ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/257890444

Towards a Simulation of Information Security Behaviour in Organisations

Article · July 2012

DOI: 10.1007/978-3-319-04447-7_14

CITATIONS
4

READS
171

3 authors:

Martin Ruskov
University of Milan
18 PUBLICATIONS **54** CITATIONS
SEE PROFILE

Paul Ekblom
University of London
79 PUBLICATIONS **1,304** CITATIONS
SEE PROFILE

Angela Sasse
Ruhr-Universität Bochum
379 PUBLICATIONS **13,648** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Attributes affecting user decision to adopt a Virtual Private Network (VPN) app View project

Multimedia conferencing View project

All content following this page was uploaded by Paul Ekblom on 04 December 2018.

The user has requested enhancement of the downloaded file.

Towards a Simulation of Information Security Behaviour in Organisations

Martin Ruskov, M. Angela Sasse
Information Security Resarch Group
University College London
London, UK
m.ruskov(a.sasse)@cs.ucl.ac.uk

Paul Ekblom
Design Against Crime Research Centre
Central Saint Martins
London, UK
p.ekblom@csm.arts.ac.uk

***Abstract*—In this paper we propose the fundaments of a design of an exploratory simulation of security management in a corporate environment. The model brings together theory and research findings on causes of information security risks in order to analyse diverse roles interacting through scripts. The framework is an adaptation of theoretical and empirical research in general crime prevention for the purposes of cybercrime. Its aim is to provide insights into the prerequisites for a more functional model.**

Keywords—information security; conjunction of criminal opportunity; crime scripts; simulation

I. INTRODUCTION

Research in the recent decade, e.g. [1], [2] demonstrates the importance of addressing the human factor in information security: attackers often obtain information, access to systems or money by tricking customers or employees. This calls for security models that capture the complexity of the wider socio-technical system. Examples of such models are the Mechanics of Trust [3] and the Compliance Budget [4]. Of interest is the unification of these models in the search for a more general theory of how we can design systems that prevent this sort of attack.

In 2004 in a report for the UK Government Foresight Programme, Collins and Mansell [5] suggest the adoption of a framework from conventional crime science - the Conjunction of Criminal Opportunity (CCO) framework [6] - as a basis for developing and designing resilient systems and effective cyber defences. The CCO framework presents a systematic and conceptually rigorous categorization of immediate contributing causes to criminal events (with the potential to trace back to distal causes). Compared with prior frameworks it captures a much wider range of causes for attacks. The CCO framework unifies traditional offender-oriented with situational crime prevention and is explained further in this paper along with its potential application in cybercrime. It has already been suggested [6] that CCO can combine well with the Crime Scripts approach [7] in which the various agents interact with one another and exploit or harm the technical settings, often combining factors from the physical environment and cyberspace.

This makes CCO generally applicable, yet simple enough to serve as a framework in which other theories of causation of criminal events could be unified in an exploratory simulation. Such a reusable framework that incorporates domain knowledge could be seen to be very similar to the formal patterns used in software engineering and architecture [8]. A potential resulting simulation can deliver a learning experience exploring an actual research framework. Moreover, challenges encountered during simulation design provide feedback that tests the consistency of the theoretical research, as has been done with simulations in conventional crime science by Birks, Townsley and Stewart [9].

Quantitative simulation models already exist. For example, the Naval Postgraduate School developed a game to spread awareness about cyber security called CyberCIEGE [10]. It is a customizable platform that allows designers to develop scenarios for their organisations. A typical scenario in CyberCIEGE is about preventing users from letting malware into the corporate intranet, preventing social engineering and safeguarding data. Unlike CyberCIEGE however, the simulation model proposed here seeks theoretical (and eventually empirical) validity.

II. BACKGROUND

In his research on insider attacks Schultz [11] considers the CMO model consisting of *capability* to commit attack, *motive* to do so and *opportunity* to do it. In his work Schultz also reviews a model insider attackers by Tuglular and Spafford [12] allegedly featuring factors describing such as *personal characteristics*, *motivation*, *knowledge*, *abilities*, *rights and obligations*, *authority and responsibility* within the organisation, and factors related to *group support*. Parker [13] develops the SCRAM model. The abbreviation reflects the factors considered: *skills*, *knowledge*, *resources*, *authority* and *motives*.

The CCO framework considers eleven overarching classes of complementary causes which come together to make a criminal opportunity. The number of these classes may seem high, but that is to model all potential contributory causes of crime in the real world. To model the contributory causes of cyber crime, the classes of causes can be considered to fit in three wider groups - personal, technical and social factors. These all are represented in the figure.

The personal (attacker) factors are:

- **Criminality** and wider personal traits influencing attacker's tolerance towards immoral or criminal deeds. This is where *personal characteristics* [12] are being addressed.
- **Anticipation of risk, effort and reward** - the rational decision and utility behind the attack
- Abundance of **resources to commit crime** - both cognitive resources and capabilities, and social factors such as trust, but also technical hacking tools - the attacker needs to be both aware of their existence and be able to operate them. Schultz's [11] *capability* and *opportunity* can be viewed as

part of the cognitive resources of inside attackers. Parker's [13] *resources* fall naturally into this category, but also his *skills*, *knowledge* and to some extent *authority*.

