Using Trusted Sensors to Monitor Patients' Habits

Alec Wolman, Stefan Saroiu, and Victor Bahl
Microsoft Research

Abstract: *Patients are notoriously inconsistent with taking their medications. Doctors and insurance companies have an incentive to monitor and collect data on whether medical patients and insurance customers are following prescriptions and maintaining a healthy lifestyle. A convenient way of gathering such data is using smartphones. For example, accelerometer readings can be used to reveal how physically active a patient is.*

Unfortunately, the readings of a sensor can be easily manipulated. This data's huge financial value makes doctors and insurance companies reluctant to use it unless it can be made more trustworthy. This paper's goal is to start a discussion on how to use trusted sensors to help doctors and insurance companies gather data about their patients' medications in a trustworthy manner.

1 Introduction

Today doctors prescribe medication but have no means of understanding how well their patients are following directions. Medical studies have shown that patients on average self-administer half the medication prescribed [2] and that 10% of hospital admissions are due to patients not taking their medication correctly [8]. The current approaches of addressing this situation, such as patient instructions and counseling, are not very effective, and the medical community is seeking innovative ways to deal with this situation [6].

Both doctors and insurance companies have an incentive to understand whether medical patients are taking their medication. This information can help doctors better understand the prescriptions' effectiveness on an individual patient. At the same time, medical insurance companies want to cut costs. These companies prize healthy customers who live longer and have fewer illnesses. Insurers make more money on healthy customers who continue to pay their premiums for longer periods of time.

One way to collect data that characterizes whether patients follow their prescription is by using a mobile device, such as a smartphone, equipped with sensors. Today's smartphones incorporate many different sensors including a camera, a microphone, an accelerometer, and a location sensor (GPS). People can use their smartphones to automatically collect data about the way in which they take their medication or the type of lifestyle they have. For example, accelerometer readings have already been shown that they can reveal whether a user is running or performing a physical activity of some sort. Similarly, taking a timestamped picture each time a user takes his medication can document the timeline of the medication treatment.

However, today it is very easy to manipulate a smartphone's readings. For example, a simple application can interfere with the readings of an accelerometer without being detected. Such an application can feed in fabricated readings about the lifestyle of a patient. Similarly, photos can be easily photoshopped to alter their timestamps. At the same time, the financial implications of collecting data that characterizes whether patients follow their prescriptions are enormous. There is already strong evidence that insurance companies can use this data as one input to pricing their insurance policies. For example, medical insurance companies have already started offering financial incentives to customers who can demonstrate they are in good physical shape and use preventive services, such as exercising regularly, getting flu shots or mammograms. Gathering such data must be done in a trustworthy manner: doctors and insurance companies must trust that the data collecting from patients and customers has not been tampered with either maliciously or inadvertently.

The goal of this paper is to present one way to collect this data reliably by using trusted sensors: sensors whose readings cannot be easily manipulated by the smartphone's OS or by applications. With trusted sensors, insurance companies can have more trust that readings are not fabricated, but correctly produced by a real sensor. In a recent publication [7] we described two alternate designs for building trusted sensors on today's commodity mobile devices, such as smartphones and laptops. These designs have different properties: the first design offers reasonable security guarantees while it has a low barrier of deployment, while the second design offers much stronger security properties but it requires hardware modification to the actual sensors.

In the remainder of the paper we start by giving a brief background on trusted sensors and the two designs that we are pursuing. We then present our preliminary ideas on how to use them to increase the confidence on the data gathered by sensors. Our goal is to start a discussion on what is the best way of using trusted sensors for gathering data. We also describe a few mechanisms incorporated in our design aimed at providing users with privacy guarantees.

2 Trusted Sensors

This section presents a brief description of two architectures for building trusted sensors together with our approaches to preserve the users' privacy. A more detailed description of these architectures can be found in [7].

Software-only Architecture This architecture makes use of no additional hardware other than a TPM chip available on the mobile device's motherboard. Many laptops today already ship with TPM chips included. This architecture's goal is to isolate a piece of code capable of reading the device's sensors and sign them before passing them to an untrusted application or to the cloud. We use virtualization to achieve this goal and we place the trusted sensor code inside the host virtual machine (e.g., dom0 in Xen or root VM in Hyper-V). Our system returns the signed sensor readings together with a remote attestation whose role is to attest that the mobile device is running the correct software configuration. The combination of these two pieces of data demonstrates that the sensor was read by a "trusted" piece of software that signed the reading before passing it to an untrusted OS or application.

