Part

I

Cyber Network Security Concepts

In This Part

CHAPTER

1

Executive Summary

Effective cybersecurity is a critical capability for the defense and preservation of civil society. Cyber crime is one of the world's largest and fastest-growing categories of crime. Cyber criminals are responsible for more than $1 trillion USD in stolen funds and other assets, with crime in some segments growing 300 percent per year. Cyber espionage is epidemic and pervasive; even the world's smartest companies and government institutions have terabytes of intellectual property and financial assets being lost annually via the Internet. Concealed malicious actors even threaten our electrical power grids, global financial systems, air traffic control systems, telecommunications systems, healthcare systems, and nuclear power plants.

Chances are good that your current organization is being attacked right now: cyber criminals, civilian/military cyber warriors, and global competitors are deeply entrenched in your network. If you have information worth stealing, it is likely that the attackers are on your internal network, exfiltrating data from your end users, and controlling key administrative nodes. If organizations don't change the way they are defending themselves, personal identifying information, bank account and credit card numbers, and intellectual property that defines competitive advantage will continue to be stolen.

The threat is to all civil society. If cyber attackers scrambled all the data on Wall Street and Bond Street, wiping out all investments and retirement accounts based in the U.S. and U.K., the consequences are unthinkable. (And this scenario is a real possibility.) The goal of this book is to lay the foundation for solving this critical problem in earnest.

U.S. government policy experts are quite concerned about the strategic gap in cyber skills, claiming that in 2008 the U.S. had only 1,000 world-class cyber experts but would require 20,000 to 30,000 to adequately handle cyberspace offense and defense. I believe that estimate is quite low. There are 25,000,000 business establishments that need cyber defenses in the U.S. alone, according to the census bureau. Certainly, hundreds of thousands of technologists with the kinds of skills and education presented in this book will be needed to fully defend civil society.

Why Start with Antipatterns?

To successfully make a change, the first step is to admit you have a problem. The civilized world is in a dire predicament regarding cyber threats. Solving cybersecurity issues requires radical new ways of thinking, and, paradoxically, a return to first principles and common sense—in other words, ruthless pragmatism.

Antipatterns employ psychological frameworks for solving problems whose causes involve habitual mistakes. Antipatterns require a mind shift from the dispassionate mindsets of mathematics and engineering into the judgmental milieu of enterprise architecture and organizational change.

NOTE **Some people have criticized antipatterns as being anti-intellectual. Antipatterns are a way of thinking clearly about habitual causes, serious problems, and effective solutions.**

Antipatterns have been summarized by the quip, "Technology is not the problem…people are the problem." But, changing people's minds is very difficult. So, you need powerful psychology to do that.

NOTE **The classic paradigm of organizational change is: You send your people out on a rickety bridge toward a pot of gold and then start a fire behind them so they can never go back to old ways.**

Antipatterns have ancient roots in governance, law enforcement, religion, and public administration. In a perverse sense, antipatterns are an adult form

of name-calling used to control society. We invent pejorative names and make public examples of miscreants to prevent other people from misbehaving.

For the sake of clear definition, here are a few examples of modern-day social antipatterns used in general society: liberal (lily livered), racist (bigot), terrorist (violent extremist), convict (felon, violent offender), street criminal (thug, gang banger), drug addict (junkie), corrupt politician (crook), and all terms for sex criminals. Words have baggage. Even the term hacker has antipattern connotations.

Although this book does not emphasize the name-calling aspect of antipatterns, the goal is the same: to clearly articulate habitual mistakes (in IT) and then rapidly transition the discussion toward pragmatic solutions.

In this chapter, a basic form of antipattern is introduced. Basic antipatterns include two parts: (1) a description of the antipattern problem, and (2) a description of an improved solution, called a *refactored solution*. In some cases in this chapter, I present the antipattern without the refactored solution. Chapter 2 introduces the full antipatterns template.

Security Architecture

The cybersecurity crisis is a fundamental failure of architecture. Many of the networked technologies we depend upon daily have no effective security whatsoever. (See the "Networks Always Play by the Rules" antipattern in Chapter 2). The architecture of the Internet and the vast majority of deployed software create significant opportunities for malicious exploitation.

It is worth stating that if infrastructure and software technologies were engineered properly, they would be built to withstand known and manage unknown risks, and they would be significantly more secure than current-day technologies.

