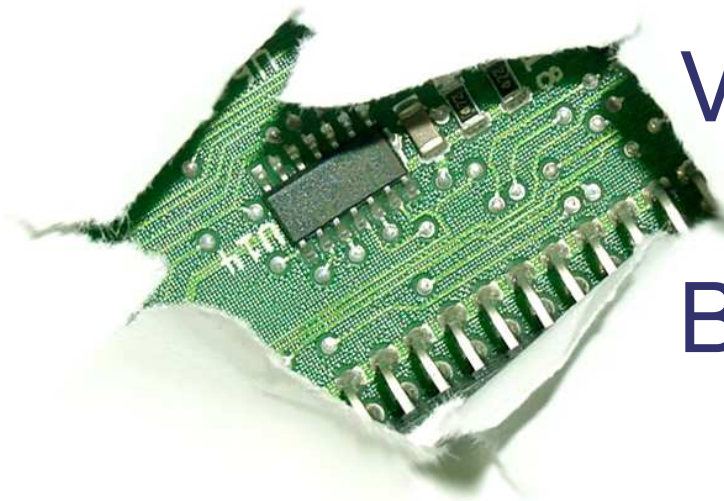


COMPSAC 2009, Seattle, WA  
Workshop on Security Aspects of Process  
and Services Engineering (SAPSE)



# Vulnerability Analysis of SOA-based Business Processes

Lutz Lowis  
Department of Telematics  
Institute of Computer Science and Social Studies (IIG)  
University of Freiburg, Germany  
lutz.lowis@iig.uni-freiburg.de  
<http://www.telematik.uni-freiburg.de>



# Vulnerability Classifications

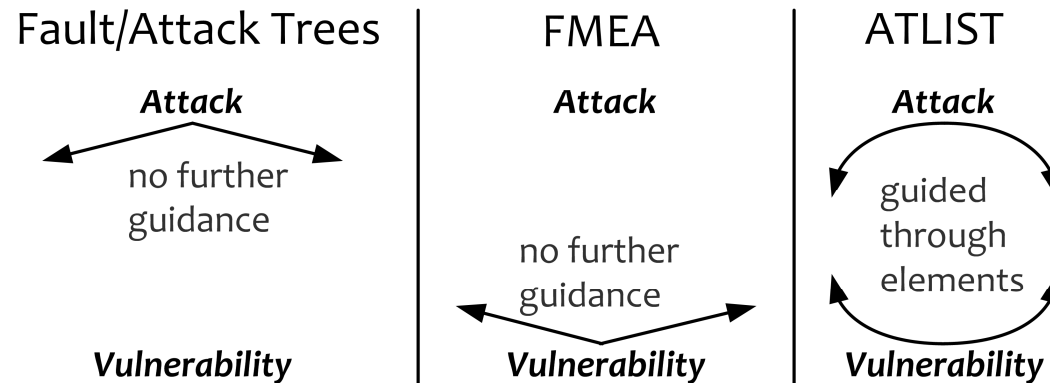
Name	Year	Focus	Attack Effect	Active Component	Involved Standard	Triggering Property
RISOS	1976	os	yes	indirect	-	indirect
Prot. Analysis	1978	os	-	-	-	yes
Hogan	1988	-	-	indirect	-	yes
Neumann	1989	sys/net	yes	indirect	-	yes
NRL	1994	sw	indirect	yes	-	yes
Brinkley	1995	sys	yes	-	-	indirect
Aslam	1996	os	indirect	indirect	indirect	yes
Cohen	1997	sys	yes	indirect	-	yes
Lindqvist	1997	-	yes	indirect	-	yes
Du	1997	sw	yes	-	indirect	yes
Howard	1998	-	yes	indirect	-	indirect
Krsul	1998	sw	indirect	indirect	-	yes
Piessens	2001	sw/net	indirect	indirect	indirect	indirect
Jiwani	2002	sw	yes	yes	-	yes
Alvarez	2003	web	yes	yes	yes	yes
WASC	2004	web	indirect	indirect	yes	yes
Langweg	2004	app sw	yes	yes	-	yes
Lindstrom	2004	w. services	yes	indirect	yes	yes
19 Sins	2005	sw	indirect	indirect	-	yes
7 Kingdoms	2005	sw	indirect	indirect	yes	yes
Weber	2005	sw	-	-	-	yes
Vanden Berghe	2006	w. services	-	yes	indirect	yes
PLOVER	2006	-	indirect	indirect	indirect	yes
OWASP	2006	web	-	indirect	-	indirect
Parrend	2007	java comp.	yes	yes	indirect	yes

