BIOMEDICAL TELEMEDICINE

Jeffrey Lee
Sanjeev Oghra

CSCI E-170
January 11, 2005

Introduction

Modern Wireless Devices

The concept of a device that can execute complex computational functions has changed substantially over the past decade. What was once thought to just be a computer has evolved from desktops to laptops, to PDAs and cellular phones. Everyday over one billion people carry around devices that have sensors, location beacons, a connection to the Internet to download and upload information, images, video, and sounds, and storage capability. With the right technology, a person's cell phone can be used to pin point their location. One's entire life can be stored on a PDA or a cell phone and in a moment's notice that information can be downloaded from the device or intercepted in transit.

Growing concerns of such security threats has not dissuaded the people's yearning for further advancements in these devices. In the past several years, wireless technology has become increasingly more popular in every day activities. Examples of such modern day amenities include wireless network connections, wireless toll collection systems (FastLane and EZ Pass), and wireless credit keys (SpeedPass). With these advances, the question of "what's next" in future wireless devices lingers on mind.

Wireless Telemedicine: The future EZ-Pass?[1]

On October 12, 2004 the Food and Drug Association approved the use of an RFID chip implanted in a human called VeriChip. The purpose of this chip is to enable hospitals to retrieve medical records of a patient by utilizing a scanner to read the chip. The VeriChip has raised many security concerns regarding privacy issues. Fears regarding the security of the information communicated by the chip worry many potential users.

Is VeriChip the new wave of wireless technology that will become integrated into future healthcare? Other medical devices have emerged in today's healthcare market and been dubbed "wireless telemedicine."[2] Such devices transmit information that is extremely sensitive to the wearer such as vital signs, pin-point position, or even medical history, so the question of whether this information is secure is a relevant issue. Many of these devices utilize GSM mobile communications, Bluetooth, and RFID all of which are widely used wireless technologies and have valid security concerns.

Benefits of Medical Wireless Devices in Healthcare

The emergence of wireless medical devices is in response to the growing request for advanced healthcare and homecare. Currently Americans spend $27 billion on healthcare other than traditional medical practices because they find it difficult to access, expensive, and painful (www.rwjf.org).[3] This need for integration of home and healthcare environments and the need for precise and detailed diagnosis data are the driving forces of the production of these devices.

The most common use of wireless medical devices would be to eliminate the need to venture into a hospital or doctor's office, leading to lower healthcare costs. This would allow the elderly to stay at home as doctors monitor their vital signs such as ECG, heart rate, and blood pressure from a remote location and reduce the length of time needed to stay in a hospital after an operation. In addition to that, the benefit of real time readings on a person's physiology has allowed preventative measures to be

taken. This has caused caregivers to turn to these wearable computer devices for aid. Although the devices offer a large benefit to patients and caregivers alike, the potential damage the devices can inflict is far worse.

Compromised Privacy

Wireless telemedical devices offer a wide range of benefits and cause great concern in regards to the privacy of individuals.

- Health insurance companies can base their coverage and rates given to a family on data retrieved from these devices.
- Life insurance companies may be able to track eating habits or drug use by monitoring clients remotely by using these devices.
- Spouses or parents can monitor and track spouses or children to discover if they are cheating or using narcotics.

In this day and age, privacy is becoming a rare commodity. With the introduction of these wireless devices, privacy of individuals who need to be monitored for illnesses will be in jeopardy. Unless these devices have specific security measures against such threats, individual privacy will be compromised.

Statement

With the endless possibilities of privacy violations, an analysis of four wireless telemedical devices has been done. A detailed description of the product, security analysis and conclusions drawn from these observations will be provided.

Background

RFID Definition and History

Radio Frequency Identification (RFID) is an all-encompassing term used for technologies that use radio waves to transmit, typically, data from portable tags to a reader that provides information on that individual item. The data transmitted may provide identification information, the location of the item, or specifics of the item that the tag is attached to (such as price or other product information). The Caregiver's Assistant and VeriChip products that we discuss here both make use of some form of RFID technology.

Dating back to 1948, the founder of the technology (Harry Stockman), published the paper "Communication by Means of Reflected Power."[4] In fact, these early versions of "RFID-like" systems were used in WWII as friend-or-foe beacons in Allied aircraft. Following in the tradition of microwaves, automatic weapons, and M&M's this military application has become a staple in the world of consumer goods. RFID use in access control systems emerged in the 1980s and became popular in its ability to track moving objects. The main obstacle to widespread use of the tags in its early years was the exorbitant price per tag. However, as the price dropped (as of 2004, passive tags cost ~US$0.40[5]) the use has increased.

Today, variations of RFID systems are used in a wide range of applications. Inventory from clothing to televisions, animal identification, car anti-theft and ignition systems, toll collection, access control, seismic sensors enabling remote data collection, and pallet/container tracking are some of the myriad of uses. This list is growing as the price and size of the chips are shrinking. The ability to manufacture tags as small as 0.4 x 0.4 mm and as thick as a piece of paper has led to embedding the tags within currency, driver's licenses, and passports.

