



Security Testing

Axel Rennoch
Fraunhofer FOKUS

28. September 2012,
BSI-FOKUS Tagesgespräch



- Security Testing Aktivitäten
 - Model-based Security Testing
- Das ITEA2 DIAMONDS Projekt
 - Standardisierung und R2GS-Initiativen



- **Security Testing Aktivitäten**
 - Model-based Security Testing
- Das ITEA2 DIAMONDS Projekt
 - Standardisierung und R2GS-Initiativen



Software Security Testing – **Prozeß** zur Erkennung der Übereinstimmung von Sicherheitseigenschaften einer Software-Implementierung gegenüber dem Entwurf

- **Funktionales Security Testing** – **versichert**
ob Software-*Sicherheitsfunktionen* korrekt implementiert sind und mit der Beschreibung der Sicherheitsanforderungen übereinstimmen.
 - **Software-Sicherheitsanforderungen** beziehen sich auf *Daten Vertraulichkeit, Vollständigkeit, Verfügbarkeit, Echtheit, Vollmachten, Zugangskontrollen, Prüfung, Geheimhaltung, Sicherheitsmanagement, usw.*
- **Security Schwachstellen Testing** (“*Penetrationstests*”) – **ermittelt**
Sicherheits-Schwachstellen aus der Sicht von Angreifern.
 - **Schwachstellen** beziehen sich auf Fehler bezüglich *System Entwurf, Implementierung, Betrieb, Management*. Schwachstellen können zu Angriffen genutzt werden und zu unsicheren Zuständen führen.

Klassischer Ansatz: Testen von Gegenmaßnahmen



- **Bereitstellung:**
 - **Verschlüsselung**
Sicherheitsdienste
 - **Firewalls**
 - *Authentifizierung, Vollmachten, Verantwortlichkeits-Dienste*
 - **Watchdogs**
 - **Diagnose-** und **Prüf-**Dienste
 - *Plausibilitäts-Überprüfung, Redundanz*
- **Analyse:**
 - **Testen**
(funktionale Gegenmaßnahmen, simulierte Gefahren)
 - **Konformitäts-Testen**
 - Code und Model **Inspektion**

Schwachstellen und Gefahren-basierte
Risikoanalyse

Spezifikation und
Realisierung von
Gegenmaßnahmen

Bestätigung und
Gültigkeit von
Gegenmaßnahmen

Security Argument

Security Testing Richtlinien und Techniken



Vorhandene Richtlinien

- **Technical Guide to Information Security Testing and Assessment**, Recommendations of the *National Institute of Standards and Technology (NIST)*;
- **Open Source Security Testing Methodology Manual (OSSTMM)**; *Institute for Security and open Methodologies (ISECOM)*
- OWASP **Testing Guide**; The *Open Web Application Security Project (OWASP)* Foundation 2008

Szenario-basierte Ansätze

- "Missbrauch" *Fallabdeckung*
- "*Penetration*" Tests (analytisch)

Search-based Ansätze

- *fuzzing* ("zufällig")
- evolutionary testing

Knowledge-based Ansätze

- *Schwachstellen*-Suche

Model-based Security Testing

- *Gefahrenmodelle* und Angriffs-basiertes Testen
- *smart fuzzing* (specification-based: Syntaxtests, Fehler-Einschleusung, ...)
- *Risiko-basiertes* Testen

