Content-Sharing for Dummies

A Secure and Usable Mechanism in Wi-Fi Infrastucture Home Networks

Sung-Min Lee† Se-Hee Han† Kang G. Shin‡

†Software Laboratories
SAMSUNG ELECTRONICS CO., LTD.
Suwon-City, Gyeonggi-Do, Korea 443-742
{sung.min.lee,sehee7.han}@samsung.com

‡Department of EECS
The University of Michigan
Ann Arbor, MI 48109-2121,U.S.A.
kgshin@eecs.umich.edu

Abstract—**This paper proposes a content-sharing mechanism, which is both secure and usable for wireless guest devices. It is very difficult for average users to allow a guest device to share its content with the users' devices supporting the principle of least privilege in the current Wi-Fi infrastructure home network environment. As a result, most people do not configure the security feature of their devices. The proposed mechanism frees users from security and tedious operations, thus enabling secure content sharing by a simple and intuitive user interaction via just one touch. Our evaluation shows that the proposed mechanism is secure and usable.**

Keywords-Contents sharing, temporary wireless access

I. INTRODUCTION

In recent years, there has been significant effort to develop and deploy home network technologies. As a result, the Digital Living Network Alliance (DLNA) [1] has been organized to support the interoperability of home network devices manufactured by different vendors. DLNA has specified Wi-Fi as one of lnk-layer communication mechanisms [2]. This will make Wi-Fi even more popular in the home environment in addition to the enterprise environment. DLNA also collected use-cases from various vendors and prioritized them, choosing content-sharing as the most important use-case based on the fact that four out of the top five use-cases are related to content uploads and downloads [3]. This indicates the importance of providing average users with an easy and secure content-sharing mechanism. In fact, it is essential to provide security features in wireless environments for user privacy, and "ease-of-use" is crucial to the success of home networks.

In this paper, we consider a content-sharing mechanism between a guest device and a home device in the Wi-Fi home network environment. In order to support such a mechanism, the following requirements should be satisfied for both security and usability.

- A guest device should not be able to eavesdrop the traffic between other devices.
- A guest device should only be allowed to access the wireless home network temporarily.
- A guest device should be able to access only the permitted (not all) devices in the network.
- The above security mechanism and configurations must be transparent to users because average users are unfamiliar with security jargons and technologies. However, a high level of security should be provided, i.e., the "ease-of-use" requirement should not degrade security.
- User intervention required for content-sharing should be minimal.

Researchers proposed to use location-limited channels for secure association between devices [4,5,6]. They focus on ad-hoc networks, not an infrastructure network environment, i.e., they do not consider the situation where a guest device associates itself with a home device within an infrastructure network. Moreover, they do not provide the proof of concept with any implementation and user test. Even though Lee *et al.* [7] proposed a temporary access mechanism in infrastructure networks, it was possible for the guest device to access *every* network device. Furthermore, they did not consider an intuitive (hence easy-to-use) content-sharing mechanism.

We propose a new content-sharing mechanism, which is both secure and usable in the Wi-Fi home network environment where even average users can transfer content from a guest device to a home device or vice versa with a simple intuitive user interaction. The proposed mechanism uses an ISO/IEC 14443 [8] proximity RF method so that each device recognizes approached devices and exchanges security information and meta-data for audio content automatically. Unlike the existing Wi-Fi security mechanism [9,10] used in the IEEE 802.11 infrastructure mode, a wireless guest device can only access a home device temporarily. This is because the home device gives the guest device a temporal key rather than a permanent key (i.e., Pre-Shared Key, or PSK) and sends its own address and guest device's address to the access point (AP) to allow communication only between the two touched devices. In order to make the guest device access the wireless home network temporarily, a home audio device embedded with a smart card participates in the Wi-Fi 4-way handshaking protocol [11,12] to generate a temporal key on the guest device's behalf. After establishing a secure session, a guest device decides whether to

1-4244-0667-6/07/$25.00 © 2007 IEEE

upload its content to the home audio or to download content from the audio device with meta-data and a simple inference rule. All security settings and content-sharing can be executed with an intuitive user interaction, just one touch.

