Secure and Usable P2P VoIP for Mobile Devices

Joakim Koskela[†] Kristiina Karvonen[†]

Theofanis Kilinkaridis[†] Andrei Gurtov[†‡]

[†]Helsinki Institute for Information Technology HIIT
PO Box 19800, 00076 Aalto
[‡]Department of Computer Science and Engineering, Aalto University
{joakim.koskela, kristiina.karvonen, andrei.gurtov}@hiit.fi
theofanis.kilinkaridis@electrabel.com

ABSTRACT

The use of Voice over IP (VoIP) applications involves a number of security threats and usability issues, leading to possible breaches of security and privacy. With the adoption of future peer-to-peer communication systems, the challenges grow even more as we rely on untrusted peers to access the service. We are developing a peer-to-peer VoIP system which features techniques for improving the security and privacy of users in future networks. However, as the threats are seldom well understood, presenting them in a usable manner is problematic. Implemented on a mobile device, the small user interface provides additional challenges for the end user. Via interviews, a questionnaire and usability testing, we seek to improve both the usability of managing and understanding the additional security, as well as the overall user experience of the emerging application.

Categories and Subject Descriptors

H.5.2 [**Information Interfaces and Representation**]: User Interfaces—*Evaluation/methodology*

General Terms

Human Factors, Security

Keywords

Usable security, VoIP, user study, peer-to-peer

1. INTRODUCTION

With the rapid spread of security breaches, information security has become important to every computer user. Spyware, worms, and other malicious software present daily threats online. As countermeasure, security mechanisms, methods and tools are created to protect users' security and privacy.

For good security, technological advancements are not enough. In practice, poor usability is often more detrimental to system security than the weaknesses in the underlying security mechanisms. Increasing usability without simultaneously decreasing technical security, and vice versa, has been a longstanding problem [12][13][3]. Already in 1975, Saltzer and Schroeder stated the principle of psychological acceptability [10] as a key criterion for evaluating a system's overall security. Usable security as a research area has since emerged, combining human-computer interaction (HCI) and computer security.

The use of Voice over IP (VoIP) applications involves a number of security threats and usable security issues. Unsecured VoIP communication can be easily eavesdropped and by using misconfigurations and software faults, an attacker can harvest personal information such as buddy lists and call records. In the worst case, they can be later used for malicious purposes: sending spam, identity theft, or entry vectors for more elaborate hoaxes.

In peer-to-peer (P2P) VoIP systems the problems become even more tangible. Regarded as the next evolution of VoIP, able to provide more fault-tolerant, robust and cost-efficient networking, P2P VoIP systems depart from the traditional centralized model and harness the shared resources of the end-users to provide the service. This creates even more opportunities for exploitation as users have to rely on possibly untrusted peers to manage the system. Although P2P VoIP shows potential, additional security is needed in order to make VoIP a secure choice also.

We are developing a secure P2P system for mobile VoIP communication similar to the work of the P2PSIP working group [6]. It implements privacy protecting methods and utilizes technologies such as the Host Identity Protocol (HIP)[8] to secure the communication. However, how these technologies can be presented to users in an understandable and usable way on mobile devices is not clear, especially when the users may not even be aware of the threats, and the mobile user interface (UI) is quite restrained. In this paper we examine the usability attributes of P2P VoIP usage: attitudes towards security in VoIP and the usability of our solutions through user studies.

2. RELATED WORK

Whitten and Tygar [12] define security software usable if the people who are expected to use it 1) are reliably made aware of the security tasks they need to perform; 2) are able to figure out how to successfully perform those tasks; 3) do not make dangerous errors; and 4) are sufficiently comfortable with the interface to continue using it.

MobileHCI 2010 September 7-10, 2010, Lisboa, Portugal.
ACM 978-1-60558-835-3/10/09.

The consequences of misusing an unusable system can lead to dangerous or even fatal errors with respect to security[12].

Security and usability are often seen as competing goals [3][4]. However, a more usable system reduces confusion and is thus more likely to be secure. Adams and Sasse [2] found that users often give up security for easy access [3]. If security becomes an obstacle in conducting everyday tasks, it is turned off [9]. According to [4], users may be aware of the risks based on their experience, but are unable to make appropriate security decisions due to bad usability.

3. CHALLENGES AND SOLUTIONS FOR P2P VOIP

As peer-to-peer systems lack a trusted service provider, users must use a different strategy to fend off possible threats. Without central control it is hard to identify malicious peers, and users must take great care to protect personal information usually managed by a trusted service provider. For this study, we have examined the usability of two of the security solutions implemented in our mobile P2P VoIP system; spam filtering and a privacy enhancement mechanism.