RFID systems may consist of tags, tag readers, tag programming stations, circulation readers, sorting equipment, and tag inventory wands. Typically, tags are attached to individual items. The tags consist of a silicon chip (transponder), an optional power source, and an antenna. The reader that interrogates the tag contains an antenna, transceiver, and decoder. It emits an RF signal and activates the tag, facilitating the transfer of data, where it can decoded by the reader and passed on through the network. The system is capable of providing information without line-of-sight, through most non-metallic materials, and in situations where there's bright sunlight (a problem with optical barcodes).

RFID is rife with security issues. In the case of access control, an attacker can read a tag at any time (especially if the user carries it with them), clone it relatively easily, and have instant access to the same locations that the original tag had. Encryption has not been able to be implemented in the most common tags (passive devices) due to limitations of the current technology. Passive tags are powered by the reader, they're designed to be simple and it is very difficult to build cryptosystems into a chip meant to be that simple.

Bluetooth Definition and History

Aptly named after the Danish King Harald Blatand who unified warring tribes in Denmark during his reign, Bluetooth is a metaphor for allowing the communication between various devices through its protocol. It's a low power wireless radio protocol designed for short distances (10-100 meters), enabling wireless connection of peripheral devices such as keyboards, printers, cell phones and PDAs. It operates in the ISM band (2.45 Ghz) and version 1.2 has transmission speeds of up to 723.1 kbit/s. (version 2.0 will reach 2.1 Mbit/s).

It is possible to password protect a connection between two Bluetooth products. As the popularity of the protocol has grown, the security issues have become better known and some more have developed. For instance, the first virus spread via Bluetooth among mobile phones was produced in 2004.[6] And directional antennas have been shown to extend the range of Bluetooth devices up to one mile (far greater than typically seen and illustrates a vulnerability of Bluetooth to eavesdropping).[7]

Current Wireless Telemedical Devices

Lifeguard Overview

Being developed jointly between NASA Ames Astrobionics and Stanford National Biocomputation Center, the Lifeguard System is a real-time mobile monitoring device used with astronauts in NASA that is now being adapted for home use. This wearable, small, and unobtrusive device is used to monitor the physiology of the user. The system combines a series of lightweight medical sensors, base computer (Tablet PC), secure wireless network architecture, and software for data storage, display and analysis. This device is currently designed for monitoring vital statistics in extreme environments remotely and not yet tested for everyday home use[8].

Lifeguard Specifications

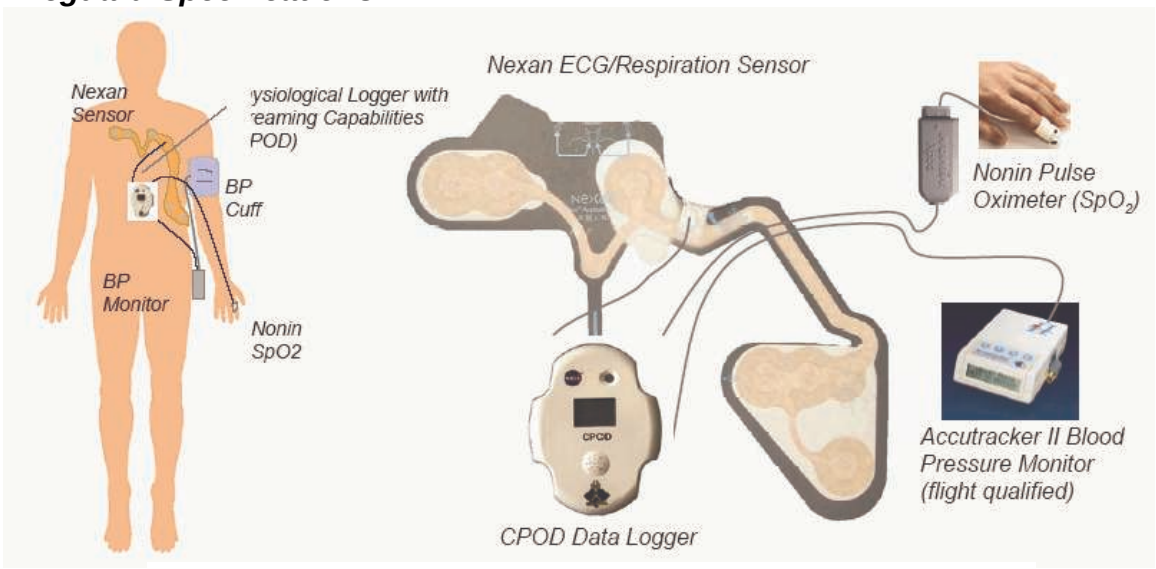

Figure 1: Lifeguard Component Diagram
c/o Stanford National Biocomputation Center

The Lifeguard System core device is called the Crew Physiological Observation Device, CPOD. Currently, up to three sensors can be attached to the CPOD and record for up to eight hours after the device is turned on. The CPOD itself has sensors built in to measure activity and skin temperature.

