniques, particularly in military applications. Spread spectrum provides the most effective general-purpose protection for both confidentiality and availability.

Spread Spectrum

Although spread spectrum techniques evolved to resist jamming on the battlefield, they also resist civilian sources of radio interference. As the civilian radio spectrum has grown

more crowded, designers have used these techniques to make radio systems more reliable and efficient.

The earliest spread spectrum techniques relied on *frequency hopping*. The transmitter divided the message into separate pieces and transmitted each piece at a different frequency, hopping from one frequency to the next. Eavesdroppers might see a brief, burst-like transmission at a particular frequency, but they wouldn't know which frequency held the next part of the transmission. If we think of this in terms of transmitting data on a "carrier wave," we change the carrier wave's frequency each time we hop.

For example, the transmission might use the range of frequencies between 100 KHz and 200 KHz in 10 Hz increments. This provides 100 possible frequencies to use. The transmitter divides the message into 10 millisecond chunks and sends each one on a different frequency. In a trivial case, the transmitter sends the first chunk at 100 KHz, the second at 110 KHz, the third at 120 KHz, and so on.

In practice, the transmitter uses a pseudorandom sequence to choose the frequencies. The sender and receiver agree on the sequence; they exchange a nonce that selects the sequence to use. In commercial devices, we use the hopping to avoid noisy channels and other forms of interference. These are more-or-less random events, so we can rely on a pseudorandom generator that produces easy-to-compute patterns.

In military applications, the frequency hopping sequence may be controlled by a cryptographic device. The sender and recipient use a shared secret key and a transmitted nonce to produce the sequence. As with all Type 1 keys, management follows COMSEC procedures.

Navigational satellites, older wireless LANs, and some cell phone technologies use a different form of spread spectrum called "direct-sequence spread spectrum," or DSSS. Instead of hopping between frequencies, DSSS applies a function to the carrier wave that spreads the binary data across the signal. The function is a pseudorandom sequence of +1 and 21 signals called "chips" that occur at a higher rate than the underlying binary data rate. Thus, the transmitter uses several chips to encode each bit. The DSSS receiver applies the same pseudorandom sequence of chips to recover the binary data.

17.5 Data Protection

Data can't always be encrypted. Working data must be in plaintext. We need reasonably safe techniques to handle plaintext data and to prevent leakage. Here we review a few examples of special techniques to protect plaintext data:

- Digital storage media
- Protected wiring arrangements
- Unintended data emanations called TEMPEST

Media Handling

Storage media include portable or removable hard drives, flash drives, DVDs, and even older media like recordable tapes. If they contain sensitive or classified information, we must treat them like any classified paper or device:

- External marking. We mark all portable media with a visible label indicatingthe highest classification level of the data it contains. If the level itself contains classified code words or compartment names, then we must keep the media in a cover that protects the names from disclosure.
- Continuous protection. We keep portable media locked up except when we are using it. When not locked up, the media remains under our direct physical control or under the direct physical control of someone else with authorized access to the information.
- Secure transportation. The media never leaves our cleared facility unless we wrap it properly for shipment and transport it via an authorized courier service.

Earlier, we discussed the exposure and quarantine analogy for how classified information affects digital storage: When we "expose" a device to data at a higher classification level, the storage instantly is classified at that level. If the drive contains Confidential information and we store Secret information on it, we must now label it as a Secret drive. If the drive contains Top Secret BOONE data and we store Secret MALBEC data on it, we must now label it Top Secret BOONE MALBEC.

The DOD provides procedures and standards for downgrading or sanitizing media at lower classification levels, like Confidential or Secret. The procedures rely on overwriting, as described in Section 7.4.3.

Media Sanitization and Destruction

However, military and intelligence agencies don't always believe these measures are completely effective. Media containing Top Secret information can't always be sanitized. Some organizations may allow a device containing SCI or code word data to be sanitized and reused with different compartments or code words. However, organizations rarely allow sanitized media to be used in Secret or lower environments. They destroy the media instead.

Media destruction, however, can be a challenge. The NSA has established standards for destroying hard drives and other portable media. Use the following procedures with NSA-approved devices for erasure or destruction:

- Hard drives—either destroy the hard drive or disassemble it and apply a ***degausser*** (a strong electromagnet for erasing magnetic media) to every recording surface. The disassembly process renders the drive unusable in normal circumstances and the degausser removes the data.
- DVDs—physically destroy the readable surface or destroy the entire disk using an approved shredder, grinder, or incinerator.
- Diskettes and tapes—use an approved degausser to erase the media or disintegrate in an approved disintegrator.

Although earlier research suggested that flash drives could be easily and reliably sanitized, more recent studies indicate problems. Simple rewriting of flash drives may be adequate for the risks faced in most commercial applications. However, the ongoing recommendation for high-security applications requires that drives be destroyed if they contain highly sensitive information.

17.5.1 Protected Wiring

Informally, it may seem easy to transmit information safely. We connect a wire from Point A to Point B and we watch that wire very, very carefully. In practice, this can be very difficult, especially if we are sending highly classified data through less-protected areas.

For example, a shipboard sensor may need to transmit classified information to an analysis center elsewhere onboard. The natural solution is to run a cable from the sensor to the center. However, we must remember that the cable carries classified information. It probably will travel across parts of the ship where people aren't cleared for the information it carries. What if one of them taps the cable and extracts classified information?

