Mind Your Manners: Socially Appropriate Wireless Key Establishment for Groups*

Cynthia Kuo Ahren Studer Adrian Perrig
Carnegie Mellon University
{cykuo, astuder, perrig}@cmu.edu

ABSTRACT

Group communication is inherently a social activity. However, existing protocols for group key establishment often fail to consider important social dynamics. This paper examines the human requirements for wireless group key establishment. We identify seven social and situational factors which impact group formation. Using these factors, we examine the requirements of four common classes of group communications. Each scenario imposes a unique set of requirements on wireless group key establishment.

Categories and Subject Descriptors

H.1.2 [**Models and Principles**]: User/Machine Systems

General Terms

Security, Human Factors

1. Introduction

Cryptographers dine at fine restaurants [5]. They compose poetry about the lives they have [10]. They thwart Mallory's middling attempts to launch a man-in-the-middle attack on Alice and Bob. Most importantly, modern cryptographers attend conferences and meetings. They collaborate with colleagues from different institutions. They share sensitive information.

All cryptographers can relate to attending a meeting and communicating with other members after the meeting. Not surprisingly, this scenario drives many group key establishment schemes. Is it a reasonable scenario? Undoubtedly, it possesses traits common to other groups.

*This research was supported in part by CyLab at Carnegie Mellon under grant DAAD19-02-1-0389 from the Army Research Office, and grants CNS-0627357, and CCF-0424422 from the National Science Foundation, and by the iCAST project, National Science Council, Taiwan under the Grants No. (NSC95-main) and No. (NSC95-org). The views and conclusions contained here are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either express or implied, of ARO, CMU, iCast, NSF, or the U.S. Government or any of its agencies.

WiSec'08, March 31–April 2, 2008, Alexandria, Virginia, USA.

However, the meeting scenario may lack features of other group communication scenarios. For example, human rights activists may need the ability to deny group membership, while cryptographers generally do not. College students may want to (quietly) opt out of their friends' illicit file trading activities, but academics rarely want to opt out of a grant proposal. Group communication is inherently a social activity, and social dynamics can differ dramatically from one situation to another. Existing group key establishment protocols often fail to consider relevant social dynamics, limiting their applicability to real-world communications.

In this paper, we first characterize the social aspects of wireless group formation and communication. Previous work focuses on the cryptographic aspects of protocol design. Next, we present four classes of common group interactions. Using these group scenarios, we analyze how the social aspects affect the design and selection of wireless group key establishment protocols. Protocols that are appropriate for one context may be inappropriate for other contexts.

This paper lays the groundwork for framing and developing user-centric wireless key establishment protocols. We will not propose a perfect solution which solves all of the issues we raise in this paper; one protocol cannot be appropriate for every situation. For some scenarios, combining existing protocols is a fine solution. For others, a good solution has yet to be developed.

2. Aspects of Group Formation

We identify seven group characteristics that impact the design of key establishment protocols. This list is not comprehensive, and further work is required to truly understand the relevant factors. We assume that key establishment occurs when group members (and their devices) are physically present in the same location.

1. Group size. Most groups are composed of very few people. According to a classic article in the Harvard Business Review, groups of up to seven individuals are ideal for effectiveness. A group of ten is tolerable, and twelve is the maximum [8]. In this paper, we categorize groups of more than twelve people as large groups, and groups of twelve or fewer people as small groups.

Group size may limit key establishment protocols in two ways. First, key establishment must be completed quickly, before end users grow impatient. This caps the number of communication rounds of key establishment protocols. Second, group size dictates what types of user actions are acceptable. For example, touching one's device to all other members' devices is easy for a group of five, but impractical for a group of 20.

2. Device affordances. Device affordances are the "perceived and actual properties" of a device that govern how it can be used [13]. For example, a device with a keyboard affords the entry of alphanumeric characters.

For wireless group key establishment, the perception of device capabilities is extremely important. The use of infrared, Bluetooth, NFC, or 802.11 for key establishment can only be successful if end users *know* whether their devices possess the wireless capability. Key establishment will fail if users try to run the protocol without the necessary hardware and software.

Protocol designs are also constrained by device affordances. Since users do not tolerate inconvenience, key questions for protocol designers include: What hardware and software capabilities are available on users' devices? What actions are end users required to perform? How many actions are users willing to take? How much time does group key establishment take? How much time will users tolerate? If users establish keys with different types of devices, do all users perform the same actions? Would it make sense to delegate more work to more capable devices?

