# Who are you now? Fading to multiple personas

Sven Dietrich
CUNY John Jay College &
The Graduate Center
New York, USA
spock@ieee.org

Michael Brenner
Leibniz University Hannover
Germany
brenner@dcsec.uni-hannover.de

Katharina Krombholz
SBA Research
Austria
kkrombholz@sba-research.org

## 1. MOTIVATION

There is strong support for single sign-on, using methods such as Facebook, Google, or Amazon for providing third-party sign-on to websites [3]. While it is practical to the user, it carries a large risk: a compromise of the account credentials can lead to a severe impact on the websites the user authenticates to, and unwanted linkages between intentionally separated social roles, or personas. Moreover, we increasingly use mobile devices and theft of a device carrying credentials could have dire consequences, potentially based on different perceptions of risk [8]. Our perceptions of risk we may assign to each world we authenticate to may be different and very individual, and that separation may be indeed necessary, albeit cumbersome.

## 2. SEPARATION VS. CENTRALIZATION

Due to recent paradigm shifts towards a more centralized Internet, the information-sharing models have changed. Services such as Facebook and Google are aiming to provide a centralized platform for multiple use-cases. The provided functionality is often used by a single person in association with a different social role, e.g. the user as a private person, or the user as an employee of a company.

Depending on our role, users may want to keep separate clusters in our social networks: our co-workers, our professional colleagues in the field, our friends and our family [3]. Others may lump them all together in one big happy family on Facebook, for example.

Removing these boundaries creates a lack of separation of privileges. Knowledge intended for one particular group can easily leak into another. We may keep different personas for each group depending on the particular role we play in that network or group, and we must realize that we have overlapping networks and roles that are not fully separable. This online behavior mirrors our real-world behavior. As an example, something that is considered acceptable behavior (e.g., personal preferences, political views) in one network will not carry well into another group. As users often do not fully understand the underlying information-sharing models, they may mix their roles across their social contexts and therefore unintentionally share information.

Facebook strongly favors a single user account and actively seeks duplicate accounts for the same physical user. Advertisers want to characterize us and force us (or perhaps incentivize us by offering rewards) to use single sign-ons to ease the profiling. Some websites, such as the alternative housing website AirBnB, even encourage linkage between multiple identifiers, such as Google+, LinkedIn, and Facebook, as a form of authentication or identification.

However, in real life we do have natural needs to compartmentalize our networks, whether it is for social reasons or to limit a breach in authentication that would permit an attacker to freely roam into other realms frequented by the user. We may choose to create credentials for a short-lived realm, such as serving on a scientific program committee, or a one-time purchase on a very specific website. We may even choose weaker credentials in the interest of usability, because we understand that the impact of a compromise would be limited.

## 3. PREVALENCE OF BEHAVIOR

While some users succumb to the temptation to use single sign-on, others proactively create unlinkable identities across realms/websites. As one method of identification, one may want to look for common passwords across websites to link such users. Such convenience (laziness) may help ease the keeping of multiple identities across realms from a usability perspective. A user who is a privacy fundamentalist would even vary those identifiers and one would have to look for alternate links to reconnect the users across social networks for example [1, 2].

During the evolution of the web, or more specifically, the evolution of economy to use the web as the preferred sales channel, users got overwhelmed with accounts. E-mail, banking, shopping, social networks, all of these functionalities required isolated registrations with a specific subset of the identity's attributes. To keep track of these accounts, a distinct family of software was invented: the password manager that mapped login credentials to web sites, and the caching of web credentials in browsers. In times of increased mobility, the next logical step seemed to be to store all that data in the much hyped cloud, trading security for convenience. The last step on that path is to not only give away the data that protects your banking account and your personal communication, but to completely delegate your identity to


*Who are you?! Adventures in Authentication. SOUPS Workshop. Symposium on Usable Privacy and Security (SOUPS)* 2016, June 22–24, 2016, Denver, Colorado.

someone else. Want to read news? Login with your Facebook account, and let us link your interests with keywords in your messages, your clicks and behavior on the web to present ads for products you will love, statistically speaking. Want to buy stuff? Let us know so we can show to your buddies what you just purchased.

A convenient way to manage multiple accounts (or identities) is vital to security. It makes people pick better passwords that do not relate to a certain pattern. So why not use a software to manage IDs? Because if this software is compromised or just fails, then all of your identities are at danger or simply lost. Some techniques, such as Versipass, have tried to mitigate that by creating password cues [6].

