Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted E-Mail

Shirley Gaw
Dept of Computer Science
Princeton University
Princeton, NJ USA
sgaw@cs.princeton.edu

Edward W. Felten
Center for Information
Technology Policy
Dept of Computer Science
Princeton University
Princeton, NJ USA
felten@cs.princeton.edu

Patricia Fernandez-Kelly
Dept of Sociology and
Office of Population
Research
Princeton University
Princeton, NJ USA
mpfk@princeton.edu

ABSTRACT

We consider the social context behind users' decisions about whether and when to encrypt email, interviewing a sample of users from an organization whose mission requires secrecy. Interview participants varied in their level of technical sophistication and in their involvement with secrets. We found that users saw universal, routine use of encryption as paranoid. Encryption flagged a message not only as confidential but also as urgent, so users found the encryption of mundane messages annoying. In general, decisions about encryption were driven not just by technical issues such as usability, but also by social factors. We argue that understanding these social factors is necessary to guide the design of encryption technologies that can be more widely adopted.

Author Keywords

Security, extended case method, encrypted e-mail, activism.

ACM CLASSIFICATION KEYWORDS

J.4 Social and Behavioral Sciences: Sociology; H.5.2. User Interfaces: Evaluation/methodology.

INTRODUCTION

What will it take to make the use of encrypted e-mail universal and routine? Despite encouragement from the security community, the vast majority of users have not adopted encrypted email. HCI and security researchers have identified some barriers to adoption – for example, difficulty of use and mismatch between user interfaces and user's models of the technology – but we believe other barriers exist. In this paper we try to identify additional barriers by interviewing a set of users from an organization that relies on secrecy. Our interviews demonstrate that users' attitudes about encryption, and the social significance users attach to it, are an important factor in limiting adoption.

Here is the textbook example of how public key encryption is meant to work. Suppose Alice wants to send Bob a secret message but Mallory, an adversary, wants to read it. Alice generates a public and private key pair and shares her public key with Bob. Bob similarly generates keys and shares his public key. Then Alice and Bob use the keys to communicate confidentially and guarantee the integrity of their messages. Mallory is foiled.

Things are never this simple, though. For one, Alice may not realize that there is anything secret in her messages to Bob. Even if Alice knows, she doesn't want to bother Bob with a public key exchange. More likely, someone like technical support staff member Chris advises Alice to encrypt. Of course, Alice may just think Chris is paranoid, because Mallory would never target her. Quickly the textbook example becomes entangled with discussions of the expectations, attitudes, and needs of the users.

Knowing that few workplaces actually use encryption, and few think it is needed, we were lucky to have access to a group of employees who had a stronger incentive to encrypt. In semi-structured interviews, these employees revealed their motivation for using (and not using) this technology. Secret plans were at the forefront of their work at ActivistCorp[1], a non-violent, direct action (NVDA) organization, and this was cited as a factor for using encrypted e-mail. Employees at ActivistCorp had opponents working against them, they had secrets to protect, and colleagues' freedom was at stake when security failed.

This paper moves beyond speculation about barriers to adoption of encrypted email, to look at the factors governing the decisions of real users at ActivistCorp. Our research contribution is primarily empirical insight into how using encrypted e-mail depends on more than individual perceptions of usability; *individual users also consider their interaction with others in a social context.*

RELATED WORK

This work contributes to the growing literature in HCI and security (HCI-SEC). Cranor and Garfinkel outlined HCI-

CHI 2006, April 22-27, 2006, Montreal, Quebec, Canada.

[1] The name "ActivistCorp" and the names of all individuals associated with this work are pseudonyms to protect anonymity.

SEC research as having two approaches: 1) hiding security within applications (avoiding inconveniencing an uninformed user) or 2) highlighting security (informing an unaware user) [7].

Invisible Security

Protocols such as SSH (Secure SHell) are designed to avoid user decisions: end users only agree to recognize a SHA (Secure Hash Algorithm) fingerprint but avoid negotiating the actual encryption decisions communicated between the two computers [20]. Another example is the Secure Sockets Layer (SSL) used in web browsers. Instead of concerning themselves with the method used to secure a channel, users only need to recognize an encrypted channel from an unencrypted one when they look for the lock icon in their browser.

Several projects at PARC have pushed avoidable security decisions away from the users, calling for "implicit security" [20]. In Casca, the system provided an environment for users to easily share devices while abstracting the underlying security structure by taking advantage of physical proximity[10]. Similarly, the network-in-box also used physical proximity (user gestures) to help users set up a secure wireless network[3]. Hiding the use of digital certificates, ESCAPE provided a system for inviting users to view material published online while providing access control[2].

Informative Security

In this area, researchers evaluate designs for getting users to adopt more secure practices. The ubiquitous example is Whitten and Tygar's work, which highlighted usability issues in PGP 5.0 with the Eudora e-mail client[24]. The first part discussed ambiguities in the interface while the second part summarized observations of twelve users attempting to send encrypted messages. This work was followed by Garfinkel and Miller, who showed how using colored backgrounds could aid users in determining their success at sending an encrypted message without succumbing to new-identity attacks[14]. Similarly, Garfinkel et al. described how merchants prefer their suppliers to certify e-mail messages and how changes to e-mail clients could simplify comprehending this service[13].