3. Robustness to error. Users are not programmable key establishment robots. For wireless group key establishment, common errors are wireless communication failures, human mistakes, or human actions which violate the protocol's assumptions. Examples of the latter include: neglecting to compare two strings with appropriate care; operating a device or its software in an unanticipated manner; and failing to verify that all the intended members of the group actually joined the group (and no others). Protocols often assume that users will always perform the right actions in the right way. In general, robustness entails that errors are detected – and ideally corrected.

4. Group structure. Security protocols for groups with a trusted leader (or leadership committee) differ from protocols for peer-to-peer groups lacking centralized, trusted authorities. A leader device(s) may be responsible for generating a shared secret, validating identity information, computing a key, making membership decisions, and so on. In a peer-to-peer group, each device in a group may be equally (un)trusted.

For key establishment, group members must determine which device (if any) will function as the protocol leader. If there is a leader, will all group members still perform the same actions? Can (or should) the work be delegated to the leader? Should the leader delegate some responsibilities to subleaders? Note that the device which assumes a leadership role during key establishment may not be owned or managed by the group's human leader(s). Also, the selection of a leader (or leader device) may be fraught with political implications; for some groups, the wisest choice is no leader.

After key establishment, there is the question of leadership for group maintenance.

5. Membership flexibility. Wireless group key establishment protocols often create a key by combining pieces of information from each protocol participant [9, 17]. They implicitly assume that all of the intended group members are present and that their devices are operational.

However, the circumstances of group formation, as well as the duration and nature of a group, may necessitate flexibility in the group's membership. What happens if an intended member's device is unavailable (forgotten, lost, fails to support correct software, battery dies, member is absent, etc.) during key establishment? What happens if the group's duration is long enough that new members want to join, or existing members want to leave? How many members need to agree before a member can be removed from the group? How many members need to agree before a member joins?

Group membership may also be role-based, particularly in the business world. For example, various individuals may rotate into a position to represent their organization at an external body (e.g., a standards group).

Finally, social norms dictate that people should be polite. Courteous behavior may introduce membership issues during group key establishment. For example, Alice, Bob, and Carol may form a group – ostensibly for file sharing – while Ophelia is sitting at the table. They feel obliged to invite her to join, but they do not want her to know that they also trade homework answers. At the same time, Ophelia may feel peer pressure to join the group. Ophelia suspects that Alice, Bob, and Carol trade homework answers and wants nothing to do with it. However, there is no way for her to politely refuse to join the group. For all parties, the ideal solution would be for Ophelia to "join" the group in such a way that a setup error or expiring key will not be discovered until a comfortable amount of time has passed.

6. Legality. The use of encrypted group communication cannot be separated from legal issues. Researchers have already noted that people switch communication media for security reasons [7]. People also switch communication media for documentation purposes. They send letters or email to record that information was communicated; they conduct conversations over the telephone so that no record exists of their exact words. In some contexts, provability is critical; in others, deniability is essential.

Group membership may be sensitive information. Provability or deniability of group membership may be important evidence for court cases. Provability and deniability are mutually exclusive properties.

7. Attacker assumptions. Existing wireless security protocols often judge themselves against the Dolev-Yao attacker model, which models a single communication channel. In this paper, we consider the entire system. For example, if the room is filled with untrusted individuals, a protocol should not rely on an out-of-band channel that can be observed by someone the room. We also touch on the threat of insider attacks against group communications.

3. Related Work

In reviewing the existing protocols for wireless group key establishment, we find that most lack meaningful consideration of the social and situational dynamics. Below, we discuss four classes of wireless group key establishment protocols, based on the mechanism which ensures secure communication: PKI, password entry, comparison of alphanumeric strings, and location-limited channel. Our evaluation is summarized in Table 1. We make some inferences, since many factors are not addressed in the authors' original work.

Note that this section only includes authentication mechanisms that explicitly accommodate wireless group key agreement. Schemes limited to pairwise key agreement or public key exchange are omitted.