An Architecture with Minor Hardware Modifications This architecture assumes that TPM-like functionality is integrated into each individual sensor. One way to accomplish this is to equip each sensor with an additional chip that is able to perform crypto operations such as signing a piece of data, and seal both chips into a tamper-resistant case. Once the sensing hardware obtains its reading, the sensor uses the crypto chip to sign its data before returning it to the device. We are currently pursuing an implementation of this design with a hardware engineering research group. The challenges of this design are three-fold: the additional crypto functionality should have (1) high performance, (2) low power needs, and (3) low cost.

Privacy Since trusted sensors' readings are signed, the signature can be used to trace back to the identity of the sensor producing the reading. Such functionality raises serious privacy concerns. We are pursuing three approaches to mitigate these concerns. First, the readings of a trusted sensors should be able to be stripped of their signatures if users choose to do so. This would allow people to switch on and off the "trusted" aspect of their sensors' readings. Second, TPMs offer support for anonymity by using group signatures to sign their attestations. With group signatures, a verifier can still detect whether a sensor reading has been tampered with without being able to infer which sensor or smartphone signed the reading. Finally, we are also pursuing the design of a protocol that can provide the non-transferability of the readings' signature. With such a property, users are able to ensure that no one else can prove the validity of the trusted sensors' signature. We use a variant of a zero-knowledge protocol [5] to achieve this property.

3 Monitoring Patients' Habits

This section's goal is to present a few scenarios on how to use trusted sensors to gather data about patients' habits in a trustworthy manner. We believe there are many possible uses of trusted sensors for such a task and the role of our scenarios is to serve as preliminary examples.

Recording Active Lifestyles People have already started using smartphones' sensors to record their daily activities. For example, smartphones can easily be equipped with pedometers to record how many steps a user has taken. Similarly, accelerometers can be used to detect whether people are walking, running, or riding a bike. A smartphone application can keep a log of a user's physical activities over a longer period of time. Such a log can help shed light on how active users' lifestyles are.

One way to obtain even more detailed information on whether a user is pursuing an adequate level of physical activity is to use body sensors that communicate their readings to a smartphone over a short-range wireless radio. Body sensor networks are already actively developed by industry [4].

Following Prescriptions when Taking Medication An automatic way to record data about following medical prescriptions is to use a pillbox equipped with a trusted pressure sensor. The pillbox would record changes in pressure whenever its compartments are opened to record when a person takes their medication.

Another approach is to have patients use a trusted camera to take timestamped pictures whenever they take their medication. The collection of pictures could be used by doctors to increase their confidence in patients following their prescription correctly.

Documenting the Use of an Electric Toothbrush Dental insurance companies want to encourage their customers to develop healthy dental habits [3]. One example is using electric toothbrushes which have been shown to be more effective at removing dental plaque than regular toothbrushes [1]. An electric toothbrush could be equipped with a trusted sensor, such as an accelerometer, that detects and logs its use. The toothbrush can periodically dump its data to a computer that can process it and send the processed information to a dentist or an insurance company. Some electric toothbrushes are already equipped with timers that tell people how long they need to brush for [1].

4 Conclusions

This paper described how trusted sensors could be used to gather data bout people's health. Our goal is to start a discussion on the use of such technology in helping doctors and insurance companies obtain a more clear picture of people's health. Such a discussion must include both the benefits of collecting such data and the potential privacy risks.

References

[1] Animated-Teeth.com. How effective are electric toothbrushes? `http://www.animated-teeth.com/electric_toothbrushes/t2_sonic_toothbrushes.htm`.

[2] D. L. Sackett and J. C. Snow. *Compliance in Health Care*. Baltimore: Johns Hopkins University Press, 1979.

[3] dentalinsurance.com. Oral Health, 2006. `http://www.dentalinsurance.com/di/web/articles/OralHygiene/index.aspx?year=2006&quarter=1`.

[4] E. A. Moore. Coming to a bedside near you: Body sensor networks, 2009. `http://news.cnet.com/8301-27083_3-10323325-247.html`.

[5] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. In *Proceedings of the 17th STOC*, Providence, RI, May 1985.

[6] R. B. Haynes and E. Ackloo and N. Sahota and H.P. McDonald and X. Yao. Interventions for enhancing medication adherence. *Cochrane Database of Systematic Reviews*, 2(CDCD000011), 2008.

[7] S. Saroiu and A. Wolman. I am a Sensor, and I Approve This Message. In *Proc. of the 11th Workshop on Mobile Computing Systems and Applications (HotMobile)*, Bolton Landing, NY, February 2010.

[8] Woman's Day. Everything You Need to Know About Your Meds, 2010. `http://www.womansday.com/Articles/Health/Everything-You-Need-to-Know-About-Your-Meds.html`.