# 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

J
Elevation of Privilege
An attacker can reflect input back to a user, like cross site scripting

# Product Security Assessment

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

**and can not do a deep threat analysis of his application**

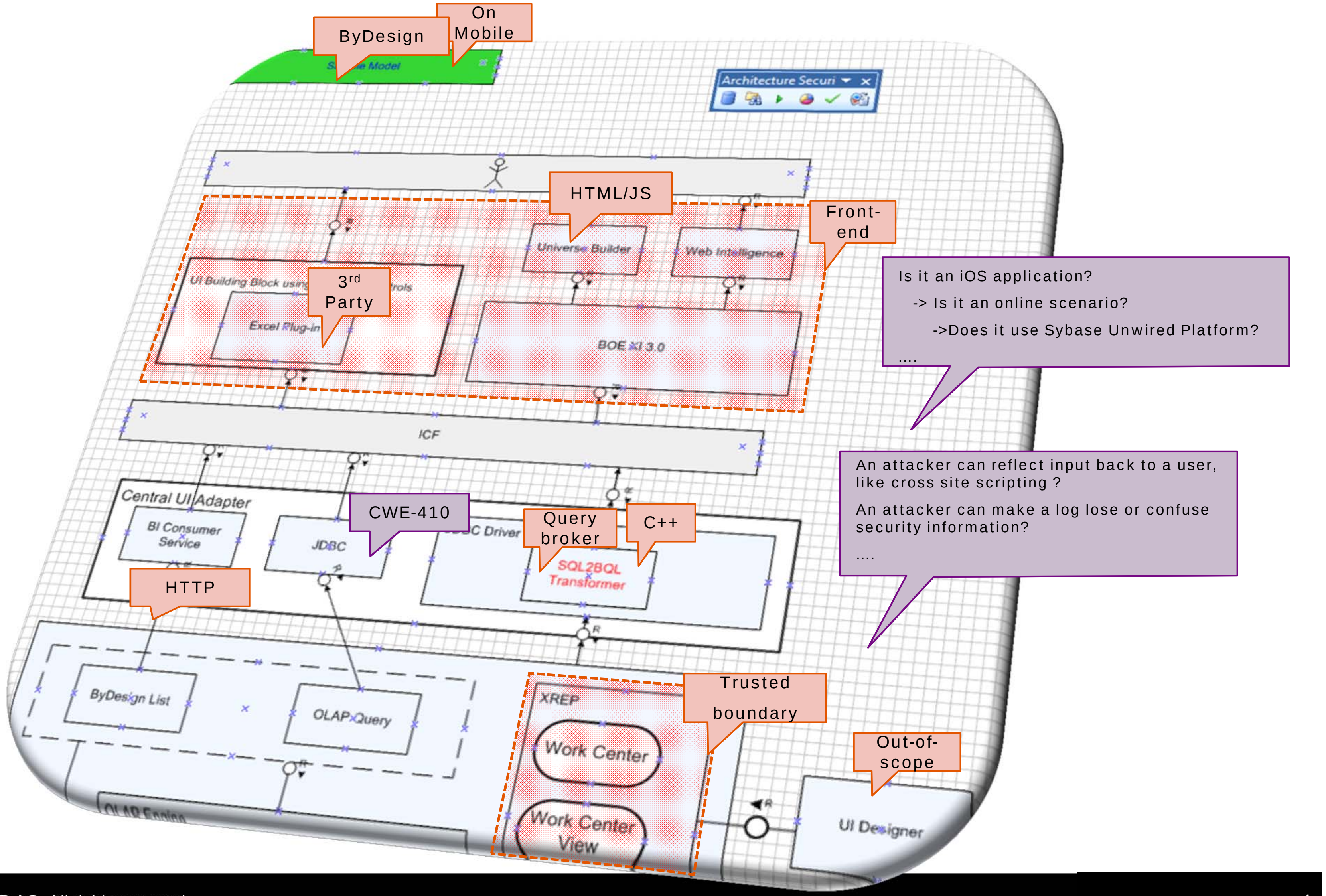
**What if a Security Expert is not the Product Owner or the Product Architect?**

**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



Is it an iOS application?

-> Is it an online scenario?

->Does it use Sybase Unwired Platform?

