

Usable Security in Smart Homes

Saad Shakhshir and Dimitris Kalofonos, Member, IEEE

Nokia Research Center,

Burlington, MA, USA

saads@mit.edu dimitris.kalofonos@nokia.com

Abstract—A number of technologies are emerging that enable the creation of “Smart Homes”, which are households containing numerous networked devices all interacting with each other over the home network. As these Smart Homes become increasingly prevalent and users become more reliant on mobile devices to handle sensitive information, research related to the development of a usable security framework for Smart Homes is increasing in importance. In this paper, we first give some of the motivating use cases for such a security framework. We then describe some of the design challenges presented by the creation of usable Smart Home security frameworks. With an emphasis on usability, we proceed to highlight the hardships users face when interacting with currently available security frameworks and substantiate the need for a significant improvement in this field. Finally, we summarize and conclude.

Key words: Smart Home, home networking, security, usability.

1. INTRODUCTION

Traditionally, computer security has been a high priority only for entities dealing with extremely sensitive data, such as the military, the government, and banks. Information Technology (IT) experts in each individual branch or institution were able to configure and manage their own internal security mechanisms. However as consumer devices become smaller and more powerful, average users are becoming increasingly reliant on these devices for storing and relaying sensitive information – such as bank account and contact information.

In tandem with the extensive proliferation of portable devices, there has been a considerable increase in connectivity. Today, there are more than 350 million hosts on the Internet [1]. Additionally, wireless networks are being set up in homes, offices, cafes, and malls thereby increasing interconnectivity even further. In fact, the number of home wireless networks in the USA reached 8.7 million in 2004. That number is expected to increase rapidly in the near future and analysts estimate that there will be 28 million home wireless networks in 2008 [2]. At the same time, however, the lack of security is staggering. Estimates

vary, but most analysts seem to agree that “between 60% and 70% of all existing wireless networks – corporate and personal – have no external security at all”. In fact, the act of snooping around for unprotected wireless networks has become popular enough for it to merit a special name – Wardriving [3].

One factor that substantiates the large projected increase in home wireless networks is the introduction of new network-capable household products. Microwaves, fridges, TVs, and almost any other consumer product will soon have some form of network connectivity thus transforming the average home into what is known as the “Smart Home”. There are various initiatives currently working on standardizing the framework for interoperable device interaction within the Smart Home. For an example of such an initiative, see the Digital Living Network Alliance (DLNA) at [4].

The emergence of the Smart Home coupled with the increased reliance on portable devices to handle sensitive information is ushering in a new status quo. This requires a paradigm shift in the design of secure systems. The average consumer cannot be expected to interact with security in the ways that IT experts traditionally have. These systems are not designed with non-expert users in mind. Furthermore, consumer products within the Smart Home will communicate over several different wired and wireless media, such as Bluetooth, 802.11, Ethernet, etc. The varied nature of the underlying network medium only exacerbates the burden of security on the non-expert user.

In this paper we discuss the introduction of a usable security framework in the Smart Home environment. We shortly review related work on home network security and present several of the most interesting basic use cases. We discuss the challenges that non-expert users face when configuring security for their Smart Homes and setting up multiple devices to connect to the Smart Home network. We also discuss the difficulties users encounter when granting temporary access to visitors for specific services in the home. We then outline several approaches to creating an intuitive Smart Home security framework and discuss the advantages and disadvantages of each. Finally, we conclude.

The remaining of this paper is organized as follows: Section 2 presents a brief overview of related work;

Section 3 introduces some basic use cases for Smart Home security and Section 4 introduces the challenges of creating an intuitive Smart Home security framework. Section 5 discusses several different approaches to creating a usable security framework. Finally, we summarize and conclude in Section 6.

2. RELATED WORK

The issue of usability in the specific context of security frameworks has not been addressed in the literature until quite recently. One example of a security framework that was intended to be usable but was never widely adopted is that of Pretty Good Privacy (PGP), which is an encryption and authentication framework for email. In [5], Whitten and Tygar evaluate the usability of PGP and conclude that the system is not in fact usable. Therefore, despite all the security threats that email exposes users to – such as viruses, phishing scams, spam, etc – the framework is still not widely used. This highlights the importance of usability when it comes to security.