3.1 Public Key Infrastructure

In PKI-based key establishment, each user has a public/private key pair and a certificate of the public key that is signed by a certification authority (CA). The CA is trusted by all users, and all users know the CA's public key. Numerous research papers have been published on this subject, e.g., [2, 4, 9, 16, 17]. Unfortunately, many of the assumptions underlying these protocols are impractical. Users may not have certificates. Even if they do have certificates, users may not trust the CA certifying other users' keys.

Moreover, these approaches are not secure against *group-in-the-middle (GitM)* and Sybil [6] attacks. In a GitM attack, a malicious member splits the legitimate members into at least two groups. To form a group with the correct number of members, the attacker must know the private keys of other users who are not present. During key establishment,

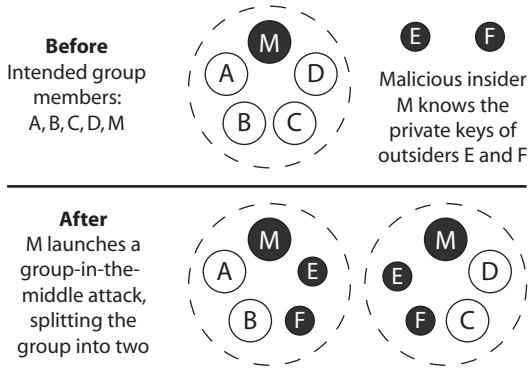

Figure 1: Example of a Group-in-the-Middle Attack

the attacker impersonates these users. For example, suppose five individuals initiate group key establishment, and the malicious user can impersonate two other users. The attacker creates two groups of five members; each group is composed of two legitimate members, the attacker, and two impersonated members. This example is illustrated in Figure 1. If the legitimate users do not verify the other members' certificates (e.g., the task is delegated to the attacker), the attacker controls the majority in each group.

In a Sybil attack, a malicious user would simply impersonate additional users and add them to the current group. To prevent this attack, the legitimate members need to verify the total number of group members. Unfortunately, such a counting protocol can be tricky for humans to perform reliably, especially in large groups.

Group size. In contributory key agreement mechanisms, the required number of communication rounds is logarithmic in the number of participants [9], while some protocols are linear in the number of participants [17]. A low number of communication rounds is especially important as the group size increases.

Device affordances. Besides wireless communication interfaces, no special hardware is necessary.

Robustness to error. From the user's perspective, key agreement happens automatically . Such transparency makes it difficult for users to detect protocol failures, such as the GitM and Sybil attacks mentioned above.

Group structure. Most protocols automatically elect a group leader, either based on resource availability or based on deterministic selection (e.g., the node with the lowest id).

Membership flexibility. Protocols in this category provide mechanisms for member addition and deletion. Members can obtain special roles based on certificates. Unfortunately, no provisions for politeness exist or were considered by protocol designers.

Legality. Members can prove group membership but cannot deny being members based on the asymmetric cryptographic primitives used.

Attacker assumptions. To join and participate in the group, an attacker must produce a valid certificate signed by a trusted CA and know the private key associated with the certificate. Assuming the CA verifies customers' identities before issuing a certificate, the protocols in this category defend against outsiders inside and outside of the room. There is no protection against insider attacks.

3.2 Password Entry

In password-based group key agreement protocols, users leverage a shared short secret to encrypt communication during key agreement [1, 2, 19]. This encryption is meant to provide a form of authentication such that only parties with knowledge of the password can properly encrypt data. If attackers can participate in a session, some of the protocols are no longer secure.

Group size. The proposed protocols are computationally inexpensive. Thus, group size is only limited by usability concerns. The probability that at least one user will incorrectly enter the password increases as the number of members increases. Since an incorrectly entered password causes the protocol to fail, the chance of a failed protocol run increases with group size. It is also more difficult for larger groups to keep the password secret in an untrusted environment.

Device affordances. Password entry protocols require an input mechanism for the password and an output mechanism for feedback during password entry. For most devices, this means a keyboard (or keypad) and screen.

Robustness to error. Group key establishment will fail safely if users enter the password incorrectly, neglect to perform a necessary action, or make other serious mistakes. Several protocols assume that users count and enter the correct number of expected members into their devices; counting may be an issue for large groups.

Group structure. Both Asokan and Ginzboorg and Valkonen et al. require a leader who acts as a hub for communication. In Abdalla et al., devices act as peers, sharing computation and communication responsibilities.

