CHAPTER 15

Web Application Security Organizations

THERE IS NO SINGLE NATIONAL OR INTERNATIONAL governing body for information security. A large number of national security interests exists—private and government sectors and academic and commercial interests, among others.

In addition, a wealth of information security qualifications and education programs is available, ranging from academic and professional to independent and vendor certifications. In short, it's no easy task to understand all the details and match them with your particular requirements. This chapter discusses the key qualifications in information security and sheds light on the purpose of each one.

Chapter 15 Topics

This chapter covers the following topics and concepts:

- What the Department of Homeland Security (DHS) is
- What the National Cyber Security Division (NCSD) is
- What the United States Computer Emergency Response Team Coordination Center (CERT®/CC) is
- What the MITRE Corporation and the CVE list are
- What the National Institute of Standards and Technology (NIST) is
- What the International Information Systems Security Certification Consortium, Inc. $(ISC)^2$ is
- What the Web Application Security Consortium (WASC) is
- What the Open Web Application Security Project (OWASP) is

Chapter 15 Goals

When you complete this chapter, you will be able to:

- Understand the responsibilities and interests of various national and international security organizations
- Understand some of the non-vendor certificates and programs available
- Determine which qualifications are applicable to your areas of interest

Department of Homeland Security (DHS)

The DHS is responsible for a wide area of the federal coordination of security issues and the specification and implementation of security controls. Within the information security arena, DHS has specific management responsibility for the National Cyber Security Division, the National Infrastructure Advisory Council, and the Critical Infrastructure Partnership Advisory Council.

The DHS also manages the U.S. Secret Service, which used to be part of the Department of the Treasury. Other DHS components that have significant information security responsibilities include Customs and Border Protection and the Transportation Security Administration (TSA).

Advisory Bodies

The National Infrastructure Advisory Council is a presidential advisory panel of up to 30 appointed members. Its role is to provide advice on securing key sectors of the economy and government. This covers many areas, including finance, utilities, telecommunications, transportation, and health care. The focus is on public-private cooperation.

The Critical Infrastructure Protection Panel is a much wider membership organization that promotes cooperation between the government and sector councils in support of the National Infrastructure Protection Plan. More information about DHS cybersecurity initiatives can be found at *http://www.dhs.gov/topic/cybersecurity*.

The U.S. Secret Service (USSS)

The U.S. Secret Service (USSS) has a historic role in protecting the stability of the national financial system. It initially started with an anti-counterfeiting role in 1865. Its official mission is "to safeguard the nation's financial infrastructure and payment systems to preserve the integrity of the economy."

The 2001 U.S.A. PATRIOT Act approved the creation of a network of electronic crimes task forces (ECTFs), and over 20 have been established in the United States. Any crime or investigation involving electronics/technology—including the Internet—can fall within the task forces' range of operation. Additionally, since 1994, the Secret Service has provided technical and computer forensic support to law enforcement in the investigation of missing and exploited children. More information on the USSS electronic crimes task force is available at *http://www.secretservice.gov/ectf_about.shtml*.

The Federal Law Enforcement Training Center (FLETC)

FLETC runs a range of technology and security training programs in its Technical Operations Division. Some programs of interest are:

- **Computer Network Investigations Training Program (CNITP)**—This program is designed to allow participants to conduct digital forensic seizures and investigations on networked systems.
- **Seized Computer Evidence Recovery Specialist (SCERS)**—This is an introductory program to computer forensic principles. It introduces students to leading forensic software products. It's used as a preliminary requirement for many other training programs.
- **Digital Evidence Acquisition Specialist Training Program (DEASTP)**—This is a fast-paced introduction to evidence recognition and seizure. It's a prerequisite for SCERS training.
- **First Responder to Digital Evidence Program (FRDE)**—A short program for first-response personnel, covering recognition and seizure principles.

Mutual Legal Assistance Treaties

Mutual legal assistance treaties (MLATs) define, in many cases, how law enforcement agencies in different countries should cooperate. For the United States, these agreements are generally managed through the legal attaché offices in embassies and consulates, which often are staffed by FBI Special Agents who pass requests to relevant national or local FBI teams.

MLAT activities are often inaccessible to the private citizen or corporate investigator. Processing requests generally takes considerable time both for authorization—necessary at the requesting and providing nations—and the communication of requests through diplomatic channels.

