Security in Private Networks of Appliance Sensors and Actuators

Stu Mesnier, csm1@seas.wustl.edu (A project report written under the guidance of Prof. Raj Jain)

Download

Abstract

An explosion of networked appliances is approaching. The idea of wiring home appliances for control and analysis has been around for decades [X10 Industry Standard], but market and technology obstacles have long prevented acceptance. Cost, convenience, compatibility, reliability, and utility are among the top issues retarding consumer acceptance of network-connected appliances. Cost has been dropping as a result of Moore's Law and its corollaries. [Moore65]. Compatibility continues to increase as manufacturers agree upon standard protocols. Utility refers to the incremental services a consumer derives from network connectivity, and convenience refers to the transparency of establishing and maintaining the network connection, including, if necessary, changing or charging batteries. Reliability is always a genuine concern and being rapidly addressed because of pressure from mobile devices.

Technological barriers are lowering and soon companies will offer specialized but useful services relying upon web-enabled appliances and devices organized into Private Appliance Networks, or PANs. Despite progress, special considerations are necessary for home and small business devices connected to a LAN and internet. This paper introduces the subject, offers a background existing communications and security services, and exposes and analyzes some activities and vulnerabilities that are peculiar for private home and small office appliance networks.

Keywords: private appliance network, PAN, appliance, web-enabled device, access point, security, cryptography, vulnerability, attacks, defenses

Table of Contents

1. Introduction

The value of web-enabled home appliances has centered on contrived and unproven but emotionally appealing convenience and novelty applications. Have you heard of the web-enabled microwave? It reads a product bar code and sets cooking time appropriately for the power that it can deliver [THALIA01]. This can save the consumer a few keypresses, and few seconds of reading the packaging, and making mental adjustments to compensate for the oven's power and the product's temperature. Sadly, the web-enabled microwave can only obtain information regarding the energy required to heat a standard sized portion of a product from a typical starting to a typical ending temperatures, though perhaps additional, non-web related sensors can detect actual serving sizes and temperatures and adjust cooking times and energy profiles accordingly. It is an open issue how the web-enabled microwave oven will determine desired final temperatures or how they are met, or what mix of items might be present for heating in the absence of product barcodes? But if you don't mind storing unrefrigerated dinner in your oven all day, then you can text or email it to start cooking so that dinner is ready to eat as you are walking in the door!

Do you rely upon a programmable coffee maker that you load with water and fresh grounds then program to brew 10 minutes before you awake? If so, then you may wish to upgrade to the web-enabled version. Why? Because maybe on Sunday you want to sleep a bit later yet still wake in time for church, so you don't program the coffee maker but only your alarm clock, and since the two talk over the network, the coffee maker adjusts its start time to your new alarm clock setting, and even then only if you set the alarm. In fact, when you set the clock, you are warned if the brewer needs charging with water and fresh grounds! Unfortunately, without additional robotic controls you might run out of fresh java because you have unexpected guests, or brew too much, or the wrong flavor. And you will still have to fry your own bacon and eggs even if the toast is timed perfectly to pop up as you walk in.

Cost, convenience, and utility are all practical barriers to the adoption of complex technology to accomplish relatively simple or minor tasks. Nonetheless, some appliances are amenable to web-enabling, and not merely for vanity or trivial convenience. Appliances that supply security and durable appliances that required maintenance to forestall or prevent costly repairs are candidates for web-enabling. In place of a web-enabled coffee maker, you may prefer that your furnace alerts you and possibly the service company that an operational fault has disabled the system. So even if you are on business seven time zones away you can take action for quick and necessary repairs to keep your water pipes from freezing and bursting. In order for the service technician to enter your premises, you will need to prepare and activate a one-time-use password allowing entry and access to only the parts of your home containing the furnace and its controls.

Behavior of web-enabled devices generally fall into two categories: sensing and actuating. Sensors detect states or perform measurements then deliver the information according to a policy. Depending on the nature of the device and the importance of its information, a sensor could send information periodically (such as by time schedule), sporadically (such as when predefined thresholds are exceeded), or in response to command. Actuators cause a change to the device state, usually to cause work to be performed or prevented. Enabling network connectivity allows both kinds of activity, not only locally, but also globally when appropriate.