We use a ***protected distribution system***, or PDS, to transmit plaintext classified information through an area of lesser classification or control. The PDS provides safeguards to prevent physical access or exploitation of electrical or electronic signals. In practice, a PDS primarily serves to slow down such an attack and to make it visible. National PDS guidance is established in NSTISSI-7003.

The simplest possible PDS consists of a single piece of pipe, conduit, or other uncut enclosure. The pipe carries the cables through the less-cleared area between the closed areas. We run the cables inside the pipe. The cables must reach the full length unbroken between the two closed areas. Any joints, breakout boxes, or other access points to the cables must appear only inside an area cleared for the information carried by the cables.

A simple PDS is appropriate to carry lower-level classified data through uncontrolled areas. They also may carry highly classified data through a controlled area intended for less-classified information. For example, two Top Secret areas may run a simple PDS through a closed area used by people cleared for Secret data.

A typical installation places the PDS in plain sight. This makes it easy to keep the PDS under observation and to inspect it for penetration attempts or possible tapping. Some environments install cameras to continuously monitor the PDS.

Higher-risk environments require a "hardened" PDS. Such installations typically use metal conduit or pipe to protect the cables. Some installations use airtight pipes with controlled air pressure to detect penetration attempts. A pressure sensor monitors the pipe continuously and sounds the alarm if the pressure changes.

In a hardened PDS, all connections or bends between components are completely sealed using welding, epoxy, or other permanent closure. Access covers and breakout boxes must be secured with government-approved combination padlocks. If this level of construction isn't practical, then the PDS must carry an alarm to detect tampering or it must be under continuous 24-hour surveillance.

The PDS provides *physical* protection of the cables and may provide some degree of electromagnetic protection as well. The PDS helps protect the inside cables against exterior eavesdropping. Problems may arise, however, if a PDS carries several cables, and the cables carry data at different classification levels. There are risks of "crosstalk" in which data on one cable may generate signals in a nearby cable. This may leak data from a higher-classified communications line to a lower-classified one. This is a type of TEMPEST problem.

17.5.2 TEMPEST

During World War II, teletype transmissions produced enormous amounts of electronic noise. In fact, researchers easily recovered plaintext messages across the street from a military crypto center in downtown New York City. A properly tuned radio receiver could detect the signals at fairly long distances.

This posed numerous practical problems for military and intelligence organizations. Secure rooms already were overloaded with equipment. It wasn't always affordable or even practical to move communication centers or to take other measures to reduce this "radiation leakage." The security measures often were judged too difficult to implement and skipped due to operational necessities.

Because the problems couldn't be solved quickly or easily, all issues associated with them were classified in the early years of the Cold War. The NSA assigned the problem the code word TEMPEST. Techniques to detect and exploit such signals progressed much faster than techniques to suppress them.

Victor Sheymov, a KGB security expert who defected from Russia in the 1980s, described an unusual set of empty tunnels, too narrow to fit a person, found in the Soviet Embassy in Beijing. Research eventually determined that the tunnels served as acoustical channels to allow different types of eavesdropping on embassy activities. However, the tunnels may have been for more than simply eavesdropping on conversations. When U.S. researchers found microphones in U.S. embassies, they feared the intent was to eavesdrop on *acoustic* signals from cipher machines or even from typewriters.

TEMPEST does not limit itself to studying electromagnetic signals. It studies all forms of compromising emanations because the signals may arise in many unexpected forms. Although many problems arise from unintended electromagnetic noise, we also face risks from acoustical signals and even from power line variations. These early problems yielded five countermeasures:

1. Shielding. Put shields around the equipment to block acoustical or electromagnetic signals. This was often a problem, because secured spaces tended to be overfilled with equipment already. Adding shields after the fact wasn't always practical.
2. Filtering. Put filters on the power lines and other outbound connections to ensure that sensitive data wasn't radiated through power fluctuations or other signals. In some cases, the filters intentionally limit radiated signals to specific frequency bands ("banding").
3. Masking. Structure the devices to emanate signals that don't distinguish between different data values. Early masking attempts operated several devices at once, in hopes that their combined output would mask individual signals. This rarely was effective. Typically, a device had to be redesigned to radiate a uniform signal.
4. Attenuation. Adjust the device so that it uses less power and radiates a weaker signal. In some cases, we must redesign the equipment to attenuate its emanations without reducing its effectiveness.

5. Zoning. Establish a controlled area between the vulnerable, emanating equipment and potential attackers. In theory, the zone should place threat agents outside the range for detecting exploitable emanations.

The specific requirements for TEMPEST protection vary significantly from one application to another. The rules vary between agencies and projects and according to the sensitivity and perceived risks faced by the site. In some cases, sites could not implement all TEMPEST protections because of impacts on day-to-day operations.

TEMPEST Zones

The earliest TEMPEST security strategy was to establish a ***zone of control*** around sensitive equipment and restrict access to that area. Following the trouble detected with teletypes in New York, the U.S. Army recommended a 100-foot (30 m) zone of control around communications centers. The zone radiated in all directions, horizontally and vertically. By the mid-1950s, the recommended control zone had doubled in size, though researchers continued to improve their interception capabilities.

