Usable Key Agreement in Home Networks

Ramu Panayappan, Tom Palarz, Lujo Bauer and Adrian Perrig
CyLab / Carnegie Mellon University. {pramu, tpalarz, lbauer, perrig}@cmu.edu

***Abstract*—With the rapid emergence of new home networking technologies and proliferation of devices that use them, innovation has focused on rich functionality and largely ignored the associated security threats. The heterogeneous set of home appliances, their varied communication mediums, the lack of any ubiquitous standard to manage the communication across these devices, and the lack of a skilled security administrator all pose significant new challenges in securing these networks.**

In this work, we identify security challenges and considerations that are unique to home networking and take a first step toward solving one of the key security issues—key establishment. We describe a simple, secure and user-friendly solution to handle the special case of a device rejoining its home network after a brief absence. Our approach serves as a basic building block to ensure security and privacy in a home network.

***Index Terms*—Home Networks, Security, Key agreement**

I. Introduction

The landscape of home networks is undergoing a rapid and dramatic shift. In the early 1990s, home networking was typically limited to a couple of personal computers connected via a local area network within the home. Today, this landscape is considerably more complex. Many homes are inhabited by multiple desktop and laptop computers, digital video recorders, portable or streaming media players, game consoles, etc., all communicating via a variety of different protocols.

The home of the future will be even more complex. The number and types of devices will increase, with smart appliances like Internet-connected refrigerators and microwaves, home automation and security systems, and remote-controllable sensors and switches becoming commonplace. The methods and protocols by which these devices interact will also change. Today, many of the devices within the home (e.g., the components of a home automation system that controls lights, shutters, motion sensors, and alarms) interoperate only selectively and via application-specific protocols like X10 [1], Insteon [2], or Home RF [3]. Future home networks, on the other hand, will be characterized by more high-level, application-agnostic modes of interaction such as is made possible by UPnP [4], Jini [5], or HNAP [6]. This will make possible vastly greater interoperability between devices, resulting in home networks that transparently combine consumer electronics with mobile and traditional computing devices to provide greater functionality and convenience [7].

With these, however, will come the potential for abuse if home networks are not designed with security in mind at the forefront. Though reusing tried and tested solutions and approaches has great value, we believe that solutions to secure home networking warrant special attention and will involve a different set of approaches than those used in other environments. For example, traditional security solutions used in the enterprise are often heavyweight and too difficult for the typical home user to manage [8]. Enterprise security solutions usually assume strong threat models, since enterprises often possess valuable data attractive to attackers (e.g., collections of millions of credit card numbers) and the effect of successful attacks can be devastating (e.g., confidential product plans and business strategies can be leaked to rivals). Enterprise solutions typically assume that a trained security administrator or team of administrators will manage servers and protocol configurations.

Security and privacy are key pieces of the home networking puzzle. Home networks already hold much information, like tax records or treasured family photos, that consumers want to feel is not at risk of theft or deletion. Future home networks will

additionally include many devices that are privy to the private details of our daily lives, for example, light switches and motion sensors, security cameras, and Internet-enabled refrigerators with shopping lists. As has recently been seen with social networking applications and mobile phones [9], [10], this information is an attractive target for stalkers and can often be used to infer much more about people's movements and details of their private lives than is immediately obvious from the collected data. Finally, a home is a place of comfort and refuge, and, as such, consumers need to be confident that the devices and technologies they use in their homes cannot be used against them or to other malicious or mischievous ends.

This paper discusses mechanisms for enabling secure home networking. Section II points out some of the unique characteristics of home networks and why traditional IT security solutions are inadequate. Section III discusses requirements for a complete solution to the secure home networking problem. In Section IV, we present a first step toward solving one of the key problems in home networking—key agreement. In particular, we present a user-friendly scheme that enables devices returning to the home network after a short absence to join the network seamlessly. The details of the scheme are described in Section V and the solution is analyzed in Section VI. We conclude with a review of related work.

II. Unique Characteristics of Home Networks

Many traditional IT security solutions cannot be directly applied to home networks. The salient characteristics that distinguish home networks from other networked systems include the following.

