SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Using Threat Model for Scoping of Penetration Testing

Daniel Kefer

1&1 Internet AG

Whoami

- VUT Brno – FEKT
- AEC, spol. s.r.o. (2005 - 2011)
- 1&1 Internet AG (2011 -)

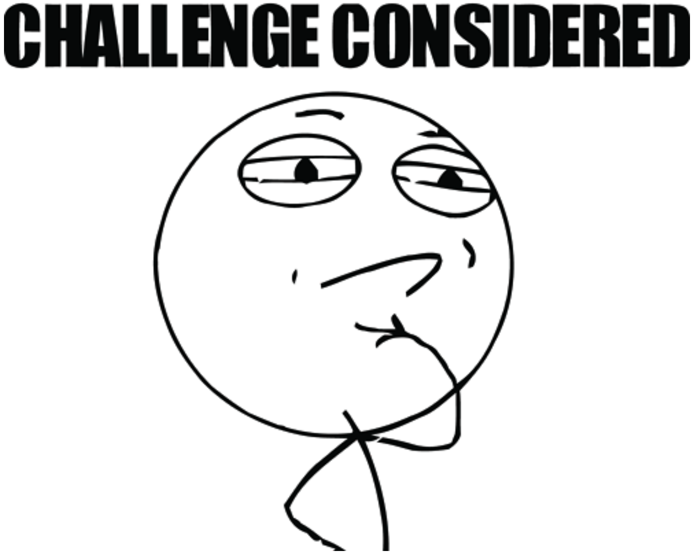
- Penetration tester since 2007
- Security in SDLC since 2008

Agenda

- Challenges
- Threat model and common techniques
- Integration of the threat modelling approach into a pentest project

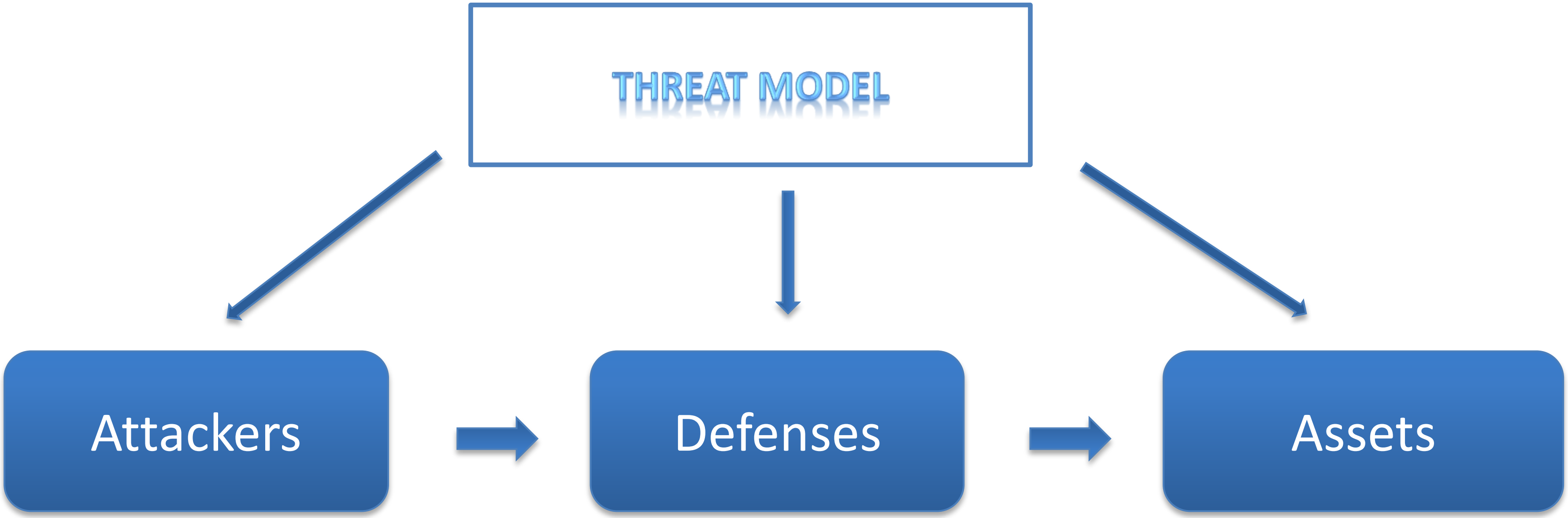
Challenges

- Security audit = penetration test?
- How much to invest?
- Scoping/coverage of a test?
- Pentester vs pentester.sh?



