

The TREsPASS project



Technology-supported Risk
Estimation by Predictive
Assessment of Socio-technical
Security

Dr. Lorena Montoya
Services, Cyber-security and Safety Dept.
University of Twente



Motivation



May 9, 2011

Sony suffers an estimated **\$ 1.25 billion** damage through hacking attack



April 23, 2013

Cost of cyber attacks **triples** in a year



Jan 30, 2013

New York times **infiltrated** by Chinese hackers

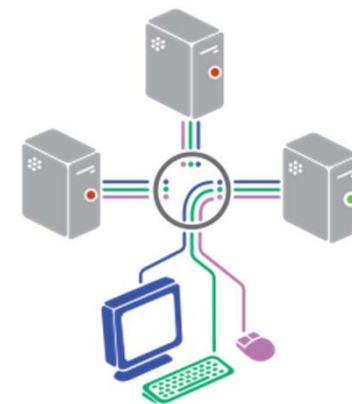
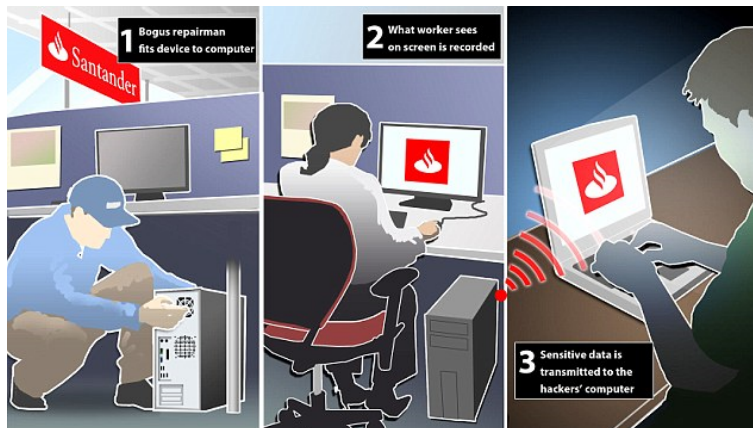


DBIR 2013

Social engineering a key factor in 92 % of industrial espionage attacks

Complex attacks cost billions

Barclays hacking attack: unusual pairing of physical deception (i.e. bogus IT guys) and advanced surveillance via a KVM switch – 1.3 million UK pounds



Source: Daily Mail, UK (20-9-2013)

Goal

Which are the possible attacks?

- currently field works on basis of checklists/experience

Which attacks to block?

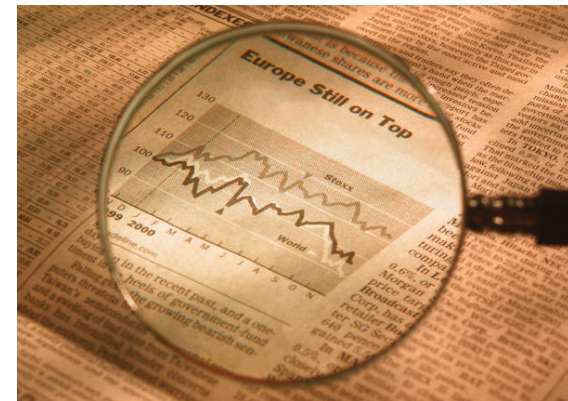
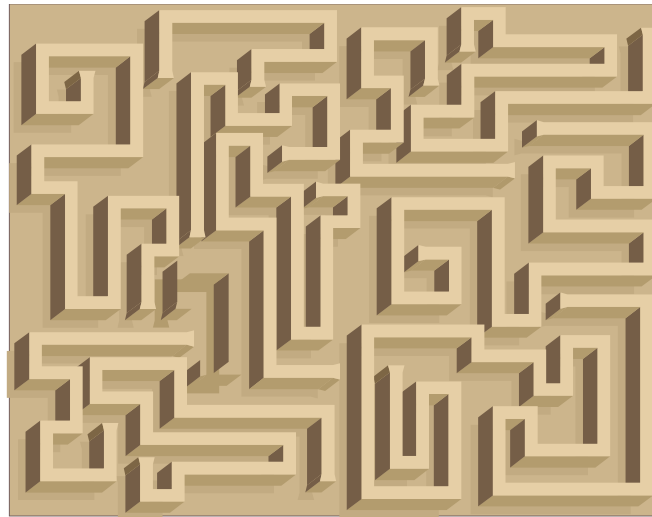
- attacks need to be ranked (financial, reputation).

