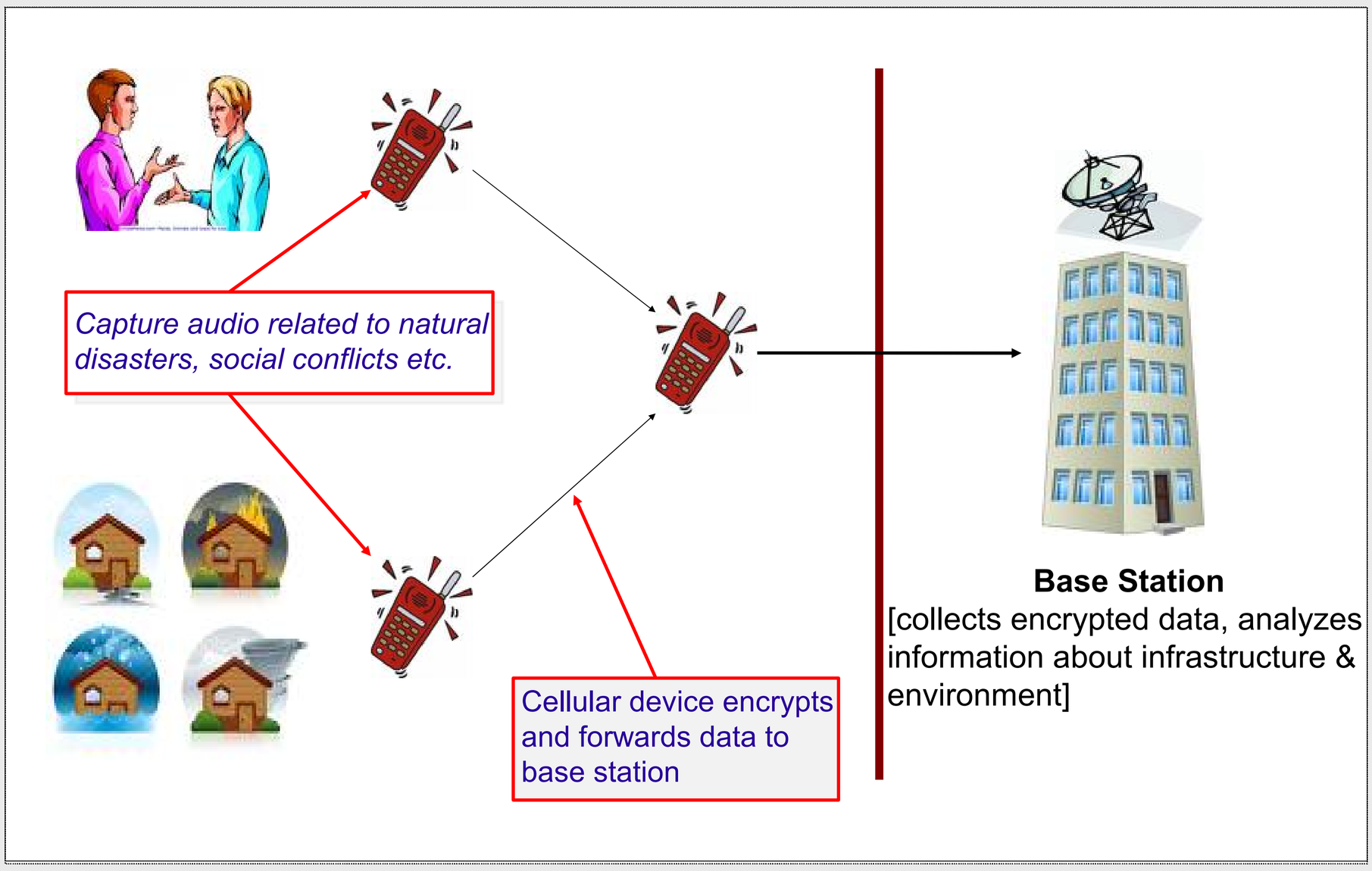
Deploying Trusted Hardware to Secure Urban Sensing

Ajay Venkateshan Krishnaprasad, Radu Sion
{ajayvk, sion}@cs.stonybrook.edu
http://crypto.cs.stonybrook.edu

