# Social Learning in Systems Security Modelling

Tristan Caulfield, Michelle Baddeley, and David Pym

University College London
t.caulfield@ucl.ac.uk, m.baddeley@ucl.ac.uk, d.pym@ucl.ac.uk

**Abstract** Systems modelling can be used to help improve decisions around security policy. By modelling a complex system, the interactions between its structure, environment, technology, policies, and human agents can be understood and the effects of different policy choices on the system can be explored. Of key importance is capturing the behaviour of human agents within the system. In this paper we present a model of social learning from behavioural economics and then integrate it into a mathematical systems modelling framework. We demonstrate this with an example: employees deciding whether or not to challenge people without ID badges in the office.

## 1 Introduction

Deciding about security policy is complicated. Security policy effectiveness depends on many factors: choice of technologies; system structure; system processes; the system's environment; and the behaviour of the human agents that constitute and interact with the system. Given these complexities, it is hard to predict what effects different policy choices will have on the performance and security of a system. Models are useful for predicting the consequences of design decisions, and systems models, which can capture the structure, behaviour, and environment of a system as well as the behaviour of agents interacting with it, are particularly suited to this task. Recent work has looked at using systems models to improve security policy decisions [11,12,13], focusing on physical security, such as how employees and attackers can tailgate through access control at building entrances. These models captured agent's behaviour, using standard utility rmaximization principles to model decision-making. In reality however, human behaviour and decision-making is complicated by social influences and peer pressures. Insights from behavioural economics can be used to better model the way people make decisions. In this paper, we look at how social learning can influence decisions, leading to herding behaviours. We integrate this model within the existing systems modelling framework and demonstrate social influences via an example, in which employees must decide whether or not to challenge a person without an ID badge in an office.

## 2 Systems Modelling

Mathematical modelling is a key tool in designing and reasoning about the complex systems of systems upon which the world depends. For modelling complex

information processing systems, including both logical and physical components, the classical theory of distributed systems — see, for example, [16] for an elegant account — provides a suitable conceptual basis [15] for a modelling discipline. Executable modelling languages are important supporting tools, providing methods for simulating — using both Monte Carlo and what-if methods — systems that are too complex for useful analytical solvable descriptions.

The model and simulations in this paper are created and executed using a systems modelling framework, written in the julia language [18], and developed in recent work [11,12,13]. This framework is built upon a compositional mathematical systems modelling theory, which is grounded in process algebra [20,21] and logical resource semantics [22,17,15,3], and has been developed in detail by some of us elsewhere [14,15,3].

The structure of models in the framework and in the underlying theory is based on the following concepts from distributed systems theory, each of which is handled compositionally:

- *Location*: Places are connected by (directed) links. Locations may be abstracted and refined provided the connectivity of the links and the placement of resources is respected. Mathematically, the axioms for locations [15] are satisfied by various graphical structures, as well as various topological constructions [14,15,3];
- *Resource*: The notion of resource captures the components of the system that are manipulated (e.g., consumed, produced, moved) by its processes. Resources include things like computer memory, system operating staff, or system users, as well as money. Conceptually, the axioms of resources are that they can be combined and compared. Mathematically, we model this notion using *(partial commutative) resource monoids* [17,15,3];
- *Process*: The notion of process captures the (operational) dynamics of the system. Processes manipulate resources in order to deliver the system's intended services. Mathematically, we use algebraic representation of processes based on the ideas in [20], integrated with the notions of resource and location [14,15]. The execution of models based on these concepts, as formulated in [15], is described by a transition system with a basic structural operational semantics judgement [23,20] of the form

$$L, R, E \xrightarrow{a} L', R', E',$$

which is read as 'the occurrence of the action $a$ evolves the process $E$, relative to resources $R$ at locations $L$, to become the process $E'$, which then evolves relative to resources $R'$ at locations $L'$'. The meaning of this judgement is given by a structural operational semantics [23,20].

It is important to note that not only are these structural building blocks of models set up to be compositional but models themselves are compositional. Interfaces define how models compose together: which locations are shared between models, and how process execution transitions from one model to another. Compositionality of models is important. It lets complex systems be modelled by

building less complex models that represent parts of the original system and combining them together.