The rest of this paper is organized as follows. Section 2 describes the existing technologies and our design goal. Section 3 details the proposed mechanism. Section 4 evaluates the proposed mechanism in terms of security, performance, and usability. Finally, Section 5 concludes the paper.

II. EXISTING TECHNOLOGIES AND DESIGN GOALS

This section describes Wi-Fi security for home networks and content-sharing based on UPnP. It also presents their problems and our design goal.

A. Wi-Fi Security for Home Networks

The Wi-Fi Alliance (WFA) developed the Wi-Fi Protected Access (WPA) as a specification of standards-based, interoperable security enhancements, which increases the level of data protection and access control for wireless LANs. It is forward-compatible with the IEEE 802.11i standard [11]. The WFA has been conducting WPA certification since 2003. WPA certification is divided into two areas: WPA-Enterprise and WPA-Personal [10]. WPA-Enterprise [13] is used in conjunction with an authentication server such as RADIUS [14] to provide centralized access control and management. It is suitable for enterprise environments equipped with an authentication server and a security administrator.

For personal environments like homes, WFA suggests WPA-Personal, which does not require central authentication servers or the Extensible Authentication Protocol (EAP) [12]. It uses a PSK that allows the use of manually-entered keys or passwords, and is designed to be easy and simple for home users to set up without requiring authentication server management. Therefore, it is feasible for home network security. However, there are still several problems in using it for home network security. First, as shown by several researchers [15,16], most average users cannot configure the security feature although the security setting of WPA-Personal is much simpler than that of WPA-Enterprise. Second, WPA-Personal does not distinguish home devices from guest devices. It assumes that all devices on a network are fully trusted. So, once a guest device connects to a wireless network, it obtains permanent access right on the wireless network because it has the knowledge of the permanent key, PSK, like any other home device. It can also overhear all messages among other home devices if it has the PSK. Third, currently most wireless home networks are based on the Wi-Fi infrastructure mode. If a guest device knows the PSK in that mode, it can access all network devices, even if a network owner wants the guest device to access only a specific device that he allows. In such a case, one of the important security principles, least privilege, cannot be met.

B. Content-Sharing Based on UPnP

Universal Plug and Play (UPnP) [17] was designed to support zero-configuration, invisible networking, and automatic discovery for a breadth of device categories from a wide range of vendors. Despite the simplicity of networking and device discovery, it needs additional user interactions for content-sharing after establishing network connectivity. For example, if a user wants to copy an MP3 file, which is being played by UPnP audio to his UPnP mobile device, the following user interactions are required:

1. A user has to find a UPnP audio device among the discovered UPnP devices with the browser (Control Point) on his mobile device.
2. If there are two or more audio devices in a home network, it is necessary for the user to find the right one and find the MP3 file via browsing.
3. He has to select the file and take an action for download (e.g., pressing button).
4. He has to find the downloaded file from his local directory and play it.

UPnP assumes that users are good at basic operations of computer systems (i.e., browsing, selecting, etc.). However, this assumption doesn't hold; many people can use TVs but cannot use computers at all. Most of them cannot even use the complicated functions on a TV remote controller. Although content-sharing is the most important use-case in the home network, these people may not follow the above steps. Security-related steps, before content-sharing, are even more difficult for average users to use.

C. Design Goal

The first goal of the proposed mechanism is to satisfy the principle of least privilege by improving the current WPA-Personal in the infrastructure mode because a guest device will be given restricted access rights. To meet the principle of least privilege, the proposed mechanism should have the following properties:

- *Authentication*: the proposed mechanism must prevent a revisiting guest device from joining a wireless network without a new permission.
- *Confidentiality*: the proposed mechanism must prevent a guest device from overhearing communications between home devices.
- *Access Control*: the proposed mechanism must prevent a guest device from accessing all of the interacting devices other than the one it received permission to access.

The second goal is to free users from the tedious operations for both security and content-sharing. If average users have to configure security functions whenever a guest device comes for content-sharing, the security feature will not be used because they do not fully understand how important security is and why security is needed in the first place. Therefore, the proposed mechanism should be able to configure needed security functions automatically without explicit user participation for security.

