2-2012

An Amulet for Trustworthy Wearable Mhealth

Jacob Sorber
Dartmouth College

Minho Shin
Myongji University

Ronald Peterson
Dartmouth College

Cory Cornelius
Dartmouth College

Shrirang Mare
Dartmouth College

See next page for additional authors

Authors

Jacob Sorber, Minho Shin, Ronald Peterson, Cory Cornelius, Shrirang Mare, Aarathi Prasad, Zachary Marois, Emma N. Smithayer, and David Kotz

An Amulet for Trustworthy Wearable mHealth

Jacob Sorber, Minho Shin†, Ronald Peterson, Cory Cornelius, Shrirang Mare, Aarathi Prasad, Zachary Marois, Emma Smithayer, David Kotz

Dartmouth College, Hanover, NH; USA †Myongji University; South Korea

ABSTRACT

Mobile technology has significant potential to help revolutionize personal wellness and the delivery of healthcare. Mobile phones, wearable sensors, and home-based tele-medicine devices can help caregivers and individuals themselves better monitor and manage their health. While the potential benefits of this "mHealth" technology include better health, more effective healthcare, and reduced cost, this technology also poses significant security and privacy challenges. In this paper we propose *Amulet,* an mHealth architecture that provides strong security and privacy guarantees while remaining easy to use, and outline the research and engineering challenges required to realize the Amulet vision.

1. INTRODUCTION

Mobile phones, coupled with wearable sensors, implanted medical devices and home-based tele-medicine devices, can help caregivers and individuals themselves better monitor and manage their health [23]. Products are already emerging to support long-term continuous medical monitoring for outpatients with chronic medical conditions [27], individuals seeking to change behavior [6], physicians needing to quantify and detect behavioral aberrations for early diagnosis [2], or athletes wishing to monitor their condition and performance [10]. In all of these examples, the health-related data is typically stored in the Patient's mobile phone, or in a cloud-based health records system (HRS) operated by a healthcare provider or device vendor. In this paper, we use the term "Patient" to describe the subject of sensing in all such use cases, using the capitalized form as a reminder of its broader meaning.

While the potential benefits of patient-centric "mHealth" technology include better health, more effective healthcare, and reduced cost, this technology also poses significant security and privacy challenges [22]. To be successful, mHealth technology must be (1) trusted by the Patient to ensure the privacy of the personal information collected, (2) trusted by both Patient and Provider to ensure the integrity of the data and the security of any actuators in the system, and (3) usable without technical expertise. Current approaches fail to provide the desired security, privacy, and usability goals, or are limited to a specific solution isolated to a particular product. In this paper we propose *Amulet,* an mHealth architecture (shown in Figure 1) that provides strong security and privacy guarantees while remaining easy to use, and outline the research and engineering challenges required to realize the Amulet vision.

To enable trustworthy patient-centric mHealth we need to ensure several important properties. The system must provide data confidentiality (avoiding exposure of patient data to unauthorized parties), data integrity (protecting data from tampering, or replay of stale data), data authenticity (ensuring that the data comes from the correct sensor, on the correct patient), data availability (limiting data loss and latency), and command authenticity and integrity (ensuring that commands sent to actuators are not forged, tampered, or replayed). Furthermore, given the likely use of wireless body-area communications, the system should protect patient anonymity (preventing bystanders from learning the Patient's identity or inferring their medical condition). Most challenging, such systems must also support interoperability and modularity (to avoid device proliferation), and ease of use (regarding both functionality and security). For a comprehensive overview, see our earlier work [1, 25].

Existing approaches do not provide all of the above properties. Although space is too limited to list all existing systems, all of them fit into one of four models, each having significant limitations, as shown in Figure 2. Many interesting mHealth applications involve sensors that must be on the body, periodically or continuously, obviating the first approach shown in the figure; but providing the necessary computational and network infrastructure on every sensor node is expensive, obviating the fourth approach. A mobile phone or base station is often needed to provide computational and network support. A base station (model 3) remains at home, and thus is not always present. A mobile base station (e.g., HealthPAL [13]) or mobile phone (model 2) provides portability, and yet may be set aside, left behind, lost, or lent to another, thus it too may not be present. General-purpose computing platforms, like mobile phones, are difficult to secure [9]. Many critical applications (monitoring the heart for atrial fibrillation, or managing blood glucose through an insulin pump) require continuous presence of a trusted device.