In addition to the structural components of models, we consider also the environment within which a system exists:

- *Environment*: All systems exist within an external environment, which is typically treated as a source of events that are incident upon the system rather than being explicitly stated. Mathematically, environments are represented stochastically, using probability distributions that are sampled in order to provide such events [15,11,12,13].

The framework for building and executing these models corresponds directly to the mathematical concepts above. Processes, written as functions in julia code, claim and manipulate resources, moving them between the connected locations in the model, and can then release them so that they are available to other processes. A scheduler, in the style of discrete event simulation, manages the execution of the model, keeping track of simulation time and ordering the execution of processes.

In this modelling framework [11,12,13], agents are constructed out of a combination of a process, a resource, and some number of locations. The resource represents the agent's physical location within the model; the locations are used to model, for example, things the agent is carrying, or information known and remembered by the agent; the process controls the agents behaviour: it moves the agent's resource through the various physical locations in the model, interacts with other processes, including other agents, by manipulating resources, and defines how the agent makes decisions.

In previous work, agents' decision-making has been implemented as straightforward utility rmaximization. An agent, such as an employee, has preferences towards productivity and security, and makes the choice that rmaximizes utility based on these preferences and the current state of the simulation.

## 3 Social Learning and Information Cascades

Social influences on decision-making have been identified across a range of literatures; for example, see Baddeley [5,6]. Social psychologists have also explored the power of social influences, for example Solomon Asch's line experiments showed that experimental participants can be manipulated by information about wrong choices into making mistakes, even with very unambiguous tasks, such as judging the length of a line [4]. This finding that has been replicated in a large number experimental studies [10] and captures the impact of peer pressure and social influence on decision-making. Bikhchandani, Hirshleifer and Welch [8,9] enumerate a range of mechanisms encouraging people to imitate others: sanctions on deviants; benefits of buying into an asset market propelling further price rises; preferences for conformity; communication; and social learning, the focus of this paper. This uniform social behaviour can explain a wide range of phenomena

from political campaigning successes, foraging and mating behavior amongst animals, and competing bids during corporate takeovers.

Economic models of herding describe imitation as a boundedly rational strategy given information constraints. Herding emerges as a Bayes-rational sequential learning process, generating 'information cascades': people observe social information about others' actions and apply Bayes' rule to update their probability estimates. They balance their private information and prior probabilities against the probabilities they infer from the social information. Differences in posterior probabilities across individuals are not necessarily the result of heterogeneity in personality and preferences, but may instead reflect differences in private versus social information. If an individual comes from a position of relative ignorance or inexperience, then they may rationally decide to embed social information into their probability judgements, assuming that other decision-makers' have superior information and so their actions are informative.

Bikhchandai et al. [8] show localized conformity emerging when it is optimal for an individual to follow the actions of his/her predecessor and to disregard his private information, generating information cascades. Banerjee [7] develops a similar herding model, illustrating with the example of choosing a restaurant. If we are choosing between two restaurants, A and B, we may have our own private information that Restaurant B is very good; for example, we've recently read a good review, or had a recommendation from a friend. But then we see a queue of people wanting to eat next door, at a very crowded Restaurant A, whilst restaurant B is empty. We may infer that the people in the queue have better information than we do about the relative quality of the two restaurants and so we decide to follow them. In this way, social learning leads to social information about others' decisions cascading through the herd. Herding is neither correct nor incorrect (it depends whether or not the herd is right) but Banerjee identifies some of the inefficiencies that emerge when we follow others.

This can be explained using Bayesian principles, as follows. Assume Restaurant A is favoured a priori by 51%; Restaurant B is favoured a priori by 49%; and 100 people are deciding about Restaurant A versus Restaurant B. If each of them then receives a private information signal: 99 of them have private information that B is a better restaurant; 1 person has misleading private information that A is better. Overall the aggregate evidence is in favour of Restaurant B. Whether it is preferred in practice will depend on the herd's choices. Assume that the first person to choose is the person with the misleading private signal; for example, a review written by a biased critic. The first person chooses A. Then the second person is deciding and they must balance three pieces of information: the prior probability favouring A; their correct private signal, favouring B; and the social information; that is, their predecessor's choice of A. Applying Bayes' rule, the decision-maker will balance the second and third pieces of information equally, so these conflicting signals will cancel each other out. Restaurant A is chosen in spite of a lot of private information indicating that B is better. Once the second person has gone down the wrong route, if the rest of the herd is also Bayes-rational, then a long queue will build-up for restaurant A. From the

second person onwards, all private information is discounted, even though it is useful for generating a negative herding externality. People are led into a choice which contradicts their private information during an information cascade, so anyone watching them will be unable to observe the private information that they are balancing with the social information (the actions of the herd). In the context of organizations' security policies, this is an important insight because similar negative herding externalities are likely to emerge if employees follow their colleagues in ignoring security breaches.

