Identity in the Browser – Putting the Cart Before the Horse

Andy Steingruebl and Jeff Hodges
{asteingruebl,jeff.hodges}@paypal.com
PayPal Information Risk Management

Position Paper for W3C Workshop on Identity in the Browser
May 24 and 25, 2011 – Mountain View, CA
(updated 27-May-2011)

Introduction

Multiple attempts have been made over the years to improve authentication on the web. Despite multiple proposed specifications such as new browser chrome to prompt for *usernames* and *passwords*, better user interface (UI) treatments to tell a user what web application they are actually using, and myriad other schemes, we find ourselves back to square one. Usernames and reusable shared passwords (i.e., *shared secrets*) are still the most common way to authenticate online, phishing is still remarkably easy and lucrative for criminals, and few serious proposals exist for increasing the confidence we can have in online authentication.

Instead, various *web application service providers* (i.e., web sites) and web browser vendors are looking for yet more UI treatments to improve "identity in the browser" rather than addressing the fundamental flaws in user interfaces and authentication mechanisms, and move toward a world where phishing is not only less common, but arguably unworkable. This is the world we should strive for, a world where phishing for authentication credentials themselves[1] is ineffectual.

We should be careful to note that user education isn't necessarily as effective as we'd like, and that we need to make user experience a first-order consideration for solution approaches [5].

Additionally, practitioners in the identity and security space have largely focused on traditional computer systems (laptops and desktops) and only nominally on truly mobile devices. Given that shipments of handheld mobile devices will soon, if they haven't already, outstrip those of traditional systems [12], we need to factor the mobile space's unique attributes [7] into our considerations.

This position paper first notes our present user authentication paradigms and their susceptibility to phishing. We argue for rethinking these paradigms and provide some pointers to research in such directions. We then note that there is also a looming related problem in the context of web-enabled devices and their configuration UIs. We conclude by proposing refined, more specific goals for this workshop which we hope will help guide us in working towards addressing the underlying, fundamental user authentication issues that continue to plague us.

1 Distinct from personally identifiable information (PII) which is a separate problem.

Re-think our Fundamental User Authentication Paradigms

A fundamental issue of classical username-plus-reusable-shared-passwords as login credentials is that they can typically be wielded by anyone who knows them. That is to say, they are subject to *theft* or *borrowing*. Another fundamental issue is that typical non-specialist users can be easily mislead into revealing or sharing their credentials [3].

Phishing of users' credentials is critically dependent upon these phenomena [4], and will continue to be effective even if we deploy new "identity systems" and/or authentication protocols, unless those above noted phenomena are mitigated.

This augers for more holistic thinking in regards to the types of credentials users wield, how users are informed of and assess the risks of online interactions (i.e., via *security indicators*), how new approaches satisfy web application deployers' needs and desires, and providing more support to web application deployers for proper deployment of the security aspects of their applications. A perusal of the recent literature in these areas indicates that some researchers are pursuing these avenues.

For example, in terms of credential types, recent work on *implicit authentication* [6, 10] illustrates how a device may construct a complex, subtle notion of its user, and be able to notice, and express, if someone different is using it. These credentials aren't necessarily transferable to other contexts, and change over time. The device user isn't aware of these credentials' components or their representation due in part to never having to directly wield them.

With security indicators, research indicates that we need to much more carefully research the human factors aspects and think out-of-the-box. [11] is a recent illustration, presenting not only their own user study of their own EV certificate annunciation design, but also a brief survey of research in this area, as well as leveraging a design discipline known as *affordance*. [9] presents the results of a diary study of users' perceptions and use of security indicators, deriving broad themes from the collected data characterizing how the users conceptualized what they saw and how they subsequently made decisions.

Web application deployers may well have underlying psychological and economic reasons for perpetuating the username-and-password registration ritual. Such a website feature is *traditional*, and it also provides cover of collection personal information such as email addresses and other user attributes [1].

However, given that typical user authentication, based on reusable shared passwords, is often inconsistently and sloppily deployed [1], deployers and web application platform vendors likely could benefit from a more consistently specified and packaged approach to "username and password". The cited study's findings also illustrate the barriers to entry that any fundamentally new approaches will likely need to overcome in order to attain wide deployment.

Yet the migration to mobile handheld ubiquitously connected devices poses new challenges, thus we should be thinking about how to actually apply new paradigms such as implicit authentication to the real world, as illustrated in [2].

