Authentication Technologies for the Blind or Visually Impaired

Nitesh Saxena
Computer Science and Engineering
Polytechnic Institute of New York University

James H. Watt
Communication Sciences
University of Connecticut

Abstract

Current research on "Usable Security" is still in its infancy and usable security solutions are often designed without paying attention to human disabilities. This paper aims to help fill this void in the realm of blind computer users. More specifically, we discuss research challenges we are faced with and the directions we can take towards developing authentication technologies suitable for the blind or visually impaired. Our focus is on two technologies: *user authentication*, i.e., how a blind user can securely authenticate to a device (remote or otherwise) and *device authentication*, i.e., how a blind user can securely establish private and authenticated communication between two wireless devices. We hope that our work would inspire other researchers to design security solutions keeping in mind not only human abilities but also their disabilities.

1 Introduction

Modern users heavily rely on their computing devices and constant networked access. This computing and technological revolution also growingly involves users with various disabilities. In fact, computing and networked devices have increasingly been becoming an indispensable part of the lives of the disabled. Unfortunately, with computer usage arise various security risks. Security of computer systems often relies on actions or decisions taken by the end users. For example, a user is asked to pick long and "hard-to-guess" passwords, expected to distinguish between a real and phishing web-site [4], timely install security patches, pay attention to security warnings and so on. Although an able and a healthy computer user might be successfully able to manage various security related tasks, disabled users, especially those with with significant vision impairments, might not be able to do so. Thus, it is our conjecture that blind or visually impaired users are usually at a higher risk of various security vulnerabilities and attacks.[1]

Unfortunately, current research on "Usable Security" is still in its infancy and usable security solutions are often designed without paying attention to human disabilities. Proposed solutions are thus not necessarily usable by the disabled, and extending existing work to support human disabilities presents unique challenges. A higher level goal of this paper is to help fill this void in the realm of blind computer users. More specifically, we discuss research challenges in developing authentication technologies suitable for the blind or visually impaired. Our focus is on two technologies: *user authentication* and *device authentication*.

User(-to-Device) Authentication. User authentication is a classical problem in computer and information security. The problem occurs whenever a user, wanting access to a computing device (remote or otherwise), has to prove to the device her possession of certain credential(s), that she has pre-established with that device. The primary goal of user authentication is to ascertain that only a legitimate user, possessing appropriate credentials, is granted access. In other words, any entity not in possession of appropriate credentials, must not be able to impersonate a legitimate user.

ASCII password and PIN mechanisms are the dominant means of authentication used today, ranging from authentication to remote servers and automated teller machines to mobile phones. However, to be usable, passwords need to be easy to memorize, which leads to "weak" choices in practice. For example, users often tend to choose short and "low-entropy" passwords, enabling dictionary attacks and brute-forcing attempts, or they write passwords down or use the same password at multiple sites. Passwords are also susceptible to a variety of eavesdropping or observation attacks (e.g., shoulder-surfing, keylogging, videotaping) and social engineering trickeries (e.g. phishing).

Research Challenges: The research on user authentication has failed to address an important aspect of human disabilities. We argue that currently used password- or PIN-based authentication methods when used by blind or visually impaired people, are highly vulnerable to various observation attacks, more so than they are when used by people with no vision impairments. In such attacks, an attacker can eavesdrop on the password/PIN typed by the user using hidden cameras, key-loggers or simply by shoulder-surfing or peeping. Since it is very difficult for a blind person to detect the presence of hidden cameras or key-loggers

[1] A recent attack on *JAWS 9.0* [26], a very useful and popular screen reader software among blind computer users, serves as an example to illustrate an alarming fact that computer attackers would not be reluctant to target the blind and disabled user population.

near/on the authentication terminals or to gauge the existence of a nearby shoulder-surfer, such attacks are perhaps quite easy to launch. The blind users are also more vulnerable to various phishing attacks, as detection of such attacks often requires the user to heed to *visual* indicators (e.g., the SiteKey images used by BankofAmerica.com). In Section 2, we put forward various possible approaches to address these challenges.