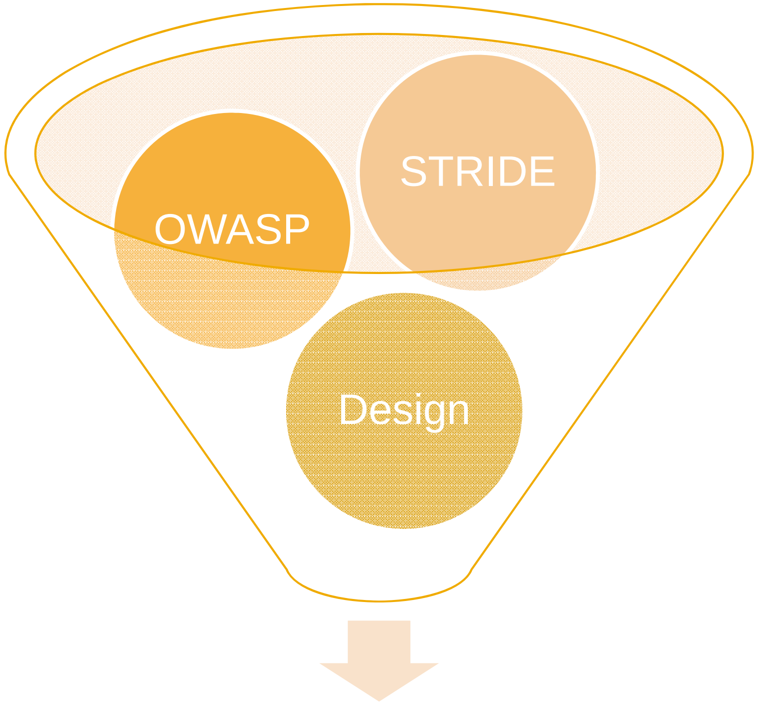
….

An attacker can reflect input back to a user, like cross site scripting ?

An attacker can make a log lose or confuse security information?

….

# Assessment Questions, Architecture Properties



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**?”

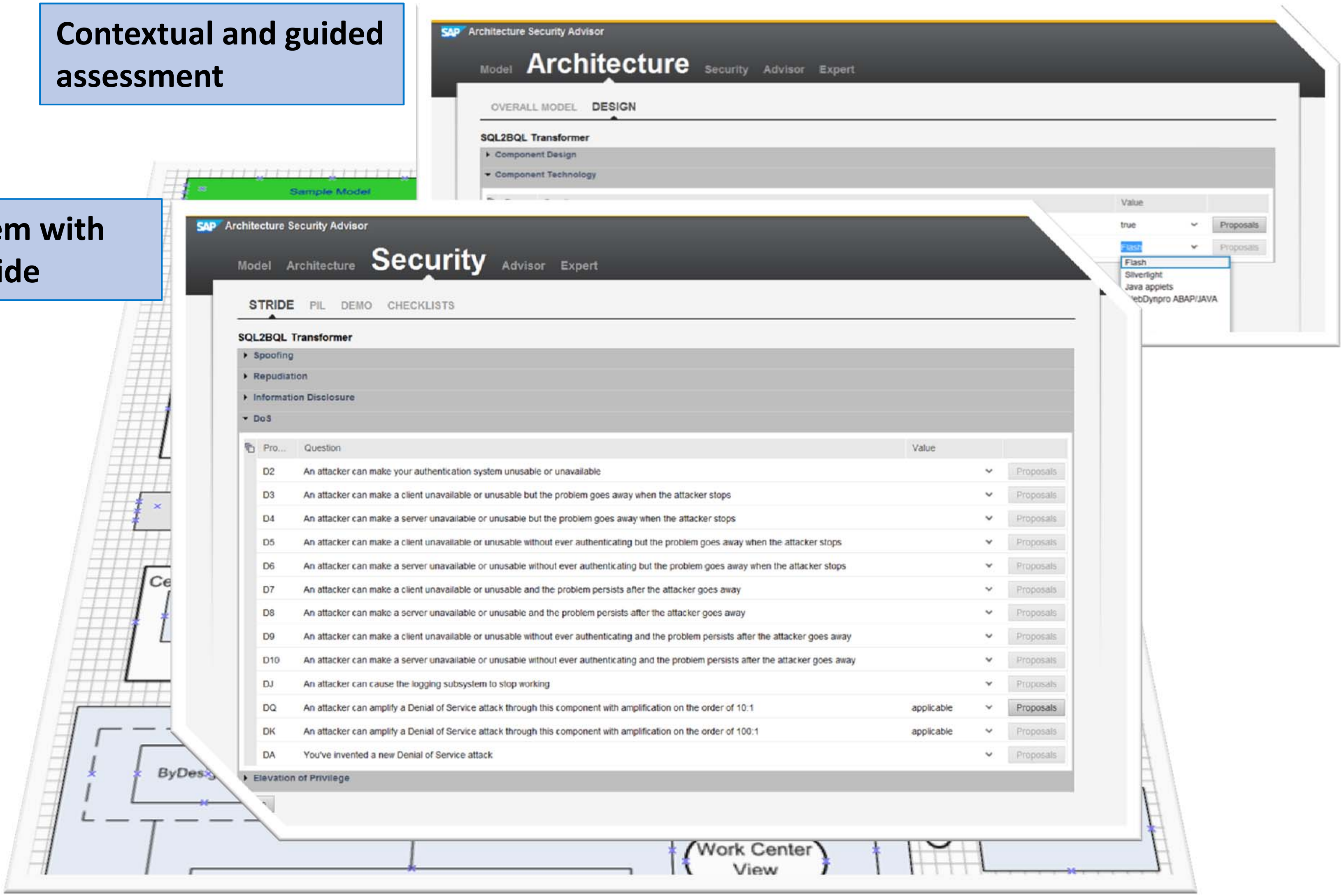
value „**true**”

