Mobile Token-Based Authentication on a Budget

Hristo Bojinov, Dan Boneh
Stanford University
{hristo,dabo}@cs.stanford.edu

ABSTRACT

We propose a light-weight, cheap authentication device for unlocking a user's smartphone. The device can be carried on a key chain and automatically unlocks the smartphone whenever its owner wants to use it. Our goal is to build a device that works with existing smartphones, requires no recharging or maintenance, and is always available. We propose two approaches: one based on magnetic fields detected by the smartphone's compass and the other based on an acoustic transmitter that generates a signal picked up by the handset's microphone. We experiment with both approaches and report on their effectiveness. These devices may find applications beyond smartphones, such as unlocking laptops, cars, and homes. These designs show that contactless authentication can offer a convenient and secure alternative to PIN-based unlocking.

1. INTRODUCTION

Mobile electronic devices hold increasingly sensitive or valuable information that needs to be protected. The typical protection mechanism used by smartphones or PCs is a password that the user supplies in order to unlock the system. The approach is problematic because passwords are often easy to guess, or otherwise people have a hard time remembering them [9]. What is more, passwords are difficult to enter when the dimensions of the device do not permit a standard-sized keyboard, and this is the case with all smartphones.

Practically all users are familiar with the paradigm of a physical, mechanical key. A physical key has clear security implications that everyone is trained to recognize from an early age. Motivated by the specific application to smartphones, we set out to explore the possibilities of implementing a low-cost device that can serve as an authenticator to other electronic devices, and possibly as a token that can grant access in a conventional sense, such as for entry into ones home. This kind of authenticator can have several advantages compared to traditional keys: it can be easily programmable to a new state (thus cheaper to maintain when rekeying is needed), it can be more secure, and it can combine several identities in one—removing the need to carry a physically large key chain. We aim to build an inexpensive device that can become ubiquitous; in contrast, current hardware authentication comes at a significant cost, so in the consumer space it is only marketed to online banking customers.

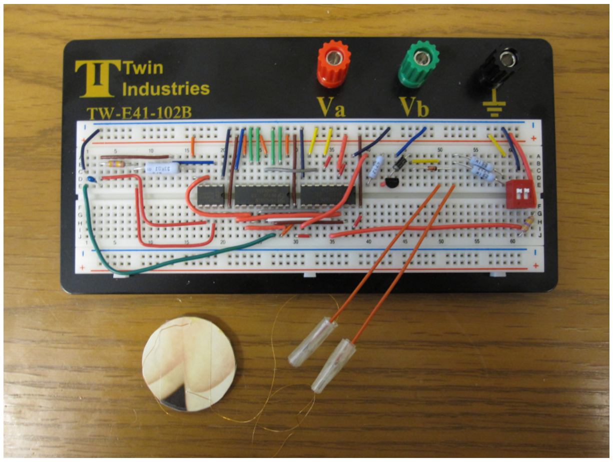


Figure 1: A photo of the working Magkey prototype. The handcrafted inductor at the bottom has a ferrite core and 300 coils of AWG 36 copper wire.

To explore the potential of our approach, we built Magkey and Mickey, simple token prototypes which can communicate either via a weak magnetic field (Figure 1), or audible sound. In the following sections we give some background information on related work (Section 2), describe our threat model (Section 3) and prototype designs for communication via a low-frequency magnetic signal (Section 4) and via sound (Section 5). We then evaluate our work with respect to security, usability, and power consumption (Section 6) and give ideas for future work (Section 7). Section 8 concludes.

2. BACKGROUND

Hardware tokens today.

There are a number of approaches to hardware token-based authentication currently in use. These range from contactless proximity cards and regular contact smartcards, to one-time PIN generators such as the RSA SecurID [8]. Common to all of these are a relatively high cost and a need to deploy a central authentication server. Some of them require high power and two-way communication, while others depend on a specific receiver design (such as a smartcard reader or an inductive coupling device). Table 1 lists some representative examples of hardware tokens in use today.

