© iStockphoto.com/alxpin

International Secure Software Engineering Council (ISSECO)

by Petra Barzin

Certified Professional for Secure Software Engineering

Secure Software Engineering

Security concerns at the application level are a growing risk to the IT community and one of the biggest challenges for IT security in the next years. Security vulnerabilities are not limited to a few products, but affect almost all vendors and products available on the market. Although the vendors provide security patches free of charge, the roll-out of patches produces extra costs and bears the risk of new security vulnerabilities and critical incompatibilities in complex IT environments. The everlasting race against time to find security vulnerabilities before an attacker will find them or before published exploits can cause any harm before security patches are available does not seem to be the best approach to gaining confidence in the security of software. In order to win the race, the real causes of security vulnerabilities rather than their effects must be eliminated.

Security vulnerabilities may be exploited in order to steal critical company data, to distribute viruses and worms or to "rat" computer systems. Firewalls or Intrusion Detection Systems are no longer sufficient to avert danger, because they cannot prevent attacks on the applications themselves. I.e. a firewall cannot decide whether an input parameter is valid or implies a "code injection" attack. This decision can only be made by the particular application itself. Consequently, possible attacks must already be eliminated during the development of the application. Unfortunately, security aspects in the software development life cycle usually do not receive enough attention at the universities or later in the day-to-day business of software engineering in order to counter security vulnerabilities at an early stage when they are emerging.

Secure software development demands security-conscious and well-educated software architects and developers. Today, this type of qualification that attests the very best skills to produce secure software is missing. ISSECO aims at filling this gap of qualification by providing an international personnel certification standard for secure software engineering.

ISSECO Education and Certification

The scope of ISSECO is the education of people involved in the software development life cycle. The education covers all topics relevant in the area of software development. Excluded are safety matters such as perimeter and infrastructure security. Furthermore, information security management as well as cryptography are out of scope for the ISSECO foundation level, but might be addressed by further advanced level certifications (cf. section 4 ”Future prospects”). Also, ISSECO does not perform security assessments of processes or IT products.

This personnel certification addresses everyone who is directly involved in the software development life cycle, i.e. requirements engineer, software architect, designer, developer, software quality manager, software tester, project manager and all related software development stakeholders.

No formal entry qualifications - such as work experience or university degree - are required to take an ISSECO training course and the examination. However, some knowledge of information technology and basics in quality assurance are expected from a candidate for Certified Professional for Secure Software Engineering.

Current accredited ISSECO training providers who offer training seminars for the Certified Professional for Secure Software Engineering include Diaz&Hilterscheid, Fraunhofer Institute IESE, Secorvo, Secunet, SQS, and VirtualForge. Other training providers that choose to support the Certified Professional for Secure Software Engineering in the future must be accredited by the ISSECO board.

ISSECO training providers and ISSECO examination providers must be independent from each other. All candidates for Certified Professional for Secure Software Engineering must take their exams at the International Software Quality Institute (iSQI).

ISSECO Syllabus

Software security is not a test case before deploying an application, and it is not an add-on feature of software. Software security is an integral component of every phase in the whole software development life cycle. Thus, the structure of the ISSECO syllabus is based on the different phases of the software development life cycle.

At the beginning the view of the attacker and of the customer need to be understood in order to be able to create secure software. In order to see with the eyes of the enemy, the Certified Professional for Secure Software Engineering must know the motivations of hackers, their skill level and resource situation, as well as typical hacker thinking when attacking systems. Furthermore, the Certified Professional for Secure Software Engineering must have understood what customers expect in terms of software security and why, in order to classify the customers' requirements. Describing use cases of the customer, his assets, threats and risks helps to avoid security conflicts which may arise when a customer has a different use case in mind than the software architects and developers.