Three components are necessary to enable web (or Local Area Network, LAN) connectivity: the special sensing and activating systems required to support a device's ordinary utility, reporting and control software, and a communications link. Each of the first two components will contain numerous elements engineered for the type of device it supports, such as thermocouples in furnaces or refrigerators, and pressure sensors in air conditioner coolant lines, or magnetic locks in security systems, along with application software for configuring, displaying status, and initiating operations. Building in cost-effective utility and convenience both in terms of connectivity and ease-of-use are the responsibility of the designers of these first two components.

Much of the work of communicating data from devices to control stations is already established in the form of standard network configurations and protocols. However, adding a class of consumer-oriented devices to a network offers special challenges for communications and security engineers. In many cases, existing standards and protocols will meet or exceed requirements for secure and reliable operation. Devices that employ standard household current are already connected by wire and can employ it effectively for many applications. Other devices, such as security or environmental sensors can rely upon wireless technologies. However, there are special challenges facing designers of network and web-enabled devices and appliances used in homes.

Wireless devices are especially vulnerable to hackers. This is not news. Wired Equivalent Privacy, WEP, and WiFi Protected Access, WPA, among other methods, were designed to provide security both in terms of privacy and integrity. These qualities are essential, as home appliances offer a rich pool of temptations and motivations for hackers to attack. Social miscreants may simply desire to overtly or covertly hijack control of your appliances. Commercial hackers may attack in order to cripple an appliance forcing either a repair or replacement. Thieves would attempt to disable your perimeter security allowing undetected intrusion. Wired devices communicating using power circuits are not immune! Every power socket on the outside of the home could act as a portal into the home's LAN.

This paper examines some of the peculiar vulnerabilities of homes and small businesses that are motivated to enhance their areas with network and web enabled devices and appliances.

2. Background

Aside from cost, utility, and value that consumers perceive by networking their appliances, they are absolutely concerned by the privacy and reliability that supports them. "Dumb appliances", DAs, defined here as "appliances (and devices) not connected to a LAN or internet", usually work predictably. Of course they do wear out or suffer other hazards that impair their operation, but these are among the normal expectations for appliance behavior, even if undesirable. DA usually do not require more than simple instruction to operate safely and effectively.

2.1 Essential Features

Networked appliances should offer similar ease-of-use, enhanced utility, without a decrease in predictable and reliable operation. Consumers will not tolerate a networked alarm clock that spoils their expectations because a mischievous hacker reprograms it remotely. They will not tolerate service technicians arriving unexpectedly to service a major appliance because a spoofed service request was received by the repair company. Consumers will not tolerate garage doors that mysteriously open under command of marauding thieves. In fact, they do not, because 40-bit security codes and predictable random nonce schemes are built in to the better remote door openers. [TexasInstruments1300] Similar levels of security, or better, must be achieved by appliances used in the home in order for consumer adoption to occur.

