FUEL: Fast, Ubiquitous, Easy-to-use, and Low-cost Authentication for Smartphones

Kaustubh Dhondge Hyungbae Park Baek-Young Choi
University of Missouri - Kansas City
{kaustubh.dhondge, hpark, choiby}@mail.umkc.edu

Sejun Song
Texas A&M University
sjsong@tamu.edu

***Abstract*—As smartphones have become highly ubiquitous, it is often used as a primary gateway for many online services that require authentication. However, the traditional authentication approach using a user id and password can be inconvenient or impossible to use in certain cases. We propose Fast, Ubiquitous, Easy-to-use, and Low-cost (FUEL) scheme for authenticating users by leveraging existing ambient light sensors on smartphones. FUEL utilizes a light sensor available on a smartphone and a low-cost hardware token in order to authenticate a user of a smartphone to unlock it or to allow access to web and cloud services. Our experiments with a prototype system validate the feasibility of FUEL in authenticating a user on a smartphone in fast and secure way. It is aimed for emergent scenarios such as solders in a battle field, and for handicapped people with fine motor control problem who have difficulty in typing in user authentication information. It can also be used as one of multi-factor authentication.**

I. Introduction

The exploding popularity of smart devices such as smartphones and tablets renders them to function as primary devices for online services. A great portion of our online activities requires authentication, let alone the access to the smart device itself. However, its small screen and keypad make it challenging for users to enter user id and password every time to access the device as well as services. It can be especially difficult or impossible to use for soldiers in a battlefield during covert surveillance missions, or for people with disorders that causes difficulty in fine motor control. It is thus important to develop authentication techniques that are fast and easy-to-use while being secure and reliable.

There are many authentication approaches available that are based on biometrics or tokens. Biometrics based authentication techniques [1], [2] rely on the uniqueness of certain physical traits in humans such as finger prints, retina, and walking patterns. Biometric based authentication techniques are however, computationally expensive, and are hard to replace once their security is compromised. Hardware tokens, on the other hand, can be easily replaced if they are lost or stolen. In token based authentication schemes [3], [4], an additional token such as a NFC chip, QR code, or magnetic keys have been used for authentication. Recently, sensor based authentication techniques [5], [6] have been proposed. They rely on the various sensor readings such as the location sensor, and orientation sensor when smartphone is in use. However, those sensor based token authentication techniques are likely need additional filtering techniques due to the sensitivity of noisy environment. Communication sensors on smartphones such as WiFi or Bluetooth tend to consume relatively high energy, require longer time due to its own authentication and can be vulnerable to snooping or jamming attack. Signal emitters of such RFs would also be relatively expensive.

In this poster, we present Fast, Ubiquitous, Easy-to-use, and Low-cost (FUEL) scheme for authenticating users on smartphones by leveraging their ambient light sensors. Not only that modern smartphones come with sophisticated light sensors, but also the light encoding and emitting devices can be designed very inexpensively as well. We have designed and built a hardware token that emits light according to a key bit string that a user has encoded for its security. The low-cost token can be carried with on a key chain or by a wrist watch, and its near contact with a smartphone can unlock it or allow access to web/cloud services in a fast and secure way. Our prototype experiments indicate that the use of ambient light sensor of smartphones is very promising.

II. FUEL Approach

The secure FUEL hardware token should be first encoded with a key bit string. We envision the token as an ultra portable token embedded in daily use objects such as key fobs and watches. Then, when a user wants to unlock the smartphone or log in to the web services, instead of entering a complex password the user has to just place the token on the surface of the smartphone where a light sensor is located. Once the secret bit sequence is relayed through the LED, and verified by the smartphone correctly, the user's authenticity is verified. The conceptual approach of our proposal is illustrated in Figure 1.

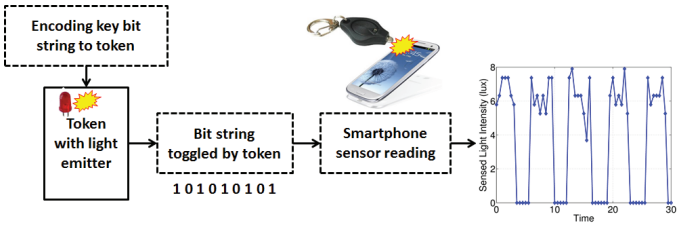
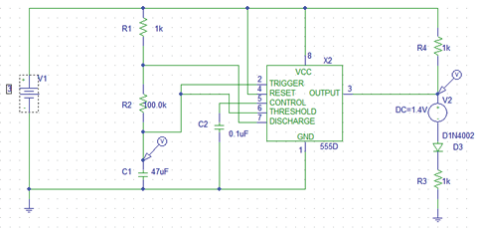
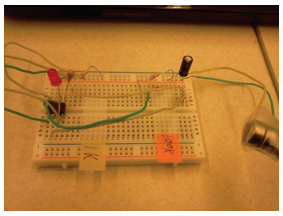