Currently the CPOD can sustain up to three separate sensors to measure vital statistics. The commonly used sensors are listed as follows:

- Traditional electrode buttons measure the ECG and respiratory signals of the wearer.
- Blood oxygenation is measured with a pulse oximeter attached as a finger clip or an ear clip.
- A cuff based auscultator device called the Accutracker II is used to measure blood pressure.[9]

The CPOD itself is a low-powered microcontroller that controls all external sensors, the internal A/D controller and the onboard flash memory. To extract the data from the CPOD there are three modes of transfer; using a hardwired RS-232 port or one of two wireless technologies, Bluetooth, or 916MHz FSK.

Lifeguard Analysis

The Lifeguard system is a necessary first step towards global telemedicine. The usability of the device proves to be simplistic, after connecting the sensors to the CPOD, the sensors to accurate parts of the body, and turning the device on. Usability tests have already been conducted with both knowledgeable and users unfamiliar with the system.

Currently utilizing Bluetooth and the 916MHz FSK wireless technology does not provide extremely quick transfer of data to doctors. One experimental analysis of the Lifeguard system included the use of the device and sensors to transmit vital signs from Licancabur volcano in Chile at 19,700 feet. In this test, the Lifeguard system was capable of transmitting real-time data from the CPOD, reflected off an Inmarsat

satellite, downlinked via France Telecom, sent across the Internet, and observed in real-time from NASA, Stanford, and Monterey, California.[10]

As the Lifeguard System is still in its early stages of development it would require rather expensive equipment to download information from the CPOD across great distances, so a security attack from a neighbor is highly unlikely. With that said there is a relatively large security risk if a remote connection is made. In accessing data from the CPOD, there is neither an authentication mechanism nor other security. All that is required to gain access to the CPOD is to obtain the Lifeguard system software and install it on a Tablet PC and a connection. After those two steps have been accomplished, anyone can extract logged data or real-time vital statistics[11].

In order to preserve sensitive vital statistic information, it is necessary to institute a secure method to access data collected from the device. The current method of data extraction allows for the data to be downloaded without the wearer's consent or knowledge. The Lifeguard System can fortunately only accept one connection at a time, so multiple people cannot download data from the device.

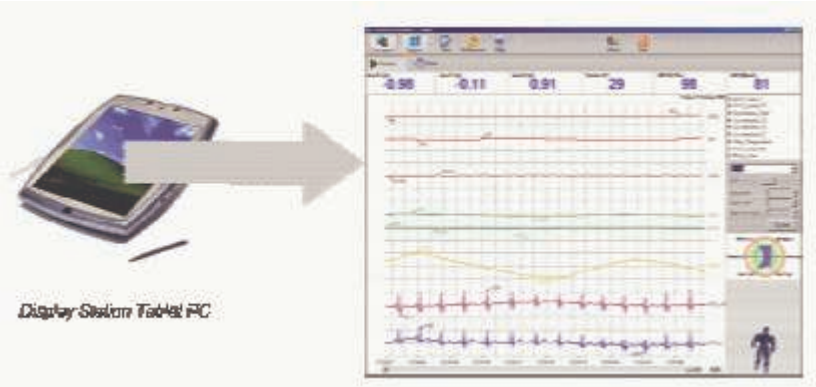

Figure 2: Lifeguard System Base Station Software
c/o Stanford National Biocomputation Center

Improvements needed on the Lifeguard System

The current Lifeguard System is not yet easily accessible across great distances as current tests show that the farthest distance that the base station can be to form a direct connection to the CPOD is 33 meters. Nonetheless, as the Lifeguard System undergoes improvements, the performance of the device will increase. One day data transfer over 33 meters will be possible and a truly remote monitoring device will be distributed. Before such a device can be mass distributed, it is necessary to address the following security concerns:

- Lack of verification of data
  - A hash of the logged data should be sent in addition to data to ensure the integrity of the data.
- Lack of verification of user access
  - The issue of user access is not properly addressed in the current version of the Lifeguard System. An authentication mechanism must be implemented into the system before a user can gain access or else the data will not only be viewed by privileged users.
- Lack of protection against the possibility of intercepted data
  - The establishment of a secure encrypted connection over Bluetooth between the CPOD and the authenticated user's PC will prevent illegal access of the data either wirelessly or through a wired medium and

ensure that even if the signal is being intercepted that foreign users would be unable to decrypt the actual data.

Security measures need to be integrated into the Lifeguard System before it is widely used for home care and telemedicine.

Vital Positioning System Overview

Over 100 million people in the world are affected by a cardiovascular disease. Of those, many die from a heart attack due to delay in treatment. Medical Intelligence, a Canadian company based in Quebec, has for the past three years developed an early warning system that can notify emergency services up to twenty minutes prior to the actual heart attack and transmit the precise positioning of the victim[12]. Typically heart attacks are caused by blocked circulation in an affected artery causing electrocadiographic changes prior to arrhythmia or issues leading to death. The ability for a portable device to detect such signs and transmit the position of a patient through a cellular phone is considered a major breakthrough in combating death via cardiovascular diseases[13].