A typical standard for TEMPEST zones, based on the document NSTISSAM TEMPEST/2-95, identifies three critical distances:

- Zone A: controlled area of 66 feet (20 m) or less
- Zone B: larger than Zone A and less than 328 feet (100 m)
- Zone C: larger than Zone B

Individual devices then may be evaluated for TEMPEST emanations and categorized into different levels. Zone requirements are derived according to equipment TEMPEST levels.

TEMPEST Red/Black

As TEMPEST concepts evolved, a key strategy reflects the red/black technique described in Section 17.4.1. In fact, the Soviet leakage problem that led to the Berlin Tunnel was a TEMPEST red/black problem. Red and black have subtly different meanings in terms of TEMPEST.

- **Red** refers to areas or elements that carry sensitive national security data.
- **Black** refers to areas or elements that do not carry sensitive national security data and that may safely connect or emanate signals to the outside world.

When we look at a secure area in the TEMPEST context, we almost treat it like an enormous crypto device. We keep red and black elements separate so that we can control red device emanations. Unlike crypto devices, however, we try to block all paths so that red data remains in the secure area.

When we run red and black cables in a TEMPEST environment, we need to avoid accidental connections or spillage between different classification levels. We avoid the obvious mistakes by labeling cable connections: We don't want to plug the Top Secret cable into the Secret jack.

TEMPEST Separation

A less-obvious risk arises from "coupling," an electromagnetic phenomenon in which the energy produced by a signal on one wire produces a detectable signal in an adjacent wire. This leads to "crosstalk" in which the signal from one wire is apparent in the other. In typical cases, the problem is an annoyance—crosstalk introduces noise into an otherwise clean signal—but in TEMPEST, it may allow data leakage. We avoid coupling by providing sufficient TEMPEST separation between cables.

One published guideline for protecting highly sensitive data gave the following recommendations for TEMPEST separation between red and black components:

- 2 inches between shielded components, including shielded cables and TEMPEST-approved equipment
- 6 inches between unshielded cables and shielded components, except crypto equipment
- 3 feet between crypto equipment and unshielded cables
- 3 feet between equipment without TEMPEST approval and unshielded cables

Power wiring and supplies also pose a challenge. Power arrives from the public power grid, which powers black circuits. Power circuits feeding the red equipment must be filtered. Moreover, black power lines should not run near red cables or equipment. Following the recommendations just listed, black power lines should be at least 2 inches from shielded components, and at least 6 inches from other components.

Grounding problems also may cause TEMPEST emanations. Electrically, we typically measure voltage as a difference between a given point in the circuit and the proverbial "ground." People working with high-quality audio equipment sometimes may hear noise or distortion if separate components don't really share a common ground. We typically eliminate such problems by wiring the components to a common ground.

Grounding problems in a secure installation can produce undesirable currents, which in turn, may emanate sensitive data. However, we can't solve the problem by simply wiring all the grounds together. We must keep red and black grounds separate, just like we kept the power lines separate. Moreover, TEMPEST rules may call for special filters or other hardware when connecting the red ground to the common (black) ground.

17.6 Trustworthy Systems

Computers are not trustworthy, just as cities are not safe. We might trust parts of them, but riskiness in one part can yield riskiness in others. We build trustworthy environments from the ground up. We start with a safe interior and a reliable boundary. We validate trustworthy members individually before bringing them in.

The U.S. government tried to incorporate such ideas in computer systems when they developed the *Orange Book* standards in the early 1980s. The *Orange Book*'s title began with the phrase "Trusted Computer Systems." The goal was to promote the development of trustworthy systems.

The *Orange Book* defined three general levels of trusted systems, going from least trusted to most trusted:

- C—Provides "discretionary protection" in that file and resource owners may decide individually what to protect and how to share the things they own.
- B—Provides "mandatory protection" in that the system enforces access rights based on security classifications and clearances, regardless of personal access control settings.
- A—Provides "verified protection" in that the mechanisms have been formally verified to correctly enforce the mandatory protection policy.

The *Orange Book* provided a widely accepted notion of what it meant to have a "secure computer." In practice, the notion wasn't useful in most environments. The *Orange Book* focused on mechanisms to protect classified information, a policy problem shared by very few commercial organizations.

Reference Monitor

Although the *Orange Book* focused on solving a specific problem—protecting classified information—it also promoted a sound foundation for trustworthy computing. This foundation is the ***reference monitor***, a mechanism that *always* enforces its security policy. A reference monitor has the following features:

- Nonbypassable. The reference monitor makes all access control decisions. There is no way to reach a resource, except through the reference monitor.
- Tamperproof. There is no way for attackers or other system users to damage or disable the reference monitor.
- Verified. The reference monitor must be small enough so that we may analyze and test it thoroughly in order to assure that it operates correctly.

When we incorporate the reference monitor into a computing system, we can build a system that reliably enforces its security policy. We call such a system a ***trusted computing base*** or TCB. The TCB provides an effective building block for enforcing confidentiality and integrity policies. These mechanisms do not, however, provide a simple and obvious way of ensuring availability.

High Assurance

A high-assurance system is one whose behavior is verified to comply with its policy. To truly verify the TCB's behavior, we must construct a *formal security policy*; that is, a policy expressed in an unambiguous symbolic form. We also construct a *formal design*

specification in the same form. Then, we construct a mathematical proof to show that the design specification enforces the policy.