1) **User skill:** Most people in the home do not have training for security administration. However, it is desirable to allow them to perform some level of administration and control over their network. Examples include setting parental controls on the television or liquor cabinet and informing the home network of a lost or stolen device. Performing these types of tasks should not be a burden or hinder the user from utilizing the home network.
2) **Heterogeneity:** As discussed in the previous section, home devices differ from each other in terms of underlying medium used for connectivity, the power required, battery lifetime, the processor speeds, available memory, etc. One of the key challenges in designing a suitable security solution is that these devices also do not have the same way of allowing the owner to interact with them. They vary in both their input capability (ranging from a full-fledged keyboard to a single button or switch) and output capability (from a color screen to a single LED).
3) **Scale:** The number of nodes in a home network is significantly smaller (sometimes by orders of magnitude) than in most corporate networks. This could not only allow us to design simpler solutions but may also allow us to revisit solutions that were rejected because they did not scale sufficiently well. For instance, solutions like the web of trust [11] to provide authentication or manual keying to bootstrap the devices' keying information may not seem a scalable solution for the Internet, but could serve as potential solutions in a home network.
4) **Ownership:** Nodes in a home network are tightly coupled with their owners. In most cases there will be a single, easily identifiable principal owner or primary user of a device, e.g., as with a cell phone. In other cases, such as a video game console, there may be two or three people that share it equally.
   Users other than the owner, e.g., guests, may need to be granted temporary access to devices in the home network. It may be desirable for such accesses to be granted at different levels of granularity, as some guests (such as friends of family) will be more trusted than others (such as a TV repairman).

III. Security Requirements for Home Networks

Manufactures and end users are more likely to embrace security solutions that heed the following practical considerations. Providing security should not greatly increase the cost of devices. Simple architectures that are easy to implement will aid in this. As it is plausible that many home network participants will be small, cheap devices with little spare computing power, it would be best if security solutions did not assume much computational power for cryptography [12]. A digital lock on the liquor cabinet should be better than a simple physical key and lock. In other words, it should be simple, provide added value, and not be over-engineered.

In addition to the above practical considerations, a security solution should have the following properties.

- **Secure naming service:** Means by which the home devices can be identified by the home users. This would include running a name service securely that would manage the names of the home devices irrespective of the underlying communication medium. This is needed to help prevent impersonation of devices and users.
- **Secure bootstrapping:** Means by which security-enabled devices bootstrap trust in the home network when no secure network is in place. This would include secure means to detect devices and authorize them to form a secure home network. Since home networks are likely to use a shared and easily accessible communications medium such as wireless, special care needs to be taken so that adversaries cannot compromise security at manufacturing time [13] or when the network is established. Thus, solutions like that assume absence of an adversary at these times (e.g., [14]) would not be suitable.
- **Secure join:** Means by which a device joins the already established secure home network. This would include detection of the new device and authorizing it to join the existing home network. Also, the newly joined device should not be able to learn anything about the network prior to the time of joining. This property is usually referred to as *backward secrecy* [15].
- **Secure leave:** Means by which the secure home network learns about a home device leaving the network. The device could have left the network because it was lost/stolen or because it is a mobile node. The device that left the network should not be able to learn anything about the network from then onwards. This property is usually referred to as *forward secrecy*.
- **Secure partition/merge:** This is a special type of join and leave where multiple devices leave the home network together and join it together. This could be triggered, e.g., by a member (or group of members) of the household going on vacation and wanting her devices (mobile phones, tablets, gaming devices, etc.) to continue to communicate securely and then rejoin the network when she returns.
- **Secure rejoin:** Means by which the home network learns that a particular device trying to join the network was previously part of the network and was absent from the network for only a brief interval of time. This is necessary since many nodes will be mobile and entering and leaving the home throughout the day.
- **Multi-level access:** Means by which different levels of access are given to devices and people based on appropriate privilege. This is particularly common when a home owner would want to provide limited access to the devices of his guest for a brief period of time or to a television service technician who does not need access to other appliances in the home. This adopts the commonly accepted principle of least privilege.
- **Usability:** Means by which a home user could utilize the benefits of a feature-rich home network in a transparent manner and yet be assured that the interactions are secure. The home owner should be able to add devices to and remove devices from the home network with minimal inconvenience. The owner should not have to deal much with the crypto-

graphic keys that secure the network. Intuitive solutions assuming little or no administration skills of the user are most suitable (as in programming a garage door opener by just pressing two buttons at the same time). Design principles used to improve the user experience across different Bluetooth/Wi-Fi capable devices [16] can be adapted.