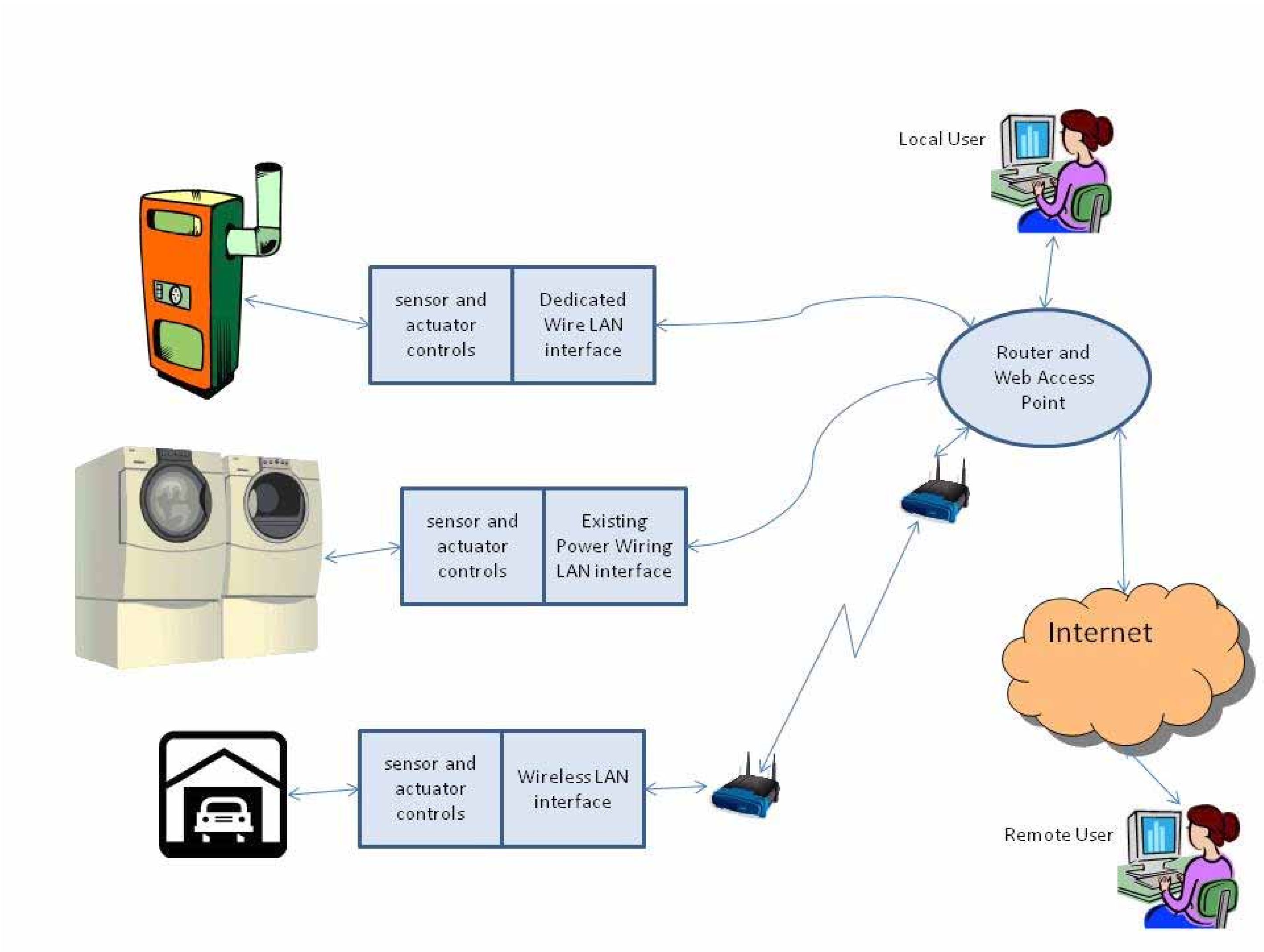
Local User
sensor and actuator controls
Dedicated Wire LAN interface
Router and Web Access Point
sensor and actuator controls
Existing Power Wiring LAN interface
Internet
sensor and actuator controls
Wireless LAN interface
Remote User

Fig 1. A Private Appliance Network connected in a single home network using three types of physical access:

2.2 Communication Mediums

Regardless the type of device, any of the three physical mediums are acceptable, however certain protocols and information requirements may require larger bandwidth and introduce unacceptable delays. Each medium offers special advantages and disadvantages.

Dedicated lines offer the highest security and bandwidth, with transmission range well suited for home and small business LANs. This realm is well established with numerous mature technologies and expertise available. Cost, both for equipment and wiring, could be a disadvantage. Installation of wiring is likely to be problematic for many users in existing structures, but would be nearly transparent if built into new homes and offices. Cost of the interface is reduced by using lower bandwidth (acceptable for many home applications), and wiring may be performed by appliance service companies supplying either DA replacements or retrofits. A full range of network communications are instantly available for appliances networked over dedicated wires. Little is necessary in the way of security considerations inside the LAN, however the devices connected in this manner are still vulnerable to attacks originating from the internet.

