Modeling and Analysing Socio-Technical Systems

Zaruhi Aslanyan, Marieta G. Ivanova,
Flemming Nielson, Christian W. Probst

DTU Compute, Technical University of Denmark

STPIS 2015, poster session

09th June 2015

DTU

predict
prioritise
prevent

TRESPASS

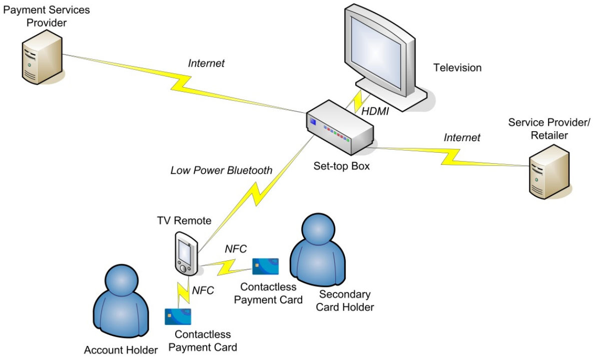
The Challenge

- Organisations are complex socio-technical systems
- They consist of a mixture of physical infrastructure, human actors, policies and processes
- Attacks exploit vulnerabilities on all different levels
- Many risk assessment methods abstract away the internal structure and ignore human factors

Contribution

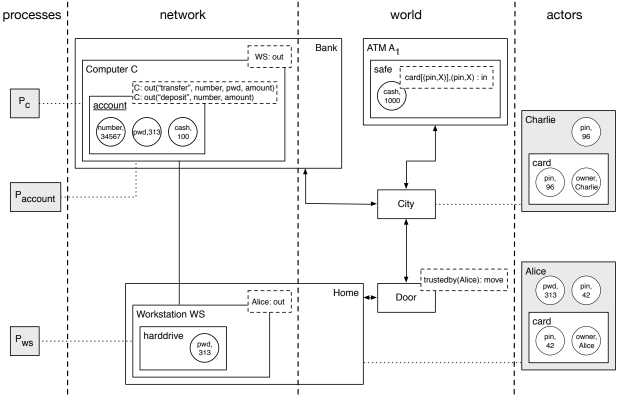
- Model all relevant levels of socio-technical systems
- Analyse the security properties of the model

Use Case Scenario

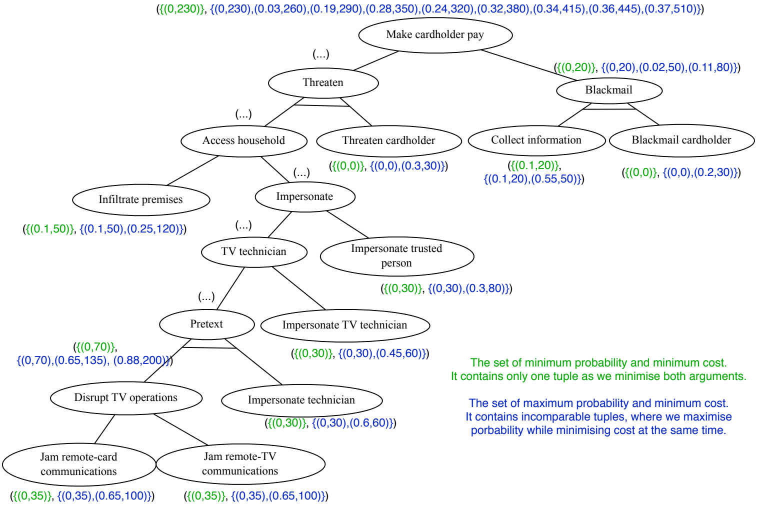


Attack goal: stealing money from the cardholder by forcing him/her to pay for fake services.

