An Assisted Device Registration and Service Access System for future Home Networks

Andreas Müller, Holger Kinkelin, Sunil Kumar Ghai[1], and Georg Carle
Chair for Network Architectures and Services
Technische Universität München, Germany
{mueller, kinkelin, carle}@net.in.tum.de, sunilkrghai@gmail.com
http://www.net.in.tum.de

***Abstract*—In today's home networks security features are very rare. Infact, the only service that is usually secured is the access to the wireless network. Services, such as video streaming and audio distribution systems, often use the popular UPnP protocol since it provides dynamic service discovery and is supported by the Digital Living Network Alliance (DLNA). However, UPnP implements no security features which is not only a problem for today's services, but especially for future services in future home networks. Part of the problem is the complexity and the effort that is needed for maintaining a security infrastructure and for the deployment of security mechanisms that are common in administrated enterprise networks. This paper addresses the problem stated above by introducing an assistance system that allows for the easy and almost automatic issuing and distribution of valid X.509 certificates to new devices. We then use these certificates for controlling network access and for the design and implementation of a secure video streaming system based on the Devices Profile for Web Services (DPWS). This system shows that certificates not only help within a home, but are absolutely mandatory when interconnecting multiple homes.**

I. Introduction

Security for home networks, especially for future networks with many devices and users, is a very important issue that is often neglected. The probably most important cornerstone that is already considered today is the protection of a home's wireless network. Meanwhile, the vulnerable and insecure WEP encryption standard got replaced by WPA/WPA2, which protects the network sufficiently. However, when considering scenarios where a guest needs access to the network as well as to certain services, WPA has some drawbacks because there is no revocation of passwords. Once the guest is leaving, the administrator of the network has to change the passphrase on all devices in order to keep the guest out of the network. Solutions to that problem, e.g. using X.509 certificates [1] for authentication, require a lot of administrative knowledge for setting them up. This is not feasible for the average user that is responsible for his home network.

Home networking scenarios of the future go far beyond accessing an internet gateway or sharing files. Small services will be deployed in the home dynamically and they require a solid security architecture for protecting them. One example could be a multimedia streaming system. Today's approaches are usually based on the Universal Plug and Play (UPnP) protocol [2], which is already integrated in many DLNA [3] enabled devices such as web-radios and TVs. However, UPnP provides no security and simply allows everyone on the network to access the shared content.

With the growing bandwidth of home internet accesses, the desires of users emerge for cross domain service usage. Content stored in one home may be needed at another or homes might want to make services globally available to everyone. These scenarios require strong authentication and authorization mechanisms that are easy to use and simple to deploy.

Both examples mentioned can be solved by using X.509 certificates issued by a Certificate Authority (CA). Remote Authentication Dial-In User Service (RADIUS) [4] could be used for getting network access and the sucessor of UPnP, the Devices Profile for Web-Services (DPWS), for streaming media. The problem still existing is that a PKI is hard to maintain and user-friendly distribution mechanisms do not exist.

This paper has two main contributions: 1) an assistance system for unexperienced users that allows to create, issue and deliver X.509 certificates that are needed for accessing the network and services within the network. 2) a DPWS-based video streaming system that uses these certificates to securely discover and stream multimedia content.

The paper is structured as follows: Section II describes our approach of an assistance system that allows to easily issue and distribute valid X.509 certificates to devices. Section III then presents a proof of concept implementation that uses these certificates for building a secure video streaming system based on the DPWS. After evaluating our approach in section IV we give a survey of related work in section V and conclude in section VI.

II. Assisted Device Registration and Authentication

This section describes the general requirements and explains the architecture for an assistance system that enables the user-friendly distribution of valid X.509 certificates among devices.

[0]The presented work is part of the AutHoNe project which is partly funded by the German Federal Ministry of Education and Research under grant agreement no. 01BN070[2-5]. The project is being carried out as part of the CELTIC initiative within the EUREKA framework.

[1]Student of the Delhi College of Engineering and an intern at the TUM.

