Passwords: If We're So Smart, Why Are We Still Using Them?*

Cormac Herley,[1] P.C. van Oorschot,[2] Andrew S. Patrick[3]

[1] Microsoft Research, Redmond, U.S.A.
[2] School of Computer Science, Carleton University, Canada
[3] National Research Council, Ottawa, Canada

Abstract. While a lot has changed in Internet security in the last 10 years, a lot has stayed the same – such as the use of alphanumeric passwords. Passwords remain the dominant means of authentication on the Internet, even in the face of significant problems related to password forgetting and theft. In fact, despite large numbers of proposed alternatives, we must remember more passwords than ever before. Why is this? Will alphanumeric passwords still be ubiquitous in 2019, or will adoption of alternative proposals be commonplace? What must happen in order to move beyond passwords? This note pursues these questions, following a panel discussion at Financial Cryptography and Data Security 2009.

1 Introduction

Passwords have served us well for many years, but they suffer from a number of problems that suggest their reign should be coming to an end. Users often choose weak passwords, making guessing and brute-force dictionary and exhaustive attacks feasible. Users also frequently forget passwords, necessitating expensive customer support calls or automated backup authentication schemes (often involving challenge questions, which may be even weaker forms of authentication). Because of these cognitive challenges, users frequently store copies of their passwords (in places vulnerable to attackers), and use the same password for multiple systems. Users also can have their passwords stolen through phishing, social engineering, man-in-the-middle, and keylogging attacks. The static nature of passwords then allows repeated unauthorized access by attackers.

Even with all of these problems, passwords remain the dominant method for access control. There are reasons to be optimistic about change, however. The popular press has frequent stories about identity theft and fraud, and there appears to be increasing awareness, even among unsophisticated users, about password issues. Few consumer security problems get more attention than banking passwords. Many banks have altered their authentication mechanisms, suggesting a willingness to adapt and go beyond traditional passwords. There has also been a surge of activity in proposing alternatives to password authentication, both in the academic research literature and the startup scene. As economic

* Version: April 3, 2009. FC 2009 post-proceedings (to appear, Springer LNCS).

gain has emerged as a primary motivation for computer security exploits, there should be increased motivation to move beyond simple passwords. On the other hand, despite these signs of real need and a desire for change, adoption of authentication alternatives has been very slow.

In this note we consider possible reasons why we are moving so slowly in replacing problematic password systems, how we might accelerate the progress, and where we might be in ten years. Rather than focus on the specifics of particular technologies, we prefer to consider forces that drive or retard progress, including technology, economics, and usability.

2 Some Proposed Alternatives to Basic Passwords

Numerous authentication alternatives and enhancements to basic passwords have been proposed, each with its own advocates. Two-factor authentication schemes, where the user demonstrates possession of a physical token, reduce or eliminate a number of problems associated with passwords. These schemes have seen relatively limited use, other than for very high value accounts, because of usability issues, cost of tokens and support (including replacement), the need for server changes, and the expanding key-chain problem (where users require a separate token for each account). Cell phones and various types of trusted mobile devices have been suggested as a means of achieving a two-factor scheme using a device that users already carry. Public-key infrastructure with client-side certificates offers significantly stronger authentication than passwords, but it has achieved very limited deployment. Biometrics, for example in the form of fingerprints or iris scans, are used in some secure settings, but there are unresolved issues around deployment, privacy, and authentication from untrusted hardware.

Alternatives that claim to preserve the usability and convenience of passwords while overcoming their most serious shortcomings are frequently proposed. For example, graphical passwords (e.g., see Chiasson [5, Chapter 2] for a recent survey) offer the possibility of improved strength, memorability, and usability. Combinations of text and graphical passwords [15] may also offer advantages.