Using a home's existing A/C power wires may be a more convenient method for communicating with plug in appliances, such as clocks, lamps and other on-off devices . Not particularly well known are the X10 [X10 Industry Standard] used both in the USA and internationally, and KNX [KNX Standard09] used mainly in Europe and China. The X10 standard was invented in the mid 1970's and has been improved as various vendors contributed new inventions, even wireless and infrared communication mediums. While somewhat cost effective, it is generally only useful for unidirectional communication of actuation commands from a control module to any networked slave devices. X10 suffers from many limitations making it unfit for all but the simplest of control scenarios: bandwidth of 60 bps, 256 addresses, 16 functions, and little or no provision for feedback or acknowledgment. Is supported by an ISO standard, ISO/IEC 14543-3 and by over 100 independent international manufacturers, some quite well known, such as Siemens, ABB, and Electolux. As with X10, KNX offers only limited bandwidth of about 2400 bps [Konnex Association04]

While the availability of X10 and KNX seem unsuitable for all but the simplest appliance controls, they demonstrate the viability of sharing existing home wiring for connecting some appliances to an access point. Some extra security precautions are necessary, as well as special considerations for loss of communication if a circuit breaker or fuse opens a branch. Unlike dedicated wires, normal home power distribution wires are connected to the homes of neighbors, raising the possibility of neighborly mischief. Also, any exterior power sockets provide a handy connection point for an attacker, and with a limited number of addresses and functions, it would take little time to play havoc in a victim's home.

Like networks using dedicated wires, wireless communication is also mature, robust, and high speed. There are several physical and data protocols from which to select, as well as variety of security features. Wireless communication frequently means RF communication, and that means exposure to a variety of passive and active system attacks. Industry has recognized this exposure and responded, particularly in the realm of mobile communication. Costs for such complex technology are reduced by the shear quantity of mass produced, standardized circuits, and because revenue models collect monthly fees from consumers. Some of these cost advantages may not be as available to the leading edge of the web-enabled appliance explosion, but as simpler and less demanding interfaces and security protocols are developed, these costs should become acceptable for even low-cost appliances.

2.3 Battery Power

Wireless devices are frequently mobile and thus battery operated. In the case of battery-operated sensor devices, longevity must be balanced with security considerations since security functions place a surprising and significant current drain on a fixed energy budget. Consumers do not like to replace batteries, so in the case of specialized battery operated passive sensor, and even active appliances, care must be taken to balance security needs and battery capacity. Challenges and opportunities arise from sensors relying upon batteries for power. These devices may be designed solely for use with batteries, or they may be forced to rely on batteries for backup power, for instance when there is a power outage, or a circuit breaker opens. Non-volatile memory keeps associations and keys intact, battery power keeps data intact.

Studies have shown that certain crypto methods are much more costly than others. In particular, asymmetric cryptography is approximately 5 times more costly in energy cost per bit than symmetric key cryptography. [Potlapally06, Wander05]. These studies suggest that 50% or more of a battery's energy is expended solely in cryptographic calculations, and that efficiency decreases with smaller messages. These results suggest that for battery operations, key generation should be conducted primarily by non-battery powered devices then communicated securely to battery powered ones, and that data from sensors should be accumulated as much as possible for transmission in efficiently sized messages, that is, as long as possible.

3. Common Private Appliance Network Features

Private home and small office based appliance LANs differ from the open internet in at least two remarkable ways. First, most of the devices communicate in a fixed architecture. Although some flexibility for establishing connectivity is necessaryl, topologies are generally flat, with one access point and single hops serving all connected appliances. Second, topology is stable. Unlike the internet, and especially unlike public access points connecting with mobile hosts, private home appliance LANs support a fixed, or slowly changing, mix of connected hosts. This offers some opportunities for establishing strong associations and endpoint hiding that are unavailable to public access points. While convenience and ease of installation and use are user friendly goals of Private Appliance Networks, PANs, forming the initial host/access point association is no more complex than pushing a button, plugging in a Universal Serial Bus, USB, device, or bringing an Radio Frequency Identifer, RFID token into close proximity with the merging appliance.