III. THE PROPOSED MECHANISM

The proposed mechanism consists of three components: wireless guest device, wired home audio device, and access point (AP) whose function includes packet filtering. A wireless guest device that wants to be enrolled in the wireless home network has an ISO/IEC 14443 reader to get a secure connection by accepting security information and meta-data for content from a home audio device. The home audio device is embedded with Ethernet interface, combi (contact and contactless) chip card and ISO/IEC 7816 [18] reader. Since the combi card can communicate with both the contact reader of a home audio device and the contactless reader of the guest device, it can be used as a storage medium between the guest device and the home audio device. Therefore, both guest and home devices can read/write information to/from the card. AP generates connection information including Service Set Identifier (SSID) and PSK for the wireless home network and allows the connection privilege to the guest device. If connection information is changed, it is sent to the home audio device to update the SSID and PSK on the smart card via a wired channel. It also allows the guest device to access the permitted device (i.e., the touched home audio device).

The overall architecture of the proposed mechanism is shown in Figure 1. When a guest touches his wireless device to the home audio device, the proposed mechanism starts automatically. In other words, audio content is transferred from one device to the other after completing the necessary security setup. The mechanism comprises three major parts: security & temporary connectivity configuration for a guest device, peer-to-peer communication only between the two touched devices, and context-aware content sharing. Each part of the mechanism is detailed below.

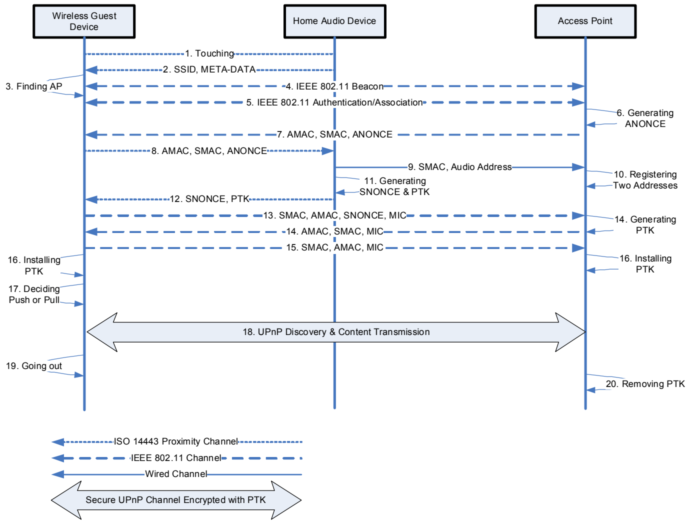

Figure 1. Overall architecture

A. *Security & Connectivity Configuration for Temporary Access*

1) *Wireless Guest Device Registration*

In order to provide a guest device temporary access, the smart card embedded in a home audio device participates in the existing 4-way handshaking. In general, an AP and a wireless device must share the PSK to establish a secure wireless session because they can build a PTK if they have five parameters including PSK. However, unlike the existing protocols, it provides only PTK to the wireless guest device (not PSK) for temporary access.

When a guest touches his device for access to the home audio device, the SSID is transferred to the guest device from the smart card in the audio device. Once it receives the SSID, it finds the AP and completes IEEE 802.11 authentication and association. It then starts the 4-way handshaking protocol. The messages 7, 13, 14 and 15 in Figure 1 indicate the 4 messages for the conventional 4-way handshaking protocol.

The first message (7) among 4-way handshaking messages has Authenticator (i.e, AP) MAC address (AMAC), Supplicant (i.e, wireless device) MAC address (SMAC), and Authenticator NONCE (ANONCE). We added the messages 8, 11, and 12 to the conventional protocol for allowing the guest device to receive only a temporal key, PTK. When the guest device receives message 7, it transfers the AMAC, SMAC, and the ANONCE to the smart card embedded in the home audio device because it does not know the value of PSK to generate PTK. The smart card in the home device generates a random number, Supplicant NONCE (SNONCE), and computes the PTK using five parameters on behalf of the guest device and finally sends them to the guest device. The following pseudorandom number generation function is used for computing 512-bit PTK [11]:

$$PTK=PRF\text{-}512(PSK,\ \text{“}Pairwise\ key\ expansion\text{”},\ AMAC||SMAC||ANONCE||SNONCE).$$