Challenges

Threat Model



Who Is the Attacker?

Who Is the Attacker?

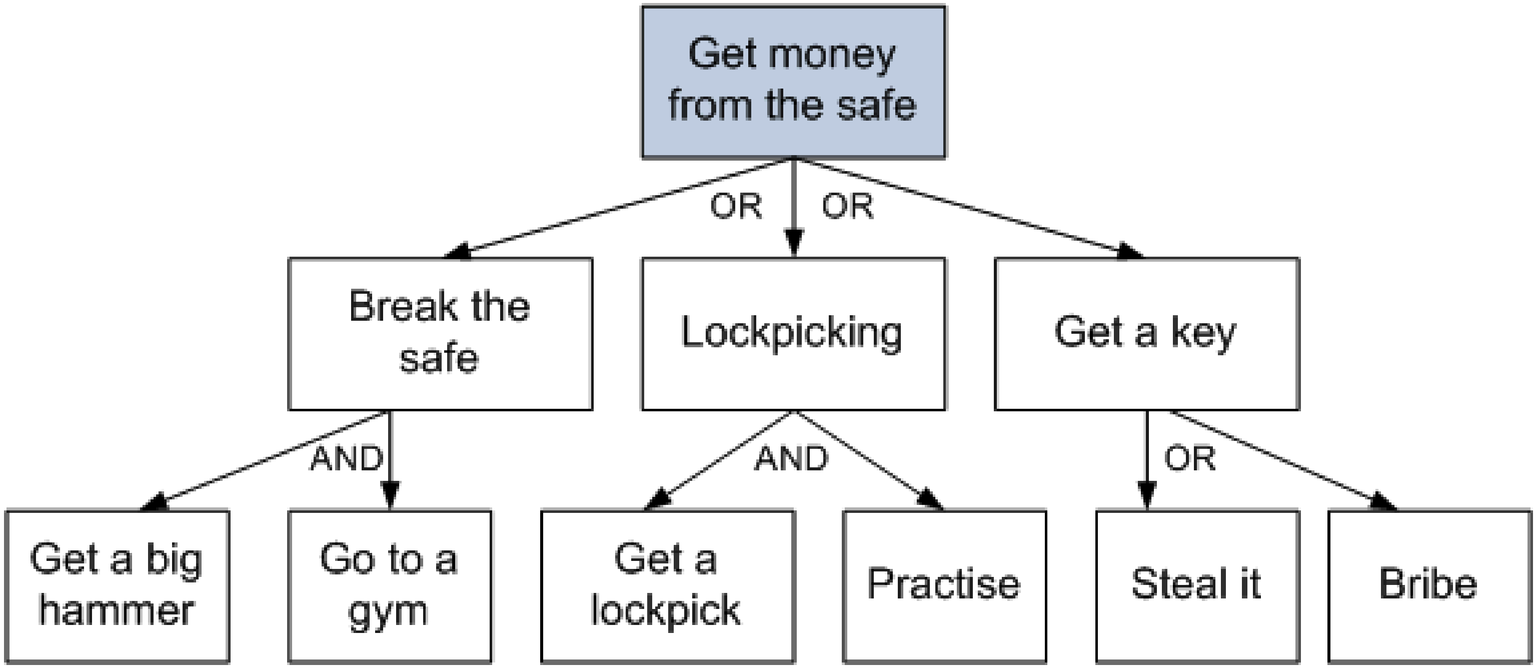
- Sandia National Laboratories: Cyber Threat Metrics
  - Motivation
  - Resources
- Take it as a starting point

Who Is the Attacker?