Device(-to-Device) Authentication. Medium- and short-range wireless communication – based on technologies such as Bluetooth and WiFi – is increasingly popular. There are many current everyday usage scenarios where two devices need to "work together," e.g., a Bluetooth headset and a cellphone, or a wireless access point and a laptop.

The surge in popularity of wireless devices brings about various security risks. The wireless communication channel is easy to eavesdrop upon and to manipulate, raising the very real threats, notably, of so-called *Man-in-the-Middle* (MitM) attacks. Therefore, it is important to secure this channel. However, secure (i.e., authenticated and private) communication must be first bootstrapped, i.e., the devices must be securely paired or initialized. (We use the term "pairing" to refer to the bootstrapping of secure communication, which covers device-to-device authentication).

One of the main challenges in secure device pairing is that, due to sheer diversity of devices and lack of standards, no global security infrastructure exists today and none is likely for the foreseeable future. Consequently, traditional cryptographic means (such as authenticated key exchange protocols) are unsuitable, since unfamiliar devices have no prior security context and no common point of trust. Moreover, the use of a common wireless channel is insufficient to establish a secure context, since such channels are not perceivable by the human user. The research community has already recognized that some form of human involvement is perhaps necessary to address the problem of secure device pairing.

One promising and well-established research direction is the use of an auxiliary channel, called an "out-of-band" (OOB) channel, which is both perceivable and manageable by the human user operating the devices. An OOB channel takes advantage of human sensory capabilities to authenticate human-imperceptible (and hence subject to MitM attacks) information exchanged over the wireless channel. OOB examples include audio, visual and tactile senses as a means of transmitting and/or or verifying information. Unlike the wireless channel, it is assumed that the attacker can not remain undetected if it interferes with the OOB channel (although it can still eavesdrop).[2]

Research Challenges: Although prior work on device pairing addresses a challenging problem of "interface-constrained devices," another important and somewhat analogous issue of human constraints, i.e., disabilities, has not been given any attention so far. In particular, a number of existing pairing methods are based on *visual* OOB channels and are thus not suitable for people who are blind or visually impaired. In addition, we believe that pairing methods which are based on auditory channels are also not suitable for the blind or visually impaired. This is because these methods are potentially vulnerable to a nearby "hidden" attacker device who can impersonate the source of the audio and thus successfully execute an MitM attack (we call this the "Fake-Audio" attack). In Section 3, we discuss our research agenda to address the problem of device authentication for the blind computer users.

2 User Authentication

We first discuss a technique for observation-resilient authentication based on short PINs (suitable for an ATM transaction or debit card purchase at retail stores). Next, we explore the use of mobile phone for strong as well as observation-resilient authentication to remote web-sites (without any server side modifications). Since they tend to be in constant possession of their mobile phones, the proposed approach is quite suitable for blind users.

2.1 Observation-Resilient Authentication using Short PINs

The threat of observation attacks has long been recognized. Many proposals require the user to perform some form of a cognitive task – so called *cognitive authentication schemes*. The problem of designing a cognitive PIN-entry method secure against eavesdroppers is truly challenging. Indeed, it was recently shown in [6] that the cognitive scheme proposed in [30] and all its variants are fundamentally vulnerable to attacks based on SAT solver. Another cognitive PIN-entry scheme [21] can also be broken by a variant of the SAT solver attack. Finally, it is an open question if there exists a PIN-entry scheme resistant against active attacks [9] (one against a MitM attacker).

We can divide existing PIN-entry methods roughly in two classes regarding information available to an adversary: (1) the adversary *fully observes* the entire input and output of a PIN-entry procedure, and (2) the adversary can only *partially observe* the input and/or output. For example, the PIN-entry method [9] belongs to the first class (*fully observable*). In this method all information exchanged between the user and the interrogator is available to the adversary. Unfortunately, this fact significantly increases the amount of cognitive effort for the user.

