An Inconvenient Trust: User Attitudes toward Security and Usability Tradeoffs for Key-Directory Encryption Systems

Wei Bai, Doowon Kim, Moses Namara, and Yichen Qian, ***University of Maryland, College Park;*** **Patrick Gage Kelley,** ***University of New Mexico;*** **Michelle L. Mazurek,** ***University of Maryland, College Park***

https://www.usenix.org/conference/soups2016/technical-sessions/presentation/bai

This paper is included in the Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016).

June 22–24, 2016 • Denver, CO, USA

ISBN 978-1-931971-31-7

Open access to the Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016) is sponsored by USENIX.

An Inconvenient Trust: User Attitudes Toward Security and Usability Tradeoffs for Key-Directory Encryption Systems

Wei Bai, Doowon Kim, Moses Namara, Yichen Qian, Patrick Gage Kelley,* and Michelle L. Mazurek
University of Maryland, *University of New Mexico
{wbai, doowon, mnamara, yqian1, mmazurek}@umd.edu, *pgk@unm.edu

ABSTRACT

Many critical communications now take place digitally, but recent revelations demonstrate that these communications can often be intercepted. To achieve true message privacy, users need end-to-end message encryption, in which the communications service provider is not able to decrypt the content. Historically, end-to-end encryption has proven extremely difficult for people to use correctly, but recently tools like Apple's iMessage and Google's End-to-End have made it more broadly accessible by using key-directory services. These tools (and others like them) sacrifice some security properties for convenience, which alarms some security experts, but little is known about how average users evaluate these tradeoffs. In a 52-person interview study, we asked participants to complete encryption tasks using both a traditional key-exchange model and a key-directory-based registration model. We also described the security properties of each (varying the order of presentation) and asked participants for their opinions. We found that participants understood the two models well and made coherent assessments about when different tradeoffs might be appropriate. Our participants recognized that the less-convenient exchange model was more secure overall, but found the security of the registration model to be "good enough" for many everyday purposes.

1. INTRODUCTION

As important communications become primarily digital, privacy becomes an increasingly critical concern. Users of communication services (e.g., email and chat) risk breaches of confidentiality due to attacks on the service from outsiders or rogue employees, or even government subpoenas. The only way to truly assure confidentiality is to use encryption so that the communication service has no access to the content. Despite considerable evidence of and front-page reporting about content breaches [3, 5, 9, 21, 24], encryption has generally not been widely adopted for person-to-person communications such as email and chat [20].

Researchers have given considerable thought to the reasons for this lack of adoption. More than 15 years of research have identified major usability problems with encryption tools, ranging from poorly designed user interfaces to the fundamental challenges of safe and scalable key distribution [16, 33, 35, 43].

Symposium on Usable Privacy and Security (SOUPS) 2016, June 22–24, 2016, Denver, Colorado.

Recently, however, progress toward better usability and thus wider adoption has been made. Apple applied seamless end-to-end encryption to its iMessage and FaceTime services [2,25]. By centrally distributing public keys, Apple ensures the encryption is transparent to users, bringing end-to-end encryption to millions of iPhone, iPad, and Mac users. This design, however, leaves open the possibility that Apple itself could carry out a man-in-the-middle attack to break its users' privacy, for example at the request of law enforcement authorities [8, 42]. Popular messaging app WhatsApp has also implemented end-to-end encryption for text, voice, and video communications [27]. As with iMessage, WhatsApp centrally distributes public keys; however, users can optionally verify each other's keys manually or via QR code. Google and Yahoo! are currently developing similar approaches, with an added monitoring protocol that allows users and third parties to audit the key directory for consistency and transparency [19, 30, 37]. Some privacy experts have suggested that given this potential man-in-the-middle attack, these services should not be recommended to end users. As just one example, one security researcher suggests that "iMessage remains perhaps the best usable covert communication channel available today if your adversary can't compromise Apple. ... If one desires confidentiality, I think the only role for iMessage is instructing someone how to use Signal[1]" [42].

In a sense, the issue comes down to whether the benefit from many more people adopting encrypted communications is outweighed by the reduced security inherent in the central key distribution model. While security experts are best positioned to understand the technical differences between models, end users will ultimately be faced with the choice of which platforms and products to install and use. Researchers have considered the needs of some highly privacy-sensitive users, such as journalists and activists [18, 28]. To our knowledge, however, no one has asked average users for their opinions about these tradeoffs. This means that although security researchers may understand the risks and benefits of different tools, as a community we do not understand how an average user will weight different factors in deciding whether to adopt or ignore various encrypted communication technologies.

To understand how non-expert users feel about these tradeoffs, we undertook a 52-person lab study. We introduced participants to two encryption models: an *exchange* model in which participants manually exchange keys (analogous to traditional PGP) and a *registration* model in which participants sign up with a central service that distributes keys (analogous to iMessage). For each model, we asked them to complete several encrypted communication tasks; we also gave them a short, high-level explanation of each model's

[1]An encryption tool: https://whispersystems.org/. Last accessed on 05/16/2016.

security properties. (We varied the order of presentation to account for biases.) We then asked participants to comment on the security and usability of each model, as well as their overall opinion of the tradeoffs involved. The experiment was designed, insofar as possible, to avoid comparisons based on user-interface design and focus instead on the underlying properties of each encryption model.

We found that participants understood the two models fairly well and expressed nuanced insights into the tradeoffs between them. As predicted, participants found the registration model considerably more convenient than the exchange model. More interestingly, while the exchange system was considered more secure overall, the difference was slight: both general trust that large email providers would not risk their reputations by cheating and reasonable concerns about participants' own ability to correctly implement the exchange model mitigated this difference. Separately, we asked about half of our participants to evaluate the auditing model proposed in CONIKS [29], which is similar to that in development by Google and Yahoo!, and we found that for many users it provides a meaningful additional degree of confidence in the registration model's privacy.

Overall, our results suggest that users recognize the benefit of the exchange model for very sensitive communications, but find the more-usable registration model sufficient for the majority of everyday communications they engage in. While there are risks to this model, some of which can be alleviated by auditing, we argue that the marginal benefit of broad adoption will outweigh these risks. Historically, encryption schemes that require significant user effort have never gained broad popularity. Trying to convince average users to exclusively use more complicated schemes, when they often don't see a need for the added protection, may instead keep them away from using any encryption at all. Rather than spreading undue alarm about the risks of registration models, or forcing users into only exchange models, we recommend that policymakers and designers present tradeoffs clearly and encourage adoption of usable but imperfect security for the many scenarios where it may be appropriate.

2. BACKGROUND AND RELATED WORK

We briefly discuss the history of public-key-encrypted email systems and encryption usability studies.

2.1 A brief history of encrypted email

Diffie and Hellman proposed public-key cryptography in 1976, suggesting that a public directory would allow anyone to send private messages to anyone else; in 1978, the RSA algorithm made the idea practical [11]. In 1991, John Zimmerman developed PGP, which supported sending public-key encrypted email. In the second version, to alleviate the key verification problem, he proposed a "web of confidence" (later known as web of trust) for establishing key authenticity [44]. In a web of trust, users can sign each others' keys to endorse their authenticity, and can choose to accept keys that come with signatures from "trusted introducers." Despite this, key verification has remained problematic for many years.

In 1999, RFC 2633 defined Secure/Multipurpose Internet Mail Extensions (S/MIME), which takes a centralized approach to key distribution: all users have public-key certificates signed by a certification authority (CA), which are distributed along with any signed emails sent by that user [31]. S/MIME allowed straightforward integration of encryption to email clients like Microsoft Outlook and Netscape Communicator and was adopted by some corporate organizations with the capability to manage keys hierarchically, but was not adopted broadly by consumers.

More recently, several researchers and companies have explored ways to split the difference between completely decentralized and completely centralized key management. Gutmann proposed applying *key continuity management*, in which keys are trusted on first use but key changes are detected, to email [22]. In Apple's iMessage, private keys are generated on users' devices and the corresponding public keys are uploaded to Apple's proprietary directory service. To send a message to a user with multiple devices, the message is encrypted once for each device [1, 25]. WhatsApp uses a related approach based on the Signal Protocol, but allows users to confirm the authenticity of each other's keys if they choose to [27]. A recently reported vulnerability in the iMessage encryption mechanism points to the importance of validating the security of any end-to-end-messaging system [17]; however, this is orthogonal to our consideration of the underlying key exchange model.

In *certificate transparency*, publicly auditable append-only logs can be used to determine whether rogue certificates have been signed using a stolen CA key [26]. Ryan extended this approach for end-to-end email encryption [34]. CONIKS extends certificate transparency to allow users to efficiently monitor their own key entries and to support privacy in the key directory [29]. Google and Yahoo! are adopting a variation of certificate transparency for their end-to-end encryption extension [19, 30]. Each of these approaches trades off a different amount of security for convenience.

Other researchers have considered alternatives to standard public-key encryption that are designed to be more usable. Fahl et al. proposed Confidentiality as a Service (CaaS) [13], which operates on a registration model mostly transparent to users. This approach uses symmetric cryptography and splits trust between the communications provider and the CaaS provider. Neither individually can read private messages, but if the two collude they can.

2.2 The usability of encrypted email

In 1999, Whitten and Tygar published the now-seminal *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0* [43]. This paper evaluated the interface for PGP 5.0 and found that most users (two-thirds) were unable to successfully sign and encrypt an email in the 90 minute session. This led to a series of follow-on papers: evaluating PGP 9 (key certification is still a problem) [35], S/MIME and Outlook integration (KCM seems promising) [16], Facebook encryption (using CaaS) [14], and several others (e.g., [33,39]). These studies largely ask users to do tasks they are unfamiliar with and focus on success rates (key pairs generation and collection, sending and decrypting messages, etc.). They provide valuable insight into how effectively novices can learn a particular system, how specific user interface design choices impact users, and where the difficulties lie. However, users are rarely presented with multiple potential encryption infrastructure models. Ruoti et al. compared the usability of three email encryption systems using pairs of novice users [32], but this work did not consider the security tradeoffs of the systems users were evaluating.

Tong et al. re-evaluated the test of *Johnny* with a different set of terms and documentation, including using a lock-and-key metaphor for public and private keys [40]. In preliminary results, they found that the metaphors aided understanding. We adopt the lock metaphor in our study, as detailed below.

Researchers have also studied social and cultural norms that also lead to aversion to encryption. Often users believe that they have no reason to encrypt their email because they have "nothing to hide," or because they cannot imagine anyone being interested in the messages they are sending [36]. In an interview study at an unnamed

non-violent, direct-action organization (which one might expect to be more interested and aware of the benefits of encryption), Gaw et al. found that employees believed "routine use of encryption [was] paranoid [behavior]" [18]. In this work, we do not directly address social norms regarding encryption, but several participants did discuss paranoia and suggested using different systems to accommodate different levels of privacy concern.