The AP cannot yet compute PTK because it does not know the value of SNONCE. The guest device sends SNONCE and Message Integrity Code (MIC) to prevent tampering. MIC allows the AP to verify that the guest device really knows the PTK derived from the same PSK. If the guest device's PTK does not match that of the AP, the MIC check will fail. The AP checks the MIC before moving to the next phase. If the MIC is valid, the AP computes the PTK because it has the knowledge of all of the five parameters at this point. The messages 13, 14, and 15 are the same as the existing 4-way handshaking protocol. So, subsequent transmissions are encrypted with the PTK.

The guest device and the AP can share the PTK without exposing the value of PSK to the guest device using a smart card and a small change to the 4-way handshaking protocol. Namely, only those permitted guest devices can connect to the network using the proposed mechanism with an intuitive user interaction.

2) *Wireless Guest Device Invalidation*

In the real world, if a guest leaves your home, he cannot use any facility in your home. Likewise, if a guest device leaves your home network, it must no longer be able to access the resources in your home network. However, there is no physical boundary in a wireless home network, requiring a key invalidation process.

Our invalidation mechanism does not require any user interaction, because the PTK is valid if and only if the guest device is within the radio range and maintains active communication. If this condition does not hold, the device will not be able to access the home network. For instance, the maximum inactivity timer is set to about 5 minutes in the HostAP. This means that if a guest device has gone out of range for more than 5 minutes, its security and connection information is invalidated automatically.

B. Peer-to-Peer Communication Only between Two Touched Devices

As stated in Section II-A, a guest device can access every device in the IEEE 802.11 infrastructure mode. For example, even though a network owner wants a guest device to access only his audio device, but not his video device and other private devices, it can access all of the devices if it has the knowledge of PSK or PTK. This clearly violates the principle of least privilege.

In order to solve this problem, the AP in our system manages a special table which contains source and destination addresses for access control. When a guest touches his device to access a home device, the guest device's MAC address (message 9 in Figure 1) is sent to the home device to generate a temporal key on behalf of the guest device. At that moment, the home device sends the received MAC address and its own MAC address to the AP. Then, the AP registers it with the home device's MAC address in the filter table. Every time it receives a packet, the AP checks if its source address is registered in the table. The AP allows the guest device to communicate only with the corresponding destination address if and only if a guest device's address is included in the table.

If the guest device goes out of the network area, the AP removes the guest device's MAC address and the corresponding home device's MAC address from the table.

C. Context-Aware Content-Sharing

After setting up wireless network connectivity and completing the security setup, content can be transferred from a guest device to a home audio device or vice versa by using a simple inference rule. UPnP AV specification classified three logical device classes: Media Server (MS), Media Renderer (MR), and Control Point (CP) [19,20,21]. Both guest and home audio devices in our mechanism have logical devices, MS, MR, and CP. As shown in Table 1, there are four combinations of the status of each device's MR (e.g., MP3 player). When a guest touches a home audio device with his portable device, it receives META-DATA in Figure 1, which contains URI, status, and Universally Unique Identifiers (UUIDs) of MS and MR of the home audio device. The CP of a guest device plays an important role to decide whether it acts for PUSH (sending its mp3 to home device) or PULL (receiving mp3 from home device) with that rule because it has knowledge of its own status and the home device's status. If the status of the guest device's MR is STOP and that of the home device's MR is PLAY, the guest device receives audio data from the home device with the UPnP PULL method. In the opposite case, it sends audio data to the home device with the UPnP PUSH method. In this case, both devices' statuses are PLAY, and the guest device sends audio data to the home device because most people want to listen to music with a large stereo audio device rather than a small handheld device when they return home.

