André Post:
Short bio

Andre Post is a security architect and developer who sees it as his goal to raise the current level of security in the fields of software development and code reviewing.

Before starting his current career at Fox-IT, Andre worked several years for Symantec performing anti-virus research, software development, security training, and press events. Andre later pursued his own business, applying and expanding his security, development, and operating systems administration skills. Today, Andre works for Fox-IT on a variety of projects including core product development, software architecting, security code reviews, and software project management. To contact Andre, please visit the Fox-IT website at http://www.fox-it.com

Practices of developing optimal security

Methods such as SDLC attempt to provide guidelines that improve the security of software development. However, even armed with knowledge of these methods, completing software development projects that are successful both functionally and in terms of security proves to be a serious challenge. This presentation highlights a number of current practices that lead to sub-optimal security, and suggests ways of avoiding these problems, focusing on the technical side of development. The following subjects will be addressed:
*) Why do so many software projects fail?
*) Examples: Web site, secure hash implementation, e-mail address input validation
*) Addressing team-level factors
*) Helping developers write better code
*) Making software modules work together safely
*) Q & A

Erik Poll:
Short bio

Erik Poll is head of the group Security of Systems (SoS) at the Radboud University, where he is employed since 1999. After his promotion at the TU of Eindhoven, he worked at INRIA in France and the University of Canterbury in England. His research does concentrate on the security and correctness of software, in special Java, and mainly for smartcards and mobile phones.

Problems of developing secure and correct applications

In spite poorly developed software was the reason for all sort of security problems for decennia, only recently software security got recognised as an important point of attention for the IT world, but not by far the recognition should deserve (e.g. inside educational programs).

This presentation will point out different possibilities to improve software security. This by our own experiences gained from the research and from the collaborating businesses where

security has more recognition, then it is the case on average level. I will also talk about the difficulties to get sufficient time and money to spend on security. Something not only the case for software development, but also, for example, for the development of programming languages.

Dr. Rix Groenboom

Short bio

Rix Groenboom supports fortune 2000 companies in field automated software error prevention and correction for Parasoft. His main area of expertise is in the use of formal languages for the specification, design and validation of software applications. Using this knowledge, Rix Groenboom has written over 30 technical articles and presented on Open Source and quality of software development issues at many IT industry conferences in Europe and USA. He holds a MSc and PhD in Computing Science from the University of Groningen (the Netherlands) and published his thesis that focused on the formalization of domain knowledge.

Protecting Web services and Web applications against security threats

---

When exposing business information and operations via Web services, you must ensure that each part of your system is reliable, and that all parts interact flawlessly and securely.

There are numerous threats that can compromise the confidentiality, integrity, or availability of a Web service or the back-end systems that a Web service might expose. Some of these threats are shared with conventional Web application systems (or Web sites), while others are specific to Web services.

During this session, we will explore how to implement development and security best practices in the code to make sure that your web- services and applications perform solidly when they are being hacked or used in malicious ways.