Vital Positioning System Specifications

There is neither an abundance of published details involving case studies of the Lifeguard nor are there many technical aspects of the VPS published. Gathered from articles and descriptions on the Medical Intelligence website, the VPS is a belt integrating four micro devices[14]:

- Wireless digital ECG
- Cardiac activity sensors
- Small GPS
- Simple Bluetooth transmitter

According to the CTV.ca News Staff, the VPS uses “12 electrodes on the heart that feed signals to a tiny chip that never stops monitoring for aberrations”[15]. The 12 electrodes are assumed to be the cardiac activity sensors which feed into the wireless, digital ECG that monitors the heart for the electrocardiographic changes. The wireless digital ECG sends continuous data through the wearer’s cellphone, PocketPC or telephone, via the Bluetooth transmitter, to a cardiac data management system, which stores the reading, date and time.

Vital Positioning System Analysis

The Vital Positioning System was designed as a small and convenient belt to be worn at all times to monitor a patient who is in danger of a cardiovascular attack. According to reports, the belt is unobtrusive and does not use adhesive of any sort. The wearer does not seem to need to physically do anything other than attach the sensors to their body and ensure that their cellular phone, wireless phone or Pocket PC is turned on.

The VPS is also very mobile and not reliant on one type of device to transfer the data. Should the VPS become widespread, even when traveling on business or vacation the VPS should be able to contact local emergency services and send data to the local cardiac data management center. The benefits of utilizing the VPS can prove to be immeasurable to preventing death caused by heart attacks.

As multifunctional and usable as the VPS is the data that it collects and transfers is highly vulnerable to attacks. Both Bluetooth and cellular phone signals can be

intercepted without using advanced and expensive equipment. There are an abundance of devices that can be purchased on the Internet that can be used to intercept cellular phone conversations. Though not very practical, recording these conversations or transmitted cellular signals is not impossible. Currently the transmission of the data using VPS is similar to broadcasting a radio signal to anyone who can receive the signal.

Current issues regarding Bluetooth can pose a severe security threat to the VPS as Bluetooth devices and networks become more and more popular. Although it is not practical, it is possible to pull the data that is transmitted from a Bluetooth device with a "laptop, scripts and familiarity with the Bluetooth specification."[16] (John Cox, Network World, 5/17/2004) New tools are being developed everyday to scan and identify Bluetooth devices such as Bluesniff. Everyday people are finding methods to expose wireless networks such as this device and such vulnerabilities should cause valid concerns for users of VPS.

Vital Positioning System Conclusions

Overall the functionality and usability of the VPS is very attractive. The privacy and security of the issues involved with the system must be addressed before it is widely distributed. The following recommended guidelines for the security issues are as follows:

- Lack of protection against intercepted signal transmission
    - The Bluetooth protocol is built for a 128-bit encryption and should be used to prevent the data being transmitted against unauthorized users from gaining access to the information.
- Data should not be stored over a long period of time on the device itself nor in the cardiac data management center.
    - The longer the device retains data the more likely information will be extracted from the device
    - The longer the data management center keeps the data the more vulnerable the user will be prone to a privacy threat.

Even with these vulnerabilities the VPS is a major step towards advancements in common everyday wireless telemedical devices since the ability to use this system is as simplistic as using a handsfree device.

Caregiver's Assistant Overview

Intel Corporation has developed a Caregiver's Assistant product aimed at the senior citizen market. The product is designed to monitor the elderly in their home environment in an effort to enhance healthcare delivery to the users and, in the process, improve quality of life. Intel's goal is to improve care and reduce cost vis-à-vis 'proactive computing applications.' Part of their strategy is to delay the elderly moving from their homes to nursing homes and other managed care facilities; they would like the elderly to 'age in place.'[17]

Figure 3: Caregiver's Assistant portable RFID tag
c/o Intel Corp.

Basically, the system works by outfitting various items throughout the user's home (medicine bottles,

toothbrushes, keys, etc.) with RFID tags. These tags along with a tag on the user's hand (see Figure 3) make up wireless sensor networks that enable real-time monitoring of which items they are picking up. Time stamps, duration and patterns of use are extrapolated from this data and are compared to a baseline. All of this information is recorded automatically on electronic daily activity forms and presented in a user-friendly application with graphs and charts (see Figure 4).

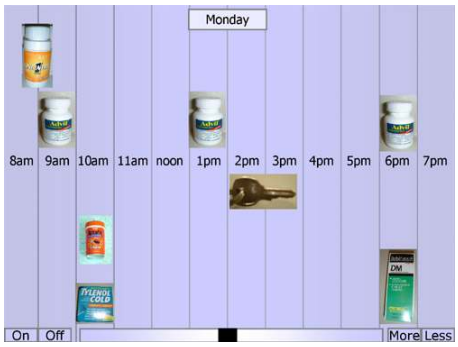

Figure 4: Screenshot of Daily Activity Form
c/o Intel Corp.

