

Deploying Trusted Hardware to Secure Urban Sensing

Ajay Venkateshan Krishnaprasad
Stony Brook Network Security and
Applied Cryptography Lab
Stony Brook, NY 11794-4400
ajayvk@cs.stonybrook.edu

Radu Sion
Stony Brook Network Security and
Applied Cryptography Lab
Stony Brook, NY 11794-4400
sion@cs.stonybrook.edu

ABSTRACT

We propose to develop an infrastructure to secure urban sensing by making use of Nokia smart phones that are equipped with trusted hardware. The cellular devices are used to capture audio in an urban environment. Confidentiality of sensed audio is ensured by encrypting it using the credentials provisioned to the cellular devices over an encrypted channel. Trusted hardware is also used to ensure privacy as civilian devices are utilized in the proposed paradigm.

Categories and Subject Descriptors

C.2.1 [Computer-Communication Networks]: Wireless communication

General Terms

Security

Keywords

Urban Sensing, Trusted Hardware, Wireless Devices.

1.INTRODUCTION

As cities grow, they become increasingly vulnerable to disruptive events, such as natural disasters, malicious attacks, and social conflicts. The consequences of adverse long-term changes in the urban environment also become more severe. Trapping the occurrence of such events in real-time does not only help in providing the imperative aid, but also prevent the repercussions of such events. This mandates the development of a system enabling urban agencies to collect and analyze information about

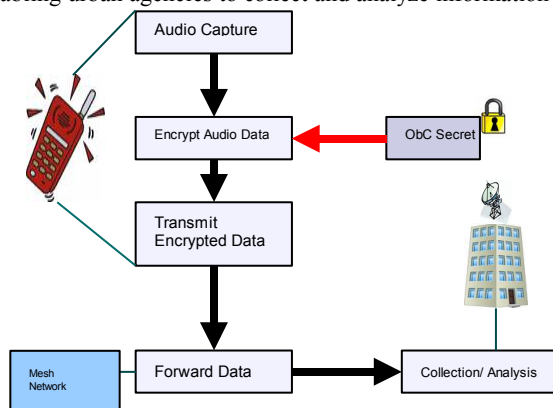


Figure 1.1: Audio capture and transmission of encrypted audio.

the infrastructure and environment, and quickly identify the occurrence and location of unusual events from such data.

The proliferation of wireless devices with increasing capacity and accessories provides an unprecedented level of resources for the development of such a system (see Figure 1.1 for illustration). At the same time, privacy-related issues with the use of civilian devices, as well as issues related to ensuring confidentiality of the captured data are a major concern in an urban setup. Present day cellular devices are equipped with powerful secure environments that facilitate secure execution of programs coupled with secure storage of related credentials. These secure environments could be leveraged to ensure security and privacy of the captured data in an urban infrastructure.

2.PROPOSAL

In this work, we propose to build secure mechanisms for urban sensing. In a proof of concept prototype, we will use the open credential platform of the Nokia N-Series cellular devices, which leverages on-board secure environments (see Figure 2.1 for illustration). Logic and data packages containing the credential

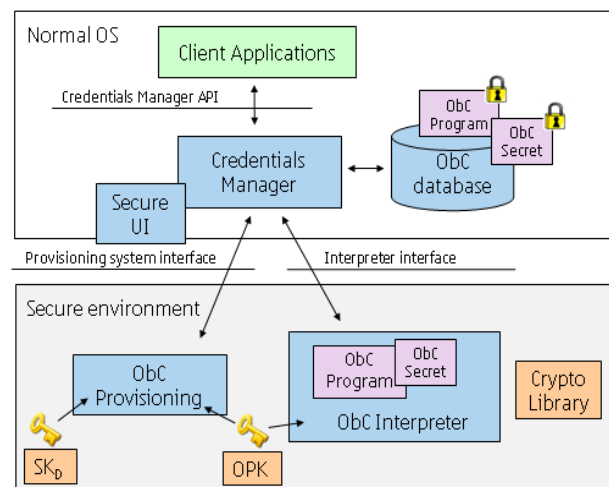


Figure 2.1: On-board Credential environment

programs and secrets that are used to encrypt the captured audio are provisioned over an encrypted channel to the cellular devices. The trusted, tamper-proof hardware in these cellular devices provides an effective mechanism to store and execute the provisioned packages in a secure environment.

3.REFERENCES

[1] Kari Kostiaainen, Jan-Erik Ekberg, N. Asokan, Arne Rantala: On-board credentials with open provisioning. [ASIACCS 2009](#): Pages 104-115.