McGregor et al. considered the specific security and encryption needs of journalists protecting confidential sources, finding that adoption is frequently driven by source preferences and that existing models do not meet some important journalistic needs, such as verifying the authenticity of sources [28]. Considering the needs and preferences of users with critical privacy sensitivity, such as activists and journalists, is an important topic, but is orthogonal to our emphasis on general users.

3. METHODOLOGY

We used a within-subjects lab study to examine participants' concerns and preferences regarding the usability and security of end-to-end email encryption. Each participant was introduced to two general models for key management, *exchange* and *registration*. For both models, we described a public key as a *public lock*. This approach, inspired by Tong et al., avoids overloading the term "key" and was used to provide a more intuitive understanding of how public-key pairs operate [40].

In the exchange model, similar to traditional PGP, participants generate a key pair and then distribute the public locks to people they want to communicate with. We offered participants several methods for exchanging locks: the same email account they would use for encrypted communication, a secondary email account, posting the public lock on Facebook or sending via Facebook Messages, or using a simulated "key server" to upload their lock to a public directory. (These options were presented to each participant in a random order.) Simulated correspondents (played during the study by a researcher) sent back their own public locks via the same mechanism the participant chose, or via the mechanism the participant requested.

In the registration model, participants again generate a key pair. In this case, they "register" their public lock with a simulated key directory service; correspondents' locks were pre-installed to simulate automatically retrieving them from the directory. Participants were thus able to send and receive encrypted email from all simulated correspondents immediately upon creating and registering their own keys. In iMessage, the key generation step itself is completely transparent to users, who may never realize a key was created; we chose instead to make key generation explicit to help users understand the process.

Within each model, participants were asked to complete a series of simulated tasks, such as exchanging encrypted emails in a role-playing scenario (see details below); they were also introduced to a brief, non-technical review of the security properties of each model. Participants were asked to give their opinions about each model immediately after completing the tasks and security learning for that model. We also conducted an exit interview regarding the overall usability and security of each model, whether participants would use it themselves or recommend it to others, and in what circumstances it might or might not be appropriate.

We chose a within-subjects study because we were primarily interested in how participants would understand and value the tradeoffs among the options. As shown in Table 1, we varied the order of activities to account for ordering effects. Participants were assigned round-robin to one of these four possible orders of activities.

First activity	Second	Third	Fourth
ET (Exchange, Tasks)	ES	RT	RS
ES (Exchange, Security learning)	ET	RS	RT
RT (Registration, Tasks)	RS	ET	ES
RS (Registration, Security learning)	RT	ES	ET

Table 1: The order of activities varied across participants. Each participant worked with either the Exchange (E) or the Registration (R) model first. Within each model, participants either completed the encryption Tasks (T) first or learned about Security properties (S) first. Throughout the paper, participants are labeled by first activity; e.g., participant RT3 completed encryption tasks for the registration model first.

3.1 Encryption tasks

The set of encryption-related tasks for each model is shown in Table 2. In both models, participants were asked to generate a key pair locally. In the exchange model, participants then exchanged public locks with simulated friend Alice, including both sending Alice their lock and importing the lock received in return. In the registration model, participants registered with a simulated central service and had their public lock automatically "uploaded" and others' locks automatically "imported." After the locks were exchanged or the participant registered, participants composed and sent an encrypted email to Alice. A researcher, posing as Alice, sent an encrypted response. As a slightly more complex task, participants were asked to send an encrypted email to a group of two recipients. This task was designed to get participants to consider how the two models scale. Finally, we asked participants to consider how they would handle several other situations, including communicating with larger groups of people and various possible errors related to losing or publicizing one's own private key or losing other users' public locks. The possible errors were specific to each model and are shown in Table 2. In the interest of simplicity, we did not include any email signing (or signature verification) tasks.

Encryption tasks were completed using a Gmail account created especially for the study and a Chrome browser extension based on Mailvelope.[2] We modified Mailvelope to remove its branding, change the labels to match our lock/key metaphor, and reduce the interface to include only those features relevant to the study tasks. Figure 1, right shows a screenshot of sending encrypted email with our extension. As in Mailvelope, users of our extension compose an email and then use an "Encrypt" button to select recipients. Upon receiving encrypted email, users are prompted to enter their password to decrypt it (with the option to save the password and avoid future prompting).

We created two versions of our extension, one for exchange and one for registration, taking care to make them as similar as possible. The only two visible differences were (1) changing the "Generate lock/key pair" menu item and subsequent screen (exchange model, Figure 1, left) to read "Register" (registration model) and (2) a lock import screen (Figure 1, center) that was only relevant in the exchange model.

We also provided participants with detailed instructions to help them use the Chrome extension. By simplifying the interface, keeping it consistent, and providing detailed instructions, we hoped participants' reactions would better reflect the inherent properties of

[2]https://www.mailvelope.com/. Last accessed on 05/16/2016.

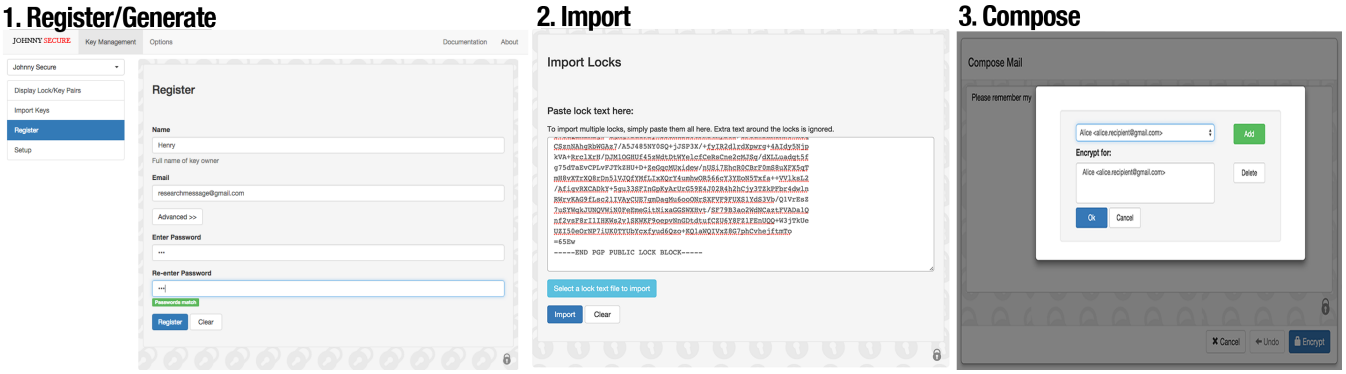


Figure 1: To use our extension, participants first generated (or registered) a key pair. Participants using the exchange model then needed to import recipients' locks. Finally, when composing encrypted emails, they clicked the Encrypt button (shown in the lower right of Step 3) to bring up a modal dialog to select recipients.

Task #	Exchange Model	Registration Model
1	Generate public lock/private key pair	Register public lock/private key pair
2	Exchange public locks with Alice	N/A
3	Send encrypted email to Alice	Send encrypted email to Alice
4	Decrypt received email from Alice	Decrypt received email from Alice
5	Exchange public locks with Bob and Carl	N/A
6	Send encrypted email to Bob and Carl	Send encrypted email to Bob and Carl
7	Decrypt received email from Bob and Carl	Decrypt received email from Bob and Carl
8	Imagine sending encrypted email to 10 people.	Imagine sending encrypted email to 10 people.
9	Consider misconfigurations: a. Lose Alice's public lock b. Lose own private key c. Publicize own private key	Consider misconfigurations: N/A b. Lose own private key c. Publicize own private key

Table 2: The encryption-related tasks completed by participants. The tasks differed slightly in the two models.

each model rather than idiosyncrasies of a particular interface.

3.2 Description of security properties

We provided participants with short, non-technical descriptions of possible attacks on each model.

Exchange model

For the exchange model, we described a man-in-the-middle attack in which the attacker could intercept or replace keys during the exchange process: "For example, when you try to get the public lock from Dave, the attacker secretly switches the public lock to his own. You think you have Dave's public lock, but in fact you have the attacker's. ... As a result, the attacker can read your email. The attacker will then use Dave's public lock and send the encrypted email to Dave, so that neither you nor Dave realize the email has been read." We also showed participants the illustration in Figure 2.

We decided not to include an option for key signing in our exchange model both because we thought it would add unnecessary complexity to our explanations and because it does not change the underlying requirement to trust some keys that are manually exchanged.

Registration model

For the registration model, we primarily described a man-in-the-middle attack enabled by the key directory service: "When you try to send encrypted emails to Dave, you think the database will return Dave's public lock to you. But in fact, it returns the attacker's lock, so the attacker can read your email. Therefore, you need to trust the email provider in this system." We showed participants the illustration in Figure 3.

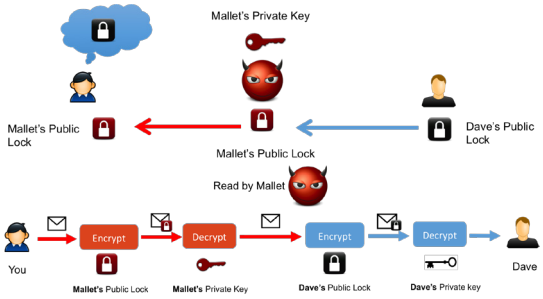


Figure 2: Possible attacks on the exchange model

In addition, we described two variations on the basic key directory approach: the Confidentiality as a Service (CaaS) variation [13,14], and an auditing model similar to the one proposed by Google and CONIKS [19, 29]. Because these approaches are not currently in wide use the way the iMessage-analogous system is, they were treated as secondary options. The auditing model was added (to the end of the interview, to maintain consistency with earlier interviews) during recruiting, and was therefore presented only to 24

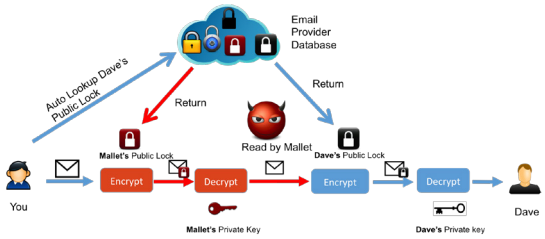


Figure 3: Possible attacks on the registration model

participants.

The security of the CaaS variation was described as follows: “There is a third-party service (not the email provider) as an intermediary. In this version, neither the third-party service nor your email provider can read your email themselves. However, if your email provider and the third-party service collaborate, they can both read your email. Therefore, you need to trust that the two services are not collaborating."

We described the auditing variation as follows: “The email provider stores all users’ public locks, just like [the primary registration model]. But there are other parties (auditors) who audit the email provider, to ensure it is giving out correct public locks. These auditors may include other email providers, public interest groups, and software on your devices. If the email provider gives you a public lock that doesn’t belong to the recipient, or gives someone else the wrong public lock for you, these auditors will notify you. You (or someone else) may use the wrong lock temporarily (for an hour or a day) before you are notified. In this model, you don’t need to trust your email provider, but you need to trust the auditors and/or the software on your device. Because there are several auditors, even if one auditor does not alert you another one probably will."