NSAC
Network Security and Applied Cryptography Lab

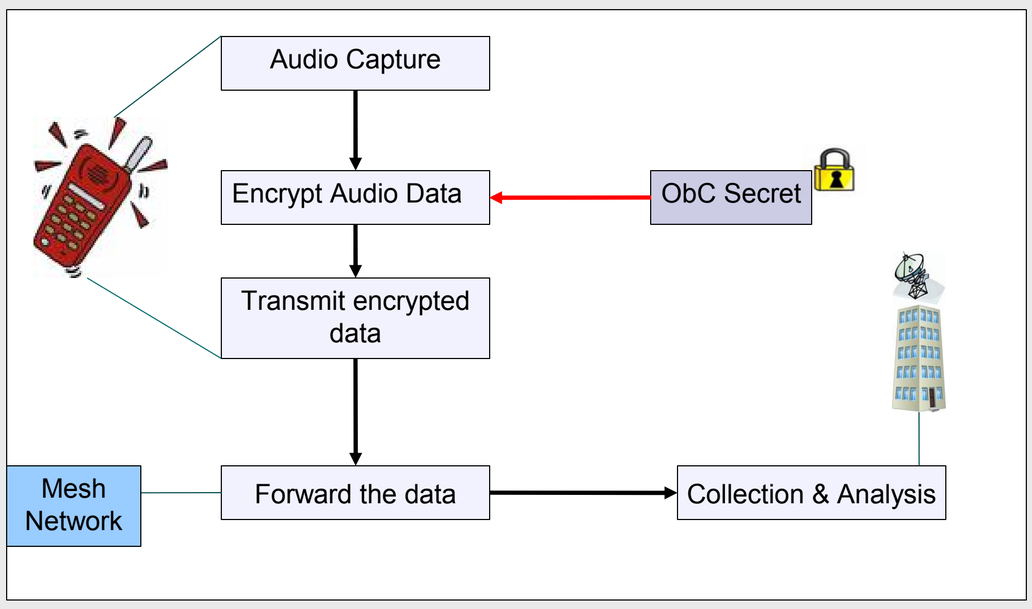
Problem: Confidentiality and Privacy in Urban Sensing.

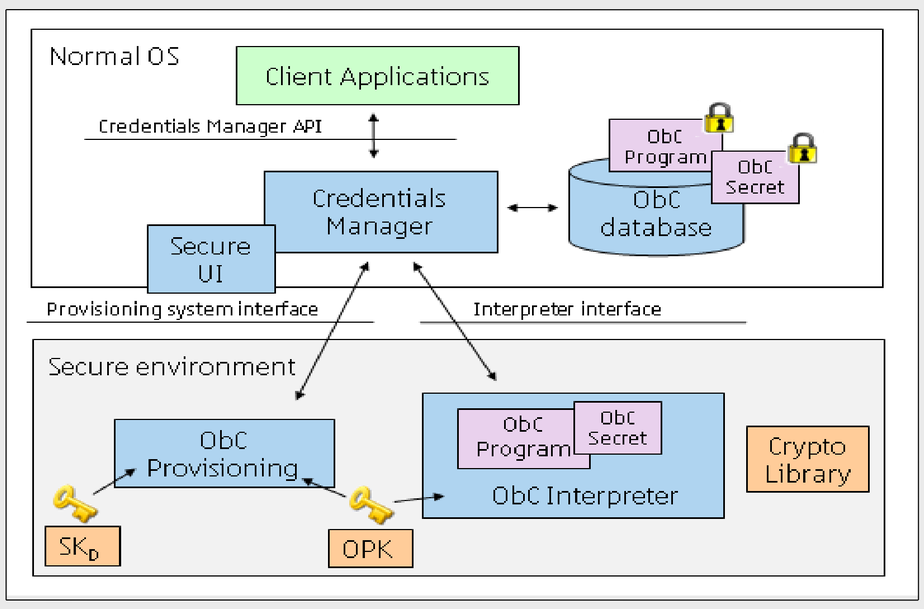
Proliferation of wireless devices with increasing capacity and accessories provides an unprecedented level of resources for the development of a system for Urban Sensing. Privacy-related issues with the use of civilian devices, as well as issues related to ensuring confidentiality of the captured data are a major concern in this setup.



Idea: Secure Hardware on Cellular Devices.

The open credential platform in Nokia cellular devices leverages on-board secure environments. The trusted, tamper-proof hardware in cellular devices provides an effective mechanism to ensure the confidentiality of the captured audio, and as well make sure that privacy is ensured.





Insight: Execution Flow

The captured audio is encrypted using the credentials stored within the secure database. The encrypted audio is then transmitted to a base station using a mesh network of cellular devices and other base stations.

Insight: Secure ObC Database

Credentials used by the client applications are stored within the secure database that is protected by tamper-proof hardware.

National Science Foundation WHERE DISCOVERIES BEGIN
NOKIA Connecting People
STONY BROOK COMPUTER SCIENCE