In addition to proposals to replace passwords, researchers and developers have explored techniques to alleviate some of the threats associated with password use. On-screen keyboards, for example, attempt to evade password-stealing key-loggers by having the user enter the password using a graphically displayed keyboard. While this helps against malware that logs keystrokes, it is vulnerable to more sophisticated logging malware and browser plug-ins. Phishing toolbars [13] attempt to alert users before they enter credentials on low reputation websites.

Techniques such as SiteKey [2] have been deployed by a number of major financial institutions; these attempt to have the user authenticate the site only after verifying that a personalized image is present. Another recent innovation, EV SSL (extended validation SSL) certificates [4], require that the grantee (i.e., the web-site) undergo greater vetting from the Certifying Authority. The real benefit of these new technologies remains questionable. Studies have shown that users largely ignore the absence of a SiteKey image and EV SSL indicators [18, 20]. The need for automated password reset mechanisms has sparked interest in systematic analysis of challenge questions and backup authentication [17].

3 Barriers to Moving Beyond Passwords

There are many barriers to moving beyond ubiquitous alphanumeric passwords.

Diversity of requirements. Passwords are used to protect a wide range of services, from financial transactions to free webmail and social networking sites. No authentication alternative proposed to date is suitable for all of these services, splintering the target markets and weakening the case for adoption of any one new technology. The best solution often depends heavily on specific use cases.

Competing technical proposals. As noted above, there is no shortage of proposed alternatives to basic password authentication. Each has different advantages, disadvantages, and costs, all competing for mindshare.

Competing goals among stakeholders. Different views of costs and benefits are held by web sites, browser manufacturers, vendors of anti-virus software and security technologies, industry standards bodies, governments, and end-users. In some cases, an organization mandating "stronger" authentication may risk customer defection to competitors who continue with "more usable" authentication technologies (such as basic passwords).

Scarcity of loss data. There is a scarcity of data on the scale, frequency, nature and financial impact of password loss incidents, as well as on the number and nature of adversaries. For example there are orders of magnitude difference between various estimates of phishing losses [11]. When password loss does occur, we seldom have good data on whether phishing, social engineering, man-in-the-middle or keylogging was responsible. It is difficult to "fix" security without reliable measurements of what is broken, especially when the solutions are not cheap or easy. Even with relevant loss-related data, it may be difficult for an organization to make trade-off decisions about known loss incidents caused by weak password authentication versus the unknown costs of possible customer defection and increased support.

User reluctance and usability. Stronger authentication often requires additional user effort and buy-in. It is notoriously hard to motivate users about "better security." Solutions that concentrate on making passwords non-guessable risk increasing the forgetting problem, while solutions that concentrate on the forgetting problem can increase the risk of guess-ability. Solutions that concentrate on lost and stolen passwords risk introducing additional costs and complexity.

Individual control of end-user platforms. Online merchants as well as service providers largely rely on leveraging existing software and platforms (e.g., browser and operating system) which end-users have individually obtained at their own expense and preference. This limits alternatives which require specific platforms or software deployments. For example, in the U.S., banks apparently cannot force users to secure their own end-systems, leaving a big technical challenge.

No single organization can impose a solution. The combination of the above factors, plus a decentralized and global Internet that no one organization owns or controls, has resulted in a lack of consensus on what we need to do to move beyond alphanumeric passwords. Anderson et al. [1] discuss related issues in their report on the broader topic of barriers, incentives, and failures in the market for network and information security within the European Union.

4 Moving Beyond Passwords

Having reviewed barriers to making changes, we next consider, through a series of questions, what it will take to move beyond passwords.

Q1: Are any of the problems with current passwords true show-stoppers?

One viewpoint is that the problem is not as large as imagined. End-users are comfortable using weak passwords and asking for password resets when they forget them. It is unclear how much password strength helps if phishing and keylogging are the main threats [9]. Parties who do suffer pain from the present use of passwords, as direct financial losses, management cost, or usability, apparently are either: (1) not suffering enough to trigger a switch to alternatives, or (2) not in a position to evoke change. Some service providers may believe that to keep costs down it is better to minimize direct contact with customers (e.g., avoiding support calls) than to deploy stronger authentication.