# ATLIST

## A New Vulnerability Analysis Approach

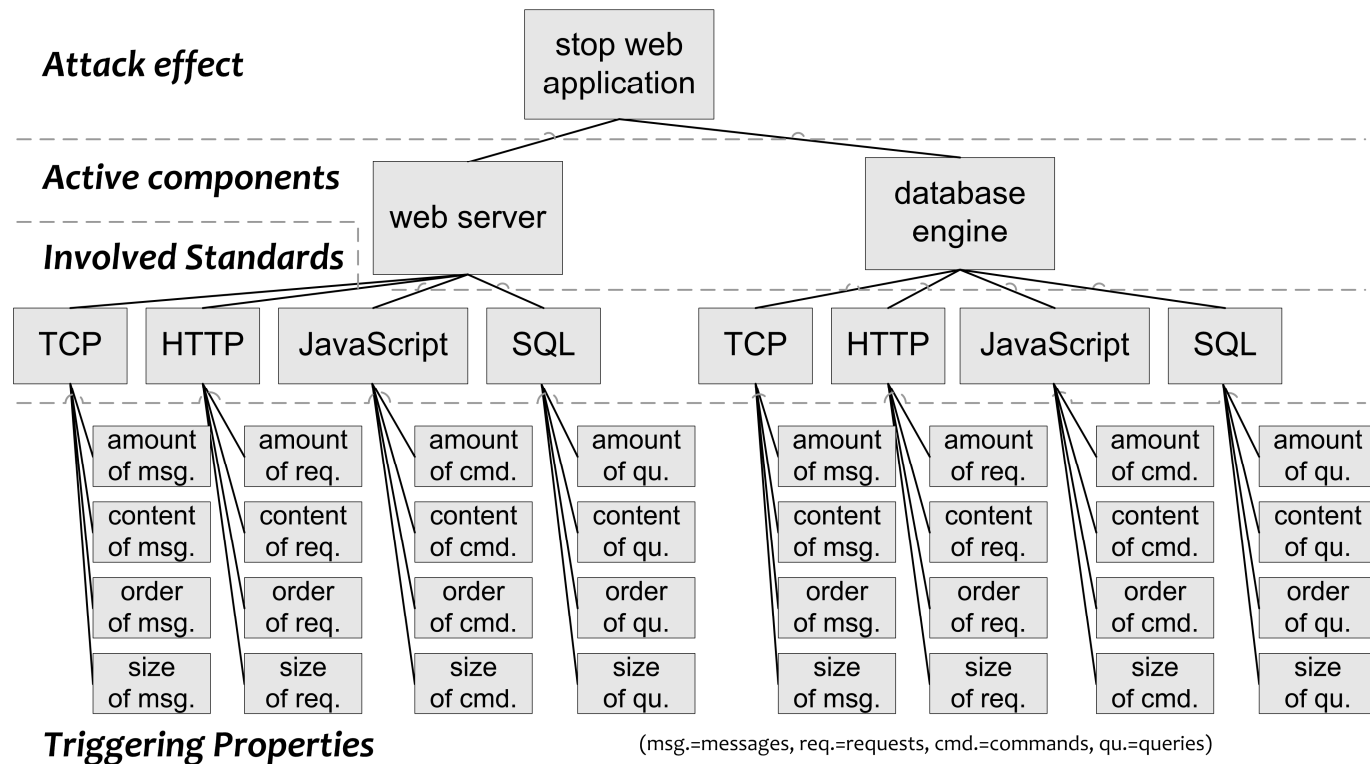
---

- Combines attack tree and FMEA notions
- Sets an explicit point of view
- Uses analysis elements for improved guidance