3.3 Participant feedback

Participants were asked questions after completing tasks for each model and at the end of the process. After completing tasks and learning about security for each model, participants were asked for their agreement (on a five-point Likert scale) with the following statements:

- The task was difficult (for each task).
- The task was cumbersome (for each task).
- The system effectively protected my privacy.

The first two questions were repeated for each task in Table 2. Before answering, participants were reminded that difficult tasks would require intellectual effort or skill, while cumbersome tasks would be tedious or time-consuming. After each Likert question, we asked participants to briefly explain their answer choice (free response).

After completing all tasks and learning about all security models, participants were asked several summative questions, including:

- Willingness to use each system, on a five-point Likert scale, and why.
- Willingness to recommend each system, on a five-point Likert scale, and why.
- What the participant liked and disliked about each system.

3.4 Recruitment

We recruited participants 18 or older who were familiar with Gmail and Chrome and who send and receive email at least 3 times per week. We placed flyers around our university campus and the surrounding area, advertised via email listservs for the university, and advertised on web platforms like Craigslist. All interviews were conducted in person at our university campus; interviews were video recorded with the explicit consent of participants. Participants were paid $20 for a one-hour study and were reimbursed for parking if utilized. Our study protocol was approved by the university’s Institutional Review Board.

Participants took part in the study in multiple batches between August 4, 2015 and Feb 5, 2016. For context, all of the participants engaged in the study well after Edward Snowden revealed details of the National Security Agency’s broad surveillance of digital communications [12], but before Apple publicly fought the Federal Bureau of Investigation to not weaken the security of a locked and encrypted iPhone [4]. We include this to note that average users’ views of security, privacy, and here specifically, encryption are a moving target. Future events may continue to shift public opinion on the importance of encrypted communications.

3.5 Data analysis

We used statistical analysis to investigate participants’ responses to the exchange and registration models. To account for our within-subjects design, we used the standard technique of including random effects to group together responses from each participant. We used a cumulative-link (logit) mixed regression model (CLMM), which fits ordinal dependent variables like the Likert scores we analyzed [23]. We included three covariates: whether the participant performed tasks or learned about security first, whether the encryption model she was evaluating was seen first or second, and the encryption model itself (exchange or registration). This approach allows us to disentangle the ordering effects from the main effects we are interested in. For each encryption model, we tested regression models with and without the obvious potential interaction of encryption type with order of exposure to that type, selecting the regression model with the lower Akaike information criterion (AIC) [6].

Qualitative data was independently coded by two researchers using textual microanalysis [38]. After several iterative rounds of developing a coding scheme, the researchers each independently coded the full set of participant responses, with multiple codes allowed per response. The researchers originally agreed on more than 94% of the codes, then discussed the instances of disagreement until consensus was reached. Where appropriate, we report prevalence for the final qualitative codes to provide context.

3.6 Limitations

Our methodology has several limitations. Our lab study participants had only limited exposure to the different encryption models, and their opinions might change after working with the models for a longer period. Participants also only imagined their responses to misconfigurations, rather than actually handling them. Nonetheless, we argue that first impressions like the ones we collected influence whether people will try any tool for long enough to develop more-informed opinions. It is well known that study participants may rate tools they examine more favorably (acquiescence bias) [41], which may explain the high rate of participants reporting they wanted to use or recommend each model. Because we are primarily interested in comparing results between models, we believe this has limited impact on our overall results; however, the absolute ratings should be interpreted as a ceiling at best.

In order to provide participants with any understanding of the security properties of each model, we had to prime them with descriptions of possible attacks. While this priming was unavoidable, we endeavored to keep the security descriptions as neutral as possible so that priming would affect both models approximately equally.

To avoid overwhelming participants, we evaluated a limited subset of possible encryption models and possible tasks; in particular, we left out key signing as well as any email signing or signature verification tasks. We did this because we believe signing to be the most difficult aspect of cryptography for non-experts to understand (see e.g., [43]), but including it might have provided a broader spectrum of user opinions.

Our registration model, unlike for example iMessage, was not completely invisible to participants. We believe it was necessary to give participants something to do other than just sending a normal email, in order to help them think through the tradeoffs involved. While presumably using a fully transparent variation would only have increased the convenience gap between the two models, prior work indicates that taking any steps at all increases feelings of security [33]. This may have contributed to the small observed security gap between the two models, but we argue that a version with no intervention required would lead to underestimations of security. Because we added the auditing model late, we were not able to get as much feedback about it or to compare it quantitatively to the other models we examined. In addition, because all participants encountered it last, their responses may reflect some ordering effects. Nonetheless, we believe the qualitative data we collected does provide interesting insights. Future work can examine all these alternatives in more detail.

As with many lab studies, our participants do not perfectly reflect the general population, which may limit the generalizability of our results.

4. PARTICIPANTS

A total of 96 people completed our pre-screening survey. We interviewed the first 55 who qualified and scheduled appointments. Three participants were excluded for failing to understand or respond coherently to any directions or questions.

Demographics for the 52 participants we consider are shown in Table 3. Among them, 60% were male and 80% are between the ages of 18-34, which is somewhat maler and younger than the general American population. Almost 85% of participants reported "primarily" growing up in the United States, South Asia, or East Asia. 40% of participants reported jobs or majors in computing, math, or engineering.

Despite this high rate of technical participants, most had little experience with computer security. We measured security expertise using a slightly adapted version of the scale developed by Camp et al. [7]. Higher scores indicate security expertise; the maximum score is 5.5 and the minimum score is zero. Only two of our participants scored 3 or higher.

Using a Kruskal-Wallis omnibus test, we found no significant differences among our four conditions in age, gender, country of origin, or security expertise ($p > 0.05$).

ID	Gend.	Age	Occupation	Security Expertise	Where grew up
ET1	F	25-34	Other	0	United States
ET2	F	45-54	Education	0.5	United States
ET3	M	21-24	Education	1.5	United States
ET4	M	25-34	Education	2	Middle East
ET5	M	21-24	Computers/math	1	South Asia
ET6	M	25-34	Engineering	2	East Asia
ET7	M	45-54	Life Sciences	2	United States
ET8*	M	18-21	Engineering	0.5	East Asia
ET9*	F	21-24	Computers/math	1	South Asia
ET10*	F	35-44	Computers/math	2	United States
ET11*	M	35-44	Transportation	0.5	United States
ET12*	M	21-24	HealthCare	1.5	United States
ET13*	M	21-24	Social Service	0.5	Western Europe
ES1	M	35-44	Engineering	0	United States
ES2	M	21-24	Sales	0.5	United States
ES3	F	25-34	Health Care	0.5	United States
ES4	M	21-24	Computers/math	4	South Asia
ES5	M	21-24	Computers/math	1	East Asia
ES6	M	25-34	Computers/math	1.5	South Asia
ES7	F	21-24	Education	0.5	United States
ES8*	M	25-34	Engineering	0.5	East Asia
ES9*	F	21-24	Engineering	1	South Asia
ES10*	M	25-34	Engineering	1	United States
ES11*	F	45-54	Business	0.5	United States
ES12*	F	21-24	Communications	0	United States
ES13*	F	25-34	Education	0.5	Latin America
RT1	M	25-34	Computers/math	3	East Asia
RT2	F	25-34	Sales	0.5	United States
RT3	M	21-24	Engineering	2.5	South Asia
RT4	F	21-24	Engineering	1.5	United States
RT5	M	21-24	Business	2	East Asia
RT6	F	25-34	Other	1.5	United States
RT7	F	25-34	Health Care	0	United States
RT8*	F	18-20	Sales	0.5	United States
RT9*	M	18-20	Education	0.5	United States
RT10*	M	25-34	Engineering	2	Middle East
RT11*	F	35-44	Admin. Support	0.5	United States
RT12*	M	35-44	Admin. Support	0.5	United States
RT13*	M	21-24	Production	0	United States
RS1	M	21-24	Other	1	East Asia
RS2	M	25-34	Life Sciences	1.5	Middle East
RS3	M	21-24	Computers/math	0	Africa
RS4	M	21-24	Computers/math	0.5	South Asia
RS5	M	25-34	Life Sciences	2	Middle East
RS6	M	25-34	Other	0.5	United States
RS7	F	25-34	Health Care	0	United States
RS8*	F	45-54	Sales	0	United States
RS9*	F	25-34	Engineering	1.5	East Asia
RS10*	M	21-24	Engineering	1	United States
RS11*	M	25-34	Architecture	0.5	United States
RS12*	F	25-34	Life Sciences	0.5	United States
RS13*	M	25-34	Construction	0	United States

Table 3: Participant Demographics. The columns show: participant identifiers (coded by activity order), gender, age, occupation, security expertise, and place where the participant grew up. The * indicates participants who were exposed to the auditing model.

5. RESULTS AND ANALYSIS

We present participants' reactions to the convenience and security of each model, followed by a discussion of their overall preferences among the models.

5.1 Registration is more convenient

Unsurprisingly, our participants found the registration system considerably more convenient, rating the exchange system as significantly more cumbersome and more difficult. Figure 4 and Tables 4 and 5 show the results of the CLMM for cumbersome and difficult, respectively, for Task 8: imagining sending email to a group of 10 people. In reading the CLMM tables, the exponent of the coefficient indicates how much more or less likely participants were to move up one step on the Likert scale of agreement.

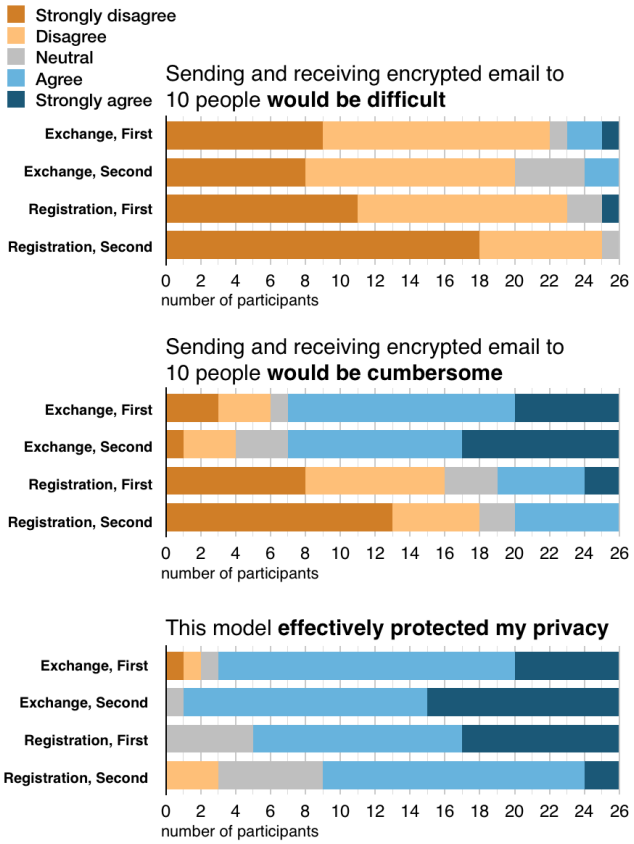


Figure 4: Participants' ratings of difficulty and cumbersomeness (Task 8) as well as whether participants thought the model protected their privacy. Labels indicate which model participants evaluated along with whether they saw that model first or second; e.g., "Exchange, First" indicates ratings for the exchange model among those who saw it first, which includes ET and ES participants.