In practice, the formal design specification describes the system's API. The description reflects the behavior of its inputs, outputs, and internal states when it processes different requests. The policy provides a formal definition of "secure" versus "insecure" system states. We verify the system successfully if the proofs show that the system always remains in a secure state or never enters an insecure state.

This process helps locate flaws at different steps in the software development process. The very act of formalizing the policy and design often uncover misunderstandings on how the system should operate and ambiguities in behavior. Formal methods detect additional flaws while developing the formal proofs. More flaws emerge as developers confirm that the formal specification matches the implemented code. As developers detect and patch flaws, they incorporate the changes into both the code and the formal specifications. This process may detect flaws in the patches themselves.

Trusted Systems Today

In this context, a "trustworthy" system is one that always remains in one secure state or another or a system that never enters an insecure state. In practice, very few real-world systems use TCBs. For many years, this was because the standards for TCBs were skewed in favor of systems to share classified information in a controlled manner. More recently, vendors have produced systems that focus on high-integrity operation, though the market still remains small. High-assurance processes also are expensive. In one case, the formal assurance efforts *doubled* a TCB's development cost.

Assurance must always focus on behaviors described in the formal policy. If the policy doesn't ensure reliability, then the formal methods won't verify system reliability. In the TCB just noted, formal assurance accounted for only 19 percent of the flaws detected in the deployed system. Most of those flaws involved security-critical mechanisms to protect classified information and such assurance may be justified in some environments.

Because of the expense and complexity, few modern systems achieve such high levels of assurance. Today, the term "trusted systems" is applied to systems that meet certain analysis and testing requirements defined in terms of the Common Criteria. Many organizations consider systems trustworthy out of necessity; too often critical systems rely on Microsoft Windows and other large commercial operating systems simply because it's affordable. It is relatively expensive and time-consuming to develop a software product using a high-assurance platform.

Modern high-assurance computing systems comply with special Common Criteria Protection Profiles and with other trusted computing standards. For example, some vendors offer products that comply with DO-178B, the accepted standard for high-assurance software in the aircraft industry. Modern high-assurance systems often produce a ***separation kernel***—a system that divides processing resources among several isolated subsystems that may only communicate with one another through explicitly established communications links.

National Standards

The CNSS has published several standards to establish information assurance requirements for national defense systems:

- Policy for space systems: CNSSP-12, which is mapped to DOD Directive 8581.1
- Policy to provide products to nongovernment users: CNSSP-14
- Policy on assured information sharing: CNSSP-24
- Policy on controlled access protection: NSTISSP-200
- Instruction on reserve equipment: CNSSI-4008

17.6.1 Integrity of Operations

Most computing operations must achieve a certain level of integrity to provide a measure of reliability. As operations become more critical, so do the requirements for high integrity. In a few cases, we seek to achieve the highest possible assurance that operations take place as planned with no accidents or surprises. Nuclear weapons provide the most compelling example; we tolerate as few errors as possible when managing, operating, or moving them. Although a great deal of secrecy surrounds nuclear operations, the motivation is to ensure the correct operation of U.S. nuclear forces.

According to U.S. defense policy, nuclear weapons are supposed to deter attacks by enemy forces by threatening nuclear retaliation. However, the mere existence of nuclear weapons poses an enormous threat: If only one weapon explodes by accident, it could devastate several square miles of land and spread toxic radioactivity over a vast area. To properly control nuclear weapons, we must prevent mistakes or abuse while ensuring that a valid launch order is always carried out.

The risks posed by nuclear weapons are so acute that all activities surrounding them must follow special procedures that include redundant checking. Every operation is checked and verified. Any errors or shortfalls in the procedures may have serious consequences, even if no nuclear-related losses or injuries occur.

Example: In 2007, the U.S. Air Force disciplined 70 airmen for accidentally carrying nuclear-tipped cruise missiles on a B-52 bomber. From one standpoint, the incident was minor: No weapons were launched or detonated and the weapons were always in the custody of appropriate U.S. military forces. On the other hand, the incident took place because several nuclear management procedures were either ignored or botched. One observer speculated that the weapons were essentially missing without being missed for at least 10 hours. If the weapons had left U.S. custody, 10 hours would have allowed thieves to thoroughly cover their trail.

There are two parts to the U.S. military policy for controlling nuclear weapons:

1. Positive control. The weapons shall always be deployed when a legitimate order is given.
2. Force surety (or "negative control"). The weapons shall never be deployed without a legitimate order.

Both parts of the policy pose significant challenges, because both make global statements ("always" and "never"). U.S. nuclear command and control implements these policies

through a large collection of interacting procedures. The steps in different procedures require separate personnel to cooperate to implement the policies. This is a sophisticated example of Defense in Depth. The multiple procedures also help verify the work of other personnel. The procedures construct a "cocoon" of protection around the weapons, so that if one procedure fails, others detect and help cover any protective gaps.

Although the 2007 incident reflected failures in several procedures, no one was hurt and no weapons detonated. Moreover, a vigorous response to incidents like the one in 2007 may serve as a warning to commanders who cut corners on nuclear operations.

Nuclear Operations

During the 1960s, the United States and Soviet Union developed nuclear forces to counter the perceived threat posed by each against the other. Both argued that the forces were meant to deter the other from attacking. For both, the worst-case attack was for the opponent to launch a surprise attack that destroyed the other's nuclear missile force. This set the stage for a second attack that devastated what was left of the victim's country.