- **Remote access:** Means by which a mobile device, when away from the home network, can authenticate itself to the home network and interact with other home devices (to see how much milk is left in the refrigerator, for example).

We believe these security requirements, coupled with the properties of home networks discussed in Section II, suggest that significant progress needs to be made in addressing the following.

- **Automatic inference of access-control policies:** Means by which the home network could automatically infer the access-control policies pertaining to an individual without the home owner explicitly having to grant or deny access. For example, the manner by which the owner of the house greets a guest may be used to infer the level of access rights the owner would want to grant to that guest. This addresses the multi-level access requirement and doing it in an automatic fashion aids usability.
- **Ensuring privacy and integrity of message exchanges:** Means by which the messages exchanged between any two devices of a home network respect the privacy of the home owner. The dual of the problem is to ensure accountability of the devices to help identify malicious devices. This is closely related to the group secrecy properties of join, leave, and rejoin.
- **Key agreement:** Though key agreement in itself is not a requirement unique to home networks, special care must be taken to keep usability in mind and not hurt the consumer's experience. Key agreement serves as the basic building block for privacy and integrity and in fulfilling the bootstrapping, join, leave, and rejoin requirements. Multiple keys might be used to satisfy multi-level access.

Since key agreement is the cornerstone for many of the desired properties of a final solution, we attack this problem as a first step towards the goal of enabling secure home networking.

IV. A New Key Agreement Scheme for Home Networks

We believe that the majority of communications will occur in naturally forming groups (smoke sensors, multimedia devices, etc.). Also, the 'secure join' and 'secure leave' requirements of a home network, described in Section III, can be achieved by the 'join' and 'leave' properties of most group key agreement schemes. Thus, group key agreement schemes with appropriate re-keying would serve as a base solution for key agreement in a home network. Rekeying should be performed periodically (to prevent brute force attacks on static keys) and on any change in group membership [17].

Many of the existing group keying mechanisms efficiently handle adding members to a group or expelling them [18], [19], but to the best of our knowledge, the rejoin property (as defined in Section III) has not been explored. A contribution of our work is a novel technique for a member to rejoin the group by retaining some information from communications while a member of the group and by setting some reasonable time constraints on within how long it can rejoin.

A. Problem Definition

In this section we propose a key agreement scheme for secure home networks that would:

1) Allow devices to join the network while maintaining backward secrecy;
2) Allow devices to seamlessly leave the network while maintaining forward secrecy;
3) Leverage the fact that a returning device was previously part of the network to allow this device to seamlessly rejoin the network.

B. Solution Overview

We describe a generic solution to achieve the rejoin property on top of any of the existing group keying mechanisms. The basic idea behind the solution is that all the devices in the home network

agree on a group key and this key is used to encrypt communication between any two devices in the network. The main advantage of such a scheme over establishing pair-wise keys is that only one key needs to be stored at every device at a given instance. Also, devices that would want to broadcast or multicast messages within the home network can take advantage of this group.

On the flip side, the devices need to be aware of new devices joining the network and devices leaving the network. This is required because the group key has to be changed whenever these events occur to maintain forward and backward secrecy. Also, this approach assumes that all the devices in the network are trusted, as any device can eavesdrop the message exchanges between any two other devices.

C. Assumptions

The following are a few of the broader assumptions that were made in our solution to the key agreement problem. More specific assumptions will be pointed out in Section V as the pertinent details are provided.