# ATLIST

## Exemplary Analysis Tree

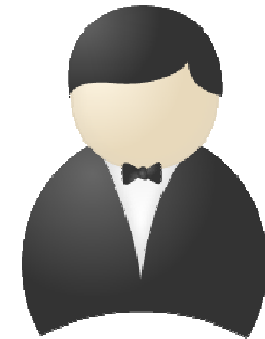


- Cross-layer challenge
- Pre- and post-conditions vs. “everything becomes possible“

# Business Processes and Compliance

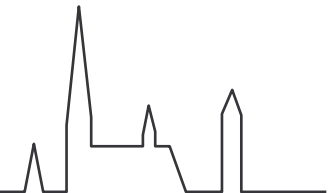
---

- Wide range from purely human to fully automated processes
- Compliance requires various controls, e.g., HIPAA's Privacy Rule
- Security and privacy controls must be included in the processes ("rewriting")
- Controls must be validated after execution ("audit")

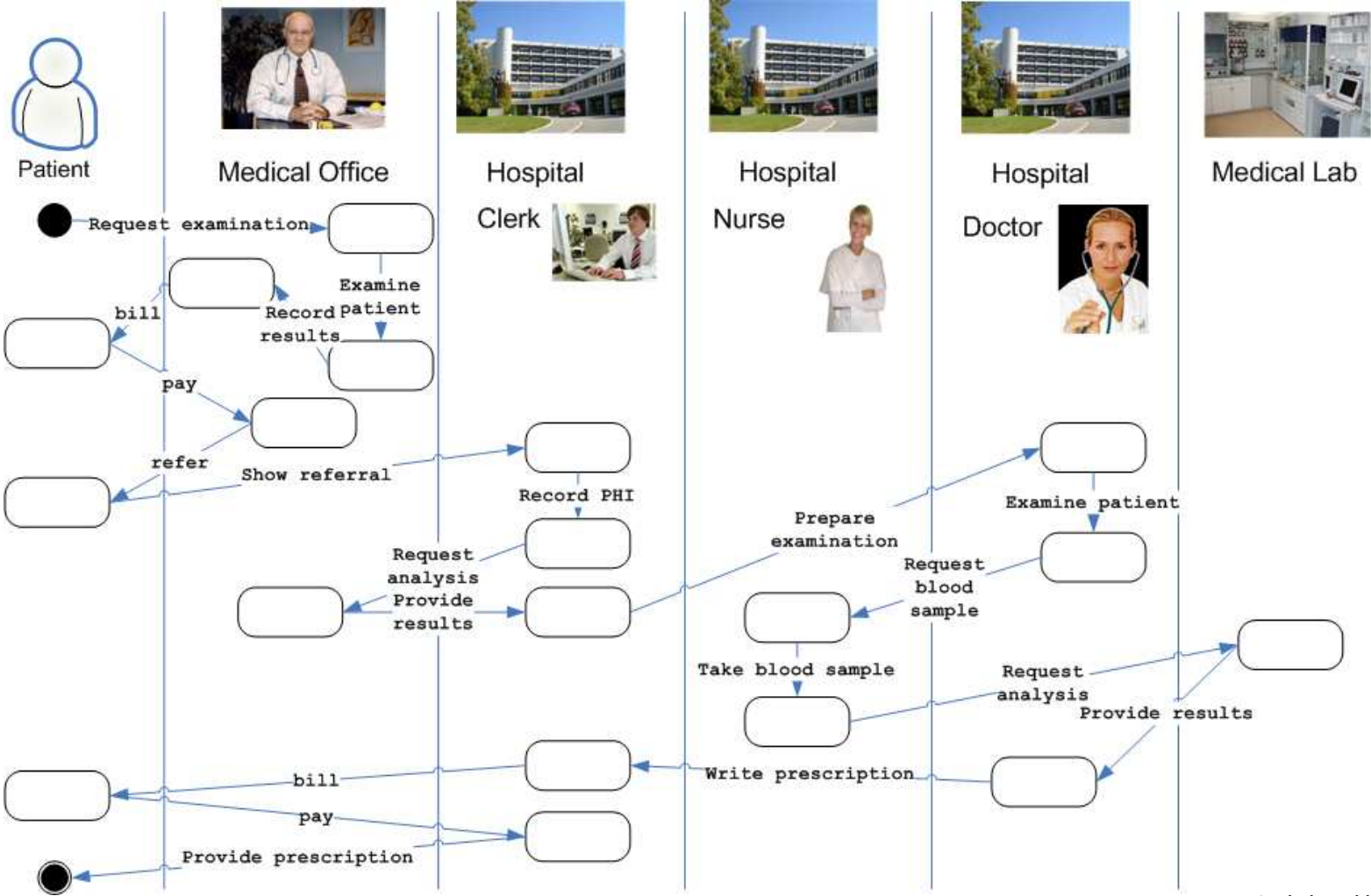


*Rewriting:* S. Höhn, "Model-based reasoning on the achievement of business goals," Proc. of the ACM SAC, 2009.

*Audit:* R. Accorsi "Counterexample-driven Audits," Submitted ACM TISSEC, 2009.



