

# Architecture Security Advisor

Jakub Sendor, Wihem Arsac, Cédric Hébert, Elton Mathias, Gilles Montagnon

SAP Labs France | SAP Research Security & Trust

*System Testing and Validation Workshop 24/10/2012*





# STRIDE

---

- Elevation of Privilege Card Game, Microsoft
- STRIDE
  - Spoofing
  - Tampering
  - Repudiation
  - Information Disclosure
  - Denial of Service
  - Elevation of Privilege



# Product Security Assessment

---

**What if an Architect is not a Security Expert?**

and can not do a deep threat analysis of his application

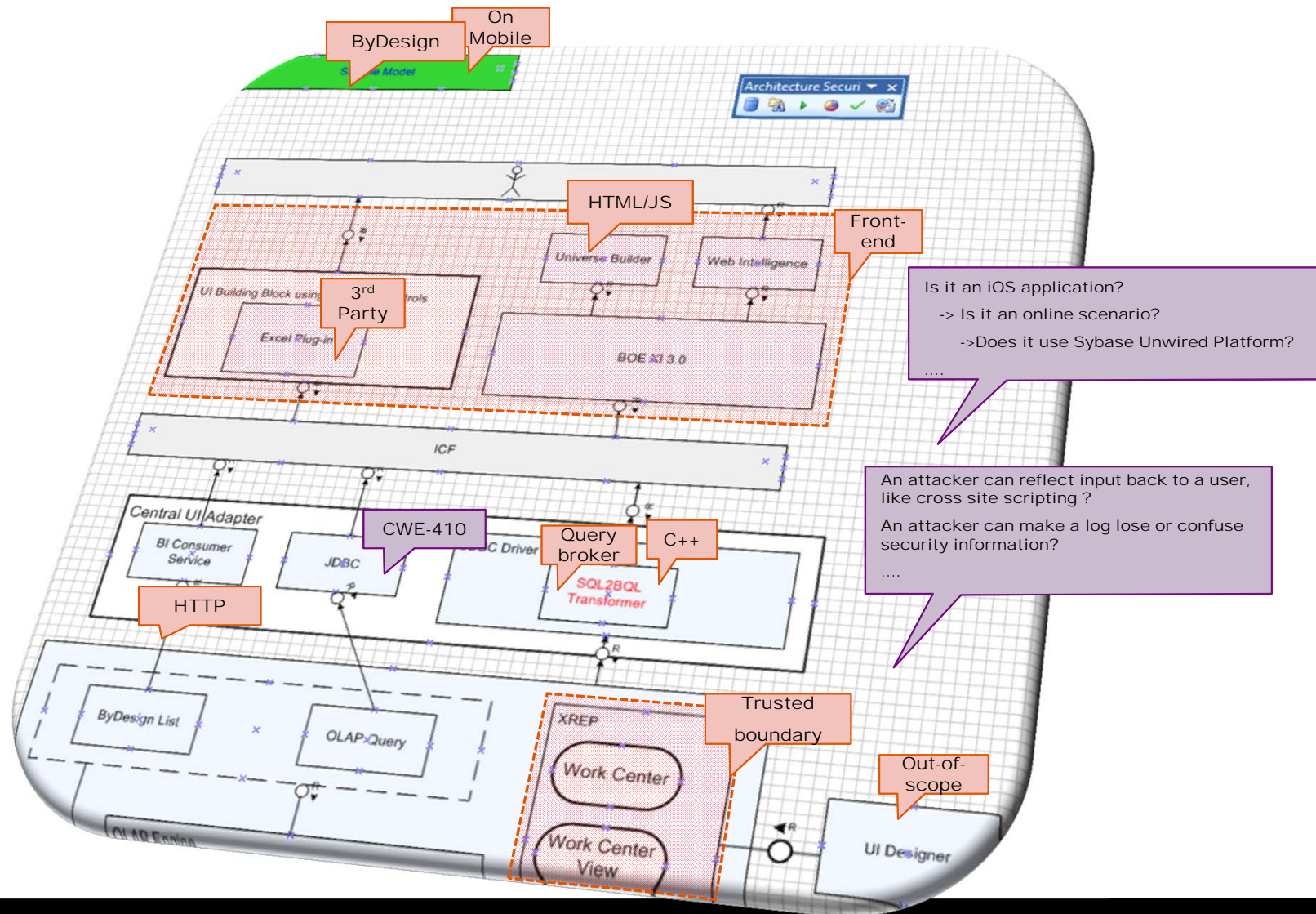
**What if a Security Expert is not the Product Owner or the Product Architect?**