To prevent such an attack, both forces developed early warning mechanisms to detect incoming bombers or missiles. They also developed mechanisms to ensure a counterattack despite imminent devastation. Part of the counterattack relied on missiles kept on hair-trigger alert. As soon as the incoming attack was detected, the targeted country would launch its nuclear missiles at the attacker. The entire process, from detecting the incoming attack to the launch of counterattacking missiles, was designed to take place in a matter of minutes.

Positive Control

National military commanders in the United States issue an Emergency Action Message, or EAM, when they need to give time-critical orders or other guidance to commanders and combat units. Commanders issue an EAM to order the launch of nuclear weapons or to initiate a drill to exercise the readiness of U.S. nuclear forces.

Formal authority to launch nuclear weapons rests with the president. However, military forces must retain the ability to launch a counterattack if a surprise attack kills the president or places the president out of touch with military forces. Thus, there are several underground and airborne command posts that also are authorized to issue an EAM.

A valid EAM uses a special set of authentication codes. These codes are changed regularly to reduce the risk of forged orders. When an EAM reaches a weapons platform like a missile launch control center or a nuclear submarine, two people must independently authenticate it. Then those two work together, and possibly with others, to implement the attack order. Teamwork serves both to ensure that launches are based on authenticated orders and that the order is carried out as stated.

Force Surety

To prevent the improper use of nuclear weapons, U.S. forces must deal with several risks:

- A nuclear war occurs because of an accidental or unauthorized missile launch.
- An adversary manages to steal a nuclear weapon.
- A nuclear weapon detonates unexpectedly.

Force surety relies heavily on two-person integrity controls. All locations that house nuclear weapons or elements of the nuclear command and control system are no lone zones (Figure 17.8). Military units that handle or use nuclear weapons deploy additional guards and other protective measures. The actual launch of a nuclear weapon requires coordinated action by at least two separate people.

For example, it requires a two-person crew to launch Minuteman nuclear missiles. The equipment will not allow the launch if either is absent. Each crew member authenticates the EAM independently, then the crew members strap themselves into their respective chairs in front of their control panels: The panels won't start the launch procedure until then. The panels are placed far enough apart and the steps in the launch procedure are so time-critical that one crew member can't perform the procedure on both panels.

Nuclear weapons also contain special design features to prevent accidental or unauthorized detonation. Weapons follow a two-step process when detonating:

1. Arm the weapon.
2. Detonate the weapon.

An unarmed weapon can't possibly detonate. At most, high explosives inside the weapon might detonate, but this causes orders of magnitude less damage. Missile-based weapons include sensors to track its trajectory. The weapon won't arm itself unless it reaches a planned altitude on its flight path and starts to descend toward its target. This prevents a disaster if the rocket motor fails shortly after launch. If the missile fails to reach the right altitude, it won't arm itself before it crashes. If it crashes on friendly soil, it won't detonate.

The arming procedure on nuclear weapons relies on a secret code. Some weapons use the code to encrypt their timing logic; without the code, the weapon won't perform the precise timing steps needed to produce a nuclear explosion. Without the code, the device can't detonate. This makes accidents with unarmed weapons somewhat less catastrophic and prevents stolen weapons from being detonated by adversaries.

Achieving Nuclear High Assurance

Nuclear weapons pose a particularly difficult assurance problem. We can experiment with parts of the system, but we can't test everything. The U.S. military relies heavily on component testing, crew training, and periodic drills to validate the nuclear command system. Component testing and simulations help ensure the quality of the weapons themselves.

Physical protection follows examples shown earlier for handling critical documents: Keep under continuous control, keep strict accounts, perform regular inventories, and so on. We achieve higher assurance by implementing these procedures redundantly, so that there are multiple accounts, multiple guards, and multiple inventories.

Nuclear assurance is extremely expensive. The day-to-day operating procedures for the nuclear forces primarily pay for keeping the forces alert and ready to respond to an attack. Extra guards protect the weapons and control centers. Extra personnel perform nuclear-related paperwork. Nuclear assurance dramatically increases staff and administrative costs.

Moreover, critical nuclear information is properly classified Top Secret. This includes lower-level details of EAM transmission and validation of weapon system operation and of the nuclear bombs themselves. It is costly to create and distribute up-to-date codes (classified Top Secret) for authenticating an EAM and for arming weapons. Like all nuclear costs, lower assurance is not an acceptable option.

17.6.2 Multilevel Security

Computer-sharing techniques like multitasking and timesharing arose in the 1950s and 1960s in response to extremely high computing costs. Most military and government agencies couldn't afford to dedicate individual computers to specific classified programs. They needed a way to share computers without leaking information between programs or between classification levels.

It is difficult to share classified information on a computer because it is hard to prevent leakage. Transitive Trust produces the most significant leakage threat; people with a higher clearance must not leak information to those who have a lower clearance. The basic problem is the Trojan horse, which we examined in Section 4.5.

The term ***multilevel security*** (MLS) refers both to the sharing problem and to a particular mechanism to implement that type of sharing. The sharing problem involves two parts:

1. Grant access to a file if its classification level is equal to or less than the clearance assigned to the user.
2. Never allow access to information whose classification level is greater than a user's clearance.