Thus, caregivers are able to effortlessly monitor any deviations from the elderly user's normal activities (which may be indicative of illness). Also, the Caregiver's Assistant system would aid doctors in monitoring their patients dosing regimen (addressing another major issue in the medical field). Caregiver's Assistant can "analyze sensor data from drawers, medicine cabinets, pill bottles- wherever medications are stored- and deliver timely reminders via cell phone, TV, or whatever device is preferred or nearby."[18] It has even demonstrated the capability to use wearable sensor tags in concert with the wireless sensor network to alert caregiver's if a person falls and "sensors in footwear which could monitor a person's gait for irregularity and prevent a crippling fall."[19]

One of the major benefits of this product is that the elderly are able to live at home longer and are not being placed in nursing homes. The US spends approximately $100 billion annually to treat illness related to social isolation among seniors.[20] The cost of nursing homes is prohibitively expensive in many cases and Caregiver's Assistant may be a viable alternative to lower costs.

How it works…

Sensor networks are established throughout the user's home. When the user picks up an item, the tag on the item and the tag on the user communicate. The data is transmitted to a reader within the user's home. This could be a personal computer where the user may access the data or simply a black box that has a connection to the Internet. The user may switch off this reader at any time. The data is transmitted via RFID to the reader, over the Internet to the caregiver who monitors the data streaming in.

The raw data coming into the system is translated via an activity tracking system that uses dynamic Bayesian networks and artificial intelligence technology to "meaningful trending information about what activities people are doing in the home."[21]

Security, Privacy, and Usability…

Intel also stresses that usability is a paramount concern and they address it in their design of Caregiver's Assistant. Through the Caregiver's Assistant system any computer and many electronic devices that the elderly are already familiar with (televisions, phones, etc.) may be used to access and view the applications. And because the users are able to use these familiar interfaces, they will not be forced to learn new technologies. There are some wearable components involved in the technology that may prove inconvenient for users and may effect compliance. As shown in Figure 3, one option is to have a tag fitted onto a glove that is worn around

the home. However, every year the technology to miniaturize tags progresses and it should be fairly easy to improve in this area.

Intel hopes that the Caregiver Assistant will drastically improve care to seniors, lower costs, and ease the strain on the healthcare system. However, the cost saved in dollars will cost seniors another kind of wealth- their privacy will be shattered. A diabetic will not be able to open the fridge and eat a piece of cake without being asked one of two questions, "Why did you turn of the system?" or "Why are you eating something you're not supposed to be eating?" Granted, if a diabetic shouldn't be eating cake then maybe this is a good technology that makes the user think twice or feel shamed about not following his doctors orders. But in using this technology, a basic freedom is being taken away from him; he is no longer able to eat a piece of cake in his own home in peace or sneak in a glass of scotch at night without somebody looking over his shoulder and **that** may be a problem to many seniors.[22]

The system is open to attack at many levels. The Internet is used to transmit the data from the home wireless sensor network to the caregiver(s). The wireless sensor network does not use encryption and is open to eavesdropping attacks. Interested parties may learn all sorts of information about the user. A nosy neighbor may have detected foul-breathe on the user and is now able to get definitive proof as to whether that person is brushing his or her teeth. Or more sinister, those criminals who prey on the elderly may learn when that person is most vulnerable (after taking a nauseating cancer medication perhaps) and decide this is the time to rob them.

The user has the option to disable the monitoring, however, in switching it off caregivers would be alerted and this would be monitored as well. Disabling the reader would defeat the purpose of having the Caregivers Assistant in place but it does place some level of control with the user.

VeriChip Overview

VeriChip Corporation, a wholly owned subsidiary of Digital Angel Corporation (which is majority owned by Applied Digital Solutions), makes an RFID device called the VeriChip® that has garnered a lot of attention in the media over the last few years. The VeriChip is a noteworthy product in many respects. It is being marketed as a chip that is implantable within humans that can communicate lifesaving information when the user is unable to (to physicians in emergency rooms, for instance). The buzz in the investment world is that RFID will change the landscape of supply chain management and create innumerable efficiencies and cost savings for all sorts of companies. This has added a certain aura around all things RFID related. Stocks in companies facilitating the 'RFID revolution' have soared on news that top retailers such as Walmart and Microsoft have set deadlines for vendors to start using the technology.

The Food and Drug Administration (FDA) fueled the VeriChip speculation when they released a report Oct 12th, 2004 saying that they had found that the VeriChip and similar devices were medical devices and therefore not an FDA regulated product.[23] This essentially fast-tracked the VeriChip and any similar devices to market.