Fig. 1. Conceptual illustration

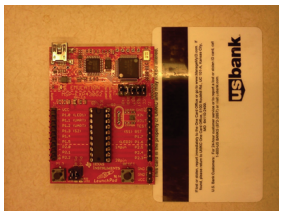
The major threats that FUEL can address include i) unauthorized access, ii) device theft, and iii) snooping. In addition to threats that are addressed by typical token based authentication



(a) Timer circuit design in PSpice



(b) Timer circuit implementation



(c) MSP430 ultra-low power microcontoller

Fig. 2. FUEL light encoder implementation

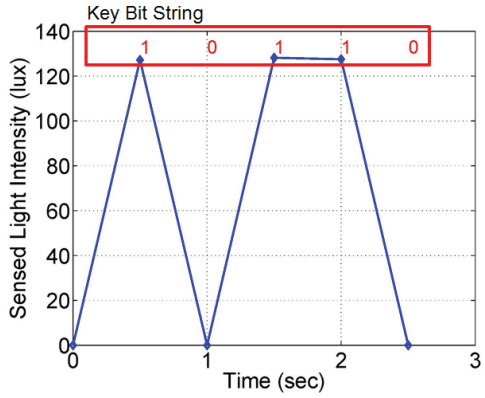


Fig. 3. Sensor readings for bit pattern 10110 from MSP430

(i) and ii)), FUEL light emissions can be done short enough bit interval that is not discernable by human eyes while still being effective for correct reading. Furthermore, the line-of-sight constraint and a guard around the token light emitter to isolate it from interference or noise offer an excellent opportunity against a snooping threat. Note that other sensors which are embedded deeper inside the smart devices can not be isolated easily in a similar fashion. For example, schemes that use magnetic sensors or microphones [3] would pick the magnetic fields and background noise that are commonly present in the environment, requiring special filtering techniques.

III. Prototype Implementation

We used Samsung Galaxy S3 and Galaxy Tab powered with Android 4.0, and employed an application AndroSensor [7] to capture the ambient light sensor readings. We have built a circuit that is capable of modulating a digital bit string as a sequence of lights toggling on and off for a controlled time interval. The time should be small enough to transfer the bit string in a short time and not to be easily detected by human eyes. We modeled the circuit in PSpice simulator shown in Figure 2 (a), and then designed a prototype model with hardware components Figure 2 (b). For a prototype implementation, we programmed the ultra-low power microcontroller MSP430 developed by Texas Instruments [8]. The MSP430 development board is smaller than a size of a credit card as shown in Figure 2 (c). The total retail price of the light encoder and emitter components were only about $4 that is by far lower cost compared to other available tokens such as RSA SecurID or VASCO Digipass. We have used its on-board LED to generate a key bit string for the prototype for this work-in-progress, but this can be packaged into a key chain or a wrist watch in practice. Figure 3 shows light sensor reading/decoding of a bit sequence of 10110, as an example. We have experimented sensor readings of a light emitting token for a bit sequence multiple times, and found that the sensor readings are very reliable (about 98%) with a sensor scan rate of 4 bps.

IV. Conclusion and Future Work

We have presented a token based authentication scheme for smartphones, called FUEL, which leverages an existing light sensor of a smartphone. We have built prototypes of a light encoder and an emitter, and our experiments indicate a high efficacy of a smartphone light sensor using an inexpensive encoder and an emitter. We plan to further evaluate FUEL efficacy with a wide range settings for bandwidth and reliability under various conditions. The proposed authentication can be used not only as a fast and easy-to-use alternative for emergent or challenging usage scenarios but also as a part of multi-factor authentication scheme.

References

[1] C. Nickle, T. Wirtl, and C. Busch, "Authentication of Smartphone Users Based on the Way They Walk Using k-NN Algorithm," in *Proc. of International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, 2012, pp. 16–20.

[2] C. Stein, C. Nickel, and C. Busch, "Fingerphoto Recognition with Smartphone Cameras," in *Proc. of International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2012, pp. 1–12.

[3] H. Bojinov and D. Boneh, "Mobile Token-Based Authentication on a Budget," in *Proc. of Workshop on Mobile Computing Systems and Applications (HotMobile)*, 2011, pp. 14–19.

[4] R. Rijswijk and J. Dijk, "Tiqr: A Novel Take on Two-Factor Authentication," in *Proc. of International Conference on Large Installation System Administration (LISA USENIX)*, 2011.

[5] T. Vu, A. Ashok, A. Baid, M. Gruteser, R. Howard, J. Lindqvist, P. Spasojevic, and J. Walling, "Demo: User Identification and Authentication with Capacitive Touch Communication," in *Proc. of International Conference on Mobile Systems, Applications, and Services*, 2012, pp. 1–12.

[6] F. Zhang, A. Kondoro, and S. Muftic, "Location-Based Authentication and Authorization Using Smart Phones," in *Proc. of International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2012, pp. 1285–1292.

[7] "AndroSensor," http://fivasim.pcriot.com/androsensor.html, 2012.

[8] "MSP430 Ultra-Low Power 16-Bit Microcontrollers," http://www.ti.com/tool/msp-exp430g2, 2012.