Authentication and Authorization in Universal Plug and Play Home Networks

Mauri Kangas
Helsinki University of Technology
maukan@cc.hut.fi

Abstract

The breakthrough of digital technologies is paving the way for remarkable enhancements to the entertainment experiences within the home. In the future there is expanding need to enjoy rich multimedia entertainment throughout the home regardless the physical location of the content. Such high band-width networking technologies, which enable seamless media distribution, and user-friendly access to the home network services and devices has not yet reached real mass-market adoption. Currently home networks have technical possibilities to support these requirements, but installation, configuration, and network management are too complicated for average users. This paper gives one possible solution to this problem by introducing the Universal Plug and Play (UPnP) technology, and its use in home network environment.

KEYWORDS: UPnP, IPv6, service discovery, home networking, authentication, authorization

1 Introduction

Internet is an evolving concept, which is expanding as well into mobile networks as residential environment, and the implementation of all communication devices and networks must take the Internet access into account. Mobile devices are based on microprocessor technology, which leads into smaller, faster, more power-efficient and less expensive mobile devices, which contain an increasing amount of storage capacity.

The increasing mobility of users, the number of various user devices, and new types of mobile applications are shaping the habits and ways to use the Internet enabled equipment. Wired and wireless bandwidth in home networks is expanding, and there will become an increasing need to connect more and more devices together, first for point-to-point communication between two devices at a time, and later for any-to-any communication over a wired or wireless home network. The increasing number of devices and service together with the increasing amount of available content in the home network is challenging for some kind of universal connectivity and plug-and-play functionality in home networks.

The installation and configuration of the network must be easy and should not require any professional personnel to be involved. There is always need for network configuration, because at least the access rights and rules for different services and devices must be inserted to the system. This can be made easy by introducing user-friendly configuration software for this purpose. After the installation and configuration, the use of the network must be much easier than in the installation phase. Later on there is continuous need to add new services, devices, and users to the network with minimal intervention from the user. Also when services, devices, and users are removed from the network on daily basis, the status of access rights, information on available services and devices, must be kept updated. The the usability of the network resources is most important thing in the home network operations.

Device interoperability between consumer devices at home has been discussed already for decades, but consumers have adopted only a few interface and content format standards into global use. This is also true for the polymorphic situation with Personal Computers (PC) and their peripherals, but they have a lot in common from physical connectors to communication protocols. The commonalities between different equipment, transmission, and communication protocols are increasing in the cellular and other wireless technologies, but unfortunately the high development speed of the entertainment industry combined with the Internet and mobile technology evolution is requesting for increasing amount of different transmission media, content format, and communication protocols.

Sections 2 and 3 give an overview of the Internet Protocol version 6 (IPv6) and UPnP technology, respectively. Section 4 is devoted to an Audio/Video (AV) application in an illustrated UPnP home network. Section 5 concentrates on the authentication and authorization in UPnP home networks. The scope of this paper is in the UPnP technology, its co-existence with IPv6 technology, and authentication and authorization of the user and user devices, which utilize different services in the UPnP home networks.

2 Highlights of IPv6 Technology

Today the IP technology is based on the use of IPv4 addressing mechanism having 32-bit address space, which has appeared to be too small for expanded use of IP-enabled devices. A solution to this problem is the IPv6 technology, which is based on 128-bit address space. The IPv6 technology ensures enough stable and unique addresses for all devices, allows continuous growth of the Internet, and restores the end-to-end transparency of Internet. The IPv6 technology ensures also plug and play features, verifiable end-to-end packet integrity, and simpler mobility without need fora foreign agent function.

IPv6 technology uses several kinds of addresses: unicast, anycast, multicast, link-local, site-local, loop-back, IPv4-embedded, care-of, manually assigned, DHCP-assigned, self-assigned, etc. The key to IPv6 deployment is a smooth transition from current IPv4 based networks to new IPv6 based networks. During the IPv6 deployment phase, there will be IPv4 and IPv6 islands, which are connected with several kinds of tunneling methods.

Address auto-configuration, which can be stateless or stateful, is one essential feature of IPv6. Stateless address auto-configuration happens in two steps. The node first identifies its link-local address using a neighbor discovery mechanism. The next step, which is actually a plug and play type of operation, acquires the unique, globally routable address without manual intervention from users or operators. The use of stateful mechanism such as Dynamic Host Configuration Protocol (DHCP) requires one additional server and more operations and maintenance effort.

