Wireless Communication in Ubiquitous Environments, an Easy Target to Attacks

Doina Bein, *Member IEEE,* and Wolfgang W. Bein, *Member ACM*

***Abstract* — In ubiquitous computing the user is surrounded by many computational devices and systems. Ordinary actions and different parameter values of the environment being sensed by these devices trigger actions of which the user may not necessarily be aware. Privacy protection as part of network security refers to the protection of sensitive, personal information stored or collected during the lifetime of a pervasive (ubiquitous) device. Privacy and protection of pervasive devices which are part of ordinary daily life (smart homes, smart offices) is not fully addressed when such devices are built or upgraded. These devices are responsible for capturing, storing, and transmitting data related to the user context, in order to be interpreted by computers to identify actions to be taken. Data may be generated by different devices, which were produced by different manufactures. Thus each device has to trust and rely on others for functionality and proper security. "A chain is as strong as the weakest link."**

***Keywords* — pervasive devices, smart environments, ubiquitous computing, WLAN.**

I. Introduction

A ubiquitos computing environment comprises of devices (sensors, home and office appliances, etc.), applications, and services that can predict the demand of users and act on their behalf. Ubiquitous computing is also called pervasive computing, ambient intelligence, or more recently, everyware [1][2].

In ubiquitous computing, data is generated by different devices, which were produced by different manufactures. Thus each device has to trust and rely on others for functionality and proper security. Privacy protection as part of network security refers to protection of sensitive, personal information stored or collected during the lifetime of a pervasive (ubiquitous) device. There is a tradeoff between information necessary for the environment to function and the opportunity of extending the environment to include future devices. Generally it is better to minimize the amount of information being acquired by the appliances, since minimal information is required to be available for in order for a smart environment to work. But in case the smart network is extended to other devices, it is required that new types of data will be generated by the current devices. If the current devices are built by the manufacturer to acquire a restrictive set of data from the environment, then they need to be replaced to accommodate the new smart environment. Before designing any protection scheme for the current smart environment, a software analyst must determine who should have the access right to what data and under what conditions [3].

In a smart home, a server (or a group of servers) run context-aware applications for the user's comfort (see Figure 1):

- When the user wakes up (based on a sensor detection action), certain personal actions may be taken by appropriate devices (e.g. the radio is on, the curtains are open, the coffee maker starts up, etc.).
- When the user moves from one room to another, the lights are turned according to needs at locations throughout the home.
- Based on identity and factors such as the time of day, month, year, outside weather, the temperature, or humidity inside the house, or individual rooms, the hot water is adjusted.
- When leaving the house, additional measures for security are taken such as locking windows and doors, adjusting the temperature to reduce the power usage taking into account indoor plants or animals.

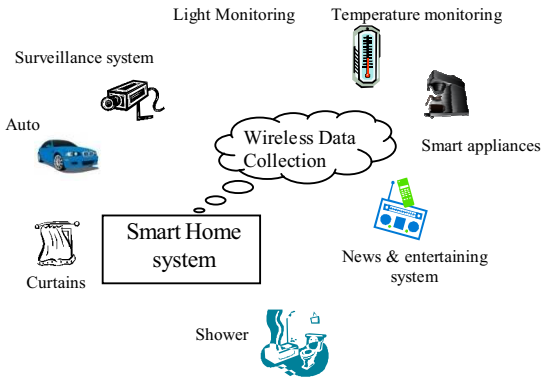

Figure 1. Smart home environment

Similarly, in a smart office, a server might run appropriate services (see Figure 2):

- Upon entry, office equipment such as the office computers, PDAs, answering machines etc. report on various current events related to the job. Also personal adjustments for temperature, humidity, and lighting are quietly executed.
- Whenever leaving the office, automatic security

Doina Bein is with the Department of Computer Science, University of Texas at Dallas (phone: +1(972) 519 0965; fax: +1(972) 883 2349; email: siona@utdallas.edu).

Wolfgang W. Bein is an Associate Professor in the School of Computer Science, University of Nevada Las Vegas, USA (Phone: +1 (702) 895 1477; fax: +1 (702) 895 5222; Email: bein@cs.unlv.edu).

measures are taken.