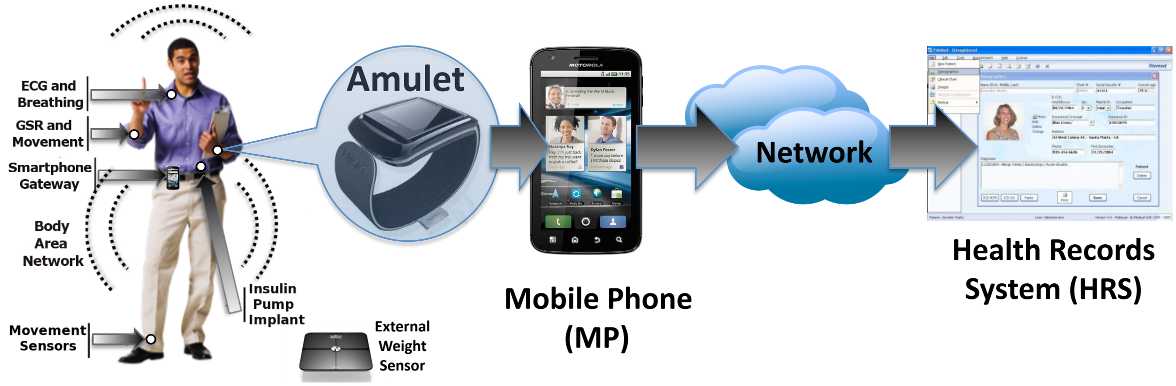
Our position. To reach their full potential in transforming healthcare, wearable networks of sensors and actuators must be able to operate continuously and securely without relying on mobile phones and other non-wearable personal computing devices. We need a personal device that is with the user at all times, can authenticate its wearer, can be secured independently of other apps on the mobile phone or home computer, can provide a trustworthy interface to the user, and support mHealth devices with computation and a network link to the mobile phone or other Internet gateway.

This paper describes our research vision for a trusted wrist-worn platform called *Amulet.* An amulet is "an ornament or small piece of jewelry thought to give protection against evil, danger, or disease" [MacOS dictionary]. Unlike prior approaches, Amulet is designed to enable continuous sensing and actuation, requiring a wireless gateway (mobile phone or access point) only for occasional connectivity to back-end servers and other off-body network resources.

When complete, Amulet makes six contributions. (1) Amulet is an omnipresent, trustworthy hub for patient-centric mHealth that is usable, secure, and interoperable. (2) Amulet provides a means to authenticate its wearer, and to determine which set of sensors are on the same body. (3) Amulet provides a trustworthy path for mHealth devices to communicate with their wearer, the Patient. (4) Amulet provides a physically secure but easily accessible port for access to data in emergencies. (5) Amulet is a robust security architecture based on a tamper-resistant physical platform, cleanly separates the health-related apps on Amulet and the Patient's other

HotMobile'12 February 28–29, 2012, San Diego, CA, USA.

Figure 1: Our proposed architecture is built around a trustworthy wrist-worn Amulet device.



apps on a mobile phone or PC, and supports a secure method for software distribution and management. (6) Amulet provides a safer programming model for safety-critical processes, automating data provenance and other security tasks.

In the following sections we describe Amulet, discuss its many advantages over the existing models, address some of the potential disadvantages, and outline the research and engineering challenges required to realize the Amulet vision.

2. AMULET VISION

In this section we describe our Amulet vision with two scenarios.

Scenario 1 (Diabetes). Susan is a diabetic who finds it difficult to manage her condition effectively, resulting in significant variation in her diurnal blood-glucose levels. Susan visits her doctor for consultation. Her doctor prescribes a continuous glucose monitor, an insulin pump, and a particular insulin therapy and adds this prescription to her health record. Susan's pharmacy has access to the prescriptions in the health record, and provides her with a glucose sensor and a pump (both approved by a trusted third party, e.g., the FDA). The pharmacist calibrates the two devices and then installs appropriate trusted software, configuring it to provide the sensing regimen and the insulin therapy as prescribed by the doctor. Finally, the pharmacist enters Susan's information (her patient ID, and her Amulet's public key) in the devices.

After receiving the devices from the pharmacy, Susan associates them with her Amulet. She presses a button on the Amulet that tells the Amulet that it needs to associate with a nearby device, and moves her wrist over the glucose sensor. The NFC signal from the Amulet activates the glucose sensor and it associates with the Amulet, after the sensor verifies that it is indeed Susan's Amulet and Susan's Amulet verifies whether this type of glucose sensor was prescribed to her. (Her Amulet syncs with her health record periodically and knows what medical devices have been prescribed.) She repeats the association process with the insulin pump. During the association process, the devices share a URL with the Amulet, which points to a signed piece of code (much like an 'app' on a mobile phone) that the Amulet downloads, verifies, and installs. The Amulet uses this app to communicate with and manage the devices.

The Amulet discreetly alerts Susan whenever her glucose levels require attention, through visual, audible, or tactile feedback; if she wants to see more detail, the Amulet shares the data with her phone or tablet to leverage the larger display. The Amulet periodically sends the glucose readings and insulin dose information to the hospital HRS via her mobile phone.

