Security goes to ground: on the applicability of Security Entrepreneurship to Grassroot Activism

Shamal Faily
Computing Laboratory,University of Oxford
Wolfson Building,Parks Road,Oxford UK OX1 3QD
shamal.faily@comlab.ox.ac.uk

ABSTRACT

Designing security for grassroot movements raises several challenges not particular to the organisations that conventional approaches to security design cater for. Drawing on analogies between Social Entrepreneurship and Grassroot Activism, adopting an entrepreneurial approach to security design may lead to security design decisions which are both in-tune with a grassroot movement's aims and cost effective. This position paper considers the applicability of Security Entrepreneurship for security design in grassroot movements. Using a SWOT analysis, we discuss the strengths and weaknesses or this approach, before considering external threats and opportunities arising its prolonged adoption.

Author Keywords

Social Entrepreneurship, Security Entrepreneurship, User-Centered Design

ACM Classification Keywords

K.6.0 General: Economics

SECURING THE GRASSROOTS

Grassroot Activism raises two unique challenges for the design of security to protect its interests.

First, security design approaches are geared towards large, well-funded organisations. In contrast to grassroot movements, such organisations have the time and resources to pay for dedicated security staff, and the supporting infrastructure needed to ensure their interests remain protected as the organisation grows, and the environment around it changes.

Second, from their initial inception, some movements will be construed as a threat. While security proponents argue that security should be designed into any system from its inception, it may be unrealistic to expect all nascent grassroot movements to simultaneously think about their causes and possible threats to their existence. Unfortunately, without developing an appreciation of the threat landscape surrounding a movement, security decisions may be over or under-commensurate to the risks it faces.

Many of the security problems faced by conventional organisations arise because security is considered to be a product that can be simply purchased and bolted-on to an organisational infrastructure. Moreover, when security chafes the ability of staff to be innovative, attempts will be made to circumvent security. The knee-jerk reaction of security administrators in such instances is to treat users as miscreants. The negative impact this can have on morale and productivity in commercial organisations is damaging, but not fatal. At a grassroot level, however, such behaviour could de-motivate volunteer activists from contributing to a movement altogether.

As Bruce Schneier states, security is a "process rather than a product" [10], and configuring this process for any organisation involves more than simply installing software on a PC or a network server. However, there are no obvious solutions for what such a process might look like for small, grassroot movements. Moreover, what might be a reasonable security strategy for one movement might be completely inappropriate for the problems faced by another.

FROM ACTIVISM TO SECURITY ENTREPRENEURSHIP

Previous work [11, 5] has linked Grassroot Activism with *Social Entrepreneurship*, although, as Stryjan [11] notes, these analogies may not be immediately obvious. A succinct definition for what Social Entrepreneurship is eludes us; Nicholls suggests that this might be the basis of its success, in that Social Entrepreneurs will exploit a variety of different tools and techniques to maximise the creation of social value [8]. In a talk given at Oxford last year, serial entrepreneur Jerry Sanders stated that entrepreneurs were successful because they "sell the dream". However, fostering innovation is also a system integration problem, and many elements in a social system need to be configured and re-configured if ideas are to have impact, and social capital is to be created.

Recent work has examined how the principles of Social Entrepreneurship can be used to design innovative security solutions. This has led to the new paradigm of *Security Entrepreneurship*: the application of innovation models and principles to organise, create, and manage security design elements to bring about improved system security [3]. This work is motivated by the observation that situating security attuned to the physical and social contexts it needs to operate

