

# Security as a Practical Problem: Some Preliminary Observations of Everyday Mental Models

Paul Dourish, Jessica Delgado de la Flor, and Melissa Joseph

School of Information and Computer Science

University of California, Irvine

Irvine, CA 92697-3425

jpd@uci.edu

## ABSTRACT

Although security is normally thought of as a technical problem, we believe that it is more appropriately formulated as a practical problem that users routinely encounter and solve. Essentially, their problem is to determine the match between a system's configuration and their needs. However, the resources to make informed decisions are rarely available. As a first step towards solving this problem, we present some preliminary findings from a study currently under way, which seeks to investigate the mental models and conceptual arrangements by which people understand the problems of everyday security.

## INTRODUCTION

Security is normally imagined as a technical problem. When challenged to improve the state of information security or privacy in electronically mediated settings, security researchers and specialists offer technical solutions that are provably, robustly, mathematically secure. However, everyday experience suggests that effective security – the actually level of security achievable in practice – falls somewhat short of this mathematical ideal. Some (e.g. Whitten and Tygar, 1999) have suggested that the reason for this breakdown is that security applications are insufficiently usable. However, although the question of usability is certainly important, our work has taken a different tack. In particular, we conceptualize security differently. Rather than believing that security rests in technology, we believe that security rests in practice, and in the detail of what people do. Security is an achievement of people interacting with technology. It is not all-or-nothing, but a matter of degree. Faced with a variety of technologies, infrastructures, applications and tasks, people must continually determine whether the configuration of technologies available to them offers enough security for the task at hand. I may want quite different levels of security when I am sending an email message to my boss, submitting a grade report, or filing a tax return; and what I am prepared to settle for may depend on the urgency of the situation as well as the nature of the task and the options available to me. The question, then, is what helps people achieve security. We believe that one problem with current technologies is that they provide people with inadequate resources to make informed decisions about their current behaviour and about security-related practices.

Our current approach is based on the dynamic visualization of aspects of software system behaviour that relate to network activity, file activity, and security configuration. Aspects of this system have been described elsewhere (Dourish and Redmiles, 2002). In this workshop paper, we briefly discuss some preliminary observations from an interview study designed to probe people's mental models of security.

Mental models<sup>1</sup> of security are critically important for our approach. Since we believe that security is something that people must continually and ongoingly attend to in the course of their interactions with technology, a critical element is clearly how they see and interpret security happening in the software systems that they already use. This can provide us with three things. First, it provides an understanding of the level of description that might be appropriate for the kinds of information we would like to provide. Second, it lends some insight into current problems that can motivate and support our design efforts. Third, it helps to motivate the problem as a serious one that requires some effort to address.

## INITIAL OBSERVATIONS

Our approach has been to conduct ethnographic-style semi-structured interviews of end users of Internet technologies. Our data collection is currently under way. We have conducted a small number of preliminary interviews and are currently expanding this corpus with some more detailed interviews. Although the full set should be complete by the time of the workshop, this paper is based purely on the first few interviews. These were conducted with administrative and staff members of two university units (one teaching department and one research unit.) None of our subjects had formal training in computers or computer science.

### Security as a Barrier

One feature of our interview data that immediately stood out was the set of issues that arose under the auspices of security. Our questions were oriented around problems of security and information protection. However, we found that respondents would persistently turn to other issues

---

<sup>1</sup> It should be noted that we mean this term fairly loosely. Our goal is to uncover the structure of the domain and the terms and concepts that users bring to bear when considering security issues.

that, to them, are intimately related to information security. Of these, perhaps the most prevalent is unsolicited email. For our subjects, security and spam are two aspects of the same problem. What is more, they think of the same technologies as providing solutions; firewalls are described both as technologies to keep out unwelcome visitors but also unwelcome email messages. Similarly, viruses are part of the same problem. People seem to both imagine and seek unitary solutions to these problems. When we think of the real-world experiences on which people base their experiences, they think of security as a barrier (a gate or a locked door); security is, generically, something to keep things out, and so the various threats – the things that are being kept out – become co-constructed as the entities against which security protects. A security solution that solves one problem but not others is seen as being an inadequate protection.