# Exemplary Process under HIPAA Privacy Rule



# Changes Introduce Vulnerabilities

---

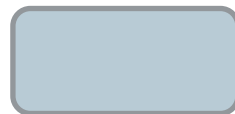
- Process flexibility is often used to sell SOA
- Changes can make the process insecure



Vulnerability regarding HIPAA's Privacy Rule "minimum necessary" req.:  
a flaw that allows to obtain more data than necessary for the given purpose



V1.0:  
**blood sample id**



*Request blood  
sample analysis*



V1.1:  
**name**  
**birth date**  
blood sample id



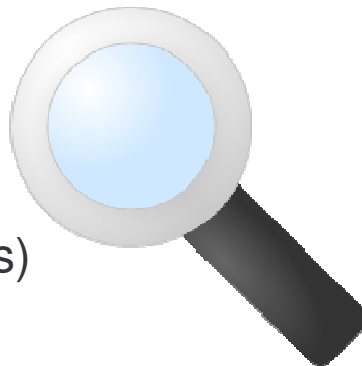
# Checking Processes For Vulnerabilities

---

- Policies are expressed in ExpDPT  $[[\neg](user, action, data, purpose)]+, condition, (ruling)$
- Processes are described in BPEL
- Services are described in WSDL

## **ExpDPT**

(external lab,view,  
blood sample id,analysis)