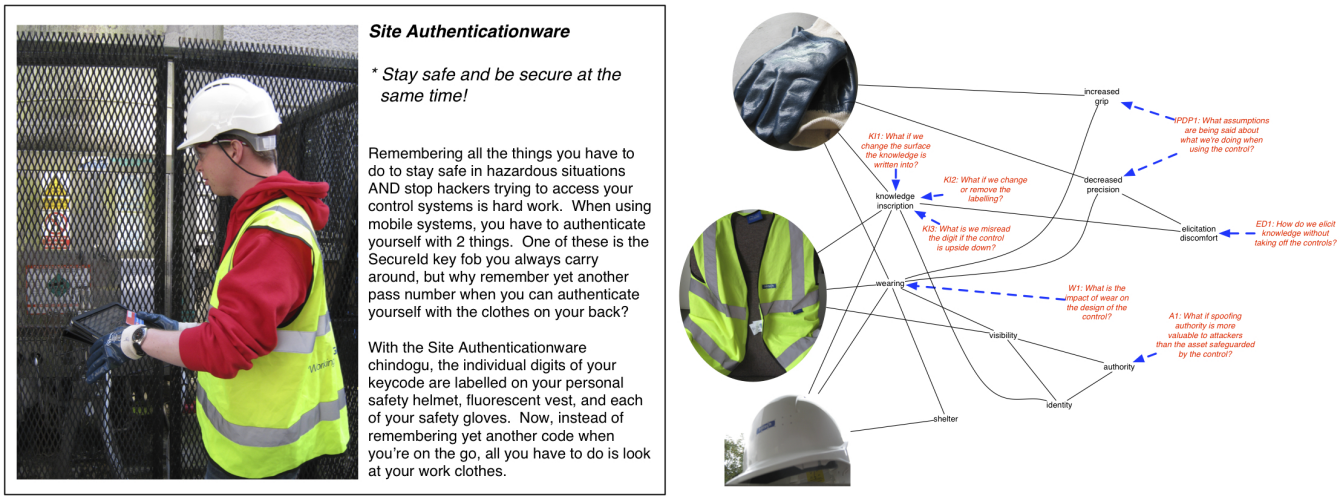

Figure 1. Site Authenticationware Chindōgu

in is akin to solving a *wicked problem* [9]; this is because of the lack of clarity about what it means to secure a system, or even test that a system is secure. We have specifically drawn three analogies between Security and Social Entrepreneurship:

- Both approaches deal with problems with a social context.
- The value propositions nurtured by both approaches are designed to empower under-served or neglected communities.
- The success of both innovations is marked when traditional organisations attempt to enter the hitherto ignored market.

SWOT ANALYSIS

To examine the applicability of Security Entrepreneurship to security design for Grassroot Activism, we have carried out a SWOT (Strength, Weaknesses, Opportunities, and Threats) analysis of this position. We first consider the strengths and weaknesses associated with adopting this approach, before discussing possible external opportunities and threats associated with its prolonged adoption.

Strengths

Security Entrepreneurship is built on Technology and Social Entrepreneurship principles, many of which underpin the growth philosophy of grassroot movements. Many successful innovation models can be repurposed, leading to innovative security which can be both situated to the needs of the movement and are cost-effective. In [3], we demonstrated how existing work on Social Network Theory can be used to re-configure the social network in an organisation to optimise the flow of information in a particular security activity. We also showed how Value-added Chains could be used to model how disruptive security controls might be to different stakeholders on a project.

We have also found that Security Entrepreneurship can inform security design using techniques from the HCI vernacular. In a recent case study, we discovered design criteria for security controls in water-treatment plants based on observational data, and artifacts commonly found in the environment where the controls would need to be situated in. These artifacts were used to fashion a *Chindōgu*: an ingenious gadget which may seem like an ideal solution to a problem, but introduces so many new problems that it effectively has no utility [6]. Figure 1 (left) illustrates the *Site Authenticationware* Chindōgu we developed as a "solution" to the problem of unusable two-factor authentication. Using the literary device of Defamiliarisation [2], we uncovered the affordances of the Chindōgu using an ontology chart (Figure 1 (right)) and discovered vulnerabilities which might arise when building controls for this environment. These insights led to innovative usability design criteria for security controls that would make them usable by plant operators and technicians. Our rationale for developing a control as a Chindōgu rather than a more useful prototype is that building an artifact which looks useful but is deliberately designed to be useless is unorthodox to most engineers, and demands creative thinking. Breaking from conventional orthodoxy is useful for viewing the artifact from an unfamiliar standpoint.

Weaknesses

While Security Entrepreneurship can complement participatory design approaches, it is more contingent on the role of the entrepreneur than participatory approaches are on the role of the facilitator. Similarly, while traditional design leads might be focused on conceptual integrity, the entrepreneur is *opportunity-centered*. Specifically, the Security Entrepreneur is looking for opportunities for system insecurity, before exploring solutions for dealing with them, and re-configuring the system to remove the insecurity. Indeed, [3] suggests that what distinguishes the entrepreneur from other design roles is that, rather than working within the confines of a particular scope, an entrepreneur is prepared to re-configure the world around him to ensure the environment shapes a de-

sign, rather than vice-versa. Although this mind-set is emancipatory and makes the design of security a pro-active rather than re-active process, it is also unorthodox and, therefore, a possible cause of contention during the design process.

A further weakness relates to the Security Entrepreneur's role as an agent of change. [3] suggests that the disruptive innovation these entrepreneurs generate may lead to an *innovation design dilemma*, where the diversity caused by applying innovation techniques leads to conflict that hampers the implementation of the innovation [4]. For this reason, we need to consider how suitable different grassroot organisations might be as a context for this kind of intervention.