Not Every Web Application is Just a Simple Web Server

In terms of broadening our paradigmatic conceptions, we need to also realize that not every web application is sitting in a server farm somewhere busily processing and presenting data. Rather, we have a plethora of embedded devices leveraging the web platform for their administrative interfaces. While *cross-site scripting* (XSS) is currently a predominant attack vector (along with *SQL injection*) for the former sorts of web applications, the latter embedded devices are ripe targets for *Cross-Site Request Forgery* (CSRF) attacks [8]. Someone taking over and transforming swaths of home routers into an army of Men-In-the-Middle bots will add impetus, we're sure. New approaches to identity and authentication will need to be applicable to such devices. This also illustrates the need to make progress in developing general solutions to the CSRF class of exploits and the underlying vulnerabilities.

Rethink Our Goals?

We argue that before we collectively head down the "identity in the browser" path, we ought to see about addressing the overall UI issues various studies and papers illustrate, as well as see about addressing the plethora of issues HTTP+HTML+Cookies+AJAX, aka "the Web Platform", has in terms of protocol-level authentication, "session management", and actors' behaviors. Such improvements are needed to address CSRF exploits, for instance.

This can be approached as a refinement of our goals for this workshop, which are presently stated as:

> Solutions to be explored are effective enhancements to Web browsers that lead to trustworthy benefits that can be realized in the near term

But they should perhaps be refined as probing questions to which we are seeking answers. For example (in no particular order):

> What are the key underlying facets of today's web platform that we can address such that we mitigate phishing and attenuate the effectiveness of the coming spate of CSRF-based exploits?
>
> How do we need to change our mental models and design paradigms to accommodate the new different world of ubiquitously connected mobile handheld devices? What about web-enabled embedded devices?
>
> Can we derive a new paradigm for security indicators that are more effective for the "common" consumer user, especially in the mobile handheld context?
>
> What can be done to achieve more uniform security characteristics across the major web browsers?

We feel that if we can develop answers, or at least leads to answers, to such questions, and that after we as an industry make progress on them, then notions such as "identity in the browser" will more naturally emerge and be more useful.

References

[1] J. Bonneau, S. Preibusch. The password thicket: technical and market failures in human authentication on the web, In proceedings of WEIS 2010. http://weis2010.econinfosec.org/papers/session3/weis2010_bonneau.pdf

[2] R. Chow, M. Jakobsson, R. Masuoka, et al. Authentication in the Clouds: A Framework and its Application to Mobile Users, In proceedings of ACM CCSW'10, October 8, 2010, Chicago, Illinois, USA. http://www.eecs.berkeley.edu/~elaines/docs/ccsw10.pdf

[3] BBC. Passwords revealed by sweet deal, 20 April, 2004 http://news.bbc.co.uk/2/hi/technology/3639679.stm

[4] R. Dhamija, J. Tygar, and M. Hearst. Why Phishing Works. In Human Factors in Computing Systems (CHI 2006), Quebec, Canada, Apr. 22–27, 2006. http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf

[5] S. Görling. The Myth of User Education, Virus Bulletin Conference, 2006. http://www.gorling.se/files/texts/StefanGorlingVB2006.pdf

[6] M. Jakobsson, E. Shi, P. Golle, R. Chow. Implicit Authentication for Mobile Devices, USENIX Hot Security 2009. http://www.parc.com/content/attachments/Jakobsson-Shi-HotSec09.pdf

[7] M. Jakobsson. Why Mobile Security is not Like Traditional Security, invited paper, Financial Cryptography and Data Security 2011. http://www.markus-jakobsson.com/wp-content/uploads/fc11jakobsson.pdf

[8] R. Poyar. Cross-Site Request Forgery Attacks Against Linksys Wireless Routers, CERIAS Tech Report 2010-15. https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2010-15.pdf

[9] K. Radke, C. Boyd, M. Brereton, J. G. Nieto. How HCI Design Influences Web Security Decisions, In proceedings of OzCHI 2010, November 22-26, 2010, Brisbane, Australia. http://kennethradke.com/Papers/radke_OzCHI2010.pdf

[10] E. Shi, Y. Niu, M. Jakobsson, and R. Chow. Implicit Authentication through Learning User Behavior, Information Security, LNCS Volume 6531/2011. http://www.eecs.berkeley.edu/~elaines/docs/isc.pdf

[11] P. Shi, H. Xu, X. Zhang. Informing Security Indicator Design in Web Browsers, In proceedings of ACM iConference 2011, February 8–11, 2011, Seattle, WA, USA. http://portal.acm.org/citation.cfm?id=1940839

[12] S. Weintraub. The numbers don't lie: Mobile devices overtaking PCs, Fortune, August 11, 2010. http://tech.fortune.cnn.com/2010/08/11/the-great-game-mobile-devices-overtaking-pcs/