

Uma Revisão Sistemática em Teste de Segurança Baseado em Modelos

Carlos Diego Nascimento Damasceno,
Márcio Eduardo Delamaro, Adenilso da Silva Simão

Laboratório de Engenharia de Software – LabES
Instituto de Ciências Matemáticas e de Computação – ICMC
Universidade de São Paulo – USP
São Carlos – SP – Brasil
damascenodiego@usp.br, {delamaro,adenilso}@icmc.usp.br

26 de setembro de 2014



Agenda

- ▶ Contextualização
 - ▶ Teste Baseado em Modelos (TBM)
- ▶ Revisão Sistemática
 - ▶ Questões de Pesquisa
 - ▶ Bases de Dados e String de Busca
 - ▶ Seleção de Estudos e Extração de Dados
- ▶ Resultados
- ▶ Conclusões



Contextualização

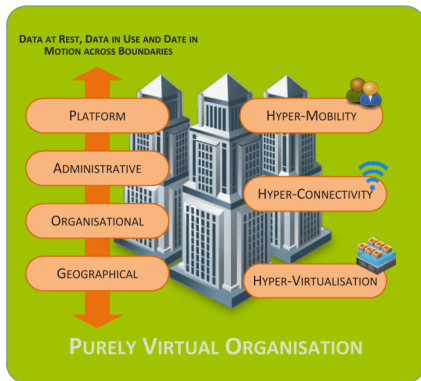


Figura 1 : Organizações Puramente Virtuais [Rashid et al. 2013]

Contextualização

- ▶ Teste de Software
- ▶ Segurança da Informação
 - ▶ Estratégias de Defesa à Ataques Virtuais
- ▶ Mecanismos de Segurança
 - ▶ Firewalls
 - ▶ Sistemas de Detecção de Intrusão
 - ▶ Controle de Acesso



Contextualização

- ▶ Exfiltração de Dados
 - ▶ Vazamento não autorizado de dados sensíveis
 - ▶ Técnicas sofisticadas

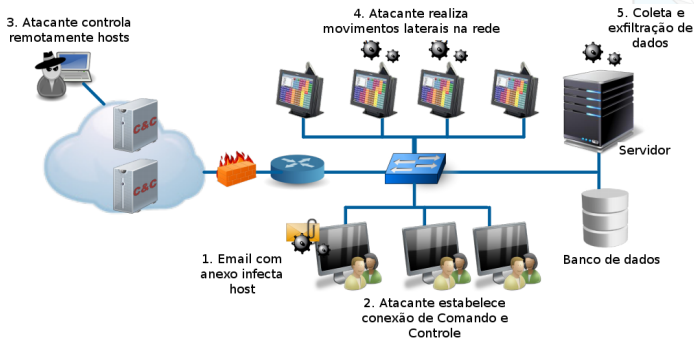


Figura 2 : Cenário de Ameaça Persistente Avançada [Rashid et al. 2013]

Contextualização

- ▶ Teste Baseado em Modelos (TBM)
- ▶ Automatiza geração de teste
- ▶ Modelos formais explícitos
- ▶ Critérios de Geração

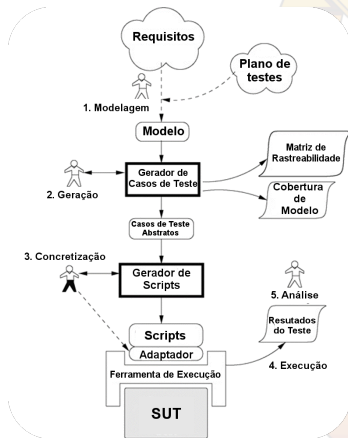


Figura 3 : Etapas do TBM [Utting and Leggard 2007]

Contextualização

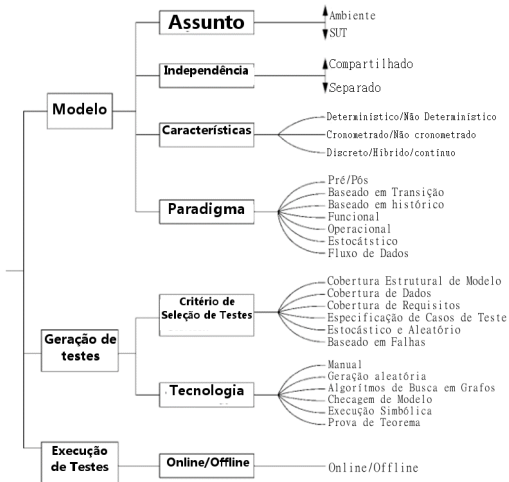
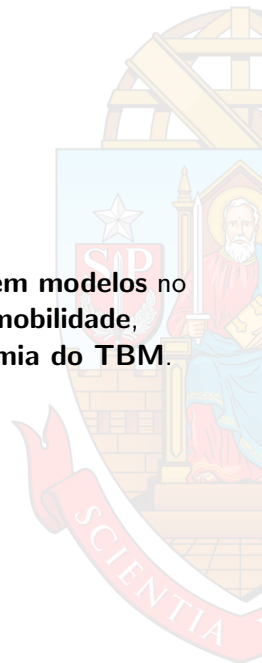


Figura 4 : Taxonomia do TBM [Utting and Legard 2007]

Categorizar **estudos** que apliquem **teste baseado em modelos** no **teste de segurança** em serviços baseados em **mobilidade**, **virtualização** e **conectividade** segundo a **taxonomia do TBM**.



