Analysing chindōgu: applying defamiliarisation to security design.

FAILY, S.

2012

Analysing Chindōgu: Applying Defamiliarisation to Security Design

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

CHI 2012, May 5–10, 2012, Austin, TX, USA.
ACM xxx-x-xxxx-xxxx-x/xx/xx.

Abstract

Envisaging how secure systems might be attacked is difficult without adequate attacker models or relying on sterotypes. Defamiliarisation removes this need for a priori domain knowledge and encourages designers to think critically about system properties otherwise considered innocuous. However, questions remain about how such an approach might fit into the larger design process. This paper illustrates how security requirements were elicited by building a security chindōgu, and using defamiliarisation to help analyse it. We summarise this technique before briefly describing its use in a real-world setting.

Keywords

Security, Defamiliarisation

ACM Classification Keywords

H.5.2 [**User Interfaces**]: User-centered design.

General Terms

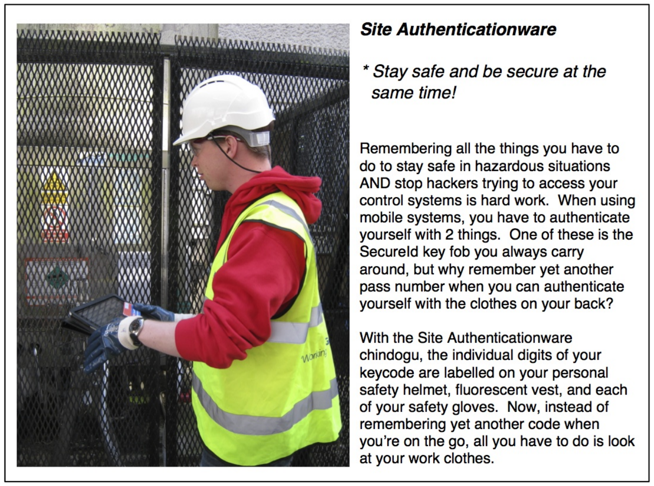
Human Factors

Introduction

One of the biggest problems affecting the design of secure systems is envisaging ways it might be attacked. While a security engineer may have a sound understanding of security controls and the broader threat landscape, a designer's abstraction of a system does not always match the abstraction used by an attacker to exploit it. While user-centered design techniques for building attacker models [1] provide one solution to this problem, many practitioners instead resort to stereotyping potential attackers to glean possible threats. Unfortunately, this approach leads to a myriad of problems ranging from unbalanced security due to assumptions about *super-hackers*, through to disempowering end-users by treating them all as potential inside attackers.

Defamiliarisation offers a fresh alternative to these two options; rather than eliciting or inventing domain knowledge, defamiliarisation involves divorcing oneself from the norms and values associated with the domain, and questioning features that might otherwise have seemed innocuous. As a creativity technique, defamiliarisation stimulates new ideas about the nature of a design problem and its possible solutions. However, to be an effective innovation technique, defamiliarisation needs to fit into the larger design process to ensure these new ideas have impact.

Security chindōgu



Site Authenticationware

** Stay safe and be secure at the same time!*

Remembering all the things you have to do to stay safe in hazardous situations AND stop hackers trying to access your control systems is hard work. When using mobile systems, you have to authenticate yourself with 2 things. One of these is the SecureId key fob you always carry around, but why remember yet another pass number when you can authenticate yourself with the clothes on your back?

With the Site Authenticationware chindogu, the individual digits of your keycode are labelled on your personal safety helmet, fluorescent vest, and each of your safety gloves. Now, instead of remembering yet another code when you're on the go, all you have to do is look at your work clothes.

Figure 1: Site Authenticationware chindōgu

We have used defamiliarisation to support innovative security design by analysing *security chindōgu*. Chindōgu are gadgets invented to address a particular problem which, while initially appearing to be an ideal solution, ultimately introduces so many new problems that it effectively has no utility [5]. The security chindōgu technique was first introduced in [2], and motivated by the belief that requiring engineers to build purposefully useless artifacts might stimulate creative thinking. To integrate the use of this technique into a larger design activity, we devised a process for analysing chindōgu. This involves using defamiliarisation to inspect the artifact and eliciting an initial set of its affordances. After reflecting on the intentional and unintentional possibilities associated with these affordances, we model both the initial affordances and their ontological dependencies using the semiotically-informed ontology charting technique [6]. Where applicable, we annotate the affordances to describe ambiguities that may lead to unintentional use of the artifact. Based on these annotations, we specify requirements to discharge each identified ambiguity.