Many law enforcement organizations don't accept direct reporting from outside their local jurisdictions. This is known to significantly discourage victims from reporting Internet-related crime. However, both the ECTFs and the FBI Internet Crime Complaint Center (IC3) will accept notifications of Internet-related crimes if either the victim or the alleged criminal is in the United States.

- **Macintosh Forensics Training Program (MFTP)**—Specific training in forensic issues and activities for Apple systems running Mac OS.
- **Mobile Device Investigations Program (MDIP)**—Training focused on forensic recovery and interpretation from cellular telephones and fusion devices.

You can learn more about these training programs by visiting *https://www.fletc.gov/*.

National Cyber Security Division (NCSD)

Established by presidential decree, the NCSD is part of DHS and has responsibility for protecting the security of cyberspace and U.S. cyberassets. It works with federal, state, commercial, and international organizations. NCSD runs the National Cyberspace Response System and a range of cyber-risk management programs.

The National Cyberspace Response System is a comprehensive program that covers:

- **Computer vulnerabilities**—Under the Cybersecurity Preparedness and the National Cyber Alert System and the vulnerability investigation capabilities of US-CERT
- **Computer incident response**—Under US-CERT and the National Cyber Response Coordination Group
- **Information sharing**—Among attack investigators via the Cyber Cop Portal

United States Computer Emergency Response Team (US-CERT)

Founded in 2003, US-CERT is the operational arm of the NCSD, responding to incidents for the federal government. It cooperates with other national and commercial **computer incident response teams (CIRTs)** and law enforcement agencies to investigate and stop online attacks and restore services. It also provides a public threat and vulnerability alert service.

National Cyber Alert System

US-CERT takes Really Simple Syndication (RSS) feeds from several government agencies to make available several e-mail lists and associated feeds. Presently, five RSS feeds can keep you up to date on security tips, bulletins, and alerts, as well as the most recent security activities with leading vendors. The feeds range from detailed technical alerts for system administrators to a "tips" feed aimed at the home or non-technical user.

Cyber-Risk Management Programs

Currently, the NCSD offers three main public risk management programs:

- **Cyber Exercises: Cyber Storm**—A biennial event for federal and state agencies, international partners, and businesses, this exercise covers different industry sectors to provide practice and improve coordination and information-sharing in case of a massive cyberattack.
- **National Cybersecurity Awareness Month**—Every October since 2004, this event has provided the general public and smaller businesses with education and tools on basic Internet security techniques.
- **Software Assurance Program**—Through initiatives such as "Build Security In" and the Community Resources and Information Clearinghouse, this program enables software developers and vendors to deliver more secure and reliable products.

Additionally, the National Cybersecurity Awareness Campaign Challenge was set up to crowdsource new ways of communicating information security advice and techniques to the American public.

Computer Emergency Response Team Coordination Center (CERT®/CC)

CERT/CC was founded in 1988 under contract from DARPA, after the Morris Worm attack used various UNIX vulnerabilities and weaknesses (and a basic programming error) to bring a significant percentage of the fledgling Internet to a halt. CERT/CC is part of the Software Engineering Institute at Carnegie Mellon University. Although it no longer plays an active role in the investigation of computer incidents, CERT/CC conducts research and training for the wider **computer security incident response team (CSIRT)** community. (A CSIRT is an all-hours or on-call group for an organization, a corporation, or even a country designed to respond to online attacks or similar events.) CERT/CC also is a major sponsor of the international **Forum of Incident Response and Security Teams (FIRST)**. FIRST is a worldwide voluntary and collaborative body bringing together incident response teams and related organizations.

CERT/CC has a wide role in software assurance, secure systems engineering, risk management, and governance. It provides development support for countries and organizations wishing to implement CSIRTs and conducts significant research into new attack methods and forensic analyses of attacks.

Its education program, which is open to the public, includes:

- **The Certified Computer Security Incident Handler qualification**—A range of courses and an online

examination to support a DoD 8750.1M-compliant certification in incident handling.

- **CSIRTs**—Courses are available for organizations in the creation and management of CSIRTs.
- **OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Exposure)**—This is the risk management methodology developed at CERT/CC.
- **Malware**—Training in the analysis of malicious code is provided. This course is currently open only to employees of the U.S. government or its contractors.

Training is also provided in the application of various metrics and models developed by CERT/CC and in secure coding.

The MITRE Corporation and the CVE List

The MITRE Corporation is a major government and defense contractor, albeit one set up and operating as a not-for-profit corporation. MITRE runs four Federally Funded Research and Development Centers (FFRDCs) and provides technical consulting to federal agencies and other bodies. The MITRE Corporation also maintains the **Common Vulnerabilities and Exposures (CVE) list**. The National Cyber Security Division of the Department of Homeland Security sponsors the CVE.