The information cascade hypothesis has been tested across a wide range of experimental studies, starting with Anderson and Holt's [1,2] urn experiments. Experimental participants were told that the experimenters were using two urns: Urn A — containing two red balls and one black ball; and Urn B containing one red ball and two black balls. Then participants were shown an unmarked urn, and were instructed to draw a ball from the urn but to conceal the ball they'd drawn from the other participants. Then they were asked to guess whether it was Urn A or Urn B and announce their guess to the group. The ball that they draw is their private information, which others do not have: all things being equal, if they draw a red ball, then they may rationally conclude that the urn is more likely to be Urn A, because A contains a higher proportion of red balls. The social information is the choices announced by the previous experimental participants. When making their guess about which urn the experimenters are using, a given participant will balance their private information (the colour of the ball they drew) and the social information (the public information from the guesses of their predecessors). If a person sees their predecessor picking Urn B, then they will update their probabilities, increasing their judgement of the likelihood that the urn is Urn B.

Anderson and Holt hypothesize that participants balance prior probabilities and conditional probabilities inferred from the sequence of predecessors' guesses to calculate posterior probabilities from the balance of private and social information, according to Bayes' rule. This is done in the following way: If $\Pr(A)$ and $\Pr(B)$ are the prior probabilities that the urn is either Urn A or Urn B, and the selection of the urn is determined by a coin toss, then $\Pr(A) = \Pr(B) = 0.5$. For the conditional probabilities, each player infers from predecessors' choices the colour of balls that they have chosen and includes this information with the private information they get from picking a red or black ball. If they see a predecessor selecting Urn A then they infer that their predecessor picked a red ball; then if the participant also picks a red ball, then they infer a succession of two red balls picked from the urn. If n is the number of urn A choices, and m is number of urn B choices, then from the sequence of social and private signals $(n, m)$ each participant will infer which urn is more likely using the conditional probabilities of signals $(n, m)$ if the urn is Urn A and Urn B, $\Pr(n, m|A)$ and $\Pr(n, m|B)$ respectively. The posterior probability that it is Urn A, is then calculated using Bayes' rule:

$$\Pr(A|n, m) = \frac{\Pr(n, m|A)\Pr(A)}{\Pr(n, m|A)\Pr(A) + \Pr(n, m|B)\Pr(B)} = \frac{2^n}{2^n + 2^m}$$

For example, if after three rounds, a player has signals that two red balls and one black ball have been drawn then $\Pr(n, m|A) = 2/3 \cdot 2/3 \cdot 1/3 = 4/27$, and $\Pr(n, m|B) = 1/3 \cdot 1/3 \cdot 2/3 = 2/27$. Applying Bayes' rule gives the posterior probability of Urn A: $\Pr(A|n = 1, m = 2) = 2/3 = 67\%$.

Anderson and Holt [1,2] use this urn experiment to test the Bayesian herding as social learning hypothesis and found that their experimental participants choices were broadly consistent with Bayesian social learning. They observed information cascades in 41 of 56 periods in which there was an imbalance between private signal and previous inferred signal.

### 3.1 Social Learning and Organizational Security Access Policies

These Bayesian social learning and information cascade models can be used to capture the processes operating in organizations when employees do or don't challenge potential impostors who are not wearing an ID/visitor's badge. In deciding whether or not to challenge potential impostors, employees will think about imitating their colleagues' actions. For example, if a new employee observes long-term employees ignoring potential impostors, then the new employee may rationally decide that this is because the long-term employees recognizes the person and knows that they are not an impostor, even though the potential impostor is not wearing a visitor/ID badge. On the other hand, a long-term employee may be more likely, all thing being equal, to challenge potential impostors because they know better the familiar faces; they may recognize most visitors who regularly come to the office, and so are more alert to the genuinely unfamiliar people, who are more likely to be imposters.