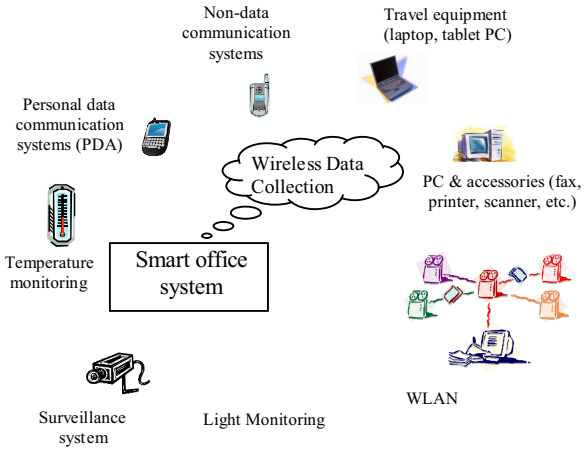

Figure 2. Smart office environment

Privacy protection as part of the network security refers to the protection of the sensitive, personal information that is stored or collected during the lifetime of a pervasive (ubiquitous) device. Protection of the network is the owner's responsibility. Privacy and protection of the pervasive devices that are part of ordinary daily life (smart homes, smart offices) is not fully addressed when such devices are built or upgraded. They are responsible for capturing, storing, and transmitting data related to the user context, in order to be interpreted by computers to identify actions to be taken. An attacker can target the home network for collecting personal information. Wireless and sensor networks do not have physical protection to prevent unauthorized access.

II. First Step in Privacy Protection: Securing the Data Locally

Protection at the physical layer refers to protecting the data collected and locally stored on the server(s). An anonymity mechanism that is hardwired can provide data without disclosing information about the owner of the data. For example, the Bluetooth SIG has proposed the *anonymity mode* [4] for devices in order to prevent location tracking by changing the device address (BD_ADDR) that makes the device identifiable. Regularly changing the device address creates the need for address management [5].

There were cases where private data has been unintentionally disclosed over the Internet, offices of public or private institutions have been subject to hacking attacks and credit card numbers, personal data, email addresses, and the like have been compromised.

A criminal investigation conducted by the FBI, the Dallas Police Computer Crimes Squad and other local law enforcement agencies is being conducted after an attempted attack on the network at the University of Texas at Dallas was identified on December 10, 2006. Information Resources (IR) determined that personal information of 35,000 applicants, students, faculty and staff might have been exposed through a weakness in the network. (Initially, only 6,000 individuals were identified as having had information put at risk.) Activities resembling those of a ”bot” - an automated computer program that searches for and scans large amounts of data on private networks - spurred concern about the network's security. For more information, see [6].

The University of Texas at Dallas is not the only university to report a recent Internet attack. Texas Woman's University reported December 22, 2005, the exposure of 15,000 students’ Social Security numbers during a transfer of information over an insecure connection to a data storage facility. However, officials later said the information was not likely stolen because it was exposed for only a few nanoseconds.

The University of California, Los Angeles on December 12, 2005, also reported a network attack in which a hacker retrieved Social Security numbers of approximately 28,600 individuals.

On March 18, 2005, a hacker broke into the University of Nevada, Las Vegas computer system and retrieved information about international students and scholars.

Currently, third-party interfaces (anonymizers) protect the physical location of the user obtained from his IP address, cellphone location, etc.. An anonymizer or an anonymous proxy is a “middleman” between the user and the Internet that accesses the Internet on the user's behalf, protecting personal information by hiding the source computer's identifying information [7].

But if the user protects itself by using a counterfeit ID (called *pseudonym*), its identity can be still detected by tracking the location record of the user.

III. Second Step in Privacy Protection: Securing the Communication

Although major network providers such as cellular phones carriers, Internet service providers (ISP), may be trustworthy, hotspots are based on the Internet Protocol (IP), thus tools as “traceroute” can expose the routing of the packets and ultimately the device location.

Huang et al. [8] propose the concept of a *silent period*. For a moving node, its consecutive, spatial anonymous locations are detected at a constant interval of time, and not continuously, and are thus harder to correlate between a specific user and its anonymous context.

The Cricket Indoor Location System [9], developed by MIT, consists of beacons mounted in walls and on ceilings that communicate through RF-signals and ultrasonic pulses. The user location is known only by the individual sensing devices worn by the user, and not by the central server collecting the data. But it requires the user to wear devices compatible with the sensors of the network, and the sensors to be powerful enough to process some control operations.

The Platform for Privacy Preferences (P3P) project [10], Privacy Awareness System (pawS) [11], and Location Service (LocServ) [12] control the user access through a set of validator modules which contain the privacy requirement of each user for each location server. Given a location request and the privacy policy supplied by the user, validators decide whether to release information

and/or to reduce the accuracy of the data supplied.

Location-based services (LBS) can work with different levels of user's identity: some need only the users' location but not its real identity, some need users' real identity but not (current) location.

IV. Protecting Data of WLAN

Wireless Area Networks (WLANs) are deployed at home and at work to improve the communicability between different compartments. Most of WLANs work on a 2.4 or 5 GHz frequency with a proposed throughput of 11 to 54 Mbps and a range that depends of the specification of the version of 802.11 (see [13] for detailed specifications). They do not have physical protection to prevent unauthorized access and are targets for security attacks (see Figure 3) such as capturing the SSID, jamming the traffic, insertion attacks, interception and monitoring wireless traffic, misconfiguration, etc. [13,14].