Systems typically implement multilevel security by using the "Bell-LaPadula model." To implement this, we establish security labels that we assign to all processes, users, files, and other resources. The security label reflects the classification level of information. When applied to a user or process, the label reflects a security clearance the user holds. If a user holds a Top Secret clearance, then the user also holds all clearances below that. To implement multilevel security, the Bell-LaPadula model enforces two properties:

1. The Simple Security Property. A process may read from resources whose security label is at or below the process' own security label.
2. The * Property. A process may write to resources whose security label matches or exceeds its own. When speaking, we call this "the star property."

These rules are *always* enforced. For this reason, the multilevel security mechanism often is called ***mandatory access control*** (MAC). There are other mandatory access control mechanisms, but multilevel security is the most common. Here are examples of mandatory access control with multilevel security:

- If a system administrator has access to administrative mechanisms on a system, but only has a Secret clearance, the Simple Security Property will block all attempts to retrieve Top Secret files. (In practice, it's rarely practical to administer a system without having access and Need to Know for all data stored on the system.)

- If Bob is working with Top Secret information, for example, the * property prevents his processes from writing Top Secret information to Secret files. The * property is intended to block Trojan horse attacks. A Trojan horse might write the data to a different Top Secret file, but that prevents the information from leaking to someone without the proper clearance.

In a sense, multilevel security behaves like volume encryption; we protect everything whether we need to or not. Everything on the system carries a security label and has its accesses checked, even globally shared "unclassified" resources like application program files.

Rule- and Identity-Based Access Control

Multilevel security and similar mechanisms sometimes are called "rule-based access control," because they are based on a fixed set of rules that the system enforces continuously. Although mandatory access control is the traditional term and remains widely used, some sources use the other term. To some extent, multilevel security mechanisms are intended to enforce access restrictions on behalf of third parties; the authorities who classified the information.

The two Bell-LaPadula rules are not sufficient by themselves to protect classified information. Access to classified information also is restricted by Need to Know. Most systems rely on conventional file-based access controls, like those in Chapters 3 and 4, to enforce Need to Know. Such rules are often called identity-based access control because they are based on user identities and controlled by the identified owners of files. The *Orange Book* called such rules "discretionary access control" because restrictions are applied at the discretion of those who had access to the files. Today, standards for such controls often refer to them as *controlled access protection.*

Covert Channels

Multilevel security works effectively only if all data paths between processes are controlled by the system security mechanisms. In fact, most systems provide many unplanned and unexpected ways to communicate between two processes. For example, if the system lets processes take exclusive control of a file, then one process can send a series of signals to the other by holding and releasing particular files. Processes may also communicate by producing delays in other shared resources, like the hard drive or available RAM.

These mechanisms create ***covert channels*** between processes. The channels aren't restricted by the Bell-LaPadula rules. Successful multilevel security enforcement relies on being able to restrict how processes communicate with each other. Researcher Butler Lampson called this "the confinement problem."

As secure system design evolved in the 1970s and 1980s, researchers developed techniques to locate, assess, and block covert channels. The basic strategy was to eliminate as many shared resources as possible. Designers assessed the remaining shared resources and tried to block or at least restrict any covert channels that arose.

Covert channels provided an additional reason to apply formal methods to system design. A well-designed formal specification helped locate and identify shared resources.

Certain types of formal analysis would locate covert channels because they violated the security policy. Unfortunately, no technique could identify all possible covert channels. Experts dispute whether a practical system could eliminate all covert channels.

Other Multilevel Security Problems

Covert channels were not the only persistent problem with multilevel systems. When the government began promoting multilevel systems using the *Orange Book*, it was easy for many people to argue that the highest-rated "A1" systems were secure by definition because they had to meet stringent requirements, including formal security proofs. In fact, *all* multilevel secure systems suffered from two security problems:

1. The virus problem. The Bell-LaPadula rules do not—and cannot—prevent a virus present at a lower classification level from propagating to higher classification levels.
2. The redaction problem. Users routinely rely on large and unreliable application programs to edit classified documents and to create less-classified versions of such documents by removing the more-sensitive data. Unfortunately, the programs were rarely—if ever—analyzed to verify correct behavior. This may lead to unfortunate surprises like the one described in Section 17.1.1.

The redaction problem is very challenging, especially when faced with general purpose, free-format information. There are a handful of automated techniques that can reliably sanitize information of specific types and formats.

17.6.3 Computer Modes of Operation

When we deploy a computer system to process classified information, it is accredited to operate in a particular "mode." The different modes reflect the different types of classified information that might be present on the system and the clearances of potential users. There are four recognized modes. Each represents either tighter security requirements on the data and user community, or tighter requirements on the host computing system.

1. Dedicated
2. System High
3. Compartmented or Partitioned
4. Multilevel

We describe each mode here.

Dedicated Mode

This mode places the fewest requirements on the computer itself, but places the most restrictions on the data being processed and on the user community. A dedicated computer operates on data at or below one classification level. Everyone with access to that computer must be cleared for the data it handles, and must have a Need to Know for all data it handles.

Almost any computer may be used in dedicated mode. All security relies on physical protection. The operating system and hardware do not need to provide authentication, access control, or other security measures.

