Individual Certification of Security Proficiency for Software Professionals: Where Are We? Where Are We Going?

Dan Shoemaker

January 2009

ABSTRACT: The software industry needs a universally acknowledged credential to document that a software professional has all of the requisite knowledge and skills to produce a secure product. This article describes some of the existing professional certifications in information assurance and emerging certifications for secure software assurance.

INTRODUCTION: REASSURING TRUST

It goes without saying that we should be able to trust people who do life-critical work. That's the reason my MD had to pass the medical boards, my lawyer had to pass the bar exam, and the folks who fly me around the country have commercial pilot's licenses. Formal certification of capability is important in all of their cases because those people do things that require a high degree of public trust. Accordingly, their fundamental capability has to be unquestioned.

Unfortunately however, the only proof of capability that software professionals can offer is the unsubstantiated opinion of their peers. That begs an obvious question, which is "can we trust them?" Or, to put this in more personal terms, when I am at 35,000 feet I would really like to be assured that the people who created my aircraft's avionics system were up to the task.

When the only problem facing the industry was quality, it might have been acceptable to let software people build products, without first finding out whether they were capable. However, we can't afford to be so accommodating now that the exploitation of a single flaw might conceivably bring down our entire cyber infrastructure. That leads us to the thesis of this article: Given the critical importance of software in our society, the software profession has to find a standard, commonly accepted way to attest to the security knowledge of its workforce.

Notwithstanding the fact that national security requires assurance of critical software at an acceptable level of trust, common, industry-wide certification of

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

Phone: 412-268-5800
Toll-free: 1-888-201-4479

www.sei.cmu.edu

individual capability would also be a valuable business asset. Certification would let organizations know the actual capabilities of the people they were hiring. Even better, it would also let companies manage their software work with certainty since they would know in advance who was capable of producing secure products and, more importantly, who was not.

A COMMON PROOF OF SECURITY COMPETENCY FOR SOFTWARE PROFESSIONALS

The key concepts in this discussion are the terms "security" and "commonly accepted." Certification in the computer industry is a very profitable business. In fact, since the 1980s certificates spanning the alphabet from "A+" to "Ubuntu Certified Professional" have become something of a cottage industry in the profession [Webopedia 2008]. That profit motive probably also explains why more than 200 new certificate products were added to an already overpopulated field in the past ten years [IEEE 2008].

Nonetheless, what we are discussing here is the need for a universally authoritative credential to document that a software professional has all of the requisite knowledge and skills needed to produce a secure product. Right now, there are vendor- or product-specific certifications that relate to some aspect of securing a computer, such as networks, operating systems, and even applications [MC MCSE 2008]. The problem is that none of the products on the market right now certifies an individual's knowledge of secure development, sustainment, or acquisition practice [MC MCSE 2008].

The idea of an omnibus certificate of security capability is a relatively new concept in the field of software. However, it is not a new idea in the overall field of information assurance. That is because, over the past 30 years, the professional capabilities of professionals in that field have been underwritten by a number of established credentials. These certifications document that the holder possesses "a common understanding of the concepts, principles, and applications of IA", as certified by that particular certification agent.

INFORMATION ASSURANCE PROFESSIONAL CERTIFICATION EXAMPLES

The certification of competency in information assurance is underwritten by a long list of well-validated and standard certification tests. Vendors on that list

include ISC2, ISACA, SANS, EC-Council, CompTIA, and many others. As examples, some of these certifications are described below.

The Certified Information Systems Security Professional (CISSP)

The CISSP is granted by examination and based on experience requirements [ISC2 2008]. The exam is derived from the CISSP Common Body of Knowledge (CBK), which encapsulates ten domains, or areas of information assurance knowledge. These ten domains are considered comprehensive for information assurance work. Currently, the CISSP certification covers the following ten domains [ISC2 2012]:

1. Access Control
2. Telecommunications and Network Security
3. Information Security Governance and Risk Management
4. Software Development Security
5. Cryptography
6. Security Architecture and Design
7. Security Operations
8. Business Continuity and Disaster Recovery Planning
9. Legal, Regulations, Investigations and Compliance
10. Physical (Environmental) Security

One of the features of the CISSP is the requirement that it must be renewed every three years. That renewal is based on the holder's ability to document 120 Continuing Professional Education (CPE) credits obtained since the previous renewal. These credits are typically derived from formal continuing education conferences.

The Certified Information Systems Auditor (CISA) and the Certified Information Security Manager (CISM)

Both of these are certification products of the Information Systems Audit and Control Association (ISACA). Both certifications are based on knowledge captured in a four domain, control objective based model called COBIT. The four domains of COBIT are [ISACA 2008b]

1. Planning and Organization
2. Acquisition and Implementation
3. Delivery and Support
4. Monitor

Each of the 34 high-level control processes that comprise these domains is implemented by anywhere from 3 to 30 specific control objective activities, amounting to 318 total standard activities specified for control of IT and information assets [ISACA 2008b].