- Immediate **readiness to undertake an attack**, e.g. the commonly modelled motives to do it like disgruntlement [11], [13].
- **Lack of skills to avoid crime** - potential skills that would reduce attacker's need to commit crime. For insiders this could be ability to manage stress, soft skills to improve common understanding of potentially discouraging issues, etc.
- **Attacker presence in situation** - circumstances like the fact that this person is part of the organisation, but also that they have certain access privileges that might allow them to abuse the organization.

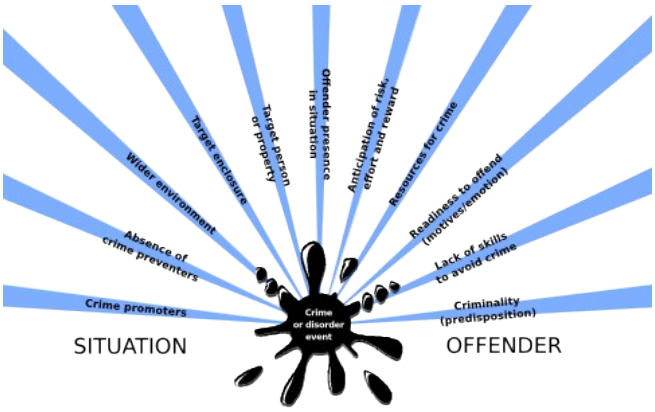

Figure 1: The diagram visualizing the eleven generic causes in the Conjunction of Criminal Opportunity framework

Situational factors contributing to the criminal opportunity capture the predisposition of the environment to allow for criminal behaviour. In the context of cybercrime as such can be seen aspects like scamming and social engineering [2]. These could be both social and technical and are represented by the following:

- **Presence of crime promoters** - people (or roles, or organisations) that deliberately or unintentionally make the crime more likely, such as potential buyer of stolen data, hacker technology providers or someone who carelessly does not log out from the system after having used it.
- **Absence of crime preventers** - people that intentionally or not would discourage or deter attackers, be they security officers, technology providers or management and staff ready to help disgruntled colleagues resolve their grudges.
- The **target** of the attack, in the digital context commonly information or finances, but indirectly could also be the person or organisation which might suffer from a leak.
- The **enclosure around the target**, having both the digital aspect of firewalls and authentication systems and physical access.
- The **wider environment** which could contribute towards attacks and discourage or restrict potential preventers. *Authority* can be thought of as a feature of the organisational environment that allows misuse, e.g. lifting doubt from people with authority that demand information which they don't possess.

The issue of *authority* as considered by previous models comes to illustrate the interactions of these different factors. On one hand *authority* is a *resource* that a potential offender possesses and enables them to commit the attack. On the other one's *authority* also is a function of the *wider environment* - it is the organisational culture that allows authority to be exercised without protective questioning from others.

III. Crime Scripts

One technique used in conventional crime prevention is that of crime scripts [7]. These are sequences of events characteristic of recurring, or similar, attacks. Typically a script would also capture the preparatory and consummatory sequences of actions that attackers engage in before and after the actual attack, thus providing a wider picture and context to how attacks commonly happen.

Research in design against crime has revealed that not only are the scripts of attackers insightful tools, but also the scripts typical of ordinary users who may or may not be acting in the role of crime preventers [6]. Being a normal business routine, this category of non-criminal scripts can possibly be extracted from the established business processes in an organisation. These processes could either be designed or ad-hoc; with the former it could be that the actual routine is different from the one designed, e.g. in cases when users find it difficult to comply with designed procedures [4].

Sample of scripts of attackers and regular users are illustrated below:

Users' generic script:

1. User is asked to create an account.
2. User generates a password, according to own cognitive scheme.
3. User stores password (either mentally or physically)
4. If stored physically password needs to be secured.
5. User devises restoration procedures, e.g. reminder question or location to where file is stored.
6. Generation of procedure to restore passwords.
7. Using password (or subset of its letters) for authentication.
8. Make sure password is not retrievable after end of use.

Script instance illustrating misuse:

1. Change password (due to a system request to change regularly).
2. Store new password on a piece of paper, convenient for frequent referencing.
3. Because it is already stored externally and thus easier to reuse, use new password for several systems in company.
4. Skip anti-virus checks so that they do not slow down work.

5. Reschedule anti-virus checks for non-working hours.
6. Log out when done working for the day.

Hostile insider script:

1. Decide to cause harm to company and identify target and what to do with it (e.g. upload internal financial data onto internet).
2. Choose mode of access and tactics to reach target (e.g. plan on time when target company's office will be unlocked and empty).
3. Acquire target's externally stored password (e.g. on piece of paper).
4. Access target system, retrieve asset and copy it (e.g. physically access office computer of Accounts department, deploy trojan).
5. Distribute valuable asset to market analysis.

External attacker script:

1. Try target technical system for potential backdoors or exploits.
2. Research social networks of potential human targets that have access to system.
3. Infect a computer of trusted peer of user.
4. Have trusted computer send trojan to user.
5. Infect computer with access to secured network.
6. Copy data out of the secured network.

