Compositional Security Modelling: Structure, Economics, and Behaviour

Tristan Caulfield [1] David Pym [1] Julian Williams [2]

[1]Department of Computer Science, University College London
[2]Business School, University of Durham

26th June 2014

Security Policy

- Security managers must choose policies.
  - Subject to economic and regulatory constraints.
- Security policies are often onerous and can inhibit productivity.
  - Employees circumvent them to fulfil higher priority tasks (i.e. work).
- Currently hard to analyse consequences of policy decisions.
  - Managers must rely on their own judgement.
  - Difficult to show how optimal these decisions may be.

Goal

- Develop a framework for modelling security policy decisions and consequences.
- Capture not just policy, but also system architecture and user behaviour.
- Express the optimality of decisions in terms of security manager's preferences.
- Should be compositional.
  - Allows complex systems to be divided into manageable pieces.
  - Lets us examine the interactions between models.

Approach

- Develop a framework based on Distributed Systems Modelling
  - Offers a convenient abstraction.
  - Rigorous mathematical treatment.
  - **Processes**: process algebra.
  - **Resources**: resource semantics, BI, separation logic.
  - **Locations**: directed graph-like structure.
  - **Environment**: stochastic processes. Does an action happen?
- Implement a framework and models in the Julia language.

Agents and Decisions

- Agents have preferences.
  - For productivity, security, individual welfare, etc.
- Make decisions based on these preferences and on the current state of the model.
- Decisions are in Cobb-Douglas form: $D = \delta X^{\alpha} Y^{\beta}$
  - X and Y are values of different alternatives.
  - α and β are the relative likelihood of these alternatives. ($\alpha + \beta = 1$)
  - Allows for composition.

UCL

Security Manager's Utility

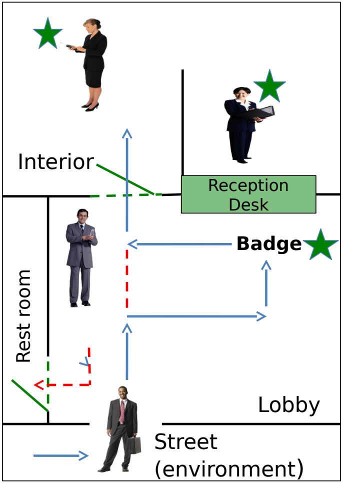
- Each model execution has a set D of decisions made.
  - $D = \{ D_i = \delta_i X_{i_1}^{\lambda_{i_1}} \ldots X_{i_k}^{\lambda_{i_k}} \mid i = 1, \ldots, m \}$
- Security managers care about particular attributes.
  - These are determined by decisions in the model.
  - An attribute V has a target value, $\bar{V}$.
  - A manager assigns a value to the deviation from the target value $f(V - \bar{V}.)$

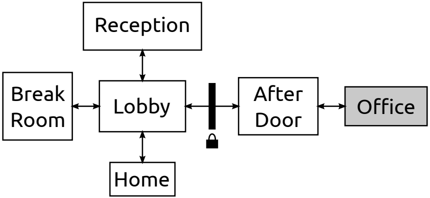
Overall Expected Utility

$$\mathbb{E}[U(D_1, \ldots, D_m)] = \mathbb{E}\left[\sum_{r=1}^{n} w_r f_r(V_r(D_1, \ldots, D_m) - \bar{V}_r)\right]$$

Models

Tailgating

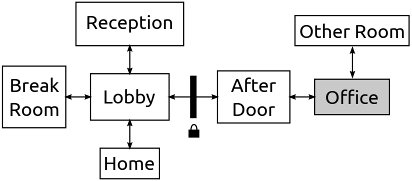




Models

Composed

- Another model: Screen Locking.
- Composed with tailgating model.
- Allows us to examine interactions between models.
  - Do entry security controls mitigate lapses in other areas?



Results

Rec	Grds	Prod	Sec	Wait	Tail	Succ	Access
60	0	0.2	0.2	1995.73	9.56	5.42	8.76
60	0	0.8	0.2	929.68	11.58	5.47	10.48
120	0	0.2	0.2	3156.48	12.78	5.20	9.05
120	0	0.8	0.2	1517.90	14.62	6.15	13.63
60	1	0.2	0.2	1863.38	8.13	1.50	3.27
60	1	0.8	0.2	1160.51	12.80	2.53	6.00
120	1	0.2	0.2	4126.91	12.85	2.17	5.68
120	1	0.8	0.2	1981.08	15.50	2.48	4.02

Further Work

- Mathematical definitions of models and composition.
- Library of scenarios.
- Integration of modelling and data collection.

Thanks!

Any questions?