A computer in dedicated mode may process data at different classification levels for different groups of users, as long as it happens at different times. This is called "periods processing." For example, Secret Project X can use the dedicated mode computer in the mornings, and Top Secret Project Y uses it in the afternoons. The computer must support a procedure that completely erases its storage between periods if it is used for periods processing.

System-High Mode

In this mode, the system may process data at multiple classification levels. The entire user community must be cleared for the highest level present on the system, but they do not all require a Need to Know. The system must enforce Need-to-Know controls between users.

Computers used in system-high mode must be evaluated to ensure that they can in fact enforce Need-to-Know restrictions between users. The system must be able to enforce controlled access protection (also called "discretionary" or "identity-based" access control). Most of the better-known commercial operating systems are approved for system-high mode. In general, such systems must undergo a Common Criteria evaluation that assesses the system against the "Controlled Access Protection Profile."

System-high mode is the most common mode used with both computers and computer networks that process classified information. A system-high network must be entirely protected in accordance with the requirements for its classification level. However, because we isolate the network from less-cleared users and networks, we can build the network from commercial products.

The proliferation of system-high networks has led to a new problem: the challenge of ***cross-domain sharing***. People working on a network at a higher classification level often produce material for people working at a lower classification level. Separate classification levels represent different domains. This arrangement also is called ***multiple single levels*** or MSL (in contrast to MLS). Although it may be a challenge to share properly sanitized information without accidentally spilling more-sensitive information, there are reliable and effective ways to sanitize and share certain types of information.

Compartmented or Partitioned Mode

In this mode, everyone who uses the system is cleared for Top Secret and for access to special program or intelligence data. However, the system contains data belonging to different SCI compartments or possessing different intelligence or special program code words. Not all users have formal access permission to all compartments or code words.

This is similar to the multilevel security problem in that users are not cleared to see information marked with particular compartments or code words. Because all users have been cleared for data above Top Secret, the risk of spillage is somewhat less than that we face if a Secret user receives Top Secret information.

The system requires multilevel security protections, but does not require the same degree of assurance. To address this, the intelligence community developed the Compart-

mented Mode Workstation (CMW). A CMW's underlying operating system enforces multilevel data flow between partitions, but does not necessarily concern itself with blocking covert channels. Because a covert channel won't spill data unless someone intentionally implements a program to exploit one, the risk should be minimal in the CMW environment.

Multilevel Mode

In this mode, the system may serve users with different security clearances and may store data which some users aren't cleared to receive. The system must implement a reliable and effective multilevel security mechanism. Today, multilevel servers often appear in two particular applications:

1. Multilevel servers—server systems that provide information to clients operating at different classification levels.
2. Guards—high-assurance firewalls that pass information between different security domains and MSL environments.

These applications easily provide data sharing in the low-to-high direction; users with lesser clearances can easily provide information to users with higher clearances. However, modern military operations require an effective flow of information in the opposite direction: high to low.

For example, a combat team is directed to attack a target; their orders may be classified Confidential or Secret. However, the Secret orders are created by an officer at a command post who uses online information from a Top Secret intelligence summary. The Top Secret summary was created from SCI and code-word intelligence that was sanitized by intelligence officers before being sent to the command post.

At each step, someone must sanitize a document and release it to a less-sensitive domain. Although there are some tools to help streamline and automate the release of sanitized documents, the process is hard to automate reliably.

17.7 Resources

IMPORTANT TERMS INTRODUCED

ADVERSARY
AGGREGATION AND INFERENCE
CLASSIFICATION LEVEL
CLASSIFIED INFORMATION
CODE WORD
COMPARTMENT
COMSEC CUSTODIAN
COMSEC MATERIAL
COVERT CHANNEL
CROSS-DOMAIN SHARING
DEGAUSSER
HIGH ASSURANCE
HOSTILE INTELLIGENCE SERVICE
INFORMATION OPERATIONS
JAMMING
NO LONE ZONE
POLYGRAPH
RED/BLACK SEPARATION
REDACTION PROBLEM
REFERENCE MONITOR
SECURITY CLEARANCE
SECURITY FAULT ANALYSIS
SEPARATION KERNEL
SIDE CHANNEL ATTACK
SPREAD SPECTRUM
TEMPEST
ZEROIZE
ZONE OF CONTROL

ACRONYMS INTRODUCED

AIS—Automated information system
C&A—Certification and accreditation
CCI—Controlled cryptographic item
CMW—Compartmented Mode Workstation
COMINT—Communications intelligence
COMSEC—Communications security
DSSS—Direct sequence spread spectrum
DTD—Data Transfer Device
EAM—Emergency Action Message
EKMS—Electronic Key Management System
EW—Electronic warfare
FOUO—For Official Use Only
GAO—Government Accountability Office
HUMINT—Human-based intelligence gathering
LMD—Local management device
MAC—Mandatory access control
MLS—Multilevel security
MSL—Multiple single levels
NISPOM—National Industrial Security Program Operating Manual
NOFORN—No foreign distribution
NSTISSC—National Security Telecommunications and Information Systems Security Committee
NSTISSI—National Security Telecommunications and Information Systems Security Instruction
OPSEC—Operations security
ORCON—Originator controlled
OTAR—Over-the-air rekeying
PDS—Protected distribution system
RMF—Risk management framework
SAP—Special Access Program
SCI—Sensitive Compartmented Information
SI—Special Intelligence
TCB—Trusted computing base
TPI—Two-person integrity
TRANSEC—Transmission security

17.7.1 Review Questions

R1. Identify cybersecurity risks and threat agents that apply particularly to information systems in government organizations.

