

TECHNOLOGY TRANSFER PRESENTS

KEN  
**VAN WYK**

---

**SECURE CODING:**

---

**Building Secure**

---

**Web Applications**

---

**in Java/J2EE**

---

**NOVEMBER 3-5, 2008**  
RESIDENZA DI RIPETTA - VIA DI RIPETTA, 231  
ROME (ITALY)



info@technologytransfer.it  
www.technologytransfer.it

## ABOUT THIS SEMINAR

This class starts with a description of the security problems faced by today's software developer, as well as a detailed description of the Open Web Application Security Project's (OWASP) "Top 10" security defects. These defects are studied in instructor-lead sessions as well as in hands-on lab exercises in which each student learns how to actually exploit the defects to "break into" a real Web application. (The labs are performed in safe test environments.)

Remediation techniques and strategies are then studied for each defect. Practical guidelines on how to integrate secure development practices into the software development process are then presented and discussed.

### WHO SHOULD ATTEND

The ideal student for this tutorial is a hands-on Web application Developer or Architect who is looking for a fundamental understanding of today's Best Practices in secure software development:

- Software Testers
- Software Developers
- Development and Test Managers
- Security Auditors and anyone involved in software production for resale or internal use will find it valuable
- Information Security and IT Managers
- Information Assurance Programmers
- Information Security Analysts and Consultants
- Internal Auditors and Audit Consultants
- QA Specialists

### REQUIREMENTS

Each student will need to provide a laptop computer for the hands-on lab exercises. Recommended configurations include the following:

- Windows, Linux, or Mac OS X
- Local administrative privileges for installing and configuring software
- Java development environment (Sun SDK and Eclipse IDE recommended, although other SDKs and IDEs will work)
- Approximately 5 gigabytes of available disk space
- 1 gigabyte of RAM is recommended

## 1. Preparation Phase:

### Understanding the problem

- What are the issues that result in software that is susceptible to attack?
- Why do software developers continue to develop weak software?

### 2. Overview of available solutions

- Top-level discussion of Best Practices for developing secure software
- Security activities that can be integrated throughout a typical software development lifecycle

### 3. Lab setup and demo

- Students install and configure software tools to be used in the upcoming exercises
- The instructor demonstrates the tools and runs through a sample exercise to ensure all students can use the tools correctly
- Review of Web application basics
  - HTTP methods (e.g., GET, POST)
  - Identification and authentication
  - Session Management

### 4. Exploiting Web application weaknesses

- Introduction to OWASP top 10 (and other) security weaknesses in Web applications
- How do attackers exploit these weaknesses?
- Class exercises of the most common Web application weaknesses

## 5. Secure development processes

- A detailed look at three common secure development methodologies, and their strengths and weaknesses
  - Microsoft's SDL
  - Cigital's Touchpoints
  - OWASP's CLASP
- Group discussion of the feasibility of the processes

### 6. Introduction to Design Review exercise

- Group exercise to review an example of a flawed design for security weaknesses

### 7. Processes in depth: Design Review

- Architectural risk analysis in detail
- Attack resistance
- Ambiguity analysis
- Weakness analysis
- Compare and contrast common processes for reviewing designs

### 8. Architectural and Design exercises

- Team exercise to review a flawed design using the processes described
- Abuse cases and design flaws

### 9. Processes in depth: Static code analysis

- Description of static code review processes
- Automated vs. peer review comparison of benefits and weaknesses
- Background of available automated static code review tool technology

- Integrating a static code review tool into a software development process effectively

### 10. Static code analysis exercise

- Group exercise in which a simple program is analyzed using a commercial static code analysis tool
- The results are reviewed and analyzed by the class
- Group discussion about how to best utilize a static analysis tool

### 11. Processes in depth: security testing

- Black box vs. white box security testing of software
- Overview of common testing methodologies and tools
- Penetration testing
- Fuzz testing
- Dynamic validation

### 12. Getting started

- Key elements to succeeding with a software security initiative
- Developing an action plan
- First steps

## INFORMATION

<p><b>PARTICIPATION FEE</b></p> <p>€ 1500</p> <p>The fee includes all seminar documentation, luncheon and coffee breaks.</p> <p><b>VENUE</b></p> <p>Residenza di Ripetta Via di Ripetta, 231 Rome (Italy)</p> <p><b>SEMINAR TIMETABLE</b></p> <p>9.30 am - 1.00 pm 2.00 pm - 5.00 pm</p>	<p><b>HOW TO REGISTER</b></p> <p>You must send the registration form with the receipt of the payment to: TECHNOLOGY TRANSFER S.r.l. Piazza Cavour, 3 - 00193 Rome (Italy) Fax +39-06-6871102</p> <p><b>within</b> <b>October 20, 2008</b></p> <p><b>PAYMENT</b></p> <p>Wire transfer to: Technology Transfer S.r.l. Banca Intesa Sanpaolo S.p.A. Agenzia 6787 di Roma Iban Code: IT 34 Y 03069 05039 048890270110</p>	<p><b>GENERAL CONDITIONS</b></p> <p><b>GROUP DISCOUNT</b></p> <p>If a company registers 5 participants to the same seminar, it will pay only for 4. Those who benefit of this discount are not entitled to other discounts for the same seminar.</p> <p><b>EARLY REGISTRATION</b></p> <p>The participants who will register 60 days before the seminar are entitled to a 10% discount. The participants who will register 30 days before the seminar are entitled to a 5% discount.</p> <p><b>CANCELLATION POLICY</b></p> <p>A full refund is given for any cancellation received more than 15 days before the seminar starts. Cancellations less than 15 days prior the event are liable for 50% of the fee. Cancellations less than one week prior to the event date will be liable for the full fee.</p> <p><b>CANCELLATION LIABILITY</b></p> <p>In the case of cancellation of an event for any reason, Technology Transfer's liability is limited to the return of the registration fee only.</p>
--	---	--

**KEN VAN WYK**  
**SECURE CODING:**  
**BUILDING SECURE**  
**WEB APPLICATIONS**  
**IN JAVA/J2EE**

November 3-5, 2008  
Residenza di Ripetta  
Via di Ripetta, 231  
Rome (Italy)

Registration fee:  
€ 1500

*If registered participants are unable to attend, or in case of cancellation of the seminar, the general conditions mentioned before are applicable.*

first name .....

surname .....

job title .....

organisation .....

address .....

postcode .....

city .....

country .....

telephone .....

fax .....

e-mail .....



Stamp and signature

Send your registration form with the receipt of the payment to:  
**Technology Transfer S.r.l.**  
Piazza Cavour, 3 - 00193 Rome (Italy)  
Tel. +39-06-6832227 - Fax +39-06-6871102  
info@technologytransfer.it  
www.technologytransfer.it



## SPEAKER

**Ken Van Wyk** is an internationally recognized information security expert and author of the O'Reilly and Associates books, "**Incident Response and Secure Coding**". In addition to providing consulting and training services through his company, *KRvW Associates, LLC*, he currently holds numerous positions: as a monthly columnist for on-line security Portal, eSecurityPlanet and a Visiting Scientist at Carnegie Mellon University's Software Engineering Institute. Mr. Van Wyk has 20+ years experience as an IT Security practitioner in the academic, military, and commercial sectors. Mr. Van Wyk also served a two-year elected position as a member of the Steering Committee for the Forum of Incident Response and Security Teams (FIRST) organization. At the Software Engineering Institute of Carnegie Mellon University, Mr. Van Wyk was one of the founders of the Computer Emergency Response Team (CERT®).