Security by Design, Lifecycles, and Visions

Prof. Dr. Michael Waidner
Director, Fraunhofer SIT and CASED
Professor, TU Darmstadt, CSc/CASED/Security in IT
Center for Advanced Security Research Darmstadt
Alliance for Fundamental and Application-oriented Research in IT Security

Fraunhofer SIT
160 Researchers in IT security and privacy

Technische Universität Darmstadt
10 Chairs with strong focus on IT security and privacy; more than 100 researchers

h_da
8 Chairs with strong focus on IT security and privacy

Director Fraunhofer SIT & CASED
Prof. Dr. Michael Waidner
Application Security – Samples from 2nd Half of February 2013

CVE-2013-0255: PostgreSQL DOS Vulnerability

PostgreSQL database management system vulnerable to a denial-of-service (DOS) vulnerability discovered by Sumit Soni. The vulnerability is confirmed in version 9.2.2.1-64-bit. Prior versions may also be affected. The vulnerability is caused due to a validation error within the "enum_recv()" function (backend/utils/adt/adt/enum.c) and can be exploited to crash the server if crafted SQL query is run. All users should update their PostgreSQL installations as soon as possible.

Adobe issues another path for Flash vulnerabilities

Summary: In its third update this month, the Flash developer rolls out another emergency patch addressing three vulnerabilities — one of which has been exploited in targeted attacks.

VMware patches privilege escalation vulnerability

Summary: The virtualization specialist releases an update to address a flaw in its ESX, Workstation, Fusion and View software.

Microsoft fixes critical Windows, Office, IE security flaws

Summary: Microsoft today released five critical patches that fix more than a dozen security vulnerabilities in all versions of Internet Explorer 6 and above, Windows, and Office.

E-Mails of Reporters in Myanmar Are Hacked

BANGKOK — Several journalists who cover Myanmar said Sunday that they had received warnings from Google that their e-mail accounts might have been hacked by “state-sponsored attackers.”

Zero-day vulnerability in Adobe Reader

Adobe Reader appears to be suffering from a critical zero-day vulnerability that allows criminals to inject malicious code into a system. A report by researchers from FireEye says they have encountered a specially crafted PDF document which, when opened, drops two DLLs into Windows.

The first of these DLLs runs for the other by displaying a fake error message and opening a decoy PDF document. The other DLL includes a callback component which talks over HTTP to a remote domain. According to FireEye, the exploit used has been successful on Adobe Reader 9.5.3, 10.1.5 and 11.0.1. Older versions might also be affected.
Security is complex

Flaws and defects in development and administration

For web applications

- 86% configuration flaws
- 79% integration flaws

Could have been avoided easily!

Source: IBM X-Force® Research and Development, 2012 + OWASP Top Ten 2010
What Can we Hope For?

- We are here
- We may get here
- We cannot get here

Security

Euro
“Secure software development, more than any other discipline, is where the largest gap between risk and response attention by the information security profession exists.”

Source: Frost & Sullivan. The 2013 (ISC)² Global Information Workforce Study. 2013

"More than 90% of attacks cloud have been avoided if they had maintained their systems"


Security problems due to configuration flaws in SAP (applying web technologies, mobile access)

Source: Sicherheitsschwachstellen in SAP-Systemen

11.02.2013 | von Michael Kallus

Computerwoche
We already know a lot about Security by Design...

Threat & Risk Analysis

- Microsoft Threat Modeling Process
  - STRIDE
  - DREAD

- CORAS
- OCTAVE
- CVSS
- TRIKE
- AZ/NZS 4360

Implementation

- Secure Coding Guidelines
  - Microsoft SDL
  - The CERT C Secure Coding Standard
  - The CERT Oracle Secure Coding Standard for Java
  - Secure Coding in C and C++

Secure Development Lifecycles / Frameworks

- Microsoft SDL
- OWASP CLASP
- Cigital Touchpoints

General Models for Systematic Development

- Rational Unified Process
- Scrum
- V Model
- Spiral Model

Abstract Model Principle

Plan | Do | Check | Act
Cost of Fixing Critical Defects

<table>
<thead>
<tr>
<th>Stage</th>
<th>Critical Bugs Identified</th>
<th>Cost of Fixing 1 Bug</th>
<th>Cost of Fixing All Bugs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements</td>
<td>$139</td>
<td>$977</td>
<td>$195,400</td>
</tr>
<tr>
<td>Design</td>
<td>$455</td>
<td>$977</td>
<td>$195,400</td>
</tr>
<tr>
<td>Coding</td>
<td>200</td>
<td>$7,136</td>
<td>$356,800</td>
</tr>
<tr>
<td>Testing</td>
<td>$7,136</td>
<td>$14,102</td>
<td>$2,115,300</td>
</tr>
<tr>
<td>Maintenance</td>
<td>$14,102</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>200</td>
<td>$195,400</td>
<td>$2,472,100</td>
</tr>
</tbody>
</table>

Identifying the critical bugs earlier in the lifecycle reduced costs by $2.3M

SOURCE: Digital, "Case Study: Finding Defects Earlier Yields Enormous Savings"

We even know...

...about its impact

Microsoft products: Vulnerabilities reduction after SDL implementation

- Windows: 45% reduction of vulns disclosed one year after release
- SQL Server: 91% reduction of vulns disclosed three years after release

Sources: Microsoft Security Blog and Microsoft TechNet Security Blog
…but existing Approaches do not solve all practical Problems!

Tools and methods are not made for today’s software development characteristics

How do we handle

- Distributed development
- Product lines
- Third party code supply chains
- Enterprise application integration
- Customized software
- Legacy software

Practice needs Research...

Fundamental Research

Application-oriented Research

Joint Laboratory for Secure Engineering

Joint Research for Secure Engineering

Security Test Lab

...and that’s what we are doing!
Early Evaluation of Runtime Monitors with CLARA (Compile-time approximation of runtime analysis)

“no access without previous authorization”

Specification Compiler

Application to be secured

Monitor Definition in AspectJ

AspectJ Weaver

Quick Check

Orphan Shadows

Nop Shadows

Original Software

© Fraunhofer-Gesellschaft 2013

CASED

Fraunhofer SIT
SPL lift: Securing Conditional Compilation for Product Lines

Example: Are there combinations of preprocessor commands that let secret flow to print?

- Problem: Space over all potential instantiations of preprocessor commands explodes
- Number of instantiations in real-world examples requires days for analysis
- SPL lift solves this problem in a much more efficient way
- Divide and conquer over preprocessing commands
- Analysis is now possible in a few minutes
Security Support for Application Development: Operational Threat Analysis (OTA)
Appicaptor: Framework for Efficient App Tests
Where should we be heading for in the next ten years?

Distributed development and integration will be characterized by unified, organization-overlapping and supply-chain-comprising security processes applied early in lifecycles.

Security tools will be integrated in the design and development process, even in development tools, that help to avoid or to detect security flaws caused by human developers as early as possible.

Usage of legacy software will follow strict security processes that allow estimation of the security status of the software and help even to achieve better security.

Challenging for research!

Requires developing companies to understand the strategic dimension of security by design!

Close cooperation between industry and research necessary!
Prof. Dr. Michael Waidner
michael.waidner@sit.fraunhofer.de

Fraunhofer Institute for Secure Information Technology (SIT)
Rheinstrasse 75
64295 Darmstadt
www.sit.fraunhofer.de

Technical University of Darmstadt
Department of Computer Science (FB20), Chair for Security in IT (FG SIT)
Mornewegstrasse 30
64289 Darmstadt
www.sit.tu-darmstadt.de