NOTE

SecurityFocus is now part of Symantec Corporation.

Why CVE?

In the 1990s, there was no commonly accepted reference system for computer and software vulnerabilities. The famous Bugtraq and Vulnerability Development (Vuln Dev) mailing lists were run by the private SecurityFocus organization. In addition, many Web sites, conferences, and other private, public, and academic mailing lists announced new vulnerabilities.

These lists allow researchers to release a brief description of a problem, a full academic paper, or a proof-of-concept exploit. Individual software authors and vendors published details about problems and patches. Keeping track of whether a particular problem was relevant to your systems and whether a patch was available was not a trivial issue, especially across large organizations with heterogeneous IT architectures.

Many security testing tools used their own reference system. This helped IT managers determine whether a detected problem was common between different parts of an organization or even different architectures within the same business area. This required a detailed knowledge of the security vulnerability publication process. However, systems administrators—then and now—are generally responsible for maintenance and update, not security. However, the lack of a commonly accepted system existed until the Common Vulnerabilities and Exposures (CVE) list was created.

Common Vulnerabilities and Exposures (CVE) List

MITRE established the CVE list in 1999 in collaboration with a number of software and security vendors. The CVE list was rapidly accepted by the general industry as a basic reference. In 2003, "CVE-Compatible" accreditation for testing products was launched. To date, nearly 100 products from more than 50 companies have been formally certified, with over 150 more declared compatible.

CVE does have its problems. For example, when an entry is initially added to the CVE list, the entry has a status of "candidate." After the entry has been reviewed and accepted, its status is changed to "entry." There can be a long delay between a candidate appearing on the list and finally being accepted as an entry. However, its enormous success has been its near-universal acceptance as a single reference for vulnerability reports, allowing effective cross-reference between detection engines, vendor bulletins, patch management software, and other utilities.

What Is a CVE Identifier?

CVE is intended to be a basic list, neither a database nor the repository of all information about a particular

vulnerability. A single entry on the list is known as a "CVE identifier" and is composed of the following information about a vulnerability:

- **CVE number**—This is in the form of CVE-YYYY-nnnn, for example, CVE-2010-1868.
- **Identifier status**—Either "candidate" or "entry." Before 2005, candidates were identified with a "CAN" label rather than a "CVE" prefix.
- **Description**—This is a brief, standardized description of the vulnerability. In the case of 2010-1868, the description is "The (1) sqlite_single_query and (2) sqlite_array_query functions in ext/sqlite/sqlite.c in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to execute arbitrary code by calling these functions with an empty SQL query, which triggers access of uninitialized memory."
- **References**—These may be to the discoverer's announcement, the vendor's security bulletin, or third-party reports such as the Open Source Vulnerability Database at *http://osvdb.org*.
- **Additional**—Candidates may also have information on the stages of the CVE process, and any votes from the CVE Editorial Board. This also includes a comment field.

Quite deliberately, there is a lack of data within each CVE identifier. More information is available through other tools such as the National Vulnerability Database.

Generating New List Entries

Anyone who discovers a potential vulnerability can report the basic details directly to MITRE or to one of the CVE Numbering Authorities. MITRE also scours public vulnerability lists for new vulnerabilities.

A "candidate number" will be assigned and the basic information can be recorded. Before a candidate can become an entry, it must be reviewed by the members of the CVE Editorial Board, who then vote for it to be rejected, modified, or accepted. Once sufficient votes are cast for acceptance, the vulnerability will be published as an entry. Entries may continue to be modified after publication, normally to add additional references.

Sincere Flattery

The success of the CVE model has led to the creation of a number of similar ones. These include Common Configuration Enumeration (CCE) and Common Attack Pattern Enumeration and Classification (CAPEC), which are also run by MITRE. The requirement for categorization has led to the creation of a number of formalized language schemes such as MAEC (for malware), CWE (for weaknesses), and OVAL (for vulnerabilities).

An exception is in the world of malicious code. Although the Computer Antivirus Researcher Organization (CARO) has been in existence since 1991, antivirus products continue to use naming schemes particular to each vendor. This can make it difficult, if not impossible, to determine common cause between infections in different organizations or even different parts of the same organization.