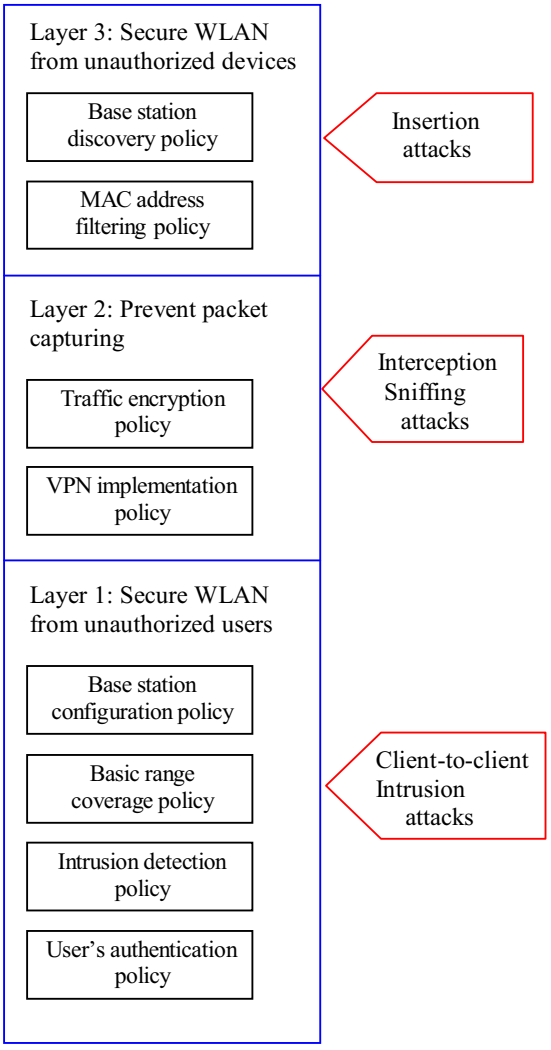

Figure 3. Attacks towards security and policy levels

Most of the WLANs work on a 2.4 GHz frequency. A basic WLAN configuration includes the mobile devices that have a wireless network interface card (NIC), the wireless access point (WAN) that is the router that enables wireless devices to access the wired network. The 802.11 versions can use wired equivalent privacy encryption (WEP) and encryption of Service Set Identifier (SSID).

WEP uses a RC-4 cipher for a 40-bit, 128-bit, or 256-bit key. The encryption keys are static, thus sniffing many packets eventually converges to obtaining the key. An SSID uniquely identifies a WLAN.

The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is a 32-character unique identifier attached to the header of WLAN data packets. An SSID is also referred to as a network name because essentially it is a name that identifies a wireless network.

SSID is a configurable identification of the base station that allows only clients with the same SSID to communicate with the base station. Because an SSID can be captured (sniffed) in plain text from a packet, it does not supply any security to the network.

Jamming traffic can be done (intentionally or not) by flooding the 2.4 GHz frequency such that the signal to noise drops below a certain threshold and the network ceases to function. Examples of such devices are infant monitors, cordless phones, and Bluetooth devices.

An *Insertion attack* occurs when an unauthorized device is placed physically in the network without a security process. Example: plug-in unauthorized clients or base stations.

Interception and monitoring wireless traffic attacks are similar to Ethernet attacks. They are possible because of weaknesses of the software running inside the system (such as buffer overflow in IMAP and POP servers, default Simple Network Management Protocol SNMP, default accounts and accounts with weak passwords). The attackers, using wireless sniffers can obtain copies of the packets. Alternatively, they can execute session hijacking by spoofing the source address of the packets (Address Resolution Protocol (ARP) spoofing). Base station cloning (phishing) convinces legitimate wireless clients to connect to the attacker base station that has a stronger signal.

Misconfiguration of an access point can result in extracting the SSID.

To protect from attacks, a fist step is to secure the wireless access point (WAP), in order to prevent unauthorized users from gaining access to the network.

Second, the wireless LAN transmissions should be kept from being captured and having the packets decoded.

Currently, the tools for cracking WEP keys can have a successful result in the order of minutes for a busy network (several million packets are required), depending on the traffic rate. In Figure 3, Retina and Dsniff can be linked to Layer 1, AirSnort and Kismet can be linked to Layer 2, and Network Stumbler can be linked to Layer 3.

Created by Dug Song, Dsniff [15] is a packet sniffer and contains a set of tools targeting ARP spoofing. Retina [16] targets vulnerability assessment and is able to scan an entire Class C network in about 15 minutes.