Scenario 2 (Emergency access). Helen has cardiac complications after suffering a stroke last year. She has since been conscientious about managing her health. She upgraded her Amulet with an app that tells her about her physical activity, and her sleep quality (using the accelerometer in her Amulet). She bought a body scale, blood-pressure cuff, and a treadmill—devices that can be bought without a doctor's prescription. She associates the scale and the treadmill with her Amulet by swiping the Amulet near the scale and the treadmill and pressing a button on her Amulet to approve adding new devices. Now, whenever Helen steps on the scale it displays her weight, fat percentage, and body mass index. Whenever she steps on the treadmill to workout, the treadmill recognizes her (using her Amulet as an identity proxy), and picks a pre-configured workout. Periodically, the scale and the treadmill upload their data to the cloud using the home network (the devices can connect to the home network because the Amulet shared information about the home network with the devices during the association process). She also actively logs her diet in her iPhone (and the iPhone shares this data with her Amulet). Weeks later, when she visits her parents, Helen tells them about her efforts and how she keeps track of her health. She walks near the display in their house and uses gesture recognition to associate the display to her Amulet. She uses her Amulet to select which information is shown on the television.

Her new job is demanding and requires long hours, which negatively affect her stress, diet, and sleep. While walking home one day, she collapses. When emergency responders arrive on the scene, and prepare to take her to the nearby hospital, one responder opens a flap over the mini-USB port on the side of the Amulet. The responder then plugs a USB cable from his PDA to the Amulet. The Amulet provides information, in a standard format, about her medical history, allergies, medications, insurance details, emergency contacts, and a log of the past 24 hours (which includes her sleep data from last night, her activity level, and diet information). The emergency responder forwards this information to the nearby hospital, which uses it to make the necessary preparations while she is en route.

3. AMULET ADVANTAGES

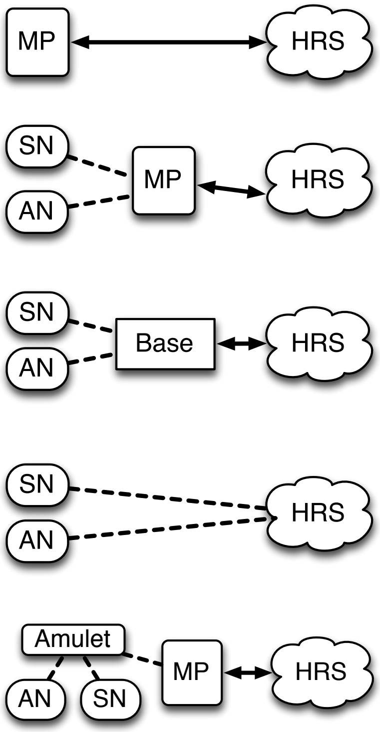
As a small form-factor special-purpose device that is tightly coupled to a Patient's body, Amulet has significant usability, security, and interoperability advantages over existing mobile phone and home base-station systems. We summarize those advantages here.

Usability is a critically important consideration for any mobile device, and even more so for wearable devices. To be successful, patient-centered mHealth devices must be simple, require minimal configuration, and blend into the Patient's daily life.

The Amulet is tightly coupled to the Patient, unlike a mobile phone – phones are often lost, left at home, temporarily lent to others, or cannot be carried everywhere (e.g., contact sports). Any device that provides support for safety-critical sensors and actuators must be ever-present. The wrist-worn Amulet can comfortably be worn at all times (even when sleeping); it may even be waterproof to allow bathing. (Even if the Amulet is removed for some activities, it will likely be more present than a phone, and it would never be lent to another like one might lend a phone.)

The Amulet is in a socially-accepted form factor – a wrist-watch – that is functional jewelry for both genders and most cultures, unlike other wearable alternatives. Such a common form factor is actually beneficial from a privacy point of view, because unlike a mobile base

Figure 2: Various approaches to patient-centric mHealth.



1. Mobile Phone (MP). A phone's internal sensors can be used for health-related monitoring, but some health conditions require other sensors or require contact with a specific part of the body. If the phone is compromised (mobile phone malware is an increasing risk), lost, set aside, or lent to someone else, data may be exposed to, or collected about, the wrong person.

2. MP + wearable or home-based actuator node (AN) or sensor node (SN). The MP may communicate with wearable or nearby devices like a blood-pressure cuff; this architecture is common in the literature. One early example [20] imagined a PDA or cellphone as the hub of a body-area network of mHealth sensors; that paper, like most, did not address the security issues. Again, what if the mobile phone is absent, lost, or compromised? Likewise, are we sure the phone is on the same body as the sensor or actuator [7]? And are they on the *right* body?

3. Base station (Base) + AN/SN. In many current products, the device vendor provides a proprietary base station (or PC dongle), which provides a gateway to the Internet and in some cases a user interface. With a base station for every device, homeowners must configure each base station for their home network, which is inconvenient. Base stations could be equipped with a cellular modem to provide Internet access, increasing cost; Qualcomm's 2Net product is one example. Movement of sensor nodes (SN) outside the range of a base station limits the timely delivery of data.

4. AN/SN with direct connection to HRS. Some home devices have an integrated Wi-Fi or cellular connection and therefore require no communication gateway. Many of the problems described above remain, and the resulting increases in size, weight, power, and cost may be prohibitive for many wearable devices. Cellular modems can draw up to two watts of power, and even the smallest Wi-Fi modems draw more than 100mA of current in their range-limited low-power transmit mode. Other challenges include increases in complexity (more bugs) and an independent network connection that increases exposure to network-based attacks.

