SECURITY ENHANCEMENT WITH FOREGROUND TRUST,COMFORT, AND TEN COMMANDMENTS FOR REAL PEOPLE

STEPHEN MARSH, ANIRBAN BASU, AND NATASHA DWYER

Abstract. Security as an enabling paradigm has not succeeded half as well as we might have hoped. Systems are broken or breakable, and users (people) have something of a lack of faith, understanding, or patience with security measures that exist. Whilst secure systems and solutions are the backbone of a working interconnected system of systems, they are not people-oriented, and they are oftentimes arcane enough to have an air of 'security theatre' about them. We can also assume that they will continue to grow in both complexity and application if we continue as we are in our arms race.

To answer what we perceive to be a problem here, we are working on the integration of socio-psychological notions of trust into computational systems where it makes sense (both human- and system-facing). This work includes the development of our Device Comfort paradigm and architecture, wherein mobile devices and nodes in infrastructures have a embedded notion of comfort that they can use to reason about their use, behaviour, and users. This notion, contextually integrated with the environment the device is in, aids in decision making with regard to, for instance, information flow, security posture, and user-oriented advice. Most importantly, the notion embeds trust reasoning and communication into the device, with which the user can be aided to understand situation, risk, and actions by device, infrastructure, and themselves - which we call Foreground Trust, after Dwyer. We conjecture that comfort and foreground trust both enhance security for devices and increase the understanding of security for the user, through use of human-comprehensible and anthropomorphic concepts. In this paper, we discuss some security problems, address the misnomer of trusted computing, and present an overview of comfort and foreground trust. Finally, we briely present our ten commandments for trust-reasoning models such as those contained within Device Comfort, in the hope that they are of some use in security also.

1. Introduction

We live in a complex world, one in which decisions about security of many kinds occupy an important place. For as long as there have been people, these decisions have been important. The difference between ten, a hundred, or a thousand years ago and now is the tools we use. Like any power tool, computers, either desktop, laptop, or in our pockets, help us to do things more quickly. They also help put us into difficult situations more quickly. Information power tools, which is what computers are, have potentially exposed their users' information - private, heretofore shared only with a chosen few, to the many. Protecting this information, as well as the tools themselves and the access they have to others' tools and information, is

Key words and phrases. Trust, Device Comfort, Foreground Trust, Human Computer Interaction.

the task of information security. Attacking the information, for pleasure or profit, is the 'task' of the 'adversary.'

We have reached an unfortunate stage in the evolution of information systems, however - we conjecture that, if a system is not compromised it most certainly can be, and that the attacks are coming faster and most importantly in unique ways - while we still have the worms and viruses of the past, we now have to contend with social engineering and targeted attacks. To do this, we pour more and more intellectual capital into defences against the adversaries. But to what end? Systems now not compromised can be, and many are, with or without our knowledge. Couple this with the increasing complexity of the defences themselves, which ultimately results in more frustration at the very least on the part of the users we are trying to defend, and we arrive at a challenging confusion: the system is broken. An arms race has been carrying on for many years, and the only loser is the person who wants to get her job done, or play.

Enhanced security mechanisms, better passwords, different kinds of passwords, more complex login procedures, more demands on users, or abrogation of responsibility are not the answers at least, they're not the answers that make for security with users in mind. We find a little solace in usable security, but ultimately we feel that we should look for a more human-centric approach to security. To achieve this, we approach the problem from the point of view of human social norms, in particular, ion our work, trust and comfort, and their darker siblings distrust an discomfort. In fact, these are topics we have been dealing with for some time in different areas, including agent systems and critical infrastructures. They lend themselves particularly well to human-oriented security because they are in essence human-oriented security - and they have worked for humans for millennia. The paradigm that most interests us in this instance is what Dwyer [4] calls Foreground Trust - in essence the ability of technological devices to present information to users in order to allow them to make security-focused (trust-focused) decisions. Our most recent work in this area has been concerned with integrating comfort and trust reasoning techniques into mobile devices, which we call Device Comfort.

This paper discusses the Device Comfort paradigm as a security tool for both information and personal security from a high level perspective (interested readers can find more information in other work [11]). As well, we will discuss a set of 'commandments' for trust and comfort facing the user, commandments that we feel can benefit any security technology where humans are a concern (and this is, of course, all of them). The next section introduces and briefly discusses Foreground Trust, before we proceed to a slightly more in depth discussion of Device Comfort as a form of Foreground Trust in section 3. Section 4 takes the form of a discourse on presenting information to the user, and is an extension of work we did in [9]. After a discussion and a brief look at ongoing work in Device Comfort in section 5 we conclude in section 6.