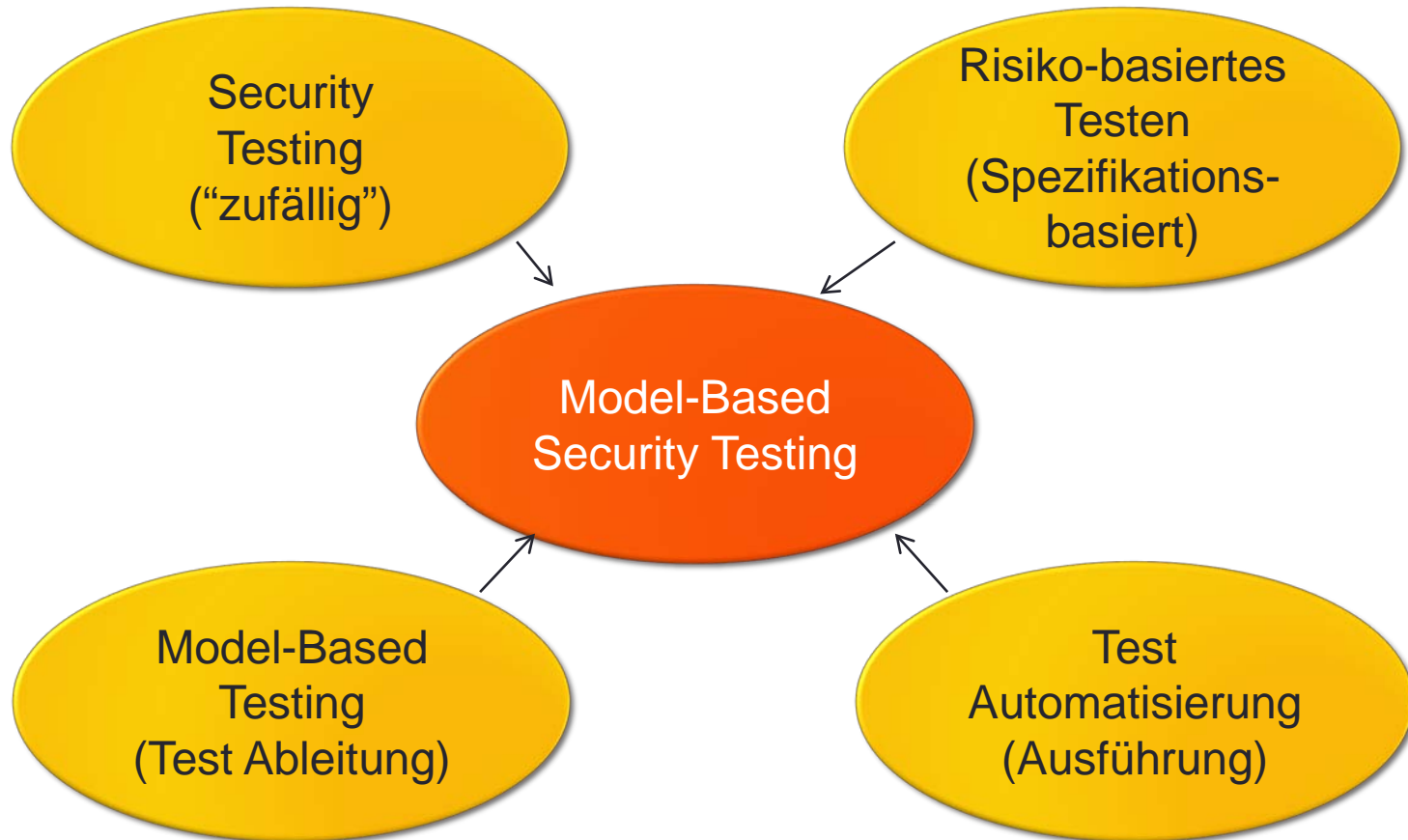


- Das erwartete Verhalten eines **Angreifers** kann *nicht immer* vorhergesagt werden (**vorsätzliches** "Hacking").
- Die **meist manuelle Durchführung** erfordert hohes Expertenwissen bei der Erkennung von Schwachstellen.
- **Fehlende Garantien:**
 - *Garantie* für das Kompromittieren eines Systems (z.B. ein System versagt während eines "Penetrationstests"), **aber**
 - *keine Garantie* für ein bestimmtes Niveau der Systemsicherheit.



- **Nutzung** von *Modellen* mit **Sicherheits-Annotationen**
 - zur Ermittlung des *Testaufbaus*,
 - zur Testableitung und *Abdeckung* modellierter *Sicherheitsfunktionen*
 - für *Testfall-Auswahl* bzw. Erzeugung (für kritische Sicherheitsfunktionen) *entsprechend ihres Schweregrades*.
- **Ableitung von Tests** aus **Umgebungs-** oder **Systemmodellen** unter Beachtung der logischen und physikalischen Gegebenheiten, inkl.:
 - *automatisierte Schwachstellensuche* für komplexe System-Konfigurationen (z.B. aus Einsatzmodellen),
 - systematische *Test-Erzeugung aus Angriffsmodellen* (z.B. Mißbrauchs-Modell) oder *Umgebungsmodellen* (z.B. Protokolle),
 - Einbeziehen von *Risikomodellen* (Bedrohungen und "Schätze") zur Erkennung, Erzeugung und Auswahl von Testfällen.

