A Survey to Guide Group Key Protocol Development

Ahren Studer
Dept. of Electrical and Computer Eng.
Carnegie Mellon University
astuder@ece.cmu.edu

Christina Johns
Dept. of Electrical and Computer Eng.
Carnegie Mellon University
cjohns@andrew.cmu.edu

Jaanus Kase
Dept. of Human Computer Interaction
Carnegie Mellon University
jkase@andrew.cmu.edu

Kyle O' Meara
Heinz School of Public Policy & Management
Carnegie Mellon University
komeara@andrew.cmu.edu

ABSTRACT

A large number of papers have proposed cryptographic protocols for establishing secure group communication. These protocols allow group members to exchange or establish keys to encrypt and authenticate messages within the group. At the same time, individuals outside of the group cannot eavesdrop on group communication or inject messages. However, group protocols are rarely used in the real world. In this work, we conducted a survey to help uncover why the general population ignores such mechanisms for group communication. We also tried to determine what protocols would best match subjects' current expectations for group protocols and methods for establishing trust. The survey indicated that a group protocol that leverages PKI or Web-of-Trust authenticated public keys and allows addition and deletion of members fulfills the majority of users' expectations.

1. INTRODUCTION

Group key protocols allow a number of individuals to securely exchange cryptographic keys or establish a shared key using an insecure medium (e.g., wireless or Internet connectivity). After forming a group, members can encrypt, decrypt, and authenticate messages to and from other members of the group. Provided secure underlying cryptography, anyone outside of the group cannot eavesdrop on the communication or inject a message that will successfully authenticate. Prior works on group protocols [3] often use examples of collaborating researchers at a conference to motivate their work. In addition, the general population also naturally forms groups to communicate about potentially secret information. Friends try to plan surprise parties. Business partners collaborate on new projects. A group of doctors may want to discuss a specific patient's condition. However, people rarely use group key protocols to secure their communication. The goal of this work is to uncover why "average users" do not use these protocols and to determine which protocols match users' mental models.

Prior work by Kuo et al. [3] analyzed group protocols with respect to different social requirements, but did not collect any end user data. Rather than postulating what users' want in a group key protocol, we use a survey to help gain insight into users' threat models and group interaction habits. To help answer the question of why users ignore group protocols, our survey was designed to help answer several subquestions about group communication: do people not worry about protecting their communication, do current protocols not provide the necessary group management functionality, and do people only meet in scenarios where these protocols are inapplicable (e.g., a protocol that uses infrared communication [1] ceases to work when individuals communicate over the Internet). Using subjects' responses, we can propose what type of group key protocols best match current users' practices.

2. DATA COLLECTION

To collect data about user's communication habits and how users manage groups and establish trust, we conducted a survey of end users ($n = 122$) using SurveyMonkey,[1] with advertisements on Online Carnegie Mellon Forums, Pittsburgh's Craigslist,[2] and the authors' blogs. To help encourage participation, we used a drawing of three $50 gift certificates.

2.1 Respondent Profile

We performed no screening and accepted any responses from individuals that completed the survey. More technically experienced users browse the advertising venues which biases our survey population towards more technically inclined individuals. Some questions on familiarity with various electronic forms of communication (email, email lists, chat, social networking sites, mobile messaging, and group pages) indicated that respondents used every technology (except group pages) frequently (on average at least once a day) and had "moderate experience" or were "very comfortable" with using the programs and their functionality. With such experience, our respondents include a larger number of users that may consider security as an issue when communicating online. A greater interest in technology also may bias respondents to try new technologies, such as security software, as opposed to average computer users that are slower to adopt new software or services and focus more on completing a task. However, we still see our survey respondents as a greater representation of the population as whole since prior works on group key protocols only considered how security researchers would manage groups.

[1] http://www.surveymonkey.com

[2] http://pittsburgh.craigslist.org/

2.2 Protecting Communication

To determine respondents' threat models and defensive actions, we asked participants if they thought others could access their communication and if so what steps they took to maintain privacy. 96% of respondents felt it was possible for others to access their communication. However, few respondents took appropriate steps to maintain secrecy. Only 15% claimed to use security software to maintain privacy of communication (e.g., PGP or Skype). A large portion of the respondents trusted servers to protect their information with 47% of respondents stating they would send a direct message to protect others from seeing it, 16% stating they relied on their passwords to keep information private, and 6% stating they used privacy settings. 7% of respondents limited what information they disclosed due to a lack of faith in electronic communication. 7% did nothing to protect their communication. The high number of respondents who trust others to protect their information and the relatively low number of people who use secure software indicates respondents' unwillingness to take additional steps to secure communication.