The network interface component turns a DA into a networked appliance that is readily web enabled through a web access point and software. The circuitry for sensor and actuator controls is obviously wedded to the function of the device, and a specialized interface, likely in the form of shared memory, exposes the data to reading and writing by the LAN interface, LANI circuits. LANIs will differ slightly depending upon physical communication channel they support and the sophistication of security they must provide. Wireless devices are likely to require greater security provisions simply because of the potentially hostile environment in which they must operate. Nonetheless, LANIs will share some common features.

The best way to ensure private data exchanges is with all data transfers being encrypted, including the unique Medium Access Control Address, MAC address, or Object Identifier, OID. The LANI must have sufficient non-volatile memory, such as electronically erasable programmable read only memory, EEPROM, to store master keys and the MAC address(es) of legitimate associated APs. Each LANI will also have sufficient RAM and processing power to accomplish its encryption, decryption, authentication, and integrity functions, including random number generation and hashing.

The four phase operation described by 803.11i is probably more complex than necessary. [Kurose07]. It assumes that any user or device can connect to the net through any AP. This is not the case with PANs. Also, it is actually important that appliance devices associate with precisely one AP and communicate exclusively with it until told otherwise. While the use of Master and Temporal keys are incorporated in PANs, the added burden of net connectivity to an Authentication Server is unnecessary, and the AP has all provisions needed to conduct its own authentications and key generations.

4. Common Private Appliance Network Functions

Every PAN will require adding, configuring and removing devices. These are discussed here. At a minimum, the PAN requires at least one device or appliance with a LANI and a channel enabling it to communicate (either wired or wirelessly) with a private AP. In all likelihood, the AP will be connected to both a PC and the internet, and while virtually pointless, the AP may not be connected to either. Refer to Figure 1.

4.1 Adding an Appliance

Methods for adding a device into a wired association with an AP are trivial, unless it is possible for an attacker to make an unauthorized and undetected physical connection. In this case, the best defense is a service that can report changes to the network host list to the consumer (or his trusted agent) so that the addition (indeed any changes) can be verified.

Adding a new device in a wireless RF network is only slightly less convenient. This activity should be required at most just once per valid access point. At least one method is available that does not require an operational PC connection. It employs a physical RFID token that can be read by the new host device. The RFID token is brought into close proximity with the new appliance, which acknowledges the close contact and creates a master key using Diffie-Hellman, DH, key exchange [Kaufman02]. The token is returned to the access point and then master key is encrypted using the current session key in the RFID token to encrypt the new master key. The AP then communicates directly with the new host. This initial association key establishment must be completed within a short duration, or the sequence must be repeated.

In the event that an unauthorized sniffer is able to observe the key exchanges, they would be unable to determine the shared secret key establishhed by DH. Periodically, perhaps daily with highly active hosts, the master key is replaced. In the event that the RFID token passes several devices and completes DH exchanges with more than one, all of them are examined by the AP when the RFID token is returned, and the key exchange association is finalized only with hosts with the new MAC addresses.

In the event that the RFID card is lost or stolen, the memory of any previously saved DH key particles and encrypted MAC addresses are erased as soon as they are absorbed by the AP. Also, one RFID card is as good as another, so a replacement in case of loss, theft, or damage, is trivial. The RFID card is simply a secure way of transporting authenticating identity information between the host and AP.

Other methods are less secure for establishing the association because of the possible presence of nearby but illegitimate APs. If an operational PC is connected to the AP or to the new device, then a simple and secure method can associate the new device with desired AP, though some specialized information (the hardcoded MAC addresses of the device and AP) are needed to prevent spoofing from successfully hijacking the association.