The IPv6 technology provides a remedy for the problems found in IPv4, and the differences between these technologies are listed as follows:

- By provisioning 128-bit address space, compared to 32-bit address space of the IPv4 technology, IPv6 can assign global addresses to every Internet endpoint for several decades.
- When IPv6-enabled endpoint is connected to a network, it will automatically acquire IPv6 addresses, which contain local and global addresses, and the endpoints can be re-addressed in a quick, and flexible manner.
- IPv6 provides better support for fine-grained Quality of Service (QoS) and the packet flow identification for QoS handling is included only in the IPv6 header
- IPSec support is optional in IPv4, but in IPv6 it is built into the protocol itself.

Furthermore IPv6 tehnology has the following improvements compared to the IPv4 technology:

- IPv6 packet fragmentation is done only by the sending host, while in IPv4 fragmentation can also be done by routers
- IPv4 Address Resolution Protocol (ARP) uses broadcast ARP Request frames to resolve an IPv4 address to a link layer address, while in IPv6 ARP Request frames are replaced with multicast Neighbor Solicitation messages.
- IPv4 Internet Group Management Protocol (IGMP) is used to manage local subnet group membership, while in IPv6 IGMP is replaced with Multicast Listener Discovery (MLD) messages.
- ICMP Router Discovery is used to determine the IPv4 address of the best default gateway, while in IPv6 the ICMP Router Discovery is replaced with ICMPv6 Router Solicitation and Router Advertisement messages and is required.
- Broadcast addresses are used to send traffic to all nodes on a subnet, but in IPv6 a link-local scope all-nodes multicast address is used.
- IPv4 address must be configured either manually or through DHCP, but IPv6 does not require manual configuration or DHCP.

3 Universal Plug and Play Technology

3.1 UPnP Technology Overview

UPnP is broad in scope targeting to home networks, proximity networks, and networks in small businesses and commercial buildings. It enables data communication between any two devices under the command of any control device on the network. UPnP is independent of any particular operating system, programming language, or physical medium.

UPnP supports zero-configuration networking and automatic discovery, whereby a device can dynamically join a network, obtain an IP address, announce its name, convey its capabilities upon request, and learn about the presence and capabilities of other devices. DHCP and Domain Naming System (DNS) Servers are optional and will be used if available on the network. Furthermore, a device can leave a network smoothly and automatically without leaving any unwanted state behind.

UPnP learns from the Internet's success and heavily leverages its components, including IP, Transmission Control Protocol (TCP), Universal Datagram Protocol (UDP), Hyper Text Transfer Protocol (HTTP), and Extensible Markup Language (XML). UPnP involves a multi-vendor collaboration for establishing standard Device Control Protocols (DCPs). Similar to the Internet, these are contracts based on wire protocols that are declarative, expressed in XML, and communicated via HTTP.

Universal Plug and Play (UPnP) architecture supports zero-configuration networking and automatic discovery of services, where DHCP and DNS servers are optional. The UPnP architecture has the following universal features:

- It is independent of the underlying physical media and transport mechanisms
- Devices connected the UPnP network can be implemented with whatever programming language and operating system
- UPnP technology enables vendor control over device user interface and interaction via a browser

UPnP is not only a technology, it is also an outcome of a cross-industry UPnP Forum, which has in November 2002 more than 500 industry members. The primary task of that forum is to produce Device Control Protocols (DCPs) that describe standard methods for device interaction using XML. The UPnP specification is still in a preliminary stage; major issues like security have not yet been addressed.

The UPnP specification contains six layers: (0) getting IP addresses of the devices, (1) discovery of the devices, (2) obtaining the device description, which includes service description(s), (3) control of UPnP devices, (4) event messaging, and (5) presentation. Layers 0 to 2 exist in all UPnP-enabled devices and control points, but the rest of the layers are optional. The UPnP protocol stack is presented in Figure 1, which shows the UPnP vendor specific layer above the layer defined in the UPnP Forum. The UPnP device architecture specific parts of the application layer above the HTTP protocol layer are UPnP Forum and vendor independent.