- Several (at least 2) devices have storage capacity on the order of several megabytes. This is reasonable given the prevalence of personal computers and the low cost of digital storage.
- Devices can be uniquely addressed. Device discovery and addressing is an independent problem and we assume a solution to it exists.
- Devices are embedded or bootstrapped with private signing and encryption keys. The corresponding public keys can be obtained by external means. For instance, vendors can host a web portal that would provide the public key for a device given its serial number.
- Existence of a user interface to perform administrative tasks.

V. Details of the Solution

We will first describe the types of participants in the home network. The remainder of the section will describe how they interact in different scenarios.

A. Types of Nodes

- **Coordinators:** Coordinators are fixed nodes that have sufficient storage capacity. A computer or DVR are examples.
- **Mobile participants:** These nodes are ones that may leave and the network and attempt to rejoin it upon return.
- **Non-coordinators:** All fixed nodes that do not have sufficient storage capacity to function as coordinators, but do have some minimal storage.

B. Registering Nodes

When a new device is to be added to the network, the device name and the public signing key of the device are added to the coordinator. This may be accomplished by the user authenticating to the coordinator (as will be described in Section V-G) and typing in the hexadecimal representation of the public signing key. We believe this to be a reasonable approach given our previous observations regarding scale and manual keying; however, more user-friendly approaches are possible and preferable. Let this addition of device to the coordinator take place at time τ.

After the device is added to the coordinator, it then registers on the network by sending a REGISTER message containing the device's address, as provided by the naming service, and a public encryption key, all signed with the device's private signing key K_{sd}. This must be sent within time $\tau + \delta$. The user can cause the device to send the REGISTER message by actuating a master or enable switch on the device. The time δ is the time between the user adding the device to the coordinator and operating this switch, and may include, e.g., the user walking to a different room to access the new device if the device is not mobile.

We call δ the 'interval of vulnerability'. Within this interval, a malicious device could impersonate the device in question and assume its identity. It should be noted that this impersonation is not trivial, as the malicious node also would require the private key of the device to successfully register. However, as devices may have lifetimes of many years, it is

possible that a device's private key could eventually be compromised.

Upon successful registration, the coordinator encrypts the network's group key with the public encryption key of the new device and sends it to the newly registered device. The coordinator also stores the device name and address along with its public encryption and signing keys for future use. Depending on the underlying group keying mechanism, the rest of the devices in the network may also have to rekey the group key.

C. Node Operation

The network's group key is used to encrypt the messages that are exchanged between any two nodes in the home network.

Each node maintains a ring buffer for every other node. Thus, in an n node network, each node maintains $n-1$ ring buffers. Every time a node communicates with another node, it stores the hash of the message in the ring buffer. For each device, several (we suggest 3) of the most recent hashes are stored. Section V-E will discuss how these message hashes are used.

Since there will likely be only tens to low hundreds of nodes in a home network and each ring buffer is on the order of ≈ 60 bytes (assuming SHA-1 as the hash function), the amount of storage each node will have to dedicate to this will be on the order of tens of kilobytes, i.e., not a great burden on the node's resources.

D. Leaving the Network

We assume that appropriate mechanisms exist in the home network for any node to detect that a particular node has left the network. One such mechanism could be the use of heartbeats between the communicating nodes; loss of the heartbeat would imply a node has left the network.

Whenever a node A detects that node B has left the network, it announces to the network that node B has left. All the nodes in the network send to the coordinator their ring buffer for node B. The coordinator collects the ring buffers from all the nodes and stores them, along with the current group key and node B's public signing key. Along with these, the coordinator also stores a validity interval value (by default, 24 hours). Figure 1 shows the information that is stored by the coordinator when a mobile node B leaves the network. Node B also stores the last group key used when it was on the home network.