2. Foreground Trust and Related Work

Trust Enablement was presented in [4], where it was applied to the task of the system to connect people through technology by giving them the tools and information they need to make trusting decisions regarding other people. Extended to Foreground Trust, it was further expounded upon in [13]. The basic premise of Foreground Trust is this: if people have enough information to make trusting

decisions, they will do so. We acknowledge that there is, of course, rather a lot of trust placed in the person in this instance, which we will address with regard to information security in the next section. However, the premise is inherently sound - people 'get' trust, they understand it in a very deep sense, and it is a tool that has evolved over millennia to allow humans to make decisions or handle complexity in the face of risk [2, 6, 3, 7, 12].

Extending the concept of Foreground Trust to a human-technology relationship is a necessary next step in evolving a security solution that is human-oriented. In some settings this should be closely integrated with societal behaviours and norms. Work by Murayama et al on the Japanese concept of Anshin is closely related work in this area [5, 14]. In [1] we find behavioural history based reputations to inform security decisions in networks, and also the outlook that one entity's view of the network is its own when it comes to security; and that this 'personal' view (i.e. local reputation of other entities) is more important than the global view.

The benefits of this approach are manifest: humans, as has already been noted, understand trust, and they understand how trust decisions are made. Integrating these decisions into the interface between human and 'security' is, we conjecture, a sensible approach to allow the human to understand the security risks and resultant posture of the systems they are using to get their work done. Ultimately, the Device Comfort paradigm is an extension of trust reasoning into mobile devices that are inherently human-facing.

3. Device Comfort

Device Comfort extends trust reasoning technologies by allowing mobile devices to reason with and about computational trust [7] and to communicate these reasonings to the owner of the device in a human-oriented manner. The Device Comfort paradigm goes further in that it allows the device itself to make trust-based decisions, comfort-based decisions, and policy-based decisions independent of the user, and adjust its security posture accordingly. We have written extensively about Device Comfort elsewhere [8, 10, 11] and so only briefly discuss the notion here as it applies to a non-traditional security measure.

Device Comfort was initially envisaged as a tool to help teens using smartphones make more sensible decisions about what they are using the phones for (in particular, with regard to the phenomenon of Sexting). However, we quickly became aware that the paradigm had applicability in many different uses of mobile devices for many different users, and have altered our outlook accordingly.

The premise of Device Comfort is quite simple: to Advise, Encourage, and Warn (as for a constitutional monarch, in fact) and ultimately be able to proscribe actions for the users of the mobile device (call it AEWP). Indeed, we'd go as far as claiming that this is what all security methodologies and tools should be doing. It does this by using the strengths of the device as a sensing mechanism, as well as having inbuilt security policies. Device comfort is a dynamic phenomenon the more sense-capabilities a device has the more we can integrate into comfort. Currently we see Device Comfort as a measure based on reasoning about the following:

- The user's identity
- Enhanced trust reasoning about the user, and the ongoing relationship with respect to trust that the device has in the user (and/or owner);

- The current task (for instance, making a call, sending text, sending pictures, email, etc.)
- The current location (which virtually all mobile devices can determine with some accuracy)
- A Comfort Policy-base (provided by the owner of the device, as well as the owners of any information the device stores or can access, basically presented to the device, and thus the user, on access.)

A more formal exposition is given in [11]. We see Comfort as a dynamic, context-based reasoning mechanism. The internal architecture of the technology is based on sensing tools communicating with a comfort agent via tuple spaces, and the agent communicating with the user through a sensible interface. We have very carefully considered how the mechanism becomes human-oriented through the interface, both as what we call 'annoying technology' [11] and as an embodiment of the AEWP concept. We aim, through the interface to give the user second thoughts, encourage anticipatory regret if possible, and learn from what the device can tell them about the situations they find themselves in - and in this way, to learn about security for themselves and their information.

