Principles of Authentication

Ed Talbot
UC Davis
California, USA
edward.talbot@gmail.com

Sean Peisert
UC Davis and Berkeley Lab
California, USA
peisert@cs.ucdavis.edu

Matt Bishop
UC Davis
Calfornia, USA
bishop@cs.ucdavis.edu

ABSTRACT

In the real world we authenticate hundreds of times a day with little effort and strong confidence. We believe that we should do so in the digital world as well. We consider authentication for critical systems, and the results developed are broadly applicable. Specifically, we suggest principles that enable a system to measure the assurance that someone is who they say they are. We present a "gold standard" for authentication that builds from what we naturally do every day in face-to-face meetings. We propose a "Authentication Processing Unit" that provides continuous authentication for critical systems. This work differs from other work in authentication by positing principles as a basis for integrating multiple authentication factors without adding burdensome overhead to the users.

1. INTRODUCTION

> *Who are you?" said the Caterpillar.*
>
> *Alice replied, rather shyly, I hardly know, sir, just at present at least I know who I was when I got up this morning, but I think I must have changed several times since then."*
>
> —Lewis Carroll, *Alice's Adventures in Wonderland (1865)*

Systems can be developed using clean-slate, ground-up techniques involving combinations of formal verification and both technological and human Byzantine fault tolerance in such a way that conformance to specific security requirements can be measured. Underlying these requirements and measures is the assertion that a specific user has been properly validated. Thus, we need authentication assurance, especially in critical system environments such as nuclear command and control systems [2].

Authentication, sometimes called *origin integrity*, is the binding of an identity to a representation of that identity (such as a physical body or a login identifier). Authentication *assurance* is a means of measuring the degree of trust that one can have that the source of data is who it purports to be [3]. Humans have authenticated each other throughout history. Sometimes physical proximity enables great assurance in authentication. Sometimes two people cannot be near each other or may not know each others' appearance, so alternate means such as using the impressions of signet rings in wax, secret handshakes, or passwords, have been used to assure the authentication. The reality of these latter techniques is that they often fail. Today, we still authenticate each other by recognizing one another when we are in close physical proximity.

But current physical techniques often fail, especially when we need to authenticate someone with high assurance at a distance. One problem is that techniques currently used for authentication over a distance do not measurably provide a degree of trust. Knowing a password may indicate nothing more than that the password has been guessed, and possessing an RSA token may indicate nothing more than it has been stolen. In general, it is impossible to measure the risk of either.

Thus, our interest in authentication assurance is twofold: first, it is about methods for measurably evaluating whether or not someone is who they say they are, and not, for example, performing a masquerade attack [4] by presenting stolen, forged, duplicated, guessed, or mimicked credentials. Second, we are interested in making sure that the authentication is intentional and not coerced. These two concepts—assurance and intent—form the basis for definitive command and control of critical systems [5]. Securing systems against people who are already trusted and who then decide to do something malicious (e.g., "insiders" [6]) is a timely and related topic but we can use system design, formal methods, and fault tolerance as defenses to address such threats [1].

2. PRINCIPLES OF AUTHENTICATION

We posit four "principles of authentication" [8] that systems must adhere to in order to measurably capture the elements that make the current gold standard of in-person, human-to-human function well. These principles describe a basis for measuring the amount of trust that one can place in a process of authentication:

1. Identity should be verified as long and as frequently as access to a resource is permitted. If access is continuous, then identity verification should be continuous.
2. Authentication must be done in such a way that one can measure the degree of assurance that someone is who they claim to be, and whether that person intends to authenticate or is being coerced.
3. In-person, human-to-human authentication is the "gold standard." When this is not possible and computers must be involved, then computers should provide measurable assurance (or lack thereof) to humans. Those humans should ultimately make authentication decisions, not computers.
4. Authentication should be trivial for the person legitimately authenticating but infeasible for an adversary posing as that person.

Using these techniques, we assert that humans should judge things based on the confidence level a computer provides. Moreover, instead of a single sign-in event enabling access until the user logs out, rich authentication intelligently fuses sensor data with predictable human behavior and limitations to enable measures of confidence (assurance) that the specific user is at the machine.

3. IMPLEMENTATION IDEAS

Surprisingly, these principles of authentication may not be as difficult to implement as first thought. Most of the capabilities

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

enabling such implementations (for example, cameras, navigation, accelerometers, and speech recognition) already exist in modern smartphones. Writing software linking these existing capabilities in a manner consistent with the principles is straightforward. The challenge lies in assuring the security of the completed system and for this, experience shows that general-purpose computing systems cannot be made secure enough to resist compromise by a determined adversary.