Although they do not deal with encrypted e-mail, other projects have also tried to improve informing the user. Good et al. described how accompanying End User License Agreements (EULAs) with simplified and standardized versions was ineffective at communicating information[15]. Dhamija and Tygar used background random graphics ("security skins") to inform users of possible phishing attacks [8]. Millet et al. proposed a just-in-time plugin to aid users in understanding cookies implanted by websites [17] .

As Dourish et al. pointed out, "effective security will require that we examine the conceptual models on which our systems are built"[9]. We cannot expect that tweaking the usability of existing systems will lead to usable, secure, and readily adopted systems: they are fundamentally existing systems with more restrictions and less control. Informative security approaches expect we understand how to sift information in a way that is consistent with how users would want it sifted if security had been their first priority. Invisible security, which avoids hassling the user, also makes them "pay a price for such convenience"[3]. Invisible security approaches expect that we understand how to make decisions on behalf of the user in a way that is consistent with how they would decide if they were given the choice. Even if we understood, it may "not [be] possible to seamlessly integrate security and user goals in every situation"[20]. Instead of making assumptions about users, our work redirects discussion towards considering the context of user's work and values.

Sociological Security

While the above approaches tended to compare design A versus design B, some researchers have adopted sociological methods to explain how systems succeed and fail. Two papers have used Grounded Theory to frame observations and interviews. In Grounded Theory, researchers enter the field and later develop theory to explain observations[21]. This is most appropriate when starting a new area of research. For example, Adams and Sasse used this method to identify factors affecting secure password practices[1]. Similarly, Dourish et al. used Grounded Theory to investigate people's strategies toward security management[9]. Our work continues in this area to understand how people interact with security technology and what barriers discourage adoption.

DATA COLLECTION AND METHODS

Methods

With his Extended Case Method, Burawoy encouraged researchers to explicitly describe their assumptions and use these to guide observations: "rather than theory emerging from the field, what is interesting in the field emerges from our theory"[5]. With this method, researchers refine and evolve existing assumptions. As we had assumptions from our experiences and prior research, we felt that the Extended Case Method would be appropriate for focusing observations at ActivistCorp.

Prior to visiting ActivistCorp, we expected technical support staff would want everyone to use encrypted e-mail, but that other employees would see this as an unnecessary precaution. Beznosov et al. highlighted an underlying conflict between the goals of users and the goals of support staff (or security teams) within an organization[4]. With roughly a hundred users in the US and thousands more internationally, users would probably see themselves as obscure members of a larger group, like the people interviewed by Weirich and Sasse [22, 23].

As suggested by Schneier, people probably avoid security technology because of the inconvenience to their work and because of inexperience with available technologies[18]. We already knew the technical support staff had little opportunity to educate users. While general users might delegate security decisions to technical support [9], that department lacked the resources to implement encrypted e-mail for universal use.

We also wondered if employees would resent a requirement that impedes their work. They may subvert security policy [1], and we thought many would see precautions as paranoid behavior[22]. In short, we believed we would find few people who used encrypted e-mail routinely and many employees who thought using encrypted e-mail was unreasonable.

Site Selection

As mentioned earlier, we interviewed employees at an a nonviolent, direct action (NVDA) organization because we believed they had more incentive to protect secrets than typical industry workers. One example of this is how members of the organization portrayed themselves in an internally circulated document:

> As an organization, we have certain values and tactics that differentiate us from other groups. We are not afraid to stand up to corporations or governments, put our lives on the line or block roads.
>
> Even though all of us here are on the payroll ... try to avoid referring to us as "staff" or "employees" in materials. If someone works for [ActivistCorp], he or she is an activist. If someone is participating in an action, he or she is a supporter or [an] activist (or [a] professional for the dangerous ones).

Considering how employees also work as activists, we expected that working for ActivistCorp was a personal decision and people would emphasize supporting the organization—whether that means taking a pay cut or being arrested for your support. If ActivistCorp believes using encryption would help protect the organization, we expected the employees would try to implement the policy.

The national office managed the technical support for employees across the country. Dependent on donations, ActivistCorp spent little on software purchases. Although Microsoft Windows remained a popular operating system, many employees used free software to meet their needs. Pegasus Mail was the primary e-mail client. Those who needed encryption used Pretty Good Privacy (PGP) with an idw plugin. PGP is a program that implements public key encryption, helping users to generate a public key and private key pair, to encrypt and decrypt messages, and to attach digital signatures. idw provides a free plugin, PGP for Pegasus Mail, that is an interface for using PGP within the Pegasus Mail client.

The interviewer spent two days visiting ActivistCorp's national office, talking with nine employees from five departments: two from technical support, three from campaigns, one from development, one from media, one from legal, and one from human resources. Interviews were semi-structured. Discussions with two employees from technical support were unstructured. Interviews ranged from ten minutes to an hour and a half. Because we originally requested twenty minutes per interview, we asked permission before continuing to interview for longer than the agreed period. The interviewer also asked for verbal consent before recording the interviews; all of the employees consented although the free-form discussions with technical support staff were not recorded.

PRACTICES OF ADOPTERS AND NON-ADOPTERS

The following excerpts highlight a few perspectives from the nine interviewed employees. Each of the four vignettes describes the employee's job and their use of encrypted e-mail in the workplace.