Membership flexibility. Valkonen et al. address some issues of group dynamics. The group leader acts as a gate keeper to authenticate new devices and provide them a copy of the key. Member expulsion requires the formation of a new group which excludes the undesired member.

With respect to politeness, none of the protocols allow a user to quietly "opt-out" or allow a device to participate without receiving the appropriate key.

Legality. The symmetric cryptographic functions underlying the protocols provides deniability, but prevents provability. Without digital signatures, a participant cannot attribute a message to a sender or prove a party was a member of the group.

Attacker assumptions. Password entry protocols may be vulnerable if attackers are in the room. They may be able to see the password if it is written down or hear the password if it is spoken. Assuming attackers outside of the room cannot acquire the password, key establishment is secure. There is no protection against insider attacks.

3.3 Comparison

Only Valkonen et al. [19] propose a comparison-based key agreement protocol for groups. A group establishes a shared key, and members compare a hash of the final key to detect if some members received incorrect values from outside parties.

Group size. As group size increases, comparison with each group member may become a burden. Users may simply check values with one or two other members who are physically proximate. An attacker performing a GitM attack could bisect the group if no members from the two subgroups compare values (i.e., one subgroup agrees on key K_A, the second subgroup agrees on key K_B, and the attacker knows both keys). This approach is inappropriate for large groups, especially if the room's layout divides the group.

Device affordances. All of the protocols require a display and a confirmation button.

Robustness to error. The comparison protocol is failsafe with respect to device errors, but may become vulnerable in the face of user errors. Users could claim the values are the same when they are different or claim the values are

	PKI	Password Entry		Comparison	Location-limited Channel	
	All	Asokan, Valkonen	Abdalla	All	Resurrecting Duckling	Talking to Strangers
Group Size						
Large (> 12)	Y	Y	Y	N	Y	?
Small (≤ 12)	Y	Y	Y	Y	Y	Y
Device Affordances						
User Action Required	N	Y	Y	Y	Y	Y
Hardware Required	-	Screen, Keyboard	Screen, Keyboard	Screen, Speakers, Keyboard	Physical Contact, Button	Location-limited Channel, Button
Robustness to Error						
Verification of Group Members (Users)	N	N	N	N	N	N
Detection of Protocol Errors (Devices)	N	Y	Y	Y	?	Y
Group Structure						
Leader during Establishment	Y	Y	N	Y	Y	Y/N
Leader for Maintenance	Y	Y	N	Y	Y	Y/N
Membership Flexibility						
Member Addition after Setup	Y	Y	Y	Y	Y	Y
Member Ejection after Setup	Y	N	N	N	N	N
Role-based Membership	Y	N	N	N	N	Y/N
Politeness Allowance	N	N	N	N	N	N
Legality						
Provability of Group Membership [1]	Y	N	N	N	?	Y/N
Deniability of Group Membership [1]	Y	Y	Y	Y	?	Y/N
Attribution of Messages to Sender [1]	Y/N	N	N	N	?	Y/N
Attacker Assumptions						
Defends against Attacker in Room	Y	N	N	Y	Y	?
Defends against Attacker Outside of Room	Y	Y	Y	Y	Y	Y
Defends against Insider (Attacker as Member)	N	N	N	N	N	N

Legend for table values:
'Y' denotes property is supported
'N' denotes property is not supported
'Y/N' denotes support for the property depends on the implementation
'?' denotes property value is unknown
'-' denotes property value is not applicable
[1] Relative to outside parties (i.e., non-group members)

Table 1: Properties of Wireless Group Key Establishment Protocols

different when they are the same. If the values are different, users may simply ignore the discrepancy and assume it is a device malfunction. Uzun et al. discovered that user error rates on pairwise comparison protocols may be as high as 20% [18].

Group structure. A leader mediates the broadcast of information. Devices broadcast one value before hearing from the leader and broadcast a second value after hearing from the leader.

Membership flexibility. A leader manages the addition of new devices. A new group must be formed to remove a device.

Legality. The comparison protocol's symmetric cryptographic functions provide deniability. Without digital signatures, a participant cannot attribute a message to a sender or prove a party was a member of the group.

Attacker assumptions. Valkonen et al. assume that users will count the number of intended group members and enter this number into their devices before key establishment begins. If this number is correct *and* group members diligently compare their hash values, the numeric comparison protocol defends against (outsider) attackers inside and outside of the room. However, there is no protection against insider attacks.