A. Identities in future home networks

In future home networks we have many entities and devices that are all interconnected. To identify them, each entity should have an identity for addressing and routing. We therefore propose an approach similar to the Host Identity Protocol (HIP) [5] where each entity has a public/private keypair and derives the identificator from the public key. But different to HIP, we propose that instead of having a global Certificate Authority (CA) for all entities, each home runs its own CA and is responsible for the entities belonging to it (its own users and visiting guests). This means, each entity (device, user, service) gets a certificate signed by its home CA and is only globally reachable by a combination of DeviceID and HomeID. A global CA is not intended because it would expose the details of the home network to the CA, thus causing privacy issues. Moreover, the centralized creation of certificates would come with undesirable administrative burdens and possible costs, again something users would not accept. In our approach trust between homes is established through a web-of-trust approach or through a secured exchange of home certificates, the so-called ”trust exchange”, which is out of scope for this paper.

Once issued, the clients use the certificates to get access to the network, to services and for a secure communication with other devices. One of the main questions is how to issue, maintain and distribute valid certificates if we assume that the average user of such future home networks is not an expert. Thus, the following sections present the idea of an assistance system that automatically bootstraps a device into a network.

B. Requirements

Since the assistance system is targeting average users it must be easy and intuitive to use (Requirement R1) and support both users and the administrator of the home network in a semi-automatic fashion during the registration and certificate creation process (R2). Since the process is very critical, we have to make sure that we only issue certificates to those devices that actually belong to the network. Man in the middle attacks during the registration have to be inhibited (R3). The system must also guarantee that the certificates can be used for authenticating devices at services (R4), otherwise they would be useless. Finally the interoperability of the system with devices belonging to different home networks (e.g. guests) must be feasible (R5).

C. Architecture

Once a new device is brought to the home it will discover two wireless networks: An open (or password protected) WLAN is used for issuing certificates which can then be used to enter the protected network. Fig. 1 shows the basic setup. We use the virtualization capability of modern access points to separate the WLANs. The home server runs two virtual machines and the network traffic is separated by using VLAN tags between the Access Point (AP) and the home server. Thus, only one AP and one home server is needed. Although this setup sounds complicated, providers and service operators may sell pre-configured systems and use open source software already available today at no cost. In this paper we only focus on the wireless part. However, our scenario could be easily extended to wired networks as well.

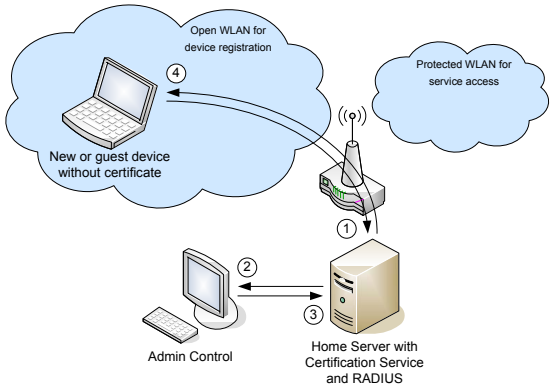

Fig. 1. Simplified registration process of a new device

The client only has to install a tiny application that connects it to the open WLAN, finds the home server and generates a Certificate Signing Request (CSR) to be sent to the home CA (step 1 in Fig. 1). This application could be pre-installed on new devices or directly accessible via the open network. The administrator of the home network gets informed about the pending request and decides about it (2). Once the administrator has accepted the request (3), the certificate gets issued and provided to the device (4).

Since the issuing of a device certificate equals the registration of the device within the home network, we also refer to this process as *Device Registration*. However, the same process can also be used to issue certificates to previously unknown guest users.

Once a client is registered to the home (obtained a certificate from the home CA), it can access services within the home network by connecting to the protected WLAN (see Fig.2). After the device provided its certificate to the AP (1), the AP forwards the authentication request to the home's RADIUS server (2) and eventually receives the access decision of RADIUS (3). After being successfully authenticated, the client is connected to the WLAN (4) and has access to the home network. Access to certain services available within the home network requires further authentication and authorization.

In the following sections more details and a deeper insight into the inner working of the device registration part of our system is provided.

