"I'm Listening" :
Risk assessment culture with encrypted e-mail

Shirley Gaw
Dept of Computer Science
Princeton University
35 Olden Street
Princeton, New Jersey 08540
sgaw@cs.princeton.edu

Patricia Fernandez-Kelly
Dept of Sociology
Princeton University
Wallace Hall
Princeton, New Jersey 08540
mpfk@princeton.edu

Edward Felten
Dept of Computer Science
Princeton University
35 Olden Street
Princeton, New Jersey 08540
felten@cs.princeton.edu

ABSTRACT

Why has encrypted e-mail failed to gain popularity? In this study, we interviewed people that might be persuaded to use it, nine employees of an organization involved with acts of civil disobedience. While most e-mail users might not view themselves as potential targets, these employees believed the organization was a likely target of eavesdropping by adversaries. Adoption of encrypted e-mail was related but not directly tied to the the inconvenience it would cause. Employees thought such a policy was reasonable for internal messages, but it was more complex for external communications. If the relationship with the outsider was tenuous, such as the relationship with volunteers, enforcing a strong computer security policy was unreasonable. Another issue was how people were motivated to use of encryption. Although computer support staff favored using encrypted e-mail all of the time, most people saw encryption as necessary for protecting secret and only secrets. In all other circumstances, people saw using encryption as being paranoid.

1. INTRODUCTION

Suppose Alice wants to send Bob a secret message but Zeke wants to read this message. Alice shares a secret with Bob. This secret helps Alice make her messages unreadable to anyone but Bob. Zeke is foiled from listening to the communication channel.

This is the textbook example of how encryption is supposed to work. Unfortunately, real life application of encryption and other computer security mechanisms rarely execute cleanly. Whitten and Tygar [5] observed user interface problems that made it difficult for untrained computer users to properly encrypt e-mail messages. Garfinkel's thesis [3] demonstrates how changes in the design of e-mail client interfaces can remove some of the confusion.

We can continue trying to design more usable encrypted e-mail systems. The question is how much can we improve? Stepping away from interface design issues, instead of asking "Why Johnny Can't Encrypt" [5] maybe we should ask "Would Johnny Want to Encrypt?"

2. STUDY DESIGN

The goal of this study is to understand the choices people make about choosing to send clear-text and choosing to send encrypted e-mail messages. We framed our observations and analysis with sociologists' extended case method [1]. In the extended case method, the researchers draw upon previous work to form hypotheses that describe or explain social behavior. They apply these hypotheses to focus observations in the field, particularly noting where theory does not match observed practice. These contradictions then help the researchers evolve theoretical explanations of social phenomena.

2.1 Hypotheses

Our hypotheses about reasons for failing to adopt encrypted e-mail are drawn from the work by both Weirich and Sasse [4] and Dourish et al. [2]:

H1 *Perception of vigilance as paranoia* : While users may understand that protecting messages from observation is a positive measure, they probably see application of encryption as unnecessary. Making the effort to encrypt would be considered paranoid behavior.

H2 *Delegation and subversion of authority*: We expect that people who use encrypted e-mail were told to do so by someone in the computer support staff. A natural reaction would be passive resistance of orders to use encryption. Resistance should grow as the overhead to executing the orders increases.

H3 *Perceived unimportance or obscurity*: Users are likely to believe that information they handle is not worth protecting. Similarly, they may see themselves as unlikely targets of eavesdropping.

H4 *Annoyance or frustration with security systems*: Security mechanisms require the users to do something beyond their average, non-secure behavior. Users are likely to see the extra steps to be more secure as annoying or frustrating additions to their normal work.

2.2 Participant Selection

Although we are interested in why general e-mail users have failed to adopt the practice of encrypting e-mail, we particularly selected interviewees who had a strong motivation to encrypt their e-mail messages. We contacted non-profit groups involved with advocacy, as their work may involve controversial issues. In addition, the groups may have adversaries attempting to prevent their desired actions from seeing fruition.

Members from a group involved with acts of civil disobedience participated in semi-structured and unstructured interviews. The departments represented include finance, legal, computer support, public relations, and activity planning. Activities include protests, sit-ins, and human-chains. There were five male and four female interviewees. Interviews ranged from ten minutes to one hour long.