Group	Intensity	Stealth	Time	Personnel	Cyber-knowledge	System-knowledge	Access	Total
Admin	2	3	2	1	3	2	3	16
RoleA	1	2	1	2	2	3	2	13
RoleB	1	3	1	2	1	2	2	12
Employee	1	2	1	3	1	1	1	10
Former E.	1	1	3	1	1	2	0	9

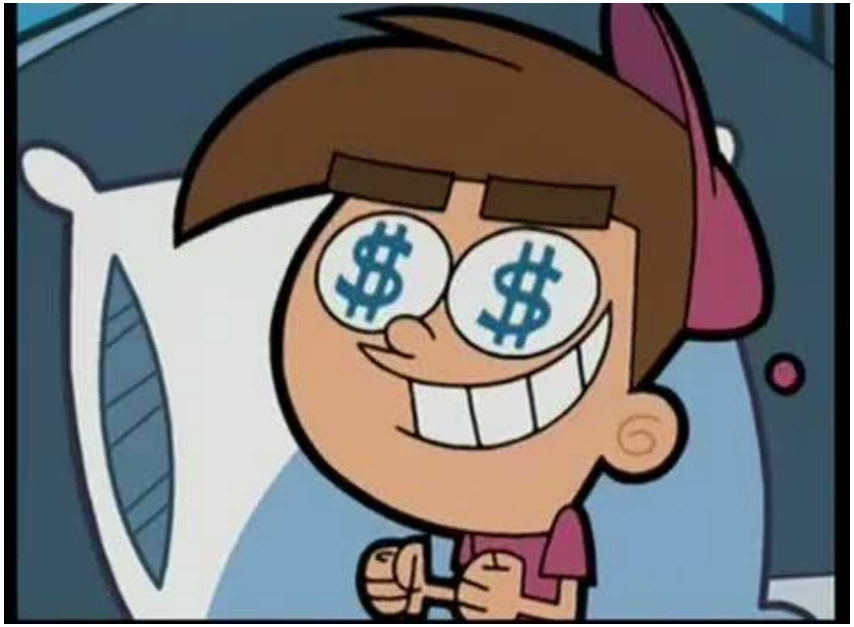
Attack Trees

- Bruce Schneier: Modelling security threats (1999)



Attack Trees

- Definition of targets:
  - Worst-case scenarios for particular assets
  - Examine functional requirements for underlying risks
  - Negation of use cases