5. Amulet model. The Amulet model adds another device to the picture, but it has many advantages (described in Section 3) largely because it operates independently of the mobile phone, is physically attached to the Patient, and is specifically designed for supporting mHealth sensors and actuators.

station (e.g., HealthPAL [13]) the presence of an Amulet does not reveal anything about the Patient's medical condition, or even that she has a condition. Not everyone wears a watch, but if the Amulet is comfortable, stylish, and provides an important health-related function, we expect people will be willing to wear one.

Because it is physically attached to the wearer, the Amulet serves as an identity token when interacting with shared health devices (at home or in clinic) such as a scale, BP cuff, or display. In Scenario 2, recall that the treadmill recognized Helen by her Amulet. The Amulet's form factor also ensures that it is always in the same position on the body, while a phone in a pocket or purse tends to be loose and even a holster may change position from day to day. This tight coupling to the Patient's body provides a natural opportunity for improved accelerometer-based activity recognition [4], for one-body authentication [7], and for seamless gesture-based interfaces [15]. The Amulet is constantly in contact with the skin, which provides the opportunity to measure many of the Patient's physiological parameters, like heart rate, blood oxygenation, galvanic skin response (GSR), and electrical impedance – parameters that are useful in a wide range of medical contexts and may also be useful for automatically authenticating the Patient to the Amulet, without the need to enter pins and passwords [24].

The Amulet is readily accessible at all times; it has a small glanceable display (which is better than any pocket or holster device); with an internal accelerometer and gyroscope it can detect many different gestures, which would make interacting with devices intuitive and easy. Mobile phones have a rich interface and more resources compared to the Amulet, but most people still find it difficult to connect them with other devices (e.g., consider the challenge of securely pairing a device with a mobile phone) [14].

Security is critically important to medical-grade applications. The Amulet provides complete (physical) isolation between general-purpose applications (running on the mobile phone) and critical applications (running on the Amulet); with appropriate hardware support, the Amulet could provide strong isolation between individual apps. In contrast, today's phones are complex multipurpose computing platforms that host a variety of applications provided by different sources, some of whom the Patient may not trust. This makes them susceptible to malware [9] and other software-based attacks. Dual-persona phones [8] can provide some software-level isolation among applications, but none of the other usability advantages outlined above. Nonetheless, Amulet would find a dual-persona phone to be a good partner, when it is available, to provide a larger display or extra computational power.

The Amulet, as a limited-function device running only mHealth apps, can provide much tighter security than a general-purpose phone. Its very simplicity reduces the attack surface. The Amulet supports a relatively narrow range of apps, making it possible to manage execution more strictly. One could re-think the OS design, and design-in security mechanisms (crypto, audit logs, data provenance) as first-class primitives.

Amulet provides a path for discreet output to the Patient (on a small screen, with audible tones, or with vibration). A phone may be infected with malware, and fail to maintain confidentiality or integrity of data displayed. Alerts displayed on the phone may be visible to others who pick up or borrow your phone.

Amulet provides a path for trusted input from the Patient. As a small special-purpose device it can guarantee apps secure access to its limited interface (a few buttons, a small touch-screen, gestures). The Amulet can verify whether it is on the right Patient (see below), and determine whether the user input is coming from the right person. A smartphone, in contrast, can be borrowed or shared, and its input can come from someone other than the Patient, or a malicious program on the smartphone can alter the user's input.

Amulet can include tamper-resistant secure storage for keys – private keys for authenticating the patient, or public keys for authenticating the provider and HRS servers, or session keys with various devices and services. A phone is not suitable for this purpose unless a major manufacturer decides to build in secure storage and make it available to developers. Capacity is cheap; even microSD cards have multi-gigabyte storage, and can be secured with encryption.

The Amulet maintains a secure audit log of its activities – including installation of apps, association of devices, actions taken by actuators, and uses of the emergency-access port – for later review by the Patient, health provider, or even forensic examiners.

Interoperability between wearable devices, mobile devices, and cloud-based services poses significant challenges. The drive for long operational lifetimes has inspired the development of a wide range of low-power wireless technologies (Zigbee, Bluetooth Low Energy, ANT, and various proprietary technologies). An Amulet with multiple low-power radios can make it possible to build mHealth WBANs from devices with heterogeneous radio technologies, and can provide a gateway between a WBAN and a mobile phone. (Phone designers include common standards, such as Bluetooth, but mHealth devices may have (or need) a different radio; Amulet can be designed with these medically-relevant radios inside.)

Emergency access is enabled because the Amulet is always present on the Patient, always on the wrist; conversely, a mobile phone may have been left behind, separated from the Patient during a traumatic accident, or difficult to find in backpack or handbag. The Amulet includes a mini-USB port for emergency responders to retrieve basic information about the Patient's identity, medical history, allergies, prescriptions, and recent medical condition. Physical access to the port would be difficult without the Patient's knowledge, preventing mis-use in non-emergent conditions, and yet access is easy when the Patient is unconscious (under implied consent). Indeed, the USB port would provide access to the data only when the Amulet is on the wrist of its Patient; otherwise the data remains encrypted within the Amulet. This approach ensures that the data is secure even if the Patient loses the Amulet.