TABLE I. RULE FOR DECIDING PUSH OR PULL

Guest Device	Home Device	Decision
STOP	STOP	No Operation
STOP	PLAY	PULL
PLAY	STOP	PUSH
PLAY	PLAY	PUSH

If the decision is PUSH, the UPnP sequences are as follows. A CP in a guest device finds the MS and MR in a home audio device by multicasting the UPnP M-Search message. The home audio device responds to the message with its device descriptions. Originally, a user has to browse an audio content list and select one to be sent to the home audio device. However, the guest device knows the ObjectURI of its playing content. It also has knowledge of the UUIDs of MS and MR in the home audio device from the META-DATA shown in Figure 1. Therefore, it can push the audio stream to the audio device and transfer the MP3 file by using an ImportURI action.

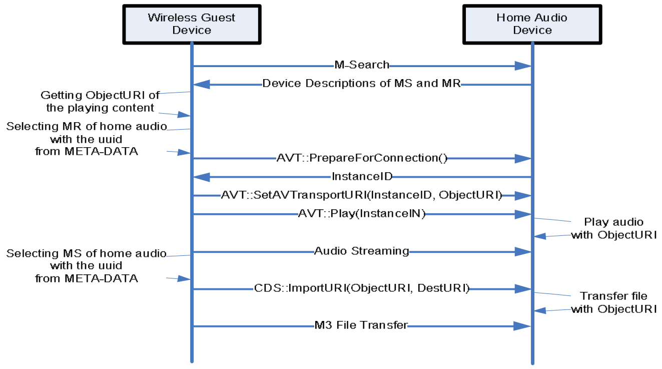
Wireless Guest Device
Home Audio Device
M-Search
Device Descriptions of MS and MR
Getting ObjectURI of the playing content
Selecting MR of home audio with the uuid from META-DATA
AVT::PrepareForConnection()
InstanceID
AVT::SetAVTransportURI(InstanceID, ObjectURI)
AVT::Play(InstanceIN)
Play audio with ObjectURI
Selecting MS of home audio with the uuid from META-DATA
Audio Streaming
CDS::ImportURI(ObjectURI, DestURI)
Transfer file with ObjectURI
M3 File Transfer

Figure 2. Content sharing via PUSH

If the decision is PULL, the UPnP sequences are as follows. Similar to the operations of the above PUSH scenario, it also needs the UPnP device discovery phase. The CP in the guest device then connects to the MS of the home device by using the UUID and ObjectURI obtained from META-DATA. It receives an audio stream from the MS of the home audio device. Finally, it copies the MP3 file from the home audio device.

IV. ANALYSIS

This section analyzes the proposed mechanism in terms of security, performance, and usability.

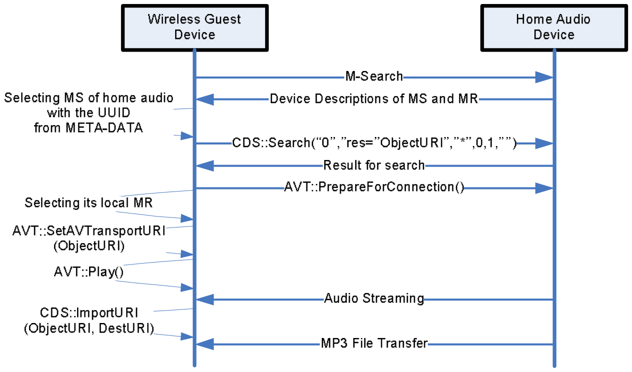
Wireless Guest Device
Home Audio Device
M-Search
Device Descriptions of MS and MR
Selecting MS of home audio with the UUID from META-DATA
CDS::Search("0","res="ObjectURI","*",0,1,"")
Result for search
AVT::PrepareForConnection()
Selecting its local MR
AVT::SetAVTransportURI (ObjectURI)
AVT::Play()
Audio Streaming
CDS::ImportURI (ObjectURI, DestURI)
MP3 File Transfer

Figure 3. Content sharing via PULL

A. Security

As stated in Section II-C, security is our primary goal. The proposed mechanism supports the principle of least privilege by satisfying the following properties:

- *Authentication*: The proposed mechanism does not provide PSK to a guest device. Instead, it provides PTK that is generated on the smart card embedded in a home audio device. The PTK is used for only one secure channel and is destroyed after the guest device leaves the network. Therefore, if the guest device wants to re-join the network, it must get permission again from the network owner. Consequently, it only has temporary access.