Develop a toolkit for enterprise risk management

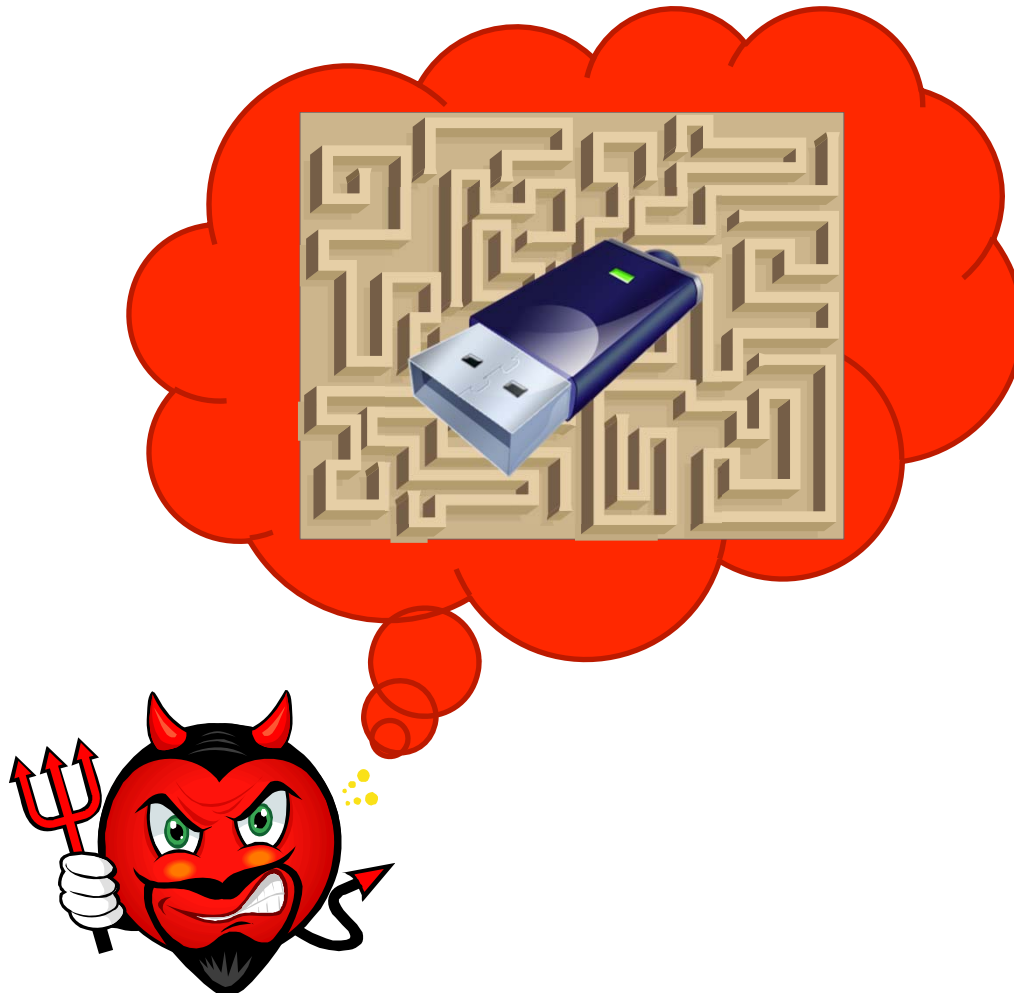
- lightweight version of the toolkit aimed at SMEs