The Amulet can verify whether it is on the right Patient using physiological parameters (e.g., GSR, pulse) as biometrics when it is worn, and it can assume that it is on the right Patient until it is taken off the wrist (an action we expect can be detected reliably). Thus, even in an emergency situation where a reliable biometric is no longer available, the Amulet knows it is still on the right Patient. (There should be a "Break the Glass" (BTG) access mechanism that emergency responders can use when all other emergency access mechanisms fail. For example, Gardner et al. [11] use a special key share (BTG-share) to decrypt the PHR data on the phone, and emergency responders obtain this share through a special authorization process, independent of any input from the Patient.)

4. AMULET DISADVANTAGES

There are some obvious disadvantages to Amulet. Patients might not want to wear an additional device like an Amulet. However, we expect that a Patient's concern about their health along with a general desire for the security and privacy of their health information will be motivation enough to wear an Amulet. Additionally, such a device might be too expensive for Patients to purchase. Relevant platforms are starting to reach the market, such as the MetaWatch [17] and MOTOACTV [18]; their retail cost of US$200 will doubtless come down with scale. Insurance companies might subsidize the cost of an Amulet because it might lower their own costs.

From a technological standpoint, one might criticize the relatively limited resources on an Amulet: with less processing power than a mobile phone an Amulet cannot accomplish some of the things that a phone could. We anticipate that such a device will be powerful enough for most health-monitoring applications, and the power of the device will grow over time while maintaining the same form factor. The TI CC2540 Bluetooth Low Energy radio consumes 55 mW when transmitting and 47 mW when receiving at 1 Mbps; a two channel Holter monitor with a 1 kHz sample rate could send data continuously (batched every 10 s) via an Amulet with a 100 mA 3V battery for more than seven days. Data compression could further extend battery life for transmission. The limited nature of an Amulet also allows us to keep our design simple, which benefits the security of the device by shrinking the attack surface.

Finally, Amulet adds some complexity to the existing systems in place; indeed it is yet another device to configure and a potential point of failure. However, the security Amulet provides to the system as a whole outweighs the added complexity, and the hardened nature of Amulet makes it resistant to targeted attacks.

5. RESEARCH CHALLENGES

Many systems and techniques exist that can be leveraged in order to realize the Amulet vision, including protocols for energy-efficient privacy-preserving wireless communication [16] and secure key management [3, 26], as well as OS-level techniques for code isolation [5, 12] and gesture-based interactions [15].

Many of these techniques are too heavyweight for use on low-power wearable devices and will have to be adapted or redesigned. Furthermore, Amulet's success depends on overcoming several additional challenges and taking advantage of key opportunities related to the hardware design, usability, programming model, and code deployment. In this section we list these challenges and sketch some research directions.

5.1 Hardware platform

An ideal Amulet will be small, easily wearable, have long battery life, one or more low-power radios, and sufficient processing power to handle data from a variety of sensor types and provide strong cryptographic algorithms. While we expect future improvements in processor and radio efficiencies and energy storage to ease the tension between battery lifetime and capabilities, we explore Amulet feasibility here in the context of existing hardware. A TI benchmark study [19] that computes a Finite Impulse Response (FIR) filter, similar to tasks an Amulet might execute, showed the TI MSP430 and ARM processor family can compute 20,142 FIR's per second (ARM) and 233 FIR's per second (MSP430). These microcontrollers are used in the MetaWatch [17] and WIMM Labs WIMM commercial platforms [28], two candidates for an Amulet platform. Our initial experiments using the TI CC1101 low-power radio in the MSP430-based Chronos wristwatch platform, with a continuous stream of three-axis accelerometer data at 33Hz, resulted in a CR2032 button battery lasting a week. Many Amulet apps will require less communication and may also be able to harvest energy in order to achieve longer lifetimes. The research challenge here is to balance the form factor, CPU and radio characteristics, workload allowance, and battery life to design an Amulet that is useful for a wide range of applications. And, furthermore, to incorporate hardware support for secure key storage and strong isolation between mHealth apps on the Amulet.

5.2 Usable wearable security

The hardware and form-factor constraints inherent to Amulet demand a fundamentally different approach to security. In addition to having scant processing and energy resources, the Amulet's user interface is limited as well. For example, it is unreasonable to expect users to type strong passwords using a few buttons and a tiny screen. Furthermore, the security of Amulet must be mindful of processing and energy overhead as well as usability.

In spite of its limitations, a wearable Amulet has many security-related advantages of over traditional computing devices. For example, a mobile phone can be in many locations over the course of a day. Its owner might carry it in a pocket or purse, hold it in their hand, set it on the table, or lend it to another person. A loose coupling between a device and its owner makes it difficult to provide guarantees about the authenticity of the data, and it may not be possible to associate sensor data to the correct Patient.