2.3 Managing Groups

To determine how users manage groups we presented respondents with a group scenario and asked how respondents would add or remove a member from an existing group. In current group key protocols, changes to the group often mean forming a new group. However, this does not agree with respondents' practices. When asked how to add a member to a group, 90% of responses indicated the preference to add the member directly rather than forming a new group. How respondents would handle removing a member from a group was situation dependent. In long lasting groups, such as business projects, 86% of respondents wanted to evict the unwanted group member. In short-term groups, such as planning a surprise party, 75% of respondents preferred to simply form a new group. These results indicate a group key protocol should at least accommodate addition to groups and that deletion is desired in some scenarios.

2.4 Establishing Trust

To determine how communicating parties establish trust, we asked respondents how they verified they were communicating with the right person online (e.g., check that an email address matches the individual from last weeks meeting). This is relevant to group key protocols because different protocols leverage different means for trust and eventually security (third party authenticated public keys, shared passwords, and location-limited channels). These were open ended questions and many respondents gave more than one technique so percentages do not add to 100%. 6% of participants checked that the other person possessed information that was not general knowledge. This type of verification via a challenge is similar to passwords (i.e., knowledge based authentication). The largest percentage (64%) leveraged third parties to verify an identity (e.g., checking for shared friends on social networking sites, browsing university directories, or searching corporate websites). Such trust in third parties corresponds to the use of public key based group protocols where some authority signs a certificate or friends sign public keys in a web-of-trust. 41% of respondents indicated they exchange business cards or email addresses in person to verify online identities. Such mechanisms correspond with the use of location-limited channels that require respondents to meet in person. Users can also leverage location-limited channels to exchange authentic public keys. If location limited channels were used to exchange public keys, groups could meet in person and use a public key based protocol. 85% of respondents indicated using trusted third parties or physical interaction to verify an identity. As such, the solution that would agree with the most respondents would be to use a public key based group protocol where users exchange public keys in person or utilize certificates from third parties to ensure the correct public keys were received.

3. SUGGESTIONS FOR GROUP KEY PROTOCOLS

Based on our findings, users will avoid adopting group key protocols unless users' views on security tools change and tools are better integrated and automated. However, the need for dynamic groups and users' trust in third parties and physical interaction present clear guidelines for group key protocols. Group protocols must allow adjustment of the group (addition and deletion). Respondents in current groups often add and remove members without thinking about reinitializing the group. Current groups seem to use a wide range of mechanisms to establish trust, but for a simple generalizable approach public keys appear to fit users' trust models. A large portion of users trust web services to identify online identities. In social networks, users frequently trust their friends to identify other individuals (a form of web-of-trust) and they trust the server to present those relations correctly. In other scenarios, users utilize corporate or academic directories to verify an online identity. These corporate or academic institutions could act as certificate authorities that would sign certificates to identify online identities when users do not meet in person. When users meet in person they can utilize location limited channels to securely exchange public keys (here the signature on the certificate is irrelevant since the key is received from the user and the communication channel ensures integrity). Once groups have exchanged public keys, a public key based protocols that allow addition and deletion of members [2, 4] present the best match to current users' habits and threat models.

4. REFERENCES

[1] D. Balfanz, D. Smetters, P. Stewart, and H. Wong. Talking to strangers: Authentication in adhoc wireless networks. Feb. 2002. Network and Distributed Systems Security (NDSS).

[2] Y. Kim, A. Perrig, and G. Tsudik. Simple and fault-tolerant key agreement for dynamic collaborative groups. In *Proceedings of the 7th ACM Conference on Computer and Communications Security*, pages 235–244. ACM Press, Nov. 2000.

[3] C. Kuo, A. Studer, and A. Perrig. Mind your manners: Socially appropriate wireless key establishment for groups. *Proceedings of First ACM Conference on Wireless Network Security (WiSec '08)*, Mar. 2008.

[4] M. Steiner, G. Tsudik, and M. Waidner. Key agreement in dynamic peer groups. 11(8):769–780, Aug. 2000.