# Global Information Assurance Certification Paper

Matthew J. Brodeur
SANS Security Essentials
GSEC Practical Assignment
Version 1.2e
27 June 2001

# Security Concerns In Home Automation Technologies

## Introduction

The marketing departments of many companies have been selling the promise of smart houses for years. These "Homes of The Future" would make life easier for their inhabitants by automating control of climate, lighting, security, entertainment, and just about any electronic appliance. The residents could be content knowing that they would always be safe and comfortable, have their household chores lightened, and never miss their favorite shows. Unfortunately, in the wrong hands, this dream house could become a nightmare.

Current technologies like X10 and emerging standards such as Universal Plug and Play are turning some of these promises into reality. However, the security of the Home Automation systems themselves is an afterthought at best. By tightly integrating household electronics with a home LAN, one could be giving a system cracker access to not just online information, but physical possessions as well. Security needs to be built in to every device at the lowest level that is practical.

## Defense in Depth

A vital concept in Information Security is Defense in Depth. The military definition of the term is, "The siting of mutually supporting defense positions designed to absorb and progressively weaken attack, prevent initial observations of the whole position by the enemy, and to allow the commander to maneuver his reserve." (DoD) From an Information Assurance (IA) standpoint, this means that any given system should be protected with multiple layers of different types of defensive and reactive security. It should be hard for a cracker to see protected portions of a network, hard to break in, and easy for an administrator or home-owner to react to an intrusion by repelling the attack and repairing the damage. A layered defense makes compromising a network more difficult, and minimizes the effect of a successful intrusion.

While a firewall or filtered gateway should provide perimeter security for Home Automation devices, it is simply not enough. A network is only as secure as it's weakest member. The fact that most Home Automation systems lack any built-in security provisions leaves them open to exploit in a number of ways. These devices can then provide unauthorized access into more secure areas of the network. Where it is possible for general purpose computers to filter connections, authenticate hosts and users, and provide detailed security logging, automation devices often provide none of these provisions. This presents a problem since "Control and automation networks need to be more reliable and secure than the other forms of home networking. For example, a security system cannot tolerate ... intentional attacks from hackers." (Raji)

## X10

The most widely used Home Automation technology today is from X10, Inc. X10 provides appliance and lamp power switching, A/V transmission, physical security sensors, and PC interfaces. X10 uses a combination of RF wireless and power line signaling to communicate between modules. The devices generally have multiple communication channels to choose from in order to avoid interference from other devices nearby. (X10)

While multiple communication channels provide a convenience and courtesy measure, only physical barriers actually prevent an outsider from hijacking a device. Anyone who can physically reach an X10 automated house can potentially attach a control module to an available receptacle or monitor a wireless camera signal. Most of the devices only provide a one-way interface, so they are not even capable of acknowledging a signal. (Kramer) Since there is no authentication or encryption on the devices themselves, it takes only trial and error to gain control of an existing module. At this point the controller has no knowledge of the state of the module, unless it it one of the few capable of bi-directional communication. Once connected to the X10 network, the intruder can gain the same level of access to automated devices that the home-owner has, possibly including the home security system.

## Universal Plug and Play

Universal Plug and Play (UPnP) is being positioned as the technology to allow every electronic device in the home to communicate. It is not an interconnect technology itself, but rather a standard for device control procedures. UPnP is designed around automatic discovery of attached devices as follows:

> UPnP includes five basic phases:
>
> 1. Discovery. In this first phase, control points search for devices and services. Similarly, devices multicast announcements of services they offer.
>
> 2. Description. Once a control point finds an interesting device or service, it requests from the device for a complete description of the device, its component devices, and services.
>
> 3. Control. This phase allows control points to enact changes in the state of a device thus causing the device to perform some action.
>
> 4. Eventing. The eventing phase allows control points to keep in synch with the state of services in which it is interested. Control points subscribe to the event server for a particular service and receive event notifications when that service's state changes.
>
> 5. Presentation. The presentation phase allows a device to host a document, written in standard HTML, which can be a user interface for that device.

(Baumberger, p. 3)

UPnP is quite powerful and flexible. The current specification allows a new control point to be added to the network at any time. The necessary software is included with the latest version of Microsoft Windows (Windows Me) and is planned for inclusion in future versions of most operating systems. Therefore, any standard PC with an ethernet card can become a control point on an IP based UPnP network. Each controlled device has no real preference for which control point it's talking to, or receiving commands from. The controllers are indiscriminate about their communications as well, and will initiate control of any device that are deemed "interesting."

The real risk of a system such as UPnP stems from its flexibility. The design goals include ease of use and simplicity of configuration, so any security model could be viewed as a hindrance. An automated house is at risk from both malicious users and rogue devices. Anyone with access to the physical network, such as with an unsecured wireless LAN, can become a control point.

UPnP's only apparent strength in security terms is be that any changes will be seen on the authorized control points. This allows one to monitor the status of device and respond to unexpected changes. While this does provide a type of security, it is only reactive in nature. It would be difficult to determine the cause or source of the changes, and therefore almost impossible to prevent future problems.

**Internet Integration**

Home Automation networks are now being interfaced with existing home data networks in order to further simplify Home Automation tasks. Many automation devices can utilize or even require a connection to the Internet. Linksys has recently incorporated "Universal Plug and Play (UPnP) open networking architecture into its line of popular selling broadband Cable/DSL Routers, Print Servers, Network-Attached Storage and upcoming line of Residential Gateways solutions." (EHOnline) Moves like this one make interconnection of home electronic devices as simple as attaching power and network cables.