A different viewpoint is that there are big problems, which are either hidden, unknown, or knowingly under-stated. Surprisingly little is actually known about large-scale usage of passwords on the Internet. For example, despite conditions in banking user agreements (e.g., in Canada) which stipulate that users must not re-use passwords across applications [14], a study of the Internet password habits of half a million browser toolbar users [8] indicates that cross-site password re-use is very common. A related problem, largely unstudied to date, is the impact on memorability and usability when end-users must remember many different passwords.

While passwords and credit card numbers are largely transported over SSL today, the roll-out of EV SSL certificates [12, 20] apparently complicates the task for end-users already struggling with interpreting the previous browser security cues (e.g., lock icon, https indicator). This may be viewed as negative progress in the usability of certificate interfaces over the past fifteen years.

One emerging use of passwords in Europe and Canada is PINs related to chip-cards (smartcards) – cards with embedded micro-processors. In the U.K. “chip and PIN” intiative [7], signatures authorizing financial transactions are replaced by consumer entry of a 4-digit PIN. The vendor motivation for adopting the new system is an off-loading of liability. Users become responsible for all approved transactions where authorization relied on a correct PIN, whereas for traditional magnetic-stripe technology with signatures, users are liable for losses in disputed transactions only if they are shown to be negligent or involved in fraud. (From a legal perspective in countries like the U.K., liability related to signature forgery falls on the relying party. PIN-authorized transactions apparently fall outside the scope of such statutory protection, and banks assert that use of a PIN implies cardholder negligence.) Consumers may be particularly unhappy to learn this detail of the new technology in light of prior demonstrations [6] that chip and PIN readers can leak user PINs.

Q2: What major security improvements have been adopted in the past 15 years by banks, related to online banking security and passwords?

In an attempt to reduce password theft (i.e., phishing attacks), online banks are starting to employ site verification schemes. For example, SiteKey [2] asks users to assign a unique image to their login credentials, and to only proceed with a login if their image is displayed back to them. An empirical study [18] suggests, however, that users will still enter their banking passwords when presented with fraudulent messages claiming that the image authentication server is down (although these results may be problematic [16]). Sitekey may be more effective as marketing effort (users feel more secure) than as a security enhancement.

SSL continues to be used for protecting passwords for countless online banking sites, and for protecting credit card numbers during online transactions. For the latter, security "enhancements" such as the third party verifier services Verified By Visa and Mastercard SecureCode have emerged. During a registration phase, a user must enter the 3-digit sequence printed on the back of their credit card along with other personal information, and choose a (new) password. On subsequent online card usage, the verifier service requests this password, but not the 3-digit code. (Oddly, some vendor sites request the 3-digit sequence be re-entered, before transferring the user on to the verifier service.) Of course, once such a 3-digit number is input to the Internet, its security value erodes. Users trained to do so make easy prey for phishers; and, this approach gives end-users the privilege of remembering yet another password. Some banks in Canada similarly now require or recommend a second (extra) password be used for higher risk financial transactions. Whether to consider these as "improvements" is unclear.

Banks are starting to deploy dynamic challenge questions and two-factor authentication. Orthogonal to these is a move towards authentication of specific transactions. Bank of America's optional SafePass, for example, requires that customers register a mobile phone that can receive text messages that contain one-time authentication codes [3]. It will be interesting to monitor the success of this program, its support costs, and how often people lose or change cell phone numbers, or claim they don't have their cell phone handy. Software implementations of one-time passcodes generators are receiving renewed interest – e.g., a new iPhone application [10] supports one-time passwords for AOL, eBay, and PayPal. Ideally, transaction authorization or transaction integrity systems will cryptographically bind one-time authorization codes with specific transaction details.