Historically, special-purpose computing needs have resulted in the development of dedicated, special-purpose computing hardware. Early in the history of computing, the Arithmetic Logic Unit (ALU) was developed to augment the numerical processing capabilities of more limited general-purpose CPUs. Likewise, Graphics Processing Units (GPUs) were developed to provide high-performance graphics handling. Similarly, designing and implementing a hardware "Authentication Processing Unit" (APU) implementing the principles of authentication outlined above would be an expected outcome of such consideration.

An APU would need an extraordinary level of assurance. Like the approaches used in other high-assurance systems, formal methods would figure prominently in such analysis. Though hardware assurance is a critical aspect of APU implementation, adversaries can expected to exploit vulnerabilities in the human-machine interface as well. Therefore, an APU-human interface would need to be highly intuitive and clearly communicate its being used, making any attempt to subvert secure operation blatantly obvious to even novice users. Any adversarial compromise in the interface would need to produce an outcome that would convince the user that the system was "sick" and, therefore, not to be trusted. Arguably, video game interfaces provide the most intuitive user experiences available. This suggests that adoption of video game interfaces and metaphors would significantly improve overall system assurance.

These two APU design imperatives (formal methods at the lowest level and intuitive interfaces at the highest level) indicate that APU implementation must be a cross-disciplinary endeavor. An adversary would be expected to exploit any weakness across the "full-scope stack" [1].

4. SUMMARY

Online activities can approach the same level of clarity, certainty and intuitiveness as activities in the physical world. Physical world metaphors drive the entire user experience. However, the misapplication of some of these metaphors—such as resemblance as opposed to mere consistency—to online actions can create anxiety and confusion for users. Moreover, a mismatch in goals—preventing an attacker cracking a captured set of password hashes, rather than validating user identity—lead to solutions that are inappropriate in some situations, and certainly in critical environments, because they solve a different problem than high-assurance authentication. Our principles of authentication are a solution to this mismatch. By properly ensuring consistency between the physical and online worlds and appropriately managing the role of humans vs. the role of computers, the "membrane" between the physical and online world effectively disappears.

5. ACKNOWLEDGMENTS

This abstract is derived largely from our paper at NSPW 2013 [8].

This research was supported in part by the Director, Office of Computational and Technology Research, Division of Mathematical, Information, and Computational Sciences of the U.S. Department of Energy, under contract number DE-AC02-05CH11231. It is also supported in part by the National Science Foundation and the GENI Project Office under Grant Number CNS-0940805, and by the National Science Foundation under Grant Numbers CCF-1018871 and CCF-1049738.

Matt Bishop was supported by the National Science Foundation under Grant Numbers OCI-12456061, CNS-1258577, and the National Institute of Standards and Technology Grant Number O-60NANB13D165. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation or the National Institute of Standards and Technology.

Some of this work was completed while Ed Talbot was a Distinguished Member of Technical Staff at Sandia National Laboratories. Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect those of any of the employers or sponsors of this work.

6. REFERENCES

[1] S. Peisert, E. Talbot, and M. Bishop. Turtles All The Way Down: A Clean-Slate, Ground-Up, First-Principles Approach to Secure Systems. In *Proceedings of the 2012 New Security Paradigms Workshop (NSPW)*, pages 15-26, Bertinoro, Italy, September 19-21, 2012.

[2] R. J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems, Second Edition*, chapter 13, Nuclear Command and Control. Wiley Publishing, second edition, 2008.

[3] M. Bishop. *Computer Security: Art and Science.* Addison-Wesley Professional, Boston, MA, 2003.

[4] T. F. Lunt and R. Jagannathan. A Prototype Real-Time Intrusion-Detection Expert System (IDES). In Proceedings of the 1988 IEEE Symposium on Security and Privacy, pages 59-66, Oakland, CA, April 18-21, 1988.

[5] R. J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems, Second Edition*, chapter 13, Nuclear Command and Control. Wiley Publishing, second edition, 2008.

[6] M. Bishop, S. Engle, S. Peisert, S. Whalen, and C. Gates. We Have Met the Enemy and He is Us. In *Proceedings of the 2008 New Security Paradigms Workshop (NSPW)*, Lake Tahoe, CA, September 22-25, 2008.

[7] S. Peisert, E. Talbot, and T. Kroeger. Principles of Authentication. In *Proceedings of the 2013 New Security Paradigms Workshop (NSPW)*, pages 47–56, Banff, Canada, Sept. 9-12 2013.