D. Protocol for Distributing Device Certificates

In our setup, the home CA is connected to the network that belongs to the open WLAN. We use Zero Configuration Networking (Zeroconf) to automatically find the responsible registration service at the home server. First the client assigns itself an IPv4 link local address [6] and queries the network via Multicast DNS (mDNS) [7] for a registration service. We use the DNS based service discovery (DNS-SD) [8] protocol and defined a new record called

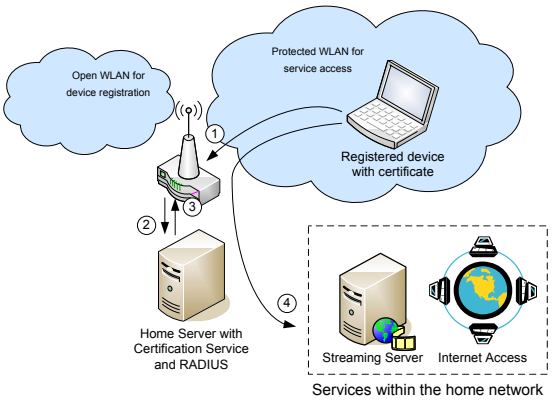

Fig. 2. Network access using device certificates

_registrationservice_homeserver._tcp. The service replies back with its IP address and port and the device directly establishes a TCP connection to it. The detailed flow of the protocol is shown in Fig. 3.

The registration process is divided into two steps to prevent man in the middle attacks. In the first step, the registration application asks the user to provide some details (e-mail address and common name) for the certificate. It then automatically creates the CSR and runs the zeroconf protocol as described above. As soon as it gets connected to the home CA, the CSR is sent. The home CA maintains a database for all pending requests and notifies the administrator if a new one appears. No further progress is made until the administrator approves the signing request by looking into the details of the CSR (e.g. name and e-mail address).

Once the details have been verified, the administrator directly contacts the user of the client over a side channel (e.g personally or via phone), to verify the identity of the user and to pass him a PIN number. This step is very important in order to prevent man in the middle attacks. However, if we already have a shared secret or some kind of trust relationship (e.g. exchanged home certificates) this step could also be automated. To complete the process, the user enters the PIN number which then gets encrypted by the private key. The encrypted PIN is sent back to the home CA, which then verifies it using the public key as provided in the initial CSR. If the PIN matches, the home CA finally issues the certificate to the device.

III. Secure Video Streaming using DPWS

This section explains how to use the automatically distributed certificates to enable secure video streaming in a home network environment by using the Devices Profile for Web Services (DPWS). We first give an introduction to the DPWS and explain the advantages over UPnP. Section III-B then focuses on our implemented scenario and shows how DPWS can be used for streaming videos in a secure manner. Finally we present an extension to the scenario which describes an approach that allows the interconnection of several homes.