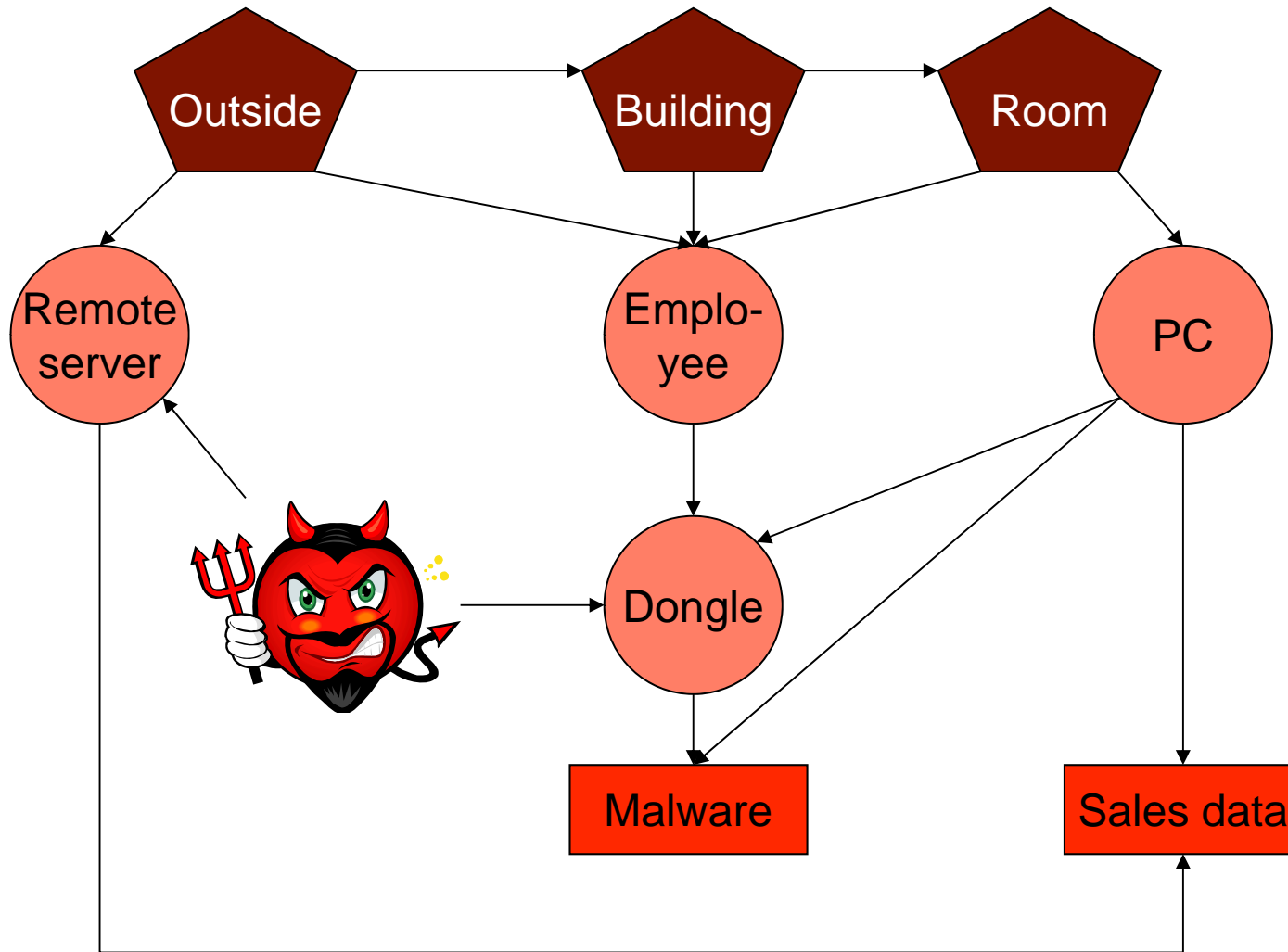
rapidly changing infrastructure, including physical security and human behaviour

How to get the data?