HotMobile 2011, Phoenix, Arizona

Device	Price (USD)		Power		Usability
	Token	Reader	Token	Reader	
RSA SecurID	\$50	$> \$10,000$	low	low	poor
Vasco Digipass Go	\$10	\$500	low	low	poor
Car RKE fob	\$5	\$5	low	low	average
HID Proximity	\$2	\$100	none	average	good
RFID (or NFC)	$< \$1$	\$50	none	average	good
Smartcard	\$2	\$10	none	low	poor
Magnetic stripe	$< \$1$	\$50	none	low	poor
QR (via camera)	$< \$1$	\$10	none	low	poor
Bluetooth	\$10	\$5	average	low	average

Table 1: A representative list of hardware authentication tokens, along with their salient features. Receiver (reader) power consumption is rated as "average" if the receiver powers the token.

The paradigm that we strive to emulate in this work is that of a classic key made of metal. Such a key is inexpensive to produce, requires little maintenance, is carefully guarded by its owner, and has a concrete, easily defined use: it unlocks a protected space, or a group of protected spaces. Such a device is available today: RFID tags (and the closely related passive NFC devices) cost a fraction of a dollar. The main issue with RFID is the higher cost and low availability of the reader in smartphones—a \$50 add-on SD card; car Remote Keyless Entry (RKE) fobs suffer from the same problem: no smartphone today incorporates an RKE receiver. If RFID readers become commonplace in mobile handsets, RFID may indeed become the communication technology of choice for hardware authentication. The Nexus S smartphone from Google and future iPhone models will have NFC support built-in, which implies that RFID-related technologies might become attractive for authentication purposes in the near future.

At the bottom of Table 1 we have included Bluetooth for comparison purposes. While there are currently no low-cost hardware authentication tokens based on it, we believe that Bluetooth is another one of the few alternatives to our proposals with the potential of becoming low-cost, ubiquitous, and usable for security applications—all at the same time. In fact, as the Bluetooth Low Energy specification gets implemented in the majority of smartphones and laptop computers, using Bluetooth is likely to become the best (though likely not the cheapest) route towards universal hardware authentication, allowing for sophisticated two-way protocol implementations between devices that are able to perform relatively sophisticated cryptographic operations.

Communication media.

According to our threat model, the device we construct must be able to communicate inexpensively and easily with smartphones, laptop and desktop PCs, as well as other pieces of security infrastructure. The technology used should be readily available. Table 2 lists the receivers that are available on a typical smartphone today, along with the medium they use and characteristics relevant to our work.

Note that regardless of their classification as sensors or "real" signal receivers, all of the above can be used to receive a properly modulated sequence of bits. In this work we focus on using the microphone and digital compass as receivers for the signal generated by our token. We made our choice based on ease of use and cost. On the one hand, sound and magnetic fields propagate well over short distances and do not require direct line-of-sight contact, removing the need for careful positioning during use. On the other hand, sound and magnetic fields are easily generated, transmitted, and received by simple circuitry, which makes them promising candidates for emulating a traditional key when interfacing with personal computing devices, as well as for deployment in more traditional settings such as in doorway deadbolt controllers.

Name	Medium	Comment
Microphone	Sound	audible
Radio	RF	restricted
GPS	RF	restricted
WiFi	RF	expensive
Bluetooth	RF	expensive
Compass	Magnetic	low bandwidth
Accelerometer	Mechanical	high power
Camera	Light	line of sight
Light	Light	line of sight
RFID	RF	expensive

Table 2: Receivers (sensors) typically found in modern smartphones.

Of the remaining receivers, we stay clear of the camera and ambient light sensors due to the line-of-sight requirement and difficulty in actively synthesizing images for transmission to the camera. Indeed, while QR codes can in theory be used as simple authentication tokens, they would have to be placed on the user's clothing for ease of use which would at the same time severely undermine security: almost any high-resolution photo of the user will contain enough information for an attacker to bypass the protection.

We also avoid the radio and GPS because they use restricted frequencies. The accelerometer is a poor choice because it detects the motion of the whole receiver device—making the receiver (e.g. a smartphone) vibrate requires a motor which draws considerable current. Finally, we are not interested in using WiFi or Bluetooth because of their combination of power consumption and cost of components. While Bluetooth devices are intended to be low power, the power used is still non-trivial as the protocol is too complicated for the small amounts of data we are trying to transmit. Additionally, while not too expensive, the Bluetooth stack typically costs several dollars to embed which already stretches our budget. Wider adoption of Bluetooth and advances in low energy technology [3] could eventually make Bluetooth a viable option.