In contrast, the Amulet is physically strapped to a Patient's body, and it is not likely to be shared. Furthermore, the Amulet can always know when it is strapped to a Patient. Gesture recognition, using a built-in accelerometer, could be used for active authentication, or biometric sensors could authenticate the Patient passively. In contrast, there is no unobtrusive way for a mobile phone to authenticate which Patient is carrying it.

The biggest risks result from the loss or theft of a Patient's Amulet. An adversary may seek to extract stored sensor data or medical information, use the Amulet to authenticate as the Patient to various other devices, or use the Amulet to obtain live access to the Patient's sensors and actuators; such threats can be reduced if the Amulet has the capability to reliably authenticate its wearer as described above.

Even if a mobile phone could authenticate the Patient, wearable sensor nodes present another problem. Because such nodes typically communicate with a mobile phone wirelessly, the mobile phone now needs to verify that the sensor is collecting data about the same Patient the mobile phone has authenticated. Not doing so would violate the authenticity of the data since Patient A could authenticate with the mobile phone while Patient B could be wearing the sensor. The mobile phone would then be labeling sensor data about Patient B as coming from Patient A. Thus, the mobile phone needs to be able to perform some type of "same-body authentication" when other sensor nodes are present. Our prior research has shown that accelerometer-based techniques can be used to determine whether two devices are worn on the same body [7], although detecting *which* Patient is wearing a device remains an open and challenging problem. In both cases, a device, like Amulet, that is tightly coupled to the Patient's body is likely to improve both the feasibility and accuracy of these authentication schemes.

Poon et al. [21] demonstrate that it is possible to use biometrics, specifically the inter-pulse interval (IPI), as a shared secret that can be used to securely share encryption keys among sensor nodes on the same body. It is conceivable that this technology could be incorporated to the Amulet or its wristband, providing one means of bootstrapping secure communications with nodes in contact with the skin elsewhere on the body.

5.3 Programming model

In addition to enabling automatic authentication, a more focused device, like Amulet, also has the opportunity to provide a much safer and trustworthy computing environment than a mobile phone or PC. During operation, Amulet runs apps that interact with wearable sensors, actuators, or home devices. These apps may collect health information and forward it to a health record system. They may give feedback or encouragement about fitness-based data. Amulet may also provide limited access to its data to emergency responders.

In spite of this variation, Amulet's apps share many common functions, including sensor discovery, wireless connection handling, encrypting and decrypting data, managing cryptographic keys, processing sensor data streams, routing data and commands to the cloud or to a medical actuator, and securely managing metadata for post-facto auditing and establishing data provenance. These functions add complexity to apps, and the safety and security of the system depends on these tasks being implemented correctly. Amulet's execution environment will provide OS-level support to mHealth apps, with the goal of allowing App developers to focus on the health-related logic and data processing while the Amulet system automates many security and networking tasks. Our focus is on determining what abstractions are most useful, which tasks should be completely automated, and how to balance the need for developer flexibility and security.

5.4 Code Deployment

Finally, the security of Amulet's programming model depends in part on our ability to safely deploy code to a Patient's Amulet, and manage that code throughout the deployment lifecycle.

Amulet setup. How can the Patient's Amulet ensure that it is strapped to the right Patient and that it is linked to the right Patient record? While pairing with mHealth devices, how can the Amulet verify that it is associating with the right mHealth devices, that are collecting health information about the same Patient? As we mention above, the Amulet may use gesture recognition or Patient biometrics to identify the right Patient. The Amulet generates cryptographic keys, saved in tamper-resistant secure storage; it uses these keys to provide encrypted data storage, an encrypted audit log, and an API for secure communication.

Prescription. To safely deploy software to an Amulet, we envision a prescription-based approach, in which a provider writes a software prescription, similar to how medications are prescribed, using terms familiar to physicians. An "application pharmacy" could translate a healthcare provider's nontechnical prescription into a combination of application software and configurations. The pharmacy might also be tasked with detecting harmful interactions between apps. We also expect that a Patient would be able to purchase and install some devices and apps without a prescription.

Developing a workable ecosystem for sensor-software prescriptions will require consideration of the interests and demands of manufacturers, physicians, patients, and FDA regulators, and will likely require precise definitions for types of sensing that might be useful to providers which may or may not fit well with existing medical terminology.

Installation. Once the Patient obtains a new device, how can she verify that it is the right device, as prescribed by the doctor? How can the Patient easily pair her Amulet with the device? To avoid any misuse of medical devices, how can the pharmacist ensure that the purchased medical device is being used by the intended Patient? We sketch some ideas in preceding sections, leveraging existing trust relationships between Patient and provider, Patient and pharmacist, to ensure that only trustworthy apps and authentic devices are installed.

Collection. How can we ensure that the devices associate with the app on the patient's Amulet without patient intervention every time? During installation (above), the device and Amulet exchange keys that allow them to re-discover and re-connect in the future. Whenever the device discovers and authenticates one of its associated Amulets, the data collected is encrypted and sent to the relevant Amulet app for processing.