How it works…

The VeriChip system consists of an electronic device implanted subdermally (preferably in the triceps area between the elbow and the shoulder of the right arm) within humans that has the capability to communicate information about the person via the VeriChip Subscriber Number (a unique ID number) and the Global VeriChip Subscriber Registry (a centralized database). It is a noninvasive, outpatient procedure to insert the chip (painless, takes a few minutes, and inconspicuous when inserted is what's advertised).

Essentially, it is a very simple device roughly the size of a grain of rice (see Figure 5). The VeriChip itself is a passive RFID chip that transmits a simple identification number when interrogated by a scanner. Passing the scanner briefly over the area of insertion causes low-power radio frequency energy to pass through the antenna in the scanner to the antenna in the dormant VeriChip. It uses this energy to power the integrated circuit and communicate with the scanner, transmitting the unique ID number. [24] Using that number and knowledge-based privileges to the database a doctor, for instance, can enter a password and retrieve medical records; valuable information to treat that patient. This is one advertised scenario that Applied Digital gives to show device efficacy.[25]

Figure 5 VeriChip System Overview
c/o Applied Digital Solutions

Security, Privacy, and Usability…

The VeriChip has a certain 'coolness factor' about it. An implantable microchip that can communicate potentially life-saving data via RFID technology appeals to a certain subset of the population. Patrons of 'cutting edge' bars are already able to have their chips scanned in order to enter VIP areas of the establishment. Indeed, there is a waiting list on the Applied Digital website for those interested in "pre-registering for your personal VeriChip."

The VeriChip has the ability to make certain mundane aspects of life very convenient. The chip can be used to pay bills. The unique identification number is communicated to the scanner when a user purchases an item. The reader connects to the central database and uses the number to look up the user's banking or credit card information which is used to pay the bill. A simple scanning of the user's arm on the way out of the store pays his or her bill. From a usability perspective, the VeriChip may be extremely easy on the user.

At the same time, another subset of population reacted very differently on hearing details of the VeriChip. The possibility of users being tracked and their personal information being at risk is a likely danger. To many in the general public the premise elicits visions of cyborgs and other science fiction legends. To privacy advocates the

technology screams slippery slope. In fact, Applied Digital's subsidiary has created technology that can be used to track via Global Positioning Systems.

Privacy guidelines have been set by Applied Digital. Released during the 2004 World ID conference, they speak to the VeriChip being a "voluntary" technology (nobody should be forced to get 'chipped' and removal at any time), establishing a CPO (Chief Privacy Officer) to oversee development, their documentation will include privacy information, the VeriChip user decides who has access to their database, and they add a privacy pledge as a sort of mission statement.[26]

The system is vulnerable from a security perspective. If the VeriChip is used to transmit credit card information (as in the payment system outlined above), it would not be difficult for an attacker to breach the system. For example, an attacker could obtain a reader for a nominal sum and use the reader to intercept the signal (and the unique number of) a victim's VeriChip. Once armed with that number, the attacker could write another VeriChip or similar RFID tag and then use that to transmit payment information wherever they choose. Recognizing the vulnerability, the VeriChip has been marketed as a security enhancing technology by having users implanted with the chip use it to verify their identity when they also present their credit card to merchants.

Irrespective of the controversy stirred up by the VeriChip, the product (as marketed to humans) actually represents a negligible proportion of Digital Angel's revenue stream. Their 'bread and butter' is the sale of RFID tags for the "companion animal, livestock, laboratory animal, and fish and wildlife market".[27] In 2004, Digital Angel's sales of these tags rose by more than 400%. National and global programs to trace livestock in light of recent cases of mad cow disease have fueled these growth rates. However, these tags were not for humans. The sale of VeriChips represents a small aspect of Digital Angel's (and even less of Applied Digital's) business. According to Applied Digital's quarterly report for Q3 2004, they had an astounding debt of over $417 million and while 23% of their total revenue came from RFID tags, implantable microchips **for humans** wasn't even listed on their sources of revenue.[28] It is estimated that roughly 2,000 people worldwide have the VeriChip implanted.[29] Given the concerns surrounding the technology, there must be an informed public, discussion on the technology, and privacy protecting policy should be created. However, barring a teenage VeriChip fad akin to body piercing and branding, VeriChips are not likely to proliferate throughout society anytime soon.

Privacy

In today's world of spam, hackers, and the Internet, privacy is truly a rare commodity. A conversation you have at a bus stop with a friend can suddenly appear on a stranger's web blog hours later. Identity theft is quickly becoming a lucrative crime as everyday activities such as throwing out the ATM receipt after retrieving cash. At every turn it seems there is a new threat to privacy as technology advances. With each modern convenience some part of an individual's privacy can be compromised. How does that impact wireless telemedicine?