Related topics.

Much work has been done on second factor authentication in the

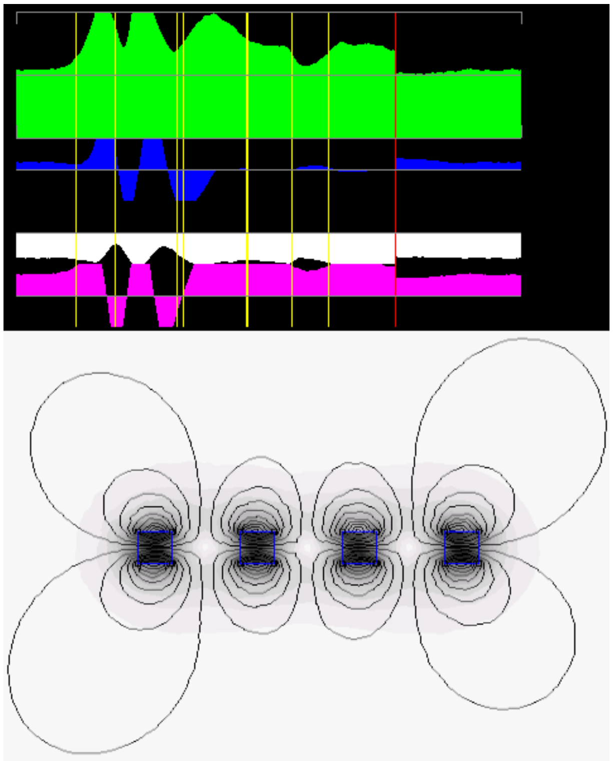


Figure 2: *Top:* Actual plot of the sensor reading from a simple NS-SN-NS-SN magnet layout. Magnets are approximately 2" apart, and the scan took about 5 sec. *Bottom:* simulated magnetic field of the same permanent magnets, with polarity aligned horizontally.

past. For the sake of brevity we will not review any variations of password authentication, such as graphical passwords [5] or multimode authentication [2]. We will also not discuss biometrics: while usable, biometric data can not be discarded, or replaced by the user and thus represents an altogether different dimension in the quest for security. In a similar fashion we will not discuss authentication by using multiple inputs such as user gait or skin resistance measurements: it is likely that smart authentication systems in the future will indeed rely on multiple factors to make application-specific access control decisions—while receiving a phone call or making an emergency call might require a minimum amount of authentication, access to email or calendar applications could trigger rigorous authentication involving hardware tokens and PIN entry.

3. THREAT MODEL

Our primary goal is to build low-cost hardware tokens which consume small amounts of power. The major threats that we are trying to address are:

- **Device theft.** We want to prevent unauthorized persons from using a device after it has been lost or stolen.
- **Unauthorized access.** We want to protect infrastructure (electronic devices, offices, buildings) from unauthorized access.

We explicitly leave snooping attacks on the authentication channel out of scope. Such attacks can be thwarted by extending the hardware token to emit unique, time-dependent authentication codes.

We also do not directly address how data is protected inside a smartphone. The authentication key can serve as a simple password that unlocks the device, or possibly for deriving a key that protects all data on it. These are design choices that should be made outside the scope of this work.

4. MAGNETIC TOKEN

Our initial idea was to use a fixed arrangement of permanent magnets in order to encode a number which can be "scanned" by the smartphone's digital compass. We could use the orientation of permanent magnets in our encoding, similar to the way this is done in credit card magnetic strips. Figure 2 shows the detected signal versus the simulated magnetic field of such an arrangement. A reliable reading can only be obtained with a generous spacing of the magnets and a careful, uniform swiping movement.

While this encoding works well for credit cards, using a spatial layout proves to be unreliable when scanning by casually moving the phone over the token. The problem stems from the low default resolution of magnetic sensors, as well as the relatively large distance from the sensor to the magnets (e.g. 20mm or more).

