AcousAuth: An acoustic-based mobile Application for user authentication

Si Chen, Muyuan Li, Zhan Qin, Bingsheng Zhang, Kui Ren
Department of Computer Science and Engineering
The State University of New York at Buffalo
E-mail: {schen23, muyuanli, zhanqin, bzhang26, kuiren}@buffalo.edu.

***Abstract*—Short-range wireless communication technologies have been used in many security-sensitive smartphone applications and services such as contactless micro payment and device pairing. Typically, the data confidentiality of existing short-range communication systems relies on key-exchange then encryption mechanism, which is inefficient, especially for short communication sessions. In this work, we present AcousAuth, a smartphone empowered system designed for personal authentication. AcousAuth adopts the emerging friendly jamming technique from radio communication for data confidentiality and it features a seamless, faster, easier and safer user authentication process without the need for special infrastructure. Our system is intended to provide security assurances comparable to or greater than that of conventional authentication systems while offering the same user experience as inputing a password alone. AcousAuth provides a purely software-based solution to secure smartphone short-range communication without key agreement phase and it is potentially well suited for legacy mobile devices. Despite the computational restrictions and bandwidth of mobile device, our mobile application is able to maintain real-time performance.**

Keywords*—*Acoustic short-range communication, Security and Privacy, Smartphone wireless communication, Friendly jamming

I. Introduction

Data confidentiality of the existing short-range communication systems relies on so-called "key-exchange then encryption" mechanism, which is inefficient for short communication sessions. The state-of-the-art NFC-based short-range communication requires special hardware, i.e. NFC chips that are not common on most low-cost smartphones. Thus, we propose AcousAuth, a system that enables a seamless, faster, easier and safer user authentication process without the need for special infrastructure. Potentially, any mobile device or computer with microphone and speaker can use AcousAuth, regardless of the hardware and operating system. Our work leverages the following key insights. First, a mobile device can utilize acoustical channel to communicate directly with a cloud-based terminal automatically. Second, it is possible to provide a layered approach to security, whereby a web server can enact different policies depending on presense of the user's mobile device.

AcousAuth incorporates keyless acoustic short-range communication techniques and an intuitive user interface. To the best of our knowledge, our mobile application demonstrates the first secure acoustic-based approach chiefly on friendly jamming technique [1] for short-range communication.

With very little modification, such system can be extended to an acoustic mobile payment system. Hence, we can turn the smartphones into magnetic stripe cards. Unlike Google Wallet [2], the bank card information is only stored in the user's own smartphone instead of a third party server. Therefore, the users' private bank card information is safe as far as their smartphone is not compromised.

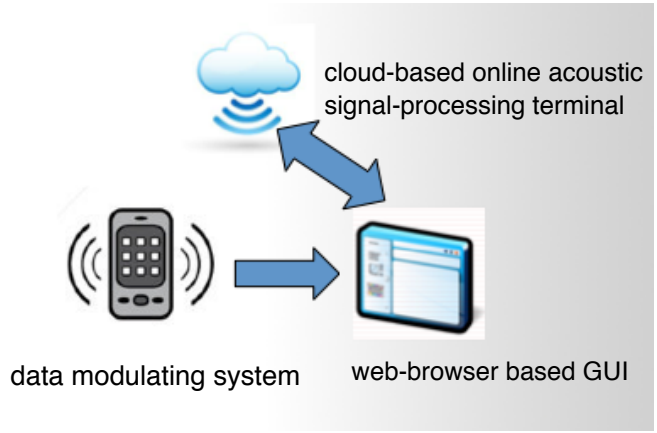

Fig. 1: AcousAuth System Architecture

Secure and Robust: AcousAuth employs a purely software-based solution to secure smartphone short-range communication without the key agreement phase. In this system, we adopt the emerging friendly jamming technique from radio communication for data confidentiality. Therefore, the authentication process is very straightforward and fast. It makes our system robust and enables the short-range personal authentication functionalities without relying on complex supporting infrastructure. AcousAuth's security has been analytically and experimentally studied in our research paper [3]. We proved that the acoustic-based short-range communication implement in this application is secure and can protect the confidentiality of the transmitted data against many passive attacks (e.g. passive blind signal segmentation attacks). Plus, our system is also naturally resistant to many active attacks, like data injection and jamming. This is due to the reason that the carrier frequencies of AcousAuth lie in the audible bandwidth, hence the short-range acoustic communication is noticeable by the users.