The CISA is the more common of the two certificates since it predates the CISM by 25 years. Because the focus of both certificates is on explicit and documentable controls rather than best practices for security, the CISA in particular has more of an accounting and business flavor than the technical and practitioner feel of the CISSP. Like the CISSP, however, the CISA documents a specific set of skills and practices oriented toward ensuring the confidentiality, integrity, and availability of information. On the other hand, the CISM certification is oriented toward the assurance of information itself.

The CISA was introduced in 1978, while the CISM was introduced in 2003 [ISACA 2008a]. As the name implies, the CISM is designed for managers, designers, and overseers of an organization's overall information security program. Thus, the knowledge and competencies certified by the CISM are more oriented toward the fulfillment of the management responsibilities for information assurance rather than the technical aspects of the profession.

The SANS Global Information Assurance Certification (GIAC)

Like the CISSP, GIAC is a practitioner certificate designed to validate real-world skills. Its intent is to "provide assurance that a certified individual has practical awareness, knowledge and skills in key areas of computer and network and software security" [SANS 2008].

The GIAC is much more of a technical credential than the CISSP and the CISA/CISM. Also, the GIAC specifically documents capabilities for more than 20 types of professional areas [SANS 2008]. So in that respect the GIAC is more a series of potential certifications that an individual can earn rather than a general-purpose certification of information security knowledge. This fact should be kept in mind in the discussion in the next section.

EC-Council Certification (C|EH, C|HFI, C|CSA, L|PT, E|NSA)

The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in various e-business and information security capabilities. Its most recognizable product might be the Certified Ethical Hacker (CEH) credential. However, it also offers Certified Forensics Investigator (CHFI), EC-Council Certified Security Analyst (ECSA), and License Penetration Tester (LPT) certifications [ECC 2012].

These certifications are recognized worldwide in the sense that they have received endorsements from the agencies of various governments around the globe, including the US Federal Government. That endorsement was given substance through the inclusion of the Certified Ethical Hacker certification program within Directive 8570. In that regard, EC-Council satisfies DoD requirements for four personnel categories of Computer Network Defender (CND) service providers: analysts, infrastructure support, incident reporters, and auditors [Mont 2010].

The EC-Council certificates are similar to the SANS GIAC in that they provide substantive certification for a specialized area of expertise. The areas are concentrated in the technical specialties of information assurance, certified ethical hacker, certified computer hacking forensics investigator, certified security analyst, licensed penetration tester, and certified network security administrator. In that respect, EC-Council certificates address specific areas of need in the profession. One area is secure programming, and that should be noted when reading the next section.

CERTIFICATIONS FOR THE FIELD OF SECURE SOFTWARE ASSURANCE

More recently, we have observed an increase in training courses and certifications for secure software development. It is not surprising that some of the same organizations with certification products in information assurance would migrate into the field of software assurance. At present, three certifications are being developed for two different client bases in the secure software assurance community. These are the CSSLP (ISC2), which should appeal more to lifecycle managers, and the EC-Council Certified Secure Programmer (CSP) and the SANS secure coding assessment, which should appeal more to programmers themselves.

Certified Secure Software Lifecycle Professional (CSSLP)

The CSSLP parallels the CISSP in that it takes a holistic view of the entire process of software development. As such, it is a general assessment of an individual's general security competency across the software life cycle. Like the CISSP, the CSSLP assesses breadth of knowledge rather than depth in any particular area. The CSSLP is based on a set of general best practices for secure software assurance, which are organized into seven domains [ISC2 2008]:

1. Secure Software Concepts - security implications across the life cycle
2. Secure Software Requirements – how to elicit security requirements

3. Secure Software Design – how to embed security requirements in design
4. Secure Software Implementation/Coding - security functionality testing, secure code development, attack and exploit mitigation
5. Secure Software Testing - testing for robustness and security functionality
6. Software Acceptance – getting security into the software acceptance phase
7. Software Deployment, Operations, Maintenance and Disposal – how to securely sustain software throughout its useful life cycle

Like the CISSP, practitioners have to prove that they have three or four years of professional experience in secure software work. The proof of competence comes from a qualifying exam that is administered similar to that of the CISSP. In addition, once the CSSLP has been granted to an individual, the certification must be maintained through continuing education [ISC2 2008].

Like the CISSP, the CSSLP is an attestation to a broad range of minimum competencies in secure software work, rather than in-depth substantiation of mastery in some particular aspect of that work.

The SANS Secure Coding Assessment

The SANS Secure Coding Assessment, which is a part of the overall SANS Software Security Institute certification, is designed to certify that the holder has the requisite set of skills in secure coding. In this case, the objective is for the holder to achieve GIAC Secure Software Programmer (GSSP) Certification. This is done through an exam process similar to the ones utilized by SANS in the information assurance areas.