Overall, whether or not employees imitate their colleagues' decisions will be driven by a complex interaction between socio-psychological influences, including susceptibility to peer pressure. For simplicity, in these scenarios we assume that it is a less complex process of Bayesian social learning, as described above.

## 4 Example: Challenging

Security policies often require that employees and visitors wear ID badges when at work and state that employees should challenge people who are not wearing a badge. This example explores how the concept of herding can be used to understand the behaviour of employees making decisions about whether or not to challenge. The model for this example consists of three physical locations: a starting location, an office, and a destination location. This set-up can be seen in Figure 1. Impostors and legitimate personnel — visitors or employees from a different part of the building, for example — must move from the start location, through the office, and to the goal location. The office location is filled with a number of employees who, from time to time, briefly stop working and observe the room. If an employee is observing the room and sees someone pass through without an ID badge, the employee must make a decision about whether or not to challenge that person.

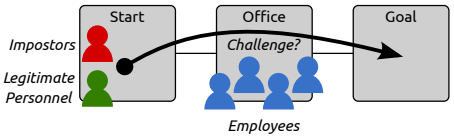


**Figure 1.** The Challenging model. Impostors and legitimate personnel, all without badges, must move from the start, through the office, to the goal. A number of employees observe them and must decide whether or not to challenge them.

If multiple employees are observing the room at the same time, the decisions about challenging happen in sequence and the employees are aware of the actions (to challenge or not) of earlier employees. This matches the structure of the herding model described in Section 3.

The social learning model specifies that agents have a private signal. Here, the private signal is recognition: whether or not the employee recognizes the person without an ID badge as legitimate or not.

This example is designed to demonstrate the integration of the social learning model with the systems modelling approach and so is intentionally simple. It could easily be incorporated into larger, more complex models.

### 4.1 Integrating Social Learning and Systems Models

We integrated the notion of Bayesian social learning as given in Section 3 into the systems modelling framework described in Section 2. In doing so, it was important to preserve the ability to compose models together. We began by introducing the notion of an event and an observation. A process creates a resource, which represents an event, and add it to a location. The presence of such a resource in a location indicates that an event is ongoing. When the event has finished, the creating process claims the resource and removes it from the location. Instantaneous events can be modelled by adding and removing the resource without advancing simulation time.

Other processes can watch for events. They attempt to claim an event resource at a location, waiting either indefinitely or until a specified amount of time has elapsed, or until they successfully claim an event resource. Since the events are resources and use the standard claim/release mechanisms in the framework, they can be used in similar ways; processes can wait until combinations of multiple events occurs, for example.

If multiple processes are waiting to observe the same event they form a queue. The first to claim receives the event first. This process then has two choices: it can ignore the event, and release it back to the location for the next process to claim, or it can handle the process, in which case it sets a flag so the event is not claimed by any subsequent observing processes. We created functions to start, end, ignore, and handle events that make it easy to use this functionality.

Since the events are built on top of the location, resource, and process primitives built into the framework they automatically maintain the compositionality

of the framework. A location where events are placed could be part of an interface that defines how models compose together, allowing processes to observe events created by other models.

The challenging model here was built using this new event concept. Employees watch, from time to time, for people without badges; the employee processes are observing for a short duration, waiting for an event indicating that a person without a badge is crossing the room. This event is generated by the impostor/legitimate person process, and stopped when they leave the room. The observing process then either handles the event, if challenging, or ignores it.

### 4.2 Parameters

Now, we need to define the parameters of the model. People without badges can be either impostors or legitimate personnel. $\Pr(I)$ is the prior probability that a person without a badge is an impostor; $\Pr(L) = 1 - \Pr(I)$ is the prior probability that the person is legitimate. Upon observing a person without a badge, an employee receives a private signal about whether or not the person is an impostor. Signal $X$ corresponds to a belief that the person is an impostor; signal $Y$ corresponds to a belief that the person is legitimate.