UPnP-network-device implementers use protocol standards, such as GENA (General Event Notification Architecture), SSDP (Simple Device Discovery Protocol), and SOAP (Simple Object Access Protocol), to enable automatic discovery and description. UDP is used for discovery and events because it is multicast. TCP handles description, control, and presentation. A device uses HTTPMU to broadcast its presence to the network, and a control point uses HTTPMU to ask what devices are present.

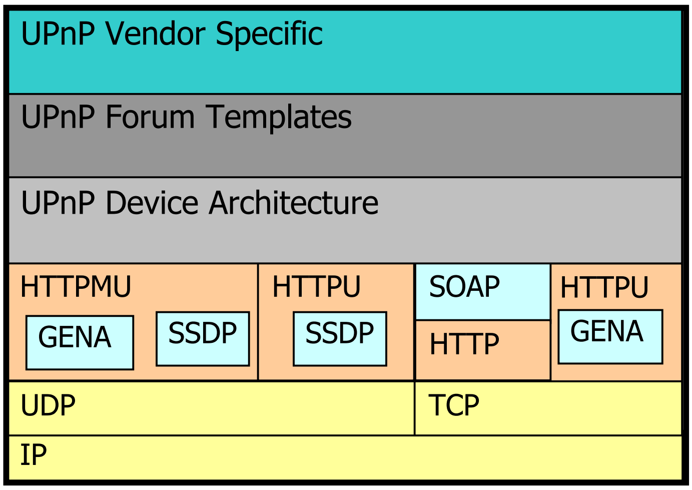

Figure 1. UPnP Protocol Stack [2]

When a device is added to the network, it can advertise its services to control points on the network, and when a control point is added to the network, it can search for devices of interest on the network. Both of these happen by using the UPnP discovery protocol. The principle of the UPnP discovery protocol can be studied from Figure 2, where devices advertise their services to control by multicasting advertisement messages to the control points in the system. On the other hand when a control point is added to the network, it will multicast search messages to the home network, and the devices in the network will respond as unicast messages to the device, which sent the search message.

The device description contains several pieces of vendor-specific information, definitions of all embedded devices, URL for presentation of the device, and listings for all services, including URLs for control and eventing. In addition to defining non-standard devices, UPnP vendors may add embedded devices and services to standard devices.

When a device is advertised with its services, a control point can ask those services to invoke actions and the state variables of the services can be polled. Control points may invoke actions on a device's services and receive results or errors back. The action, results, and errors are encapsulated in Simple Object Access Protocol (SOAP), and communicated into HTTP requests and responses, respectively.

Eventing is linked with the control where control points send actions to devices. Through eventing, control points listen to state changes in device(s). Eventing messages are delivered via HTTP (over TCP/IP) that has been extended using General Event Notification Architecture (GENA) methods and headers.

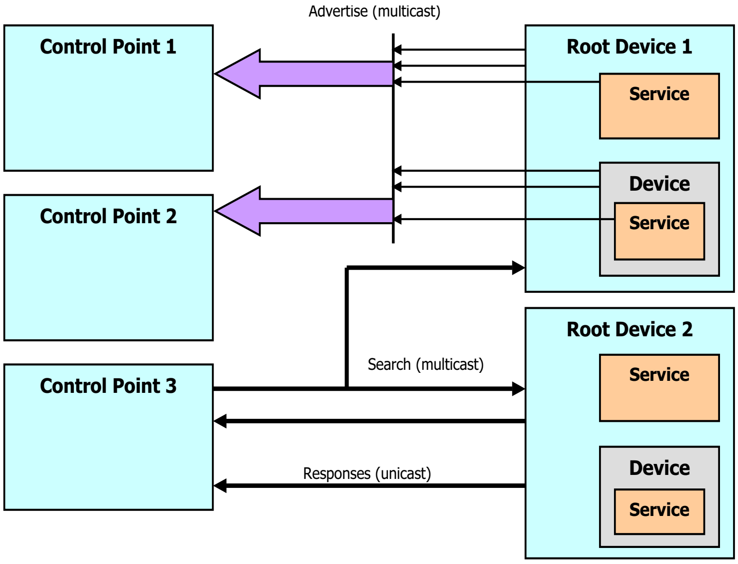

Figure 2. UPnP Discovery Protocol

Unlike the UPnP device and service templates, the capabilities of the presentation page are completely specified by the UPnP vendor. The presentation page is not under the auspices of a UPnP Forum working committee, but the presentation page has been defined to be made with HTML 3.0 or later version. Other design aspects, such as the capabilities of the control point browser, scripting language or used browser plug-ins, and means of interacting with the device, are left to the vendor to specify.