National Institute of Standards and Technology (NIST)

Founded at the turn of the 20th century as the National Bureau of Standards, NIST has both a historic and a continuing role in information security, largely through its Computer Security Division. As the name implies, it's the U.S. federal authority on standards. NIST publishes essential information such as the Federal Information Processing Standards (FIPS) series, the Special Publications 800 series of guides and recommendations, and the Federal Desktop Core Configuration. The United States Government Configuration Baseline (USGCB) initiative provides security configuration baselines for information technology products widely deployed within the federal government—primarily Microsoft products, including operating systems and firewalls.

However, NIST does not play a significant role in U.S. representation to the International Standards Organization, responsible for the ISO 27000 series. That is coordinated by American National Standards Institute (ANSI). ANSI is also the U.S. national representative body for the International Electrotechnical Commission (IEC).

Technical Security Standards

The FIPS series sets specifications for essential security components. For example, FIPS 197 covers the Advanced Encryption Standard (AES) algorithm. FIPS 180-3 details the Secure Hash Standard, including SHA-1. FIPS 140

covers security requirements for encryption modules across four levels. Standards also exist for security areas as wide as personnel vetting and automated password generators. Although these standards are generally binding only on the U.S. federal government, many are widely used commercially and internationally.

technical TIP

When you are looking for an evaluated encryption product and the salesperson claims FIPS 140 certification, your first question should be "To what level?" If you require multifactor authentication for crypto administration—a common control within Payment Card Industry Data Security Standard (PCI DSS) encryption management schemes—this is not mandated until the highest level, which is 4. In comparison, solutions at level 1 don't require any form of user authentication.

NIST also runs the processes for replacement standards, such as the competition for an AES algorithm to replace DES between 1997 and 2000, won by the Rijndael algorithm. In October 2012, NIST announced that Keccak (pronounced "catch-ack") would become NIST's SHA-3 hash algorithm. It was created by Guido Bertoni, Joan Daemen, and Gilles Van Assche of STMicroelectronics and Michaël Peeters of NXP Semiconductors. Their entry beat out 63 other submissions that NIST received after its open call for candidate algorithms in 2007.

Publications that don't meet the requirements for issue of a FIPS are often issued under the "Special Projects" report system. Titled "Guide to" or "Recommendation for," these publications don't have the legal force of FIPS and cover wider areas of general interest to the information security community. Recent reports have included guides to protecting personally identifiable information, the use of encryption algorithms and appropriate key lengths, and the secure deployment of Internet Protocol version 6 (IPv6) addressing technologies.

NOTE

Data Encryption Standard (DES) FIPS 46 was based on the IBM Lucifer cipher. The cipher was developed by Horst Feistel, a German and naturalized American citizen. Joan Daemen and Vincent Rijmen, who developed AES, the replacement for DES, are both Belgian citizens.

Computer Security Resource Center (CSRC)

Within NIST, the Computer Security Division was established as part of the Information Technology Laboratory in response to Section 303 of the Federal Information Security Management Act of 2002. The act requires NIST among other things, to "develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets."

Within the Computer Security Division, the CSRC provides public access to NIST final and draft reports, the Federal Computer Security Program Managers' Forum, and the work of the three operational groups. It also hosts the National Vulnerability Database.

The National Vulnerability Database

To allow for rapid and open dissemination of new vulnerability data, CVE identifiers contain minimal information about the actual vulnerability.

The National Vulnerability Database (NVD) is intended to allow automation of vulnerability management activities and the production of compliance metrics, as part of the Federal Information Security Automation Program. The NVD provides a standards-based repository, using the Security Content Automation Protocol and standard dictionaries such as the Common Platform Enumeration (CPE) standard. Although it's funded and hosted by the U.S. government, the database is freely accessible and incorporated into many security testing and management tools.

In fact, PCI DSS documentation requires the incorporation of NVD reference data into vulnerability reports.

International Information Systems Security Certification Consortium, Inc. (ISC)²

The **International Information Systems Security Certification Consortium (ISC)²** is a nonprofit professional and certification body that focuses on programs for information security professionals. (ISC)² is one of the largest and

oldest information security qualification organizations in the world.

(ISC)² runs a variety of widely accepted security certifications. Launched in 1989 in the United States, it now claims over 70,000 qualified members in 135 countries. As well as providing certification examinations and training, it hosts monthly e-symposia and coordinates the "Safe and Secure Online" education program for children between 11 and 14.

Since 2004, the organization has been gaining accreditation for its certifications, as well as expanding the range and depth of certifications available. Gradually, the examinations are being moved to an online format through the Pearson VUE network of test centers.