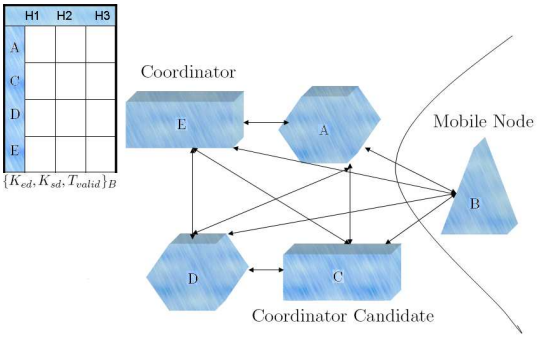

Fig. 1. Information stored by the coordinator when a device leaves network

The validity interval determines how long the device that has left can be away from the network before it will be forced to rejoin as a new member. The validity interval is configurable by the home owner and its choice depends on the following considerations.

- The interval should be long enough for most rejoins to happen within the interval, so that the user is not inconvenienced by having to register the nodes anew.
- The interval should be short enough for the device not to be accepted back to the network if it was sold or stolen and the user forgot to notify the coordinator of this.

This validity interval may provide a short window of opportunity for an attacker who has captured a device to rush to the home in which the device was a member of the home network and cause damage. This window of opportunity ϕ is the time remaining until the validity interval would expire. In many cases, the attacker will physically be far away from the owner's home and would also need to know the owner's address. However, in some cases the device may be sold to a neighbor or to someone who can reach the owner's home quickly. In those

cases, the owner may need to shorten the interval to a few minutes. In event of theft of a device, the owner can reduce the validity interval for that device to 0 so that the device cannot rejoin without human intervention. Similarly, the interval may be extended when the owner is going on vacation, for convenience. The default 24-hour interval should be sufficient in most cases—since a person will typically leave and come back home in the same day—and can be modified if the home owner would like stricter or more flexible security bounds.

E. Rejoining the Network

On rejoin, the node will send a REJOIN message along with its id and a nonce n_d to the network. The coordinator will then send a nonce n_c along with the MAC of the nonce n_d to the rejoining node. The MAC key K_{md} is computed by applying a pseudorandom or hash function to the group key that was stored when the rejoining node left the network. The rejoining node computes the same MAC key and verifies the nonce n_d. This assures the rejoining node that the coordinator is legitimate, i.e., that it is rejoining the right network.

It may be necessary to change coordinators while a mobile node is away from the home network. In this case, to maintain backward secrecy, the new coordinator is given this MAC key (rather than the group key) to authenticate itself to the mobile node.

The rejoining node will then create a signature using its private key over the saved message hashes that it has stored (in the order of node identifiers) and the nonce n_c and present it to the coordinator for re-entry. The coordinator will first check that the device has returned to the network within the validity interval and then verify the signature. The use of a challenge guarantees the freshness of the rejoin request. The use of message hashes as opposed to the actual messages not only saves space, but also preserves the privacy of the nodes' communications. A pre-image resistant cryptographic hash function guarantees that the original message can not be retrieved from the hashed messages.

If the signature verifies and the validity time interval is within bounds, the coordinator re-keys the group key of the network and the node rejoins the network seamlessly without involving the owner. The sequence of messages exchanged on a successful rejoin is depicted in Figure 2.

If the signature is not valid or the time interval is not within bounds, the owner should be notified to explicitly authenticate the device. In effect, a device presenting an invalid signature or rejoining after the validity time interval has passed is considered to be joining the network for the first time.

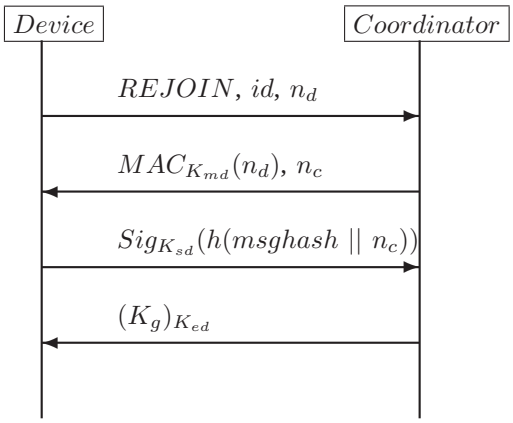

Fig. 2. Message sequence on successful rejoin

F. Issues with Selling or Removing Nodes

It is quite possible that an owner of the device would want to sell the device or remove the device from the network for reasons such as obsolescence.