For cumbersomeness the exchange model was associated with almost a 20x increase in likelihood of indicating more agreement. The exchange model was also about 5x more likely to be perceived as more difficult.

Factor	Coef.	Exp(coef)	SE	p-value
tasks first	0.010	1.010	0.589	0.986
second model	-0.166	0.847	0.393	0.673
exchange	2.978	19.656	0.567	<0.001*

Table 4: Regression table for cumbersomeness, Task 8. The non-interaction model was selected. Non-significant values are greyed out; significant values are indicated with an asterisk.

Factor	Coef.	Exp(coef)	SE	p-value
tasks first	-0.282	0.754	0.747	0.706
second model	-0.726	0.484	0.460	0.115
exchange	1.674	5.333	0.520	0.001*

Table 5: Regression table for difficulty, Task 8. The non-interaction model was selected. Non-significant values are greyed out; significant values are indicated with an asterisk.

Participants' comments generally supported this finding: that the exchange model was dramatically more cumbersome and somewhat more difficult. Within the exchange model, the most tedious task was manually exchanging locks and the most commonly mentioned reason was waiting for a correspondent's public lock. ES9 was concerned that the exchange model was "time-consuming, especially sending urgent emails. I have no choice but to wait for" the correspondent's public lock. RS5 agreed, saying "There are so many steps to exchange locks." RS13 mentioned that the cumbersomeness of exchanging locks was mainly related to initialization: "If their locks are already there, it would not be cumbersome. But if I have to ask them to send me locks person by person, it's more cumbersome." One participant (ET10) worried it would be additionally cumbersome to use the exchange model on a phone.

Several participants expressed concern that users with low digital literacy might have trouble with the exchange model or prefer the registration model. For example, RS12 recommended the registration model "especially to people that don't know very well how to use a computer . . . old people, like my father." ET2 agreed that the registration model is "easy to teach others to use."

While few participants considered any of the tasks very difficult, choosing a mechanism for exchanging locks was considered the most difficult step by a few participants, such as RS4, who mentioned having to "think about a safe way to exchange public locks," and RS10, who was concerned about making an exchange error while multitasking.

Other concerns related to the general issue of convenience included scalability and misconfiguration. As RT9 said, "When I send to more people, I have to be very careful, especially when I choose to send them my public locks separately. I need to control every step is correct." ET13 said, "When I exchange locks with ten people, I can send my lock, which is kind of easy. But I have to get ten replies for their locks. I can easily get lost. And if I exchange with 100 people, it'll be a nightmare." A few participants were concerned about the difficulty of recovering from misconfiguration, and ET10 was particularly worried that others' mistakes could cause additional hassle for her: "If other people lose their private keys and send me new public locks, I will be overwhelmed." RS12 agreed that "if accidents or mistakes happen, it bothers both parties to do extra steps."

The inconvenience of the exchange model could potentially be mitigated somewhat by posting the key publicly or semi-publicly (on a key server or Facebook profile), rather than sending it individually to different recipients. About a third of our participants chose this option: 34 used the primary email, 20 used the secondary email, 10 used Facebook chat, five posted to the Facebook profile, and 13 used the key server. (Some participants chose multiple methods during different tasks.) However, few of the participants who used the public or semi-public methods mentioned the added convenience as a reason for their choice. RT12 said exchanging locks is "not too cumbersome, it's manageable through the lock server to exchange locks". On the other hand, a few participants chose the key server because they thought it was more secure than other choices we provided.

5.2 The perceived security gap is small

We found that participants understood and thought critically about the security properties we explained to them for each model. Surprisingly, they found the exchange model to be only marginally more secure than the registration model, for a variety of reasons.

Exchange: Manual effort may lead to vulnerability

Most participants believed the exchange model was most secure overall, with 48 (out of 52, 92.3%) agreeing or strongly agreeing that this model protected their privacy. Nonetheless, participants also expressed concern that managing key exchange themselves would create vulnerabilities. More than half (27 out of 52) of participants were concerned about the security of the medium used to exchange locks.—ET4 worried that 'the key server [could] be manipulated or compromised." RT7 had several such concerns, including that an attacker could break into her Facebook account to post an incorrect public lock, or that public Wi-Fi in a coffee shop could be unsafe for transmitting locks. Overall, she said, "There are too many exchanges between different people. Exchanging [locks] to many people may go wrong." Others, like RS5, worried that their internet service provider could "sit between my recipient and me" and switch locks to execute a man-in-the-middle attack. ET7 was one of several participants who noted that "If I send the public locks and encrypted emails using the same email provider, it's not very secure." RT9 thought the ability to choose from different mechanisms to exchange locks provided added security, but worried that "people may choose a particular way in real life. It's their habits, so that attackers may anticipate" their choices and take advantage of their known routine. ES10 asked his recipients to send back his public lock, both through Facebook and via email, so he could verify for himself that the received public locks were not altered.

Other participants were concerned about making a mistake during the ongoing responsibility of managing keys. As ET10 put it, "Every time when I send or get a public lock ... there is a probability, even though not high, that my privacy is compromised. Then when I exchange public locks with many people, this probability will increase exponentially." RS12 worried that "I don't know what I actually need to do when I lose or publicize my private key. I am not confident about my answers. Non-tech experts may make mistakes."

Other participants mentioned that careless or compromised users could ruin the security of a whole group. ES12 said, "If I send to Alice, and she decrypts and goes away, then other people can see the email or even copy that email." ET8 said that "Within a company, if one person is hacked, then the whole company is hacked. It's hard to track the source, just like rotten food in the refrigerator." ET4 agreed that "There can be attacks on users with weak security, which may impair the whole user system."

Registration: Some concern but generally trusted

As expected, many participants were concerned about the need to trust email providers in the registration model. As ES5 said, having the email provider store "all public locks ... is not very comfortable." Despite this, however, most participants (38 out of 52) trusted the system protecting their privacy. Also, the CLMM results in Table 6 and Figure 4 indicate that the order in which the models were introduced played a significant role. Participants who saw the registration model first were more comfortable with it: 9 of 26 who saw registration first strongly agreed that the model protected their privacy, compared to only 3 of 26 who had already heard about the more-secure exchange model. None of the participants who saw registration first disagreed that the model protected their privacy, while 3 did so after seeing the exchange model first.

This general confidence in the registration model reflects many participants' belief that even though email providers could compromise the security of the primary registration model, they would be unlikely to. Ten participants mentioned that they trust their own email provider (presumably if they didn't they would switch services). ET11 mentioned that his email provider "knows me, I have my name there," and ET12 said that "All public locks are stored in a database, and I trust the database. This database provides extra security." ET13 provided a slightly different view: that some email providers are untrustworthy in well-known ways. "Everyone knows the Gmail potential vulnerabilities. And some people who are particularly hiding some information from the U.S. government, they will choose Yandex email from Russia, because they'd rather be intercepted by the Russian government, instead of the U.S. government. ... If you are an activist in US, and you don't want the U.S. government to know what you are up to, so I will choose some email services I feel comfortable with."

Several (7 participants) were specific about which kind of providers they would trust: RT8 would trust "certain big companies, not small companies," because big companies must protect their reputations. RT10 felt similarly, with an important caveat, mentioning that big companies like "Google and Yahoo! don't do such things [violate users' privacy] usually, unless the government forces them to do so. In general, it's secure." ET11 would choose an email provider with many users since "the more people using it, the more reliable." RT2, on the other hand, preferred to trust institutions like universities that "own their own email server" to better protect her privacy.

Also contributing to the general comfort level with the registration model is that participants do not believe most or any of their communication requires high security. RT4 said "encryption is not necessary for me," and RS8 agreed, saying "If I have some private information, I won't put it on the Internet."

CaaS and auditing: Some additional perceived security for registration

Twenty-two participants preferred the CaaS variation to the primary registration model, and 12 preferred the primary model to CaaS; the rest rated the two variations the same. The most popular explanation for preferring CaaS was a belief that different companies would not collude. RS7 said that the two parties would not collude because they do not "even trust each other." ES12 was cautiously positive, saying "This separation makes me feel good. However, [the two parties] still can possibly collaborate." Relatedly, ES8 suggested that the CaaS approach was more secure because "If one party is screwed up, you have another one to protect [your email]. You are still safe." These comments have implications for the auditing model as well; belief that different parties are unlikely to collude and recognition that distributing trust spreads out possible points of failure would also point to more trust in the auditing model.

On the other hand, four users thought the primary registration model was more secure than the CaaS variation because adding more intermediate systems and providers reduces overall security. RS1,

Factor	Coef.	Exp(coef)	SE	p-value
tasks first	-0.332	0.717	0.527	0.528
second model	-1.684	0.186	0.699	0.016*
exchange	-0.288	0.750	0.670	0.668
second model :: exchange	2.818	16.740	1.124	0.012*

Table 6: Regression table for privacy. The interaction model was selected. Non-significant values are greyed out; significant values are indicated with an asterisk.

for example, said that "involving more systems may complicate the system, so it is less trustful." A few users said that the possibility of collaboration invalidates the entire model: for example, ES13 said "I don't trust that much the whole system. I am afraid they may collaborate." Two participants (ET4, RS13) were afraid that in CaaS the two parties might collaborate for a sufficiently large gain. For example, RS13 said "They will not collaborate for one or two person's email, but for many, a group of people."

Other participants were concerned about whether the third party in CaaS was trustworthy. ET11 worried that "the third party service is not verified," and RT9 said his opinion "depends on who the two entities are. If the two companies are big names, like Gmail and Facebook, it seem more secure. Also if they do different types of services [from each other], it's more secure."

The 24 participants who were briefly exposed to the auditing variation gave generally positive feedback. ES9 was happy that "somebody is supervising" lock distribution and watching for problems, and ET13 said "Obviously it's extra secure. Other parties are verifying it, like an anti-virus system telling me if something goes wrong." ET8 appreciated that "if something goes wrong, I will be notified." The presence of many auditors reassured participants that collusion was unlikely; for example, RT10 commented that "it's less likely that all auditors [would] do something bad," and RS12 appreciated that "there are many auditors who can notify me."

Several participants, however, were concerned about the reliability of the auditors: RS9 said, "I want to know who these auditors are, ... their reputations, and whether they are truly independent." Similarly, RT13 said, "Am I able to choose auditors? This is a big question. The principle is good ... but I want to know who they are and how to choose them, because I need to trust them." One user (ET10) was concerned that auditors from competing companies might have incentives to lie about each others' behavior, making it hard to know who to trust. According to ET11, involving more parties reduced the overall trustworthiness: "Putting trust to only one party is better."