## **BPEL**

invoke  
analysis

## **WSDL**

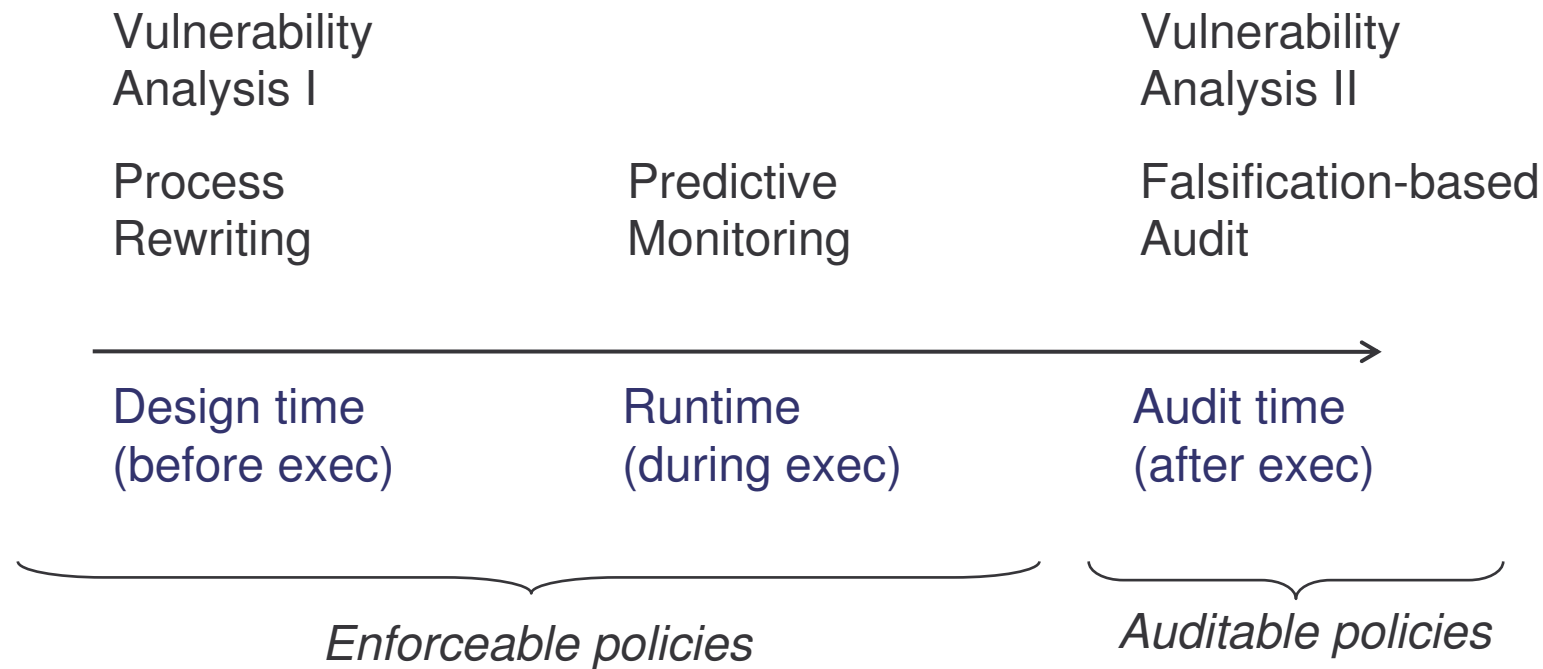


blood sample id,  
name, birth date

*Policies:* M. Kähler “Automating Privacy Compliance with ExpDPT,” IEEE CEC, 2008.

# Checking Timeline

---

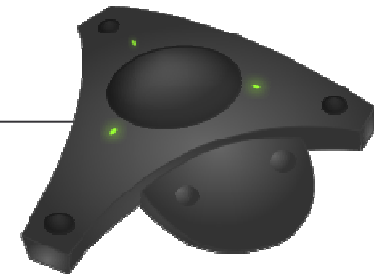


*Monitoring:* M. Gilliot et al., “Runtime prediction of policy violations in automated business processes,” IFIP, 2009 (to appear).

*Infowflow:* C. Wonnemann et al., “On Information Flow Forensics in Business Application Scenarios.,” Proc. IEEE COMPSAC, 2009.

# Let's talk!

---



- Vulnerability Analysis, Rewriting, Monitoring, Audit
- IIG Telematics:  
Information flow related analysis of business processes
  - explicit and implicit flows,
  - analysis before, during, and after process execution,
  - analysis of single processes, process interactions, and sets of processes,
  - analysis regarding various policy violations in terms of security and privacy; HIPAA Privacy Rule “minimum necessary“ is just one example.

Lutz Lowis  
Department of Telematics  
Institute of Computer Science and Social Studies (IIG)  
University of Freiburg, Germany  
**[lutz.lowis@iig.uni-freiburg.de](mailto:lutz.lowis@iig.uni-freiburg.de)**  
<http://www.telematik.uni-freiburg.de>