Control. Apps on the Amulet are responsible for controlling the actions of the sensor and actuator nodes; in the case of sensors, the application monitors the sensors and other contextual information to adjust (as needed) sensing parameters like sample rate. For actuators, of course, the application has overall responsibility for ensuring the actuator is operating correctly according to the treatment protocol. What programming model most effectively splits these duties between Amulet apps, sensors, and actuators?

Processing. Sensor-data processing can occur on a sensor device, the Amulet, a backend server, or on a mobile phone (for less-sensitive applications). What programming abstractions can help the developer work with this split-computation model? The Amulet provides common functions for processing and aggregation of sensor data, and access to greater computation power, while processing on the sensor reduces WBAN bandwidth requirements. An Amulet app collects the data from one or more sensors and sends it to the Patient's health record, so that it can be shared with the Patient's health providers, family and friends. How can the data recipients verify whether the data is coming from the right sensor, was used by the right Patient and in the right manner? To verify the provenance of the Patient's health data, the recipients might need information about the sensor, the Patient and the context in which the data was collected. The Amulet can act as the coordinating device to gather provenance data. How can the Amulet understand the applications' requirements and act efficiently to gather this metadata?

Uninstallation. How many apps and devices should an Amulet support? There might be a limit to the number of apps that can be installed on the Amulet or the number of devices that it can manage. Who should be able to remove apps from the Amulet? Some apps should be at the discretion of the Patient, but there may be medically-critical apps that should only be removed by a physician or pharmacist.

6. SUMMARY

We propose Amulet, a trustworthy mHealth companion device worn like a wrist watch. Our position is that mHealth will only succeed in achieving its goals of improving health and reducing the costs of healthcare if the envisioned health-monitoring and health-management applications are trustworthy. Amulet provides a basis for trust in body-area mHealth systems. Amulet is easy to use, omnipresent, able to authenticate its wearer, and able to mediate communications between the WBAN and smartphone or access point. Amulet provides a path for trusted input from and output to its user, and a secure execution platform for small "apps" that monitor the Patient's health or manage treatment. We outline Amulet's advantages and disadvantages, comparing it to other current approaches, and we identify the key research challenges required to make Amulet a reality.

Amulet has security, usability, and interoperability advantages over the other approaches outlined in Figure 2. Specifically, it has many security and privacy advantages: (1) The Amulet is tightly coupled to the Patient, unlike a mobile phone, which makes it ideal for safety-critical sensors and actuators. Emergency access is enabled because Amulet is always present on the Patient, always on the wrist. (2) Authorized parties (e.g., emergency responders) can access Patient's data through a USB port, but only when the Amulet is on the wrist of its Patient; otherwise the data remains encrypted within the Amulet. (3) The Amulet provides complete (physical) isolation between general-purpose apps (which could be susceptible to software-based attacks), running on the mobile phone, and critical apps (running on the Amulet). (4) Amulet provides a path for discreet output to and trusted input from the Patient, whereas a phone could be accessible to someone other than the Patient and also susceptible to malware attacks. (5) The Amulet is in a socially-accepted form factor; the presence of an Amulet does not reveal anything about the Patient's medical condition. (6) The Amulet can include tamper-resistant secure storage for keys and could maintain a secure audit log of all its activities.

Acknowledgments

This research results from a research program at the Institute for Security, Technology, and Society at Dartmouth College, supported by the National Science Foundation under award numbers 0910842, 1143548, and IIS-1016823, and by the Department of Health and Human Services (SHARP program) under award number 90TR0003-01. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the sponsors.

7. REFERENCES

[1] S. Avancha, A. Baxi, and D. Kotz. Privacy in mobile technology for personal healthcare. *ACM Computing Surveys*, 2012. At http://www.cs.dartmouth.edu/~dfk/papers/avancha-survey.pdf.

[2] E. M. Berke, T. Choudhury, S. Ali, and M. Rabbi. Objective measurement of sociability and activity: Mobile sensing in the community. *Annals of Family Medicine*, 9(4):344–350, July 2011.

[3] D. Bichler, G. Stromberg, M. Huemer, and M. Löw. Key generation based on acceleration data of shaking processes. *Proceedings of Ubiquitous Computing (UbiComp)*, 4717:304–317, 2007.

[4] A. G. Bonomi, A. H. C. Goris, B. Yin, and K. R. Westerterp. Detection of type, duration, and intensity of physical activity using an accelerometer. *Medicine & Science in Sports & Exercise*, 41(9):1770, 2009.

[5] S. Bugiel, L. Davi, A. Dmitrienko, S. Heuser, A. R. Sadeghi, and B. Shastry. Practical and lightweight domain isolation on android. In *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, SPSM '11, pages 51–62, New York, NY, USA, 2011. ACM.

[6] F. Buttussi and L. Chittaro. Smarter phones for healthier lifestyles: An adaptive fitness game. *IEEE Pervasive Computing*, 9(4):51–57, Oct. 2010.