We consider the weaker partially observing adversary. The design choice to include the protected channel in our proposed technique is motivated by the following observations about the methods from the first class (the "fully observable" model). Firstly, designing secure cognitive PIN-

[2] Pairing based on password-authenticated key exchange requires secrecy as well as authenticity of OOB channels. This approach is susceptible to observation attacks and thus not suitable for the blind.

entry schemes in the fully observable model is challenging as shown by the SAT-solver based attacks. Secondly, secure PIN-entry schemes from this model involve multiple rounds of a basic challenge-response protocol and they require users to perform complicated mathematical calculations [9], which is a major deterrent to the acceptance of such technology (an average authentication time of about 166 seconds using the scheme of [9]).

Kuber and Yu [17] and Sasamoto et. al. [22] proposed PIN-entry methods secure against a partially-observing adversary. These methods use a tactile channel as a secure hidden challenge channel. In the first solution, the user is given a sequence of tactons to remember. To authenticate, the user rolls with a mouse over nine blank squares on the display causing an unique pattern appear under fingerprints. In the second solution, the user simultaneously receives a visual challenge and a hidden tactile challenge via a protected channel. To authenticate, the user has to answer correctly to several challenges. One of the drawbacks of above solutions is that they require non-standard (potentially hard to use) hardware.

On the contrary, the PIN-entry scheme that we propose to explore is quite simple and require minimal hardware (e.g., ear-phones). Basically, it implements the *one-time pad* paradigm. To enter a single digit of a (random) secret PIN, a user first receives a challenge c_i (a random number between 0 and 9) from an interrogator (e.g., ATM) over a protected channel, i.e., which ensures secrecy and integrity (e.g., via earphones). Next, the user simply has to perform a modulo 10 addition of c_i with the corresponding PIN digit p_i, such that the entered value is $(c_i + d_i) \bmod 10$. As long as the protected channel remains hidden from an attacker, our scheme offers perfect security (just like one-time pad). In other words, the only possibility for an attacker to learn the PIN is equivalent to a random guess. We call our method Mod 10 PIN-entry.[3]

One research task is to study the Mod 10 PIN-entry method in more detail. This includes investigating the secrecy properties of a hidden channel (e.g., based on earphones). We note that the adversary could try to use a parabolic reflector to collect sound energy produced by ear-phones. This threat can be mitigated by reducing sufficiently the volume level of an audio challenge. More advanced protection would involve sound and noise reduction techniques. In-ear monitors are a passive counterpart to active noise canceling headphones [8]. They offer portability similar to earbuds, and also act as earplugs to block out environmental noise. According to [1], canalphones may reach isolation levels of -30dB to -40dB, which implies a lower sound level of an audio challenge. Laser beam eavesdropping [12] is another potential threat. Canalpohones can mitigate this threat too.

Another obvious research task would be to implement the Mod 10 method and test it with a sample of blind users. We hypothesize that our method would be reasonably efficient, robust to errors and usable, since modulo 10 is a simple computation that most blind users (who are math-literate) should be able to perform without much mental strain.

2.2 Strong and Observation-Resistant Authentication Using a Mobile Phone

Motivated by the indispensability of mobile phones for blind users, we propose a generic approach of strong as well as observation-resistant authentication. We believe that a mobile phone can significantly aid blind users in achieving strong and universally applicable authentication.

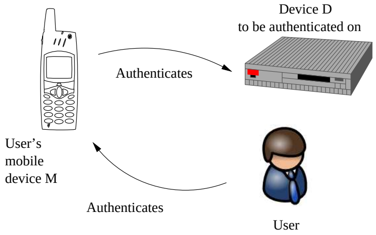

Figure 1: Proxy-based Strong Authentication Approach (ideally, biometrics, e.g., voice-recognition, can be used for strong user-to-phone authentication; phone-to-device (cryptographic) authentication can take place via a challenge-response protocol over Bluetooth, e.g.