Each (ISC)² qualification requires:

- A set amount of professional experience, from one to five years, requiring endorsement by a current (ISC)² member
- Adherence to the (ISC)² code of ethics
- Self-certification regarding the applicant's criminal record and background
- Completion of a multiple-choice examination

Once qualified, an (ISC)² certification is valid for three years. Certificate holders must pay an annual maintenance fee. They must also complete annual, continuing professional education (CPE) credits.

Certified Information Systems Security Professional (CISSP)

The Certified Information Systems Security Professional (CISSP) is the first (ISC)² certification, launched in 1994. With over 67,000 qualified professionals, this is the must-have qualification in the eyes of many recruiters and human resources (HR) departments.

U.S. DoD Directive 8570

The trend in the information security community is toward increased, verifiable professionalism. A strong driver for the rapid growth in formal security certifications has been the December 2005 introduction of DoD Directive 8750.

In the recently revised and reissued Directive 8750.01M, the U.S. Department of Defense (DoD) requires that anyone with privileged access to departmental information systems obtain and maintain a commercial information security qualification accredited to ISO 17024. This applies to military personnel (regular or reserve) and civilian and contract employees, and is being extended to DoD contractors. Overall, the directive affects an estimated 110,000 people—about the same number as the total certified membership of the two largest certification bodies—(ISC)² and ISACA.

There are 22 qualifications on the basic approval list, which you can find in Appendix 3 of the directive. The approved suppliers are (ISC)², CERT-CC, SANS GIAC, CompTIA, ISACA, and SecurityCertified. The precise qualifications depend on the role(s) you might fill: technical, manager, engineering, or computer network defense. As many as five qualifications or as few as one are currently approved depending on role or level: for the System Architect and Engineer specialization, only CISSP and its concentrations are currently acceptable.

Like the rest of the (ISC)² programs, the CISSP is based on a published Common Body of Knowledge (CBK). The CBK includes several domains, or topic areas. The CISSP examines the following domains, requiring you to have five years of practical experience covering at least two of the domains:

- Access Control
- Application Development Security
- Business Continuity and Disaster Recovery Planning
- Cryptography
- Information Security Governance and Risk Management
- Legal, Regulations, Investigations, and Compliance
- Operations Security
- Physical (Environmental) Security

- Security Architecture and Design
- Telecommunications and Network Security

Criticized in the early 2000s for its focus on U.S. law and jargon, $(ISC)^2$ began a comprehensive internationalization program and now offers the exam in multiple languages based on a comprehensive, internationally relevant question bank.

The exam has 250 questions; candidates have six hours to complete it. This exam format differs from similar certification tests elsewhere in the world, such as in Europe. Nevertheless, at least 138 countries accept the certification. There are, in fact, more than 36 countries with at least 100 qualified CISSPs.

CISSP Concentrations

Although promoted as the gold standard information security certification, the CISSP is a generalist qualification, lacking the depth to assess more detailed areas of knowledge. As a result of industry demand, three concentrations were introduced in 2004:

- CISSP Information Systems Security Architecture Professional (CISSP-ISSAP)
- CISSP Information Systems Security Engineering Professional (CISSP-ISSEP)
- CISSP Information Systems Security Management Professional (CISSP-ISSMP)

Each of these credentials requires the holder to have the CISSP qualification and two years' experience in the relevant discipline. The candidate must also pass an additional three-hour, 125-question exam.

The Architecture and Management concentrations are fully international, with residents of over 40 countries holding each qualification. The Engineer concentration was developed with assistance from the U.S. National Security Agency. Although it's available internationally, it focuses on U.S. laws, regulations, policies, guidelines, and standards. It also addresses U.S. federal government information assurance governance. Accordingly, over 95 percent of ISSEP holders work in the United States, with Canada the only other country to have more than 10 qualified people. Table 15-1 lists the three CISSP concentrations and the CBK domains they cover.

With over 600 holders of each concentration, and especially considering the higher attainment requirements, these qualifications seem to be a moderate industry success. All three concentrations have been ISO 17024 accredited since October 2008. (**ISO 17024** is the international standard for accrediting schemes that certify personal competences.)

Systems Security Certified Practitioner (SSCP)

Introduced in 2001 as a more focused technical certification, the SSCP requires only one year of professional experience and is significantly narrower in scope than the CISSP. The SSCP covers the following seven domains in the CBK:

- Access Controls
- Cryptography
- Malicious Code and Activity
- Monitoring and Analysis
- Networks and Communications
- Risk, Response, and Recovery
- Security Operations and Administration

TABLE 15-1 CISSP concentrations and associated CBK domains.