Selling or removing a non-coordinator device is equivalent to the non-coordinator device leaving the network and the *validity interval* being made 0. It is the owner's task to inform the coordinator that a node has been sold or removed. The coordinator, in turn, can then mark the validity interval for that device as 0.

However, selling or removing a coordinator is a potential problem. For this reason, we propose that the coordinator be a rotating role, similar to a token ring. Whoever holds the current token acts as the coordinator for some reasonable time period. If a device is sold and leaves the network while it is serving in the coordinator role, then, when the network detects that the coordinator has left, the next node will step up and immediately acquire

the current token. As earlier, we assume appropriate means (like heartbeats) by which nodes detect that the coordinator has left the network. This serves two purposes. First, there is a clearly identifiable coordinator that the rejoining node responds to. Second, the network continues working without interruption when a coordinator is removed.

The assumption that there will always be multiple potential coordinators in a home network is a reasonable one. If, for example, the coordinator was the user's computer, then the owner will likely buy a new computer first before selling or removing her old one. Also, a home network is likely to contain multiple personal computers, any of which should be capable of acting as a coordinator.

G. User Authentication

As described earlier, for node registration or when a node cannot rejoin automatically, the owner will need to be involved. Other instances when an owner needs to be involved could include administrative tasks where the owner would want to inform the home network that a device is compromised and should be blacklisted, or if she is going on vacation and wants to adjust the validity interval. We assume that the coordinator would have sufficient I/O capabilities to allow interaction with the owner.

We propose that the owner be authenticated via a simple two-factor authentication mechanism consisting of a password (something you know) and a USB token containing authentication material (something you have). The owner inserts her USB token into the coordinator and types her password into the user interface. If both forms of authentication succeed, the user is given privileges to perform the desired tasks.

VI. Discussion

A. Salient features

Usability: The usability requirement is achieved, first, by reducing administration and details of the solution to simple and easy to understand scenarios (selling a device, going on vacation); and, second, by making the user interaction as infrequent as possible. We note that the usability and security are inversely related. The usability of the scheme we described in Sections IV and V is driven by the choice of δ and ϕ. δ describes the amount of time until the user activates the enable switch during a join and ϕ governs how long a device is allowed to be absent before a seamless rejoin. Higher values of δ and ϕ would imply greater usability, but reduced security, and vice versa.

Group secrecy: By providing a generic extension to the underlying group key agreement protocol, the scheme does not compromise group key secrecy. Group key secrecy [17] is the property that guarantees that it is computationally infeasible for a passive adversary to discover any group key. As the scheme uses an arbitrary group key agreement protocol effectively as a black box, the properties of that protocol are not compromised.

Resilience against impersonation: The scheme is also resilient against device impersonation. As described in Section V-E, by verifying that the coordinator possesses the correct MAC key K_{md}, the rejoining node is assured that it is running the protocol with a legitimate coordinator. Similarly, by verifying the hash of the most recent messages, the coordinator is also assured that it runs the protocol with a legitimate device. Any failure during this verification would result in the rejoin operation falling back on a normal join operation. Mutual authentication ensures that a malicious device that previously was not part of the home network cannot seamlessly join the network and that a foreign coordinator or malicious device impersonating a coordinator cannot to force a device to unwittingly join a different network. It should be noted that this resilience is achieved only if none of the nodes that are part of the home network collude with any node that has left the network.

By using two-factor authentication, the scheme is resilient against impersonation of the home owner. A malicious user would require both the password and the USB token to break into the network. This two-factor authentication also ensures that that the scheme is resilient against coordinator theft. The malicious user in this case will not be able to retrieve the keying material unless the password is also compromised or a brute-force attack can be mounted on the encrypted key material.

B. Limitations

Though this scheme meets most of the security requirements of a secure home network as outlined in Section III, it is not without limitations. The following are some of them.