The Habitual User: Cautious or Paranoid?

Woodward worked for the campaigns[2] department as a researcher. While interviewing Woodward, his officemate Stefan (a research manager) periodically interjected comments.

As the interviewer walked up to Woodward's desk, she heard a whirring sound and realized he was shredding a document; it was an unusual start to a conversation asking him about his security precautions. Such measures are actually unremarkable given his job. Woodward looks for incriminating evidence against ActivistCorp's opponents. Not all of this information is easily obtained; Woodward might use atypical channels to retrieve it. For example, after recalling the last time he encrypted an e-mail, he described why he used encryption in that message:

> That's not public information. [pause] And we got that information through ways—and it's not information that's publicly available and it's known that it is not publicly available, also.

Part of the reason he felt it was necessary to encrypt a message was that he might inadvertently reveal his source. With a job so focused on gathering information, he was naturally protective of his own information flow:

> I know how people get information from companies and corporations. That's part of what we do.

He also cited concern over who might be watching:

> I'm aware of the level of government surveillance that's happening. Most people aren't aware of the FBI's Carnivore program, you know.

He added, "there are a lot of people that are interested in what we are doing." Not only did he encrypt messages, but he also encrypted part of his hard drive:

> 'Cause otherwise, if I lost my laptop, you know, then someone would just be able to read everything on it. And so then, what would be the point of—what would be the point of encrypting anything, you know, if—if everything I have is—someone could just read it on my laptop?

[2] Campaigns are "a connected series of operations designed to bring about a particular result" (Merriam-Webster) rather than simply political bodies. Actions or direct-actions are the high-profile events staged by activists. The actions are grouped by goals known as campaigns.

In addition, he distrusted plugins for e-mail programs, relying on encrypting the text of a message first and copying it into his e-mail client later. He feared a plugin that simplified the process might be a Trojan horse or an improperly implemented program. He was careful enough to encrypt a message, so Woodward also carefully avoided compromising an e-mail through a software hole. He said his vigilance was related to his background in understanding the weaknesses of technology. He encrypted messages whenever he used wireless "and that's just because wireless Internet is so inherently insecure." He knew because he had sniffed traffic in wireless hotspots himself.

Woodward's concern may or may not be justified [16]. He cited the multiple instances where ActivistCorp's offices were infiltrated or raided. The possibility of espionage made him vigilant. He admitted that there were times when he used encryption without need but he justified this behavior:

> Oh, sure. I'm sure there's many times where it's not absolutely necessary, but I'd rather err on the side of caution.

At the same time, Woodward said he did not encrypt public information, though. If it was public, he would send the information in plain text.

Woodward was surprisingly more cautious than what we initially expected from employees at ActivistCorp. While he was vigilant about protecting secret information, he still limited his use of encryption.

A Middle Ground

While Woodward may have displayed extreme vigilance with information, campaigns and actions provided the visible accomplishments of ActivistCorp. Woodward was involved with confidential aspects of the organization. Most people are not. A large portion of the employees keep the organization afloat with extensive administration, including departments for human resources, development (fundraising), finance, legal, technical support, and media.

These two vignettes are from administrative employees describing how they have used encryption in ActivistCorp. As they were peripherally involved with actions, they were practical about taking security precautions.

The Self-Sender: "Don't Go Overboard"

Abe worked in development, helping ActivistCorp's fundraising efforts. Because he handled financial data, Abe used encryption frequently, particularly when he received records from online donations ("I tend to try and be sure I PGP everything that has a credit card number on it.") He also communicated with an external vendor for recruitment. They used encryption to protect financial data when they synchronized their copies. Abe believed this setup was simple; he also thought some people in ActivistCorp needed to be more vigilant. He described how he tried to convince the head of campaigns in his home country to use encryption:

> Why? Because it was just good. If the ... police ever come and bust into the office, you shouldn't have a document saying "Hey, I'm discussing how I'm going to campaign against [a controversial issue]." It's not the kind of information you want them to have.

Despite his reasoned argument, his colleagues were uncooperative, "most people see this as more work and want things simpler."

Abe saw himself and believed others saw him as someone comfortable with technology:

> I use computers a lot at [ActivistCorp]. I'm—I'm actually considered a "techie"—that's what other people say, "Oh, you're being a techie."

Abe's attraction to adopting PGP was related to his love of technology and the excitement or importance implied by use:

> [When] it wasn't forced upon me, I was willing to try it. For boys at least, there's a "gadget factor" because [I was told] it would take five years for the CIA to decrypt it, so you felt a bit like a secret agent.

He qualified his interest, however:

> I figure I'm a hundred times better than most people if I've encrypted. Don't go overboard.

He estimated that encrypting every e-mail message would add another hour to his workday unless it was automated. He said encrypting is like healthy eating and exercise as you admire those who do it because you know it's the right thing to do, but you do not actually do it yourself. He just wanted to be responsible; he would encrypt some things but not everything. Fear of attackers was less important than ease of use. If it was easier to encrypt everything, he would. He likened this to backing up data; there was "no fun factor" and encryption was a chore, "like housework."

Abe was another example of a user who was aware of the secrets he accessed within the organization. He was also technically savvy, although perhaps not as absorbed as Woodward. Unlike Woodward, however, Abe saw the technology as difficult to set up for ordinary users.