The concept of global wireless telemedicine is quickly approaching common use in healthcare with new technology bringing the world closer and diminishing the size of electronic devices. But who will ensure that privacy concerns are properly addressed in this new age where your location can be tracked from a computer without your

knowledge. As Morgan and Newton suggest in 'Protecting Public Anonymity'[30], the optimal situation would be if designers of the products were to take it into account as they build the systems. In fact, this is being implemented at Applied Digital where they've appointed a Chief Privacy Officer to manage the privacy-side of design and implementation of products in an attempt to be proactive rather than reactive to the onslaught of media and privacy advocates fighting their VeriChip product.

The wireless telemedical devices presented in this article have the potential to accumulate vast quantities of personal data. Although the immediate goal of the data collection is not commercial, such information can be used by businesses and advertisers. There is an established history of cases where individuals have endured privacy infractions and still there are very few regulations or laws that deal with this issue. The information generated, the personal details of people's lives, in most cases is protected only by a weak privacy statement issued by the company, which in many cases is invalidated upon the transfer of company assets during an acquisition. For instance, if a drug company has a person's home address, a detailed list of current treatments, and doctors' names, then, in some instances, upon their purchase this data will not be protected by the original clause provided. This information can also be unknowingly leaked if the data storage devices of the company are not properly sanitized.

Most of the devices mentioned here are designed to benefit the ill and the elderly. For instance, the Caregiver's Assistant is a product targeted towards the elderly population; a population that is frequently preyed upon by the nefarious people of this world. With the security issues inherent in RFID, certain people would benefit greatly if they could access this sort of data to know exactly when to strike. Eavesdropping on the communication between the wireless sensor networks of Caregiver's Assistant would be feasible to those with the motivation and knowledge of RFID technology.

In addition to the personal dangers involved in the wireless medical devices, these products also present the threat of legal and sociological prejudicial injustices to the users. One possible scenario is in the case of healthcare and life insurance companies' rates. Life insurance rates are based on the risk that is taken on by the company. If an insurance company opens a new policy with a 25 year old, married, non-smoker the rates would be lower than that of a smoking, skydiving, race-car driving single male. So if a life insurance carrier discovers, through the Caregiver's Assistant, that an individual is consistently eating the wrong foods or occasionally skips a medication regimen the carrier may be inclined to raise the rates on this person. Also, if it is discovered through the Lifeguard System's logged data that a person's heart rate is always racing three times a day, a life and healthcare insurance company could conclude that the person eats poorly and could be in danger of a cardiovascular disease. This client could have their rates increased or be denied insurance. Although the Caregiver's Assistant program and Lifeguard System are designed to enhance healthcare and lower costs, if the data is not securely managed and implemented properly, the exact opposite effect may occur.

An individual's right to privacy and to simply be alone without having your actions tracked is another privacy right that is in danger of being compromised with many of these devices. Currently, if a person installs a lo-jack system in their car, the police are capable of tracking the location of the car to the block that it is located. This technology is meant for a vehicle to be found in case of a theft, however, there have

been cases where suspects in a criminal case have been tracked via the lo-jack installed on their own vehicle. Similarly, the wireless telemedical devices that have the ability to locate individuals in case of an emergency offer an amazing benefit to a patient if emergency assistance is needed. This feature is unfortunately not always able to be properly controlled at all times and has the potential to violate the privacy of an individual. Law enforcement officials can track suspects via the VeriChip (or Lifeguard, VPS, or Caregiver's Assistant). Parents can also track their children, spouses can track their significant others, and stalkers can track their prey easily if they can access these devices. In terms of potential abuse, this system is ripe with possibilities if/when an unauthorized person gains access to the tracking technology.

Privacy in this modern age grows distant by the second, with broadband access becoming common across the nation, a growing Internet population, a growing crime rate in identity theft and a newer generation with the ability to adapt to newer technology without the proper responsibility. Even in the most remote areas of this world satellites can detect signals transmitted from a device. For this reason companies today must be responsible in addressing security concerns of the growing field of wireless telemedical devices to preserve the privacy of individuals. Without proper security, the dangers of these devices outweigh the immense benefits of these devices.

Conclusion

When interviewed under condition of anonymity, four individuals representing four different communities in this society, their major concern regarding future advances of wireless telemedical technology was data security. From this small sampling and countless other media and privacy advocates, it is clear that should the healthcare system adopt this fledgling branch of technology, the largest concern to be addressed should be privacy. Most people are not concerned about the physiological data gathered from a person should the proper authorized individuals be the sole recipients of this data. It is the potential for foul play by parties who are capable of obtaining this data that causes patients to be wary of this technology. Currently, these devices do not meet the following pre-requisites that would allow for the mass distribution to patients in the healthcare environment:

- A secure method of transferring the data gathered from a body to the designated individuals who must garner the consent of the patient.
- Secure guidelines for the management of the data received from the wireless telemedical devices.
- Secure sanitation methods and enforcement of the data storage devices that contain the data obtained from the patient.
- Corporate responsibility of the data being captured.

Only when these four conditions are met should the healthcare industry begin to utilize wireless telemedical devices. Otherwise patients may suffer severe violations of their privacy that will prove to do more harm than good. Perhaps in the next decade a new realm of patient diagnosis will not require a patient to leave their personal abode, post-operational hospital stays will be shortened, and emergency services will be capable of arriving on the scene prior the start of a life threatening attack.