- RQ 1:** Que **resultados** o uso de **Teste de Segurança Baseado em Modelos (TSBM)** em serviços ligados a **mobilidade, virtualização** ou **conectividade** tem proporcionado?
- RQ 2:** Quais as **características** predominantes nos estudos de TSBM?
- RQ 2.1:** Considerando a **taxonomia do TBM**, como as abordagens de TSBM podem ser categorizadas?
 - RQ 2.2:** Que **tipo de SUTs** estas abordagens utilizam em seus estudos empíricos?
 - RQ 2.3:** Quais as **desvantagens e limitações** destes estudos?
 - RQ 2.4:** Estes estudos podem ser aplicados no tratamento de **exfiltração de dados**?

Revisão Sistemática (Bases de Dados e String de Busca)

("security testing" OR "security" OR "data exfiltration" OR "data extrusion" OR "data theft" OR "data leakage" OR "intrusion" OR "malware" OR "vulnerability") AND ("threat modeling" OR "model based" OR "model based testing" OR "model based security testing")



Revisão Sistemática (Seleção de Estudos e Extração de Dados)

- ▶ Seleção de Estudos
 - ▶ Etapa 1 (Inclusão):
 - ▶ Título, Abstract e palavras-chave
 - ▶ TBM, Segurança e Experimento
 - ▶ Etapa 2 (Exclusão):
 - ▶ Estudos duplicados
 - ▶ < 3 páginas
- ▶ Extração de Dados
 - ▶ Taxonomia, Tipo de SUT, e Ameaça
 - ▶ Mobilidade, Conectividade ou Virtualização
 - ▶ Exfiltração de dados



Resultados

- ▶ 227 Artigos Retornados
- ▶ Critérios de inclusão/exclusão:
 - ▶ Etapa 1: 50 artigos
 - ▶ Etapa 2: 23 artigos

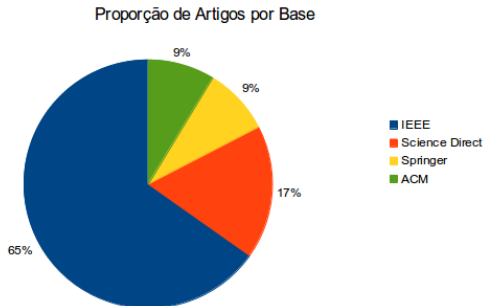


Figura 5 : Distribuição dos trabalhos por Base

- ▶ RQ1 - **Benefícios** do TBM no teste de segurança em **mobilidade, virtualização ou conectividade**
 - ▶ Abordagens identificadas permitem:
 - ▶ **Especificar** o comportamento de **sistemas e atacantes**
 - ▶ **Redução da ambiguidade** do plano de testes
 - ▶ Facilita **geração e replicação** de testes
 - ▶ Reuso de modelos: 7 trabalhos
 - ▶ Trabalhos futuros (2 trabalhos)
 - ▶ Casos de Teste **com oráculos**
 - ▶ Automação do teste de segurança
 - ▶ **Mobilidade, virtualização ou conectividade**: 6 estudos



Resultados

- ▶ RQ2 - **Perfil das abordagens** de TBM para teste de segurança
 - ▶ **Crescimento** na quantidade de estudos por ano

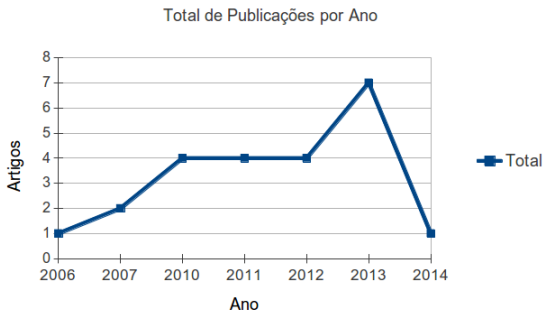


Figura 6 : Distribuição dos trabalhos ao longo do tempo

Resultados

- ▶ RQ2 - **Perfil das abordagens** de TBM para teste de segurança
 - ▶ Predominância de trabalhos usando **modelos baseados em transição**