- *Confidentiality*: Suppose the smart card embedded in a home audio device does not generate a SNONCE and uses the SNONCE from the guest device like a conventional protocol. Then, a malicious guest device can use the smart card in a home device to generate other devices' PTKs. For example, if a guest device monitors the 4-way handshake of a target device, then it easily receives the SNONCE and SMAC from the device. It then sends the SNONCE and the SMAC to the home audio device to get the target's PTK. Once the malicious device calculates the PTK, it could monitor all messages to/from the target. To prevent this scenario from happening, the proposed mechanism forces a home device to generate SNONCE and PTK on behalf of the guest device.

- *Access control*: In the IEEE 802.11 infrastructure mode, any wireless device that knows network and security credentials, can access each and every device in the wireless network. However, the proposed mechanism makes a guest device access only one device that the homeowner explicitly permits it, since the two addresses of the two touched devices are registered to the AP's packet filter table. Therefore, the guest device cannot access any device other than the touched home device.

B. Performance

To evaluate the performance of the proposed mechanism, we experimented with our test scenario five times. The average time taken for each part is given in Table 2. Our experimental environment is composed as follows: Zaurus PDA which has an Intel XScale 400MHz processor, SpringProx ISO 14443 RF reader, and Linksys WCF-12 802.11b WLAN card were used for a guest device; Bare-bone PC that includes Intel Pentium4 3GHz processor, 1GB memory and ACS ISO 7816 smart card reader with IBM JCOP30 combi card, was used for a home audio device and Pentium4 PC that installed Host AP software was used for AP.

After touching, 2.11 seconds was taken to establish a secure Wi-Fi connection using the 4-way handshaking protocol. It took 1.24 seconds until the UPnP-based audio streaming started after the connection establishment. Therefore, when a user touches his device to connect to an audio device, he can listen to MP3 music via UPnP audio streaming in approximately 3 seconds, including the time for secure connection establishment. Although 802.11b theoretically provides 10Mbps data rate, it took about 11 seconds for copying an MP3 file of about 3.5 MB owing to the interferences from other APs near our test environment. Our experimental result has shown the proposed mechanism to perform reasonably well and be practically useful because it took about 3 seconds for network/security setup and listening to music, and completed MP3 file copying within 15 seconds.

TABLE II. SUMMARY OF EXPERIMENT

Average Time (Seconds)		
Secure Connection Establishment	***Streaming Start***	***MP3 File Copying***
2.11	1.24	10.59

C. Usability

In order to show the usability of the proposed mechanism, we conducted user tests. There were two test-cases. One was content-sharing with existing methods. The other was content-sharing with the proposed mechanism. The following coarse-grained steps were required to let a guest device share content with a home device in a Wi-Fi home network environment while satisfying the principle of least privilege as is done with the proposed mechanism.

1. A user has to see the Wi-Fi configuration including network and security information by connecting AP with PC.
2. A user has to enter the Wi-Fi security and connection information into a guest device manually.
3. A user has to check the guest device's address and register it with the home audio device's address at AP.

1-4244-0667-6/07/$25.00 © 2007 IEEE

4. A user has to find the right audio server among many UPnP devices by browsing them.
5. A user has to find the right content among many content lists by browsing them.
6. A user has to take action for play and copying the MP3 file.
7. A user has to update the Wi-Fi security configuration of every device after the guest device leaves in order to prevent the guest device's permanent access to the network.
8. A user has to delete the guest device's address from the packet filter table.

The user test was run with 7 different participants (P1~P7), all of whom were users with experience in operating PCs and their ages ranged from 25 to 35. P1, P2, P3, P4, and P5 were computer programmers with the MS degree in computer science. P6 and P7 were average users (not engineers) who had received a B.A. and M.A. respectively. Each test session lasted for 60 minutes, from the point at which the participant was given the initial task description to the point when the test monitor stopped the session. Table 3 summarizes the result of the user test.