[7] C. Cornelius and D. Kotz. Recognizing whether sensors are on the same body. In *Proceedings of the International Conference on Pervasive Computing*, Lecture Notes in Computer Science, pages 332–349. Springer, June 2011.

[8] Verizon, VMware plan dual-persona phone software. At http://tiny.cc/x0lmm, visited 2011.

[9] A. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner. A survey of mobile malware in the wild. In *Proceedings of the ACM Workshop on Security and Privacy in Mobile Devices (SPSM)*, Oct. 2011. At http://www.cs.berkeley.edu/~daw/papers/mobilemal-spsm11.pdf.

[10] G. Fenu and G. Steri. Two methods for body parameter analysis using body sensor networks. In *International Conference on Ultra Modern Telecommunications & Workshops (ICUMT)*, pages 1–5. IEEE, Oct. 2009.

[11] R. W. Gardner, S. Garera, M. W. Pagano, M. Green, and A. D. Rubin. Securing medical records on smart phones. In *Proceedings of the Workshop on Security and Privacy in Medical and Home-Care Systems (SPIMACS)*, pages 31–40. ACM Press, Nov. 2009.

[12] K. Gudeth, M. Pirretti, K. Hoeper, and R. Buskey. Delivering secure applications on commercial mobile devices: the case for bare metal hypervisors. In *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, SPSM '11, pages 33–38, New York, NY, USA, 2011. ACM.

[13] HealthPAL, mobile health monitoring device. At http://medapps.net/healthpal.html, visited Jan. 2012.

[14] R. Kainda, I. Flechais, and A. W. Roscoe. Usability and security of out-of-band channels in secure device pairing protocols. In *Proceedings of Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2009.

[15] J. Liu, L. Zhong, J. Wickramasuriya, and V. Vasudevan. uWave: Accelerometer-based personalized gesture recognition and its applications. *Pervasive and Mobile Computing*, 5(6):657–675, Dec. 2009.

[16] S. Mare, J. Sorber, M. Shin, C. Cornelius, and D. Kotz. Adapt-lite: Privacy-aware, secure, and efficient mhealth sensing. In *Proceedings of the Workshop on Privacy in the Electronic Society (WPES)*, Oct. 2011.

[17] MetaWatch. At http://www.metawatch.org, visited Jan. 2012.

[18] MOTOACTV. At http://motoactv.com, visited Jan. 2012.

[19] MSP430 competitive benchmarking. At http://www.ti.com/lit/an/slaa205c/slaa205c.pdf, visited Oct. 2011.

[20] C. Otto, A. Milenkovic, C. Sanders, and E. Jovanov. System architecture of a wireless body area sensor network for ubiquitous health monitoring. *Journal of Mobile Multimedia*, 1(4):307–326, 2006. At http://www.ece.uah.edu/~milenka/docs/coamej_jmm06.pdf.

[21] C. C. Y. Poon, Y.-T. Zhang, and S.-D. Bao. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine*, 44(4):73–81, May 2006.

[22] S. Saleem, S. Ullah, and H. S. Yoo. On the security issues in wireless body area networks. *International Journal of Digital Content Technology and its Applications*, 3(3):178–184, 2009.

[23] L. A. Saxon, D. L. Hayes, F. R. Gilliam, P. A. Heidenreich, J. Day, M. Seth, T. E. Meyer, P. W. Jones, and J. P. Boehmer. Long-term outcome after ICD and CRT implantation and influence of remote device follow-up: The ALTITUDE survival study. *Circulation*, 122(23):2359–2367, Dec. 2010.

[24] J. Sriram, M. Shin, T. Choudhury, and D. Kotz. Activity-aware ECG-based patient authentication for remote health monitoring. In *Proceedings of the International Conference on Multimodal Interfaces and Workshop on Machine Learning for Multi-modal Interaction (ICMI-MLMI)*, pages 297–304. ACM Press, Nov. 2009.

[25] J. Sriram, M. Shin, D. Kotz, A. Rajan, M. Sastry, and M. Yarvis. Challenges in data quality assurance in pervasive health monitoring systems. In D. Gawrock, H. Reimer, A.-R. Sadeghi, and C. Vishik, editors, *Future of Trust in Computing*, pages 129–142. Vieweg+Teubner Verlag, July 2009.

[26] F. Stajano and R. Anderson. The resurrecting duckling: security issues for ubiquitous computing. *Computer*, 35(4):22–26, Apr. 2002.

[27] D. Walters, A. Sarela, A. Fairfull, K. Neighbour, C. Cowen, B. Stephens, T. Sellwood, B. Sellwood, M. Steer, M. Aust, R. Francis, C. K. Lee, S. Hoffman, G. Brealey, and M. Karunanithi. A mobile phone-based care model for outpatient cardiac rehabilitation: the care assessment platform (CAP). *BMC Cardiovascular Disorders*, 10(1):5+, Jan. 2010.

[28] WIMM labs. At http://www.wimm.com, visited Oct. 2011.