Chapter 3 introduces the Zachman Framework for Enterprise Architecture and applies it to securing enterprises. The Zachman Framework is a powerful intellectual tool that enables complex organizations to describe themselves, including their mission, business, and information technology (IT) assets. With this self-knowledge comes awareness of risks and mitigations, and ways of engineering security into solutions from inception. The Zachman Framework serves as an overarching structure that organizes the problem-solving patterns catalog in Chapter 3.

The following sections begin the discussion of cybersecurity antipatterns, including some of the most significant cybersecurity challenges, including education. Antipatterns can be construed as cynical depictions of the current state of practice. Negativity and cynicism are not the goal; there are many solutions and patterns for success.

Antipattern: Signature-Based Malware Detection versus Polymorphic Threats

The conventional wisdom is that all systems with up-to-date antivirus signatures will be safe. However, many popular antivirus solutions are nearly obsolete, with many missing the majority of new malware. Current signature-based antivirus engines miss 30 percent to 70 percent of malicious code, and nearly 100 percent of zero day infections, which, by definition, are unreported exploits.

Malicious signature growth is exploding from 5 new ones per day in 2000 to 1,500 per day in 2007 and more than 15,000 per day in 2009, according to Symantec (from a 2010 conference briefing on reputational anti-malware), which is an average of 200 percent to 300 percent cumulative growth per year. Malware variability has grown so rapidly that signature-based detection is rapidly becoming obsolete.

NOTE **Each security industry vendor has its own sensor network for gathering and monitoring malware. Kaspersky Labs has seen flat growth in malware signatures since 2008, while other vendors imply exponential growth. Somewhere in the middle lies the truth.**

The proliferation of malware signatures is exploding primarily due to polymorphic malware techniques. For example, hash functions used by signature-based detectors yield very different values with only slight changes to a malicious file. Changing a string literal in the file is sufficient to trigger a false negative. Other polymorphic techniques include varying character encodings, encryption, and random values in the files.

One interesting online application from VirusTotal.com runs more than 30 antivirus programs on each file that any Internet user can submit. You can witness just how haphazard antivirus tests are.

Refactored Solution: Reputational-, Behavioral-, and Entropy-Based Malware Detection

Vendors are developing innovative techniques that can detect zero day and polymorphic malware. Several promising approaches for the future include:

- Symantec is harnessing a 100M+ global customer base to identify potential malware signatures. The technique, called reputation-based signatures, is able to identify 240 million new malware signatures by comparing binaries across millions of systems for anomalous variations.
- FireEye has created a behavioral intrusion detection system (IDS) that uses elements of honeypots and forensics to automatically identify malicious

content as it flows across corporate networks. Behavioral IDS techniques simulate the execution of sniffed content in a virtual machine, which then observes resulting configuration changes, such as changes in registry settings, services, and the file system. There are other emerging behavioral antivirus products, for example, from ThreatFire.com.

- An emerging field of research called entropy-based malware detection looks for mathematical similarity to known malware signatures. Hash functions that are used by most antivirus programs detect subtle differences between a file and its known hash. Minor changes to a file, such as modification of strings or encodings can cause a hash match to fail. Entropy-based matching uses mathematical functions that measure similarity rather than differences. If a suspicious file nearly matches the same entropy measure as malware, there is a high likelihood that the malware is present.

Antipattern: Document-Driven Certification and Accreditation

Some of the most flagrant antipatterns involve the IT security industry itself. Assessment and Authorization (A&A), formerly called Certification and Accreditation (C&A), has attracted much public criticism because it has a reputation as a paper-driven process that does not secure systems from real threats. See Chapter 7 for more information about C&A and A&A.

A&A is the process of assuring the information security of systems before they are deployed. Certification is an assessment and testing phase that identifies and confirms vulnerabilities. Accreditation is an executive approval process that accepts risks discovered during certification.

Precertification is often an arduous process of security documentation and reviews. In many organizations, certification is problematic. Often testing is waivered or done very superficially with policy scanners that check registry and configuration settings.

In the more rigorous practice of penetration testing (pen testing), vulnerabilities are thoroughly explored with state of the art tools, followed by actual exploitation and malicious user tests where unauthorized accesses are the goal.

Although A&A is formalized in government organizations, it is also widely practiced in industry. For example, payment card industry (PCI) standards require businesses that process credit cards (in other words, virtually all retail companies), to conduct penetration tests and other formal assessments.

Refactored solutions for this antipattern can be derived from the practical security testing and investigation techniques presented in this book.

Antipattern: Proliferating IA Standards with No Proven Benefits

National Institute of Standards and Technology (NIST) is a U.S. government organization with dozens of IT security publications. NIST's latest 800 series of publications are considered the new state-of-the-art gold standard for formalizing IT security controls and managing risk.