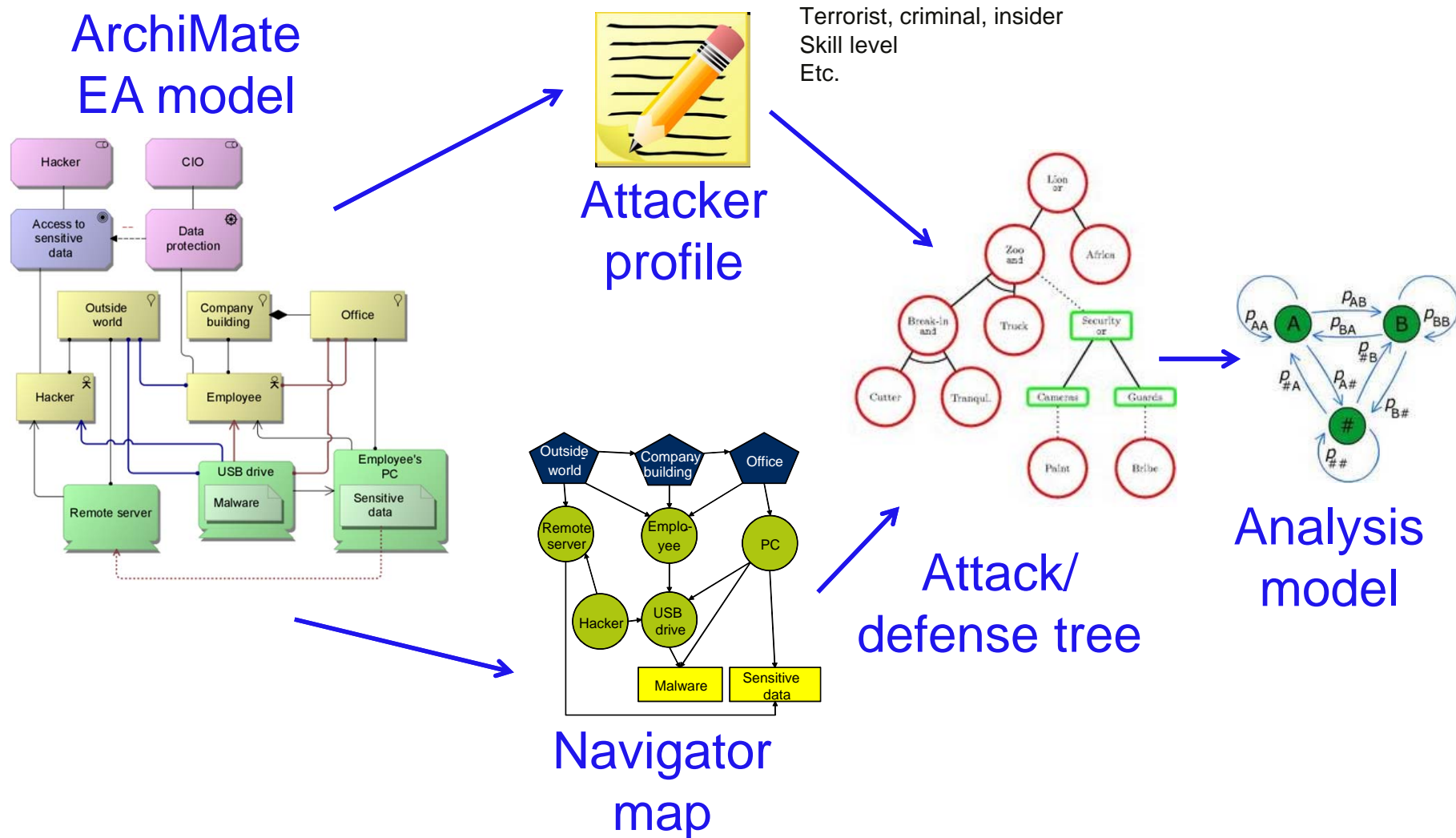


Ask the TREsPASS Attack Navigator!





TREsPASS Model Chain



Key project goals

Predict complex attack scenarios spanning *digital, physical* and *social engineering* steps

Prioritise these scenarios via a planning tool that tells defenders where to expect the most serious issues

Prevent attacks by calculating and comparing cost-effectiveness of countermeasures

The project combines

Technical sciences how vulnerable are protocols and software?

Social sciences how likely people are to succumb to social engineering?

State-of-the-art industry processes and tools

In order to

Enable informed decisions on security investments

Reduce security incidents

Increase resilience

The TREsPASS partners

- 16 partners
- From 8 European countries

University of Twente, NL

Technical University of Denmark, DK

Cybernetica, EE

GMV, PT & ES

Royal Holloway, Univ. of London, UK

itrust, LU

Goethe University Frankfurt, DE

IBM Research Zürich, CH

Delft University of Technology, NL

Hamburg University of Technology, DE

University of Luxembourg, LU

Aalborg University, DK

Consult Hyperion, UK

BizzDesign, NL

Deloitte, NL

Lust, NL

Key Year 1 Achievement

From hand-crafted attack tree

to

Explicit navigator map which automatically generates
an attack tree

Contact



www.trespass-project.eu

Email: contact@trespass-project.eu

Contact us to join our public mailing list!



@TREsPASSproject

trespass-project

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 318003 (TREsPASS). This publication reflects only the author's views and the Union is not liable for any use that may be made of the information contained herein.