Kombination mehrerer Ansätze





- Security Testing Aktivitäten
 - Model-based Security Testing
- **Das ITEA2 DIAMONDS Projekt**
 - Standardisierung und R2GS-Initiativen

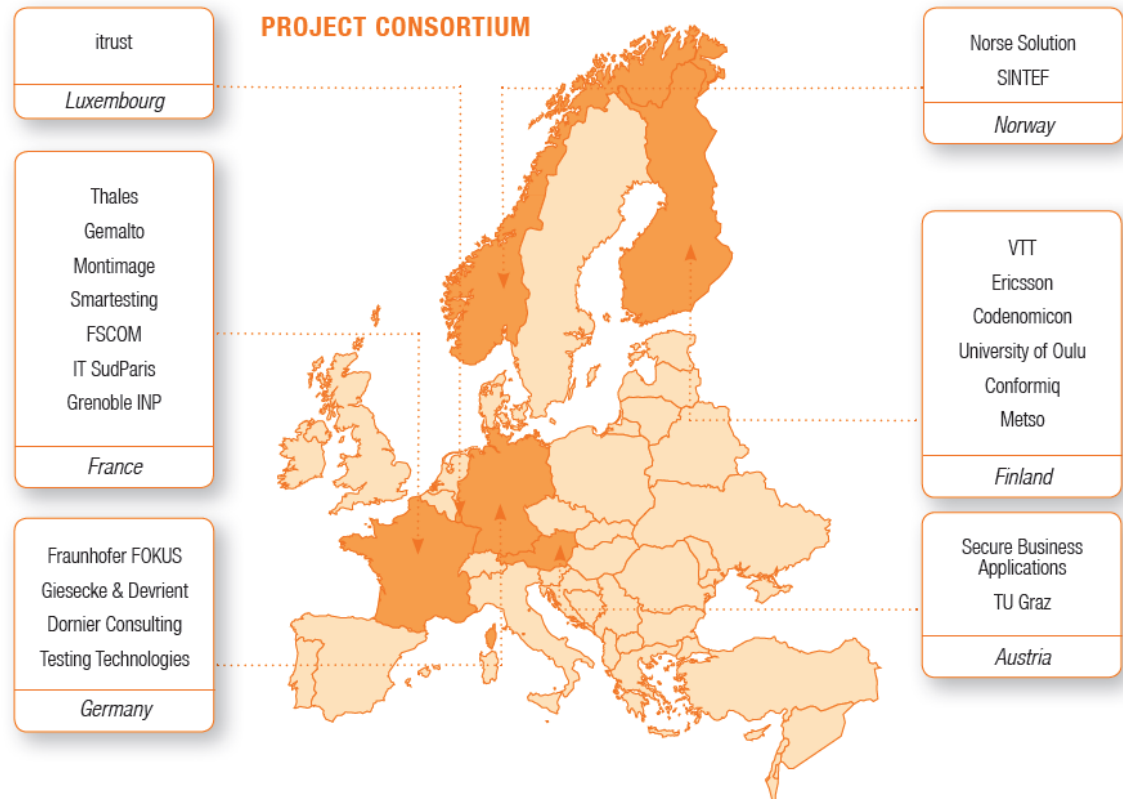
ITEA 2 DIAMONDS Projekt



DIAMONDS erarbeitet effiziente und automatisierte Sicherheitsprüfmethoden für *Systeme mit hohen Sicherheitsanforderungen* in **Industriebereichen** (z. B. für Banken, Transport oder Telekommunikation).