4.2 Configuring Appliances

Configuration is accomplished in a manner consistent with the device or appliance it supports. For many appliances, configuration of the sensor and actuation controls are factory supplied. Connectivity to legitimate APs is accomplished in the preceding step. Naturally, a consumer spending the extra money for a networked appliance is likely to adjust any configurable portions to fully utilize and exploit the investment. This may mean routing sensor information to a service facility and duplicates to personal email or text message accounts. Notification of sensed data may be routed to analysis software, either provided by the appliance vendor or by third parties to observe and manage numerous appliances from different makers. Reporting intervals and conditions may be configurable, and key management intervals may be configurable , as well. Application level configuration may allow different devices to interact, so that the novelty of starting a coffee maker depending on your bedroom alarm clock setting, or the necessity of accessing your perimeter security from a remote PC are enabled. Configuration takes place at different locations in the network depicted in Figure 1.

Depending on the appliance, sensor data transmissions may be configurable. Factory supplied settings may be inappropriate or incomplete, though any device or appliance should be able to function without a network connection or any user configuration requirements. Sending sensor data can be accomplished numerous ways. It can be accumulated and sent at regular intervals, sent only when significant changes occur, sent only when requested, or any combination. Memory and power provisions regulate the amount and duration of stored data. Data could be purged automatically or only upon acknowledgement of receipt. Policies could control transmission during times of ample power, or of limited power, such as during an outage or low battery. (Likely low battery transmission would always be transmitted without regard to long interval transmission policy.)

Configuration also extends to transmission of commands from the user via the AP to the networked appliance. Policies for some appliances are set so that only a user attached to the AP can actuate a control, others may respond to commands from a authenticated users from over the web. Users can empower trusted vendors to activate tests on specific appliances, as well.

4.3 Removing an Appliance

Removing devices from the private network is almost as common as adding new ones, but much simpler: the device is simply removed, disabled, or destroyed. All that is necessary is that the user be informed that the appliance is no longer active or responsive. This protects against the possibility that the interface has not been damaged or broken, and also that it has not been hijacked by an attacker's rogue AP. If legitimate, the absent equipment can be deleted from the AP list; if not, appropriate actions to repair and reset and re-add the appliance can be taken.

4.4 Adding or Replacing an Access Point

Adding an additional AP cannot be accomplished using an RFID token to adding each device to an new AP. Doing so could easily open an opportunity for a bad guy to trick a device into communicating with his own AP. Instead, the original and new APs are connected to a PC operated either my the system owner or trusted surrogate. Using configuration methods, all appliances or a subset are given an association to the new AP. At the same time, former association to the original AP can be severed.

In the even that an AP becomes inoperative, before the method of adding a new AP to an existing PAN can be used, then the method of using an RFID token described in Section 4.1 is used. In this case, each device LANI is reset and then a single association is established with the replacement AP.

5. General Problems and Attacks

Wireless appliances are especially vulnerable to noise and messages originating from various sources. Physical medium transmission modulation techniques such as frequency hopping and orthogonal Frequency Division Multiplexing are incorporated in Link Layer communications standards such as 802.11x and Bluetooth enabling them to isolate clear signals and portions of clear frequencies. Security protocols such as WEP, WPA, and Extensible Authentication Protocol, EAP assure private communication between authenticated devices. These protocols are well established and confirmed to be effective. Adding new devices using the aforementioned procedure makes cracking, spoofing and sniffing, at least among the private network, extremely difficult.

Some novel attacks are possible against private home and office appliance networks. Most are made possible because of wireless connection to an

AP, while others are created by longer connections from an AP to repair and maintenance vendors, including the legitimate user, over the internet. Most are defeated by using proper security protocols and firewall configurations. Naturally, these must be easy to understand and use in order to be used properly and effectively.

5.1 Sniffing Attacks

These are generally only possible using RF signals in the air. However, since it is possible for the home's own power wiring to be used, this makes even external sockets and even neighbors power wires potential sniffing points. These are easy to defeat by installing low pass filters across the wires inside the home but near the exit points.

Sniffing could indicate makes and models of durable appliances allowing a company to sell replacements or maintenance and repair services. This attack is easy to mount unless the MAC address is encrypted.

Sniffing a device's operational status allows a competitor to respond earlier than a legitimate vendor to provide service. Common devices will repeatedly send identical information, so a sniffer may listen for longer periods to discover patterns in among changing information then make reasonable guesses about which devices are sending, and what kind of information is transmitted, if not specific details. It may be possible to pinpoint devices by patterns even if MAC addresses are encrypted and then pre-empt a legitimate service vendor. This form of sniffing can be defeated by encrypting with a new initialization vector or session key with each transmission.

