SKILLS AND CERTIFICATIONS

A New Qualification to Guarantee Secure Software Engineering Skills

Petra Barzin

Why Secure Software Engineering?

Security at the application level is a growing concern and one of the biggest challenges that will face the IT community over coming years. Although vendors provide security patches free of charge, their roll-out produces extra costs and brings with it the risk of new security vulnerabilities and critical incompatibilities in complex IT environments. The constant race against time to identify security vulnerabilities before an attacker finds them, and to publish security patches before published exploits can cause harm is not the best approach to bolster confidence in the security of software. In order to win the race, the real cause of security vulnerabilities – rather than their effect – must be eliminated.

A firewall cannot distinguish between a valid input parameter and a 'code injection' attack. This distinction can only be judged at the level of the application itself. So possible attacks could be eliminated earlier, i.e., during the application development phase. Unfortunately, insufficient attention is usually paid to security aspects in the software development lifecycle in university-level curricula, or later in the day-to-day business of software engineers, in order to counter security vulnerabilities in software as they are emerging.

Secure software development demands security-conscious and well-educated software architects and developers. There is need for qualifications demonstrating that a person possesses the necessary skills to develop secure software.

The International Secure Software Engineering Council (ISSECO – www.isseco.org) aims to fill this gap by providing an international personnel certification standard for secure software engineering.

ISSECO deals with the education of people involved in the software development lifecycle. This new personnel certification is aimed at everyone who is directly involved in the software development lifecycle, including requirements engineers, software architects, designers, developers, software quality managers, software testers, project managers and all related software development stakeholders.

The ISSECO syllabus

The structure of the syllabus is based on the different phases of the software development lifecycle.

The first step in creating secure software is to understand the attacker and the customer. In order to see with the eyes of the enemy, *Certified Professionals for Secure Software Engineering* must appreciate the hackers' motives, their skills and resource situation, as well as typical hacker thinking when attacking systems. In addition, *Certified Professionals* must have understood why and what customers expect in terms of software security in order to be able to classify customers' requirements.

Next, *Certified Professionals for Secure Software Engineering* must have a basic understanding of the different trust and threat models. In contrast with threat models, there are various access control models that describe how to constrain the ability of a subject to access or perform some sort of operation on an object.

Certified Professionals for Secure Software Engineering must also feel comfortable with the methodologies for secure software development. 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 lifecycle model.

Security must be incorporated from the very beginning of the software development lifecycle. In the requirements engineering phase *Certified Professionals* should focus on developing security requirements for the respective application. There are numerous different sources of requirements and many of them are relevant to security.

Because architectural and design-level errors made during the design phase are the hardest vulnerabilities to fix and the most difficult to defend against, security principles and security design patterns must be well understood. At design reviews *Certified Professionals* must be able to focus on the areas of the application that have the most impact on security.

The creation of secure coding requires an understanding of which programming errors lead to vulnerabilities such as 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. *Certified Professionals for Secure Software Engineering* must be able to identify, avoid and remedy all of them.

During security testing *Certified Professionals* will have to verify whether all security requirements are met and that all mitigation techniques are effective. They must therefore understand the test methods of security testing and how to interpret the results.

Even when security issues are considered at the initial stages of software development and secure design and coding practice are applied during development, the security implications of deployment are often overlooked. Much vulnerability may still arise during this final phase. Thus, secure deployment is another important concern.

Once the software has been deployed, the focus shifts to 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 serve to quantify the security of an application. Security involves every stakeholder, has an impact on many features and must be considered by *Certified Professionals for Secure Software Engineering* throughout the complete software development lifecycle.

Last but not least, the correct use of code and resource protection will assure the quality of software and protect it from foreign sabotage.

Future prospects

Besides the foundation level certification, further advanced levels are planned to be defined later. These advanced levels may address security matters specific to a programming language, IT security management or other topics. In the future, ISSECO is also considering offering security auditor training for assessing software development with respect to security.

Petra Barzin (petra.barzin@secorvo.de) works for Secorvo Security Consulting and is one of the Vice Presidents of ISSECO.