3.1. **The Human Security Posture.** Because Device Comfort was devised as a tool to allow potentially less-aware (or less concerned) users to make sensible risk-based decisions, it is unique in that it is human-oriented as well as seeking to allow humans to understand their context not only for information security, but also for personal security. It is possible to envisage situations where the device is 'uncomfortable' because of aspects of its physical context location, electronic neighbourhood (what devices are present), and so on, as well as its electronic context, including policies. In these instances, it is useful to present these aspects of context to the user as something that they should be concerned about and want to change, because they themselves may be at risk, and not just the device of the information on it (and so: "leave the area" is a valid comfort response, for instance, as is "don't send that message from here"). In essence, the tool has a use in the formation of 'second thoughts' for users in risky situations [13]. Whilst we have not as yet conducted experiments involving this aspect of Device Comfort, we hope to be able to address it in the near future.

4. The Ten Commandments of Foreground Trust for Security

In [9] we presented a discussion of the complexity of trust models that are, as all should be, human-focused. The arguments there are similar to those in this paper: too much complexity is not helpful, for instance. We did, at that time, have eight commandments for trust models. In this paper, we extend this to ten (there should always be ten, after all) with the addition of two commandments which were discussed as a result of that previous work. We also extend the commandments to take into account security models and techniques, in the hope that they can be more generally applied. We make no claim to uniqueness in these commandments - indeed we would be heartily surprised if they were not in some shape or form discussed elsewhere in the usable security world. But we do claim that they are useful to bear in mind in the trust world too, an they are most certainly applicable in any case. The commandments, and a brief discussion, follow.

(1) The model is for people.

(2) The model should be understandable, not just by mathematics professors, but by the people who are expected to use and make decisions with or from it.
(3) Allow for monitoring and intervention. Humans weigh trust and risk in ways that cannot be fully predicted. A human needs to be able to make the judgement, especially when the model is in doubt.
(4) The model should not fail silently, but should prompt for and expect input on failure or uncertainty.
(5) The model should allow for a deep level of configuration. Trust and security models should not assume what is 'best' for the user. Only the user can make that call.
(6) The model should allow for querying: a user may want to know more about a system or a context.
(7) The model should cater for different time priorities. In some cases, a trust/security decision does need to be made quickly. But in other cases, a speedy response is not necessary
(8) The model should allow for incompleteness. Many models aim to provide a definitive answer. Human life is rarely like that. A more appropriate approach is to keep the case open; allowing for new developments, users to change their minds, and for situations to be re-visited.
(9) Trust (and security) is an ongoing relationship that changes over time. Do not assume that the context in which the user is situated today will be identical tomorrow.
(10) It is important to acknowledge risk up front (which is what all trust, including Foreground Trust, does).

5. Discussion and Ongoing Work

The commandments translate into design principles guiding the creation of a Comfort Device that negotiates trust, security and control on behalf of and in conjunction with the user. Knowledge about how the user would want to operate such a device is necessary. We are working on a series of research questions to inform our design perspective. For instance, we argue that there are some trust decisions that the user is more interested in than others. But how do we distinguish between these interactions? Catering for interactions will differ depending on users needs and interests. Other questions include how users differ amongst themselves between what is the priority in an interaction.

The intricacies of an interface are also relevant for a successful project. What graphic style is suitable? With what sort of language does the user want to be informed of risk in the beginning of an interaction? Formal? Colloquial? Although these questions might seem to be those that need to be addressed at the later stage of delivery or even trivial, in actuality such considerations shape how users approach issues of security and trust. Are users welcomed to consider these complicated notions on their own terms or alienated?

It should be clear that, in all cases systems such as those outlined here have a need for a solid foundation. Security, in the sense of a secure system (as secure as we may be able to make it, and at as low a level as possible), is necessary, but not sufficient to bring about the needed interactions and relationships that the system must have with the user, and vice versa. Ultimately, trust and comfort

serve to make security more flexible. The major difference between traditional security and trust/comfort is the way in which risk is handled: security, including trusted computing, aims to minimize or eliminate risk if possible, resulting in a so-called 'trusted' system. Ironically, given that trust is founded upon risk, this process would if possible reach the situation where trust was in fact not needed. Trust and comfort acknowledge, accept, and manage risk in context. We feel that this is a more flexible approach because it accepts the potential for all systems to be compromised and to try to work to the best ability anyway, whilst not failing silent (see the commandments). While we are in a position of needing security at some level, we feel that we can enhance security both by this acceptance and by the raising of awareness the trust relationship can effect with the user.

As well as the questions above, we are working on integration of trust and comfort reasoning into more complex settings including critical infrastructure interdependencies and management, and human-oriented processes.