There are literally hundreds of NIST publications pertaining to computer security. Some of the key NIST publications include the following:

- **NIST SP 800-39**: Defines integrated enterprise-wide risk management processes across entire portfolios of systems and business activities
- **NIST SP 800-37**: Defines the process for lifecycle risk management
- **NIST SP 800-30**: Defines how to conduct a risk assessment for a single system
- **NIST SP 800-53**: Contains the standard catalog of security controls. These controls are requirements that address all aspects of information security
- **NIST SP 800-53A**: Defines how to implement security controls, including test, interview, and review procedures

There is a companion to these documents: the U.S. Committee on National Security Systems (CNSS) Instruction No. 1253, which profiles the use of NIST security controls for national security applications. This publication also contains values for parameters in NIST SP 800-53 controls.

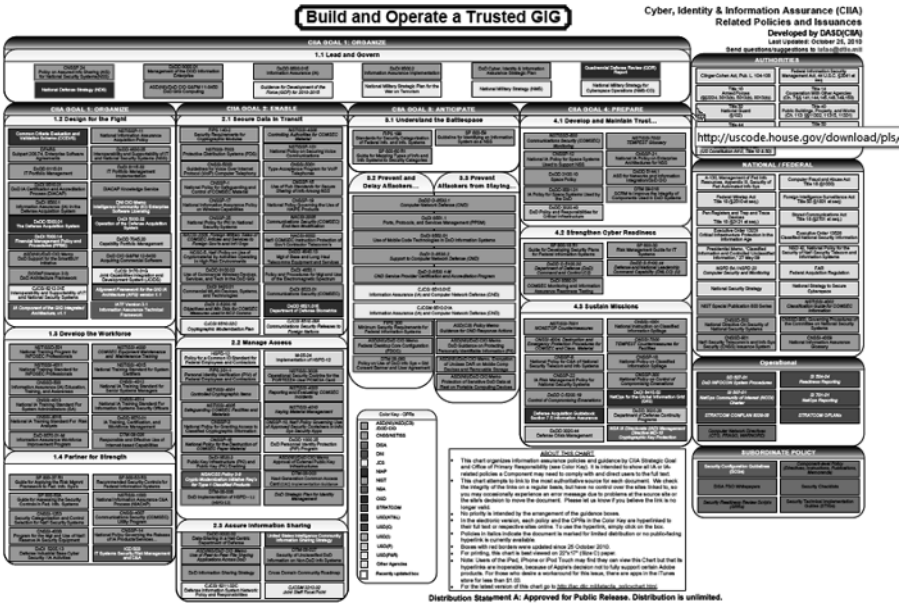
The problem with these guidelines and controls is that they are too voluminous to be applied in practice without extensive automation. A typical list of NIST security controls contains more than 600 requirements for each system. With current technology, the vast majority of those should be evaluated manually. Development schedules, commercial competition, and mission needs simply do not allow for the meticulous security audits implied by these huge lists. It will take many years to transition the government and commercial tools to the new NIST standards.

On the other hand, to date, a reasonable level of automation has been achieved for pre-existing requirements, evaluated by the DISA.mil and ONI.mil policy test suites. Commercial versions of these tests are available from Application Security Inc. and eEye Digital Security. It will take many years to transition the government and commercial tools to the new NIST standards.

An open question remains, however: After going through all the trouble to achieve security compliance, was the effort worthwhile? Are the systems actually more secure compared to currently emerging threats? Standards are not changing at the same rate that the security threats are evolving and morphing

into new attack vectors. There is an excruciatingly obvious mismatch between the world of highly innovative malware and the stodgy world of never-changing standards.

A dramatic visual example of this antipattern is the security policy landscape for the Global Information Grid (Figure 1-1).



Source: U.S. Department of Defense

Figure 1-1: Global Information Grid Policy Landscape

The diagram is really as unintelligible as it looks, even if you could read it. See the original at `http://iac.dtic.mil/csiac/download/ia_policychart.pdf`

The diagram lists more than 200 separate policies and standards documents, grouped into 17 categories. There is no way that anyone could understand all this complexity, much less, apply it to every system in the enterprise.

This is an obvious lack of common sense, and completely contrary to the pragmatic way of solving problems presented in this book. A key cause of this antipattern is that many individuals equate complexity with quality. If we have so very many policies and standards from NIST and the rest of the government, it must be very good? Right? How could it be any other way?

SANS Institute, a leading provider of hands-on cybertraining, has suggested publically that the paper-compliance-driven security regimes should be replaced by hands-on technical security expertise. So the refactored solution for this antipattern is revealed through techniques described in Chapters 4 through 9 of this book.