If the person is actually an impostor (although this remains unknown to the employee), the employee receives signal $X$ with probability $p$ and signal $Y$ with probability $1 - p$. If the person is actually legitimate, the probabilities are reversed, and the employee receives signal $X$ with probability $1 - p$ and signal $Y$ with probability $p$.

A value $p = 0.5$ represents total uncertainty; the private signal is essentially a coin toss and conveys no information about whether or not the person is an impostor. Higher values of $p$ represent increased certainty, with signal $X$ being more likely when the person is actually an impostor. In a small organization, with few employees who are likely to all know one another, the value of $p$ would be higher: they would probably recognize that a person is not a colleague. In a larger organization, with a greater number of employees, and perhaps a large number of visitors, employees might not be able to so easily discern who is legitimate, so the value of $p$ would be closer to 0.5.

In addition to these probability parameters, there are also four parameters that determine the payoff for each action: $V_{\mathrm{C,I}}, V_{\mathrm{I,I}}, V_{\mathrm{C,L}}$, and $V_{\mathrm{I,L}}$ for the reward for challenging an impostor, ignoring an impostor, challenging a legitimate person, and ignoring a legitimate person, respectively. The expected payoff for challenging is $\Pr(I)V_{\mathrm{C,I}} + (1 - \Pr(I))V_{\mathrm{C,L}}$; the expected payoff for ignoring is $\Pr(I)V_{\mathrm{I,I}} + (1 - \Pr(I))V_{\mathrm{I,L}}$.

### 4.3 Scenarios

We will look at five different scenarios, each with different parameter configurations which are displayed in Table 1. The scenarios were chosen to reflect different possible types of organizations, of different sizes and with different attitudes towards security. The aim is to explore how different parameters affect

the behaviour of employees. Each scenario was run 10,000 times and the results are shown in Table 2.

| Parameter | Scenario | | | | |
|---|---|---|---|---|---|
| | 1A | 1B | 2A | 2B | 3 |
| $\Pr(I)$ | .05 | .05 | .005 | .005 | .05 |
| $p$ | .55 | .95 | .75 | .75 | .55 |
| $V_{\mathrm{C,I}}$ | 10 | 10 | 20 | 50 | 10 |
| $V_{\mathrm{I,I}}$ | -10 | -10 | -20 | -50 | -10 |
| $V_{\mathrm{C,L}}$ | -1 | -1 | -1 | -1 | -1.5 |
| $V_{\mathrm{I,L}}$ | 0 | 0 | 0 | 0 | 0 |

**Table 1.** Scenario parameters.

| Value | Scenario | | | | |
|---|---|---|---|---|---|
| | 1A | 1B | 2A | 2B | 3 |
| Pct impostors challenged | 73.3 | 94.9 | 0.0 | 72.1 | 0.0 |
| Pct legitimate challenged | 63.8 | 8.6 | 0.0 | 24.0 | 0.0 |
| Pct imp. chal. by first obs. | 71.8 | 95.9 | — | 100.0 | — |

**Table 2.** Results for the scenarios, showing the percentages of impostors and legitimate personnel challenged, as well as the percentage of challenged impostors that were challenged by the first observer.

**1A.** In this first scenario, the parameter $p = 0.55$, meaning that the private signal received by each observing employee is imprecise. This case would be likely in a large organization where employees do not recognize each other on sight and would have difficulty discerning whether or not a person is legitimate or an impostor.

Employees who observe a person without a badge make their decisions sequentially. The sequence terminates when either the person is challenged, or all observing employees have chosen to ignore the person. Figure 2 shows the cumulative distributions (over the lengths of the sequences) of the proportion of impostors challenged and ignored, and the proportion of legitimate employees challenged and ignored. Of the impostors that are challenged, 71.8% are challenged by the first observer, with the remaining 29.2% challenged by the second. In the case of those challenged by the second observer, the first observer must have had a private signal indicating that the impostor was legitimate; the second observer receives the opposite signal and concludes, a posteriori, that challenging is the best action.

No impostors are challenged by later observers. If the first two observers both receive signals indicating that a person is legitimate, then an information cascade begins. The signal indicating that a person is an impostor received by any later observers is overwhelmed by the actions of the previous observers. This cascade can only happen in one direction; after a person is challenged, later observers do not need to take any action. For cases where the person without a badge was ignored, the number of observers ranges from 0 to 12. The number of observers depends on the state of the model at the time when the person arrives at the office: how many employees are currently observing. Overall in this scenario, the 73.3% of impostors are challenged, along with 63.8% of legitimate personnel.