AirSnort [17] is free software (it is distributed under the GNU General Public License). Based on a peculiar weakness of RC4 (the most widely used socket stream

cipher, used by SSL and WEP) [18], Hegerle and Bruestle [17] publicized AirSnort – a WEP encryption cracking tool, which cracks WEP encryption of an 802.11b network by passively monitoring the traffic and computing the encryption key when enough packets have been gathered. It must gather about five to ten million encrypted packets from a wireless access point before it can attempt to recover the wireless key. Depending on the environment, this can take as little as a few minutes or more commonly a few hours and possibly a few days. The SSID of the base station is obtained, and is later used for trying to connect to the wireless network.

Kismet [19] is a wireless detector and sniffer for 802.11b, 802.11a, and 802.11g networks. It runs under Linux, FreeBSD, NetBSD, OpenBSD, as well as Mac OS X. It is compatible with any wireless card which supports the raw monitoring (rfmon) mode for DHCP packets, Ethereal and tcpdump compatible packet dump files. Without sending any loggable packets, it is able to detect the presence of both wireless access points and wireless clients, and associate them with one another. It is also an intrusion detection system, in the sense that it detects some of the known active wireless sniffing programs. Kismet has the ability to log all sniffed packets and save them in a tcpdump (a packet sniffer) or AirSnort compatible file format. To find as many networks as possible, Kismet supports channel hopping. This means that it constantly changes from channel to channel non-sequentially, in a user-defined sequence with a default value that leaves big holes between channels (for example 1-6-11-2-7-12-3-8-13-4-9-14-5-10). The advantage with this method is that it will capture more packets because adjacent channels overlap. It also supports logging of the geographical coordinates of the network if the input from a GPS receiver is additionally available.

Network Stumbler [20], also known as NetStumbler, is a Windows software written by Marius Milner; it runs on Windows 98 up to Windows Vista (under compatibility mode). It finds open WAPs (WAPs without encryption or WEP) on 802.11b, 802.11a and 802.11g WLAN standards. "War driving" is the term used for describing the process of collecting, recording the GPS coordinates of such WAPs, and sharing them with other attackers on Internet.

V. Conclusion

Privacy and protection of pervasive devices that are part of our daily life (smart homes, smart offices) is not fully addressed when such devices are built or upgraded. Before designing any protection scheme for the current smart environment, the software analyst must determine who should have the access right to what data and under what conditions. There were cases where private data has been unintentionally disclosed over the Internet, offices of public or private institutions have been hacked in order to successfully collect credit card numbers, personal data, mail and email addresses.

References

[1] A. Greenfield, "Everyware: the dawning age of ubiquitous computing", New Riders, p.11-12, 2006

[2] U. Hansmann, "Pervasive Computing: The Mobile Word", Springer Verlag, 2003

[3] Y. Duan, J. F. Canny, "Protecting user data in ubiquitous computing: Towards trustworthy environments", Privacy Enhancing Technologies, 3424, p. 167-185, 2005

[4] Bluetooth 1.2, Draft 4, Bluetooth SIG Std., 2003

[5] C. Gehrmann, J. Persson, B. Smeets, "Bluetooth Security", Artech House, 2004

[6] University of Texas at Dallas, www.utdallas.edu/datacompromise

[7] J. Boyan, "The Anonymizer: Protecting User Privacy on the Web", Computer-Mediated Communication (CMC) Magazine, vol. 4, no. 9, September 1997

[8] L. Huang, K. Matsuura, H. Yamane, K. Sezaki, "Enhancing Wireless Location Privacy using silent period", Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), March 2005

[9] N.B. Pritantha, A. Chakrborty, H. Balakrishnan, "The Cricket location-support system", Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, p. 32-43, ACM Press, 2000

[10] World Wide Web Consortium, http://www.w3c.org/P3P

[11] M. Langheinrich, "Privacy by design - principles of privacy-aware ubiquitos systems", Proceedings of UBICOMP, LNCS 2201, Springer Verlag, pp 273-291, 2001

[12] G. Myles, A. Friday, N. Davies, "Preserving Privacy in Environments with location-based applications", Proceedings of the IEEE Pervasive Computing, vol. 2, no. 1, p. 56-64, 2003

[13] S. Deshpande, ``Secure and manageable enterprise WLAN", Computer Associate Inc. Tech. Notes, May 2004

[14] S. Barman, ``Writing Information Security Policies", New Riders Publishing Inc., 2002

[15] Dsniff Project, http://www.monkey.org/~dugsong/dsniff/

[16] Retina Network Security Scanner, http://www.aavextechnology.com/retina.htm

[17] AirSnort project, http://airsnort.shmoo.com/

[18] S. Fluhrer, I. Mantin, A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", 8th Annual International Workshop on Selected Areas in Cryptography, LNCS, vol. 2259, p. 1-24, 2001

[19] Kismet Project, http://www.kismetwireless.net/

[20] NetStumbler Project, http://www.netstumbler.com/