Antipattern: Policy-Driven Security Certifications Do Not Address the Threat

The gold standard of professional security certifications is the Certified Information System Security Professional (CISSP). It is an entirely paper-based qualification, requiring a great deal of memorization in 10 diverse security domains, such as physical security, communications security, and systems security. CISSP is required by the U.S. Department of Defense (DoD) for both management and technical security workers, and demanded in the job market. Anecdotally, the presumed goal of this certification is to produce articulate security professionals who can communicate effectively with upper management, but what does that have to do with combating emerging cyber threats?

This paradox was addressed by the Center for Strategic and International Studies (CSIS), which released a Presidential Commission report: A Human Capital Crisis in Cybersecurity (July, 2010). The report states clearly that "the current professional certification regime is not merely inadequate; it creates a dangerously false sense of security" with an overemphasis on security compliance on paper versus combating threats.

Many people in the cybersecurity community view this finding as controversial because their careers, reputations, and credentials are invested in security compliance policies and procedures. This is the industry that drives A&A, risk management, security controls compliance, and other labor-intensive security activities. Unfortunately, for most professionals, it is much easier to turn a highly technical person into a policy person, whereas it is very difficult (or impossible) to turn a policy person into a highly technical one. It is a one-way street.

Refactored Solution: Security Training Roadmap

This entire book is aimed at providing a refactored solution to the previous antipattern. What are the essential education requirements that will enable security personnel to adequately defend enterprises from cyber attack? I attempt to answer that question for the industry readers and two- to four-year college students and professors. Because there are 25 million business establishments in the U.S., a great number of trained professionals will be needed to defend those businesses' networks, systems, applications, and data.

Aside from the material presented in this book, how else might you acquire the necessary cyber defense skills? One approach is through professional training in hands-on skills, for example, at SANS Institute and a handful of other places.

SANS Institute offers a masters-level degree and a Cyber Guardian certification, which both require numerous SANS certifications to achieve. These programs

are elite and require exceptional student performance. It is hard to imagine that sufficient numbers of people could complete such a rigorous program.

The following are some suggestions for a practical SANS training regime for a network defender. The corresponding certifications are implicit in the list. The baseline assumption is that you have a technology background and are not a complete beginner. The chapters in parentheses indicate where the materials occur in this book:

- SANS SEC 401 Security Essentials: Networking (Chapter 6); network administration (Chapters 4 and 5)
- SANS SEC 504 Hacker Techniques, Exploits, and Incident Handling: Intrusion detection (Chapter 9); and security testing (Chapters 6, 7, and 8)
- SANS SEC 560 Penetration Testing and Advanced Ethical Hacking: Pen testing (Chapter 8)
- SANS SEC 503 Intrusion Detection In-Depth: Network sensors; intrusion detection/analysis (Chapter 9)

If you work for, or contract with, the U.S. federal government, another training curriculum is available from the Defense Cyber Crime Center (DC3) near Baltimore. DC3's Defense Cyber Investigations Training Academy (DCITA) is tuition free. The suggested curriculum at DC3 includes the following:

- Computer Incident Responders Course (Chapters 6 through 9)
- Network Exploitation Techniques (Chapter 8)
- Network Monitoring Course (first part of Chapter 9)
- Advanced Log Analysis (remainder of Chapter 9)
- Live Network Investigations (summarized in Chapter 9)

In addition, this book also includes essentials of network programming in Chapter 6. These topics are covered partially by SANS SEC 560 and DC3 courses, such as Advanced Log Analysis.

The preceding information defines roadmaps for computer network defense training, a role that is called Blue Team. A different cybersecurity role, Red Team, takes an offensive posture. Red Teams are expert penetration testers who attack and exploit networks, servers, and devices. In addition to the Blue Team curriculum already discussed (excluding SANS 503), the following additional SANS courses are for Red Team members:

- SANS SEC 542 Web App Pen Testing and Ethical Hacking (Chapter 8)
- SANS SEC 617 Wireless Ethical Hacking and Pen Testing (Chapter 8)
- SANS SEC 660 Advanced Penetration Testing

An alternative Red Team curriculum is offered by Offensive Security. Offensive Security is the developer of BackTrack, a penetration testing suite that's built on Ubuntu Linux (see Chapter 5). The suggested Offensive Security curriculum, along with the suggested SANS prerequisite, is the following:

- SANS SEC 401 Security Essentials (or equivalent): Solid network administration skills are needed for these courses (Chapter 4)
- Penetration Testing with BackTrack (PWB): (Chapter 8)
- Wireless Attacks (WiFu): (Chapter 8)
- Cracking the Perimeter (CTP): Advanced pen testing

NOTE **PWB, WiFu, and CTP are Offensive Security's abbreviated names for their core courses.**

Another advanced Red Team training program is offered by the University of Tulsa, Department of Mathematical and Computer Sciences. You can find more information at `http://isec.utulsa.edu/`.