CISSP CONCENTRATION	CBK DOMAINS COVERED
CISSP-ISSAP	Access Control Systems and Methodology Communications & Network Security Cryptography Security Architecture Analysis Technology-Related Business Continuity Planning (BCP) & Disaster Recovery Planning (DRP) Physical Security Considerations

CISSP-ISSEP	Systems Security Engineering Certification and Accreditation (C&A) Technical Management U.S. Government Information Assurance Governance
CISSP-ISSMP *Note*: The CISSP-ISSMP credential is intended as a higher-level management qualification than the ISACA CISM.	Security Management Practices Systems Development Security Security Compliance Management Contingency Management Law, Investigation, Forensics and Ethics

The SSCP exam has 125 questions for candidates to complete in three hours. It's pitched as a lower-level qualification. As such, it competes against a wide range of vendor technical security certifications, some SANS qualifications, and entry-level certifications such as CompTIA Security+. There are just over 1,000 SSCP certification holders in 50 countries.

The SSCP received ISO 17024 accreditation in 2006.

(ISC)^2 Associate

In November 2001, a 16-year-old Indian boy, Namit Merchant, passed the CISSP exam. A thorough investigation was conducted, and, to general incredulity, Merchant proved he had the then-necessary three years of relevant industry experience. He had started at 13 implementing security controls in financial software for the Bombay-based company Compuware. At the time of the exam, he was still attending high school and working for Network Intelligence India.

Since then, many people have wanted to take the exam while still in school or shortly after completing their education and before gaining the professional experience needed. (ISC)^2 introduced the Associate program in 2003.

Associates pay reduced fees and can take either the CISSP or the SSCP exam; they have time after passing to gain the necessary professional experience. Associate status is considered ISO 17024 accredited, provided that the candidate has passed either of the allowed exams and is working in the relevant area.

Certification and Accreditation Professional (CAP)

This qualification was introduced in 2006 and is aimed at people involved in risk management and accreditation of systems. Although this level of formalization is rare in private companies, it's common in the government and government suppliers sectors internationally. There is now a four-domain CBK, the first two of the initial five having been combined:

- **Initiate the Preparation Phase**—Formerly known as "Certification and Accreditation Process" and "Certification Phase"
- **Perform Execution Phase**—Formerly known as "Accreditation Process"
- **Perform Maintenance Phase**—Formerly known as "Continuous Monitoring"
- **Understand the Purpose of Security Authorization**

The CAP examination comprises 125 questions, and candidates have up to three hours for the exam.

Given the niche nature of this qualification and competing mandatory government qualifications in some countries, the certificate has been relatively successful, with approximately 700 issued. CAP was ISO 17024 accredited in October 2009.

Certified Secure Software Lifecycle Professional (CSSLP)

The most recent (ISC)^2 credential, CSSLP is aimed at a wide sector of the information technology profession, which rarely receives security training or testing. Since September 2008, about 900 project managers, quality assurance testers, technical architects, analysts, developers, and programmers have earned certification. The seven CBK areas are:

- **Secure Software Concepts**—Security implications in software development
- **Secure Software Requirements**—Capturing security requirements in the requirements phase

- **Secure Software Design**—Translating security requirements into application design elements
- **Secure Software Implementation/Coding**—Unit testing for security functionality, resilience after attack, and developing secure code and exploit mitigation
- **Secure Software Testing**—Integrated quality assurance testing for security functionality and resiliency to attack
- **Software Acceptance**—Security implications of the software acceptance phase
- **Software Deployment, Operations, Maintenance, and Disposal**—Security issues around steady state operations and software management

The examination is the standard multiple-choice format, with 175 questions in four hours. This is the pilot qualification for the new online examination and has been available through Pearson VUE centers since April 2010.

Web Application Security Consortium (WASC)

The Web Application Security Consortium (WASC) was founded in January 2004 to compile best practices in securing Web applications, then a relatively new area. The consortium brings together industry and academic experts and major corporations concerned with tools' development and performance. WASC contributes to the open availability of information and methods of attack research. It also contributes significantly to the effort in evaluating and ensuring consistency in the commercially available security automation tools.