References

[1] Google Answers, Retrieved December 10, 2004
URL: http://answers.google.com/answers/threadview?id=416530

[2] GPS found its way into telemedicine, Retrieved December 14, 2004
URL: http://www.gps-practice-and-fun.com/telemedicine.html

[3] Alex Pentland, Healthwear: Medical Technology Becomes Wearable, Computer IEEE 2004

[4] Harry Stockman. Communication by Means of Reflected Power. IRE, pp1196-1204, October 1948.

[5] RFID. Retrieved January 4, 2005. http://en.wikipedia.org/wiki/RFID.

[6] John Oates. The Register. Retrieved January 10, 2005,
http://www.theregister.co.uk/2004/06/15/symbian_virus/

[7] Martin Herfurt. Long Distance Snarf Experiment. Retrieved January 10, 2005.
http://trifinite.org/trifinite_stuff_lds.html.

[8] Lifeguard Overview, Stanford Lifeguard Website, Retrieved December 23, 2004
URL: http://lifeguard.stanford.edu/lifeguard_flyer.pdf

[9] Lifeguard Specifications, Stanford Lifeguard Website, Retrieved December 23, 2004
URL: http://lifeguard.stanford.edu/lifeguard_system_specs.pdf

[10] National Center for Space Biological Technologies Stanford University and NASA Ames Research Center, Lifeguard- A Personal Physiological Monitor For Extreme Environments, Retrieved December 20, 2004. URL:
http://lifeguard.stanford.edu/presentations/embc_lifeguard_paper_FINAL.pdf

[11] Lifeguard User Guide, Stanford Lifeguard Website, Retrieved December 23, 2004.
URL: http://lifeguard.stanford.edu/Lifeguard_Users_Guide.pdf

[12] PRNewswire, Medical Intelligence - A Quebec firm invents the VPS, a revolutionary wireless portable automatic cardiac alert system, Copyright 2003, Retrieved December 27, 2004. URL:
http://www.forrelease.com/D20031112/mo188.P1.11122003110609.19047.html

[13] CBC News, Quebec invention detects early signs of heart attack, October 13, 2004. URL:
http://www.cbc.ca/story/science/national/2004/10/13/heart_attack041013.html

[14] Vital Positioning System Product Page, Medical Intelligence website, Retrieved December 28, 2004. URL: http://www.medicalintelligence.ca/en/produits.html

[15] CTV.ca News Staff, Quebec detects heart attacks, calls 911, October 13, 2004

URL:http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1097684928988_93094128?hub=Canada

[16] Cox, John, Bluetooth's sprawl heightens security concerns, Network World, May 17, 2004. URL: http://www.nwfusion.com/news/2004/0517bluetooth.html

[17] Intel Corporation, Digital Home Technologies for Aging in Place. Version 1, February 2004.

[18] Proactive Health Case Study, Intel Corporation website, Retrieved January 10, 2005. http://www.intel.com/research/prohealth/cs-aging_in_place.htm

[19] Intel Corporation website, Wireless Sensors. Retrieved January 11, 2005. URL: http://www.intel.com/research/exploratory/wireless_sensors.htm

[20] Intel Corporation, Digital Home Technologies for Aging in Place. Version 1, February 2004. URL: http://www.intel.com/research/exploratory/digital_home.htm

[21] Intel Corporation website. Retrieved January 11, 2005. URL: http://www.intel.com/research/exploratory/digital_home.htm#improving

[22] Mark Baard. RFID Keeps Track of Seniors. Retrieved January 3, 2005. URL: http://www.wired.com/news/medtech/0,1286,62723-,00.html?tw=wn_story_page_next1

[23] FDA communication to J. Santelli, VP Digital Angel Corp. Retrieved January 3, 2005. http://www.sec.gov/Archives/edgar/data/924642/000106880004000587/ex99p2.txt.

[24] About VeriChip, Applied Digital website, Retrieved January 3, 2005 http://www.4VeriChip.com/nws_10132004FDA.htm

[25] About VeriChip, Applied Digital website, Retrieved January 3, 2005 http://www.4VeriChip.com/nws_10132004FDA.htm

[26] Applied Digital Sets VeriChip Privacy Guidelines, Retrieved January 3, 2005. http://www.rfidnews.org/weblog/2004/12/05/applied-digital-sets-VeriChip-privacy-guidelines/.

[27] Form 10-Q for Applied Digital Solutions Inc., Quarterly Report. November 3, 2004.

[28] Form 10-Q for Applied Digital Solutions Inc., Quarterly Report. November 3, 2004.

[29] Vincent J. Schodolski, Chicago Tribune. Chips implanted under people's skin raise privacy issues. December 25, 2004.

[30] M. Granger and Elaine Newton of CMU. Protecting Public Anonymity. October 26, 2004.