In what we call a proxy-based authentication approach (shown in Figure 1), the mobile phone is used as an authentication proxy between the user and the device the user intends to authenticate to (a local terminal or a remote server).[4] First, the user authenticates to the phone, and the phone in turn authenticates to the device. In other words, the phone acts as a "master key" that allows to *strongly* authenticate to different services. The advantage of this approach is that it reduces the authentication problem to authentication on a small, portable device, which has inherent benefits. One advantage is that strong authentication on phones can be achieved relatively easily, e.g., using biometrics suitable for the blind (e.g., voice authentication or fingerprints). In addition, shoulder surfing can be made considerably more difficult on a phone screen, due to the compact form factor, and the availability of very cheap, yet effective, optical filters. Moreover, a single interface can be used for different authentication services. At the same time, the cryptographic challenge-response authentication phase (which is resistant to any eavesdropping) between

[3] We recently investigated the usability of this method in the context of people with no vision impairments [14]

[4] Our approach can also be viewed as a novel, observation-resilient way of portable password management. Note that existing portable managers (e.g., KeePassMobile [19]) are not observation-resilient as they simply have the user type in a password displayed on the portable device onto the terminal.

the phone and the device can be made fairly automated and transparent to the user, and in particular, does not have any usability constraints.[5]

In order to address the specific problem of phishing [4], our approach can be easily integrated with PwdHash approach of [20]. Note that since our passwords are strong, a phishing site that learns the hash of a password, can not mount a dictionary attack on it. In case of temporary unavailability or permanent loss (or theft) of the mobile phone, traditional "fall-back" authentication methods, based on secret questions, are applicable [18].

In scenarios where an in-band channel does not exist (e.g., the phone or terminal might not have a Bluetooth interface), an out-of-band (OOB) bidirectional audio channel can be used for communication. However, an audio channel would typically not be as fast as the in-band channel and likely have some human annoyance factor, thus undermining usability. To remedy this, a natural direction is to focus on designing tactile channels, e.g., by utilizing the vibration capabilities of the mobile phone. Since vibration is more or less a universal interface on mobile phones and vibration, if not accompanied with audio or electromagnetic radiations, can only be perceived by the user in physical contact with the device, we believe focusing on tactile channels is a promising direction. Our proposed channel requires a phone with a vibration capability and a terminal with an accelerometer The vibration is used to encode the data to be transmitted (strong password in our case). The user is simply required to "touch" her vibrating phone with the terminal. The accelerometer on the terminal senses the vibrations, thereby decoding the data. Since this is an automated channel, data transmission can take place quite efficiently.

3 Device Authentication

We first provide some background and discuss the prior work on device pairing in the realm of people with vision loss, and then put forward our research agenda on the topic.

3.1 Applicability of Prior Pairing Methods for the Blind

A number of pairing protocols that use OOB channels have been proposed. Earlier protocols [3] required between 80 and 160 bits to be transmitted over the OOB channel. The more recent, so-called SAS- (Short Authenticated Strings) based protocols [10] [13] reduce the OOB bandwidth to about 15 bits, while still attaining reasonable security.

Based on the above protocols, a number of pairing methods have been proposed that use various OOB channels and offer varying degrees of usability. We summarize most relevant methods in the following (for a more detailed description, refer to [16]).

Infrared Transfer: Balfanz, et al. [3] proposed a method using the infrared (IR) as the d2d channel: devices communicate their public keys over the wireless channel and then exchange (at least 80-bits long) hashes of their respective public keys over infrared. The main drawback is that this method only applies to devices equipped with infrared transceivers. Also, IR is not human-perceptible and despite its line-of-sight property, it is not completely immune to MiTM attacks, in particular for people with vision loss.

Image-based Comparison: The main idea in this class of methods is to encode the OOB data into "human-distinguishable" random images. Prominent examples include the Snowflake mechanism [5] and the Random Arts Visual Hash [15]. These methods, however, require high-resolution displays and are thus only applicable to a limited number of devices, such as laptops, PDAs and certain cell phones. This method is not usable for people with vision loss; since the generated images are random, they can not possibly be described into words using an automated tool.

Seeing-is-Believing (SiB): McCune, et al. [11] proposed the SiB technique which involves establishing two unidirectional visual channels: one device encodes the data into a two-dimensional barcode and the other device "reads it" using a photo camera (operated by the user). At a minimum, SiB requires one device to have a camera and the other – a display. Thus, it is not suitable for small or low-end devices. Taking a snapshot of a barcode displayed on a device's screen would be extremely difficult for blind people and thus SiB is not suitable for them.