- The scheme necessitates the existence of a master switch in all devices to trigger the registration of the device.
- As noted in Section V-B, there is a small interval of vulnerability if the private key of the device is compromised. Since the public-private key pair of the device is not refreshed and remains unchanged even when sold to other owners, this interval of vulnerability could be exploited.
- To address the issue of lost USB tokens, the scheme necessitates periodic backup of the USB tokens. Failure to make periodic backups may result in unavailability of the network if the owner loses his USB drive.

C. Prototype Implementation

We implemented a proof of concept of the key agreement scheme. A desktop computer was used as a coordinator. A surveillance camera (Axis 207MW [20]) and a PDA (Personal Digital Assistant; Nokia N800 [21]) were used as home devices. The prototype scenario involved the home devices registering to the computer and the PDA fetching images from the camera using the group key obtained using the LKH [18] protocol. An unregistered PDA trying to masquerade as a device that was previously part of the network was not able to rejoin the network or fetch the images from the surveillance camera. Leaving, rejoining, and other interactions between devices in the network that did not require user input did not impose any latencies that were observable to a user.

VII. Related Work

As securing home networks is an emerging area of study, very little research has been performed in this problem space. However, there has been significant amount of work in related areas. Al-Muhtadi et al. developed UIUC Sesame for smart homes [22]. This solution extends Kerberos and utilizes Jini [5] to provide confidentiality and integrity of communication between devices. However, unlike our solution, the authors neither address the compromise of the central node in Kerberos nor provide a means to authenticate other devices.

Cerberus is a multi-level authentication, authorization, and inference system for smart spaces [23]. Its flexible architecture allows for multiple authentication methods (such as key-cards, passwords, and iris scanners) for the varying needs in strength of authentication. However, Cerberus assumes a skilled security administrator to set the confidence levels for the different authentication levels and to set the policies for access to devices. As noted in Section III, these tasks are non-intuitive to the average home user and they requires greater administration skills than users in the home are likely to have. Also, Cerberus does not address key agreement or confidentiality and integrity of communications.

To augment the original UPnP [4] specifications, *security ceremonies*, which are like network protocols with computers, people or possibly the environment as participants, were introduced [24]. These ceremonies strengthen the access, discovery and notification protocols of UPnP to provide secure discovery, message integrity and secrecy with the help of a centralized security console. However, in addition to the known security flaws in UPnP [25], the ceremonies assume an expert user as an administrator to modify the ownership of each device. This user intervention increases for mobile nodes which frequently join and leave the network.

Another related technology is the proprietary Home Network Administration Protocol (HNAP) [6]. It builds on top of the standardized HTTP-SOAP protocol and is flexible and extensible. Though it provides better topology discovery, and better administration by programmability of the network devices, deploying HNAP requires skilled developers and testers. Unlike our solution, the protocol does not provide any sophisticated security measures other than simple MAC filtering and use of WEP/WPA. It is also not clear under this protocol whether a rejoin of network devices would be any different from joining a new device.

Windows Connect Now (WCN) technologies help create a secure wireless network in an user-friendly manner [26], [27]. WCN-UFD (WCN USB Flash Drives) [26] uses USB flash drives to transport network settings (network keying material) to the joining devices. WCN-NET [27] uses wireless access points as proxies to securely transport network settings. Neither of these schemes addresses the issue of securely and seamlessly rejoining the network. In addition, it would be difficult to deploy WCN-UFD in a home network as it requires every node to have a USB port—an assumption which may not hold for, e.g., tiny smoke sensors.

VIII. Conclusion

In this paper, we identified the unique characteristics of home networks and derived at the salient security requirements for a secure home network. We also proposed a key agreement mechanism that enables home devices returning to the home network within a short interval of leaving it to seamlessly rejoin the network without user intervention. The simplicity, usability and security of the proposed solution were analyzed and its limitations were noted. We hope that this paper represents a useful first step towards a secure and usable key agreement solution for home networks and will motivate future work in securing home networks.