-> „**Which technology is used for encryption?**”

# Security expert system

**Contextual and guided assessment**

**Expert system with Security inside**



Architecture Security Advisor

Model **Architecture** Security Advisor Expert

OVERALL MODEL **DESIGN**

**SQL2BQL Transformer**

- Component Design
- Component Technology

| Value | |
|---|---|
| true | Proposals |
| Flash | Proposals |

Flash
Silverlight
Java applets
WebDynpro ABAP/JAVA

Architecture Security Advisor

Model Architecture **Security** Advisor Expert

**STRIDE** PIL DEMO CHECKLISTS

**SQL2BQL Transformer**

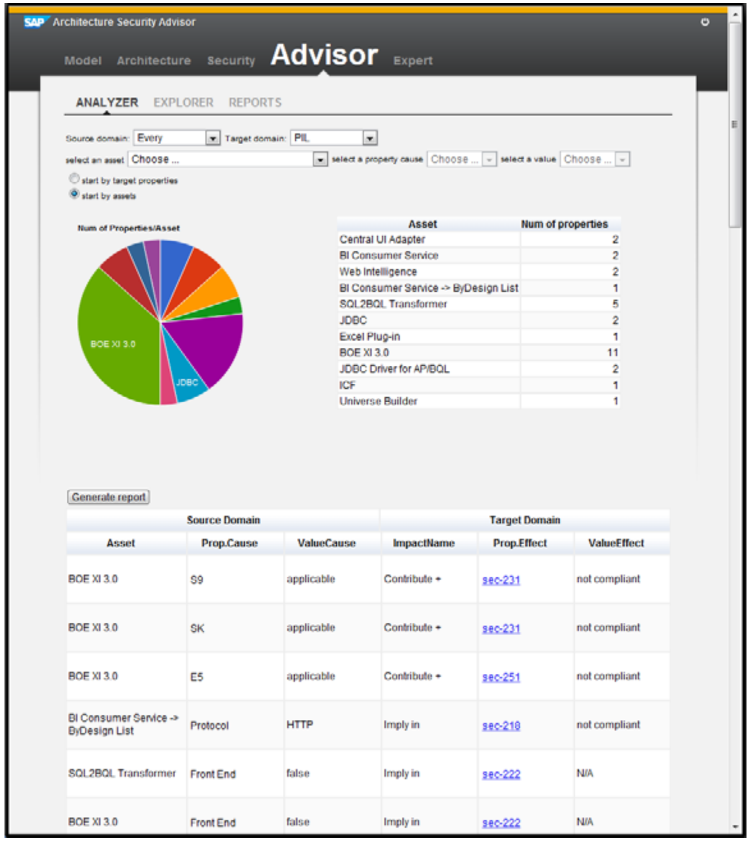
- Spoofing
- Repudiation
- Information Disclosure
- DoS

| Pro... | Question | Value | |
|---|---|---|---|
| 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 |

