Demo Abstract: A Trusted Platform Based Framework for Participatory Sensing

Akshay Dua
Portland State University
akshay@cs.pdx.edu

Wen Hu
CSIRO ICT Centre, Australia
wen.hu@csiro.au

Nirupama Bulusu
Portland State University
nbulusu@cs.pdx.edu

ABSTRACT

"Participatory sensing" is an exciting new paradigm where people voluntarily sense their local environment and share this data using mobile phones and the Internet. It can revolutionize applications such as intelligent transportation, public health and social networking. However, a major concern is the amount of trust that can be placed in the shared data. We address this concern in our demonstration by using a Trusted Platform Module (TPM) in conjunction with a smart phone. The TPM is responsible for attesting the application on the phone to assure remote entities that the application has not been tampered with. To the best of our knowledge, this is the first demonstration of application attestation on a smart phone employing a TPM.

1. INTRODUCTION

In the future, people will use their sensor equipped mobile phones to monitor the urban world. This emerging paradigm, called "Participatory Sensing" has spawned several interesting applications[2, 4]. For example, in the Nericell project[4], people share location and audio data captured by their mobile phones. An aggregation server receiving this data relies on it to predict traffic conditions. Thus, it would be desirable to provide some assurances about the reliability of the contributed data.

In this work, we demonstrate how producers of data in participatory sensing applications can prove to consumers that their data is reliable. Wang et al.[5] find that reliability and trustworthiness are one of the most important attributes consumers use to judge data quality. We provide trustworthiness by guaranteeing that the application producing the data is not modifying it in an unintended manner. This guarantee is provided by a Trusted Platform Module (TPM) at the producer, which, attests that the application binary was not modified from its original.

2. BACKGROUND

The Trusted Platform Module is a hardware security device that provides three main features: protected storage capabilities, platform integrity measurements, and platform integrity reporting. Our demonstration uses a TPM device which confirms to Version 1.2 of the TPM specification created by the Trusted Computing Group (TCG)[1].

Each TPM device comes with an Endorsement Key (EK)—a RSA public–private key pair—burned into the device by its manufacturer. This key is never exposed outside the TPM, thus, any information signed using the EK must have originated from the device using the TPM.

TPM devices are available in many of today's laptops and PCs as a standard feature. However, typical participatory sensing applications require its abilities on a mobile phone. Currently, we do not know of any commercially available mobile phone with a built-in TPM. Thus, our demonstration uses a TPM device (called *secfleck*) originally built for the fleck sensor node[3]

3. DEMONSTRATION OVERVIEW

The entire demonstration setup is shown in Figure 1. Both the TPM and the phone (Nokia N800) are Bluetooth enabled and a secure communication channel is established between them using standard bluetooth security features. An application running on the phone is responsible for taking integrity measurements and passing them on to the TPM. The measurements are then used in the remote attestation protocol to establish trust between a producer and a consumer. The integrity measurement followed by the integrity reporting procedure provides application attestation. Typically, integrity measurement begins with the producer