Ten participants expressed concern about the time lag for notification, noting that "a lot emails have already been sent" with even an hour's delay (ES10). RT11 said "It should be immediate notification. Even an hour is too late. ... Something bad has already happened." Others, however, were more pragmatic: "Immediate notification is ideal, but I don't expect immediateness in reality" (RT9). ET13 said the time lag "is a vulnerability. It depends on how often I send encrypted emails. If I use it very often, then it's vulnerable." Similarly, RT12 pointed out that "If I don't send the email, it doesn't matter, but in this case, I don't receive the wrong locks. ... Notification happens after the fact that I already received the wrong lock."

5.3 Overall comparison between systems

After exposing them to both models, we asked participants whether they would use or recommend the exchange model, the primary registration model, or the CaaS registration model. Figure 5 shows that the exchange model and CaaS variation were slightly preferred to the primary registration model. The number of participants who agreed or strongly agreed to use or recommend each model were 27, 23, and 28 (use) and 29, 21, and 28 (recommend). The CLMM results (Tables 7 and 8), which take the exchange model as a baseline, show no significant difference between exchange and either variation of registration for would-use, but do show that the primary registration was recommended less frequently than the exchange model. The 95% confidence intervals for each model indicate no

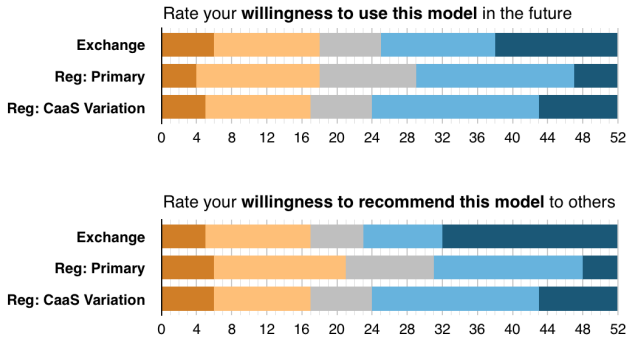


Figure 5: Participants' ratings of whether they would use or recommend each model.

significant differences between the primary and CaaS registration models in either case.

The regression models also indicate that participants who completed the encryption tasks before hearing about security properties were less likely to use or recommend any model than those who heard about security properties first. We hypothesize that participants who used the encryption extension before hearing about security anchored on the inconvenience of the tool rather than its privacy benefits. While this does not provide useful insight about comparing the different systems, it does underline the need for careful consideration about how new encryption tools are presented to the public.

Factor	Coef.	Exp(coef)	SE	*p*-value
tasks first	-0.606	0.546	0.308	0.049*
second model	-0.026	0. 975	0.291	0.930
registration (primary)	-0.376	0.687	0.358	0.294
registration (CaaS)	-0.077	0.926	0.360	0.823

Table 7: Regression table for whether participants would use each model. The non-interaction model was selected. Exchange is the base case for model type. Only whether participants completed tasks first or heard about security first was significant.

Factor	Coef.	Exp(coef)	SE	*p*-value
tasks first	-0.678	0.508	0.303	0.025*
second model	-0.198	0.820	0.291	0.496
registration (primary)	-0.915	0.401	0.368	0.013*
registration (CaaS)	-0.490	0.613	0.366	0.180

Table 8: Regression table for whether participants would recommend each model to others. The non-interaction model was selected. Exchange is the base case for model type. Primary registration is significant (less recommended vs. exchange), while CaaS is not significantly different from exchange. Participants who completed the encryption tasks before hearing about security properties were signficantly less likely to recommend any model.

We asked participants why they would or would not use each system, and categorized each participant's self-reported most important reason as related to security, usability, or both. (Details of participants' usability and security opinions for each system were discussed in Sections 5.1 and 5.2 respectively.) For participants who would not use a system, we also included having no need for

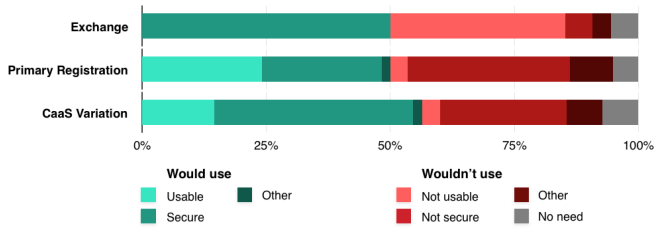


Figure 6: The most significant reason why participants would and would not use each model. We note here that while the number of participants who would use each system is similar, their reasoning varies. For example, prospective users of the exchange model uniformly cite security, while prospective users of the two registration models cite a mixture of security and usability.

encryption as a separate category. Figure 6 shows the results. Some participants gave more than one answer; a few did not give meaningful responses.

Unsurprisingly, the perception of better security attracted participants to the exchange model, while poor usability drove them away. Participants' reactions to the two registration models were more complicated. In both cases, insufficient security was the most common reason for rejecting the systems; however, participants who said they would use the primary registration model were evenly split between whether its usability or its security was more important. Participants who said they would use the CaaS model largely but not uniformly cited its security properties.

Participants who said they would use the exchange model generally described using it for high-security information only, or only at a small scale. ES6 exemplified this trend, saying the exchange model is "the safest one. I want to use it in small scale, like one or two people, ... like private and personal things. But I don't want to use it every day." RS9 felt similarly: "I think this system is more effective with fewer people, maybe under ten. I would use it when I send my credit card information to my Mom, instead of QQ or Wechat [two instant messaging services]." ES10 said he would use the exchange model for client projects, which should be kept secret until they are finished. Among the 27 participants who agreed they would want to use the exchange model, none mentioned using it with a large group; 16 said they would use it for very private information while only one said she would use it for general or everyday emails.

In contrast, participants who said they would use either variation of the registration model mentioned "contacting a large number of customers" for payroll or financial information (ET6) as well as "party and meeting announcements" (ET9, RS13). RT8 said she would use the registration model for information that was "overall private, but would not be a disaster if disclosed, e.g., my daughter is sick." ES7, a teacher, said she would use the exchange model only for "extremely sensitive information, such as SSNs," while she would use the registration model to send "location information or grade information." In total, 15 participants who wanted to use either variation of the registration model mentioned general email or large-scale communications.

These results suggest that although most participants said they would use both systems at least sometimes, quite a few wanted encryption only in specific circumstances. Between the exchange and registration models, however, our participants found the registration model useful in a broader variety of circumstances.

Using vs. recommending

As expected, most participants (44) who said they would use a system also said they would recommend it to others, and vice versa, but a few gave interesting reasons for answering differently. ET4 said he would not use the exchange model because it was too cumbersome, but would recommend it to others who have stronger privacy requirements. Similarly, RT4 said that "encryption is not necessary for me," but recommended the CaaS variation of the registration model because it is "easier to use [than the exchange model] and more secure than the vanilla [primary] registration system."

Registration vs. no encryption

We did not explicitly ask participants to compare these encryption models to unencrypted email. However, 5 participants who had concerns about the security of the registration model (total 14 rated less than 4) also mentioned that it does provide a valuable security improvement over unencrypted email. ET7 said "The email is not raw, which is another layer of security. ... Doing encryption gives me a security sense that I lock my door myself." RT12, explaining why he would use the primary registration model, noted that "I have to trust the email provider, which is problematic, but . . . it's better than raw email."

In line with findings from prior work [33], for some participants the process of taking any manual steps (such as generating a key pair in either model) increased their confidence that protection was occurring; for example, RS6 said "extra steps give me a security sense."

Auditing model

We asked participants who heard about the auditing model whether they would use it; overall, it proved popular. Of the 24 participants who were introduced to the auditing model, 15 said they would like to use it. Of these, 10 preferred it to any other model discussed. For example, ES11 said, "It's best among all systems mentioned in the experiment, because somebody else is policing them, just like watchdogs. If someone is reading your email, they might be caught." RT8 preferred the auditing model to any other option because "unlike the other models . . . instead of using [the attacker's] public lock blindly, I will get the update, 'Oh, that's the wrong public lock, you should not use this.'"

Four found the auditing model superior to the other registration models, but preferred the exchange model in at least some circumstances. RS10 said he would send personal information including banking data using the auditing model, but "if I worked in a government department, I would still use the exchange model." RT12 said the audit model is "slightly better than [the primary] registration model . . . because in [the primary registration] model I don't know if wrong locks happened. But overall, the lock exchange system has extra steps, extra layers of security, so I like it best among all the systems." Several of these 15 participants noted the possible time lag in notification as an important disadvantage, but were willing to use the model anyway. This generally positive reaction, combined with the preference to split risk among different parties in the CaaS model, suggests that the auditing model has strong potential to meet with user approval.

Eight participants said they would not use the auditing model (one was unsure). One of these (RS11) preferred it to all other models but believed he had no need to encrypt his email, and three found it worse than the exchange model. Four said it was worst among all models discussed, either because they did not trust the auditors or

because the time lag was too great.

5.4 Participant understanding

Despite receiving only a short introduction to each encryption system, most of our participants demonstrated thoughtful understanding of key concepts for each, suggesting that they provided credible opinions throughout the experiment.

Handling misconfiguration

We asked participants to consider how they would handle various possible misconfigurations in each model. Our primary goal was to prompt them to consider usability issues related to longer-term key maintenance, but this section of the interviews also offered a chance to evaluate participants' understanding of the different security models. Most participants were capable of reasoning correctly about these error scenarios.

Participants were presented with five different misconfiguration scenarios across the two models (see Table 2). Thirty-nine of 52 participants (75%) responded to all five scenarios with a straightforwardly correct answer, such as asking Alice to resend a lost public key (task 9a, exchange) or generating a new lock-key pair and redistributing the lock to all correspondents (task 9b, exchange). Seven additional participants (13.5%) provided such answers to at least three of the scenarios. One participant (RS13) mentioned recovering keys from a backup (such as a USB drive) rather than generating a new key pair.

We note several interesting misconceptions among those participants who got at least one scenario wrong. Four participants responding to task 9c (accidentally publicizing their own private key, in either model) suggested changing their password within the encryption extension; the password unlocks access to the private key, but a new password would not help if the key has already been exposed. Another participant (RS7) suggested for 9c that "I will send my email to a third person I trust, and ask that person to encrypt the email for me and send to my recipients. Similarly, he will decrypt the [response] email for me and forward it to me." This shows interesting security thinking but misses the potential for the message to be captured during the first step. Other common answers included getting tech support from the company that developed the encryption extension[3] and simply "I don't know."

Overall, participants were largely able to engage with these misconfiguration scenarios, demonstrating working understanding of the encryption tools; remaining misconceptions highlight areas in which more education, clearer directions in the tools, and more frequent use of encryption may be helpful.