Erwartete Ergebnisse

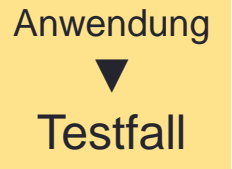
- Sicherheits *Fehlermodelle*
- *Risiko-basierte* Sicherheits-Testmethoden
- *Modelbasierte* Techniken für Sicherheitstests
- Sicherheitstest-*Musterkataloge*



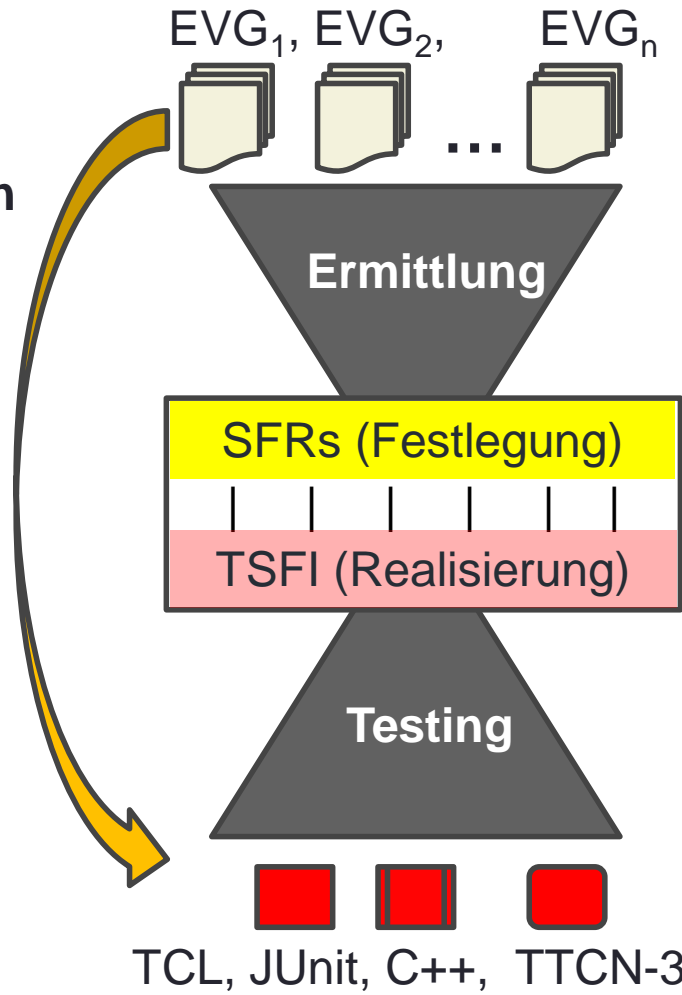
Beitrag aus DIAMONDS



**System (Risiko)
Analysemethoden
& Modelle:**
z.B. CORAS,
UMLsec

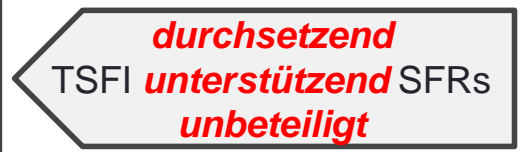


**Test Tools &
Techniken:**
z.B. *fuzzing*,
partitioning



System Definition & Analysis

- 1) EVG, Subjekte, "Schätze"
- 2) Gefahren, Regeln, Annahmen
- 3) Sicherheitsziele
- 4) Sicherheitsanforderungen (SFR)



Test Entwicklungsplan

- a) Konzepte/Architekturen
 - b) Ziele
 - c) Testkatalog Struktur
- Abdeckung der sicherheitsrelevanten TSFI

TCL, JUnit, C++, TTCN-3, manuelle Tests...