References

[1] (2008, May) X10 industry standard. [Online]. Available: http://en.wikipedia.org/wiki/X10_(industry_standard)

[2] (2008, Nov.) Insteon - wireless home control solutions for lighting, security, HVAC, and A/V systems. [Online]. Available: http://www.insteon.net/

[3] (2008, May) HomeRF. [Online]. Available: http://en.wikipedia.org/wiki/HomeRF

[4] (2008, May) UPnP forum. [Online]. Available: http://www.upnp.org/

[5] (2008, Mar.) Jini network technology. [Online]. Available: http://www.sun.com/software/jini

[6] (2008, Nov.) Pure networks HNAP. [Online]. Available: http://www.purenetworks.com/partners/hnap.php

[7] (2008, May) Home automation. [Online]. Available: http://en.wikipedia.org/wiki/Domotics

[8] (2008, Dec.) Security risk analysis of enterprise networks. [Online]. Available: http://csrc.nist.gov/groups/SNS/security-risk-analysis-enterprise-networks/index.html

[9] R. Gross, A. Acquisti, and J. H. Heinz, "Information revelation and privacy in online social networks," in *WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society*. ACM Press, 2005, pp. 71–80.

[10] (2008, Jul.) Cell phone stalking. [Online]. Available: http://www.schneier.com/blog/archives/2007/06/cell_phone_stal.html

[11] P. Zimmermann, "Pretty good privacy user's guide," *Distributed with PGP software*, vol. I, Jun. 1993.

[12] F. Stajano and R. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks," in *Security Protocols, 7th International Workshop Proceedings*, 1999, pp. 172–194.

[13] (2008, Mar.) Virus from China the gift that keeps on giving. [Online]. Available: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/02/15BU47V0VOH.DTL&type=business

[14] R. J. Anderson, H. Chan, and A. Perrig, "Key infection: Smart trust for smart dust," in *ICNP*, 2004, pp. 206–215.

[15] M. Steiner, G. Tsudik, and M. Waidner, "Cliques: A new approach to group key agreement," *International Conference on Distributed Computing Systems*, pp. 380–387, 1998.

[16] C. Kuo, J. Walker, and A. Perrig, "Low-cost manufacturing, usability, and security: An analysis of Bluetooth simple pairing and Wi-Fi protected setup," in *Usable Security (USEC'07)*, Feb. 2007.

[17] Y. Kim, A. Perrig, and G. Tsudik, "Simple and fault-tolerant key agreement for dynamic collaborative groups," *ACM Conference on Computer and Communications Security*, pp. 235–244, 2000.

[18] D. M. Wallner, E. J. Harder, and R. C. Agee, "Key management for multicast: Issues and architectures," internet Draft (work in progress), draft-wallner-key-arch-01.txt, Internet Engineering Task Force (September 15, 1998).

[19] M. Steiner, G. Tsudik, and M. Waidner, "Diffie-Hellman key distribution extended to group communication," in *Proceedings of the Third ACM Conference on Computer and Communications Security*, Mar. 1996, p. 7.

[20] (2008, Feb.) Axis Communications - Axis 207MW network camera. [Online]. Available: http://www.axis.com/products/cam_207mw/

[21] (2008, Mar.) Nokia Nseries N800. [Online]. Available: http://www.nseries.com/products/n800

[22] J. Al-Muhtadi, M. Anand, M. D. Mickunas, and R. Campbell, "Secure smart homes using Jini and UIUC SESAME," in *16th Annual Computer Security Applications Conference*, 2000, p. 77.

[23] J. Al-Muhtadi, A. Ranganathan, R. Campbell, and M. D. Mickunas, "Cerberus: A context-aware security scheme for smart spaces," in *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications (PerCom 2003)*, Mar. 2003, pp. 489–496.

[24] C. Ellison, "UPnP security ceremonies design document," *UPnP Forum*, Apr. 2003.

[25] Y. Goland. (2008, Jul.) UPnP security flaws. [Online]. Available: http://www.goland.org/upnp_security_flaws/

[26] "Windows Connect Now - UFD For Windows XP," Microsoft Inc, Technical Specification.

[27] "Windows Connect Now - CNET," Microsoft Inc, Technical Specification.

[28] C. Ellison, "Home network security," *Intel Technology Journal*, vol. 6, no. 4, Nov. 2002.