6. Conclusions

Trust and Comfort are flexible, awareness-enhancing approaches to risk in context. They encourage flexible adaptations to risk that are human oriented and seek to enhance understanding of security in the people using them. Our work in this area has been exploring formal models for comfort based on our extant trust models, the integration of comfort into mobile devices, the design of comfort enabled user interfaces, and the extension of comfort in different infrastructures and contexts.

Of necessity, space for this paper is short. There is, however, much to say and much to be done on the topics of Foreground Trust, Enablement, and Comfort for security, and we hope that this short paper has shed enough light on the topic and its considerations to interest the reader.

References

[1] A. Basu. A Reputation Framework for Behavioural History. PhD thesis, University of Sussex, UK, January 2010.

[2] S. Bok. Lying: Moral Choice in Public and Private Life. Pantheon Books, New York, 1978.

[3] M. Dibben. Exploring Interpersonal Trust in the Entrepreneurial Venture. London: MacMillan, 2000.

[4] N. Dwyer. Traces of Digital Trust: An Interactive Design Perspective. PhD thesis, School of Communication and three Arts, Faculty of Arts, Education and Human Development, Victoria University, 2011.

[5] N. Hikage, Y. Murayama, and C. Hauser. Exploratory survey on an evaluation model for a sense of security. In H. Venter, M. Eloff, L. Labuschagne, J. Eloff, and R. von Solms, editors, IFIP Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments, volume 232, pages 121-132, Springer, 2007.

[6] N. Luhmann. Trust and Power. Wiley, Chichester, 1979.

[7] S. Marsh. Formalising Trust as a Computational Concept. PhD thesis, University of Stirling, 1994. Available via www.stephenmarsh.ca.

[8] S. Marsh. Comfort zones: Location dependent trust and regret management for mobile devices. In In Proceedings TruLoco 2010: at IFIPTM 2010, Morioka Japan., 2010.

[9] S. Marsh, A. Basu, and N. Dwyer. Rendering unto Caesar the things that are Caesar's: Complex trust models and human understanding. In T. Dimitrakos, R. Moona, D. Patel, and D. H. McKnight, editors, Proceedings Trust Management VI: IFIPTM Conference on Trust Management, pages 191-200. Springer (IFIP AICT), 2012.

[10] S. Marsh and P. Briggs. Defining and investigating device comfort. In Proceedings of IFIPTM 2010: Short Papers, 2010.

[11] S. Marsh, P. Briggs, K. El-Khatib, B. Esfandiari, and J. A. Stewart. Defining and investigating device comfort. Journal of Information Processing, 19:231-252, 2011.
[12] S. Marsh and M. R. Dibben. Trust, untrust, distrust and mistrust: an exploration of the dark(er) side. In Peter Herrmann, Valerie Issarny, and Simon Shiu, editors, Trust Management: Proceedings of iTrust 2005. Springer Verlag, Lecture Notes in Computer Science, LNCS 3477, 2005.
[13] S. Marsh, S. Noël, T. Storer, Y. Wang, P. Briggs, L. Robart, J. Stewart, B. Esfandiari, K. El-Khatib, M. Vefa Bicakci, M. Cuong Dao, M. Cohen, and D. Da Silva. Non-standards for trust: Foreground trust and second thoughts for mobile security. In Proceedings STM 2011. Springer, 2012.
[14] Y. Murayama and Y. Fujihara. Issues on Anshin and its factors. In Zheng Yan, editor, Trust Modeling and Management in Digital Environments: From Social Concept to System Development, pages 441-452. IGI Global, 2010.

Acknowledgement 1. *The authors wish to thank the many researchers and colleagues who have helped on the Device Comfort project, including Tim Storer, Babak Esfandiari, Mehmet Vefa Bicacki, John Stewart, Sylvie Noël and Lewis Robart.*

(S. MARSH)
University of Ontario Institute of Technology,
Faculty of Business and Information Technology
2000 Simcoe Street North, Oshawa ON. Canada
E-mail address, S. Marsh: stephen.marsh@uoit.ca
URL: http://www.stephenmarsh.ca/

(A. BASU)
Tokai University,
2-3-23 Takanawa, Minato-ku,
108-8619, Japan
E-mail address, A. BASU: abasu@cs.dm.u-tokai.ac.jp, a.basu@sussex.ac.uk

(N. DWYER)
Victoria University,
Footscray Park Campus, Ballarat Road,
Footscray, 3011, Australia,
E-mail address, N. DWYERM: natasha.dwyer@vu.edu.au