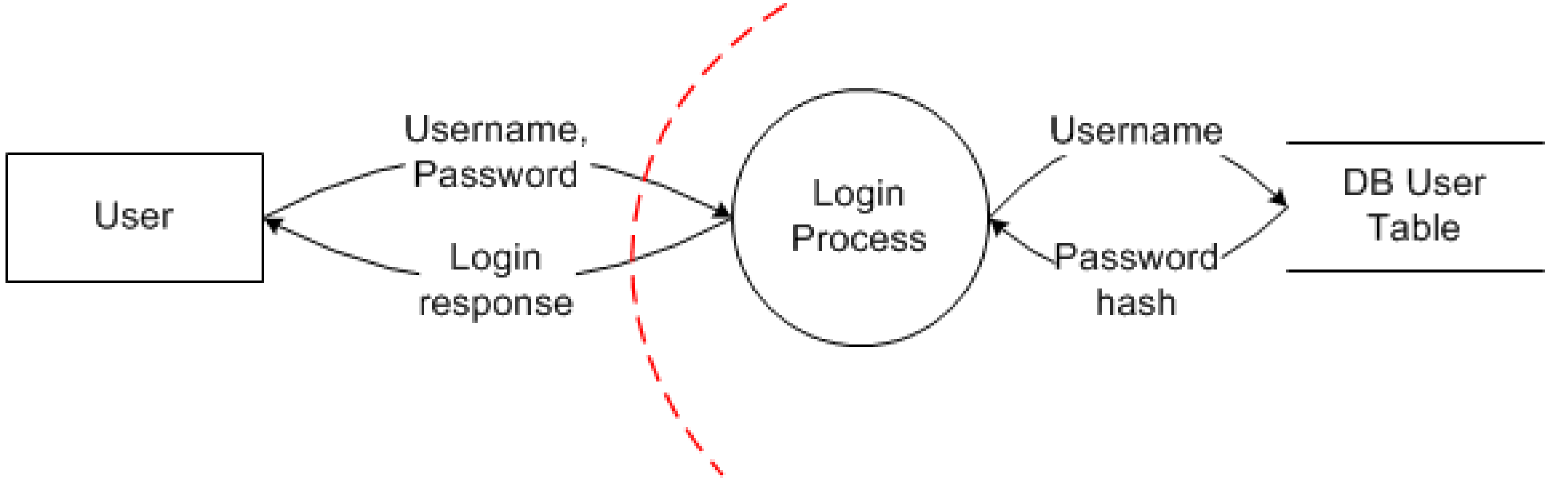
STRIDE

- One of the crucial activities in the Microsoft SDL Process:

Threat	Mitigation
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non Repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

- Application of the threats to „Data Flow Diagrams“

STRIDE



Login process

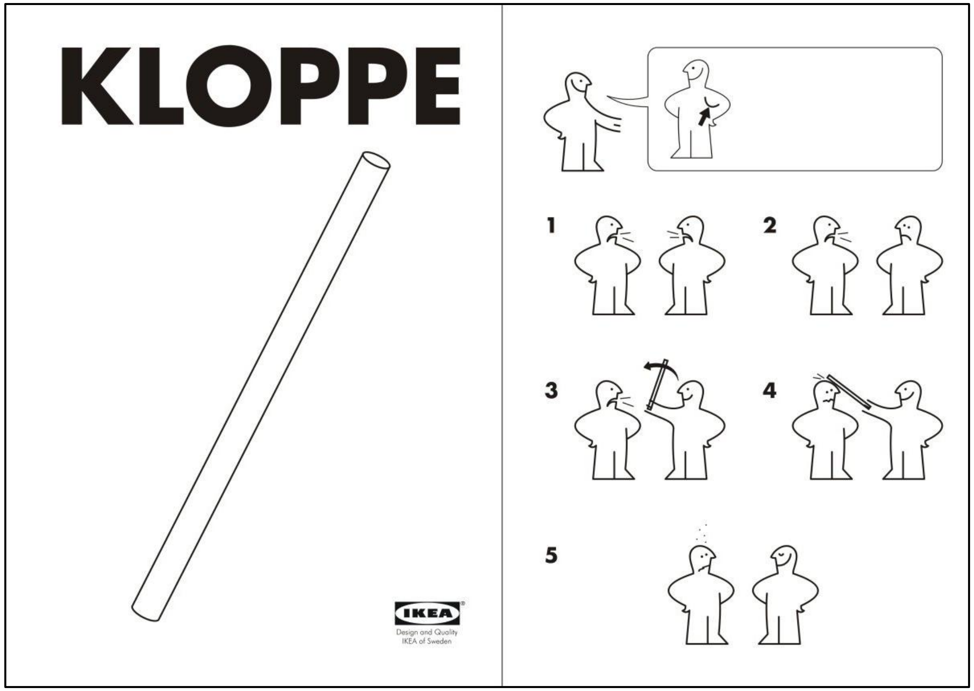
	S	T	R	I	D	E
Data Flows		X		X	X	
Data Stores		X		X	X	
Processes	X	X	X	X	X	X
Interactors	X		X			

Project

1. Documentation review, identification of the workshop team
2. Workshop
   1. HLA Diagram
   2. Asset definition (data & functional assets)
   3. Understanding of user roles & attacker groups definition
   4. Attack trees
   5. Apply STRIDE on HLA Diagram (+ attack trees)
3. Prepare the assignment (+ testing scenarios)

Toolset

- MS Word, Excel, Visio ☺
- Microsoft SDL Threat Modelling Tool
- Seamonster



Wrap-up

- Security audit doesn‘t have to be a pentest only
- Attacker doesn‘t have to be an anonymous person only
- Threat model doesn‘t have to serve to the pentest project definition only

SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Daniel Kefer

1&1 Internet AG

daniel.kefer@1und1.de

? PROSTOR PRO OTÁZKY