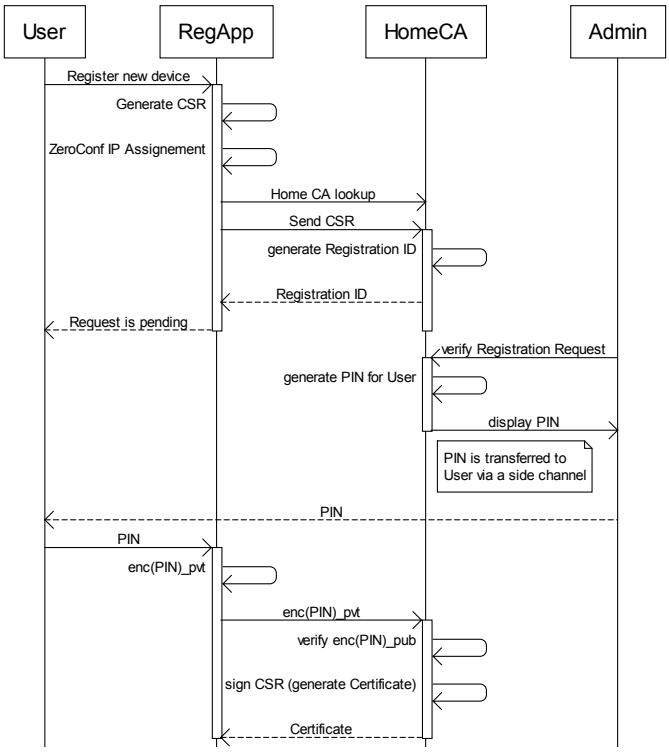

Fig. 3. The sequence diagram for the registration process

A. The Devices Profile for Web Services

The Devices Profile for Web Services (DPWS) defines a "minimal set of implementation constraints to enable secure Web Service messaging, discovery, description, and eventing on resource-constrained endpoints" [9]. Originally developed by Microsoft as a possible successor for UPnP and integrated into Vista, DPWS was approved as an OASIS standard in June 2009. DPWS not only builds on web services standards such as WSDL, XML Schema, SOAP, WS-Addressing, WS-Eventing and WS-Discovery, it also supports a subset of the security features as defined in WS-Security [10]. This allows the signing of multicast discovery messages and the encryption of the actual data exchanged between two services.

Since DPWS supports dynamic discovery it is an ideal protocol for automated home environments. Similar to UPnP, DPWS can be used for interconnecting standalone devices from many different vendors by using standardized protocols. However, UPnP uses a variety of different outdated protocols while standards such as XML and SOAP matured. Besides some other benefits such as scalability and robustness, the built-in security support is a big advantage over UPnP and allows it to be used with critical control systems such as lighting systems, heating systems and other peripherals.

B. Implementation of a Secure Video Streaming System

Nowadays UPnP is a very popular protocol in home networks and DLNA compatible devices found their way to many living rooms. However, UPnP may work well, but without any

security mechanisms it can not be seen as the most promising solution for future home networks and future requirements. One, and probably the most important reason for the lack of security is the knowledge that is needed for setting up a secure system. We argue that with the certificate distribution system as described above it is possible for the average user to secure their services in the home. Therefore, we implemented a video streaming system based on DPWS that allows the discovery of devices, content browsing and the streaming of media data. Furthermore, it also allows to automatically add a video and audio transcoder to dynamically adapt the codec and bitrate of the streams if necessary. The key feature of this system is that it uses a PKI to secure the discovery of devices, the signaling as well as the actual media streaming.

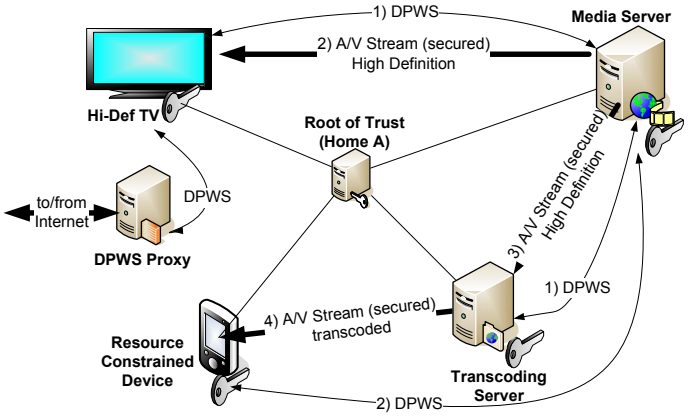

Fig. 4. The Video Streaming example scenario

Fig. 4 shows the setup of our scenario. The media server is implemented as a hosted service in DPWS [9] and holds the media content for its users. It is discoverable via WS-Discovery and uses the Video Lan Client (VLC) for streaming. Whenever a client device is switched on, it automatically queries the network for media servers using the WS-Discovery mechanisms as defined in the DPWS standard. Since each entity has its own certificate the client signs all request messages (DPWS-probe) and also expects the server to sign the responses (probe match). The encryption of discovery messages does not make sense since they should be readable by any device on the network. The server's response (probe match) contains the IP address and port of the media server which can then be contacted directly via TCP. This is done by establishing an authenticated TLS-Tunnel using the certificates in the PKI. All further signaling messages can then be sent through this protected channel.