IV. Script Clashes

Scripts on their own depict the procedural nature of everyday and criminal situations. However, they represent the routine of an individual and not the dynamics resulting from the inevitable interaction of these routines upon an encounter between their corresponding performers. For example, if a potential attack is being suspected, security officers could decide to reduce the number of people that have access to valuable data. This would be a counter-move trying to prevent data theft. It is natural that when seeing the new obstacle the attacker would decide to change their tactics of access. As a result devising a counter-counter-move which could be trying to get access through a unsuspecting colleague, trusted enough to still have the wished access.

Such a process of interruption and branching from routine scripts demonstrates the complexity of dynamic modelling of crime, and cybercrime in particular. Over time, the scripts and counter-scripts become steadily more elaborate. But there may be only a limited number of archetypical script clashes to address (such as 'conceal move versus detect move') [6].

V. Conclusions and Future Work

In the process towards a simulation of cyber crime this position paper contributes in two ways. First, it proposes an adaptation of the CCO framework to information security. And second, it suggests modelling of script clashes and discussion of potential reactive adaptations of scripts. These two patterns of representation both contribute to the fundaments of a design for a simulation of information security behaviour in a potential crime situation.

Designing and implementing a simulation of information security behaviour is a challenging task. A computer simulation typically requires a finite (and thus mathematically closed) representation. On the other hand there is an arms race between attackers and security officers which requires continuous adaptation and innovation [14] - a potentially infinite space of ideas or steps. A way out of this contradiction could be to address only the recurring attacks, but not the innovative ones. This way the hope is to get coverage of the "20% of scripts occurring 80% of the time".

The domain of simulation can be built utilizing the currently developed CCO browser game prototype [15]. This prototype features neither any simulation elements, nor crime scripts yet. Instead it guides users through a facilitated process of brainstorming crime interventions. Still, the game prototype could be used to analyse attacker scripts thus collecting user generated counter-moves. Data will be collected with the game prototype until certain level of saturation of ideas is achieved. The collected data could then be used to describe (hopefully enumerate) the space of counter-moves within certain abstraction and simplification.

References

[1] A. Adams and M. A. Sasse, "Users are not the enemy: Why users compromise security mechanisms and how to take remedial measures," *Commun. ACM*, vol. 42, no. 12, pp. 40–46, Dec. 1999.

[2] F. Stajano and P. Wilson, "Understanding scam victims: seven principles for systems security," *Commun. ACM*, vol. 54, no. 3, pp. 70-75, 2011.

[3] J. Riegelsberger, M. A. Sasse, and J. McCarthy, "The mechanics of trust: A framework for research and design," *International Journal of Human-Computer Studies*, vol. 62, no. 3, pp. 381-422, Mar. 2005.

[4] A. Beautement, M. A. Sasse, and M. Wonham, "The compliance budget: managing security behaviour in organisations," 2008, pp. 47-58.

[5] B. S. Collins and R. Mansell, "Cyber trust and crime prevention: a synthesis of the state-of-the-art science reviews," London, UK, 2004.

[6] P. Ekblom, "Happy returns: ideas brought back from situational crime prevention's exploration of design against crime," in *The Reasoning Criminologist: Essays in Honour of Ronald V. Clarke*, G. Farrell and N. Tilley, Eds. Routledge, 2011, p. 163+.

[7] D. Cornish, "Crimes as scripts," in *Proceedings of the International Seminar on Environmental Criminology and Crime Analysis*, D. Zahm and P. Cromwell, Eds. Tallahassee: Florida Criminal Justice Executive Institute, 1994, pp. 30-45.

[8] C. Alexander, S. Ishikawa, and M. Silverstein, *A Pattern Language: Towns, Buildings, Construction*, Later prin. Oxford University Press, 1977.

[9] D. Birks, M. Townsley, and A. Stewart, "Generative Explanations of Crime: Using Simulation to Test Criminological Theory," *Criminology*, vol. 50, no. 1, pp. 221-254, 2012.

[10] B. Cone, C. E. Irvine, M. F. Thompson, and T. Nguyen, "A video game for cyber security training and awareness," *Computers & Security*, vol. 26, no. 1, pp. 63-72, Feb. 2007.

[11] E. E. Schultz, "A framework for understanding and predicting insider attacks," *Computers & Security*, vol. 21, no. 6, pp. 526-531, Oct. 2002.

[12] T. Tuglular and E. H. Spafford, "A framework for characterisation of insider computer misuse." 1997.

[13] D. B. Parker, *Fighting Computer Crime: A New Framework for Protecting Information*. Wiley, 1998.

[14] P. Ekblom, "Gearing Up Against Crime: A Dynamic Framework to Help Designers Keep Up With the Adaptive Criminal in a Changing World," *International Journal of Risk, Security and Crime Prevention*, vol. 2, no. 4, pp. 249-265, Oct. 1997.

[15] M. Ruskov, J. M. Celdran, P. Ekblom, and M. A. Sasse, "Unlocking the Next Level of Crime Prevention: Development of a Game Prototype to Teach the Conjunction of Criminal Opportunity." 2012.

View publication stats