Loud-and-Clear (L&C): This technique [7] uses the audio as its OOB channel along with vocalized "MadLib" sentences. Basically, the SAS data is encoded into a Madlib sentence and emitted by the devices using a display and/or a speaker. The user simply compares displayed or spoken sentences. Naturally, L&C is not suited for devices without a display or a speaker. Clearly, L&C method with spoken sentences (or simply when used with a screen reader software) is applicable for the blind. However, the security of this method will crucially rely on whether a blind person can confidently verify that the sources of the spoken sentences are indeed the two devices being paired and not a nearby attacking device. Since it would be hard for the blind to gauge the physical presence of an adversarial device nearby, we believe that it is possible to launch a successful MITM attack on the L&C method, which we call the "Fake-Audio" attack.

Blinking-Lights: Another method taking advantage of the visual OOB channel was presented in [23]. This is geared for pairing devices one of which has a visual receiver (i.e., a video camera). First, a unidirectional channel is established by one device transmitting SAS data (e.g., by using a blinking LED) and the other device receives using a video camera (controlled by the user). Then, the latter device validates received data with its own copy and trans-

[5] This method, however, does not offer any protection against a malicious audio sniffer on the terminal.

mits the one-bit result (success/failure), e.g., by displaying it on the screen. The user finally transfers this bit over to the sending device. For reasons similar to that of SiB, these methods are also not suitable for the blind.

Numeric-Comparison/Transfer: The work in [29] presents the results of a comparative usability study of pairing methods for devices with displays capable of showing 4 decimal digits of SAS data. In the "Compare-Confirm" approach, the user simply compares two 4-digit numbers displayed on two devices. In the "Select-Confirm" approach, the user selects a 4-digit string (out of a set) on one device that matches the 4-digit string on the other device. In the "Copy-Confirm" approach, the user copies the 4-digit number from one device to another. These methods are undoubtedly simple, however, [29] indicates that Select-Confirm and Copy–Confirm are slow and error-prone. Numeric-comparison is applicable to be used by the blind (aided by the screen reader software), however, it is potentially vulnerable to the Fake-Audio attack, similar to L&C.

BEDA: A very recent proposal, [27], focuses on pairing two devices with the help of "button presses" by the user, i.e., utilizing the tactile OOB channel. The method has several variants: "Blink-button," "Beep-Button, " "Vibrate-Button," and "Button-Button". In the first three, the sending device blinks its LED (or beeps or vibrates) and the user presses a button on the receiving device. Each 3-bit block of the SAS string is encoded as the delay between consecutive blinks (or beeps or vibrations) of one device. As that device blinks (or beeps or vibrates), the user presses the button on the other device thereby transmitting the SAS from one device to another. In the fourth ("Button-Button") variant, the user simultaneously presses buttons on both devices and user-controlled (random) inter-button-press delays are used as a means of establishing a common secret. The first three variants are most relevant to this paper, as they are based on authenticated OOB (unlike button-button variant which also requires secrecy). Clearly, blink-button can be ruled our for people with vision loss; beep-button is potentially vulnerable to the Fake-Audio attack; vibrate-button is quite suitable, however, it is only applicable to pairing scenarios where one of the devices has vibration capability (e.g., cell phone).

Synchronized Comparison: [16] developed a pairing method based on "human-comparable" synchronized audio-visual patterns. Two proposed methods, "Blink-Blink" and "Beep-Blink", involve users comparing very simple audiovisual patterns, e.g., in the form of "beeping" and "blinking", transmitted as synchronized streams. One advantage of these methods is that they require the devices to only have two LEDs (one of which is to ensure synchronization) or a basic speaker. These methods were also extended for devices which have vibration capabilities [24]. Any combination which involves blinking would be unusable by the blind; a combination which involves beeping would, on the other hand, be prone to the Fake-Audio attack. The combination where both devices vibrate synchronously is perhaps most usable by the blind, however, has limited use cases (e.g., pairing of two cell phones).