An Ephemeral User

Jenny worked as a liaison between campaigns and the other departments at ActivistCorp, primarily helping people within the organization. She had used encrypted e-mail but that was over two years ago:

> Um, I've used it before. I used PGP—I don't know if that's a certain kind, or [pause] that's what we call it here. I used it before, involving—before doing some sort of action. We did a whole bunch of direct action and we had [pause] I guess two of those nationwide ... we were sending encrypted e-mails back and forth ... so, like, leading up into that so people weren't reading

> what we were doing—or would know when we were going to do it?

Since Jenny ended with a question, she might have distanced herself from encryption experts. She began the interview by nervously saying, "I hope I can be of help to you because I don't really use it that often." She also refrained from speculating about what encryption does or how people could intercept e-mail communications:

> I have no idea how it works. I guess people can hack into our system, but I have no idea, like all that kind of IT stuff.

She also said it had been so long since she used PGP that it was unlikely she could use it again:

> I use it very [pause] like I did, maybe sent two e-mails, so I didn't use it very much at all. And it's [pause] it was on my computer, but I haven't used it in so long that I probably don't remember how to use it. I'd probably have to get, like, a refresher course.

Although uncomfortable with the technology, Jenny saw encryption as helping to protect the confidentiality of messages. The interviewer asked her to speculate on why she had to use PGP two years ago:

> Well, I think the reason we use it is so that we can actually perform the action that we want to do, so that it's not like we get stopped before we've actually been able to, like, you know, put up our banners or things like that.

When the interviewer tried to get her to discuss other circumstances where she could use encryption, she did not understand. In fact, Jenny had trouble understanding why we were looking at encouraging people to use encrypted e-mail more often:

> I have a question for you ... why would people need to encrypt their e-mails, like more? Everyone, like corporations and stuff. And why would they ... why would more people want to encrypt their e-mails?

While Jenny was involved with ActivistCorp's visible action work, she rarely needed to use encryption and she only used it for short durations. She was open to receiving help on using encryption, but she was uncomfortable portraying herself as an expert. She was also unable to see why it could be used more generally than just protecting secrets.

The Uninitiated User: Without a Secret

Sandra was a co-author of a writing manual circulated within the organization. This manual advised people on how to present ActivistCorp to the public. What was intriguing about this manual was the following statement:

> Some good advice: if you don't want something you put in an e-mail to get into the wrong hands, don't write it in the first place.

Her explanation of the manual's statement was that she was concerned about accidentally sending messages to the wrong people:

> The reason I included that sentence was just, um, to make sure that people are careful because e-mails can be really dangerous. And I know I, in the past, have clicked "Reply all" instead of "Reply" or "Forward" when I thought I was replying. [My advice was] just to keep people from getting into trouble.
>
> I've sent e-mails to people that I thought, "Oh, maybe I shouldn't have sent that e-mail" but that's just 'cause I was angry. [laughs] You know? [I've never been] afraid someone would read it that shouldn't.

She limited her concern to warning against sending something personally offensive. She felt that encryption was unnecessary for her day-to-day work:

> I don't think any of my communication is anything people are dying to get their hands on. I don't—I am not involved in any of the ... protests or that sort of situation we do. So, there's not as much need for, like, me in the organization to use that kind of thing.

Sandra believed what she wrote was uninteresting to eavesdroppers. She, like the others interviewed, saw encryption as a method of protecting secret information.

Sandra believed her role in ActivistCorp was low-profile; she warned others about their use of e-mail, but her advice was about sloppiness rather than secrecy. She thought it was unlikely that governments or opponents would be interested in observing her communications.

ADOPTION CRITERIA

Having introduced a few of the employees at ActivistCorp, we now have their perspective for understanding some of the social context in adopting encrypted e-mail.

Secrets

As mentioned before, employees made the distinction between justified use of encryption for protecting secrecy and paranoid use of encryption for universal communication. Woodward's officemate, Stefan, especially illuminated the level of secrecy required to protect ActivistCorp's internal plans:

> You don't want to show your cards. You don't want that stuff out because people's lives are in jeopardy—*really*. I mean, people are taking an action and could be arrested, could be, you know, jeopardized in some way.

ActivistCorp wants to surprise an opponent when actions start. Thus, information about when an action starts is secret. Additionally, Stefan explained that the end of an action was also secret information:

> It's like if you had a strike against a company but you announce that we're gonna give in on May 7th whether

> or not we've won yet. Then the company would just say, "Well, fuck, we'll just wait ...." What we're doing is holding a protest and we want [pause] the—whoever we're opposing to think that there's no end to this protest until we give in.

He went on to say that anything related to maintaining ActivistCorp's identity needed to be protected:

> We're like a corporation, so if Nike ... said "Damn, Adidas really has us on the running shoe market" and that was printed in the paper, it would crash their stock prices. Things like that. We're in the same game. We're sort of competing for power and—and the illusion of [ActivistCorp's] power is really important, as important as our real power, like corporations and politicians fear what they think we can do.

Stefan and Woodward both felt using encryption was a necessary component of their jobs; interestingly, both worked in campaigns but drew their examples from actions. They described the need to protect the information about the start, end, and available resources of a direct action. In fact, almost all of the employees interviewed believed that only the actions department or only the actions and campaigns departments needed encryption.