Unwanted communications, or spam, is feared to become a problem in P2P VoIP as it is hard to blacklist rogue users. Our spam filtering solution is based on using relationships to filter unwanted calls. We distribute contact lists in a privacy preserving manner, and use these to establish *social links* between users. One central concept is "hops", the *social distance* (number of intermediate friends) between two users in a network of buddies. By configuring the maximum number of hops from which the user is willing to accept calls, possible spam calls can be avoided.

Without protection, the actions of users in P2P networks are easily traceable by intermediate peers. Although a malicious peer would not be able to eavesdrop, it can track call records (between whom calls are made and the location and status of users), which can be used for a number of criminal activities.

Our privacy enhacement mechanism, based on the work described in [7], protects users by using shared secrets to obfuscate the information shared with the peer network. As this affects the availability of users (pre-shared secrets are needed), the enhancement is designed to operate in three modes (Open, Relaxed and Paranoid) depending on the availability and level of protection required. The *Open* mode offers no protection. However, it allows users without shared secrets to connect (during which a secret can be established). The *Paranoid* mode uses only the obfuscated data, which enables calls to be made or received from previously known users only. The *Relaxed* mode provides an intermediate alternative; it uses the obfuscated data whenever possible, but allows also unprotected calls. This prevents tracking of calls between previously known users, while still allowing new contacts to connect.

4. THE STUDY

The usability study was based on semi-structured interviews, a questionnaire and UI mock-ups for which non-expert, but fluent computer users were chosen.

The semi-structured interview and questionnaire[1] were used to get information on users' level of competence and attitudes towards computer security and security in VoIP applications. For the interviews we had nine users, university students aged 18-25 (6 males and 3 females). All had 2-3 years of VoIP experience, but not on a mobile device. For the questionnaire, advertised on several mailing lists, we received 103 complete responses, 51/51[2] male/female. The majority (43%) were 25 to 29 years old. The respondents came from 28 countries; their educational background was diverse.

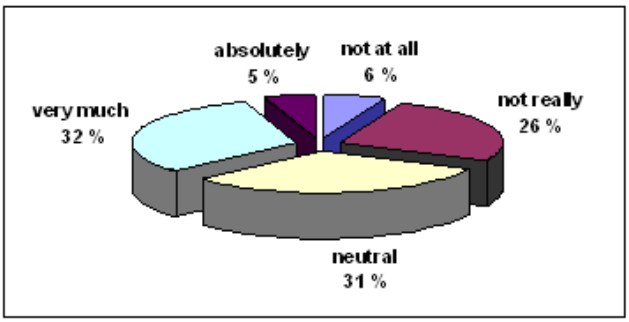

Figure 1: How well you think you are informed about computers security?

The paper mock-ups were drafted based on the findings, (c.f. Figures 2-7), covering the following use cases:

Use case 1: User calls
Use case 2: User receives a call
Use case 3: Introducing a buddy
Use case 4: Managing privacy settings

The mock-ups were designed to include elements of the security mechanisms we have developed. One was a privacy enhancing mechanism through the *privacy setting* in Use case 4. Six university students, between 18-24 years old, two female and four male, took part in the mock-up testing.

5. RESULTS

According to our findings, users tend to associate security with passwords, viruses, privacy, confidentiality, and integrity of personal information. The risks associated with compromised security included loss of personal data or money. The majority was aware of at least one major system attack and had personal experience of being infected by a virus.

5.1 Current level of security awareness

Users seem aware of the importance of computer security; 93% said they discuss issues related to security with other people; 68% with friends and 39% both at home and at work. Of the questionnaire respondents, 32% believed to be very well informed about security (Fig. 1), and only 6% believed to be badly informed. From the interviewees, the more knowledgable, the less the interviewee considered him/herself to know. But the less an interviewee knew, the safer s/he seemed to feel. This is of crucial importance: ignorance is an attack point.

The majority was unaware if encryption in VoIP applications existed while a few thought there might be some form of encryption in the VoIP applications they use. Lack of interest for secure communication in VoIP environments was prevalent. Only one participant wished for encryption in

[1]https://survey.hiit.fi/index.php?sid=57695&newtest=Y&lang=en

[2]One respondent did not state gender

Figure 2: Application main UI

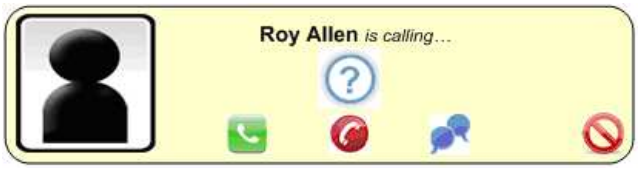

Figure 3: More reputation info

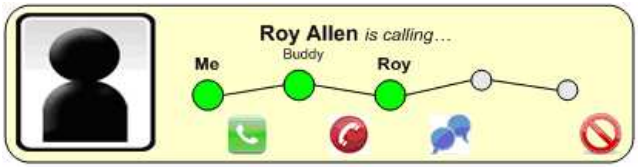

Figure 4: 2-hop connection with the caller

VoIP; three thought the need depends on the nature of the call.