Thinking about security

Our participants made several thoughtful points about encryption, security, and privacy that apply across models. ES4 mentioned that an extra benefit (of any encryption model) is a reduction in targeted ads: The "email provider can collect data through my emails, and then present ads. . . . I don't want that. [Using this tool] the ads will not appear."

ES10 expressed concern that an email encryption provider (in either model) might collect your private key, especially if you are using Apple email on an Apple device or Google email in Chrome, etc. One participant (RS9) was concerned about using public computers. This is potentially a problem for both encryption models, which assume the private key is securely stored on the user's local device. She was also concerned that the act of sending a lock might itself catch the interest of attackers; another participant (RS11) liked the sense of security provided by both encryption models but thought it might seem paranoid to worry about others reading his emails. Similar concerns were raised in [18]. ES12 expressed concern that the centralized nature of the registration model would provide a juicier target for an attacker than many individuals participating in the exchange model. ET10 worried that encryption would bypass an email provider's virus-detection system.

Several (11) participants liked that the exchange model allowed them to explicitly control who would be able to send them encrypted email. ES2 said he would "know the person whom I sent the public locks to," and RT3 liked that "who can send me encrypted emails [is] controlled by myself." RS13 said that "if I communicate with a group of people, it's easy to kick someone out of the group." A similar level of control can be implemented in a registration model; our findings suggest this is a feature at least some users value.

Although many participants understood and reasoned effectively about the security properties we presented, some retained incorrect mental models that have implications for the ongoing design of encryption systems. RS1 incorrectly believed that since he could not understand an encrypted message, no one else (including his email provider) would be able to either. Others were concerned about keeping their public locks secret in the exchange model; three split their locks across different channels in an effort to be more secure. For example, RS2 sent half of his public lock through the secondary email account and posted the other half on the key server. RT7 thought it would be insecure to store public locks: "After I send my lock to other people, others may not delete my public lock. . . . I may also forget to do so after I import others' locks. The fewer people know my public lock, the safer." Relatedly, ES13 worried that in the auditing model, the auditors "are scanning my lock. It sounds like more people are watching me besides the email provider, and I don't feel good."

Several participants also had concerns and misconceptions about how keys are managed across multiple devices, regardless of model. System designers may want to provide help or information on these points.

Evaluating tradeoffs

In deciding which system(s) they preferred, participants explicitly and deliberately made tradeoffs among their security and usability features. For example, ES13 said he would use the exchange model because "Exchanging locks makes it more private for me", despite the fact that "it takes time to exchange locks". ES10 also preferred the exchange model: "Having something better than baseline is one approach. But if I compare to perfect security I am trying to get, it's another approach. . . . When you want to use it, you really want it to be very well protected."

On the other hand, RT13, who said he would not use the exchange model, commented that "The negotiating process maybe gives me safer feelings, more protection. But on the other hand . . . the disadvantage is it is time consuming, cumbersome, tedious, more complicated, and this is the price I have to pay for more protection."

RS7 said she would use the primary registration model because it is "easy to use, and I think most of us trust our email provider", al-

[3] While completely reasonable in practice, this answer does not demonstrate understanding of the encryption model's security properties and so was not counted as "correct" for this purpose.

though she understood that "there are some possible threats." ET8, in contrast, would not use the primary registration model because "It's easy to send encrypted emails, especially to many people. But security concern is the reason I don't want to use it." According to ES12, the exchange model "is more straightforward. Only I and the other person [recipient] get involved in the communication, and no others." These comments and others demonstrate that participants understood pros and cons of the different models and thought carefully about how to balance them.

6. DISCUSSION AND CONCLUSION

We conducted the first study examining how non-expert users, briefly introduced to the topic, think about the privacy and convenience tradeoffs that are inherent in the choice of encryption models, rather than about user-interface design tradeoffs.

Our results suggest that users can understand at least some high-level security properties and can coherently trade these properties off against factors like convenience. We found that while participants recognized that the exchange model could provide better overall privacy, they also recognized its potential for self-defeating mistakes. Similarly, our participants acknowledged potential security problems in the registration model, but found it "good enough" for many everyday purposes, especially when offered the option to audit the system and/or split trust among several parties. This result is particularly encouraging for approaches like CONIKS and Google's end-to-end extension, which spread trust among many potential and actual auditors. It is important to note that understanding the identities and motivations of third-party auditors was important to several of our participants, so making this auditing process as open and transparent as possible may prove important to its success.

We believe our results have important implications for designers of encryption tools as well as researchers, policymakers, journalists, and security commentators. First, our results suggest that it may be reasonable to explain in clear language what the high-level risks of a given encryption approach are and trust users to make decisions accordingly. The Electronic Frontier Foundation's *Secure Messaging Scorecard*, which tracks the security properties of encryption tools, provides an excellent start in this direction [15]. Of course, participants in our study were directly instructed to read the materials we gave them; real users often have neither the time nor the motivation to seek out this kind of information. This magnifies the role of journalists, security commentators, and other opinion-makers whose recommendations users often rely on instead.

As a result, alarmed denunciations of tools that do not offer perfect privacy may only serve to scare users away from any encryption at all, given that many users already believe encryption is either too much work or unnecessary for their personal communications. Instead, making clear both the marginal benefit and the risk can support better decision making. This also underscores the critical importance of making risks explicit up front, in plain non-technical language; users who are misled into a false sense of security may misjudge tradeoffs to their detriment.

We do, however, advise some caution. Although most participants understood the encryption models and their security properties at a high level, there were some smaller misunderstandings that impacted their ability to make informed decisions. Despite years of effort from the security community, effectively communicating these subtleties remains difficult; however, we believe our findings demonstrate the benefits of continuing to try. Continued education, discussions in the media, and more frequent engagement with encryption tools in daily life may all assist this effort. Our own educational materials were improved through early pilot testing but not rigorously developed into an ideal or standard format; there is room to develop better materials for those users who are interested in learning more about encryption.

As end-to-end encryption is increasingly widely deployed, designers and companies must make choices about which models to adopt. We believe our results can provide some additional context for making these decisions, relative to the targeted use cases and user population. Further work in this area—for example, testing how a completely transparent registration model affects decision making and perception of security, examining an auditing model in greater detail and with reference to specific trusted auditors and notification lags, and comparing different approaches to framing security properties for non-experts—can provide further insight into how to optimize these choices.

7. ACKNOWLEDGMENTS

The authors wish to thank Elaine Shi and Christopher Soghoian for discussions that helped lead to this work; Nikos Kofinas and Yupeng Zhang for contributing to an early version of this study; members of the University of Maryland HCI Lab for their helpful feedback; and Cody Buntain for suggesting the title.

8. REFERENCES

[1] Apple. iOS security guide, iOS 9.0 or later. https://www.apple.com/business/docs/iOS_Security_Guide.pdf, Sept. 2015. (Last accessed on 05/16/2016).

[2] Apple. The most personal technology must also be the most private. https://www.apple.com/privacy/approach-to-privacy/, Mar. 2016. (Last accessed on 05/16/2016).

[3] J. Ball. GCHQ views data without a warrant, government admits. *The Guardian*, Oct. 2014. http://www.theguardian.com/uk-news/2014/oct/29/gchq-nsa-data-surveillance (Last accessed on 05/16/2016).

[4] D. Bisson. A timeline of the Apple-FBI iPhone controversy. *The State of Security*, Mar. 2016. http://www.tripwire.com/state-of-security/government/a-timeline-of-the-apple-fbi-iphone-controversy/ (Last accessed on 05/16/2016).

[5] O. Bowcott. Facebook case may force european firms to change data storage practices. *The Guardian*, Sept. 2015. http://www.theguardian.com/us-news/2015/sep/23/us-intelligence-services-surveillance-privacy (Last accessed on 05/16/2016).

[6] K. P. Burnham and D. R. Anderson. Multimodel inference: Understanding AIC and BIC in model selection. *Sociological Methods & Research*, 33(2):261–304, Nov. 2004.

[7] L. J. Camp, T. Kelley, and P. Rajivan. Instrument for measuring computing and security expertise. Technical Report TR715, Indiana University, Feb. 2015.

[8] C. Cattiaux and gg. iMessage privacy. http://blog.quarkslab.com/imessage-privacy.html, Oct. 2013. (Last accessed on 05/16/2016).

[9] C. A. Ciocchetti. The eavesdropping employer: A twenty-first century framework for employee monitoring. *American Business Law Journal*, 48(2):285–369, 2011.

[10] K. Conger. Google engineer says he'll push for default end-to-end encryption in Allo, May 2016.

http://techcrunch.com/2016/05/19/google-engineer-says-hell-push-for-default-end-to-end-encryption-in-allo/ (Last accessed on 06/02/2016).

[11] W. Diffie and M. E. Hellman. New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6):644–654, Nov 1976.

[12] K. Elliott and T. Rupar. Six months of revelations on NSA. *Washington Post*, June 2013. http://www.washingtonpost.com/wp-srv/special/national/nsa-timeline/m/ (Last accessed on 05/16/2016).

[13] S. Fahl, M. Harbach, T. Muders, and M. Smith. Confidentiality as a Service – usable security for the cloud. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, pages 153–162, June 2012.

[14] S. Fahl, M. Harbach, T. Muders, M. Smith, and U. Sander. Helping johnny 2.0 to encrypt his facebook conversations. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, pages 11:1–11:17. ACM, 2012.

[15] E. F. Foundation. Secure messaging scorecard, 2016. https://www.eff.org/secure-messaging-scorecard (Last accessed on 05/16/2016).

[16] S. L. Garfinkel and R. C. Miller. Johnny 2: a user test of key continuity management with S/MIME and Outlook Express. In *Proceedings of the 2005 Symposium on Usable Privacy and Security*, SOUPS '05, pages 13–24. ACM, 2005.

[17] C. Garman, M. Green, G. Kaptchuk, I. Miers, and M. Rushanan. Dancing on the lip of the volcano: Chosen ciphertext attacks on Apple iMessage, 2016.

[18] S. Gaw, E. W. Felten, and P. Fernandez-Kelly. Secrecy, flagging, and paranoia: Adoption criteria in encrypted email. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, pages 591–600, New York, NY, USA, 2006. ACM.

[19] Google. Google End-To-End wiki. https://github.com/google/end-to-end/wiki, Dec. 2014. (Last accessed on 05/16/2016).

[20] Google. Email encryption in transit. *Transparency report*, Mar. 2016. https://www.google.com/transparencyreport/saferemail/?hl=en (Last accessed on 05/16/2016).

[21] B. Greenwood. The legality of eavesdropping in the workplace. *Chron*, Dec. 2012. http://work.chron.com/legality-eavesdropping-workplace-15267.html.

[22] P. Gutmann. Why isn't the Internet secure yet, dammit. In *AusCERT Asia Pacific Information Technology Security Conference 2004; Computer Security: Are we there yet?* AusCERT Asia Pacific Information Technology Security, May 2004.