Security chindōgu in practice

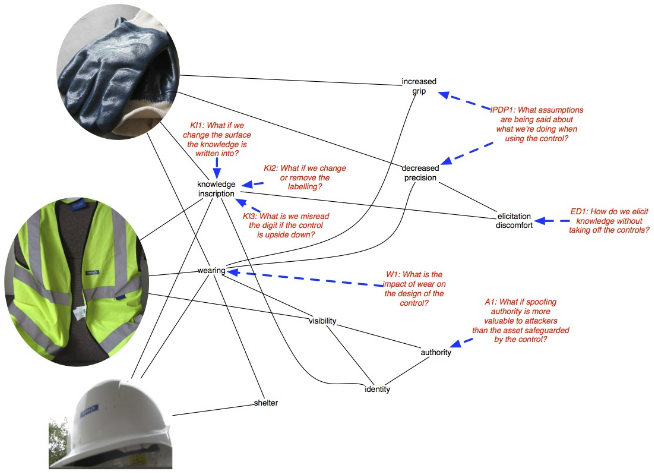

increased grip
IPDP1: What assumptions are being said about what we're doing when using the control?
KI1: What if we change the surface the knowledge is written into?
KI2: What if we change or remove the labelling?
knowledge inscription
decreased precision
KI3: What is we misread the digit if the control is upside down?
elicitation discomfort
ED1: How do we elicit knowledge without taking off the controls?
wearing
W1: What is the impact of wear on the design of the control?
A1: What if spoofing authority is more valuable to attackers than the asset safeguarded by the control?
visibility
authority
identity
shelter

Figure 2: Ontology chart of chindōgu affordances

We used the security chindōgu technique to help develop a revised information security policy for water treatment plant staff at a UK water company. The policy updates we identified were motivated by personas and scenarios we created; these were grounded in qualitative and contextual interview data from plant operators at different clean and waste water works; more information about the study can be found in [3, 4]. The stimulus for building this chindōgu arose from two observations made while carrying out fieldwork. The first was a physical security vulnerability associated with the wearing of safety clothing. We observed that wearing safety clothing appeared to afford unfettered access to much of a particular treatment works; this was irrespective of whether any form of personal identification was visible. However, *not* wearing this clothing lead to non-wearers being challenged and their movements restricted for safety reasons. The second observation arose from reported difficulties highlighted by one plant operator obtaining out-of-hours technical support for a control room workstation. Because he had forgotten his system login credentials, and had no other form of identification that call-centre support staff would recognise, he was unable unlock this workstation to remotely operate some critical hardware. To explore the externalities associated with satisfying the requirement for multiple factors of authentication, we examined some of the paraphernalia associated associated with both plant operations and information security. This inspired the *Site Authenticationware* chindōgu in Figure 1.

Defamiliarisation of the chindōgu took place in an office setting, and the affordances of the chindōgu were perceived in a number of ways; these included wearing the objects and carrying out simple office-based tasks like typing an email, feeling the textures associated with surfaces of each item, and generally playing with the chindōgu in the same way that a young child might. As each affordance was perceived, an ontology chart was drawn up of both the initial and subsequent affordances which appeared to ontologically follow; Figure 2 shows a transcription of this diagram, together with annotations made as the diagram was developed. When no more affordances seemed obvious, security requirements were elicited to mitigate each of the concerns highlighted. For example, the identification of the *knowledge inscription* affordance raised the question of what might happen if the surface that the security secret was written on was damaged or otherwise weakened. To deal with this, a requirement was specified to state that the medium for inscribing secrets on a device used for authentication shall not be modifiable within the device's warranted contexts of use.

Lessons learned

When the revised security policy was presented to senior stakeholders at the UK water company, the reaction to the chindōgu and its resulting analysis was mixed. The stakeholders appeared to be captivated by the chindōgu, and, as such, little attention was paid to the resulting analysis and requirements. This reaction indicates that, like other user-centered design artifacts, careful thought needs to be given to how chindōgu are presented to ensure the purpose of the artifact is not overshadowed by the artifact itself. From a security perspective, building and analysing the chindōgu served two useful purposes. First, it unintentionally raised awareness of an implicit vulnerability that had been hitherto overlooked. Second, the elicitation of several new policy requirements via the defamiliarisation exercise demonstrated that such requirements could be elicited without using a priori security expertise; this challenges general convention indicating that *security experts* are needed for security design. We are currently exploring how this technique, and defamiliarisation in general, can be used to guide security design decisions for the EU FP7 webinos project.

Acknowledgements

The research described in this paper was funded by the EU FP7 webinos project (FP7-ICT-2009-05 Objective 1.2).

Bio

Shamal Faily is a post-doctoral researcher at the University of Oxford; his research explores how design techniques and tools can better facilitate the design of interactive secure systems. Shamal is also interested in understanding how entrepreneurship and innovation theories can be used to better inform security design decisions. Shamal is currently working on the EU FP7 webinos project, where he is exploring how the security and privacy expectations of prospective users, developers, and attackers can inform the architectural design of a software platform for distributed web applications.

References

[1] A. Atzeni, C. Cameroni, S. Faily, J. Lyle, and I. Fléchais. Here's Johnny: a Methodology for Developing Attacker Personas. In *Proceedings of the 6th International Conference on Availability, Reliability and Security*, pages 722–727, 2011.

[2] 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 New Security Paradigms Workshop*, pages 73–84. ACM, 2010.

[3] S. Faily and I. Fléchais. Persona cases: a technique for grounding personas. In *Proceedings of the 29th international conference on Human factors in computing systems*, pages 2267–2270. ACM, 2011.

[4] S. Faily and I. Fléchais. User-centered information security policy development in a post-stuxnet world. In *Proceedings of the 6th International Conference on Availability, Reliability and Security*, pages 716–721, 2011.

[5] 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.

[6] K. Liu. *Semiotics in information systems engineering*. Cambridge University Press, Cambridge, 2000.