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

Follow this and additional works at: [https://digitalcommons.dartmouth.edu/facoa](https://digitalcommons.dartmouth.edu/facoa)  
Part of the [Computer Sciences Commons](https://digitalcommons.dartmouth.edu/computer-sciences), and the [Medicine and Health Sciences Commons](https://digitalcommons.dartmouth.edu/medicine-and-health-sciences)

Recommended Citation
Jacob Sorber, Minho Shin, Ronald Peterson, Cory Cornelius, Shrirang Mare, Aarathi Prasad, Zachary Marois, Emma Smithayer, and David Kotz. An Amulet for trustworthy wearable mHealth. In Workshop on Mobile Computing Systems and Applications (HotMobile), February 2012. 10.1145/2162081.2162092

This Conference Paper is brought to you for free and open access by Dartmouth Digital Commons. It has been accepted for inclusion in Open Dartmouth: Faculty Open Access Articles by an authorized administrator of Dartmouth Digital Commons. For more information, please contact dartmouthdigitalcommons@groups.dartmouth.edu.
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 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 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
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 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 is in a socially-accepted form factor – a wrist-watch – and 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

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.
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 – in-
cluding 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 low 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 a 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 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 can detect 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 to reach the market, such as the MetaWatch [17] and MOTOACTV [18]; their retail cost of US$200 will doubtless come.

From a technological standpoint, one might criticize the relatively limited resources on an Amulet: with less processing power than 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 (batted every 10 s) via an Amulet with a 100 mA 3V battery for more than 21 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 burdensome to be used 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, the 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 Wedge [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 being in a critical environment, an energy constrained device such as an 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 each node typically communicate with a mobile phone wirelessly, the mobile phone...
We also expect that a Patient would be able to purchase and install the device mentioned above, the Amulet may use gesture recognition or passive infrared sensors to verify that it is associating with the right mHealth devices, 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.

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, 1141354, and HS-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. Patent pending, all rights reserved.

7. REFERENCES