The Model


processes
network
world
actors
P_c
$P_{account}$
P_{WS}
Bank
WS: out
Computer C
C: out("transfer", number, pwd, amount)
C: out("deposit", number, amount)
account
number, 34567
pwd,313
cash, 100
ATM A_1
safe
card[(pin,X)],(pin,X) : in
cash, 1000
City
Door
trustedby(Alice): move
Home
Alice: out
Workstation WS
harddrive
pwd, 313
Charlie
pin, 96
card
pin, 96
owner, Charlie
Alice
pwd, 313
pin, 42
card
pin, 42
owner, Alice

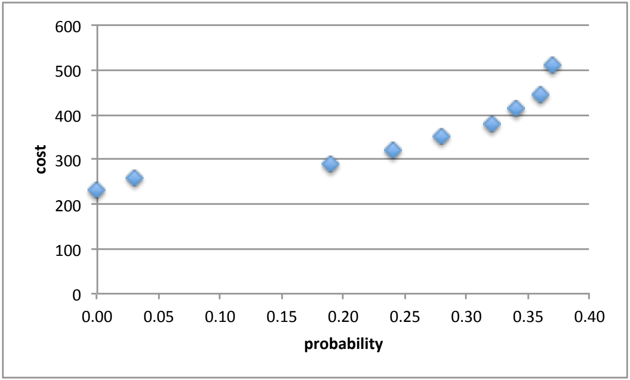
Attack Trees



The set of minimum probability and minimum cost.
It contains only one tuple as we minimise both arguments.

The set of maximum probability and minimum cost.
It contains incomparable tuples, where we maximise porbability while minimising cost at the same time.

Analysis



600
500
400
300
200
100
0
cost
0.00
0.05
0.10
0.15
0.20
0.25
0.30
0.35
0.40
probability

Future Work

- Consider different actors' behaviour
- Consider countermeasures
- Evaluate attack and defence scenarios

predict
prioritise
prevent
TRESPASS

Modelling and Analysing Socio-Technical Systems

Zaruhi Aslanyan, Marieta G. Ivanova, Flemming Nielson, Christian W. Probst
{zaas, mgiv, fnie, cwpr} @ dtu.dk
Language Based Technology, DTU Compute, Technical University of Denmark

DTU

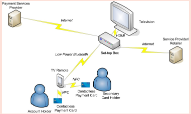
The challenge

- Organisations are complex socio-technical systems
- They consist of a mixture of physical infrastructure, human actors, policies and processes
- Attacks exploit vulnerabilities on all different levels
- Many risk assessment methods abstract away the internal structure and ignore human factors

Contribution

- Model all relevant levels of socio-technical systems
- Analyse the security properties of the model

Use Case Scenario

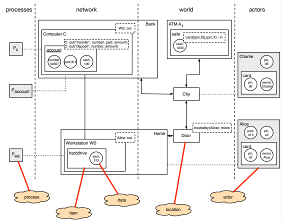


A home-payment system

- people can pay services remotely
- payment performed through a television box
- by using a contact-less payment card
- card protected by password

Attack goal: stealing money from the cardholder by forcing him/her to pay for fake services.

The Model

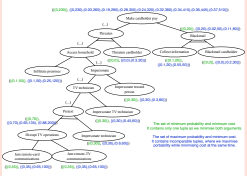


- Actors contain the items or data owned by the actor
- Solid lines represent the physical connections between locations
- Dotted lines represent the present location of actors and processes
- The dashed rectangles in the upper right part of some nodes represent the policies assigned to these nodes

Future Work

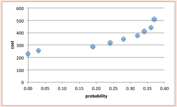
- Consider different actors' behaviour
- Consider countermeasures
- Evaluate attack and defence scenarios

The Evaluation of the Attack Tree of the Scenario



- The root - the main goal of the attacker
- The leaves - the attacker's basic actions
- The internal nodes - the sub-goals of the attacker

Pareto Efficient Solutions of the Scenario



The points in the figure illustrate the Pareto efficient solutions, the solutions with maximum probability and minimum cost. We can see the rank of the probabilities and the costs.

References

1. Probst, C.W., Hansen, R.R.: An extensible analysable system model. Information Security Technical Report 13(4) (2008)
2. Boender, J., Ivanova, M.G., Kammüller, F., Primiero, G.: Modeling human behaviour with higher order logic: Insider threats. 4th Workshop on Socio-Technical Aspects in Security and Trust (2014)
3. Schneier, B.: Attack Trees: Modeling Security Threats. Dr. Dobb's Journal of Software Tools 24(12) (1999)
4. Aslanyan, Z., Nielson, F.: Pareto efficient solutions of attack-defence trees. In: 4th International Conference on Principles of Security and Trust (2015)

Language Based Technology - DTU Compute - Technical University of Denmark http://compute.dtu.dk