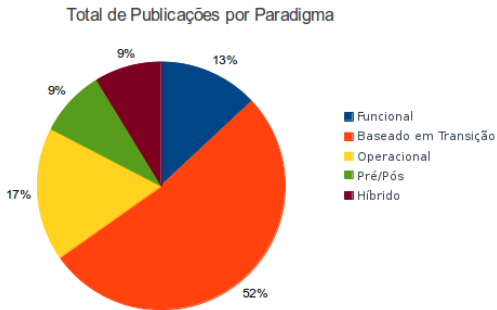
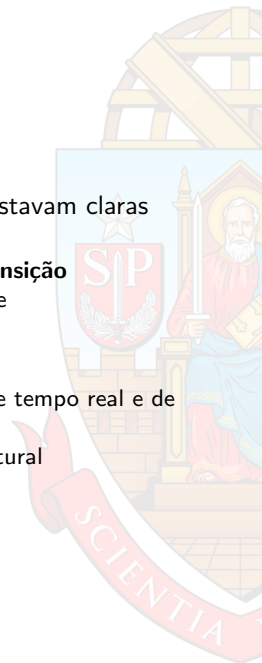


Figura 7 : Percentual de trabalhos por paradigma

- ▶ RQ2.1 - Taxonomia do TBM
 - ▶ Informações sobre as dimensões nem sempre estavam claras
 - ▶ Estava evidente:
 - ▶ Paradigma de modelagem: Baseados em **transição**
 - ▶ Assunto do modelo: $SUT > SUT + Ambiente$
 - ▶ Independência do modelo: Separado
 - ▶ Não estava claro:
 - ▶ Características de modelo: determinístico, de tempo real e de eventos discretos
 - ▶ Critério de seleção de teste: cobertura estrutural
 - ▶ Tecnologia: busca e execução simbólica
 - ▶ Online/Offline: offline



Resultados

- ▶ RQ2.2 - Tipo de SUTs
 - ▶ 74% usaram sistemas reais como SUT
 - ▶ smart-cards
 - ▶ políticas de segurança
 - ▶ aplicações móveis reais
- ▶ RQ2.3 - Desvantagens e limitações
 - ▶ Não há uma cobertura completa do processo de TBM
 - ▶ Geração de teste executável
 - ▶ Reuso de modelos
 - ▶ Esforço significativo na modelagem



- ▶ RQ2.4 - Exfiltração de dados
 - ▶ Nenhum trata especificamente sobre Exfiltração de Dados
 - ▶ Tratamento de ameaças relacionadas
 - ▶ quebra de sigilo de dados
 - ▶ requisitos de confidencialidade



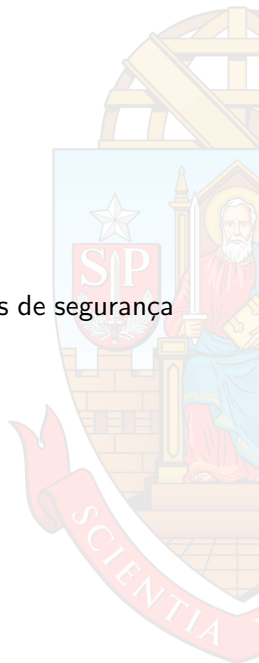
Ameaça a Validade

- ▶ Limitação da string de busca
- ▶ Sinônimos para TBM
- ▶ Termos relacionados a notações específicas
 - ▶ “Redes de petri”
 - ▶ “Máquinas de Estados Finitos”



Conclusão

- ▶ Número **crescente** de publicações
- ▶ **Automatizar a geração e replicação** de testes de segurança
 - ▶ Redução de **ambiguidade**
 - ▶ **Esforço** na modelagem: Usabilidade e Adoção





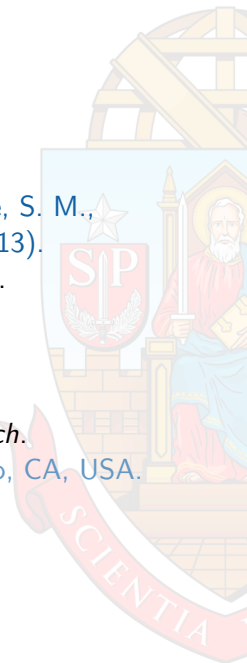
Conclusão

- ▶ Artigos analisados:
 - ▶ **Sistemas reais** como SUT
 - ▶ **Oráculos** de Teste
 - ▶ Predominância de **modelos baseado em transição**
- ▶ **Aderência parcial a taxonomia**
 - ▶ Dificulta a execução de **revisões e mapeamentos sistemáticos**
- ▶ **Lacuna** em exfiltração de dados



Referências

-  Rashid, A., Ramdhany, R., Edwards, M., Kibirige, S. M., Babar, A., Hutchison, D., and Chitchyan, R. (2013). Detecting and preventing data exfiltration report. <http://goo.gl/epK048>. Acessado em 10 de maio de 2014.
-  Utting, M. and Legiard, B. (2007). *Practical Model-Based Testing: A Tools Approach*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.



Obrigado!

