Adventures in Authentication – Position Paper

Authentication in Mobile and Ubiquitous Computing

Heather Crawford
Department of Computer Sciences and Cybersecurity
Florida Institute of Technology
150 W. University Blvd
Melbourne, FL, USA, 32901
hcrawford@fit.edu

The Problem

Authentication on mobile devices is not (and should not be) the same as on desktop and laptop computers. The differences span not only the device itself and how we interact with it ("bursty" pattern where we pick it up frequently but for short periods of time) but also with the touch screen interface provided on many mobile devices. Frequent, effortful authentication reduces the usability of any authentication method and runs the risk of annoying the user to the point that they disable it. Given that mobile devices often store sensitive information about their owner, disabling authentication has the effect of putting the data it stores at risk. The small(er) touch screen and soft keyboards on most mobile devices do not lend themselves well to typing, which makes traditional textual passwords less functional on mobiles. Furthermore, mobile devices are often used in public places, where the threat of external observation attacks such as shoulder surfing is very real and very prevalent. Even worse, password authentication is all-or-nothing, so once we have entered the shared secret, everything on the device is available. This has far-reaching consequences, since people may share their device for a short period of time, and may wish to block access to some, but not all, functionality. Finally, due to their mobile nature, smartphones are often lost or stolen, which means that any authentication method must continue to protect the information on the device in this circumstance.

Mobile Authentication Problem

Due to these inherent differences, simply deploying a method on mobile devices that is usable and useful on a desktop or laptop computer will not suffice. A new method that respects the mobile device environment is necessary. Such a method must meet all of the specifications of the *mobile device authentication problem*:

We need a method that[1]:

- Allows frequent authentication without annoying or frustrating the user;
- Provides observation-resistance, and that does not require much (if any) typing;
- Provides continued protection if the device is lost or stolen;
- Allows for granular protection of data and functionality that goes beyond point-of-entry solutions;
- Provides a level of security as high or higher than a traditional password or PIN;
- Builds trust in device owners, and is also acceptable to them;
- Respects the inherent limitations of mobile devices, specifically its bursty use pattern, and its limitations in processor speed, battery life and memory.

Proposed Solutions

Several alternatives to traditional password or PIN authentication have been proposed, including graphical passwords, biometrics, cognitive questions, and drawn passwords. These solutions, and others, show promise as a potential solution to the mobile device authentication problem. Few of them, however, have left the research lab in a major way (why? What is the perceived barrier?). Apple has begun using fingerprints as an authenticator, to derision and fear from the user community. Similarly, Windows 8 has an option to use a graphical password for authentication of which many users are still unaware (it is called the "great, untapped potential" by PC Magazine[2], a pun which is both amusing and worrying). No current solution solves all of these issues, however, so I believe more work must be done, particularly in building a solution that addresses the frequency of authentication, and trust-building in device owners.

Future Work

A solution that is based on many of these proposed alternatives would be ideal. I have previously designed a framework that provides a solution to the mobile authentication problem [3] that is showing promise in further experiments.

[1] Some of these suggestions also appear in [1]

[2] `http://www.pcworld.com/article/2028724/windows-8-picture-passwords-their-great-untapped-potential.html`. Last accessed May 21, 2014.

Symposium on Usable Privacy and Security (SOUPS) 2014, July 9–11, 2014, Menlo Park, CA.

This framework used behavioral biometrics to create a pattern of the legitimate owner's device use, and allow or disallow future access by comparing a recently gathered pattern to the ground truth pattern. From this work I have learned that the mobile device environment provides many challenges that are not adequately identified in the mobile device authentication problem. For instance, how do we convince the device owner that their device and data are protected when the protection method runs in the background? How do we manage false positives and false negatives, given that biometric matching is, by its nature, fuzzy while still providing an acceptable security level? How do we protect the device when one (or more) biometric is not distinctive? Transparent, continuous authentication solutions have also created other problems, such as the amount of time that must pass before a ground truth is laid for future comparisons, as well as the amount of time that must pass between the device being lost or stolen, and any protection of the data on it. Other similar solutions exist [1, 2, 4] and each of them come from a slightly different point of view. Research is ongoing, and a discussion of potential solutions to these and other issues would be beneficial.

I believe that a robust solution to the mobile authentication problem is possible, but that it exists in some as-yet-unimagined idea that is based on the above approaches. In terms of future work, it is possible that such a solution may be able to be used in ubiquitous computing environments, where people move frequently between rooms, networks, tasks and devices. Since mobile device are such a large part of these environments, the research into mobile device authentication solutions can be leveraged to improve authentication in ubiquitious computing environments, at least as far as human-to-device authentication is concerned.

My Interests

As shown in this position paper, I am particularly interested in transparent authentication on mobile devices. I see this as being related to authentication issues in wearable computing such as smart watches, on-head devices such as Google Glass, where the user may not have a interface that lends itself to traditional authentication methods. I am also interested in federated authentication in ubiquitous computing environments, which allows various devices to pass an authentication decision between themselves, providing a more seamless computing experience to the user. Discussion of reasons why, despite the amount of research being done in this area, the current solutions have not left the research lab in a major way is also of interest to me. Discussion of any of these issues is of interest to me, and would be areas in which I would be happy to present or otherwise participate.

1. REFERENCES

[1] Nathan Clarke, Sevasti Karatzouni, and Steven Furnell. *Emerging Challenges for Security, Privacy and Trust*, volume 297/2009 of *IFIP Advances in Information and Communication Technology*, chapter Flexible and Transparent User Authentication for Mobile Devices, pages 1 – 12. Springer Boston, 2009.

[2] Mauro Conti, Irina Zachia-Zlatea, and Bruno Crispo. Mind How You Answer Me!: Transparently Authenticating the User of a Smartphone when Answering or Placing a Call. In *Proceedings of the 6th ACM Symposium on Information, Computer, and Communications Security*, pages 249 – 259, 2011.

[3] Heather Crawford, Karen Renaud, and Tim Storer. A Framework for Continuous, Transparent Mobile Device Authentication. *Computers & Security*, Vol. 39, Part B:127 – 136, 2013.

[4] C.G. Hocking, S.M. Furnell, N.L. Clarke, and P.L. Reynolds. Cooperative User Identity Verification Using an Authentication Aura. *Computers & Security*, page in press., 2013.