### **Online and Offline**

The relationship between online and offline experience is a complex one, but is also centrally important. Online conduct seems to be continually shaped by aspects of the offline world. This happens in two ways. One is that a range of experiences in the online world provide metaphors and analogies by which people understand the online world. The brand identity of large organizations, for example, is a significant factor in how people treat online entities; institutional arrangements are perhaps even more important. (Banks, for instance, are seen as inherently more concerned about security, and therefore inherently more trustworthy.) The second relationship, one of greater import to our subjects, was the potential leakage of information between online and offline settings. While our initial expectation was that people would relate Internet security problems to internet-based fraud (e.g. forging email, identity theft, unauthorized financial transactions), a much more immediate concern for a significant number of our subjects was the possibility that inadvertent information disclosure online could create a threat offline. Most frequently, these were problems of personal security. Stalkers were an especially common reported threat, and much of people's attention to online information disclosure concerned information which might result in direct personal threat. We were struck by the regularity with which this issue arose.

### **Hackers, Stalkers, Spammers and Marketers**

Similarly, a range of different situations are classed as threats, almost coextensively. We found four broad classes of threats that people brought up in discussion. "Hackers" are individual threats who fit the expected image – people out to cause mischief and harm, generally highly skilled, but motivated by the same randomly violent impulse which leads to vandalism (rather than conducting targeted attacks). Hackers are also, perhaps, the least commonly identified threat. "Stalkers" are those who, as described above, might use information gleaned online to pursue an offline threat. "Spammers" are organizations and individuals that advertise through unsolicited messaging, wasting people's time and using up organizational resources through an implicit denial of service. "Marketers"

are people who invade individual privacy by surreptitiously collecting information about activities, purchasing patterns, and so forth. We found it interesting that the marketers are defined as threats in pretty much the same way as hackers, stalkers and spammers. People reported maintaining false identities, falsifying information, refusing to disclose identifiers, and other strategies by which they explicitly attempted to evade such tracking. To an extent, it seemed that older people (who had generally first been exposed to computers and network technologies as part of working or college experiences) seemed more likely to trust organizations and regard renegade individuals as threats; younger people (who had generally first been exposed to computers and perhaps even networks as children) were more likely to see organizations as potential threats. (Simultaneously, these younger subjects also seemed less likely to consider hackers as threats, perhaps because they expressed more confidence in their own abilities to manage their information and security online. It is possible that this greater degree of "savvy" allowed them to perceive a set of threats that others did not.)

### **Security as a Problem**

A further interesting separation between our older and younger participants relates to this issue of experience. In general, our younger subjects, with their longer exposure to computer systems (and in particular, it seems, childhood exposure) express a much greater confidence in their abilities with computer systems. In particular, they seem to have been more likely to encounter situations in which security services proved problematic, hindering rather than helping their activities. Getting files through firewalls, for instance, had been problematic for some, who found that they had to turn off or circumvent security technologies in order to get their work done.

### **Pragmatism**

In broad terms, and in line with the previous observation, the younger respondents seemed more pragmatic about their security needs, expressing more nuance about the situations in which they might need security. For instance, they discussed using known insecure technologies in settings where they felt that the risks were justified (e.g. a machine that was known to be chock full of viruses, but was otherwise unused so it didn't matter.) This pragmatic orientation in younger subjects is in line with previous findings (Sheehan, 2002). It is something that we are exploring in more detail in our later phases (and may be able to say more about at the workshop.)