R2. How is classified information different from other sensitive information?

R3. Summarize the security measures applied to classified information.

R4. Explain the redaction problem and how the exposure and quarantine model applies to sensitive information.

R5. Summarize elements of government and military information operations, of intelligence operations, and of operations security.

R6. Explain the difference between a security classification and a security clearance. How do they interact?

R7. Describe the different types of security markings that may appear on a classified document. Distinguish between genuine classification levels and other markings. What is meant by "above Top Secret?"

R8. Explain how compartments or code words might be used to protect particularly sensitive information.

R9. Summarize the major facets of national cybersecurity policy.

R10. Why does the U.S. government put special efforts into COMSEC instead of simply relying on commercial cryptographic products and mechanisms?

R11. Identify features of U.S. COMSEC measures that make them different from commercial practices described in earlier chapters.

R12. Describe the security problems associated with TRANSEC and common techniques used to address them.

R13. Explain the problems related to TEMPEST and five basic techniques used to address those problems.

R14. Identify the basic features of a reference monitor and explain its purpose.

R15. Explain the two parts of the policy used by the U.S. military to ensure the proper management of nuclear weapons.

R16. Explain the multilevel security problem and the Bell-LaPadula model.

R17. Describe the four modes of operation. Identify the most common mode used today.

17.7.2 Exercises

E1. Visit the CNSS website (cnss.gov). Locate the most recently updated policy, instruction, or standard. Identify the document, its date of issue, and briefly describe its topic.

E2. Visit the U.S. Government Accountability Office website (gao.gov). Locate a recent report on cybersecurity in the U.S. government. Review the

report and briefly describe the cybersecurity issue addressed in the report.

E3. Revisit Alice's security policy development in Section 1.5. Assume that Alice's laptop is used for highly sensitive intelligence work instead of retail work and personal activities.

a. Create an appropriate list of risks for that situation.

b. Create a new policy that addresses those risks, instead of the one shown in Table 1.5.

E4. Assuming that people have the security clearances shown in Table 17.1, and the Need to Know, list which people are cleared to read documents with the following classifications:

a. Secret

b. Top Secret

c. Secret KRUG

d. Secret KRUG MALBEC

e. Top Secret MALBEC

f. Secret MALBEC

g. Secret SAUVE MALBEC

h. Top Secret ARGUS BISHOP

i. Top Secret BISHOP KRUG

j. Top Secret SAUVE MALBEC

Each of the following problems requires the student to watch a particular dramatic film. **Each film typically runs about 2 hours.** Each problem notes the standard running time for the film; this may vary if watched on commercial television. The films are listed chronologically and not by topic or significance.

E5. Watch *Fail Safe* (1964), 112 minutes. Unrated.

a. How does the "fail safe point" procedure help ensure positive control when launching an attack with bombers?

b. How does the "fail safe point" procedure help ensure nuclear surety?

c. What error occurred to cause the bombers to attack Moscow?

d. Why couldn't the bombers be recalled?

E6. Watch *Dr. Strangelove* (1964), 95 minutes. Unrated.

a. The film portrays an unintended nuclear attack. Was the attack a failure of positive control or of nuclear surety? Why?

b. Why did the general try to block the Soviet ambassador from visiting the Pentagon's War Room?

c. The Soviet ambassador describes their automated doomsday device as intended to be a deterrent for nuclear war. List two reasons why it might

serve as a deterrent. List two reasons why it might be a bad choice for a deterrent.

d. Why did the recall order fail? Was this a failure of nuclear surety or of positive control? Why?

E7. Watch *WarGames* (1983), 114 minutes. Rated PG (USA).

a. The film opens with an incident in a Minuteman launch control center. Does the incident reflect a failure of positive control or of nuclear surety? Why?

b. The two teenagers were playing "global thermonuclear war" and they launched simulated missiles at Las Vegas and Seattle. Assume that the computer operator hadn't detected that it was a simulation. What would happen next? What subsequent steps might prevent a missile launch?

c. How did the teenagers find the dial-in port to the WOPR?

d. Should the WOPR have had the dial-in port used in the film? Why or why not? What policies might apply to this situation?

E8. Watch *The Falcon and the Snowman* (1985), 131 minutes. Rated R (USA).

a. Identify two different types of security measures that would have helped prevent theft of the crypto keys.

b. Did the NSA inspector perform a reasonable inspection? Why or why not?

E9. Watch *Crimson Tide* (1995), 116–123 minutes, depending on the release. Rated R (USA).

a. Consider the missile launch procedures portrayed in the film. Is it possible for a single person to launch a nuclear missile? Why or why not?

b. A dispute develops between the captain and executive officer about the interpretation of an EAM. Does this dispute reflect a failure of positive control or of nuclear surety? Why?

c. Under what circumstances should a recipient accept an unauthenticated message? Give an example of a circumstance in which accepting an unauthenticated message would yield the wrong result.

d. Following the final scene but before the credits, the film displays a message explaining a change to the process of authorizing nuclear missile launches. Would this change have prevented the problem portrayed in the film? Why or why not?