Over-Audio: A variant of the HAPADEP method [28], we call "Over-Audio," can be used where the OOB data is transmitted from one device to the other over automated audio streams. This would require both devices to have speakers and microphones. Although suitable for the blind, this method is also possibly vulnerable to the Fake-Audio attack.

3.2 Feasibility of the Fake-Audio Attack

Given that a large number of pairing methods rely on some form of auditory communication to the user, one research task is to experimentally evaluate the feasibility of executing a Fake-Audio attack. Although there has been some evidence that blind people (especially blind children, as shown in [2], e.g.) are better at detecting the direction of sounds compared to the sighted individuals, we believe that clearly distinguishing the source of the sounds, especially when they are emanating from devices, would be quite tough. To this end, we need to pursue a usability study in which our blind testers will be asked to perform some of the audio-based pairing methods, in the presence of a hidden mobile attacking device controlled by a test administrator, without the knowledge of the testers. This study should measure the accuracy with which the testers can detect such attacks, and estimate the upper and lower bounds of distances between the attacking device and test devices necessary to execute such attacks. While performing this study, we need to differentiate among our methods in terms of the type of audio, i.e., spoken numbers [29], spoken sentences (L&C [7]), beeps (Synchronized comparison [16] and BEDA [27]), and automated audio streams (Over-Audio [28]).

3.3 Comparative Usability Evaluation

Another usability study is needed to test the pairing methods suitable for the blind, i.e., Vibrate-Vibrate and Vibrate-Button and any successful methods resulting from the study mentioned above. To this end, as an extension of our ongoing work on device pairing, we will develop a thorough typology of various existing device pairing methods, implement them using a common software platform (now with the necessary screen reader software) and conduct a comprehensive and large-scale investigation, focusing not only on usability and security, but also on user comprehension and acceptance of the process.

Through the above usability study, our goal is to determine: (1) the most appropriate method for a given combination of devices suitable for the blind, in terms of speed, error-tolerance and usability, and (2) how these methods can be improved in terms of both usability and security.

3.4 Pairing using a Mobile Phone

In our recent work [25], we developed and tested automated versions of the Blink-Blink and Beep-Blink schemes of [16], whereby the comparison of audio/visual patterns is not performed by the user, but by an auxiliary device of hers (e.g., a personal camera phone). We showed that the automated schemes improve the efficiency and usability of pairing, and especially become much more robust against the fatal errors (or false negatives) [29]. Although, our phone-based pairing methods are not suitable to be used by people who are blind, we feel that "pairing using an auxiliary device" is a valuable research direction. This is motivated by the fact that, as mentioned in Section 2, mobile phones have become an indispensable parts of the lives of blind (and other disabled) users, offering constant availability and accessibility, and thus can be effectively used to solve the pairing problem.

Assuming that the blind users are immune to the Fake-Audio attack (i.e., if our usability study described in Section 3.2 reveals so), the automated version of the Beep-Beep method [16] would be quite useful. A technical challenge in designing automated Beep-Beep method would be the issue of dealing with distinct frequency beeps. Another possibility is that the user have her mobile record the beeping on both devices separately and have them compare the two. Automating Vibrate-Beep and Vibrate-Vibrate combinations is also possible by making use of an accelerometer-equipped phone (e.g., Iphone); here the user will simply need to physically touch the vibrating device(s).

4 Conclusion

In this paper, we set forth the research challenges towards developing authentication technologies amenable for blind computer users. We also discussed potential research directions to address these challenges. We hope that our work would motivate other researchers to design security solutions keeping in mind not only human abilities but also human disabilities. Besides several technical obstacles, one main reason Usable Security research aimed at disabled user population becomes extremely challenging is that disabled human subjects are not easily accessible to perform usability studies. This area requires a true cross-disciplinary collaboration involving experts from security, social science, HCI and relevant disabilities centers.

References

[1] In-ear Monitor. http://en.wikipedia.org, last access, December 2008.

