Developer-Centered Security Engineering Tools

Sven Türpe
Fraunhofer SIT
Tools

Problem:
Identify security concerns

Developer
Team
Process
Organization

Source: http://worrydream.com/#!/ABriefRantOnTheFutureOfInteractionDesign
Microsoft Threat Modeling Tool

1. Describe system
   - User, Browser
   - Spoofing
   - Tampering
   - Repudiation
   - Information disclosure
   - Denial of service
   - Elevation of privilege

2. Create checklist

3. Assess impact and find countermeasures for each item
Setting

IT Services

Social Scientist

Computer Scientist

Data Archive Staff

Internet

Remote access user

Usage of remote access

Remote access client

Remote access server

Preparation and maintenance of individual remote access working environments

Data archive staff

Selection and backup of social science data

Data archive

Handover of research results
Exploratory Study

1. Introductory meeting
2. Individual modeling
3. One-on-one interviews
4. Group discussion
Observation 1

Individual Perspectives
Observation 2
Making Decisions – Chicken & Egg

What can you build?

What do you need?
Conversation Tools

Knowledge & Data

Feedback

Decision Support

Boundary Objects

Micro-Artifacts
(1) Defect Analytics

<table>
<thead>
<tr>
<th>Defect Type Homogeneity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Many different types</td>
</tr>
<tr>
<td>0.0 0.1 0.2 0.3 0.4 0.5</td>
</tr>
<tr>
<td>Few different types</td>
</tr>
<tr>
<td>1.0</td>
</tr>
</tbody>
</table>

CWE-434: Unrestricted Upload of File with Dangerous Type (13 defects)
CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (7 defects)
CWE-319: Cleartext Transmission of Sensitive Information (1 defects)
CWE-352: Cross-Site Request Forgery (CSRF) (1 defects)
CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (1 defects)
CWE-598: Information Exposure Through Query Strings in GET Request (1 defects)
CWE-525: Information Exposure Through Browser Caching (1 defects)
CWE-6: J2EE Misconfiguration: Insufficient Session-ID Length (1 defects)
CWE-203: Information Exposure Through Discrepancy (1 defects)
CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (1 defects)
CWE-138: Improper Neutralization of Special Elements (1 defects)
(2) Classify User Stories

Definition of Done:

- All input + output sanitized with ESAPI (cf. Wiki:ESAPI, CWE-79)
- All stored passwords hashed with SHA-3 (cf. Wiki:PasswordHashing)
(3) IDE-Integrated Rule Validator

(1) Push Button

(2) Find Rule Violation
Examples:

“Don’t use Cipher.getInstance("DES")”

“Must use API xyz for database access”
Creative work is messy
http://sse.ec-spride.de

http://testlab.sit.fraunhofer.de

Sven.Tuerpe @ sit.fraunhofer.de

https://plus.google.com/+SvenTürpe