That is, rather than being a general assessment, these exams are tailored to specific applications. In the case of the basic GSSP, it is possible for holders to be certified in four specific programming languages. These are C/C++, Java/J2EE, Perl/PHP, and .NET/ASP [SANS 2008]. As with the other certifications, holders of the GSSP have to recertify, in this case every four years. Current holders have to pass the test that is being utilized at the time of their recertification [SANS 2008].

According to SANS, these tailored certifications will help organizations meet four objectives [SANS 2008]. First, the exam can serve as a yardstick by which an organization can measure the individual security knowledge of its programmers. That knowledge can then be leveraged into focused training for each person. Second, the exam will also allow the organization to ensure that any outsourced work is done by programmers who have a requisite level of security knowledge. Third, it will help an organization structure its hiring processes to

ensure that people who are brought into the organization are competent to start work on day one, without additional costly training. Finally, it will allow organizations to make more effective and efficient project assignments by identifying individuals with advanced security skills.

Given SANS's traditional focus on technology, the desired effect of this certification will be to provide attestation to the holder's ability to avoid or find and fix common errors that lead to security vulnerabilities in each of the languages in which they are certified. That will allow managers to ensure a base level of security knowledge in each project, and it will also help employers more objectively evaluate potential candidates for employment. Finally, it should also serve as a comparative basis for those organizations with a large proportion of GSSPs on their staff, to prove their worth when competing for business.

EC-Council Certified Secure Programmer

The aim of the EC-Council's Certified Secure Programmer and Certified Secure Application Developer credentials is to "provide the essential and fundamental skills to programmers and application developers in secure programming" [ECC 2012]. According to the EC-Council the Certified Secure Programmer provides the basic foundation needed by all application developers and development organizations to produce applications with greater stability and which pose lesser security risks to the consumer. The Certified Secure Application Developer standardizes the knowledge base for application development by incorporating the best practices followed by experienced programmers into a single lifecycle certificate.

The Certified Secure Programmer and Certified Secure Application Developer certificates are not language or architecture specific. They certified that the person holding them can "exercise secure programming practices to overcome inherent drawbacks in code" [ECC 2012]. According to the EC-Council, the distinguishing aspect of ECSP and CSAD is that, whether vendor- or domain-specific certification, it "exposes the aspirant to various programming languages from a security perspective" [ECC 2012].

People becoming EC-Council Certified Secure Programmers (ECSP), must pass the EC-Council's Certified Secure Programmer exam. The EC-Council Certified Secure Application Developer (CSAD) requires two certificates. First the application must get an application development certification from any one of the four EC-Council's recommended vendors: Microsoft, Sun, Oracle, or IBM; then they must pass EC-Council's Certified Secure Programmer exam.

Common Things a Software Security Professional Needs to Know

One obvious question is "what are the common attributes in all of these certifications?" Or, more specifically, what are the common/general requirements critical to assess the ability of software security professionals? The most practical way to answer that question is to simply compile an unduplicated list of the knowledge categories of the bodies of knowledge (BOK) of the four certification groups. That compilation reveals 22 potential learning/certification areas:

1. Secure Software Concepts (CSSLP), Introduction to Secure Coding (E/CES)
2. Secure Software Requirements (CSSLP)
3. Secure Software Design (CSSLP), Designing Secure Architecture (E/CES)
4. Secure Software Implementation/Coding (CSSLP)
5. Cryptography (GSSP, E/CES)
6. Buffer Overflows (E/CES)
7. Secure Software Testing Secure Application Testing (CSSLP)
8. Application Faults & Logging (GSSP)
9. Authentication (GSSP)
10. Authorization (GSSP)
11. Common Web Application Attacks (GSSP)
12. Data Validation (GSSP)
13. Language and Platform specific knowledge (GSSP, E/CES)
14. Software Acceptance (CSSLP)
15. Software Deployment, Operations, Maintenance and Disposal (CSSLP)
16. Secure Network Programming (E/CES)
17. Writing Exploits (E/CES)
18. Programming Port Scanners and Hacking Tools (E/CES)
19. Secure Mobile phone and PDA Programming (E/CES)
20. Secure Game Designing (E/CES)
21. Securing E-Commerce Applications (E/CES)
22. Software Activation, Piracy Blocking, and Automatic Updates (E/CES)
23. Writing Secure Documentation and Error Messages (E/CES)

Some of these are clearly high-level considerations (1, 2, 3, 7, 9, 10, 14, 15, and 23). Other elements have a low-level focus on specific concerns (5, 6, 8, 11, 12, 16, 17, 19, 20, 21, 22, and 23). Finally, there are a large number of language- and platform-specific considerations, which are folded into a single category (13). Given the diversity and broad range of these potential areas of knowledge, the actual certification process would have to be tailored to the situation. However, it

might be fair to conclude that most of the knowledge requirements for the profession are embodied in this group of 22 areas.