Several proposals have been made for one-time passwords for credit cards (e.g., [19]). Deployment examples include the American Express Private Payments scheme and Discover Card's Secure Online Account Numbers. Similar schemes allow end-users to dynamically generate one-time card numbers for online purchases (e.g., Citicards). While a promising direction, adoption has been limited, perhaps due to lack of promotion or low consumer motivation due to loss limits on credit cards. The main development for improving credit card transaction security appears to be in transaction authentication and back-end (system side) profiling. One might conclude that no password alternative yet proposed has better cost-benefit attributes, or that banks' existing back-end mechanisms are cheaper than anything involving customers more directly.

Q3: If we have made little progress on password authentication – perhaps the simplest Internet security problem – are researchers and security vendors fooling themselves if we think that our technologies solve real-world problems?

While passwords seem to be a simple technology, it seems unfair to suggest that authentication is the simplest Internet security problem. Indeed, many of the most difficult problems in Internet security can be reduced to authentication, and when we say authentication we often mean authorization.

No doubt, some researchers fail to do proper research into discovering the true real-world requirements, and fail to understand that in practice, complete solutions are needed. No doubt, some security vendors fail to build products that ideally meet needs, and under-estimate deployment and inter-operability issues with products. The economic barriers and incentives involved in security solutions are only recently receiving attention. Evidently, the solutions proposed so far would cost more than the problem, and good back-end transaction monitoring may mean that this state will remain for some period of time.

In addition, academics and researchers often have personal biases and over-position their own proposals as full solutions, in part due to a competitive process which often requires marketing in order for papers to be accepted for publication. Given the investment in passwords, both in infrastructure and in user acceptance and understanding, it is very difficult to see partial solutions displacing the incumbent technology. For example, it is hard to justify investment in a proposal that addresses phishing, but not key-logging, or one that helps when the user logs in from a particular machine, but not when roaming on other machines. This means that many proposals that have great merit and solve real problems do not achieve traction because they don't solve all the problems, or fail to solve a sufficient fraction of the problems relative to the extra costs.

Q4: Why have North America and Europe chosen different paths in online banking password authentication to date?

Many European banks use one-time password lists for authentication in online banking, while simple passwords (with presumably more back-end profiling) are more common in the U.S. and Canada. It is not clear to us which of the two is the better path. One possible reason for the difference is perhaps Europeans are more familiar/comfortable with real-world authentication and tolerate extra effort as required for security; passports are more common in Europe, for historical reasons.

It may also be that the differences are largely due to regulations related to liability for losses. In North America, banks have been largely responsible for covering losses unless there is evidence of fraud by the customer. This reduces the motivation for users to invest time and energy in better authentication. There may also be less customer loyalty in the U.S., with banking customers more likely to switch banks for competitive reasons; this might make banks reluctant to implement any changes that increase the costs or complexity for the customer.

5 Accelerating Progress and Predictions for 2019

Perhaps significant progress cannot be made without a major economic event or catastrophe that creates a tipping point – that is, only when the direct losses related to the use of simple passwords are large enough will there be a ground-swell of adoption of more efficient solutions or advanced technologies. On the other hand, an innovative, cost-effective solution may emerge and trigger widespread adoption, like the relatively inexpensive, conceptually simple, SSL in browsers.

More government regulation may be required, with serious penalties when use of weak technologies results in losses. The players with power (e.g., financial institutions) prefer to shift liability and responsibility for losses onto those without power (e.g., the customers). This is a significant problem if powerless customers are experiencing real hardships in the form of indirect costs, such as time lost and mental stress, when security breaches occur. If the direct losses, suffered by banks, are far smaller than these indirect costs, endured by customers, there will be little impetus for banks to drive change. It may be that only government regulations will address such a difference in power. Anderson et al. [1] suggest numerous policy changes involving additional regulations.

Where will we be in ten years? Will passwords be completely replaced by other authentication methods, or will we still be struggling with the same issues? Likely any adoption of stronger authentication technologies will be gradual and that decisions to deploy new schemes will be based on economic factors such as the value of transactions and the nature of the risks. Low-value, casual transactions may well still use ordinary passwords in ten years or even twenty.