- Elevation of Privilege

# Security Advisor

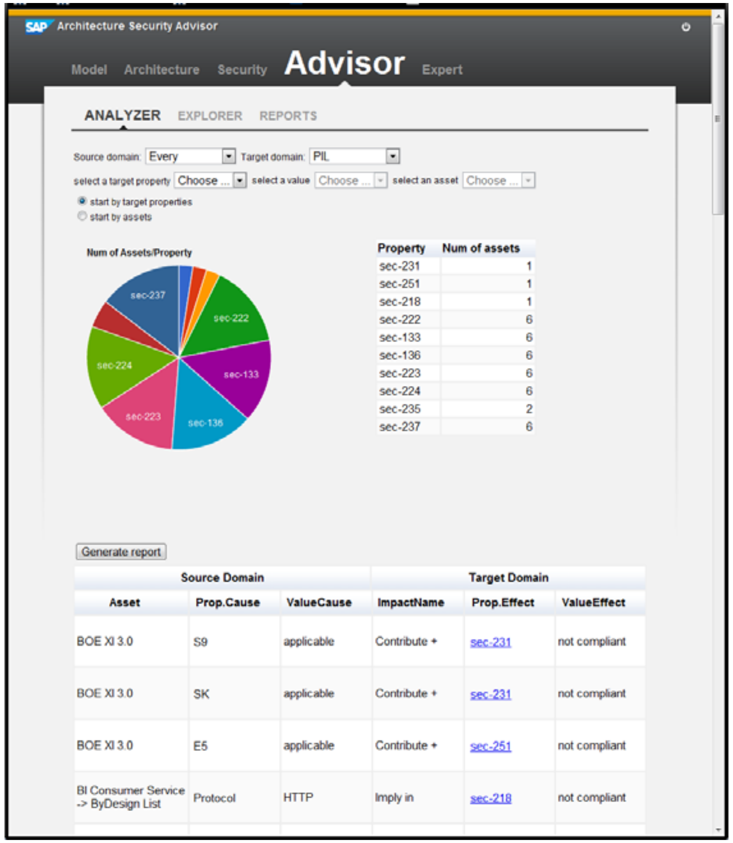
**Detect and understand the cause of potential security issues in order to mitigate and comply with Product Standard Security Requirements**



Source domain: Every
Target domain: PIL
select an asset: Choose ...
select a property cause: Choose ...
select a value: Choose ...
○ start by target properties
● start by assets

| Asset | Num of properties |
|---|---|
| Central UI Adapter | 2 |
| BI Consumer Service | 2 |
| Web Intelligence | 2 |
| BI Consumer Service -> ByDesign List | 1 |
| SQL2BQL Transformer | 5 |
| JDBC | 2 |
| Excel Plug-in | 1 |
| BOE XI 3.0 | 11 |
| JDBC Driver for AP/BQL | 2 |
| ICF | 1 |
| Universe Builder | 1 |

| Source Domain | | | Target Domain | | |
|---|---|---|---|---|---|
| Asset | Prop.Cause | ValueCause | ImpactName | Prop.Effect | ValueEffect |
| BOE XI 3.0 | S9 | applicable | Contribute + | sec-231 | not compliant |
| BOE XI 3.0 | SK | applicable | Contribute + | sec-231 | not compliant |
| BOE XI 3.0 | E5 | applicable | Contribute + | sec-251 | not compliant |
| BI Consumer Service -> ByDesign List | Protocol | HTTP | Imply in | sec-218 | not compliant |
| SQL2BQL Transformer | Front End | false | Imply in | sec-222 | N/A |
| BOE XI 3.0 | Front End | false | Imply in | sec-222 | N/A |



Source domain: Every
Target domain: PIL
select a target property: Choose ...
select a value: Choose ...
select an asset: Choose ...
● start by target properties
○ start by assets

| Property | Num of assets |
|---|---|
| sec-231 | 1 |
| sec-251 | 1 |
| sec-218 | 1 |
| sec-222 | 6 |
| sec-133 | 6 |
| sec-136 | 6 |
| sec-223 | 6 |
| sec-224 | 6 |
| sec-235 | 2 |
| sec-237 | 6 |

| Source Domain | | | Target Domain | | |
|---|---|---|---|---|---|
| Asset | Prop.Cause | ValueCause | ImpactName | Prop.Effect | ValueEffect |
| BOE XI 3.0 | S9 | applicable | Contribute + | sec-231 | not compliant |
| BOE XI 3.0 | SK | applicable | Contribute + | sec-231 | not compliant |
| BOE XI 3.0 | E5 | applicable | Contribute + | sec-251 | not compliant |
| BI Consumer Service -> ByDesign List | Protocol | HTTP | Imply in | sec-218 | not compliant |

# 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

# © 2011 SAP AG. All rights reserved