Abe in development recognized another situation, however. First, he had to protect the banking information of donors:

> We have our supporters out there—our supporters are giving us ... donations. So, they're doing it from ... the most sensitive place they can. There's no commercial reward in it for them. They've come to us and said "I have a good heart, I love what you guys do. I want to give you money so that you can do it."
>
> So then, in that respect, it would be far more damaging for us if something was to happen to those donor's records from two aspects. One, if there was any financial, uh, impropriety in their accounts. If somebody got a hold of their credit cards or something like that and eventually it was ... police researched and they said, "well, they got it because they got that file from [ActivistCorp]".
>
> Our supporters would say, [sighs] "you know what? You guys are not responsible [pause] we can't trust you with our—our credit cards. Now I'm not gonna give you any more money." And that means we're finished.

The second potentially damaging situation he wanted to avoid was release of donor identity as many donors did not want to be linked to the organization:

> I imagine that [some people] might really want to support us, but they assume that by supporting us, they put a mark on themselves as being *bad*. So, if they do, are brave enough to support us, I think, in their minds, they are pretty sure that we are going to protect their confidentiality, you know.

As a related point, he saw these identities as a target for snooping as well:

> Who knows? In a post-9/11 world, [ActivistCorp] doesn't have a lot of friends on the other side, so's to speak. The other side being the administration, industry ... the Homeland Security, you know. We're not, uh, on the same side of the game anymore. We're definitely opposed to what they do. And I think they view us far more as an enemy today than before September 11th. So there's a definite suspicion there. Maybe we're over-inflating our importance, maybe we've got a big ego, but we'd like to believe that they would be very interested to [pause] run through our database and see exactly who supports us. They would be very interested to know who our supporters are. And so, we're obliged to protect it in every possible way.

ActivistCorp employees believed it was necessary to protect internal secrets in two circumstances. First, employees encrypted internal organization secrets. Secondly, employees protected donor's financial data and personal information.

Paranoia

Many of the employees interviewed at ActivistCorp had limits to their willingness to be more secure. In fact, moving beyond that limit was seen as abnormal or paranoid. While Woodward was especially vigilant, even the technical support staff admitted he might be excessively protective. Was the effort justified? Was it reasonable precaution?

Abe explained how someone could "go overboard" when he described how a representative of the PGP Corporation visited ActivistCorp. Instead of a typical password authentication, the representative took off his necklace and used a removable flash drive that held his private key. The demonstration discouraged Abe:

> It was too over-the-top and definitely too complicated. It was like a movie.

He saw the presenter as paranoid. He went on to say:

> Yeah, I admire him because he comes in and puts his passphrase [bumps on the table] every single day, three times a day, so that's very dedicated to his stuff. He must either be very scared or very motivated.

He was not sure whether this vigilance was justified. In fact, he associated it with being fearful, perhaps irrationally fearful. Abe reiterated this when asked to speculate on why a colleague sent every e-mail message encrypted. He figured this man has an automated system for encrypting e-mail "or he's nuts."

When Sandra was asked why she said her e-mail communications were not anything people were "dying to get their hands on," she explained:

> I'm not paranoid enough to think the CIA is monitoring my e-mails or anything to that effect.

Not only was encrypting messages excessive for someone who had no secrets, it was *paranoid behavior* to assume anyone would be interested in eavesdropping on her communications.

Jenny also thought it was abnormal to encrypt non-secret information. When the interviewer abstractly explained that people in security suggest all users encrypt all messages, Jenny was baffled:

> So you're saying that ... people should just—even *normal* people? That ... you're sending e-mail to ... your mom, like "Hey, things are going [pause]" That you should encrypt your e-mail. That people should do all that.

Jenny emphasizes "normal people." *Normal* people wouldn't encrypt normal messages.

Flagging

Jenny's quote highlights another association with encryption. Encryption is a flag of message importance or secrecy. Once flagged, people will try to maintain that level of secrecy. For example, an ActivistCorp lawyer said when a message had been sent to her in encrypted form, she would always reply with an encrypted message. Jenny agreed to this as well. Jenny delegated the decision to use encryption to the head of the action, some manager. When she received encrypted messages, she just needed to make sure she could maintain the same level of secrecy someone else declared.

Encryption was seen as an annoyance in other circumstances. For Jenny, universal and routine use was incomprehensible:

> I just don't see people going, "oh, yeah, I should take the extra step to encrypt my e-mail." It's not a hard extra step, but I don't understand why. Like, I can see people saying ... I should protect this against a virus or something like that. But encryption, I just—it doesn't—I don't think people would see that as a [pause] a bonus, like something that they'd really wanna [do]—does that make sense?

Some encrypted messages violated this expectation of secrecy. Abe talked about someone who sent unimportant but encrypted messages. There was a time cost to decrypting received messages, so forcing the recipient to decrypt was considered rude:

> I work with somebody ... and he sends *every—single—message* of his is encrypted. Even if it is just saying to you, "hey, can we have a meeting tomorrow at 2:00?"—it's encrypted. Why? I think he probably has some automated system. That everything he sends gets encrypted automatically. I can't believe he's encrypting manually every time. But to me, it's like—OK, if it's automated—fine. But, it's a bit irritating, you know. I get this message and—oooh, it's encrypted. "Can we have a meeting tomorrow at 2:00?" I'm like, what's the secret? You got to justify it. I mean—unless it—if it was all happening automatically—great. If it was encrypted on his computer and he sent to my computer, automatically encrypted or decrypted it—fine. Then, encrypt everything you want. But if he's just writing to me something, why put the extra workload on me of tapping in my passphrase and opening it up separately and so forth?