**1B.** In this scenario, the precision of the private signals for employees is increased to $p = 0.95$, meaning that employees can determine whether a person

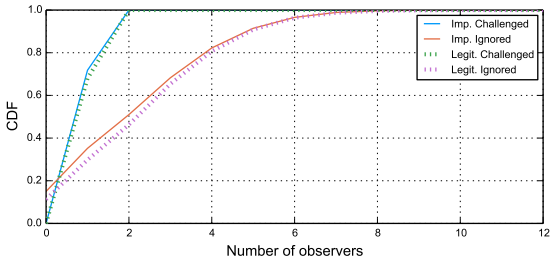


**Figure 2.** Scenario 1A. Cumulative proportion of impostors or legitimate personnel challenged or ignored after a number of observers.

without a badge is an impostor or not much more reliably. This would occur in small organizations where most employees know each other well. Here, 94.9% of

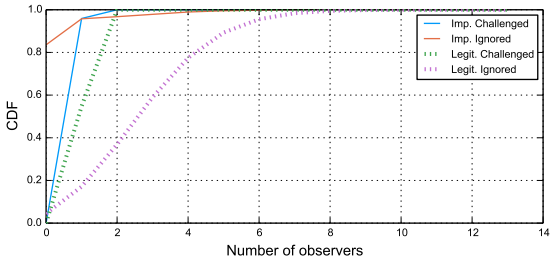


**Figure 3.** Scenario 1B. Cumulative proportion of impostors or legitimate personnel challenged or ignored after a number of observers.

impostors are challenged; of those, 95.9% are challenged by the first observer. Information cascades can still occur, but the chance of both the first two observers receiving an incorrect signal — recognizing an impostor as someone legitimate — is low. Only 8.6% of legitimate personnel without badges are challenged.

**2A.** The next two scenarios look at a situation where the prior probability of an impostor is lower; we use a value $\Pr(I) = .005$. This value could arise, for example, in a company where security controls to the building are extremely tight—it would be very unlikely for any impostor or attacker to make it into the office. In this scenario, the utility reward for challenging an impostor is $V_{\mathrm{C,I}} = 20$ and the utility for ignoring an impostor is $V_{\mathrm{I,I}} = -20$.

These parameter values lead to behaviour where employees never challenge anyone; the prior probability of a person without a badge being an impostor is low enough that the expected utility gained by the agent from challenging, even

with a signal indicating the person is an impostor, is less than the expected utility from ignoring. Although the values are symmetric for challenging or ignoring an impostor, challenging a legitimate person has a small negative effect on utility ($V_{\mathrm{C,L}} = -1$) which, given the high prior probability that the person is legitimate, has a large effect on the expected utility.

**2B.** This scenario is identical to 2A except that the utilities for challenging and ignoring an impostor are increased: $V_{\mathrm{C,I}} = 50$ and $V_{\mathrm{I,I}} = -50$. With these higher values, employees once gain challenge people they suspect to be impostors. However, the information cascade starts immediately after the first employee has chosen to ignore. With the added information from the first employee, the expected utility of challenging is lower than ignoring. This indicates that companies where employees have a very low belief that there will be an impostor must make extra effort to stress the importance of challenging. That is, the incentives for employees to do so must be high; otherwise, employees will choose to people without ID badges, even if they do not recognize them.

**3.** The final scenario uses the same values a the first two scenarios, except the utility penalty for challenging a legitimate person is increased: $V_{\mathrm{C,L}} = -1.5$. With this increased penalty, employees stop challenging.

The negative utility received from challenging a legitimate person could be attributed to the effort or time required to actually stop and question the person, or it could be a social cost incurred from the confrontation. As can be seen in this scenario, these costs can be a barrier to challenging. Companies that wish to have their employees challenge in such a manner must promote a culture of challenging. That is, they must make the social cost of challenging low, by making it encouraged and accepted by employees, and perhaps by providing training to staff on the correct way in which to do it.