3.2 IPv6 and UPnP Technology

In the future IPv6 technology is entering also into home environment, but its use in conjunction with UPnP technology requires the following aspects to be considered:

- UPnP technology currently uses IPv4 as the underlying network layer for all communication. When IPv6 needs to be used as the network layer, the UPnP protocol and specifications need to be modified accordingly.
- Residential Gateways (RGs) at the edge of home networks are regarded as Internet Gateway Devices (IGDs). The support and administration of IPv6 and IPv6-related functions used in home network request for standardized means to configure the IGDs using the UPnP protocol.
- A default configuration of the UPnP IGD should automatically detect all the IPv6 services present in the attached service provider network and advertise those services in the home network. In the absence of IPv6 services in the provider network, an RG should have the ability to support one of the transition models between IPv6 and IPv4 networks.

- Endpoints such as PCs and STBs should detect the presence of the IPv6 capabilities of an UPnP Internet Gateway and use them.

4 Home Networking with Audio and Video Applications

People purchase increasing variety of digital multimedia products for their home, and nowadays digital content is available from the Internet, PCs, Digital Video Broadcasting (DVB) receivers (satellite, cable or terrestrial), Compact Disc (CD)/ Versatile Digital Disc (DVD) players, camcorders, digital still cameras, portable audio players. The content is usually located on hard disc, CD/DVD disc, memory module, etc. and these locations may not be close to the location, which is preferable for the consumption of the content. In Figure 3 is illustrated a possible wireless home networking environment with broadband connection using Asymmetric Digital Subscriber Line (ADSL) technology, and digital set-top-boxes (STB) with connection to DVB broadcast network.

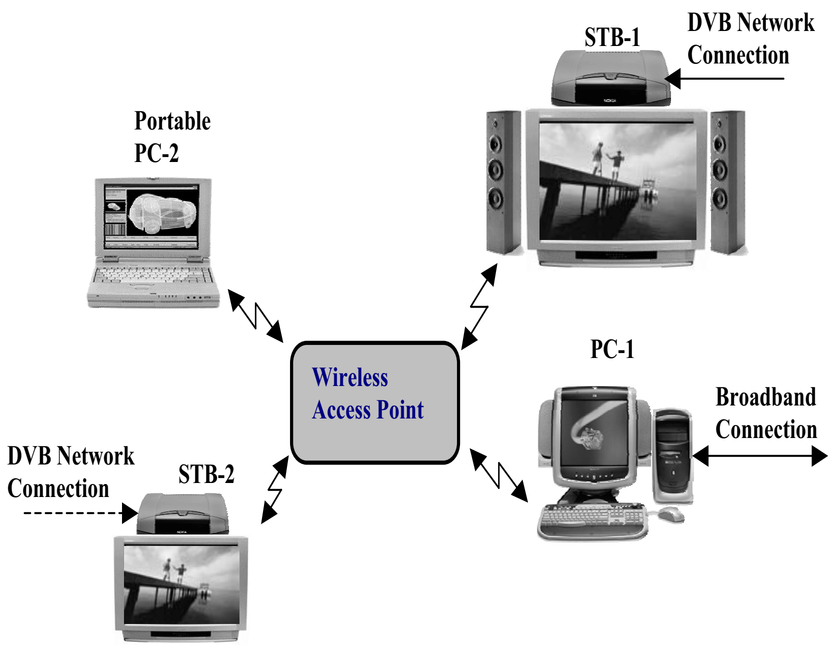

Figure 3. Digital Home Environment with Wireless Networking

We could imagine some future situation, where mother in the family is receiving digital transmission from DVB network via STB-1, and kids are downloading or streaming some cartoon from the hard disc of STB-1 to be decoded on STB-2. Father is working on his PC trying to download some files from his portable PC over the wireless network. A friend of kids arrives having PDA with MP3 playback capabilities, and (s)he wants to search available MP3 files anywhere in the network. But before (s)he can access to the wireless home network, (s)he must pass user and device authentication check, and also authorization check for the access rights to certain servers, files, and actions in the system. The implementation of the home network in this example may not be optimal, but very likely wireless home network scenario in the future.