[23] D. Hedeker. Mixed models for longitudinal ordinal and nominal outcomes, 2012. http://www.uic.edu/classes/bstt/bstt513/OrdNomLS.pdf (Last accessed on 05/16/2016).

[24] C. Johnston. NSA accused of intercepting emails sent by mobile phone firm employees. *The Guardian*, Dec. 2014. http://www.theguardian.com/us-news/2014/dec/04/nsa-accused-intercepting-emails-mobile-phone-employees (Last accessed on 05/16/2016).

[25] G. Kumparak. Apple explains exactly how secure iMessage really is. *TechCrunch*, Feb. 2014. http://techcrunch.com/2014/02/27/apple-explains-exactly-how-secure-imessage-really-is/ (Last accessed on 05/16/2016).

[26] B. Laurie, A. Langley, and E. Kasper. Certificate transparency. RFC 6962, RFC Editor, June 2013.

[27] N. Lomas. WhatsApp completes end-to-ed encryption rollout. http://techcrunch.com/2016/04/05/whatsapp-completes-end-to-end-encryption-rollout/, Apr. 2016.

[28] S. E. McGregor, P. Charters, T. Holliday, and F. Roesner. Investigating the Computer Security Practices and Needs of Journalists. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 399–414. USENIX Association, 2015.

[29] M. S. Melara, A. Blankstein, J. Bonneau, E. W. Felten, and M. J. Freedman. CONIKS: Bringing key transparency to end users. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 383–398. USENIX Association, Aug. 2015.

[30] I. Paul. Yahoo Mail to support end-to-end PGP encryption by 2015. *PCWorld*, Aug. 2015. http://www.pcworld.com/article/2462852/yahoo-mail-to-support-end-to-end-pgp-encryption-by-2015.html (Last accessed on 05/16/2016).

[31] B. Ramsdell. S/MIME version 3 message specification. RFC 2633, RFC Editor, June 1999.

[32] S. Ruoti, J. Anderson, S. Heidbrink, M. O'Neill, E. Vaziripour, J. Wu, D. Zappala, and K. Seamons. "We're on the same page": A usability study of secure email using pairs of novice users. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '16, pages 4298–4308, New York, NY, USA, 2016. ACM.

[33] S. Ruoti, N. Kim, B. Ben, T. van der Horst, and K. Seamons. Confused Johnny: when automatic encryption leads to confusion and mistakes. In *Proceedings of the Ninth Symposium on Usable Privacy and Securit*, SOUPS '13, pages 5:1–5:12. ACM, July 2013.

[34] M. D. Ryan. Enhanced certificate transparency and end-to-end encrypted mail. In *21st Annual Network and Distributed System Security Symposium, NDSS'14*, 2014.

[35] S. Sheng, L. Broderick, C. A. Koranda, and J. J. Hyland. Why Johnny still can't encrypt: evaluating the usability of email encryption software. In *Proceedings of the Second Symposium on Usable Privacy and Security*, SOUPS '06, 2006.

[36] D. J. Solove. 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review*, 44:745, 2007.

[37] S. Somogyi. Making end-to-end encryption easier to use. *Google online security blog*, June 2014. http://googleonlinesecurity.blogspot.com/2014/06/making-end-to-end-encryption-easier-to.html (Last accessed on 05/16/2016).

[38] A. L. Strauss and J. M. Corbin. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Sage Publications, Inc, Thousand Oaks, CA, USA, 1998.

[39] M. Sweikata, G. Watson, C. Frank, C. Christensen, and Y. Hu. The usability of end user cryptographic products. In *2009 Information Security Curriculum Development Conference*, InfoSecCD '09, pages 55–59. ACM, 2009.

[40] W. Tong, S. Gold, S. Gichohi, M. Roman, and J. Frankle.

Why King George III can encrypt. http://randomwalker.info/teaching/spring-2014-privacy-technologies/king-george-iii-encrypt.pdf, 2014.

[41] M. Viswanathan. *Measurement Error and Research Design*. Sage Publications, 2005.

[42] N. Weaver. iPhones, the FBI, and Going Dark. *Lawfare*, Aug. 2015. https://www.lawfareblog.com/iphones-fbi-and-going-dark (Last accessed on 05/16/2016).

[43] A. Whitten and J. D. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*, SSYM'99, pages 14–14, 1999.

[44] P. Zimmermann. PGP version 2.6.2 user's guide. ftp://ftp.pgpi.org/pub/pgp/2.x/doc/pgpdoc1.txt, Oct. 1994.

APPENDIX

This appendix contains the full survey and instructional instrument used in our research.

- Section A introduces the task and role-play to the participant.
- Section B contains the introduction and explanation of the Exchange Model.
- Section C contains the introduction and explanation of the Registration Model.
- Section D contains the post-task survey instrument.
- Section E contains the demographic questionnaire.

A. OVERALL INTRODUCTION

Welcome to our experiment. Today you will use two systems. These systems are developed to encrypt your emails so that your emails can be protected from being read by email providers (such as Google and Yahoo!), governments (e.g. NSA), as well as malicious attackers.

In this experiment, **pretend you are Henry**, and you want to send and receive encrypted emails to some people. Below are email addresses you may use in this experiment.

- Henry: researchmessage@gmail.com
- Henry2: researchmessage2@gmail.com
- Alice: alice.recipient@gmail.com
- Bob: bobby.recipient@gmail.com
- Carl: carl.recipient@gmail.com

B. EXCHANGE MODEL

Below is how *Lock Exchange System* works.

1. Every user can get a public lock and a private key.

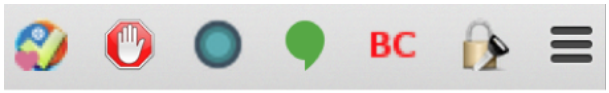
2. Users have to exchange their public locks in some way.

3. You can send encrypted emails with others' public locks, so that others' can read the emails with their private keys.

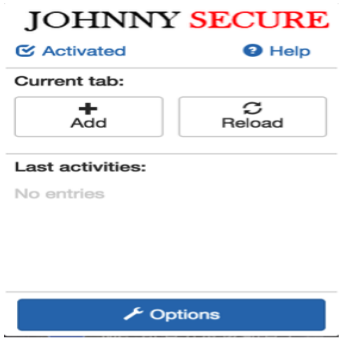
4. Similarly, you can also read any encrypted emails that are encrypted to you using your private key.

Task Instructions:

- Click the extension on upper right corner on tool bar in Chrome.



- Click "Options" for configuration.



1. Generate a public lock/private key pair.

   Go to "Generate Lock and Key" to generate a **public lock/ private key pair**. Note: The password is only for this study, and is NOT your email password. **DON'T** use your real passwords associated with any of your account in real life.

2. Exchange Public Locks with Alice.

   (a) Go to "Display Lock/Key Pair" and click the lock/key pair you just generated. Then export your public lock to Alice.
   The public lock will **start with** "-----BEGIN PGP PUBLIC LOCK BLOCK-----", and **end with** "-----END PGP PUBLIC LOCK BLOCK-----" (Note: there are FIVE "-" in the beginning and in the end).
   You can send your public lock by one or combination of ways that we **provide** you.

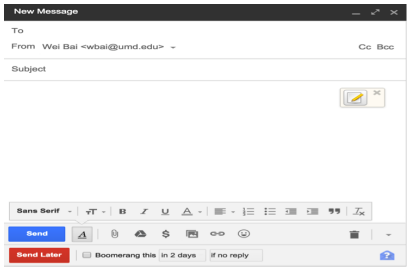
   (b) Then you will receive Alice's public lock.

   (c) Import Alice's public lock into the extension.

3. Send an encrypted email to Alice

   In the email interface, first click the encryption icon to write "What is your favorite color" to Alice. If the icon doesn't show up, please refresh the website.

   Note: you need to encrypt for Alice.



4. Decrypt the received email from Alice.

   Move your mouse to the email body. When a lock icon appears, click on the icon. You need your password (you created in step 3) to decrypt email.

   Next you will send encrypted email to two recipients Bob and Carl.

5. Exchange Public Locks with Bob and Carl.

   You can use the same way or different way provided in step 4 to exchange public locks with Bob and Carl.

6. Send encrypted email to Bob and Carl.

   Imagine that you are a financial secretary in your department, and you want to send the payroll reports to Bob and Carl by encrypted email. For simplicity, you can simply write "Here is your biweekly payroll summary: Salary is $888.88, Tax is $88.88. Your subtotal: $800.00." in the email body. You can refer to previous steps to send encrypted email.

7. Decrypt the received email from Bob and Carl.

8. Imagine that you are still the financial secretary in your department, and you will send the payroll reports to 10 people by encrypted email, what will you do? Please specify the steps.

9. Misconfiguration

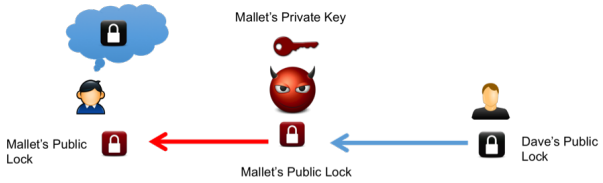
   (a) If you accidentally delete or lose Alice's public lock, what will you do if you want to send/receive encrypted email to/from Alice?

   (b) If you accidentally delete or lose your own private key, what will you do if you want to send/receive encrypted email to/from other recipients?

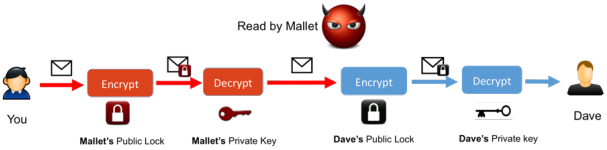
   (c) If you accidentally publicize your own private key, what will you do if you want to send/receive encrypted email to/from other recipients?

Possible Threats for *Lock Exchange System*:

These systems are developed to encrypt your emails so that your emails can be protected from being read by email providers (such as Google and Yahoo!), governments (e.g. NSA), as well as malicious attackers.



The threat may happen when you exchange public locks with others. When you try to get the public lock from Dave, Mallet (can be any type of attacker from above) secretly switches the public lock to his own. You think you get Dave's public lock, but in fact you get Mallet's.



Then when you send encrypted email to Dave, you actually use Mallet's public lock. As a result, Mallet can read your email. Mallet will consequently use Dave's public lock and send the encrypted email to Dave, so that both you and Dave don't realize the email has been read.

This threat doesn't happen usually, because it requires Mallet to have much power and resources to achieve this.

Please give your feedback about *Lock Exchange System:*

Note: We are evaluating these systems. We are not testing you. These systems are not developed by us. Please leave your feedback as honestly as you can. Your honest feedback, positive or negative, will help with our research.

For the first two questions, please note the difference between difficulty and cumbersomeness. Difficult tasks are intellectually challenging and need effort or skills to accomplish. Cumbersome tasks are tedious and need an unnecessarily long time to accomplish.

