Secure BLE-Based Authentication using Sensor Augmentation

Austin Freel, Andrew Titus

Massachusetts Institute of Technology
[afreel, atitus]@mit.edu

I. Introduction

Many multi-factor authentication schemes using external hardware exist, but few utilize the existing Bluetooth Low Energy (BLE) and sensor hardware on people's mobile devices. This lack of ubiquity can lead to significant "friction" in users - that is, users experience a level of frustration every time they need to use a separate device that can often lead to users opting for less secure but easier to use methods. Fortunately, most mobile devices manufactured in the past few years contain hardware that enables BLE and various sensors to be utilized for wireless communications and data collection. This leads us to propose that a "low-friction" system can be built for existing mobile hardware that guarantees the same level of security for multi-factor authentication.

II. Methodology

Many Bluetooth-enabled peripherals (including mobile devices) have the ability to support encrypted communication. We will build our system on iOS, as the operating system requires that all remote devices connected to it support encrypted pairing connections (https://support.apple.com/en-us/HT204387). We will start out by developing a pair of iOS 9 applications, one of which will function as a normal user and one of which will function as the BLE peripheral to which to send encrypted credentials. This will enable us to test the pairing and authentication processes without using external hardware for peripherals during testing. Then, we plan to replace this BLE peripheral iPhone with an external hardware device, such as the Anthill or a custom-built Bluetooth peripheral (perhaps a 6.115 project by Andrew).

The setup of the pairing connection will be done by standard Apple guidelines for connecting Bluetooth devices. Authentication methods, however, are much more flexible and wide-ranging. We will initially start with a simple one-factor authentication system, such as a username/password combination or certificate-based system. Then, we will move into multi-factor authentication schemes which are augmented by internal sensor data, such as gestures. We also hope to make the system more robust to spurious authentications by using sensor data as well. For example, in the use case of the BLE peripheral being a door lock, this would prevent users from unlocking a door if they are simply walking by it.

III. Plan and Schedule

Table 1: *Example table*

Name		
Scheisse 1	Scheisse 2	Scheisse 3
Hello 1	Hello 2	Hello 3
Hello 4	Hello 5	Hello 6

Bob Loblaw

$$e = mc^2 \tag{1}$$

Bob Loblaw

IV. Resources and Requirements

I. Subsection One

Bob Loblaw

II. Subsection Two

Bob Loblaw