## 5 Conclusions

Security systems modelling provides a way in which the effects of decisions about securing complex systems, with interactions between technology, policy, the environment, and human behaviour, can be explored, with the aim to improve decision-making.

An essential part of that is capturing the way human agents within the system behave and make decisions. We have presented here a model of social learning from behavioural economics and integrated it with a mathematically rigorous systems modelling framework, maintaining the important property of compositionality. We then used it to model and simulate the behaviour of employees making decisions about challenging under a variety of different parameter choices, reflecting different possible types of organizations.

The model itself is relatively simple, but could easily form part of a larger model of a more complex system. In any case, it represents an important step towards improved modelling of human behaviour in a systems models context.

## References


1. L. Anderson and C. Holt. Classroom Games: Information Cascades. Journal of Economic Perspectives, 10(4), 187-93, 1996.
2. L. Anderson and C. Holt. Information Cascades in the Laboratory. American Economic Review, 87(5), 847-862, 1997.
3. G. Anderson and D. Pym. A Calculus and Logic of Bunched Resources and Processes. *Theoretical Computer Science* 614:63-96, 2016.
4. Asch, S. E. Studies of independence and conformity: A minority of one against a unanimous majority. Psychological Monographs 70 Whole no. 416, 1956.
5. Baddeley, M. Herding, Social Influence and Economic Decision-Making: Socio-Psychological and Neuroscientific Analyses. *Phil. Trans. Roy. Soc. B* 365(1538), 281-290, 2010.
6. Baddeley, M. *Behavioural Economics and Finance.* Abingdon: Routledge, 2013.
7. A. V. Banerjee. A Simple Model of Herb Behavior. Quarterly Journal of Economics, 107(3), 797-817, 1992.
8. Bikhchandani, S. and Hirshleifer, D. and Welch, I. A theory of fads, fashions, custom and cultural change as informational cascades. Journal of Political Economy, 100(5), 992-1026, 1992.
9. Bikhchandani, S. and Hirshleifer, D. and Welch, I. Learning from the Behavior of Others: Conformity, Fads, and Informational Cascades. Journal of Economic Perspectives, 12(3), 151-170, 1998.
10. Bond, R. and Smith, P. Culture and conformity: A meta-analysis of studies using Aschs (1952b, 1956) line judgment task. Psychological Bulletin, 119, 111-137, 1996.
11. T. Caulfield, D. Pym, and J. Williams. Compositional Security Modelling: Structure, Economics, and Behaviour. *LNCS*, 8533:233–245, 2014.
12. T. Caulfield and D. Pym. Modelling and Simulating Systems Security Policy. In *Proc. 8th. SIMUTools.* ACM Dig. Lib., 2015. doi:10.4108/eai.24-8-2015.2260765
13. T. Caulfield and D. Pym. Improving Security Policy Decisions with Models. *IEEE Security and Privacy*, 13(5), 34-41, September/October 2015.
14. M. Collinson and D. Pym. Algebra and logic for resource-based systems modelling. *Mathematical Structures in Computer Science*, 19(5):959–1027, 2009.
15. M. Collinson, B. Monahan, and D. Pym. *A Discipline of Mathematical Systems Modelling.* College Publications, 2012.
16. George Coulouris, Jean Dollimore, and Tim Kindberg. *Distributed Systems: Concepts and Design.* Addison Wesley; 3rd edition, 2000.
17. D. Galmiche, D. Méry, and D. Pym. The Semantics of BI and Resource Tableaux. *Mathematical Structures in Computer Science* (2005) 15, 1033–1088.
18. The julia language. 2015. `http://julialang.org/` (visited 30/09/2015).
19. R.L. Keeney and H. Raiffa. *Decisions with Multiple Objectives: Preferences and Value Trade-offs.* Wiley, 1976.
20. R. Milner. Calculi for synchrony and asynchrony. *Theoretical Computer Science*, 25(3):267–310, 1983.
21. R. Milner. *Communication and Concurrency.* Prentice Hall, New York, 1989.
22. P.W. O'Hearn and D.J. Pym. The logic of bunched implications. *Bulletin of Symbolic Logic*, 5(2):215–244, June 1999.
23. G. D. Plotkin. A structural approach to operational semantics. Technical Report DAIMI FN-19, Computer Science Department, Aarhus University, Denmark, 1981.