3. PRELIMINARY RESULTS

While the interviews need to be formally coded and analyzed, preliminary anecdotal evidence is presented here.

Hypothesis 1. Everyone except computer support staff said encrypting all e-mail messages was unnecessary. In fact, several mentioned encrypting all messages was for paranoid people rather than pragmatic ones. The support staff saw encrypting all traffic as a means of obscuring which messages were secret and which messages were not. The other members of the organization saw an opposite equation: *Encryption = Secret.* Those outside of computer support believed encryption should only be used when handling secret information. In fact, one man mentioned how receiving an encrypted message with mundane content was annoying. Upon receiving the message, he expected that taking the time to decrypt would reveal something special. When the contents were unimportant instead, he found it disappointing.

Hypothesis 2 and 4. When asked if they would use encrypted e-mail if support staff requested it, almost all participants said they would use encrypted e-mail. While acknowledging that encrypting e-mail would be inconvenient, several participants said they trusted the support staff would only request this if it was necessary. In this case, they had no problem conforming to the policy. One exception was a lawyer. Her relations with outsiders was more dependent on altruism from pro-bono lawyers who were usually novice computer users. In these cases she was adamant about using the simplest means available - client-attorney privilege protected her from legal means of eavesdropping and she could not conceive of illegal use of these messages. Additionally, she did not want to inconvience volunteer workers. She was comfortable with using encrypted e-mail with others in the same organization since her relationship to colleagues was stronger than to outsiders. Human resources (HR) contrasted to the legal department in communication with outsiders. A women from HR said her relationship with outsiders was customer to provider. As a customer, she knew that providers relied on her business; therefore, they would accept and support a policy of using encrypted e-mail.

Hypothesis 3 Interviewees said that ordinary messages did not require encryption, consistent with seeing some information as unimportant to eavesdroppers. Surprisingly, many employees viewed the organization as targets for eavesdroppers. Encrypting messages was seen as necessary for those involved with planning civil disobedience activities. Everyone understood that the plans were secret until released. Few mentioned the finance group, but a man from finance also saw that he needed to keep information about donors secret. He explained that the release of banking information or even donor lists themselves would be damaging to the organization. This is consistent with the *Encryption = Secret* equation, but it is not consistent with an assumption of user obscurity.

4. DISCUSSION

The results of this work indicate that users believe encryption is necessary for transmitting secrets but unnecessary in other circumstances. If someone designates information is secret, colleagues are usually willing to encrypt the information.

The nature of the organization that helped with our interviews may have influenced our results. As it is a non-profit advocacy group, many employees participate in the group's protest activities. In other words, members of this group have a strong loyalty to the organization and are working to protect the sanctity of its outside identity. The successes of the organization are also personal successes. While any given misstep in security might not be pinned on a particular individual [4], the damage to the organization would be personal.

Also, the fact that the group's activities are inherently subversive means that the hierarchical structuring found in most organizations does not work well for this one. Without a strong hierarchy, it is reasonable that departments trust each other within the organization. If one department (computer support) has more knowledge and background about a particular issue, the others in the organization are willing to accept and trust decisions that this department makes.

5. FUTURE WORK

We are interested in seeing if these results apply to other non-profit groups who likely have similar organizational structure and strong loyalty from employees. We are also considering an opposite approach: observe hierarchically structured organizations, such as the certain government offices. These groups may be targets of eavesdroppers but may not have the same loyalty from employees.

6. REFERENCES

[1] M. Burawoy, editor. *Ethnography Unbound: Power and Resistance in the Modern Metropolis.* University of California Press, 1991.

[2] P. Dourish, E. Grinter, J. D. de la Flor, and M. Joseph. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal Ubiquitous Comput.*, 8(6):391–401, 2004.

[3] S. Garfinkel. *Design Principles and Patterns for Computer Systems that are Simultaneously Secure and Usable.* PhD thesis, MIT, 2005.

[4] D. Weirich and M. A. Sasse. Persuasive password security. In *CHI '01: CHI '01 extended abstracts on Human factors in computing systems*, pages 139–140, New York, NY, USA, 2001. ACM Press.

[5] A. Whitten and J. D. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *8th USENIX Security Symposium*, pages 169–184, 1999.