Next, the Certified Professional for Secure Software Engineering must have a basic understanding of the different trust and threat models. Understanding the assets and its threats is a key element of threat modeling. Since threat models help to define the security objectives of an application, the Certified Professional for Secure Software Engineering must be familiar with the different threat models. In contrast to threat models, there are various access control models that describe how to constrain the ability of a subject to access or generally perform some sort of operation on an object. It's important to have these trust models in mind when designing an application as Certified Professional for Secure Software Engineering.

Furthermore, the Certified Professional for Secure Software Engineering must feel comfortable with the methodologies for secure software development. These methodologies describe the processes and practices associated with producing secure software. Processes that consistently produce secure software do not require any particular design, development, testing, or other methods. They can be applied to any development methodology or life cycle model.

The Certified Professional for Secure Software Engineering must understand the impact of security on all phases of the software development life cycle, i.e. security requirements engineering, secure design, secure coding, security testing, and secure deployment. Security must be incorporated already at the very beginning of the software development life cycle. In the requirements engineering phase the Certified Professional for Secure Software Engineering must focus on developing security requirements for the respective application. There are lots of different areas where requirements originate, and many of them are relevant to security.

Since architectural and design-level errors made in the design phase are the hardest vulnerabilities to fix and in most cases difficult to defend, the security principles and security design patterns must be well understood by the Certified Professional for Secure Software Engineering. Security architecture and design reviews help to identify problems in the application design and to discover possible vulnerabilities. Thus, at design reviews the Certified Professional for Secure Software Engineering must be able to focus on the areas of the application that have the most impact on security.

Secure coding implies that the Certified Professional for Secure Software Engineering understands which programming errors lead to vulnerabilities like Cross-Site Scripting (XSS) or injection flaws. All vulnerabilities are introduced by so-called vulnerability patterns, e.g. buffer overflow, race conditions or improper error handling. The Certified Professional for Secure Software Engineering must be able to identify, avoid and remediate them.

During security testing the Certified Professional for Secure Software Engineering verifies whether all security requirements are met and all mitigation techniques are effective. Therefore the test techniques of security testing and the correct interpretation of security testing results must be understood .

Even if security issues were considered at the initial stages of the software development and secure design and coding practice were applied during development, the security implications of deployment are often overlooked. Vulnerabilities may still arise during this final phase. Thus, a secure deployment is another concern of the Certified Professional for Secure Software Engineering as it is important for the success of the whole software development life cycle.

Once the software has been deployed, the Certified Professional for Secure Software Engineering is concerned with the implementation of a security response process in order to make sure that security issues in software installations are fixed and communicated responsibly.

Security metrics aim to quantify the security of an application. Security is a horizontal topic that involves every stakeholder, has an impact on many features, and has to be considered by the Certified Professional for Secure Software Engineering throughout the complete software development life cycle.

Last but not least, code and resource protection is a security concern of the Certified Professional for Secure Software Engineering, in order to assure the quality of software and protect it from external sabotage.

Future prospects

Besides the ISSECO foundation level certification there will be additional advanced levels, which will be defined at a later date. These advanced levels may address programming language specific security matters, IT security management or other topics. There might also be a security auditor training for assessing software development with respect to security.

Petra Barzin, Diplom-Informatikerin (computer scientist) graduated in computer science at the Darmstadt University of Applied Sciences in 1995. From 1995 until 1999 she worked at GMD (aka FhG) in the research area of Security and Smartcard Technologies. In 1999, she changed to a leading German vendor for Public Key Infrastructures (PKI) solutions where she was head of the security consulting team for four years. Afterwards she switched into product management and was responsible for the development of some selected security products.
Since October 2004 she has been working as a Security Consultant at Secorvo Security Consulting GmbH.
Petra Barzin has many years of experience in the fields of Public Key Infrastructures, secure e-mail solutions, secure Internet e-commerce protocols, Single-Sign-On, electronic signatures and compliance to the German Digital Signature Act. Petra Barzin is a certified ISC2 Information Systems Security Professional (CISSP).