WASC Projects

WASC runs a number of projects aimed at improving the distribution of information about Web vulnerabilities. The results of these projects are distributed openly, mostly under the Creative Commons Attribution license, and are available for use in commercial products:

- **The Web-Hacking Incident Database**—A regularly updated database, containing nearly 1,000 records at the time of this writing. This is a Web-accessible, searchable 15-field database describing publicly exploited Web security issues. It's an excellent resource for researchers and security operations teams seeking to justify additional testing or controls.
- **Distributed open proxy honeypots**—A **honeypot** is a carefully monitored system set up by security professionals to be attacked, so that attack sources and methods can be analyzed. The concept of using honeypots to distract hackers became popular in 1999. Open proxies are computers that anonymously accept and forward requests for network services, and they are often used to shield attackers from tracking. Maintaining a suitably attackable Web site honeypot is a difficult and time-consuming exercise. To get around that problem, this project combines the two ideas—running a series of open proxies and allowing their use, while carefully recording and analyzing the traffic for malicious content.

FYI

Open source refers to a copyright or licensing system that, compared with conventional commercial licensing schemes, allows wide use and modification of the material. But not all open source licenses are equal. You need to take considerable care when using open source components in or as a resource for non-commercial and commercial work. Some licenses provide significant flexibility, requiring mere attribution. Others impose onerous conditions, such as requiring that derivative or inclusive work be licensed under identical terms.

- **(Web) Threat Classification**—This provides a detailed and comprehensive dictionary for both Web attack types and target system weaknesses, allowing specific vulnerabilities or incidents to be reliably categorized.
- **Evaluation criteria**—WASC supports two evaluation criteria projects, one aimed at Web application security scanning tools, the other concerned with Web application layer firewalls. Both projects produce detailed lists of expected functionality. Developers can use these criteria to ensure that functionality is comprehensive. Analysts and reviewers regularly use the lists to evaluate the capabilities of competing products.
- **Security statistics**—An annual project collates and publishes sanitized Web site vulnerability data. The latest report (2008) analyzes results from more than 10,000 site reviews, varying from simple Internet scans to white box penetration tests and nearly 100,000 specific detected vulnerabilities. Cross-site scripting issues

and information leakage form the bulk of the detected issues—together comprising nearly three quarters of all issues.

- **Additional projects**—The Web Security Glossary attempts to provide a comprehensive dictionary. The Script Mapping Project tackles the complex interactions between various Web browser versions and implementations and Hypertext Markup Language (HTML) specified "intrinsic events" that can cause script execution.

Open Web Application Security Project (OWASP)

OWASP, like WASC, is an open source community project. Unlike WASC's concentration on automation of testing, OWASP's focus is on educating application developers on security risks. It produces the OWASP Top 10 List, a number of security testing tools and security application programming interfaces (APIs), a range of guidebooks, and the Open Software Maturity Model. You'll learn about these OWASP offerings in this section.

OWASP content and tools can be distributed under any Open Source Initiative approved license. You need to ensure that the license for any tool you wish to use or modify is appropriate for your organization.

OWASP Top 10 List

OWASP maintains a Top 10 list of Web application vulnerability types. These are not specific coding errors but rather more generic groupings of potential flaws. Testing for the OWASP list is mandatory within PCI DSS and has been accepted by the Federal Trade Commission, the DoD, and a large number of government and business organizations in the United States and internationally.

You can read more about OWASP security initiatives on its Web site at *https://www.owasp.org/index.php/Main_Page*.

WebScarab

WebScarab is an application analysis tool for Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) communications. It's written in Java and therefore is relatively platform independent. It's normally used as a recording proxy server, allowing the capture and analysis of Web application data. It will intercept and re-encrypt HTTPS communications, allowing plain language analysis of secure sessions to help to identify weaknesses that would normally be hidden by the encryption.

A large number of plug-in components are available for WebScarab. They allow, for example, automated or manual modification of requests, submitting random data values, and crawling of Web content.

AntiSamy

AntiSamy was inspired by the Samy worm attack against MySpace and its users. It's a downloadable API, available in both Java and .NET, that allows you to automatically filter user-supplied HTML code. Called from your application, the API will strip out potentially malicious content, allowing that code to be incorporated into your Web site.

Four basic configurations are supplied—one based on the filtering policies of the Slashdot Web site, one on eBay, one on MySpace, and one referred to as "anything goes" or "Not even MySpace is _this_ crazy." Any of the configurations can be further tailored to meet your needs. The Java version also implements a range of directives that can further enhance security or improve the appearance of the filtered code.

No PHP version is available because the non-OWASP HTML Purifier tool fulfills an equivalent function.