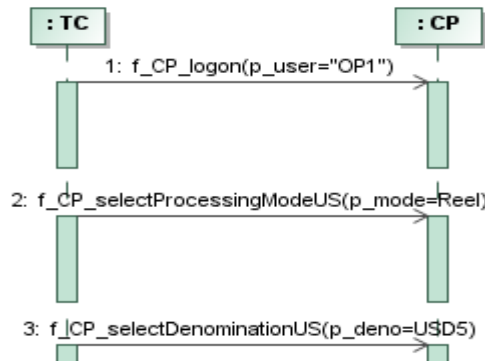
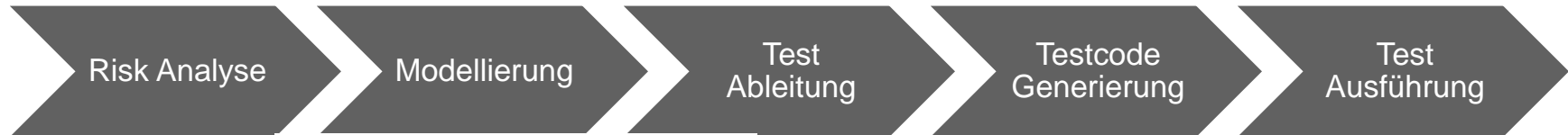
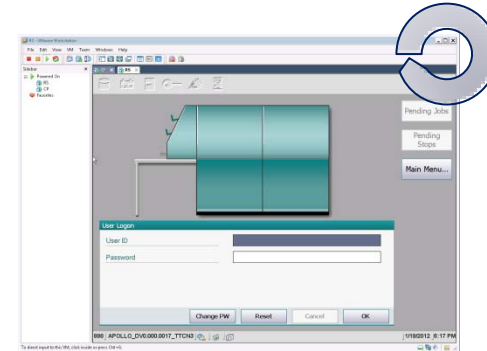
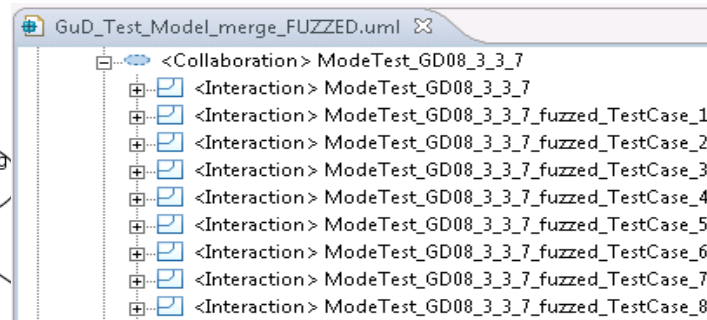
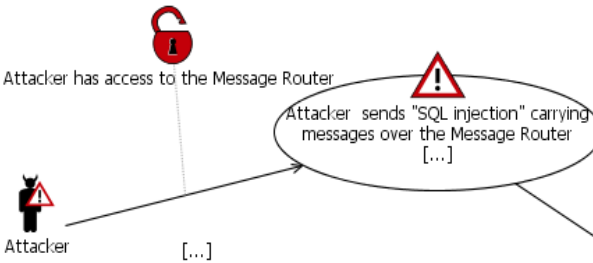
DIAMONDS Fallstudien



- Banken
- Smart Cards
- Industrie-Automatisierung
- Automotive
- Funkverbindungen
- Telekommunikations-Infrastrukturen



G&D Fallstudie: Prozeßschritte



```
testcase ModeTest_GD08_3_3_7_fuzzed_TestCase_219 ()
runs on Comp_CP_RS
system System_CP_RS
{
    var integer i, v_total, v_rjc;

    f_mtcSetup_CP_RS(CPRSStartingMode:All);

    f_CP_logon("OP1");
    f_CP_selectProcessingModeUS(ProcessingModeUS:Reel);
}
```

Standardisierungs-Gremien



Standardisierungsebenen:

- International: ISO, ITU, ...
- Europa: ETSI, ENISA, ...
- National: NIST, AFNOR, DIN, ...
- Industrieverbände: IEEE, OMG, ...



DIAMONDS Schwerpunkt ist ETSI:

- TC **MTS**: Methods for testing and specification, *Model-based testing*, Security Special Interest Group;
- TC **TISPAN/E2NA**: Threat, vulnerability and risk *analysis* (TVRA)
- TC **INT**: *IMS network testing* (*konkreter Testkatalog*)
- ISG **ISI**: *Operational Security Indicators* measuring IT security policy enforcement & effectiveness (in Kooperation mit *nationalen R2GS Clubs*)



Operational Security Management Thought and Research Clubs

- Frankreich (seit 2009, derzeit 40 Mitglieds-Organisationen)
- UK (seit Frühjahr 2012)
- Deutschland (in Gründung)

Club **R2GS**

Ziele:

- Definition einer Referenz für das betriebliche Sicherheitsmanagement (ISO 2700x- und ITIL-kompatibel)
- (Regelmäßige) Sammlung und Veröffentlichung von Referenzdaten zur externen und internen Cyberkriminalität
- Förderung des Erfahrungsaustausches im SIEM-Bereich (intern und mit Externen)



Vielen Dank!

www.ITEA2-DIAMONDS.org

(Projektberichte)