Opportunities

From a research perspective, Security Entrepreneurship at a grassroot level may lead to important insights into how security can be better designed. Because grassroot organisations have fewer resources than most organisations for designing security, it is precisely the eco-system that can stimulate inventive ideas for solving common security problems. By applying Security Entrepreneurship techniques, we can better understand what sort of environmental changes are needed to make sure these ideas have impact.

For security research, disseminating innovation arising from Security Entrepreneurship interventions would be analogous to social innovation in the developing work leading to new insights into Social Entrepreneurship theory. For example, Leadbeater's theory of Structured Self-Organisation [7] was inspired by successful city-wide waste recycling and city planning social enterprises in Curitiba, Brazil. These enterprises relied on values such as collaborative engagement and a pragmatic working philosophy. These values are not incompatible with grassroot movements, nor are they incompatible with the design of security.

Threats

Without applying Security Entrepreneurship in practice, we can only speculate what threats might arise to grassroot movements by adopting this approach. One particular threat, however, arises from the notion of the Security Entrepreneur as a potential inside-attacker. In particular, what happens if a Security Entrepreneur decides to leave a movement and join another organisation with non-complementary aims?

From a security perspective, this could lead to disaster as the entrepreneur's privileged knowledge, coupled with his innate ability to shape the environment, could lead to new innovations which might harm the movement. Moreover, a Security Entrepreneur may deliberately use innovation models and techniques to scare other members of a movement into making sub-optimal security decisions that benefit him in the future. Conversely, however, treating the entrepreneur as an outsider and gatekeeping his activities breeds an atmosphere of distrust, and stifles the spirit of innovation.

Because there is no easy solution for mitigating this threat, how Security Entrepreneurship might be used should be carefully considered before it is applied. For this reason, [3] proposes that Security Entrepreneurship should be evaluated within the context of Action Research interventions [1]. This ensures that a mutually accessible framework can be agreed between the movement benefiting from the intervention, and the researcher fulfilling the role of a Security Entrepreneur. Moreover, the intervention also provides useful results about other threats the movement might be exposed to by this approach.

CONCLUSION

Grassroot movements face a number of unique security problems that conventional approaches to organisational security are unable to deal with. Drawing on the analogies between Grassroot Activism and Social Entrepreneurship, this paper has proposed Security Entrepreneurship as a security design paradigm for such groups. To explore its applicability at a grassroot level, we have examined Security Entrepreneurship's strengths and weaknesses, and discussed consequential opportunities and threats arising from prolonged use of this approach.

ACKNOWLEGEMENTS

The research described in this paper was funded by EPSRC CASE Studentship R07437/CN001. We are very grateful to Qinetiq Ltd for their sponsorship of this work.

REFERENCES

1. R. L. Baskerville. Investigating information systems with action research. *Commun. AIS*, page 4, 1999.

2. G. Bell, M. Blythe, and P. Sengers. Making by making strange: Defamiliarization and the design of domestic technologies. *ACM Trans. Comput.-Hum. Interact.*, 12(2):149–173, 2005.

3. S. Faily and I. Fléchais. To boldly go where invention isn't secure: applying Security Entrepreneurship to secure systems design. In *Proceedings of the 2010 workshop on New security paradigms*, NSPW '10, pages 73–84, New York, NY, USA, 2010. ACM.

4. J. Hobek. The innovation design dilemma: some notes on its relevance and solution. In K. Grønhaug and G. Kaufmann, editors, *Innovation: a cross-disciplinary perspective*. Norwegian University Press, 1988.

5. M. Horwitch and B. Mulloth. The interlinking of entrepreneurs, grassroots movements, public policy and hubs of innovation: The rise of cleantech in new york city. *Journal of High Technology Management Research*, 21(1):23–30, 2010.

6. K. Kawakami. *The Big Bento Box of Unuseless Japanese Inventions (101 Unuseless Japanese Inventions and 99 More Unuseless Japanese Inventions)*. W. W. Norton & Company, 2005.

7. C. Leadbeater. The Socially Entrepreneurial City. In *Social Entrepreneurship: New Models of Sustainable Social Change*, pages 233–246. Oxford University Press, 2006.

8. A. Nicholls. *Social Entrepreneurship: New Models of Sustainable Social Change*. Oxford University Press, 2006.

9. H. W. J. Rittel and M. M. Webber. Dilemmas in a general theory of planning. *Policy Sciences*, 4(2):155–169, 1973.

10. B. Schneier. *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003.

11. Y. Stryjan. The practice of social entrepreneurship: Theory and the swedish experience. *Journal of Rural Cooperation*, 34(2):197–229, 2006.