5.2 Attitudes towards privacy in VoIP

Questionnaire respondents showed relatively strong concern for online privacy. When asked whether they believe their online activities can be monitored, 50% had wondered if their Internet calls could be listened to, and 60% had wondered if their chat sessions could be read by unauthorized parties. Only 24% thought the privacy of their calls might be violated, 21% suspected violation of chat privacy. Most users seemed to fall in the category of "privacy pragmatists", who are aware, but relatively careless about privacy, ready to trade it off for a bargain [1].

Regarding SPAM in VoIP, almost one third had had at least one call and almost half at least one chat request from an unknown caller: 17 % rejected the call; 14% also subsequently blocked the caller. For chats, 22% blocked the unknown user. However, 15% replied to the unknown contact via chat.

5.3 Findings of the mock-up tests

The UI mock-ups were used to get feedback on the intended design. Users were encouraged to criticize the design freely.

Fig. 2 shows the functions of the main UI. By clicking on an entry in the contact list, the details for that contact are shown. Online and offline contacts were visualized with different colors (green for online and gray for offline). Other information present in the main UI was: profile description (1), profile preview (2), dial pad (3), visibility status (4) and call filtering setting (5). The "Profile preview" was intended to show how the user's profile is seen by others (same for both Buddies and non Buddies). The visibility status could be set to either On, Away, Invisible or Off, and the call filtering setting controlled the acceptance of calls based on social distance (number of hops).

The main UI (Fig. 2) seemed understandable: Users were able to match the functions with the right buttons. Interpreting the colors for buddies in the contact list was easy. The buttons for calling, chatting and sending mail were also identified correctly by most users.

Use case 1 and 2: User calls and receives a call

The concept of making a call was well understood. When receiving a call from a non buddy, we provided a way for the callee to get more information about the caller: The callee was presented with a question mark button (Fig. 3) which could be clicked to reveal more information about the caller. Almost all users understood this. One user proposed the icon to be changed to a "magnifying glass", in order to show that it would lead you to more detailed information. Users who did not understand what it stood for, expressed the need for additional information. One user proposed clicking on the profile picture of the caller to get more info about him/her.

The additional information was based on the trust enhancing techniques we have developed that utilize social relationships[5]. As examples of these information displays, we presented mock-ups such as Fig. 4 or Fig. 5, showing how the user is related to the caller. The concept of displaying a common buddy was much liked and well understood by the participants.

Some users claimed they would answer the call independent of what information is shown of the caller. Unconcerned with privacy, they stated that accepting a call from a previously unknown person would depend on their mood and current activities. For others, more information seemed helpful for deciding whether to answer the call or not.

We wanted to know, what the optimal number of hops shown would be, and what number of hops would still increase the trustworthiness of the caller. Judging by the reactions to the mock-ups, it seems most users would not answer a call coming from a user further than one hop away: Four out of six users would answer only to a buddy of a buddy. One user would answer only to buddies' calls and one user would answer a call even within four hops. However, these imagined actions may differ from what would be done in practice.

