Usable and Secure P2P VoIP for Mobile Use

Joakim Koskela, Helsinki Institute for Information Technology HIIT, Helsinki, Finland
Kristiina Karvonen, Helsinki Institute for Information Technology HIIT, Helsinki, Finland
Theofanis Kilinkaridis, Helsinki Institute for Information Technology HIIT, Helsinki, Finland

ABSTRACT

The use of Voice over IP (VoIP) applications is relatively insecure and can involve a number of security threats and usability issues, potentially leading to loss of privacy. With the adoption of future peer-to-peer (P2P) communication systems the challenges grow even more as we need to rely on untrusted peers to access the service. The authors have developed a P2P VoIP system for mobile devices, which features techniques for improving the security and privacy of users in P2P networks. However, due to the fundamental differences in how the services are provided, the threats are not likely to be immediately understandable to the end users. Presenting these threats in an easy-to-use fashion can be quite challenging. The authors have sought to improve the usability of the emerging application by conducting iterative rounds of user interviews, questionnaires and usability testing with potential end users.

Keywords: Peer-to-peer, Privacy, Security, Usability, User Study, VoIP

INTRODUCTION

With the rapid spread of security breaches, information security has become of high importance to every user connected to the network. Spyware, worms, and other malicious software present daily threats to online users. New security mechanisms, methods and tools are constantly created to fight the problems. However, in order to really provide security and privacy for the end users, users need also be able to understand the threats and be able to use the security technology in a proper way. In practice, poor usability is often more detrimental to system security than the weaknesses in the underlying security mechanisms (Sasse and Flechais 2005). Currently, users are unable to use the technology appropriately: Users are unable to detect security indicators and demonstrate click fatigue when running into security warnings (Schechter et al 2005), and as Lampson (2009) put it, “the most common user model [on security] today is “Say OK to any question about security”. Even when a user sometimes does take the time to look at the security indicators and consider the warning, he may still fail to interpret and utilize this information correctly (DeWitt and Kuljis 2006). As the outcome, user may fall prey to relatively simple social engineering attacks (Balfanz et al 2004).

This is hardly news: As early as 1975, Saltzer and Schroeder added psychological acceptability as one of the basic requirements for a system to be secure (Saltzer and Schroeder 1975):

DOI: 10.4018/ijmhci.2015010102
It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user’s mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized. If he must translate his image of his protection needs into a radically different specification language, he will make errors.

Some 24 years later, in 1999, Adams and Sasse published a seminal paper on why users remained the weakest link in computer security (Adams and Sasse 1999). Furthermore, in 2005 Sasse and Flechais (2005) noted that an infamous hacker found hacking an often unnecessarily laboursome way to break a system’s security – an easier way was to fool a user to admit access. Since then, the work in trying to make security more usable has continued and steadily increased in volume year by year, yet the problem of enhancing usability of security without making security less strong seems to have remained a problem (Whitten and Tygar 1999; Yee 2003; Balfanz et al 2004).

Why is this so? One reason may be that the emerging applications seem to often just add a new layer to the existing problem. For example, the use of Voice over IP (VoIP) applications involves a number of security threats users are even less familiar with. Unsecured VoIP communication can be easily eavesdropped on and improper configuration and faults in client or server VoIP can expose personal information such as users’ passwords, buddy lists, and call records uncontrollably to unknown ears, and without user realising this information has been exposed. The exposed information can be used for malicious purposes: sending spam, identity theft, or social engineering (Zhang et al 2009).

To make matters worse, in peer-to-peer (P2P) VoIP systems the problems become even more tangible. 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 malicious peers to manage the system (see e.g. (Fessi et al 2010). Despite the risks, some users prefer VoIP for its easy availability, although it has not yet been thoroughly understood what makes up perceived quality in VoIP services (e.g. Chen et al 2012).

So, in order to protect against the additional dangers that the usage of P2P VoIP introduces, additional security is needed, and the new dangers and the tools to control the dangers - the additional security - need both be presented to the user in a way that is both understandable and usable. This is even more challenging with the demands and constraints of mobile use situation.

We are developing a secure P2P system for mobile VoIP communication similar to the work of the IETF P2PSIP working group (http://www. ietf.org/html.charters/p2psip-charter.html). It implements privacy protecting methods for P2P environments and utilizes technologies such as the Host Identity Protocol (HIP) (Moskowitz and Nikander 2006) to secure the communication and, if used properly, to minimize the risks involved. User studies were needed to understand how, when and what to communicate to the users about the novel security technology, and about the threats involved, and to see what could help them to understand and manage both the new technology and the new threats.

In this paper we provide a comprehensive look into the usability challenges of a P2P VoIP application with additional security features on a mobile device. We have gathered user feedback via interviews, an online questionnaire and a UI paper mock-up. We present and analyze the data gathered on users’ views and attitudes towards the emerging application and on Internet telephony in general. An early version of the implementation was demoed at Mobile Human-Computer Interaction 2010 conference (Koskela et al 2010), but the work is otherwise previously unpublished.

RELATED WORK

It is commonly believed that the challenges in making security usable markedly differ from the demands of so-called traditional usability
Related Content

Socio-Cultural Context of E-Government Readiness
[www.igi-global.com/article/socio-cultural-context-government-readiness/3997?camid=4v1a](www.igi-global.com/article/socio-cultural-context-government-readiness/3997?camid=4v1a)

Neighborhood Resource Center: The Library Partnership
Sol M. Hirsch (2012). *Partnerships and Collabortations in Public Library Communities: Resources and Solutions* (pp. 1-14).
[www.igi-global.com/chapter/neighborhood-resource-center/62320?camid=4v1a](www.igi-global.com/chapter/neighborhood-resource-center/62320?camid=4v1a)
Human Disposition and the Fraud Cycle
www.igi-global.com/article/human-disposition-fraud-cycle/75552?camid=4v1a

The Influences of Employees’ Emotions and Cognition on IT Adoption: Some Perspectives from Iran
www.igi-global.com/article/influences-employees-emotions-cognition-adoption/72886?camid=4v1a