Encryption was a flag that signaled a message was important. If the message was mundane, it was annoying to get overexcited or to spend the time to decrypt the message.

Key Management

Setting up encrypted e-mail is one of barriers to adopting it. Schneier writes key management is "without a doubt, the most difficult issue in cryptographic systems." [11]. From a social context, we expected overhead and intimidation prevented adoption. Abe described it as "the average person doesn't think they can set up encryption." Jenny dismissed the usability problem though:

> No, it was ... I mean, I don't remember having any problems using it ... it wasn't hard. [pause] It was just something—like, you had to ... find the right person, you know ... it wasn't like you could just send an e-mail, you had to definitely ... [pause] find the right key? In order to ... send them something. But, I didn't think it was that hard. It was easy to use, you just—you just had to learn how to use it, I guess you could say, if you remember your password, which I don't remember right now [laughs]. Like it's a different password from all the other stuff. But if I used it more often, I don't think it would be that hard.

Abe believed that encrypting messages is "really simple if it is set up for you" and having technical support staff set up the process would increase use. The technical support staff helped Woodward start using encryption:

> With my job, one day a task arose related to, um, a certain direct action that we were doing. And they were like, "Whoa, well, we can't send you this, you need a PGP key." So then I—I walked down to the IT department and said, "guys, I need this PGP thing." They're like, "OK" and they set me up with everything I needed to know.

Abe described this situation:

> [PGP is] almost, like, viral: I have got it and I want to use it and you start using it.

Considering these examples, starting to use encryption implies delegating authority [9]: someone else determines encryption is necessary and someone else sets up encryption.

Security Models

The technical support staff brought up the ideal of universal, routine encryption of e-mail, but they saw current PGP system setups as an impractical burden for a hundred ActivistCorp users. Unlike the support staff, none of the other employees interviewed (not even Woodward), mentioned this argument in their interview. The general users had another model entirely: they were willing to support a policy of encrypting secrets, whether it was information related to an action or to financial data, but it was a huge cognitive leap to go from protecting secrets in an individual message to obfuscating secrets using everyone else's messages.

Encryption was equated with stopping opponents from discovering secrets, as Stefan elaborated:

> I think the only people who do encryption in the organization are people who have been trained to be—who are associated with—specifically the [direct actions] we do. So we keep that stuff encrypted. And that's [pause] I think probably anybody outside of [ActivistCorp] would assume that's what we do.

Jenny agreed when explaining why she does not use encrypted e-mail more often:

> Um, I'm not really involved in the planning of that kind of stuff [in direct actions]. And I don't know of any other reason I would need to encrypt my e-mails 'cause most of my e-mails are just ... things public. People could learn, I mean, people could read my e-mails, they wouldn't see anything [pause] incriminating? I guess that's the only thing. [Outside of that], I don't understand why anyone would need to [pause] encrypt their e-mails, I guess, in the organization.

Equating encryption with confidentiality might disappear if encryption was invisible to the user. It also might not—consider digital signatures. The human side of cryptography is simplified if just digital signatures are used. Once a user has set up a public and private key pair, an e-mail client can automatically and routinely sign messages. The recipient can check the signature if they want but they can ignore it as well. The sender (actually, the sender's software) does all the work and the recipient benefits if they understand and observe the digital signatures.

A digital signature first demonstrates the message has not been altered—the signature contains a digest of the message so an altered message implies an altered digest. The digest is encrypted with the sender's private key, so altering the message and the digest seems to require the sender's private key. A digital signature can also warn about forgery if the public key required to decrypt the digest differs from a sender's known public key. We expected employees would value message integrity comparably to message confidentiality and would value the utility of the cryptographic methods for demonstrating integrity. Although we had not explored the topic in depth, digital signatures seemed relatively unimportant to the employees we interviewed.

Both Abe and Woodward encrypted e-mail regularly, so they both had public and private key pairs. Neither routinely signed their messages. Woodward saw signing messages as a feature bundled with encryption. He knew that there was a button to encrypt and sign, but he only signed messages that were encrypted. We speculate that since Woodward avoided encryption when sending public information, signing messages was extra effort; he only semi-regularly used the software that signed messages. For Abe, digitally signing required more cryptography than he was comfortable with:

> I probably don't know how to use it in the best possible way, but I know how to encrypt and un-encrypt. I don't explore, uh, the more complicated things.

Even with two technically savvy users, we were unable to see universal, routine use of a technology for demonstrating integrity of messages. The imminent danger was snooping [16]; discussions about catching (or warning about) forgery and tampering never started even as Abe could benefit from checking for tampering in his financial reports.