There are several papers that introduce methods for building usable security applications and for evaluating their success, as in [6] and [7]. More recently researchers have argued for modifying and supplementing these guidelines for the development of a centralized security tool, such as in [8]. There are other papers that discuss the issues of designing applications and products for smart spaces in general, such as in [9] and [10].

In the industry there have also been attempts at addressing security usability. Microsoft's next release of its Windows™ operating system promises to demonstrate a big investment in security [11].

More specific to Smart Home security is an initiative by the Universal Plug and Play (UPnP) forum [12] known as UPnP Security [13]. This was published in 2003 but it does not directly address issues related to security usability. This framework takes a decentralized approach by creating a DeviceSecurity service and a Security Console. The former is a UPnP service offered by each security enabled UPnP device that provides a network interface to view and modify security settings on the device. The latter provides the user interface for the human owner of the device. There is no discussion on making this interface a usable one.

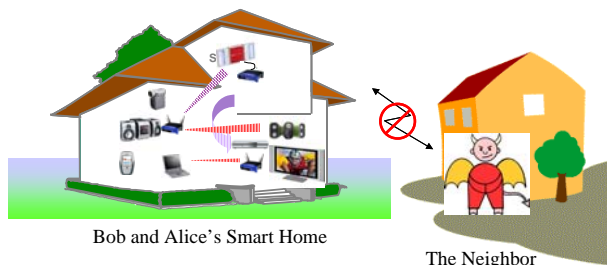
3. BASIC HOME SECURITY USE CASES

This section presents several basic use cases for user interaction with security in the Smart Home. The scenario consists of a household with a married couple – Bob and Alice.

The first use case involves bootstrapping new devices into the Smart Home. When Bob and Alice purchase a new device, they would like it to have

permanent connectivity to the Smart Home network over a secure channel. At the same time they would like to protect their home from being accessed by non-authorized users. Figure 1 illustrates this.

Figure 1: Bootstrapping and securing the Smart Home network



Once the devices are connected and can all communicate with each other securely, Bob would like to prevent Alice from accessing his devices until he explicitly grants her access. He could also opt to have his devices have some default level of access to everybody. By way of example, Bob purchases a new media server whose content he wishes to keep private. Both Bob and Alice jointly purchased the A/V renderer in the living room so they both have access to it by default. Thus Bob can now stream content from his media server and display it on the A/V renderer, however Alice cannot. Figure 2 illustrates this.

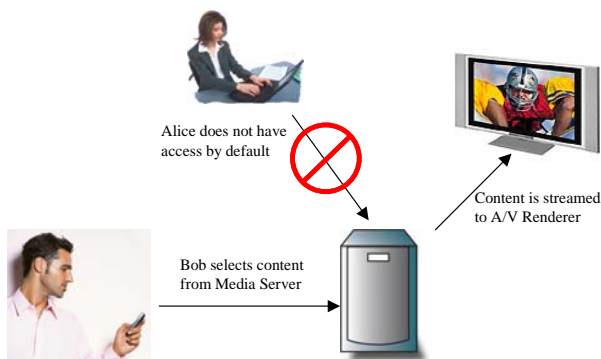


Figure 2: Before Bob grants Alice access

Alice later decides that she wants to retrieve content from the server and asks Bob to give her access. Bob agrees, but he only wants to give her permission to download music and movies from the server. He does not want her to access any other file types or to upload or delete anything. Figure 3 illustrates the situation after Bob grants Alice limited access to his media server.

