Poster: Practical Trusted Computing for mHealth Sensing

Jacob Sorber, Minho Shin, Ron Peterson, David Kotz

Dartmouth College — Institute for Security, Technology, and Society
{sorber,mhshin,rapjr,kotz}@cs.dartmouth.edu

ABSTRACT

Mobile sensing technologies present exciting opportunities for healthcare. Wireless sensors can automatically provide sensor data to care providers, dramatically improving their ability to diagnose, monitor, and manage a wide range of medical conditions. Using mobile phones to provide connectivity between sensors and providers is essential to keeping costs low and deployments simple. Unfortunately, software-based attacks against phones, which can have significant consequences for patients, are also on the rise.

This poster describes a simple, flexible, and novel approach to protecting both the confidentiality and integrity medical sensing and data processing on vulnerable mobile phones, using plug-in smart cards—even a phone compromised by malware. We describe our design, implementation, and initial experimental results using real smart cards and Android smartphones.

1. POSTER DESCRIPTION

Mobile sensing technologies are poised to improve the quality, efficiency, and cost of healthcare around the world [2]. Applications of these *mHealth* sensing technologies include both clinical (e.g. diabetes or hypertension management) and non-clinical purposes (e.g. lifestyle coaching, elder care, and personal fitness), and nearly all use a gateway to collect and process data from low-power sensors and forward it to a back-end service, like an Electronic Health Record (EHR), Personal Health Record(PHR), or a vendor-managed portal. Current gateways are typically proprietary single-purpose devices, however, using the mobile phones that patients already carry as gateways will ease the deployment of these sensing applications without further increasing cost.

Using commodity mobile phones to collect and process safety critical health data is also risky. Mobile phone software is increasingly complex and vulnerable to malware and other software-based attacks, and as phones find uses in more critical processes (e.g. banking, healthcare, and location-based services), they present an attractive target for attackers. These attacks present a significant challenge to the safety of these mHealth systems.

Our goal is to ensure the confidentiality and integrity of mHealth sensor data as it is processed by untrusted mobile phones. Our approach uses a tiny trusted component—implemented on a microSD smart card plugged into a patient's phone—that allows applications running on the phone to safely collect and process data from a body-area network of sensor devices. Even if the phone is compromised by malware, the phone will not leak sensitive sensor data, nor be able to modify the results reported to the back-end services used by the patient or caregivers without being detected.

This goal is achieved by processing sensitive data on the smart card. Using a simple API, an application imports raw sensor-encrypted data into the smart card, instructs the card how to process the data, and exports the results, encrypted for use only by backend services. Neither the values of raw nor processed data are exposed outside of the card, and a novel hashing-based technique allows backend services to verify that data was processed correctly.

This model has a number of advantages. Applications remain flexible and easy to both update and deploy. Since no application-specific software is loaded onto the smart card, the trusted computing base (TCB) is both simple and small—making it easier to secure. The generality of our smart-card API also makes it amenable to compile-time optimizations and native support in general purpose languages in order to make application development seamless.

Finally, this represents a simpler alternative to other proposed approaches including trusted hypervisors [1], trusted hardware (such as a TPM [3]) that require trust and agreement among many parties—most of whom have nothing to do with healthcare delivery—and hardware that has not yet appeared in common mobile phones.

This poster describes our system design, an implementation using Java-based smart cards and Android mobile phones, and our initial experimental results. Our experiments demonstrate that our approach incurs acceptable overhead for use in mobile devices and adequate performance for a number of applications with low-to-medium data-rate requirements. We also identify opportunities for dramatic improvements that will allow support for more data-intensive sensor applications as smart card technology evolves.

2. REFERENCES

[1] P. Gilbert, L. P. Cox, J. Jung, and D. Wetherall. Toward trustworthy mobile sensing. In *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications (HotMobile)*, pages 31–36. ACM, Feb. 2010. DOI 10.1145/1734583.1734592.

[2] 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. DOI 10.1161/CIRCULATIONAHA.110.960633.

[3] Trusted Computing Group. TPM Main Specification Level 2 Version 1.2, Rev 103. http://www.trustedcomputinggroup.org/resources/tpm_main_specification.

MobiSys'11, June 28–July 1, 2011, Bethesda, Maryland, USA.
ACM 978-1-4503-0643-0/11/06.