For the actual signaling messages that are needed to control the streaming we developed a simple XML-based protocol which runs on top of DPWS. Our protocol implements the following actions: *getDirectoryContent* asks for the content of the current directory and expects a list with all media files and directories. This is used for browsing the protected media collection. In our implementation the access to several folders is restricted and authorization (via certificates) is needed to access them. *PlayFile* invokes the actual streaming of a media file. Our XML-protocol allows the client to specify the bitrate, video size and codec it wants to receive. The server then has to decide if it streams the file directly or if it needs to dynamically insert a transcoder (see Fig. 5). Since all signaling messages are sent throught a protected TLS channel, the client also adds a random shared key to the PlayFile command. This key is then used by the server to encrypt the media stream by using the Common Scrambling Algorithm (CSA). Finally, *ControlStream* is used by the client to pause, forward/rewind or to stop the stream.

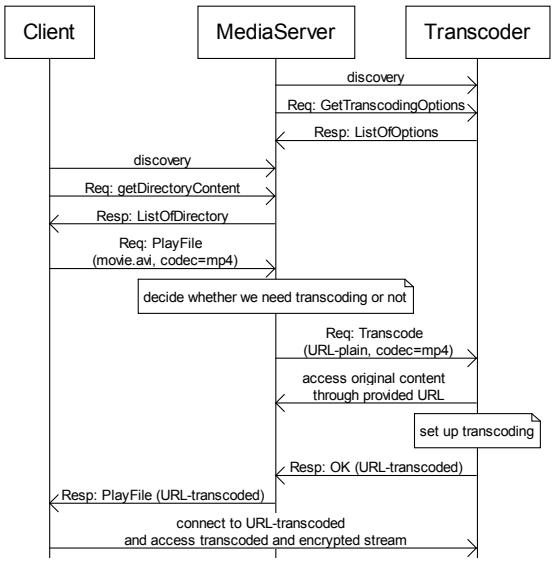

Fig. 5. The sequence diagram for the streaming system

When we now consider that the media server needs a transcoder to handle the clients request we need some additional steps (see Fig. 5): Once a media server has found a transcoding service though WS-Discovery it invokes the *GetTranscodingOptions* action to get informed about the transcoders capabilities. The *Transcode* action is invoked by the media server once a client requests a stream (at the media server) and transcoding is needed. The media server specifies the exact transcoding options (e.g. codec mp4) and the transcoder replies back with a HTTP-URL where the transcoded (and encrypted) stream can be found. The media server includes this URL in the answer to the initial *PlayFile* action and the client directly connects to the transcoder. With this extension the client always communicates to the media server and has no idea of the transcoder itself. The only indication is the URL that is replied back as an answer to the *PlayFile* request.

C. Multi Domain Scenario

DPWS, as well as UPnP, is restricted to only one broadcast domain because it uses IP multicast for discovering devices. Since UPnP does not implement any security mechanisms it does not make sense to change this. However, for DPWS we might want to allow the discovery of devices across domains,

because we are able to restrict the access on the service itself by using certificates. This example shows that for future home networks a solid security architecture is absolutely mandatory.

As a proof of concept we implemented a DPWS proxy that is responsible for forwarding multicast discovery messages from one home to another (see Fig. 4). Whenever a device queries the network asking for a service (DPWS-probe) the DPWS proxy gets this packet, analyses it and passes it (via TCP unicast) to the remote DPWS proxy which then sends the multicast packet out to its own network. The remote proxy then acts as a client and therefore gets the reply (probe match) back. This requires the proxies to maintain a state and maps between the local network and the IP address of the remote proxy. Furthermore, if a network uses Network Address Translation (NAT) the proxy also has to replace the private IP addresses and ports of the service which are used for establishing the direct connection after the discovery process. This can be done by using standards NAT-Traversal techniques and frameworks such as ANTS [11].

Future work here is to extend the scenario to a large scale network by interconnecting homes via an overlay network. The overlay is then responsible for selecting a list of DPWS proxies once a discovery message was sent to it.