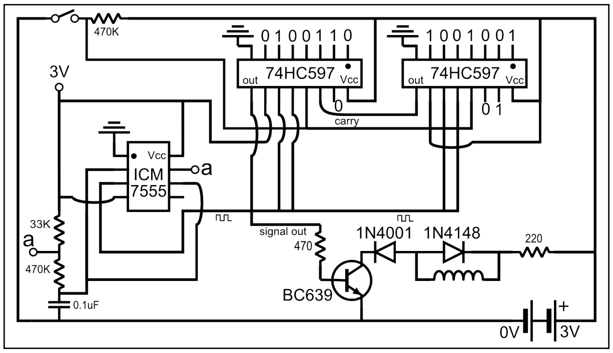


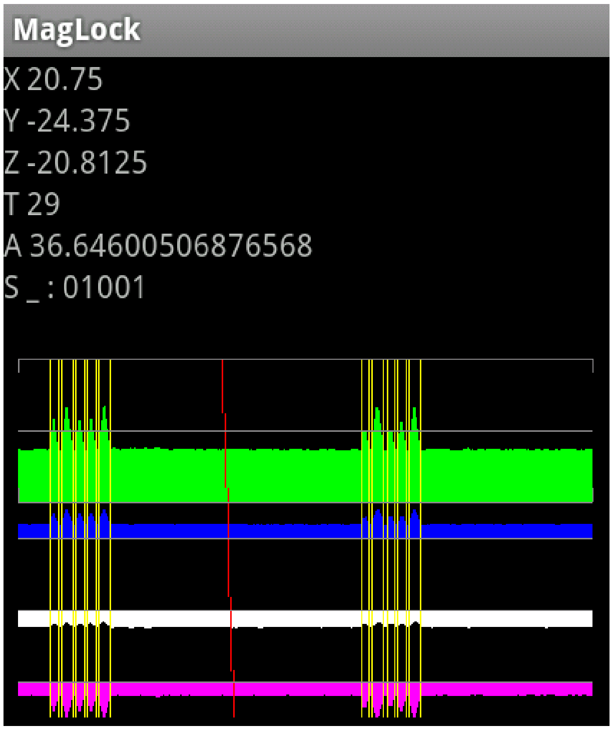
Figure 3: An active circuit which transmits a sequence of bits as the presence or absence of a magnetic field. The field created is comparable in strength to the Earth's magnetic field, which is on the order of 30uT. The sequence of bits transmitted encodes the number "01001". A zero is encoded as a small pulse, and a one is encoded as a pulse that is twice as long. The 0.1uF capacitor results in a transmission rate of about 10 baud, or about 3 bits/s with the above encoding. Better encoding and modulation mechanisms can result in a higher bit rate.

Magkey: using time-based encoding.

After a passive arrangement of magnets proved infeasible, we built an active circuit that is able to modulate a digital signal as a sequence of changes in the magnetic field created by the current in a small inductor (Figure 3).

The only part that is not readily available on the market is the inductor itself. We built it using an inexpensive ferrite disk as the core, and coiled 300 turns of AWG 36 enameled copper wire, which is rated for a maximum current of 36mA. Our estimates were that the resulting inductor will create a field of at least 10uT at a distance of about 2cm, even when slightly off-center. Our experiment proved that the estimate was correct, and moreover, that a properly placed smartphone can get an excellent reading of the signal transmitted.

When we use time-based encoding, we can obtain a much more reliable "scan" by the smartphone (Figure 4). Our experiments in-



```
MagLock
X 20.75
Y -24.375
Z -20.8125
T 29
A 36.64600506876568
S _ : 01001
```

Figure 4: The MagLock application receives the Magkey signal and decodes it to the intended string of bits "01001". The first pulse in a transmission always corresponds to a zero, and is used to calibrate the decoder.