Please rate your agreement with the following statements.

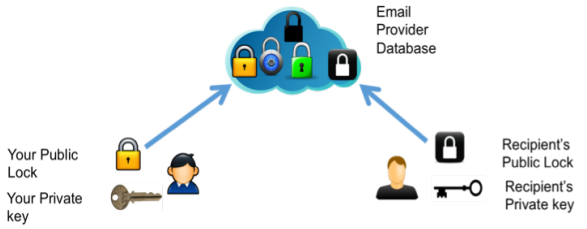
1. The following tasks were difficult.
   (a) Generate the public lock and private key pair
   (b) Exchange public lock with Alice
   (c) Send encrypted email to Alice
   (d) Decrypt email from Alice
   (e) Exchange public locks with Bob and Carl
   (f) Send encrypted email to Bob and Carl
   (g) Decrypt email from Bob and Carl
   (h) Send and receive encrypted emails to 10 people
2. The following tasks were cumbersome.
   (a) Generate the public lock and private key pair
   (b) Exchange public locks with Alice
   (c) Send encrypted email to Alice
   (d) Decrypt email from Alice
   (e) Exchange public locks with Bob and Carl
   (f) Send encrypted email to Bob and Carl
   (g) Decrypt email from Bob and Carl
   (h) Send and receive encrypted emails to 10 people
3. This system effectively protected my privacy.

C. REGISTRATION MODEL

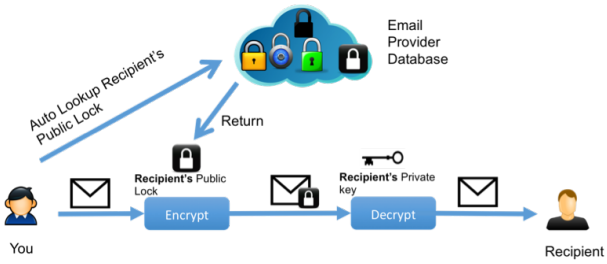
Instruction: Below is how *Registration System* works.

1. Every user can get a public lock and a private key when you register.

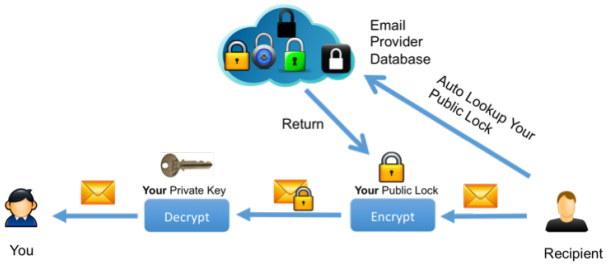
2. Every user's public lock will be automatically stored in a cloud database that is run by the email provider.



3. You can send encrypted emails with others' public locks, so that others' can read the emails with their private keys. The cloud database will return others' public locks for you.



4. Similarly, you can also read any encrypted emails that are encrypted to you using your private key.

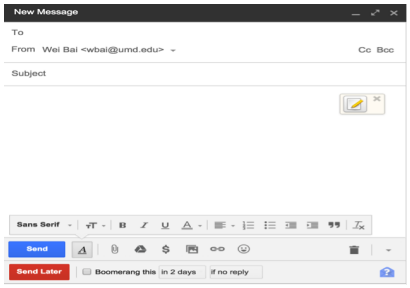


Task Instructions:

- Click the extension on the upper right corner on the tool bar in Chrome.

- Click "Options" for configuration.

1. Register
   Go to "Register" to register your email account to the email provider server. The registration will give you a public lock and a private key.
2. Send an encrypted email to Alice
   In the email interface, first click the encryption icon to write "What is your favorite color" to Alice. If the icon doesn't show up, please refresh the website.
   Note: you need to encrypt for Alice.
3. Decrypt the received email from Alice
   You need your password (you created in step 3) to decrypt email.
   Next you will send encrypted email to two recipients Bob and Carl.



4. Send encrypted email to Bob and Carl.

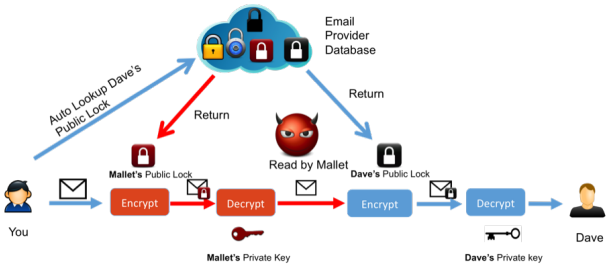
   Imagine that you are a financial secretary in your department, and you want to send the payroll reports to Bob and Carl by encrypted email. For simplicity, you can simply write "Here is your biweekly payroll summary: Salary is $888.88, Tax is $88.88. Your subtotal: $800.00." in the email body. You can refer to previous steps to send encrypted email.

5. Decrypt the received email from Bob and Carl
6. Imagine that you are still the financial secretary in your department, and you will send the payroll reports to 10 people by encrypted email, what will you do? Please specify the steps.
7. Misconfiguration
   (a) If you accidentally delete or lose your own private key, what will you do if you want to send/receive encrypted email to/from other recipients?
   (b) If you accidentally publicize your own private key, what will you do if you want to send/receive encrypted email to/from other recipients?

Possible Threats for *Registration System*:

These systems are developed to encrypt your emails so that your emails can be protected from being read by email providers (such as Google and Yahoo!), governments (e.g. NSA), as well as malicious attackers.

There are two prototypes for *Registration System*. For the first prototype (Model 1), the possible threats are as follows.



The threat may happen when you send encrypted emails to others. For example, when you try to send encrypted emails to Dave, you think the email provider database will return Dave's public lock to you. But in fact it returns Mallet's, so that Mallet can read your email. Therefore, you need to trust the email provider in this system.

In the second prototype (Model 2), there is a third-party service (not the email provider) as an intermediary. In this prototype, neither the third-party service nor your email provider can read your email themselves. However, if your email provider and the third-party service collaborate, they can both read your email. Therefore, you need to trust that the two services are not collaborating.

Please give your feedback about *Registration System*:

Note: We are evaluating these systems. We are not testing you. These systems are not developed by us. Please leave your feedback as honestly as you can. Your honest feedback, positive or negative, will help with our research.

For the first two questions, please note the difference between difficulty and cumbersomeness. Difficult tasks are intellectually challenging and need some effort or skills to accomplish. Cumbersome tasks are tedious and need an unnecessarily long time to accomplish.

Rate your agreement with the following statements.

1. The following tasks were difficult.
   (a) Register
   (b) Send encrypted email to Alice
   (c) Decrypt email from Alice
   (d) Send encrypted email to Bob and Carl
   (e) Decrypt email from Bob and Carl
   (f) Send and receive encrypted emails to 10 people
2. The following tasks were cumbersome.
   (a) Register
   (b) Send encrypted email to Alice
   (c) Decrypt email from Alice
   (d) Send encrypted email to Bob and Carl
   (e) Decrypt email from Bob and Carl
   (f) Send and receive encrypted emails to 10 people
3. This system effectively protected my privacy.

D. OVERALL FEEDBACK

Please give your overall feedback about these two systems:

Note: Again, please give your honest feedback to help with our research.

1. Please rate your willingness to use these two systems in the future.
   (a) I would like to use *Lock Exchange System*.
   (b) I would like to use *Registration System* with Model 1.
   (c) I would like to use *Registration System* with Model 2.
2. Below please rate your willingness to recommend these systems to others.
   (a) I would like to recommend *Lock Exchange System* to others.
   (b) I would like to recommend *Registration System* with Model 1 to others.
   (c) I would like to recommend *Registration System* with Model 2 to others.
3. Please rate your agreement with the following statements.
   (a) I think that I would need the support of a technical person to be able to use Lock Exchange System.
   (b) I think that I would need the support of a technical person to be able to use Registration System.

(c) I would imagine that most people would learn to use Lock Exchange System very quickly.
(d) I would imagine that most people would learn to use Registration System very quickly.
(e) I would need to learn a lot of things before I could get going with Lock Exchange System.
(f) I would need to learn a lot of things before I could get going with Registration System.

4. What do you like or dislike for each system? Why?

In Model 3, the email provider will still store all users' public locks, just like Model 1. But there are other parties (auditors) who audit the email provider, to ensure that the email provider is giving out correct public locks. These auditors may include other email providers, public interest groups, and software on your devices. If the email provider gives you a public lock that doesn't belong to the recipient, or gives someone else the wrong public lock for you, these parties will notify you. You (or someone else) may use the wrong lock temporarily (for an hour or a day) before you are notified.

In this model, you don't need to trust any email provider, but you need to trust the auditors and/or the software on your device. Because there are several auditors, even if one auditor does not alert you another one probably will.

E. DEMOGRAPHICS

1. Which of the following best describes your current occupation?
   (a) Healthcare Practitioners and Technical Occupations
   (b) Office and Administrative Support Occupations
   (c) Production Occupations
   (d) Farming, Fishing, and Forestry Occupations
   (e) Computer and Mathematical Occupations
   (f) Community and Social Service Occupations
   (g) Life, Physical, and Social Science Occupations
   (h) Management Occupations
   (i) Legal Occupations
   (j) Installation, Maintenance, and Repair Occupations
   (k) Food Preparation and Serving Related Occupations
   (l) Architecture and Engineering Occupations
   (m) Arts, Design, Entertainment, Sports, and Media Occupations
   (n) Building and Grounds Cleaning and Maintenance Occupations
   (o) Healthcare Support Occupations
   (p) Construction and Extraction Occupations
   (q) Education, Training, and Library Occupations
   (r) Protective Service Occupations
   (s) Sales and Related Occupations
   (t) Business and Financial Operations Occupations
   (u) Transportation and Materials Moving Occupations
   (v) Other (please specify)
2. Where did you grow up (primarily)?
   (a) United States
   (b) Other North America
   (c) South or Central America
   (d) Western Europe
   (e) Eastern Europe
   (f) Africa
   (g) South Asia (India, Bangladesh, Pakistan, etc.)
   (h) East Asia (China, Japan, Korea, etc.)
   (i) Central Asia
   (j) The Middle East
   (k) Australia / Oceania
   (l) Other: [please specify]
   (m) I prefer not to answer
3. What is your age?
   (a) 18-20
   (b) 21-24
   (c) 25-34
   (d) 35-44
   (e) 45-54
   (f) Above 54
   (g) I prefer not to answer
4. What is your gender?
   (a) Male
   (b) Female
   (c) I prefer not to answer
5. Please tell us whether you have the following experiences (yes or no).
   (a) I have attended a computer security conference in the past year.
   (b) I have taken or taught a course in computer security before.
   (c) Computer security is one of my primary job responsibilities.
   (d) I have used SSH before.
   (e) I have configured a firewall before.
   (f) I have a degree in an IT-related field (e.g. information technology, computer science, electrical engineering, etc.)?
   (g) I have an up-to-date virus scanner on my computer.