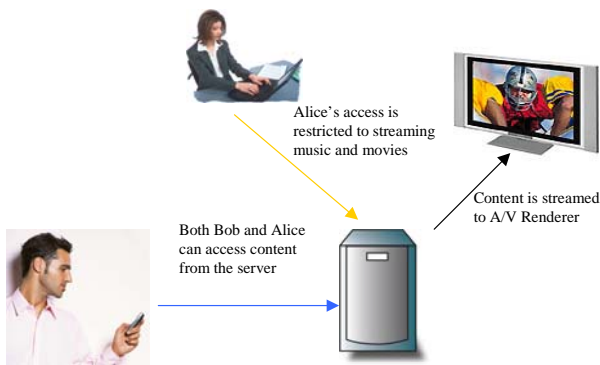


Figure 3: After Bob grants Alice access

A further use case involves granting temporary access to visitors for use of specific services in the Smart Home. Again, by way of example, the fridge in Bob and Alice's home breaks down. The repairman comes over and by default is not even able to connect to and browse their home network. However, Alice grants the repairman access for the day to selected functionality provided by the fridge so that he can perform the necessary repairs. At the end of the day, once the work is complete, the repairman automatically loses all access to Bob and Alice's Smart Home network. Figure 4 shows the repairman's access during the day.

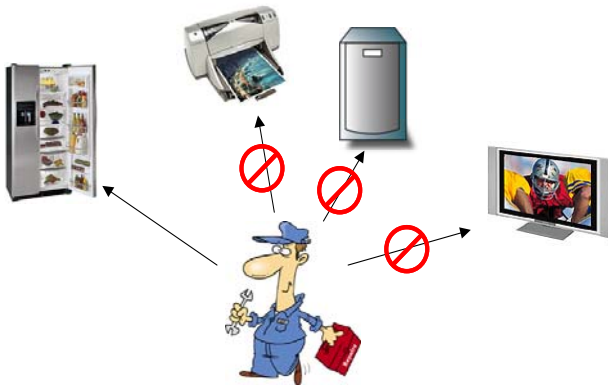


Figure 4: The repairman's access while repairing the fridge

4. DESIGN CHALLENGES

There are several challenges that designers face when attempting to create a usable security framework for the Smart Home. The first of these challenges involves understanding and accommodating the multitude of different connectivity options that are available, such as Bluetooth [14], Ultra Wide Band [15], Wireless USB [16], Wi-Fi [17], WiMax [18], etc. Each of these has its own pool of security mechanisms such as Wired Equivalent Privacy (WEP) [20] or Wi-Fi

Protected Access (WPA) [21] for 802.11, the pairing mechanism for Bluetooth [22], etc. Thus any successful attempt at creating a Smart Home security framework will have to incorporate a variety of different wireless connectivity media and their respective link level security mechanisms.

Once connections are secure at the link-level, the security framework must handle authentication and access control at the device or service level. Looking in more detail at the repairman scenario, in order for him to access the fridge, he must be given permissions at both the link level to connect to Alice and Bob's Smart Home network and at the device level, to access the fridge. The challenge here is successfully separating the policy from the mechanism in such a way that access control can take place on any type of device. The underlying mechanisms may well vary on each device; however the policy of access control should remain consistent.

Thirdly and perhaps most importantly, is the issue of usability. As the Smart Home incorporates an increasing number of devices, the complexity of the network will only increase making it less manageable for the average user. The issue of usability is one that needs to be addressed as part of all aspects of the Smart Home. However, the fact that currently around two-thirds of wireless networks are not secure demonstrates how important this factor is when it comes to creating a security framework for the Smart Home. Even more experienced users face difficulties when configuring and managing their networked devices since in most cases they must interact directly with low level security concepts, such as WEP keys and MAC address filters.

Finally is the issue of architecture. As mentioned in Section 2, there are arguments for the creation of a central security device that manages the security of various other devices. This could become a requirement of the Smart Home network and any attempt to connect to a device would first need to be approved by the central security device. However, there are strong industry initiatives pushing for the standardization of a decentralized approach where each device handles its own security policy, such as in [13].

5. USABILITY

There is a clear need to focus on usability when designing a security framework for Smart Homes. A lot of work has been done on developing the underlying security mechanisms and ensuring their cryptographic strength; however until recently there has been little emphasis on creating a consistent and intuitive interaction between non-expert users and security frameworks. Currently, most users are faced with the daunting task of dealing directly with low-level security parameters, most of which are cryptic even to the intermediate or advanced user.

For example, manufacturers of most wireless 802.11 access points currently provide users with an interface to configure the security settings of their devices over an HTTP connection. When a user first starts up their new access point, they are normally required to connect to it through a web browser after which they are presented with a page such as in Figure 5. Terms such as WPA, WEP keys, ASCII, Hex, 128-bit, easily overwhelm even the relatively knowledgeable user.