3.4 Location-limited channel

Location-limited key agreement protocols rely on physically-limited communication mediums to ensure an attacker cannot access communication or is not within communication range. Only Resurrecting Duckling [14, 15] and Talking to Strangers [3] have been extended from pairwise key establishment to group scenarios.

The Resurrecting Duckling protocol [15] leverages a direct physical connection between devices for key setup. In the protocol, a mother duck (i.e., group leader) defines and distributes a key to the ducklings (i.e., the other members of the group). During setup, a policy is uploaded. The policy specifies what actions a duckling will take.

With Talking to Strangers, Balfanz et al. [3] use demonstrative identification over a location-limited channel (e.g., infrared or NFC [12]) to exchange authenticated public keys. Group members may use a broadcast-capable location-limited channel to commit to their public keys. The authenticated keys can then be used in conjunction with an implementation-specific group key establishment protocol.

Group size. Group size is limited by the usability constraints. In Resurrecting Duckling, each device must make physical contact with the mother duck. Thus, the mother duck is a bottleneck for group formation, and key establishment may be cumbersome for large groups. In Talking to Strangers, the location-limited channel constrains the area in which key establishment can occur. Large groups may not be able to fit all of their device within a small area.

Device affordances. For both protocols, devices must support additional communication mechanisms, such as electrical contacts, infrared, or NFC.

Robustness to error. Location-limited channels provide physical assurance that the intended group members joined the group. However, it is unclear whether users will be provided with an interface to confirm the group roster. If not, the protocols may be vulnerable to a Sybil attack.

Group structure. The Resurrecting Duckling requires a leader (i.e., mother duck) for operation. The mother duck establishes the initial key and policies in devices, adds new devices to the group, and creates a new group to eject a device. Talking to Strangers can operate with or without a leader. Once devices have exchanged authenticated contact information, they can use their preferred group generation protocol (one with or without a leader). Depending on the final key(s) used for communication, a leader may be needed to manage members.

Membership flexibility. In Resurrecting Duckling, the mother duck has the authority to add or remove members from the group, either personally or through delegation [14].

If a group leader is present in Talking to Strangers, she authenticates the joining member over the location-limited

channel and sends the group key to the new member over wireless. The leader distributes a new group key to remove a member. If there is no group leader, a new member picks a random member and authenticates itself to the existing member using the location-limited channel. The existing member sends the group key to the new member.

Neither protocol allows devices to politely opt-out or to silently exclude members from the group.

Legality. The legal properties of the protocols depend on the keys used. If a group leader can act as a certificate authority which parties both in and outside of the group trust, members can have provability of group membership and attribution of messages to the sender. If symmetric keys are used, or the certifying authority is untrusted outside of the group, group members can achieve deniability.

Attacker assumptions. With Resurrecting Duckling, an attacker cannot join the group without touching the mother duck. With Talking to Strangers, any attacker must be outside of the range of the location-limited channel; it is possible that an attacker in the room may be within range. Neither scheme protects against insider attacks.

4. Example Scenarios

In the previous section, we discussed seven factors which influence the design of a wireless group key establishment protocol. To illustrate their effect, we present the following four classes of scenarios. These classes are not comprehensive. However, they capture the essence of common – but dissimilar – group situations. Due to space limitations, we only discuss the salient characteristics of each scenario below. Table 2 summarizes the desired properties of group formation for each scenario.

4.1 Business Collaboration

Users. Typical users are members of cross-organizational groups, such as business coalitions, standards bodies, and trade associations.

Salient Characteristics. Membership in business collaborations is often fluid. New members may join, and existing members may leave. Coalitions may grow to 20, 50, or even 100 members. Group membership is also role-based, since the membership belongs to an organization and not to its representative. Organizations may rotate employees in and out of a group.

The purpose of cross-organizational collaborations often involves exchanging sensitive data. Secure setup is critical. There is usually a group leader who manages key establishment and group maintenance. The responsibilities of leadership may rotate through different members.

Business meetings often occur in conference rooms. It is reasonable to expect that intended group members are the only people in the room and that some infrastructure, such as a whiteboard or chalkboard, is available.