Technologies have been proposed to facilitate the management of multiple identities across many web sites. These technologies serve as a wallet or vault in which the identities and/or credential can be stored. For example, CardSpace, now U-Prove, is a technology to support such credential storage [5]. It can handle multiple authentication protocols, not just userid/password pairs. Similarly, the Higgins project is an open source variant [7]. These technologies were created for the desktop / laptop world, but never attracted much support. We are not aware of any comparable technologies that are popular for mobile devices.

In the mobile world, in contrast, authentication and identities are often in the devices, whether through long-lived web cookies or cached in application managed storage. Caching of credentials and access tokens are, to a great extent, a usability convenience due to the difficulty of entering credentials (userid/password) on the device. The net effect is that the device becomes an authentication token. This increases the risk of loss of an account, or identity, if the device is lost or stolen.

In spite of the ease of caching credentials in mobile devices, there are no convenient mechanisms for managing personas, or collections of identities specific to a person's social roles. Apps and web sites are managed as a collection of undifferentiated code and data. The platform and supporting apps, to a great extent, provide no general organizing structure to separate the apps and data by persona. The exception is that there are commercial mobile data management (MDM) software and services to facilitate the management and protection of enterprise apps and data. Some of these technologies (e.g., Good) provide a "container" into which the apps and data are installed. MDM can provide a limited walled garden which can manage an individual's "business" persona. Management of non-business personas typically remain unorganized and unmanaged.

While using multiple identities on the web seems fairly easy in the first place, there are also a number of pitfalls when linked to the real world: in order to keep the intended separation e. g. for different shopping realms, one may want to provide different credit cards, one for a group of stores or sort of items purchased. This, however, might turn out to be limited by the person's solvency and therefore will not match the separation of web identities in all cases.

# 4. FUTURE DESIGNS

While the effort would be considerable to maintain multiple identities and personas, it would contain any compromises to smaller subgroups and allow for quicker recovery. These are normal processes we use in access control to limit breaches, such as Role-Based Access Control or Attribute-Based Access Control. One could think about creating derivative identities from a master identity to allow for easier, more usable authentication while containing a possible breach. Of course compromise of the master identity would have a detrimental impact, so additional security would have to be spent to protect the master identity. A disadvantage of this approach is that roles are not discrete variables. There are cases where roles may overlap or intersect. This should be considered for the design of future authentication technology.

Could a *trusted third party*, equivalent to a certification authority in a public key infrastructure, that issues temporary identities and acts as a proxy, be a valid solution to the problem of handling multiple identities, similar to or as an extension to OAuth [4]? It could, under the assumption that the disclosure of a real identity is not considered significantly more serious than an encryption breach while you wire your personal data. Would some form of token that we carry around with us be useful? Do we have to issue our own credentials rather than deferring to a third party? We need to further investigate methods for how we change our personas, similarly to how we slip from our work clothes into our party clothes: how can we practically organize, change, and adapt our personas.

# 5. ACKNOWLEDGMENTS

We would like to thank Cynthia Irvine, Seda Gürses, Larry Koved, and the anonymous reviewers for their contributions and comments.

# 6. REFERENCES

[1] A. Acquisti, R. Gross, and F. Stutzman. Face recognition and privacy in the age of augmented reality. *Journal of Privacy and Confidentiality*, 6(2), 2014.

[2] R. Gross and A. Acquisti. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, WPES '05, pages 71–80, New York, NY, USA, 2005. ACM.

[3] D. Hardt. Identity 2.0, Keynote at Open Source Convention (OSCON) 2005. https://www.youtube.com/watch?v=RrpajcAgR1E, 2005.

[4] D. Hardt. The OAuth 2.0 Authorization Framework. https://tools.ietf.org/html/rfc6749, 2012.

[5] C. Paquin. Microsoft U-Prove. http://research.microsoft.com/en-us/projects/u-prove/, 2013.

[6] E. Stobert and R. Biddle. A password manager that doesn't remember passwords. In *Proceedings of the 2014 Workshop on New Security Paradigms Workshop*, NSPW '14, pages 39–52, New York, NY, USA, 2014. ACM.

[7] P. Trevithick. The Higgins Project. http://www.eclipse.org/higgins/, 2008.

[8] S. Trewin, L. Koved, C. Swart, and K. Singh. Perceptions of risk in mobile transactions. In *Proceedings of the IEEE Security & Privacy Mobile Security Technologies Workshop (MoST)*, 2016.