If the described AV (audio/video) application utilizes UPnP architecture in the home network, there will be several media servers and media clients, and at least one UPnP control point. The media server has access to entertainment content and can send that content to another UPnP AV device via the network. A media client is able to receive external content from the network and consume it in local hardware. We can imagine the use of various content formats, which could be transferred over the wireless network using such transfer protocols and content formats, which both the server and client both support. In the described network many of the devices may contain both the server and client in the same device.

5 Authentication and Authorization

When we are dealing with a very small and simple home networks, the security level could be very low, and the UPnP type operations could be made very straightforward with very simplified authentication schemes. Occasional home network users should not have access to sensitive data or network connections. The access rights to the home network can be made secure by using sophisticated authentication and authorization methods, and eavesdropping of sensitive data and expensive services can be controlled by using multi-layered authentication and authorization methods.

5.1 Authentication Principles

Authentication is a process, where a network user establishes a right to an identity. There are several types of techniques, which can be used in the authentication process: passwords, biometric techniques, Smart Cards, certificates, etc. The authentication process can be divided into two parts: (1) identification, and (2) verification. In the identification process a user requests access to a domain or network by claiming a certain identity based on user name or identifier (ID). The verification process can be based on the following three approaches [5]: (1) proof by knowledge, (2) proof by possession, and (3) proof by property.

The proof by knowledge is usually accomplished by checking the secret password, which is used in the login process. The proof by possession can be based on the ownership of a Smart Card or some other physical component, which must be connected during the login process. The proof by property can be used so that the verifier directly measures certain biometric properties of the user, such as fingerprint or retina print. Proof by knowledge and possession or their combination can be very well applied to home network, but the proof by property is principally limited to the authentication of human users by a host equipped with special measuring instruments. User identity is established at login, and all subsequent access-control decisions and accounting functions are based on this identity. Correct user authentication is thus crucial to the functioning of a secure system.

The authentication process is required to ensure the authenticity of the user (and the host) identity, which is not used only for the access control, but also for billing purposes. When the home network is based on wireless technology, mutual user-host authentication, whereby communicating parties verify each other's identity, is usually required to ensure adequate security.

Another view of the authentication is the authenticity of data or message, where the authentication means assuring that the data or message is from correct source. Data or message authentication can be ensured by using asymmetric key cryptography generating digital signatures with the help of signer's private (secret) key, and the receiver can check the authenticity of the digital signature by decrypting the digital signature with the public key of the signer. If symmetric cryptography is used both the transmitter and receiver have exchanged secret key, which they use for Message Authentication Code (MAC). The symmetric algorithms used nowadays are not so secure as the widely used asymmetric algorithms, but the encryption and decryption in symmetric algorithms can usually be processed much faster than in asymmetric algorithms [6]. In the authentication process the required algorithm speed doesn't dictate the selection of the cryptographic algorithm, but for the content cryptography the symmetric algorithm is more suitable. The integrity checking of the incoming messages or commands is tied to the authentication process. The authentication should contain the integrity checking, which can usually be achieved by including all the fields in the message or command to the digital signature calculation process.

Some examples of cryptography technologies, which can be basis for the authentication processes [6]:

- Symmetric key cryptography: the symmetric key is shared by both communicating parties (DES and Triple-DES are the most common algorithms, which have recently started to be replaced by AES algorithm)
- Asymmetric key cryptography (public/private key technique): public key known by both communicating parties, but the private key is secret (RSA is the most common asymmetric key algorithm).
- One-way hash function technology (MD5 or SHA-1, for example).

5.2 Authorization Principles

When a user is requesting an access to a home network, (s)he must get the authentication to the network as explained in the previous paragraph. If the home network is such that all users have the same rights, the authentication would be enough for the user to get access to all services in the home network. Because home networks may contain some restricted data, parents want to restrict the use of some costly services, visitors are given only very limited access, etc., there is a need to form several user classes. This requirement demands for some kind of authorization process. An authorization process based on fine-grained control of access rights and service levels leads to complicated usability problems, which should be avoided.