Prior work. This class of scenario includes academic conferences and meetings. Thus, the major issues have been addressed by prior work. A password entry protocol for group key establishment with signatures over the messages and the corresponding certificates may be used to verify members' physical presence during key establishment and their [members'] identity.

In business settings, members may not know all of the other members in the room; certificates alone may fail for proper group member identification. However, certificates aid in group management. The certificate should verify the member's identity and their role in the organization. This aids the support of role-based membership. To replace an existing group member, an organization provides a certificate documenting a similar role for the new representative.

	Business Collaboration	Contract Negotiation	Acquaintances, Friends, Family	Underground Activity
Group Size				
Large (> 12)	Y	-	-	Y
Small (≤ 12)	Y	Y	Y	Y
Device Affordances				
User Action Required	Y	Y	Y	Y
Hardware Required	-	-	-	-
Robustness to Error				
Verification of Group Members (Users)	Y	Y	Y	Y
Detection of Protocol Errors (Devices)	Y	Y	Y	Y
Group Structure				
Leader during Establishment	Y	N	-	-
Leader for Maintenance	Y	N	-	-
Membership Flexibility				
Member Addition after Setup	Y	N	-	Y
Member Ejection after Setup	Y	N	-	Y
Role-based Membership	Y	N	N	-
Politeness Allowance	N	N	Y	N
Legality				
Provability of Group Membership [1]	-	Y	-	N
Deniability of Group Membership [1]	-	N	-	Y
Attribution of Messages to Sender [1]	-	Y	-	N
Attacker Assumptions				
Defends against Attacker in Room	-	Y	-	Y
Defends against Attacker Outside of Room	Y	Y	-	Y
Defends against Insider (Attacker as Member)	N	N	N	Y

Legend for table values:
'Y' denotes property is desirable for group type
'N' denotes property is detrimental for group type
'-' denotes desired property value does not matter or depends on context
[1] Relative to outside parties (i.e., non-group members)

Table 2: Properties of Group Scenarios

To defend against an insider GitM attack, the certificates gathered during group key establishment should be compared to a physical roster of meeting attendees.

4.2 Contract Negotiation

Users. This class applies to individuals and organizations who need to verifiably document exchanges of information, generally for legal reasons.

Salient Characteristics. For legal reasons, it is important that group membership can be proved to outside parties. In addition, outside parties must be able to attribute messages to the originating sender.

Common techniques for obstructing negotiations include switching representatives and sending representatives who lack decision-making authority. For this discussion, we assume that group key establishment will only occur if all parties are serious about the negotiation. Thus, the intended group members are present during key establishment, and the membership should not change. It is likely that the group dissolves after the negotiation is complete.

The security requirements during wireless group key establishment are high; members must be confident that the intended members joined the group and no others. As a result, a less convenient setup mechanism may be tolerated.

Finally, negotiating parties are sensitive about issues of control and power. To avoid the perception that one member has more power, key establishment should occur in a peer-to-peer fashion (i.e., without a group leader).

Prior work. Talking to Strangers is ideal for this class of communication. First, tractable negotiations often involve a small number of parties. Second, the location-limited channel forces people to bring their devices close together, similar to a handshake. Symbolically, it helps emphasize that there may be legal ramifications.

Like the business collaboration, the contract negotiation

assumes that group members belong to an organization which issues certificates. However, the purpose of the certificates is to support provability of group membership and attribution of messages to the sender.

To ensure that all the intended members (and only the intended members) have joined the group, the devices display basic certificate information for the users to check. If the list is correct, the devices verify the certificates. Once that occurs, a group key is established. Finally, any messages sent within the group must be signed by the member's private key and encrypted with the group key.

4.3 Acquaintances, Friends, and Family

Users. We include two types of users: casual acquaintances, who may be untrusted; or friends and family with whom users establish long-term relationships.
Salient Characteristics. User convenience during key establishment is crucial; users will not invest time or effort in secure setup.

The trappings of polite social behavior are likely to appear in this class of interaction. For casual acquaintances, group members may reason that it is no harm in "playing along" during group formation. In a friends and family relationship, users may feel compelled to join out of respect for the relationship. For this reason, members may want deniability of group membership to outside parties.
Prior work. No prior work addresses politeness.