DESIGN IMPLICATIONS

Critics may argue that ActivistCorp had adopted the least usable form of the technology. Had employees adopted implementations like HushMail, CryptoHeaven, or S/MIME support in e-mail clients like Thunderbird or Outlook, perhaps they would have encrypted more frequently or with fewer complaints. We argue, on the other hand, that employees at ActivistCorp were more than willing to withstand slight inconveniences; they already made sacrifices for the sake of ActivistCorp. At the same time, we agree that the design of encrypted e-mail systems could be improved to match how people intend to use the technology. We present three criteria for design improvements here; they are speculative at this point. Specific cryptographic primitives or system designs are areas for future work.

Tailored Interfaces

First, the results of this study indicate that systems should be tailored to fit specific users. Instead of having generic encryption systems that encompass all types of use, we need to adopt Cooper's method of "design for just one person" [6]:

> The broader a target you aim for, the more certainty you have of missing the bull's-eye. If you want to achieve a product-satisfaction level of 50%, you cannot do it by making a large population 50% happy with your product. You can only accomplish it by singling out that 50% of the people and striving to make them 100% happy. It goes further than that. You can create an even bigger success by targeting 10% of your market and working to make them 100% *ecstatic*. It might seem counterintuitive, but designing for a *single user* is the more effective way to satisfy a broad population.

For *ephemeral users* like Jenny, using encryption is an exception rather than a norm. Ephemeral users need something easy to start with and something that can be used for a short duration. They should be spared from making decisions about encryption. *Habitual users* such as Woodward have longer term encrypted communication threads. Additionally, they are comfortable with complex technology, but moreover, they may be suspicious of abstractions. They need transparency. *Self-senders* are people like Abe. Abe sent himself banking records from the server that recorded donations. Self-senders essentially want encrypted storage—users should be able to easily encrypt messages to themselves; this protects against infiltration on the mail server and provides secure storage. All three types of users encrypt messages, but they have three different needs. While a multi-layered interface [19] can simplify a habitual user's interface for an ephemeral user, this approach would have difficulty incorporating self-senders' needs. Furthermore, multi-layered interfaces fail to incorporate knowledge of how users engage in different types of communication. Instead, we want interfaces tailored to the needs of the three types of users without restricting their use.

Interoperable Systems

While we argue that encrypted e-mail systems should be tailored to an individual's needs, at the same time, the users we document here are members of a larger organization and work with people from other organizations. Within an organization, the system needs to support different types of use while simultaneously supporting interoperation. For example, habitual users and ephemeral users could work on the same projects. Woodward and Jenny could both be involved in planning an action. The action's leader should set up Jenny's system for the short term but also support Woodward's existing setup.

The project manager could send invitations via e-mail that lead group members to register with a key server. Habitual users could supply their own public keys while ephemeral users could be guided through a key generation step. After registration, the users should be able to encrypt messages by simply flagging a message as belonging to the project. Additionally, as encrypted messages are received, replies should be automatically encrypted to maintain the same level of secrecy. When the project finishes, the manager could terminate the message threads and clean up any interface changes to e-mail clients. Similarly, individual members could terminate the communication with a "panic button" in case their machines are going to be confiscated. Ideally, these interactions would be supported without a central key sever, without naming authorities, and without cooperating e-mail servers. Clearly this is far from a complete system design, but we are trying to hint at what approaches might work.

Even when designing for one type of user, we have to consider that users also work in multiple contexts. For example, Abe was a self-sender for financial reports, yet he also synchronized this data with an outsider and he used his system in both contexts. On the one hand, a self-sender should not have to use public key encryption in simplex communication; a single secret key should be sufficient. On the other hand, whatever system he uses for sending messages to himself should interoperate with the system he uses to exchange reports with his colleague. He should be able to do both without resorting to public key encryption for both circumstances; that is, supporting work in multiple contexts is more complex than reducing the problem to the most flexible encryption protocol.

The above scenerios fall short of declaring new underlying cryptographic primitives. What is required is still unclear. Intuitively, encrypted e-mail systems need to support multiple types of use while simultaneously supporting communication between the different types.

Invisible Security

Arguably, some of the stigma associated with using encrypted e-mail was tied to the overhead of the system ActivistCorp used. Where appropriate, some of the process can be removed or automated. The danger is in making decisions that conflict with users' intentions or values; the systems could impractically restrict use, preventing users from meeting their goals, or could ineffectively serve, making decisions the user finds unexpected or disagreeable. Making security invisible ultimately has to respect tailoring approaches. We advocate methods that integrate qualitative analysis of users' needs with system design such as Value Sensitive Design [12]. Future work in making security invisible has to incorporate what users believe needs increased security before making the decision for them.

CONCLUSION

The security community has long recognized the utility of encrypted e-mail: it protects the contents of messages and universal, routine use obfuscates e-mail traffic. There is also a recognized usability problem: adopting encryption incurs overhead cost and sending encrypted e-mails is less efficient than sending plain-text e-mails. Our work has contributed to prior work that qualitatively studies HCI-SEC, specifically illuminating the social setting affecting adoption of encrypted e-mail. Utility and usability influence adoption, but they are not the sole criteria.

The perspective and examples provided by our interviews offer valuable insight. First, ActivistCorp was a rare organization in that secret plans constituted a major component of the organization's mission. Second, many employees personally supported the activist group's causes and, thus, these employees had more incentive than ordinary industry workers when considering the protection of organization secrets. Lastly, ActivistCorp also granted us access to see inside the organization. These circumstances came together to make the quotes and descriptions from the interviews a unique portrait of using encrypted e-mail in the workplace.