and doesn't know about the application specificities

**How to combine the different knowledge to  
support a Product Security Assessment?**

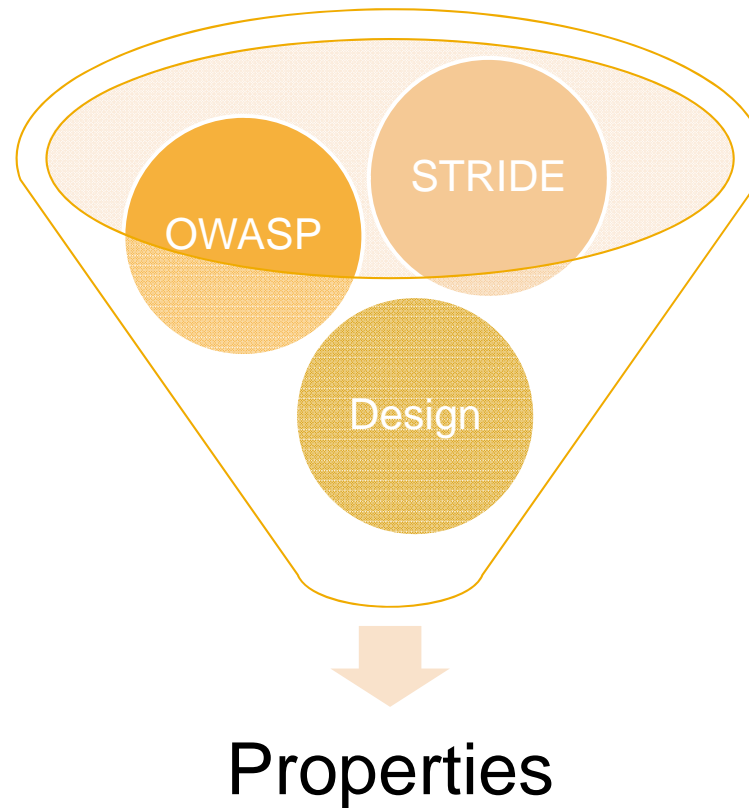
# Architecture driven security assessment

Collect architecture information and focus on security related inputs



# Assessment Questions, Architecture Properties

---



Question/Design Property/Asset type -> Property

Answer/Property Value/„Agent”/„Storage” -> Value

# Relations Between Questionnaires

---

## Value – Value Mapping

Answer to one question can propose answer to the other question

e.g. STRIDE question „**An attacker can reflect input back to a user**” (EJ)  
value „**applicable**”

-> OWASP TOP10 „**You are vulnerable to Cross-Site Scripting**”  
value „**applicable**”

# Relations Between Questionnaires

---

## Value – Question Mapping

Answer to one question can trigger asking the other question

e.g. „Is storage encrypted?”

value „true”

-> „Which technology is used for encryption?”