We expect that economics and usability are far more likely than technological developments to be the primary drivers of authentication changes. As mentioned earlier, until the direct economic losses become large enough, there may be little incentive to make changes that could lead to problems in support costs or usability. Also, in the absence of tools to measure the economic losses and the effectiveness of new technological proposals, we expect the adoption of password alternatives to continue to be difficult to justify.

Acknowledgements. We would like to thank Bob Blakley and Fabian Monrose for ideas during planning of the panel; participants of FC '09 for a lively and productive discussion; and M. Mannan, Steven Murdoch, and Susan Landau (who also graciously moderated the panel) for helpful comments. The second author acknowledges NSERC funding of his Canada Research Chair in Network and Software Security, an NSERC Discovery Grant, and NSERC ISSNet.

References

1. R. Anderson, R. Bohme, R. Clayton, T. Moore. Security Economics and the Internal Market. March 2008, ENISA (European Network and Information Security Agency). Shortened version: "Security Economics and European Policy".
2. Bank of America – Online Banking. SiteKey at Bank of America. http://www.bankofamerica.com/privacy/sitekey/
3. Bank of America. SafePass: Online Banking Security Enhancements. http://www.bankofamerica.com/privacy/index.cfm?template=learn_about_safepass
4. CA/Browser Forum, http://www.cabforum.org/
5. S. Chiasson. *Usable Authentication and Click-Based Graphical Passwords.* PhD thesis, Carleton University, Ottawa, Canada, January 2009.
6. S. Drimer, S.J. Murdoch, R. Anderson. Thinking Inside the Box: System-level Failures of Tamper Proofing. Proc. 2008 IEEE Symposium on Security and Privacy.
7. S. Drimer, S.J. Murdoch, R. Anderson. Optimised To Fail: Card Readers for Online Banking. Financial Cryptography and Data Security 2009.
8. D. Florêncio, C. Herley. A Large-scale Study of Web Password Habits. Proc. of World Wide Web Conference, 2007.
9. D. Florêncio, C. Herley, B. Coskun. Do Strong Web Passwords Accomplish Anything? Proc. of Usenix HotSec, 2007.
10. Saul Hansell. What's the Password? Only Your iPhone Knows. Bits Blog (Business, Innovation, Technology, Society), The New York Times, March 31, 2009.
11. C. Herley, D. Florêncio. A Profitless Endeavor: Phishing as Tragedy of the Commons. New Security Paradigms Workshop 2008 (NSPW'08).
12. C. Jackson, D.R. Simon, D.S. Tan, A. Barth. An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks. Proc. of Usable Security 2007 (USEC'07).
13. M. Jakobsson, S. Myers (eds.). *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft.* John Wiley and Sons, 2007.
14. M. Mannan, P.C. van Oorschot. Security and Usability: The Gap in Real-World Online Banking. New Security Paradigms Workshop 2007 (NSPW'07).
15. P.C. van Oorschot, T. Wan. TwoStep: An Authentication Method Combining Text and Graphical Passwords. 4th MCETECH Conference on eTechnologies, May 2009.
16. A.S. Patrick. Commentary on research on new security indicators (2007). Retrieved March 3, 2009, from http://www.andrewpatrick.ca/essays/commentary-on-research-on-new-security-indicators/
17. A. Rabkin. Personal Knowledge Questions for Fallback Authentication. SOUPS 2008.
18. S.E. Schechter, R. Dhamija, A. Ozment, I. Fischer. The Emperor's New Security Indicators. Proc. 2007 IEEE Symposium on Security and Privacy.
19. A. Shamir. SecureClick: A Web Payment System with Disposable Credit Card Numbers. Financial Cryptography 2001.
20. J. Sobey, R. Biddle, P.C. van Oorschot, A.S. Patrick. Exporing User Reactions to Browser Cues for Extended Valiation Certificates. ESORICS 2008.