Sniffing indicates where security sensors are located and which are active, is a bit more serious threat to home security, but as easily defeated as the previous motive for sniffing. In addition, devices that report only status changes, such as might be the case with security sensors when the owner comes and goes, could themselves be disguised by sending at random times even when no significant changes trigger a necessary transmission.

5.2 Spoofing Attacks

Spoofing the access point into believing that an operational fault requires service. In this case, the homeowner and trusted agent will likely be convinced (because of their faith in the security protocols) and arrange for service. This false alarm will become increasingly costly nuisance if an attacker can repeat it. Defeating the spoof should be easy if a method for requesting the complaining appliance verify its identity and status. If the spoof comes from the web-side of the AP, for instance from a rogue IP source, then the attacker would be unable to properly sign the homeowner's signature, and the service vendor would likely attempt to coordinate with the homeowner. However, the homeowner may simply trust "the system" and authorize the spoofed work request anyway.

Spoofing an AP into accepting an attacker's appliance or sensor device. This could be useful to mount a DoS attack by flooding the AP in an attempt to disable perimeter security. However, if appliances can only be added through the use of an RFID token, then an attacker must be able to gain entrance before the attack. This could be accomplished in one of several ways, though somewhat risky, by masquerading as a legitimate visitor, or by enlisting a trusted person as an accomplice.

5.3 Denial of Service Attacks

If an attacker is able to trick an appliance into accepting a key revision, then a DoS attack is underway, and the attacker may be able to profit by holding the appliance "hostage". (Betts, Bryan, "Encryption could make you more vulnerable , warn experts", Techworld February 11, 2008. http://www.itworld.com/encryption-makes-you-more-vulnerable-080211) This attack is easily detected and deterred by resetting and re-adding the device to the rightful AP.

A DoS attack is mounted using RF noise to prevent wireless communication from taking place can afford a thief an easier intrusion by disabling perimeter security. Not easily defeated except by sounding alarms when loss of private network communications are interrupted, but this sets up additional complications if the attack is repeated until the alarms are ignored. This provides motivation to use dedicated wiring for perimeter security, or possibly use unpopular frequencies or directional antennas.

A Dos where attacker drains the battery of a sensor or appliance. An nuisance, unless it is a critical element of security. While battery operated devices should already remain silent, they may be obligated to listen and decode all messages.

5.4 Man in the Middle Attacks

Man in the middle attacks are unlikely since success requires interception and prevention of delivery of messages between client and access point. Might be possible if an RF noisemaker could be embedded in the area that defeats direct communication with an access point forcing multi-hop. Can be defeated with directional antennas. Another potential attack relies on tricking client and access point to communicate using different frequencies.

6. Conclusion

At the highest level, wireless networks are composed of several common elements, regardless of size, area, or mobility: wireless hosts, communication links, access points, and network infrastructure. Traditionally, wireless hosts have been laptop and desktop PCs, mobile phones, and PDAs, but soon an explosion of new devices, such as durable home and office appliances and security systems will join the mix. Communication links connect wired and wireless hosts to a AP and indirectly to each other through the AP. The AP connects the wireless network to the network infrastructure of the wired internet.

Traditional wireless devices employ established standard protocols for communications and security, and rely particularly on the 802.11x family and Bluetooth. WEP, WPA protocols, coupled with specific any of numerous crypto methods provide high quality security. New application areas in

Private Appliance Networks can employ these methods effectively, though opportunities for simpler protocols supporting lower bandwidth requirements can lead to lower cost hardware. Also, several special challenges arise in the treatment of PAN, particularly in the creation of a reliable service that places little or no implementation burden upon non-technical consumers and users.

Finally, proprietary commercial grade systems are reaching the marketplace. While these systems are oriented towards specific applications, energy reduction and built for management of larger buildings [GridLogix09] and perimeter security [Inovonics09], the products and techniques they developed could gradually trickle down and establish a sizable presence in the PAN market. While they may not offer open platforms for competitors, potential consumers are already learning about these systems capabilities first hand, by using them at work.