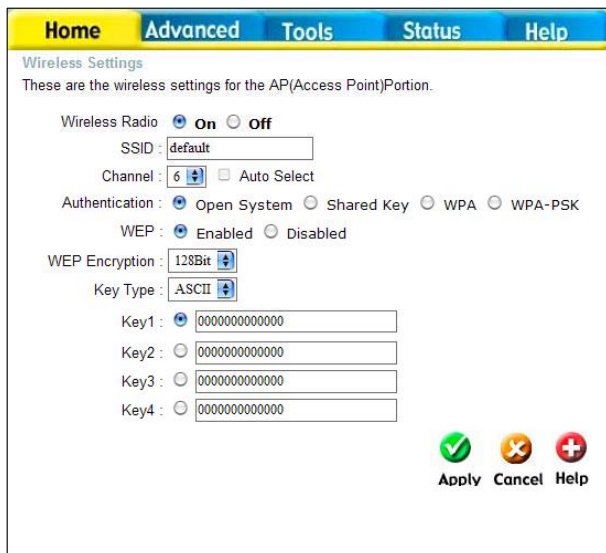


Figure 5: A typical setup screen provided by an 802.11 wireless access point

In addition to link-level security settings, users must configure their devices to grant access to specific users. This usually involves manually editing some type of Access Control List (ACL) on the device. These entries are permanent and difficult to manage as users must continually revisit the ACLs in order to remove outdated entries and update existing ones. This process is cumbersome and not intuitive.

Taking the example of the fridge repairman, current security frameworks would require Bob or Alice to either perform some type of manual configuration on their access points, such as modifying a MAC address list, or to enter a key (for WEP) or PIN (for Bluetooth) into the repairman's device. This would then grant him link level connectivity access to the home. They would then additionally have to modify the ACL of the fridge in order to grant the repairman access to whatever functionality is necessary for the repairs. Once the repairman has completed his repairs, they would have to go back and remove his entry from the ACL of the fridge. They would also need to change the link level keys to make sure that the repairman cannot reconnect to their home network.

Realizing that the complexity of these steps places an unrealistic burden on the average user, there have been several attempts at creating a more usable

interaction with security for home networks. Microsoft released a new wireless setup wizard as part of a recent upgrade to its Windows™ XP operating system. The wizard attempts to walk the user through the creation of a secure wireless network using several relatively simple steps. A screenshot of this wizard is shown in Figure 6.

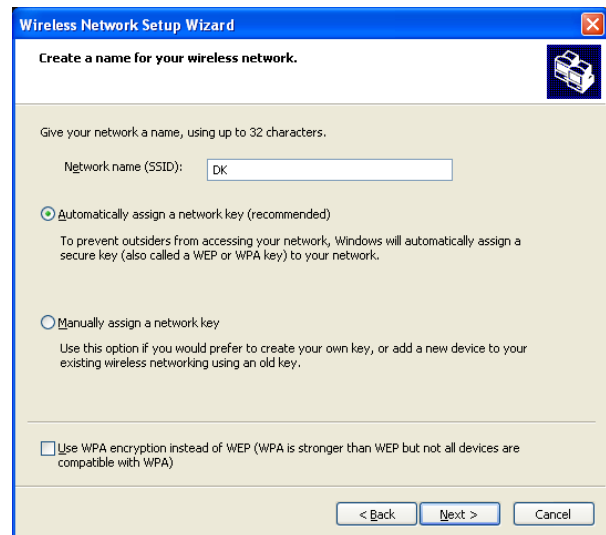


Figure 6: The wireless network setup wizard as part of Windows™ XP Service Pack 2

Two other initiatives worth noting are Buffalo Technology's AirStation OneTouch Secure System (AOSS) and Linksys' SecureEasySetup (SES), which was adopted from Broadcom. Both technologies promise quick and easy setup of secured wireless networks and have similar user interfaces despite using different underlying security mechanisms. AOSS supports security levels from the relatively weak 64-bit WEP to the strongest available WPA2-PSK, while SES supports devices capable of WPA-PSK/TKIP security. An image of the Linksys WRT54G wireless router that supports SES is shown in Figure 7. After pressing the Cisco logo, the user installs the accompanying software onto her device. The software then automatically detects and creates a secure connection with the router.