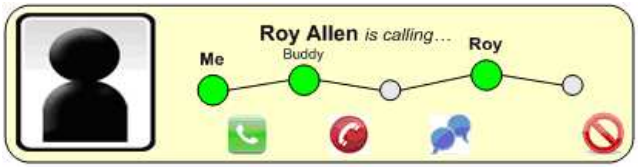

Figure 5: 3-hop connection with the caller

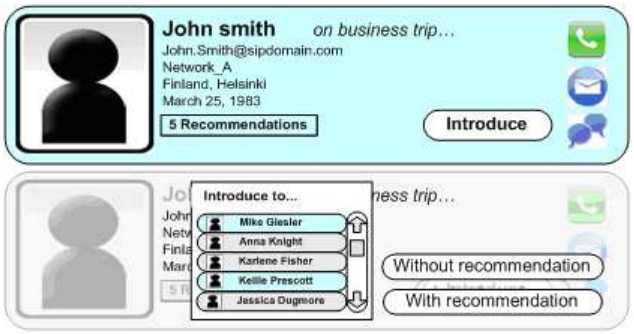

Figure 6: Introduction screenshots

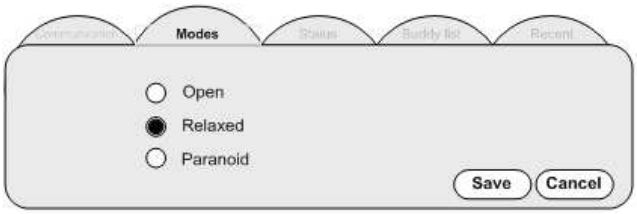

Figure 7: Modes

One user made an interesting suggestion for indicating your relationship to a person by adding a button showing a number to the user interface. The number would represent the number of common friends. Pressing the button would reveal a list of the common buddies. He further suggested that users could also prevent themselves from appearing on such lists through an option in the personal settings. Users should also be able to choose to be visible only as an anonymous "common buddy", without revealing their name.

Use case 3: Introducing a buddy

In our design, "introduction" (see Fig. 6) was possible only from a direct buddy to another buddy. The introductions could be done with or without recommendation. A recommendation (if given) could be freely formatted, and thus positive or negative.

The concept of introduction seemed easy to grasp. However the icon was misinterpreted by some. One user mistook "introduction" as a way to obtain additional information about the user; another user mistook it for an invitation to a chat session. The direction of the introduction was also misunderstood by one user: the user assumed that he would be introducing buddies to John Smith and not the other way around; in reality John Smith was being introduced. Finally, one user assumed introductions were possible only among buddies concurrently online, even though this was not the case.

Use case 4: Managing privacy settings

The default settings we displayed consisted of five parts: communication, modes, status, buddy list and recent (call log). The *modes* allowed the user to change the privacy mode, as described in Section 4. Although a new concept, most users understood that changing the mode was somehow related to security and privacy (Fig. 7). One participant mistook the modes to relate to emotional states and mood, believing that this would affect the layout and look of the profile.

6. CONCLUSIONS

Our results show that users do have an initial understanding of security in VoIP environments and the risks associated with it but work needs to be done to make managing security in P2P VoIP usable. Privacy is appreciated although often overlooked. P2P VoIP, operating by a different model than VoIP today, requires a different, user-controlled, approach to security. As it can be hard to understand the additional threats, there is clearly a need for new, usable, solutions. Our next step is to test the next, improved, version of the UI design.

7. REFERENCES

[1] M. S. Ackerman, L. F. Cranor, and J. Reagle. Privacy in e-commerce: examining user scenarios and privacy preferences. In *ACM Conference on Electronic Commerce*, pages 1–8, 1999.

[2] A. Adams and M. A. Sasse. Users are not the enemy. *Commun. ACM*, 42(12):40–46, 1999.

[3] D. Balfanz, G. Durfee, R. E. Grinter, and D. Smetters. In search of usable security: Five lessons from the field. *IEEE Security and Privacy*, 2:19–24, 2004.

[4] A. J. DeWitt and J. Kuljis. Aligning usability and security: a usability study of polaris. In *SOUPS '06: Proceedings of the second symposium on Usable privacy and security*, pages 1–7, New York, NY, USA, 2006. ACM.

[5] J. Heikkilä and A. Gurtov. Filtering spam in p2psip communities with web of trust. In Schmidt and Lian [11], pages 110–121.

[6] IETF P2PSIP WG.

[7] J. Koskela and S. Tarkoma. Simple peer-to-peer sip privacy. In Schmidt and Lian [11], pages 226–237.

[8] R. Moskowitz and P. Nikander. Host Identity Protocol (HIP) Architecture. RFC 4423 (Informational), May 2006.

[9] D. A. Norman. When security gets in the way. *Interactions*, 17, 2010.

[10] J. H. Saltzer and M. D. Schroeder. The protection of information in computer systems. In *Proceedings of the IEEE*, volume 63, pages 1278–1308. IEEE, 1975.

[11] A. U. Schmidt and S. Lian, editors. *Security and Privacy in Mobile Information and Communication Systems, First International ICST Conference, MobiSec 2009, Turin, Italy, June 3-5, 2009, Revised Selected Papers*, volume 17 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. Springer, 2009.

[12] A. Whitten and J. D. Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *In Proceedings of the 8th USENIX Security Symposium*, Berkeley, CA, USA, 1999. USENIX Association.

[13] K.-P. Yee. User interaction design for secure systems. In *In Proceedings of the 4th International Conference on Information and Communications Security*, pages 278–290. Springer-Verlag, 2003.