References

[GridLogix09] GridLogix(tm) by Johnson Controls, Inc., 2009. Retrieved April 6, 2009 from http://www.gridlogix.com/. A company web site extolling virtues of their energy monitoring technology.

[Inovonics09] Inovonics Wireless Corporation, 2009. Retrieved April 6, 2009 from http://www.inovonics.com/. A company web site extolling virtues of their perimeter security technology.

[KNX Standard09] "KNX Standard." Retrieved April 4, 2009 from http://en.wikipedia.org/wiki/KNX_(standard). A "wiki" defining and briefly describing a protocol for using a home's power wiring for creating a network.

[Konnex Association04] "Introduction to KNX and Konnex," 2004, page 9. Retrieved April 5, 1009 from http://www.weinzierl.de/download/Knx_Info.pdf. A document outlining a the capabilities of a private appliance network operating modes, but with emphasis upon marketing the virtues of the association backing the protocol.

[Kurose07] James F. Kurose, Kieth W. Ross, "Computer Networking: A Top Down Approach, 4th Edition," Pearson Education, Inc., 2007, pp. 735-736. A textbook providing in-depth treatment of computer networking and particularly internetworking issues.

[Moore65] Gordon Moore, "Made real by Intel innovation," Retrieved April 4, 2009 from http://www.intel.com/technology/mooreslaw/. A short introduction to one of the influential observations of modern transistor technology, with links to supporting and related material.

[Potlapally06] Nachiketh R. Potlapally, Srivaths Ravi, Anand Raghunathan, Niraj K. Jha, "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 5, NO. 2, FEBRUARY 2006, pages 128-143. http://palms.ee.princeton.edu/PALMSopen/potlapally03analyzing.pdf. A detailed analysis of energy costs of implementing various cryptographic algorithms including their significance with varying amounts of data.

[TexasInstruments1300] Texas Intruments "TRC1300/1315 MARCSTAR(tm) Remote Control Encoders/Decoders Datasheet", rev. 1997. PDF document downloaded April 5, 2009 from http://www.digchip.com/datasheets/parts/datasheet/477/TRC1315.php. A typical vendor datasheet providing design guidance and physical and electrical specifications.

[THALIA01] THALIA, International Housewares Show, January 17, 2000, Retrieved April 5, 2009 from http://www.reviewsonline.com/ihs00.htm. A reporters view of a commercial tradeshow, with interesting but uncompelling motivation for internetworking kitchen appliances.

[Wander05] Arvinderpal S. Wander, Nils Gura, Hans Eberle, Vipul Gupta, Sheueling Chang Shantz, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks," percom, pp.324-328, Third IEEE International Conference on Pervasive Computing and Communications (PerCom'05), 2005. http://research.sun.com/projects/crypto/wandera_energyanalysis.pdf. A detailed analysis of energy costs of implementing various cryptographic algorithms including their significance with varying amounts of data.

[X10 Industry Standard] "X10 Industry Standard." Retrieved April 4, 2009 from http://en.wikipedia.org/wiki/X10_(industry_standard). A "wiki" defining and briefly describing a moderately useful protocol for adapting a home's power wiring for creating a network.

Acronyms

AP - Access Point

DA - Dumb Appliance

EAP - Extensible Authentication Protocol

EEPROM - Electronically Erasable Programmable Read-Only Memory

KNX - Abbr for Konnex

LAN - Local Area Network

LANI - LAN Interface

MAC (Address) - Medium Access Control

OID - Object Identifier

PAN - Private Appliance Network

RF - Radio Frequency

RFID - RF Identifier

USB - Universal Serial Bus

WEP - Wired Equivalent Privacy

WiFi - the trademarked name of a type of Wireless LAN

WPA - WiFi Protected Access

Last modified on April 19, 2009
This and other papers on latest advances in network security are available on line at http://www.cse.wustl.edu/~jain/cse571-09/index.html
SHARE Back to Raj Jain's Home Page