[2] D. H. Ashmead, R. S. Wall, K. A. Ebinger, S. B. Eaton, Snook-Hill, M. M., and X. Yang. Spatial hearing in children with visual disabilities. *Perception*, 27:105–122, 1998.

[3] D. Balfanz, D. Smetters, P. Stewart, and H. C. Wong. Talking to strangers: Authentication in ad-hoc wireless networks. In *NDSS*, 2002.

[4] R. Dhamija, J. D. Tygar, and M. A. Hearst. Why phishing works. In *CHI*, 2006.

[5] I. Goldberg. Visual Key Fingerprint Code, 1996. Available at http://www.cs.berkeley.edu/iang/visprint.c.

[6] P. Golle and D. Wagner. Cryptanalysis of a Cognitive Authentication Scheme (Extended Abstract). In *S&P*, 2007.

[7] M. T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun. Loud and Clear: Human-Verifiable Authentication Based on Audio. In *ICDCS*, 2006.

[8] W. Harris. How Noise-canceling Headphones Work. http://www.howstuffworks.com, last access, December 2008.

[9] N. Hopper and M. Blum. Secure Human Identification Protocols. In *ASIACRYPT*, 2001.

[10] S. Laur, N. Asokan, and K. Nyberg. Efficient mutual data authentication based on short authenticated strings. In *CANS*, 2006.

[11] J. M. McCune, A. Perrig, and M. K. Reiter. Seeing-is-believing: Using camera phones for human-verifiable authentication. In *S&P*, 2005.

[12] K. D. Murray. Laser Beam Eavesdropping Sci-fi Bugs? http://www.spybusters.com, last access, December 2008.

[13] S. Pasini and S. Vaudenay. SAS-Based Authenticated Key Agreement. In *PKC*, 2006.

[14] T. Perković, M. Čagalj, and N. Saxena. SSSL: Shoulder Surfing Safe Login. In *Submission*, 2009.

[15] A. Perrig and D. Song. Hash visualization: a new technique to improve real-world security. In *CrypTEC*, 1999.

[16] R. Prasad and N. Saxena. Efficient device pairing using ”human-comparable” synchronized audiovisual patterns. In *ACNS*, 2008.

[17] K. R. and Y. W. Authentication Using Tactile Feedback. In *Interactive Experiences, HCI, London, UK*, 2006.

[18] A. Rabkin. Personal knowledge questions for fallback authentication: security questions in the era of facebook. In *SOUPS*, 2008.

[19] D. Reichl. Keepassmobile, 2009. Available at http://www.keepassmobile.com.

[20] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. C. Mitchell. Stronger password authentication using browser extensions. In *USENIX Security*, 2005.

[21] V. Roth, K. Richter, and R. Freidinger. A PIN-entry Method Resilient Against Shoulder Surfing. In *CCS*, 2004.

[22] H. Sasamoto, N. Christin, and E. Hayashi. Undercover: Authentication Usable in Front of Prying Eyes. In *CHI*, 2008.

[23] N. Saxena, J.-E. Ekberg, K. Kostiainen, and N. Asokan. Secure device pairing based on a visual channel. In *S&P'06*, 2006.

[24] N. Saxena and J. Voris. Pairing devices with good quality output interfaces. In *ICDCS WISP Workshop*, 2008.

[25] N. Saxena, J. Voris, and B. Uddin. Universal Device Pairing Using an Auxiliary Device. In *SOUPS*, 2008.

[26] Sophos. Blind computer users struck by a very unusual trojan attack, January 2008. http://www.sophos.com/security/blog/2008/01/998.html.

[27] C. Soriente, G. Tsudik, and E. Uzun. BEDA: Button-Enabled Device Association. In *IWSSI*, 2007.

[28] C. Soriente, G. Tsudik, and E. Uzun. HAPADEP: Human Asisted Pure Audio Device Pairing. In *eprint*, 2007.

[29] E. Uzun, K. Karvonen, and N. Asokan. Usability analysis of secure pairing methods. In *USEC*, 2007.

[30] D. Weinshall. Cognitive Authentication Schemes Safe Against Spyware (Short Paper). In *S&P*, 2006.