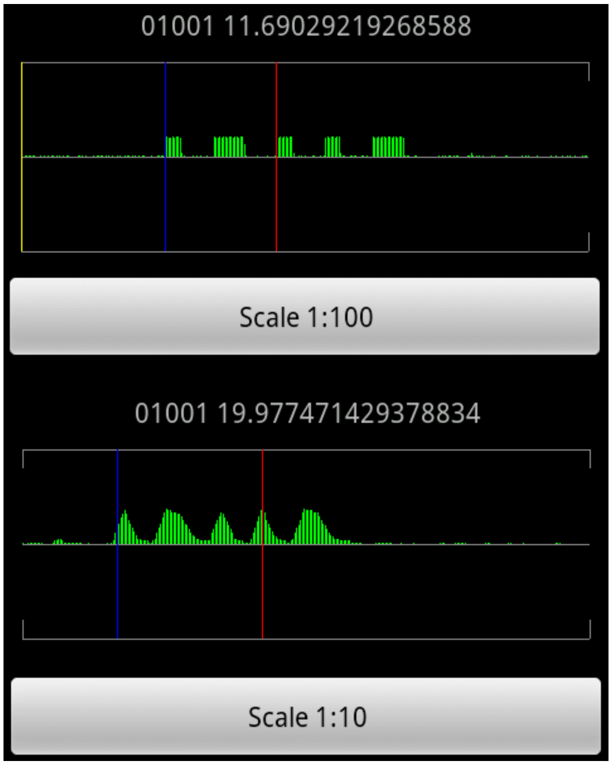
volved two Android phones, a Nexus One and a Motorola Droid. The Nexus uses a 30Hz sampling frequency, while the Droid is configured for 10Hz. As a consequence, even a 0.2uF capacitor version of the circuit results in an encoding that is too fast for the Droid to process, making a larger 0.47uF capacitor necessary.

Clearly this approach is extensible to transmitting more bits, as well as using more exotic encoding schemes to achieve better utilization of the channel. While the Nexus One sensor can support a sampling rate of at most 80Hz (confirmed by the chip datasheet as well as experimentally), Hall effect sensors on the market are rated to provide on the order of 1000 readings per second, which would offer 30 times higher bandwidth than what smartphones are currently tuned to deliver. With better sensors and appropriate modifications to the encoding scheme, bandwidth in excess of 300 bits per second should be achievable. For reference, the entropy of a typical user password is between 20 and 40 bits [4].

5. ACOUSTIC TOKEN

Due to its higher sampling frequency, the microphone offers higher communication bandwidth, at lower power consumption compared to the digital compass. Figure 5 shows a signal transmitted by our experimental setup from Figure 6, which uses a piezoelectric buzzer. In all cases the carrier frequency is audible at about 1480Hz, and simple amplitude-shift keying (ASK) is used as the modulation technique. On the receiver device (the smartphone), we first isolate the carrier frequency, then perform a decoding similar to the one we used with the magnetic sensor. The signal shown is after isolating carrier frequency and performing some smoothing.

Conceivably, the transmission could use more sophisticated modulation to achieve higher bandwidth (or shorter transmission times). For example, modulation used by now antiquated telephone line modems can be adapted to this context.



```
01001 11.69029219268588
```

```
01001 19.977471429378834
```

Figure 5: The bits "01001" transmitted as audible sound, and decoded on a Nexus One phone. *At the top,* transmitted over the course of 1 second, comprising about 10K samples; *at the bottom,* transmitted over 0.1 second, or 1K samples (using a 10nF capacitor).

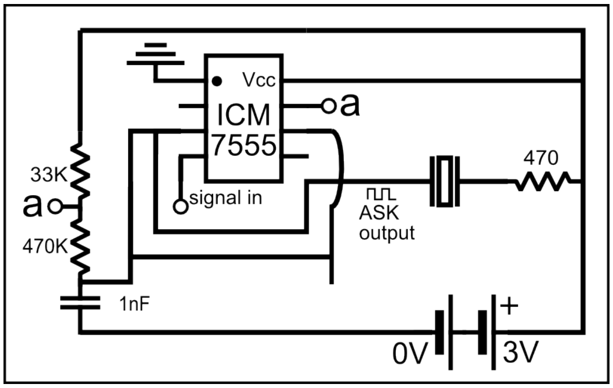


Figure 6: The 7555 timer-based add-on circuit for ASK modulation over sound. The signal input comes from the shift register output in Figure 3, and the modulated signal is directly connected to the piezoelectric buzzer as the current drawn is very low (thus a transistor is not needed in this version of the token). The 1nF capacitor used results in a carrier frequency of 1480Hz.