Cheap and Compatible: Unlike other techniques such as Bluetooth or NFC, AcousAuth only depends on cellphone's speaker and microphone to accomplish the authentication process; it does not require any additional hardware. Therefore,

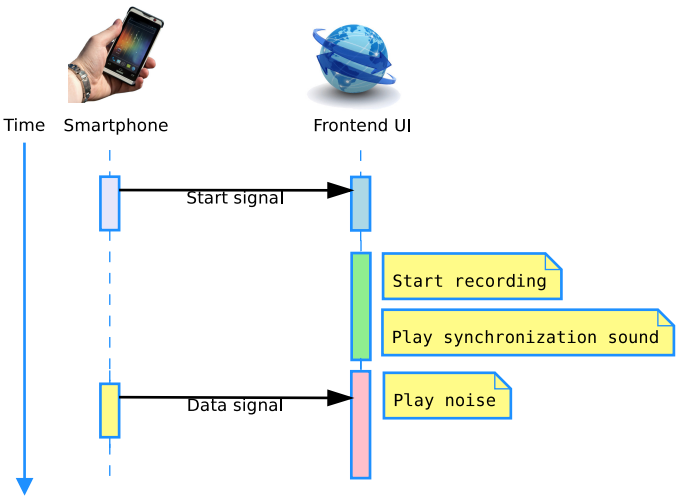

Fig. 2: Sequence Diagram

the total cost for building up this system can be greatly decreased. In addition to this, the pervasive hardware that we used in our application makes AcousAuth compatible with majority of off-the-shelf mobile devices.

Tunable and Customizable: The cloud-based architecture allows user to control AcousAuth through our incredibly simple online GUI. The tunability of this carrier frequency we used in AcousAuth creates the ability to design a customizable and tunable system.

User centric: In spite of the state-of-the-art technique that we used, our team also focuses on adding user experience enhancing features into our application. We capture and represent essential demand of users which result in building a user centric application. The prototype for demonstration is well designed and we make it visually appealing to target market.

II. System Infrastructure

A. System Architecture Overview

Our application is developed based on leading best practices in cloud based software-as- a-service (SaaS) and mobile application architecture. The system consists of three main entities (Fig. 1): a *data modulating system* running on user's smartphone, a *web-browser based graphic user interface (GUI)* running on a computer and a *cloud-based online acoustic signal-processing terminal* running on a virtual private machine (VPS).

Data modulating system is a mobile application that runs on legacy mobile devices. It is responsible to acquire user input and modulate data into acoustic signal. We employ frequency-shift keying (FSK) modulation scheme in our demonstration setup.

Web-browser based GUI is responsible for broadcasting self-jamming signal while simultaneously performing acoustic data collection from the air medium via its microphone (Fig. 3). Once finished, it pre-processed the data and upload them to the cloud. In order to achieve platform independent, we implement online GUI based on HTML5 technique, due to

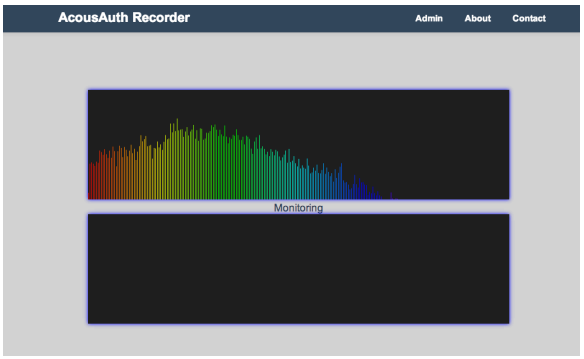

Fig. 3: AcousAuth Web-browser based Graphic User Interface

the fact that HTML5 has brought a surge of access to device hardware and its Web Audio API supports local microphone stream access and self-jamming signal broadcast.

Cloud-based online acoustic signal-processing module handles acoustic signal self-jamming and data recovery. When the mixed signal is received, this module align the noise and the mixed signal and then subtract the noise from the mixed sound track. The remaining part should only include the data signal and ambient noise with high signal to noise ratio.

B. System Workflow

At the beginning of an authentication phase, the smartphone first authenticates the user through a password or biometric based authentication scheme. Once the user is authenticated, the smartphone will sends its stored secrete to the target server using modulated acoustic signals. Fig. 2 depicts the interaction between the smartphone and the front-end UI during an authentication phase. The smartphone first sends StartSignal to the front-end UI. The front-end UI then starts recording and sends SynchronizationSignal back to the smartphone. After that, the smartphone sends the DataSignal (modulated by Whisper sender) to the front-end web based UI, and meanwhile the front-end UI is playing the jamming noise simultaneously. The front-end UI then forwards the recorded acoustic signal to the could for signal processing and authentication. Finally, the cloud server replies its decision back to the front-end UI.

Acknowledgment

This work is supported in part by the US National Science Foundation under grants CNS-1054317 and CNS-1116939, and a grant from City University of Hong Kong with Project No. 7200320. Junfei Wang, Jun Wang, Yujin Tu, and Chao Zhang have contributed to the implementation of AcousAuth systems.

References

[1] S. Goel and R. Negi, *Guaranteeing Secrecy using Artificial Noise,* IEEE Transactions on Wireless Communications, vol. 7, no. 6, pp. 21802189, 2008.

[2] Google, *Google Wallet,*, URL: http://www.google.com/wallet/ index.html, accessed: 2014-01-23.

[3] B. Zhang, Z. Qin, S. Chen, M. Li, C. Wang, and D. Ma, *PriWhisper: Enabling Keyless Secure Acoustic Communication for Smartphones*, IEEE Internet of Things Journal, 2014