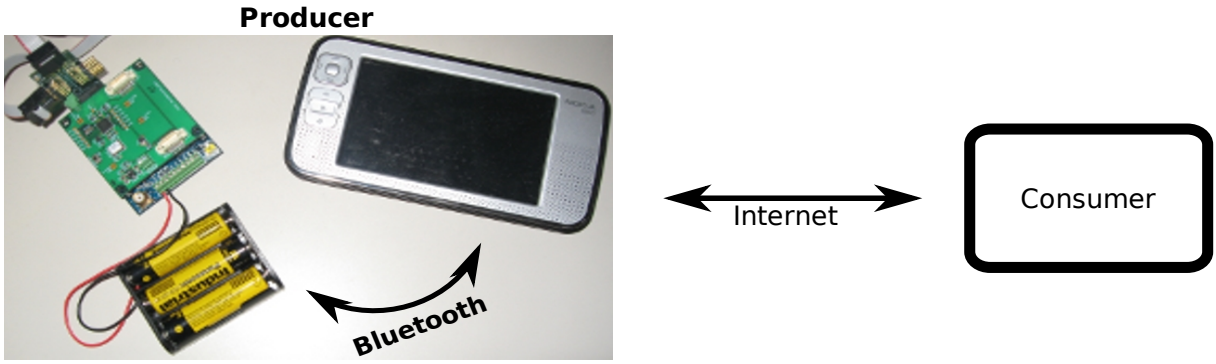

Figure 1: Demonstration setup

creating a digest of the application binary using an algorithm like SHA-1. The resulting digest is then stored securely inside the TPM in a Platform Configuration Register (PCR). We will refer to this value as V_{PCR}.

The integrity reporting phase begins when a consumer makes a request for attestation. Then, the TPM signs V_{PCR} and sends $\{V_{PCR}\}_{EK}$ back to the consumer. Here, $\{V_{PCR}\}_{EK}$ is V_{PCR} sent along with the TPM's signature created using the Endorsement Key. The consumer then creates a digest (V_{app}) of the application binary that it expects the producer is executing. Next, it verifies the TPM signature and compares V_{PCR} with V_{app}. If they match, the consumer assumes the data from the producer to be trustworthy. The entire exchange is shown in Figure 2. Note that our demonstration is based on the following assumptions: the mobile phone is trusted, the application performing integrity measurements is trusted, and the TPM is securely bootstrapped.

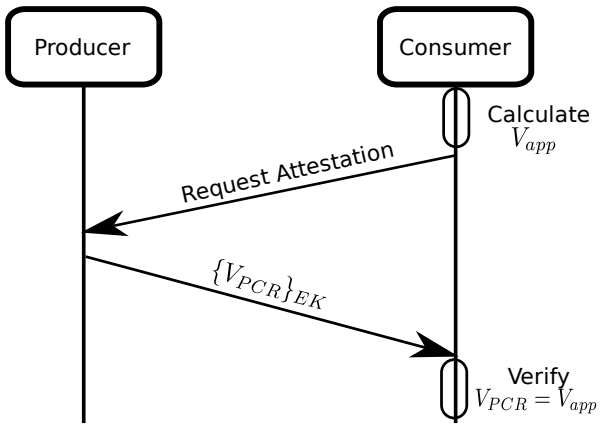

Figure 2: The producer attests the integrity of its application for a remote consumer

4. CONCLUSION

We have presented the first demonstration of remote application attestation on a mobile phone using a Trusted Platform Module (TPM). The consumers place trust in the data sent by a producer if and only if the producer's TPM can attest that the application producing the data was not modified from its original.

5. REFERENCES

[1] Trusted computing group. `https://www.trustedcomputinggroup.org/home`.

[2] Y. F. Dong, Salil S. Kanhere, Chun Tung Chou, and Nirupama Bulusu. Automatic collection of fuel prices from a network of mobile cameras. In Sotiris E. Nikoletseas, Bogdan S. Chlebus, David B. Johnson, and Bhaskar Krishnamachari, editors, *DCOSS*, volume 5067 of *Lecture Notes in Computer Science*, pages 140–156. Springer, 2008.

[3] Wen Hu, Peter Corke, Wen Chan Shih, and Leslie Overs. secfleck: A public key technology platform for wireless sensor networks. In *EWSN*, pages 296–311, 2009.

[4] P. Mohan, V.N. Padmanabhan, and R. Ramjee. Nericell: rich monitoring of road and traffic conditions using mobile smartphones. In *Proceedings of the 6th ACM conference on Embedded network sensor systems*, pages 323–336. ACM New York, NY, USA, 2008.

[5] R.Y. Wang and D.M. Strong. Beyond accuracy: what data quality means to data consumers. *Journal of Management Information Systems*, 12(4):5–33, 1996.