4.4 Underground Activity

Users. This class of activity is appropriate for human rights activists, repressed populations, government spies, criminals, and others who wish to communicate sub rosa.
Salient Characteristics. Groups in this class operate and communicate in a clandestine fashion. Thus, deniability of group membership and message origin is crucial. In addition, the security requirements surrounding key establishment are very high, and errors are not tolerated. Any member should be able to initiate re-keying.

For survivability purposes, some groups may prefer a structure without a group leader for maintenance. Some combination of members may add new members or remove existing members.
Prior work. Deniability of group membership is difficult if members' cryptographic keys can be located. After key establishment, a steganographic scheme, such as StegFS, is needed to hide group-related information [11].

Numerous group key establishment protocols, such as those which use numeric comparison or location-limited channels, could be used to create a shared group key. Until devices are universally equipped with location-limited channels, underground groups may avoid using location-limited channels to avert suspicion. Numeric comparison is effective, but individuals may miscount the number of intended members. A secure, error-proof method for counting is needed.

The most troublesome aspect of this scenario is the potential for malicious insiders. An inside attack can occur if an attacker is invited to join the group as a legitimate member; if an existing member is corrupted; or if a member's device is compromised. Existing protocols do not defend against insider attacks because it is difficult to ascertain a person's intention.

5. Conclusion

In this paper, we identify seven social and situational aspects of wireless group key establishment: group size, device affordances, robustness to error, group structure, membership flexibility, legality, and attacker assumptions. We also discuss four common scenarios for group communication, which show that wireless group key establishment protocols do not handle the intricacies of human behavior outside the workplace.

This work demonstrates that protocol designs are situation dependent. We hope that the community will embrace this framework to develop socially acceptable, user-centric technologies for wireless key establishment.

6. Acknowledgments

We thank Jesse Walker for his insightful feedback.

7. References

[1] M. Abdalla, E. Bresson, O. Chevassut, and D. Pointcheval. Password-based group key exchange in a constant number of rounds. In *Public Key Cryptography (PKC)*, 2006.

[2] N. Asokan and P. Ginzboorg. Key-agreement in ad-hoc networks. *Computer Communications*, Nov. 2000.

[3] D. Balfanz, D. Smetters, P. Stewart, and H. Wong. Talking to strangers: Authentication in adhoc wireless networks, Feb. 2002.

[4] M. Burmester and Y. Desmedt. Efficient and secure conference key distribution. In *Security Protocols—International Workshop*, Apr. 1997.

[5] D. Chaum. The dining cryptographers problem: unconditional sender and recipient untraceability. *Journal of Cryptology*, 1988.

[6] J. R. Douceur. The Sybil attack. In *Workshop on Peer-to-Peer Systems (IPTPS)*, Mar. 2002.

[7] P. Dourish, E. Grinter, J. D. de la Flor, and M. Joseph. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal Ubiquitous Computing*, 2004.

[8] A. Jay. How to run a meeting. *Harvard Business Review*, 1976.

[9] 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*, Nov. 2000.

[10] L. Marks. The Life that I Have. In *Between Silk and Cyanide*, page 497. Touchstone, 1998.

[11] A. D. McDonald and M. G. Kuhn. Stegfs: A steganographic file system for linux. In *Information Hiding*, 1999.

[12] NFC Forum. NFC Forum: Specifications. `http://www.nfc-forum.org/specs/`.

[13] D. Norman. *The Design of Everyday Things*. Basic Books, New York, 1988.

[14] F. Stajano. The resurrecting duckling - what next? In *Revised Papers from the 8th International Workshop on Security Protocols*, 2001.

[15] F. Stajano and R. J. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In *Security Protocols Workshop*, 1999.

[16] D. Steer, L. Strawczynski, W. Diffie, and M. Wiener. A secure audio teleconference system. In *Advances in Cryptology – CRYPTO '*, 1988.

[17] M. Steiner, G. Tsudik, and M. Waidner. Key agreement in dynamic peer groups. *IEEE Transactions on Parallel and Distributed Systems*, Aug. 2000.

[18] E. Uzun, K. Karvonen, and N. Asokan. Usability analysis of secure pairing methods. In *Usable Security (USEC)*, Feb. 2007.

[19] J. Valkonen, N. Asokan, and K. Nyberg. Ad hoc security associations for groups. In *Security and Privacy in Ad-Hoc and Sensor Networks (ESAS)*, 2006.