IV. Evaluation

As an evaluation of our concepts, we implemented an easy to use prototype (R1, see section II-B) that supports both the user and administrator when registering a device (R2). Man in the middle attacks are eliminated by sending a PIN via a side channel (R3). Certificates issued by our prototype implementation are used for authentication (R4) of devices towards the protected home WLAN via RADIUS and for authentication towards a prototype DPWS-based streaming service. The interoperability with foreign devices (R5) is given by the capability of issuing guest certificates. We performed a thorough security analysis of our concept and as the only weakness we identified the possibility of compromising the homes CAs private key. This would allow an attacker to issue valid certificates for illegitimate devices. Due to the missing central CA, no revocation of the compromised home CA key would be possible. We are aware of this problem and are working on a solution based on Trusted Computing Technology to make the theft of the CA key impossible.

V. Related Work

The approach of using certificates in home networks is also presented in [12]. Here, keying material and certificate signing requests are not computed by the device itself and the certificate is signed by a CA not part of the home network. This requires to trust an external entity and introduces privacy issues because the disclosure of devices to the external CA might not be desired. A concept for a personal CA for certification of devices inside a PAN (Personal Area Network) is presented in [13]. This approach is limited to devices belonging to one network only. The interconnection between PAN domains is not possible. Furthermore, they assumes to already have connectivity to the registration service whereas we show the whole bootstrapping process. When the UPnP protocol was designed, security was not considered. However, the UPnP Forum published an additional extension that specifies layer 7 security mechanisms for UPnP [14]. Unfortunately most vendors ignore this and do not implement it. And since DPWS has some more advantages over UPnP, namely scalability through discovery proxies and the robustness against denial of service attacks, DPWS is an ideal candidate for replacing UPnP in future home networks.

VI. Conclusion

Today's home networks provide only limited security features because most of the already existing approaches are neither user-friendly nor easy to set up. Solutions such as the usage of X.509 certificates are common in enterprise networks and may also help in home networks if we can manage to develop a user-friendly way to maintain them. This paper introduced an assistance system that helps to automatically create, issue and distribute valid X.509 certificates among new devices and guest users. Techniques such as Zeroconf help to automatically discover a certificate authority service which gives us great flexibility. As one explicit scenario we also implemented a video streaming solution based on the UPnP successor DPWS. The distributed certificates are now used to securely discover and use the multimedia server. Future work is the protection of home certificates and the integration of authorization policies for securing arbitrary services.

References

[1] D. Cooper and S. Santesson, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 5280, IETF, May 2008.

[2] "Universal Plug and Play," http://www.upnp.org/standardizeddcps/default.asp, 2003.

[3] "The Digital Living Network Alliance," http://www.dlna.org/.

[4] C. Rigney and S. Willens, "Remote Authentication Dial In User Service (RADIUS)," RFC 2865, IETF, June 2000.

[5] R. Moskowitz and P. Nikander, "Host Identity Protocol," RFC 5201, IETF, April 2008.

[6] S. Cheshire, B. Aboba, and E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses," RFC 3927, IETF, May 2005.

[7] S. Cheshire and M. Krochmal, "Multicast DNS," Internet Draft, IETF, September 2008.

[8] S.Cheshire and M.Krochmal, "DNS-Based Service Discovery," Internet Draft, IETF, September 2008.

[9] "OASIS Devices Profile for Web Services (DPWS) Version 1.1," http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01, May 2009.

[10] "OASIS Web Services Security Version 1.1," http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf, February 2006.

[11] A. Müller, A. Klenk, and G. Carle, "ANTS - A Framework for Knowledge based NAT-Traversal," IEEE Globecom 2009, Honolulu, HI, USA, November 2009.

[12] Y. Lee, D. Lee, J. Han, and K. Chung, "Home network device authentication: Device authentication framework and device certificate profile," pp. 573–582, 2007.

[13] E. Mobile, P. Ab, C. G. Kaisa, K. Nyberg, and C. J. Mitchell, "The personal CA – PKI for a Personal Area Network," 2002.

[14] "Device Security and Security Console V 1.0," http://www.upnp.org/standardizeddcps/security.asp, 2003.