# Security expert system

Contextual and guided assessment

Expert system with Security inside

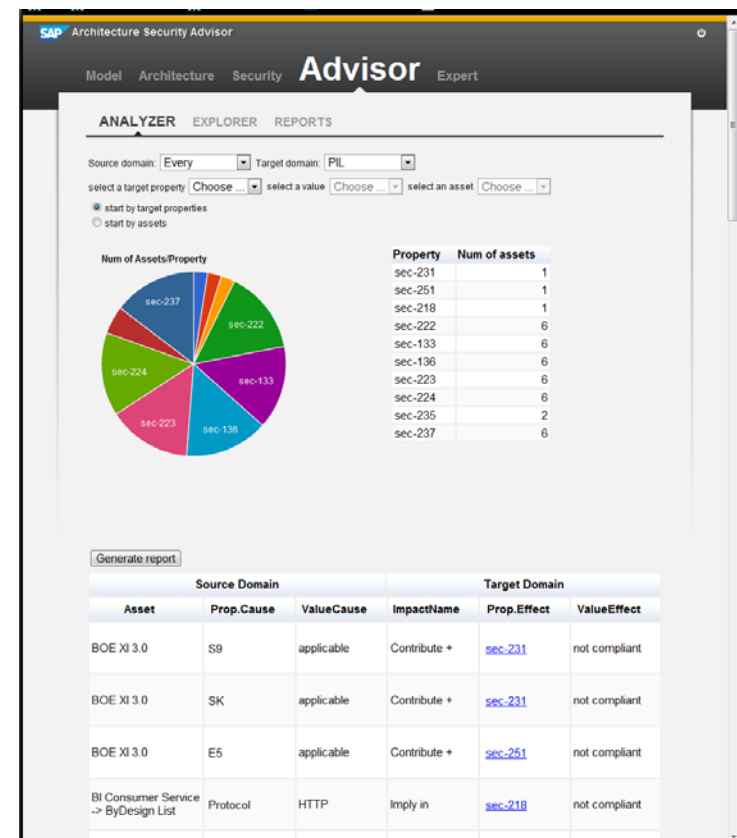
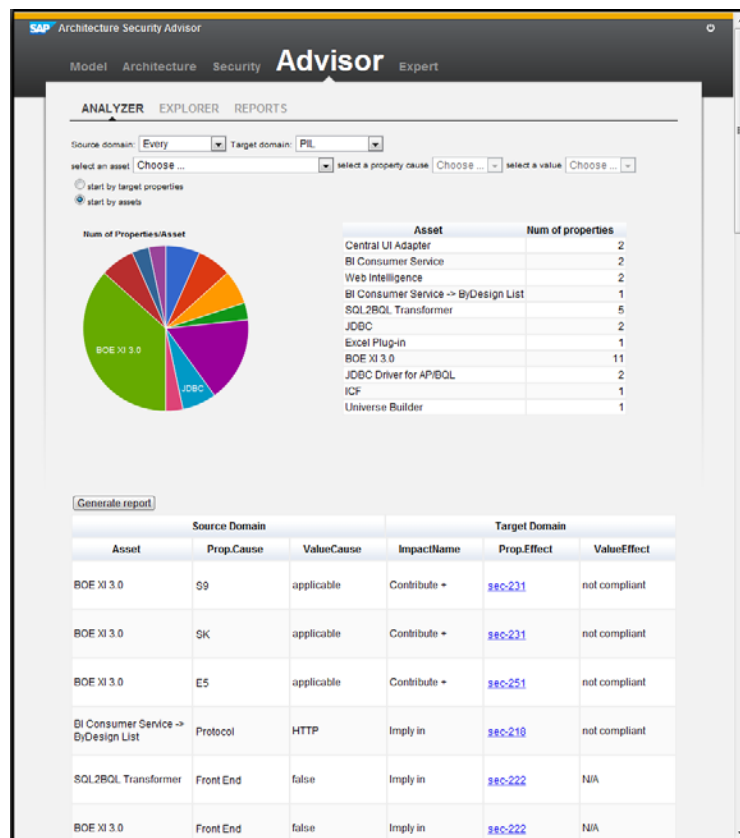
The screenshot displays the SAP Architecture Security Advisor interface. The top navigation bar includes 'Model', 'Architecture', 'Security', 'Advisor', and 'Expert'. The main content area is titled 'OVERALL MODEL DESIGN' and shows the 'SQL2BQL Transformer' component. The 'Security' section is expanded, showing a list of attack scenarios under the 'STRIDE' framework. The table lists various attack types (D2, D3, D4, D5, D6, D7, D8, D9, D10, DJ, DQ, DK, DA) and their descriptions. The 'Value' column indicates the severity or applicability of each attack. The 'Proposals' column provides links to mitigation strategies.