### **Futility**

However, even amongst those who expressed more confidence about their abilities and a more pragmatic orientation towards security, there is an overwhelming sense of futility in people's encounters with technology. They make repeated reference to the unknown others (hackers, stalkers, etc.) who will always be one step ahead, and whose skill with technologies will mean that there are always new attacks to be diverted. As a result, they talk repeatedly of security lying not so much in technology as

in vigilance; the continual, active defense against new and evolving threats.

### Delegating Security

Of course, most people, in the course of their daily work, don't have the time to be continually vigilant for new threats. One particularly interesting issue, then, is the various modalities by which people delegate responsibility for security. Security is, to some extent, turned into someone else's problem, or at least, a set of external resources are marshaled. Four forms of delegation are identifiable in our interviews. The first is to *delegate to technology*, which involves relying on some form of technology for protection. Interestingly, this was perhaps one of the least common ways of managing security that we encountered. It is also interesting to observe that this delegation is an investment of trust, and we speculate that it depends on visible presence of technology to be trusted, which questions the idea of security as an invisible or transparent facet of a system. The second mode of delegation is to *delegate to another individual*, such as a knowledgeable colleague, family member, or roommate. Often, this might be someone who set the computer up in the first place; their knowledge and skill is cited as one element of a person's defense against potential threats. The third mode is to *delegate to an organization*; like delegation to an individual, this delegates to others, but the others are organizationally defined and may not even be known personally. The skills and especially the vigilance of the organization is where people place their trust. This is one element that cropped up repeatedly, although as we extend our subject pool beyond the administrative and staff members of university units, we may find other attitudes. Finally, we also found a mode in which people would *delegate to institutions*. So, our earlier examples in which financial institutions are seen as inherently more trustworthy because they are presumed to have a primary concern with security is an example of this trust in institutional arrangements and archetypes. Again, this is an online/offline relationship; impressions of the banks' concern with physical security (locked vaults and armed security guards) are carried over to online security, even though of course online interactions with a bank depend on a complex of intermediate technologies outside of any bank's control.

### CONCLUSIONS

These observations are very preliminary; full analysis of the data has yet to be undertaken, and indeed we are only half-way through our data collection at this stage. However, the

immediately striking commonalities between different people's perceptions and considerations surrounding information and computer security are both enlightening and suggestive. In particular, we take them as being supportive of our initial intuition that the visibility of security mechanisms is critically important for their effectiveness. The problem of security, as a routine problem that people encounter and solve continually, is an assessment problem; it involves determining whether the current technical (and organization, and social, and institutional) configuration of resources is supportive of the user's immediate needs, and whether and how the current tasks should be carried out so as to meet a set of (ill-formulated and perhaps inexpressible) security requirements. We believe that the key to usable secure information systems is to be able to provide people with the resources for making these decisions more reliably and with more information than they do just now. Investigating people's conceptions of security is a critical step in this direction.

We are not the first to have carried out this style of investigation; a series of studies by Sasse and her colleagues, for instance, have looked at related issues (e.g. Rimmer et al., 1999; Weirich and Sasse, 2001). However, we believe that our study makes valuable contributions to the emerging corpus of work, and in particular, begins to point towards some of the more socially-situated considerations in the development of secure systems.

### REFERENCES

1. Dourish, P. and Redmiles, D. (2002). An Approach to Usable Security Based on Event Monitoring and Visualization. Proc. ACM New Security Paradigms Workshop NSWP 2001.
2. Rimmer, J., Wakeman, I., Sheeran, L., and Sasse, M.A. (1999). Examining Users' Repertoire of Internet Applications. Proc. IFIP Conference Interact'99.
3. Sheehan, K. B. (2002). Towards a Typology of Internet Users and Online Privacy Concerns. The Information Society, 18, 21-32.
4. Weirich, D. and Sasse, M.A. (2001). Pretty Good Persuasion: A First Step Towards Effective Password Security in the Real World. Proc. ACM New Security Paradigms Workshop NSWP 2001.
5. Whitten, A. and Tyger, J.D. (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. Proceedings of the 9th USENIX Security Symposium.