	Current		CR2450 (600mAh)		CR123A (1500mAh)	
Device	Average	Peak	On-demand	Continuous	On-demand	Continuous
Magnetic	6.91mA	16.00mA	*current too high*		$>$ 5 years	210h
Sound	0.23mA	0.25mA	$>$ 10 years	2600h	$>$ 10 years	6500h

Table 3: Current drawn by our prototypes, and estimated time between battery replacement. Note that a battery's shelf life, typically about 10 years, will in some cases be shorter than the estimated time it takes a circuit to drain the battery.

6. EVALUATION

Security.

Our token can be used for authenticating the user to smartphones: either continuously, or when access to the device is required—in addition to or instead of entering a password. For access to remote services, a PIN can be transmitted on demand. The client program running on the smartphone or PC can use this PIN for authenticating the user.

Usability.

A perfect authentication token would work transparently, without any need of interaction with the user. This goal can be achieved only by an active token which emits authentication signals continuously. Acoustic tokens appear the more promising in this respect due to their low power requirements. Allowing for a simple interaction, such as the pushing of a button, opens up the possibility to use a wider variety of approaches. In addition, user interaction will make it possible to store multiple identities in the token, invoking them as needed. For example the token can periodically unlock the phone by default, but switch to an altogether different unlock sequence by the push of a button—perhaps in order to unlock the user's home.

Using magnetic fields.

Static magnetic fields differ from electromagnetic (EM) waves in their sharp drop-off, proportional to the fourth power of the distance from the source [7]. This is explained by the fact that every magnet is a dipole, and the field connects the two poles, rather than radiate in space like a EM or sound wave. Strictly speaking, our token emits EM waves as well by virtue of varying the magnetic field around the inductor; these EM waves have such a low frequency however that their power, proportional to the frequency, is negligible.

While the sharp drop in the strength of the magnetic field created makes a magnetic token harder to use (proximity is essential), it also makes the token less prone to snooping, as an attacker would have to be close by in order to detect and record a transmission.

Using sound.

By using the phone's microphone as a receiver, we achieved acceptable bandwidth. We were pleasantly surprised by the low power required to generate sound waves using a piezoelectric buzzer. Table 3 summarizes the current drawn by the two circuits, and estimates how long the tokens can operate when powered by two different battery sources (a coin cell vs. camera battery), and in two modes: continuous and on-demand. On-demand use assumes 20 authentications per day, taking up a total of 5 minutes of continuous transmission (a very conservative estimate).

Cost of the token.

Table 4 compares the cost of materials for each of the hardware token designs. Using sound instead of a magnetic field adds a little to the cost of the device, however it significantly increases the available bandwidth and lowers the current drawn by the circuit. A hardware token meant for actual use should also carry a significantly larger PIN—on the order of 128 bits—and thus it may be most practical to switch to using a small microcontroller such as PIC10F200; this would replace the timer and shift registers with a single programmable 8-pin IC and reduce the cost significantly.

	Cost (USD)		
Type	Unit	Magkey	Mickey
Timer IC	\$0.20	\$0.20	\$0.40
Shift Register IC	\$0.25	\$0.50	\$0.50
Transistor	\$0.15	\$0.15	
Diode	\$0.01	\$0.02	
Capacitor	\$0.05	\$0.05	\$0.10
Resistor	\$0.01	\$0.05	\$0.08
Inductor (Coil)	\$0.10	\$0.10	
Piezo Buzzer	\$0.20		\$0.20
PIC IC	\$0.38		
Total		\$1.07	\$1.28
Total (using PIC)		\$0.75	\$0.96

Table 4: Components and costs of the two hardware token designs. We are not including the cost of the circuit boards, wiring, batteries, and assembly.

7. FUTURE WORK

Optimizing channel use.

Our prototype implementation is far from optimal when it comes to the throughput it achieves given a particular medium. On the one hand, a better encoding could yield better utilization. On the other hand, bandwidth can be increased by modifying the receiver to offer a higher sampling rate: from our experience, this is particularly applicable to the digital compass.

Along the same lines of achieving higher throughput, it is likely that smartphone microphones can be tuned or upgraded to receive ultrasound (and sample at an accordingly higher rate), which opens up the opportunity to transmit data over ultrasound; as a beneficial side effect, using ultrasound will make the transmission inaudible, and thus less obnoxious. Note that some TV remote controls in the past used sound before switching to infrared communication [1].