Pro...	Question	Value	Proposals
D2	An attacker can make your authentication system unusable or unavailable		Proposals
D3	An attacker can make a client unavailable or unusable but the problem goes away when the attacker stops		Proposals
D4	An attacker can make a server unavailable or unusable but the problem goes away when the attacker stops		Proposals
D5	An attacker can make a client unavailable or unusable without ever authenticating but the problem goes away when the attacker stops		Proposals
D6	An attacker can make a server unavailable or unusable without ever authenticating but the problem goes away when the attacker stops		Proposals
D7	An attacker can make a client unavailable or unusable and the problem persists after the attacker goes away		Proposals
D8	An attacker can make a server unavailable or unusable and the problem persists after the attacker goes away		Proposals
D9	An attacker can make a client unavailable or unusable without ever authenticating and the problem persists after the attacker goes away		Proposals
D10	An attacker can make a server unavailable or unusable without ever authenticating and the problem persists after the attacker goes away		Proposals
DJ	An attacker can cause the logging subsystem to stop working		Proposals
DQ	An attacker can amplify a Denial of Service attack through this component with amplification on the order of 10:1	applicable	Proposals
DK	An attacker can amplify a Denial of Service attack through this component with amplification on the order of 100:1	applicable	Proposals
DA	You've invented a new Denial of Service attack		Proposals



# Security Advisor

**Detect and understand** the cause of potential **security issues** in order to **mitigate and comply** with Product Standard **Security Requirements**



# Demo



# Concluding

---

Guided Security Assessment driven by Advisory System

# Concluding

---

## ~~Guided~~ Security Assessment driven by Advisory System

- Involve all the roles in the assessment
- Simplify assessment by offering proposals
- Visualize impact of the choices

But also:

- Suggest mitigation for security threats





# Thank you!

Jakub Sendor  
[jakub.sendor@sap.com](mailto:jakub.sendor@sap.com)

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Excel, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, System z9, z10, z9, iSeries, pSeries, xSeries, zSeries, eServer, z/VM, z/OS, i5/OS, S/390, OS/390, OS/400, AS/400, S/390 Parallel Enterprise Server, PowerVM, Power Architecture, POWER6+, POWER6, POWER5+, POWER5, POWER, OpenPower, PowerPC, BatchPipes, BladeCenter, System Storage, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, Parallel Sysplex, MVS/ESA, AIX, Intelligent Miner, WebSphere, Netfinity, Tivoli and Informix are trademarks or registered trademarks of IBM Corporation.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP BusinessObjects Explorer, StreamWork, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects Software Ltd. Business Objects is an SAP company.

Sybase and Adaptive Server, iAnywhere, Sybase 365, SQL Anywhere, and other Sybase products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Sybase, Inc. Sybase is an SAP company.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

The information in this document is proprietary to SAP. No part of this document may be reproduced, copied, or transmitted in any form or for any purpose without the express prior written permission of SAP AG.

This document is a preliminary version and not subject to your license agreement or any other agreement with SAP. This document contains only intended strategies, developments, and functionalities of the SAP® product and is not intended to be binding upon SAP to any particular course of business, product strategy, and/or development. Please note that this document is subject to change and may be changed by SAP at any time without notice.

SAP assumes no responsibility for errors or omissions in this document. SAP does not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

SAP shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials. This limitation shall not apply in cases of intent or gross negligence.

The statutory liability for personal injury and defective products is not affected. SAP has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third-party Web pages nor provide any warranty whatsoever relating to third-party Web pages.