Figure 7: Linksys WRT54G wireless router supporting SecureEasySetup

6. CONCLUSIONS

In this paper we presented an overview of issues pertaining to the development of usable security frameworks for Smart Homes. There is a clear need for the development of such frameworks and steps are already being made towards this goal, as indicated by the various industry initiatives. However, much work remains to be done. A framework that incorporates the majority of underlying security mechanisms while presenting the user with a consistent and usable interaction has yet to be achieved.

REFERENCES

- [1] Internet Systems Consortium Internet Domain Survey, <http://www.isc.org/index.pl?/ops/ds/>
- [2] R. Lieb, "Wi-Fi Moves In", <http://www.clickz.com/stats/sectors/wireless/article.php/3416331>
- [3] <http://www.wardriving.com/>
- [4] Digital Living Network Alliance (DLNA), "Home Networked Device Interoperability Guidelines v1.0", June 2004, <http://www.dlna.org>
- [5] A. Whitten and J. Tygar, "Why Johnny can't encrypt: A usability evaluation of PGP 5.0", Proceedings of the Eighth USENIX Security Symposium, 1999.
- [6] D. K. Smetters and R. E. Grinter. "Moving from the design of usable security technologies to the design of useful secure applications". In *New Security Paradigms Workshop '02*. ACM, 2002.
- [7] F. Stajano and R. J. Anderson. "The resurrecting duckling: Security issues for ad-hoc wireless networks". In 7th Security Protocols Workshop, volume 1796 of Lecture Notes in Computer Science, pages 172–194, Cambridge, United Kingdom, 1999. Springer-Verlag, Berlin Germany.
- [8] U. Jendricke and D. Gerd tom Markotten. "Usability meets Security: The Identity-Manager as your Personal Security Assistant for the Internet". In Proceedings of the 16th Annual Computer Security Applications Conference, December 2000.
- [9] W. Edwards and R. Grinter, "At Home with Ubiquitous Computing: Seven Challenges," Proc. 3rd Int'l Conf. Ubiquitous Computing, Lecture Notes in Computer Science 2201, Springer-Verlag, Berlin, 2001, pp. 256–272;
www.parc.xerox.com/csl/members/grinter/ubicomp.pdf
- [10] M. Coen, "Design Principles for Intelligent Environments," Proc. 15th Nat'l Conf. Artificial Intelligence, AAAI Press, Menlo Park, Calif., 1998, pp. 547–554.
- [11] Remarks by Bill Gates, Chairman and Chief Software Architect, Microsoft Corporation WinHEC - Windows Hardware Engineering Conference 2005 Seattle, Wash. April 25, 2005
<http://www.microsoft.com/billgates/speeches/2005/04-25WinHec05.asp>
- [12] UPnP Forum, www.upnp.org
- [13] UPnP Forum, "UPnP Security Ceremonies Design Document v1.0", October 3, 2003.
- [14] Bluetooth Special Interest Group, "Bluetooth Core", Specification of the Bluetooth System version 1.2. , November 2003.
- [15] Ultra Wide Band Technology, <http://www.intel.com/technology/comms/uwb/>
- [16] Wireless Universal Serial Bus Specification 1.0, May 2005,
http://www.usb.org/wusb/docs/WirelessUSBSpecification_r10.pdf
- [17] Wi-Fi Alliance, www.wi-fi.org
- [18] WiMax Forum, <http://www.wimaxforum.org>
- [19] EAP Key Management Framework Internet-Draft, April 2005, <http://www.ietf.org/internet-drafts/draft-ietf-eap-keying-06.txt>
- [20] As part of the [15] ANSI/IEEE 802.11, "802.11std. Wireless LAN Medium Access Control and Physical Layer specifications", August 1999.
- [21] Wi-Fi Alliance, "Wi-Fi Protected Access (WPA)", October 2002.
- [22] Bluetooth Special Interest Group, "Bluetooth Security Architecture", white paper, version 1.0, 15 July 1999.