Protection against replay attacks.

So far we have ignored the threat of an attacker capturing the transmission and replaying it to gain unauthorized entry. Indeed our model device, the physical key, is easy to copy and replicate. With active authentication tokens we have an opportunity to fix this problem [6]. Exploring both challenge-based and single-packet protocols in this context would be a desirable extension of our prototype, especially if it can be accomplished inexpensively[1].

One idea for implementing replay attack protection is to follow a model similar to that used in automotive keyless entry systems. A secret number (a "seed") is used to create an unpredictable sequence of numbers that is used for authentication. The receiver allows a window of such numbers, from S_i to S_{i+W}, to be used for unlocking the asset, and upon unlock via S_{i+q} $(0 \leq q < W)$ resets the window to span S_{i+q+1} to $S_{i+q+W+1}$. An even more secure approach involves challenge-based authentication, which requires two-way communication.

Using unpredictable number sequences will also have the advantage of making device cloning difficult, requiring access to the secret internal state of the device. Device rekeying will remain straight-forward: the device can implement an interface through which one or more of its identities can be completely replaced by installing a new seed secret.

Usable passive tokens.

We have not given up on the idea of creating passive authentication tokens: their advantages include lower cost to manufacture and operate (no need for a battery). We have identified a group of transmission mechanisms that we would like to explore in the future. The ideas for smartphone reception presented in this paper can be relatively easily adapted to such alternative transmission mechanisms:

- **Using a mechanical "clicker" as the sound generator.** Instead of an active circuit generating sound signals, the user can use a device which generates a specific sound pattern when clicked mechanically (similar to many children's toys, for example).

- **Using a mechanical system of magnets that generates a certain pattern in time and space.** This is similar to the previous idea of effectively a user-powered mechanical token, this time using magnets rather than sound.

- **Using a key which is run across the surface of the smartphone to create a vibration.** This is a human-powered transmission that can be "read" via the device's accelerometer. Such a key might be usable in conventional settings, by embedding an accelerometer in a door—the advantage over traditional keys is that such a lock will be highly pick-resistant.

- **Harvesting energy from key presses to create a battery-free active token.** While the resulting device will not be passive, it will compete with passive devices in longevity while providing the flexibility of being programmable, possibly combining the best of both worlds.

8. CONCLUSION

We have explored the possibilities for building inexpensive hardware authentication tokens that are suitable for use with smartphones, as well as laptop and desktop computers and other security infrastructure including conventional doorways. The tokens we proposed can be built in volume for about US$0.75 each and can authenticate to existing smartphones. Under normal use they run for a decade when powered by a small 3V battery. We have identified several promising directions for future work in the area.

[1] Implementing such a feature may increase the cost of the token a little due to the use of a larger microcontroller chip capable of performing hash computations.

9. REFERENCES

[1] Adler, robert (austrian-born american inventor). `http://en.wikipedia.org/wiki/Robert_Adler`.

[2] K. Bailey, A. Kapadia, L. Vongsathorn, and S. W. Smith. Twokind authentication: protecting private information in untrustworthy environments. In *WPES '08: Proceedings of the 7th ACM workshop on Privacy in the electronic society*, pages 39–44, New York, NY, USA, 2008. ACM.

[3] Bluetooth low energy technology. `http://www.bluetooth.com/English/products/pages/bluetooth_low_energy_technology__technical_info.aspx`.

[4] D. E. Burr, D. F. Dodson, and W. T. Polk. Electronic authentication guideline. Technical report, National Institute of Standards and Technology, April 2006.

[5] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin. The design and analysis of graphical passwords. In *Proc. 8th USENIX Security Symposium*, pages 135–150, 1999.

[6] D. Malan. Crypto for tiny objects. Technical report, Harvard University, 2004.

[7] Z. Popovic and B. Popovic. *Introductory Electromagnetics*. Prentice Hall, 1999.

[8] Rsa securid. `http://www.rsa.com/node.aspx?id=1156`.

[9] J. Yan, A. Blackwell, R. Anderson, and A. Grant. Password memorability and security: Empirical results. *IEEE Security and Privacy magazine*, 2(5):25–31, 2004.