I have taken several of these courses, including self-guided study. Both the SANS Institute and Offensive Security courses are surprisingly fast-paced in the classroom. The instructors explain subjects at the comprehension rate of the best students, not the stragglers. I highly recommend self-paced courses as alternatives to classroom study, or purchased as a supplement to live classes. Self-paced editions of the courses are available, such as SANS OnDemand and online versions of PWB, WiFu, and CTP. About 50 to 70 hours of post-classroom review are needed to pass the certification exams, so OnDemand with its supplemental quizzes is an excellent investment. The labs and exercises, conducted via the Internet are otherwise identical to the classroom courses.

This book offers hands-on labs from a Syracuse University source called SEED: A Suite of Instructional Laboratories for Computer Security Education. (See Chapter 4 through 9). You can read more information about SEED Labs at `http://www.cis.syr.edu/~wedu/seed/all _ labs.html`.

Cross-training in the previously mentioned skills is recommended for the entire Red or Blue Team. There are also specialist skills, which every team will need from time to time, but not every team member needs to know. The skills can be brought onboard through hiring, education, training, consulting, or outsourcing as specialists would only be called in to do novel software/hardware installation, establish enterprise standard configurations, and resolve serious network problems.

The following is a recommended list of specialized skills that should be available on-demand in IT security shops:

- **Network Device Specialist:** Vendor-certified specialist with deep knowledge for debugging and configuring the network devices in your shop—for example, routers and firewalls. Applicable certifications are from CISCO, Novell, and other networking vendors.
- **Operating System Security Specialist:** Specialist in configuring and hardening the security of each operating system in your environment. Applicable certifications and training from Microsoft, Oracle (Sun), Tresys Technology (Linux), Red Hat (Red Hat Linux), Novell (SUSE Linux), eEye Digital Security, and other operating system (OS) developers and specialists.
- **Database Security Specialist:** Specialist in configuring the security of specific database types in your environment. Applicable certifications and training from Oracle, Sybase, Application Security Inc., Well House (open source), and other database specialists.
- **System Forensics Specialist:** Specialist in in-depth analysis of systems, creating chains of evidence, and other forensic investigation techniques. Applicable training from Defense Cyber Crime Center, SANS Institute, Guidance Software, Access Data, and other forensic specialists.
- **Reverse Engineering Malware Specialist:** Security researcher who captures malware and analyzes its characteristic with the goal of permanent eradication from your networks. Applicable education and training from SANS Institute, Invisible Things Lab, Black Hat courses, and other security researchers.

Summary

This chapter introduces a new way of thinking about computer security through a high-level discussion of antipatterns, which are habitual mistakes made in the IT security industry. It provides a stark assessment of the current state of cyber threats and defenses, so that you can have a clear understanding of the growth and significance of cybersecurity threats.

The chapter discusses key concepts from antipatterns and security architecture and presents some high profile antipatterns along with their refactored solutions. The chapter's concluding solution is an in-depth discussion of cybersecurity learning opportunities.

The next chapter introduces a techno-political framework (an expanded antipatterns catalog) that can foster organizational change for improved cyber defenses.

Assignments

1. Discover additional materials that survey the current state of cyber threats and vulnerabilities, such as annual online survey reports from SANS Institute, McAfee, and Verizon. Describe your findings.
2. Investigate the use of state-of-the-art malware detection and eradication, such as the reputation-based approach by Symantec. How do these novel approaches work? How do they gather intelligence on malware threats?
3. Select one of the core NIST Special Publications on IT security (for example, 800-30, 800- 39, 800-53, or 800-53A) and report on its benefits and limitations for defending enterprises.
4. Identify alternatives to document-driven certification and accreditation such as continuous monitoring. Compare and contrast that approach to the document-driven current practices.
5. For one or more of the security specialties, identify college courses or training alternatives that would lead to that specialty. Explain your course selections. The security specialties include the following:
   a. Network Device Specialist
   b. Operating System Security Specialist
   c. Database Security Specialist
   d. System Forensics Specialist
   e. Reverse Engineering Malware Specialist