Many users want to be able to control all aspects of the house from a single point, and have that system schedule routine tasks. Some users enjoy the convenience of controlling household systems while away from home, either from another Internet connected computer or a telephone. A few appliances will even allow remote monitoring services to access them for service contract purposes.(Echelon) With the absence of tightly integrated security, this can be an open invitation to hackers.

Once an automated house and all of its components are connected to the Internet they are potentially exposed to the entire world. A determined cracker can take advantage of weaknesses in the home's network and gain control of the house itself. After taking command of lighting, security sensors, and cameras, the intruder leaves the home-owner blind and possibly defenseless against a physical attack. At the very least, access to automation controls would allow for the type of mischief that less serious crackers are known for. While possibly not damaging, actions such as resetting lighting and climate controls could prove costly in energy bills, and reprogramming of a user's VCR could be frustrating.

A Home Automation system that includes third party monitoring and control introduces yet another concern. In this case the home-owner must account for the integrity of this company's employees and systems. Since trusted access is being allowed into the home network, any insecurity in the remote network introduces additional risk to the home. If the monitoring service is compromised, it's likely that the attacker would have complete access to the managed appliances in each home. As in any trust scenario it is vital to analyse the integrity of the connection and authentication schemes as well. A connection that is spoofed as coming from the third party could be accepted by a system that relies on host based authentication only.

**Solutions**

As previously stated, the best security derives from layered defenses. Common practices such as perimeter protection and user authentication will help secure any Internet connected system, especially a Home Automation network. Additional considerations need to be made when connecting sensitive home systems to a network. Certain security features could be added to current technologies in order to provide stronger, deeper layers of defense.

A design goal of many Home Automation systems is ease of setup and use. To accomplish this, many devices talk freely with one another without any sort of authentication. Future versions of technologies such as UPnP could include device authentication as part of the identification process. A Public Key Infrastructure (PKI) solution could be implemented to provide positive identification and authentication of devices and control points. All devices on a network would have their own key that must be recognized by the other devices. New devices would have to be enabled by installing their key on the server before they could communicate on the network. This would add some complexity to initial setup, but also greatly reduce the possibility of having unwanted devices added.

Future specifications could also include provisions for devices to have their feature sets restricted by the user. A user should be able to disable features he or she doesn't intend to use in order to prevent anyone else from taking advantage of them. If the Home Automation network is intended for monitoring and alerting only, it wouldn't make sense to have appliance controls active and accessible from the network. This idea closely parallels the computer security practice of disabling all unneeded services on a host.

The devices themselves need to have some concept of user authentication built in. Password protected administration accounts would allow the device to be configured by a privileged user while leaving basic features available for common use. A user may choose to allow almost complete access to the device, but require a password to enable or disable features. By doing this, the automation server can perform whatever functions are deemed necessary, but an intruder is prevented from re-configuring the device without first cracking into it.

Devices that currently used simple powerline or wireless signaling will need to incorporate content protection of some sort. Even a simple fixed code based scrambling of the signal would stop most opportunistic attackers. Physical security systems relying on these technologies must implement strong encryption to protect their signals. Technologies such as IPSEC would find a home in this application. While usually only considered for use over an untrusted Wide Area Network, IPSEC can also be applied to extremely sensitive communications in an otherwise "safe" environment.

In situations where a compromise of the data portion of the network is likely it would be advisable to segregate the automation equipment. Anything that does not need to be connected to an Internet feed would not be. Those devices that need outside connectivity could either have a dedicated link or a tightly restricted portion of the existing connection. Using intranet filtering and firewalling prevents unauthorized or unexpected communications to or from the automation devices from affecting other parts of the network. This would be especially important in the case of the third party service provider, where their own data network could be a threat to their clients' automation systems and data network.

**Conclusions**

The current offerings in Home Automation are both exciting and frightening. The means to automatically manage almost anything that uses electricity is available today. Until security is taken seriously in these systems, though, there is great risk in doing so. The favorable trend of making high tech devices easy to use is resulting in a diminished focus on reliability and safety. Designers of these solutions need to think about security at every level and stop considering it to be "Somebody else's problem."

**Works Cited**

Baumberger, Daniel. "Intel® UPnP Software Development Kit V1.0 for Linux." Rev 1.1. 14 Sep 2000. ftp://download.intel.com/ial/upnp/upnpsdkarch.pdf

US Department of Defense (DoD). "DOD Dictionary of Military and Associated Terms." 30 May 2001. http://www.dtic.mil/doctrine/jel/doddict/data/d/01834.html

Echelon Corporation. "Linking to the Internet." 28 May 2001. http://www.echelon.com/solutions/Markets/home/linking.htm

EH Publishing, Inc. "Linksys to Incorporate Universal Plug and Play (UPnP) Capabilities Into Line Of Networking Hardware Solutions." 30 Apr 2001. http://www.ehonline.com/archives/EHBreakNews1_043001.html

Kramer, David. "Home Automation and Security." v1.1. 22 Jun 2000. http://thekramers.net/hademo/index.html

Liu, Andrew. "Universal Plug and Play Connects The Home." Intel Developer Update Magazine. July 2000. http://www.intel.com/update/departments/initech/it07002.pdf

Raji, Reza. "Home Automation And You." Home Toys Article. May 2000. http://www.hometoys.com/mentors/raji/may00/intro.htm

X10, Inc. "X10.com - Your Home Automation, Entertainment and Security Supersite!" 28 May 2001. http://www.x10.com/homepage.htm