The home network must contain authorization service, whose security information contains identities, group identities, role information, device ownerships, actions associated with action parameters, etc. Some security information is generic and static in nature, such as identity of an authorized user. Role based security information can be specific but still somewhat static in nature. There can also be security information, which is specific but dynamic, such as related to specific applications or part of the files in those specific applications. The dynamic nature comes from the tendency for state changes.

The traditional method of using access control lists, but they have seen difficult to administrate. The other well-known mechanism that has been used in the provisioning of the authorization service is a ticket that provides the holder with some type of access rights to dedicated service. The user must acquire the ticket from the system before the access, and it must be presented at the time of access. These tickets are usually protected with digital signatures against unauthorized alteration. If the authorization system is implemented so that the access rights can be resolved outside the application, the ticketing system can work well. If the necessary information to determine the access rights depends on the internal state of the application, the decision on whether or not to allow the request to take place must be made within the application and is dependent on its internal state [7].

5.3 Features of the Authentication and Authorization Solution

Based on the reasoning about the usability of the UPnP networks throughout the paper, we can propose the following approach to the authentication and authorization in the UPnP home network. The home network access is limited to the home network itself or opening a gateway to the Internet, not authenticating or authorizing services outside the home network. In the installation and configuration phase the following set-up procedures must be made:

- Making descriptions and rules for each access level (or possibly also by names), what actions are allowed
- Configuring access levels and rights to different storage devices, their directories, and different actions in the network
- Creating the set of basic users (usually family members) with user names, and giving a dedicated storage space for each user's own use

The installation can be made with the help of sophisticated user interface or can be offered by some service company. When devices under the given user names are first time plugged into the network, there is still need for some set-up procedures:

- The user must give a password, when accessing first time to the network
- There must also be a PIN code or some pairing information exchange between some network device and the newly installed device
- During later accesses only some restricted services may require typing in name, password, or PIN code, otherwise the devices do that with mutual communication.

If the main UPnP control point (having the highest access rights in the home network) is missing from the network during the process, when a new device is connected to the network, the authentication and authorization can be made with the help of some other UPnP control point. Then the highest possible access level is limited to the access capabilities and permissions of the UPnP control point in question.

6 Conclusion

Home networking may very well utilize UPnP technology, but authentication and authorization brings some extra complexity along regardless of the used tehcnology. When wireless home networks become popular and they expand to consists tens of devices, most of them portable, home networks should contain plug and play type of functionality to broad extent. The basic requirements for the home network security management aggressively request installation, configuration, management, and update operations to take place. All this means in practice that plug and play type of networking specially in wireless home networks is very difficult to implement. All of uinstallation and configuration processes could be made easy to use, or could be passed to some external company to take care of.

Universal Plug and Play functionality is, of course, in this approach the basis for plug and play type of operation, but future development of IP technology will minimize intervention in installation, configuration, or access operations also in other kind of ease of use home networks. The importance of security, authentication and authorization will increase in the future. These featurs may seem as first sight not so important in home networks, but due to the increasing complexity of the home networks, their wireless nature, and increasing remote working habits, require these mechanisms to exist with increasing importance.

References

[1] BRENT A. MILLER (IBM), TOBY NIXON (MICROSOFT), CHARLIE TAI (INTEL), MARK D. WOOD (EASTMAN KODAK); Home Networking with Universal Plug and Play; *IEEE Communications Magazine*; December 2001.

[2] MICROSOFT CORPORATION; Universal Plug and Play Device Architecture, v1.0; Microsoft Corporation, USA; June 8th 2000.

[3] SANDY TEGER, DAVID J. WAKS; End-User Perspectives on Home Networking; System Dymanic Inc.; *IEEE Communications Magazine*; April 2002.

[4] VIJAY VARADHARAJAN; Authentication in Mobile Distributed Environment; Seventh IEE European Conference on Mobile and Personal Computing, 1993.

[5] THOMAS Y.C. WOO, SIMON S. LAM; Authentication for Distributed Systems; University of Texas, Austin, USA; 1992.

[6] BRUCE SCHNEIER; Applied Cryptography, 2nd Edition; John Wiley and Sons, USA; 1996.

[7] VIJAY VARADHARAJAN, CHRIS CRALL AND JOE PATO; Issues in the Design of Secure Authorization Service for Distributed Applications; Global Telecommunications Conference, 1998; GLOBECOMM 1998; The Bridge to Global Integration. IEEE, Volume: 2, 1998.