While our findings are tied to the specific technology used by participants, they nonetheless provide insight into the non-technical aspects affecting adoption. Right now, Alice and Bob have to worry about key management; if we solve the key management problem, encrypted messages may no longer indicate the secrecy and importance they currently do. Then, Alice could invisibly or automatically exchange keys with Bob and she could forget about passphrases and software setups. In the meantime, the current context of encrypted e-mail has social meaning that explains how Alice and Bob excuse themselves from adopting increased security.

ACKNOWLEDGMENTS

We are indebted to the employees of ActivistCorp for participating in this study and are particularly grateful to our host in technical support who helped organize the interviews. We would also like to thank Pierre-Antoine Kremp, Lujo Bauer, Karyn Moffatt, and our anonymous reviewers for valuable advice and feedback. Shirley Gaw was supported by a National Science Foundation Graduate Research Fellowship.

REFERENCES

1. Adams, A. and Sasse, M. A. Users are not the enemy. *Commun. ACM 42*, 12 (1999), 40–46.
2. Balfanz, D. Usable access control for the world wide web. In *Proc. of ACSAC*, IEEE (2003), 406–415.
3. Balfanz, D., Durfee, G., Grinter, R. E., Smetters, D., and Stewart, P. Network-in-a-box: How to set up a secure wireless network in under a minute. In *Proc. of the 13th USENIX Security Symposium*, USENIX (2004), 207–222.
4. Beznosov, K., Zurko, M. E., Chan, S., and Conti, G. Usability of security administration vs. usability of end-user security. SOUPS 2005 Conference Panel, 2005.
5. Burawoy, M., editor. *Ethnography Unbound: Power and Resistance in the Modern Metropolis*. University of California Press, 1991.
6. Cooper, A. *The Inmates Are Running the Asylum: Why High Tech Products Drive Us Crazy and How to Restore the Sanity*. Pearson Higher Education, 2nd edition, 2004.
7. Cranor, L. F. and Garfinkel, S. Guest editors' introduction: Secure or usable? *IEEE Security & Privacy Magazine 2*, 5 (2004), 16–18.
8. Dhamija, R. and Tygar, J. D. The battle against phishing: Dynamic security skins. In *Proc. of SOUPS 2005*, ACM Press (2005), 77–88.
9. Dourish, P., Grinter, E., de la Flor, J. D., and Joseph, M. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal Ubiquitous Comput. 8*, 6 (2004), 391–401.
10. Edwards, W. K., Newman, M. W., Sedivy, J. Z., Smith, T. F., Balfanz, D., Smetters, D. K., Wong, H. C., and Izadi, S. Using speakeasy for ad hoc peer-to-peer collaboration. In *Proc. of CSCW 2002*, 2002.
11. Ferguson, N. and Schneier, B. *Practical Cryptography*. Wiley Publishing, Inc., New York, NY, 2003.
12. Friedman, B. Value sensitive design. In *Encyclopedia of human-computer interaction*, 769–774. Berkshire Publishing Group, 2004.
13. Garfinkel, S. L., Margrave, D., Schiller, J. I., Nordlander, E., and Miller, R. C. How to make secure email easier to use. In *Proc. of CHI 2005*, ACM Press (2005), 701–710.
14. Garfinkel, S. L. and Miller, R. C. Johnny 2: a user test of key continuity management with S/MIME and Outlook Express. In *Proc. of SOUPS 2005*, ACM Press (2005), 13–24.
15. Good, N., Dhamija, R., Grossklags, J., Thaw, D., Aronowitz, S., Mulligan, D., and Konstan, J. Stopping spyware at the gate: a user study of privacy, notice and spyware. In *Proc. of SOUPS 2005*, ACM Press (2005), 43–52.
16. Lichtblau, E. Large volume of FBI files alarms some US activist groups. New York Times Online, July 2005.
17. Millett, L. I., Friedman, B., and Felten, E. Cookies and web browser design: toward realizing informed consent online. In *Proc. of CHI 2001*, ACM Press (2001), 46–52.
18. Schneier, B. *Secrets and Lies : Digital Security in a Networked World*. Wiley Computer Publishing, New York, NY, 2004.
19. Shneiderman, B. Promoting universal usability with multi-layer interface design. In *Proc. of CUU 2003*, ACM Press (2003), 1–8.
20. Smetters, D. K. and Grinter, R. E. Moving from the design of usable security technologies to the design of useful secure applications. In *Proc. of NSPW 2002*. ACM Press (2002), 82–89.
21. Strauss, A. and Corbin, J. M. *Basics of Qualitative Research : Techniques and Procedures for Developing Grounded Theory*. SAGE Publications, 1998.
22. Weirich, D. and Sasse, M. A. Persuasive password security. In *Proc. of Ext. Abstracts CHI 2001*, ACM Press (2001), 139–140.
23. Weirich, D. and Sasse, M. A. Pretty good persuasion: a first step towards effective password security in the real world. In *Proc. of NSPW 2001*, ACM Press (2001), 137–143.
24. Whitten, A. and Tygar, J. D. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *Proc. of 8th USENIX Security Symposium*. USENIX (1999), 169–184.