

Security Sessions Bergen Congress Center April 27-29

Tuesday 28. April
9:00 - 12:00



Pravir Chandra

The Software Assurance Maturity Model

SAMM <www.opensamm.org> is a flexible and prescriptive framework for building security into a software development organization. Covering more than typical SDLC-based models for security, SAMM enables organizations to self-assess their security assurance program and then use recommended roadmaps to improve in a way that's aligned to the specific risks facing the organization. Beyond that, SAMM enables creation of scorecards for an organization's effectiveness at secure software development throughout the typical governance, development, and deployment business functions. Scorecards also enable management within an organization to demonstrate quantitative improvements through iterations of building a security assurance program. This workshop will introduce the SAMM framework and walk through useful activities such as assessing an assurance program, mapping an existing organization to a recommended roadmap, and iteratively building an assurance program. Time allowing, additional case studies will also be discussed. SAMM is an open a free project and has recently been added under the Open Web Application Security Project (OWASP).

13:30 - 16:30



Gary McGraw

The Building Security In Maturity Model

As a discipline, software security has made great progress over the last decade. There are now at least 25 large scale software security initiatives underway in enterprises including global financial services firms, independent software vendors, defense organizations, and other verticals. In 2008, Brian Chess, Sammy Migues and I interviewed the executives running nine initiatives using the twelve practices of the Software Security Framework <www.informit.com/articles/article.aspx?p=1271382> as our guide. Those companies among the nine who graciously agreed to be identified include: Adobe, The Depository Trust and Clearing Corporation (DTCC), EMC, Google, Microsoft, QUALCOMM, and Wells Fargo. The resulting data, drawn from real programs at different levels of maturity was used to guide the construction of the Building Security In Maturity Model. This talk will describe the maturity model, drawing examples from many real software security programs. A maturity model is appropriate because improving software security almost always means changing the way an organization works ---people, process, and automation are all required. While not all organizations need to achieve the same security goals, all successful large scale software security initiatives share common ideas and approaches. Whether you rely on the Cigital Touchpoints, Microsoft's SDL, or OWASP CLASP, there is much to learn from practical experience. Use the software security maturity model to determine where you stand and what kind of software security plan will work best for you.

Monday 27. April

13:00 - 14:00



Lars-Helge Netland
Black Swans in Computer Security

Risk mismanagement is one of the underlying causes of the current financial crisis. Assisted by sophisticated models for measuring risk, some of the worlds largest corporations exposed themselves to huge downside risks. What can computer security professionals learn from the excessive risk taking in the financial industry? This talk explores hard-to-predict and large-impact events in computer security.

14:00 - 16:00



Gunnar Ugland
Recent Coorporate Security Issues

A peak into what security issues trouble corporations these days, statistics/facts and a look at some recent events

Wednesday 29. April

9:00 - 11:30



Martin Knobloch
Application Security - Awareness

What is a secure application? What have we to be aware of? During this interactive session, causes of unsecure software applications will be discussed. Next to an introduction of OWASP.org, common security vulnerabilities are demonstrated, as listed in the OWASP Top Ten list, using the OWASP WebGoat and WebScarab tooling.

In experience report session from 9:00 - 11:30



Gaute Småland
Security in heterogeneous environments

State of enterprise security in medium to large organizations. Planning security: What, why and how? Introducing the "Enterprise security maturity thermometer", a tool that aspires to quickly enable measuring of the state of the security architecture of an organization.