TABLE III. RESULT OF USER TEST

Time Person	With existing mechanisms	With the proposed mechanism
P1	37 minutes	Within 10 seconds
P2	26 minutes	
P3	45 minutes	
P4	42 minutes	
P5	51 minutes	
P6	Failed	
P7	Failed	

All engineers (P1-P5) finished the test scenario successfully with the existing mechanisms in 60 minutes. However, on average, five people took about 40 minutes to complete the test scenario. The average users (P6 and P7), however, failed to finish the scenario in 60 minutes. Both of them gave up the test because it was too difficult for them to understand technical jargons and the steps were too complicated for them. It is tedious for a user to follow the above steps each time a guest comes. Consequently, an average user will never use the security features. By contrast, all participants, including average users, could finish the test scenario with the proposed mechanism successfully. Moreover, it took less than 10 seconds because one touch was all that was required. They did not have to understand the technology and security. Moreover, they did not have to perform any complicated user interactions. That is, the proposed mechanism hides security and tedious operations from the user. The test result shows that the proposed mechanism is also easy to use.

V. CONCLUSION

In this paper, we have proposed a simultaneously secure and usable content-sharing mechanism to allow a wireless guest device to access a Wi-Fi home network, satisfying the principle of least privilege. The proposed mechanism uses proximity channel for transferring security and meta-data for content-sharing. Unlike conventional Wi-Fi security, it gives a temporal (instead of permanent) key to a guest device and prevents the guest device from accessing every device rather than the explicitly permitted device. It frees users from security and tedious user interactions for content-sharing so that average home network users can use the proposed mechanism without learning how to use it. Our evaluation has shown that the proposed mechanism is attractive in terms of security, performance, and usability.

REFERENCES

[1] DLNA, "Overview and Vision," 2004. http://www.dlna.org/about/DLNA_Overview.pdf

[2] DLNA, "Home Networked Device Interoperability Guidelines v1.0," 2004.

[3] DLNA Use Case Sub-committee, "Mobile Handheld Device Use Cases," 2004.

[4] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks," 7th International Workshop Proceedings, LNCS, Springer-Verlag, 1999.

[5] T. Kindberg and K. Zhang, "Secure Spontaneous Device Association," UbiComp 2003, LNCS 2864, pp. 124-131, 2003.

[6] L. E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, and H. Gellersen, "Smart-Its Friends: A Technique for Users to Easily Establish Connections between Smart Artefacts," Ubicomp 2001, LNCS 2201, pp. 273-291, 2001.

[7] S. Lee, H. Yook, S. Oh, and S. Han, "Guest Access: Change Even Your Mother into an Effective Security Technician," CCNC '06, Las Vegas, 2006.

[8] ISO, "Identification cards – Contactless integrated circuit(s) cards – Proximity cards," 2001.

[9] Wi-Fi Alliance, "Wi-Fi Protected Access for the Home," WFA, 2003.

[10] Wi-Fi Alliance, "Wi-Fi Protected Access (WPA) Specification v2.0," WFA, 2003.

[11] J. Walker, "IEEE Standards 802.11i," IEEE, 2004.

[12] J. Edney, W. A. Arbaugh, *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*, Addison-Wesley, 2004.

[13] Wi-Fi Alliance, "Enterprise Solutions for Wireless LAN Security," WFA, 2003.

[14] P. Congdon, B. Aboba, A. Smith, G. Zorn, J. Roese, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines," RFC 3580, IETF, 2003.

[15] J. Ask, "Unwiring the Digital Home," Wi-Fi Alliance Meeting, 2004.

[16] P. Tsang, "APEC TEL Wireless (802.11) Security Workshop: Nextsteps," APEC TEL Conference, 2004.

[17] UPnP Forum, "UPnP Device Architecture 1.0," 2003.

[18] ISO, "Identification cards – Integrated circuit(s) cards – Part 4: Organization, security and commands for interchange," ISO Standards, 2001.

[19] UPnP Forum, "UPnP AV Architecture v0.83," 2002.

[20] UPnP Forum, "UPnP MediaServer:1 Device Template V1.01," 2002.

[21] UPnP Forum, "UPnP MediaRenderer:1 Device Template V1.01," 2002.