Enterprise Security API (ESAPI)

Available for a wide range of programming languages, including .NET, PHP, and Java, ESAPI is designed to enable programmers to write more secure code. Specifically, ESAPI enables security to be added to or improved in existing applications. It provides both a set of security control interfaces and a reference implementation for each security control.

WebGoat

WebGoat is a training aid for application developers and testers. Written in Java (J2EE), it guides users through a series of deliberately engineered vulnerabilities that can actually be exploited. Containing over 40 lessons at this writing, it demonstrates HTML comment weaknesses, SQL injection attacks, and cross-site scripting, among

other exploits.

Additionally, one of the project members has produced several online training videos showing practical solutions to a number of the tests.

Open Software Assurance Maturity Model (OpenSAMM)

Originally a separate project, OpenSAMM is derived from the basic structure of the Carnegie Mellon University Software Engineering Institute's Capability Maturity Model.

OpenSAMM uses a 0 to 3 grading structure across four critical business functions, each containing three security practices to rate software development activities. You can learn more about OpenSAMM at *http://www.opensamm.org*.

OWASP Guides

As well as producing documentation for its projects and tools, OWASP produces three core guides:

- *The OWASP Guide to Building Secure Web Applications and Web Services*
- *The OWASP Testing Guide*
- *The OWASP Code Review Guide*

Building Secure Web Applications and Web Services

This guide is aimed at the wide range of the developer community—from architects to auditors. It covers the principles of secure coding and a long list of security objectives and development techniques. It contains specific code examples for PHP, .NET, and Java, although the principles are applicable to any high-level coding language.

Testing Guide

This book covers a wide range of security testing—from manual inspection to penetration testing. It describes a comprehensive testing framework, based around the industry standard Software Development Life Cycle Model. Most of the book is a detailed guide to Web application penetration testing, covering test objectives, methods, and tools for more than 60 different controls groups.

Code Review Guide

Earlier versions of the Testing Guide included information on manual review of code for security flaws. This has been extracted in a separate guide, which covers 16 key testing areas and advice on reviewing standard programming languages and components.

CHAPTER SUMMARY

Large numbers of government, private, and volunteer organizations contribute to the field of information security. National and international organizations set standards. Victims of online attacks and fraud are encouraged to communicate and cooperate by law enforcement, national and industry CSIRTs. Many academic, nonprofit, and commercial organizations provide training and educational materials. Certification and examinations are available in both broad information security disciplines and narrow specializations.

The relationships among these many organizations and security professionals are complex and fluid, but the strength of the international security community is its willingness to share information, best practices, and assistance.

KEY CONCEPTS AND TERMS

Computer incident response teams (CIRTs)
Computer security incident response team (CSIRT)
Common Vulnerabilities and Exposures (CVE) list
Forum of Incident Response and Security Teams (FIRST)
Honeypot

International Information Systems Security Certification Consortium (ISC)²
ISO 17024
Open source

CHAPTER 15 ASSESSMENT

1. Which organization provides incident response support for the federal government?
   A. OWASP
   B. The Secret Service
   C. US-CERT
   D. FIRST
2. Which organizations investigate Internet crime? (Select two.)
   A. MLATs
   B. IC3
   C. ECTFs
   D. OWASP
3. Which of the following standards are governed by NIST? (Select two.)
   A. Advanced Encryption Standard (AES)
   B. ISO 27001
   C. The United States Government Configuration Baseline
   D. CISSP
4. Which of the following are (ISC)² qualifications? (Select three.)
   A. CISM
   B. CISSP
   C. CISSP-ISSEP
   D. Security+
   E. CSSLP
5. You must pass an exam to become an (ISC)² Associate.
   A. True
   B. False
6. Which certification organization is not approved under DoD Directive 8750?
   A. CERT/CC
   B. ISACA
   C. SANS GIAC
   D. FLETC
7. What is the purpose of open proxy honeypots in relation to Internet-based Web attacks?
   A. Silently record for later analysis
   B. Act as deliberate weakened targets for
   C. Obscure the source of
   D. Detect and terminate
8. Roughly how many site reviews were used to generate the most recent WASC Web Security Report?
   A. 5,000
   B. 10,000
   C. 20,000
   D. 100,000
9. ISO 17024 is the international standard for which of the following?
   A. Information security management systems

B. Web application penetration testing
C. Evaluation criteria for IT security
D. Certification programs for personal competence

10. The National Institute of Standards and Technology (NIST) represents the United States in the International Standards Organization.

A. True
B. False