CONCLUDING REMARKS

The problem of understanding the huge variety of certificates represents one of the chief hazards in using information assurance certification as a proof of capability. Because there are so many certificates and because they mean different things, it is difficult for the general population to tell what they are getting when they hire a CISA versus a CISSP, or a Security Plus versus a GIAC. Thus the National Initiative for Cybersecurity Education (NICE) was created to establish an "operational, sustainable and continually improving cybersecurity education program for the nation" [NIST 2010].The National Institute of Standards and Technology (NIST) provides the leadership for NICE. The overall aim of the NICE program is to ensure, coordination, cooperation, focus, public engagement, technology transfer and sustainability. NICE provides a definition of roles for secure software professionals in Area One, Securely Provision, of its model. This area contains a range of software engineering functions and associated knowledge, skills, and abilities (KSAs). These KSAs represent a solid first attempt to create a single point of reference for understanding the range of professional certifications, since those KSAs can be mapped directly to the knowledge requirements of each certification. In that respect, it is possible to tell for the first time which certificate would satisfy which standard job role in the field.

In the same vein, the Department of Defense has issued a revision to DoD 8570.01-M [DoD 2008]. DoD 8570 specifies the knowledge and certification requirements for the employees of the Department of Defense. This directive is important because it requires every full- and part-time military service member, defense contractor, civilian, and foreign employee with privileged access to a DoD system to obtain a commercial certification credential. In that respect, it is the first example of an across-the-board standardization of competency for security. Because the commercial credential must be certified to ISO/IEC 17024 [ISO/IEC 2003] in order to be valid, DoD 8570 ensures that employees of the Department of Defense all fit within a commonly accepted framework for workforce capability. However, 8570 only deals with competencies for the general field of information assurance.

With NICE and DoD 8570, governmental and industry leaders have begun to characterize the global knowledge and skills necessary to ensure proper software engineering work. However, NICE is still a work in progress and DoD 8570 is limited to one area of government. Therefore, given the volatility of the stand-

ards development process, it is not clear whether either of these represents the future of software security certification. It is clear that the current NICE workforce framework addresses many good things, but there are also some clearly important areas that it does not address, for example, secure supply chain and acquisition management. More importantly, most of the 22 specific knowledge areas listed in the section above are really not addressed. Nonetheless, because NICE is still a work in progress, it is not too late to include considerations of those issues; and the KSA structure of the knowledge areas lends itself to making dynamic changes.

Though the NICE model does not specifically address the skill set needed to ensure secure programming competency, this model is a start. Given the history of certification, it would be far preferable to have an explicit specification of the knowledge skills and abilities required to ensure secure code in hand before the secure software certification training landscape becomes a wilderness. Whether NICE will be able to provide that specification is yet to be determined.

BIBLIOGRAPHY

[DHS 2008]

Department of Homeland Security. "IT Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development," Sept. 2008.

[DoD 2008]

Department of Defense. "DoD 8570.01-M, Information Assurance Workforce Improvement Program," December 19, 2005; Revised, May 15, 2008.

[ECC 2012]

EC-Council, EC-Council at a Glance. Accessed 3/2012.

[IEEE 2008]

IEEE. "CSDP, Is Certification Right for You? Certification Road Map: The Journey and the Destination." IEEE Computer Society, 2008.

[ISACA 2008a]

Information Systems Audit and Control Association (ISACA). "Certification Overview." ISACA, Oct. 2008.

[ISACA 2008b]
Information Systems Audit and Control Association (ISACA). “Control Objectives for IT (COBIT).” ISACA, Oct. 2008.

[ISC2 2008]
International Information System Security Certification Consortium (ISC2). “CSSLP –Certified Secure Software Lifecycle Professional," Nov. 2008.

[ISC2 2012]
International Information System Security Certification Consortium (ISC2). “CISSP Domains,” accessed 4/2012

[ISO/IEC 2003]
International Standards Organization/International Electronics Commission. ISO/IEC 17024 - General Requirements for Bodies Operating Certification of Persons, April 2003.

[MC MCSE 2008]
MC MCSE. “Certification Resources,” 2008.

[NIST 2010]
National Institute of Standards and Technology, “National Initiative for Cybersecurity Education,” May 2010, accessed 4/2012

[SANS 2008]
SANS. “GIAC Secure Software Programmer,” 2008.

[Schneider 2008]
Schneider, Laura. “CSSLP – The Certified System Security Lifecycle Professional,” About.com, 2008.

[Webopedia 2008]
Webopedia. “Computer Certifications,” Sept. 17, 2008.

[Wikipedia 2008]
Wikipedia. “Certified Information Systems Security Professional (CISSP),” 2008.

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM-0001120