Putting Your Passwords on Self Destruct Mode: Beating Password Fatigue

Huascar Sanchez
Computer Science Laboratory
SRI International
Menlo Park, California, U.S.A.
huascar.sanchez@sri.com

John Murray
Computer Science Laboratory
SRI International
Menlo Park, California, U.S.A.
john.murray@sri.com

Daniel Sanchez
Computer Science Laboratory
SRI International
Menlo Park, California, U.S.A.
daniel.sanchez@sri.com

ABSTRACT
In this paper, we explore the challenge of Password Fatigue, which is essentially the difficulty involved with having too many passwords to remember and manage. The systemic failure to recognize the problem in the context of people's time and attention results in numerous security exposures due to bad habits and inappropriate shortcuts. To address this issue, we examine the concept of ephemeral content and discuss how it relates to password management and password fatigue. We introduce an authentication scheme based on ephemeral passwords, which utilizes a system called Synthetic Aperture Multimodal Biometric Authentication (*SAMBA*). The system relies on analyzing data from low-cost biometric sensors and, because of advances in machine learning techniques, we believe that the time is ripe for the development of ephemeral passwords.

1. INTRODUCTION
Many people feel overwhelmed by the number of Web accounts they need to access on a regular basis, because of the quantity of passwords that have to be updated, especially in the context of frequent password change mandates. This sense of challenge has been referred to as Password Fatigue [9] and is essentially defined as simply having too many passwords to remember (or deal with) on an erratic schedule and/or inconsistent basis.

People suffering password fatigue are exhausted from all the passwords they have to remember and all the work it takes to keep them up-to-date. Despite the existence of handy shortcuts and tools for automating this process [16], it all comes down to people's time and attention, which are in short supply.

Beyond the stress it causes, the danger of password fatigue and distracting password management is that it fosters bad security habits [5, 11]. One example of a bad security habit is using a single password to access protected information. The rationale of using a single password is that it is convenient as one only has to remember one sequence of characters. The problem with this is that if this password is compromised, then hostile individuals can access that protected information unhindered. Other examples include keeping passwords (digitally or physically) somewhere on one's computer, and choosing weak passwords that are easy to remember and thus easy to guess.

Symposium on Usable Privacy and Security (SOUPS) 2016, June 22-24, 2016, Denver, Colorado.

As time pushes us into this age of overwhelming numbers of Web accounts and passwords [6], it will be important to figure out ways to deal with password fatigue without overwhelming users. In an attempt to address this problem of password fatigue and other unsatisfactory issues surrounding password-based security, we explore the idea of self-destructing passwords.

Passwords are not supposed to be convenient or permanent. In fact, the best passwords are typically impossible to remember and temporary. Retaining a password for extended periods of time increases the likelihood that it will become compromised, so self-destruction is a potential direction for mitigating this risk.

The remainder of this paper is organized as follow: Section 2 examines the concept of ephemeral content and how this notion relates to passwords and password fatigue. Section 3 describes the key properties of our system; including its proposed authorization scheme. Section 4 describes its architecture. Section 5 presents related work. Section 6 concludes.

2. EPHEMERAL CONTENT
Technology has given us immense storage capabilities. However, this digital space has grown beyond our consumption capacity—both physically and mentally. We are simply storing more data than we really need or are capable of dealing with. Ephemeral content [15, 18] can help us deal with this growth of digital space. Particularly, it can help us not only reduce our digital footprint and optimize our storage capacity, but it can also ensure the privacy and security of our protected data. Ephemeral content is simply content that "disappears."

Many will remember the catchphrase "This message will self-destruct in five seconds" used in the *Mission Impossible* television and film series. This catchphrase is a good example of how ephemeral content can limit the threats of one's data from falling into the wrong hands. At the most extreme, one-time pads are a classic example of ephemeral content, allowing a single-use password that is exceptionally secure (but also exceptionally inconvenient for long-term use).

Along these lines, the sheer volume of passwords we manage in order to access social media, services, and email is truly overwhelming [6]. No wonder we're all feeling fatigue. That's a lot of passwords to manage, and the creation of new online accounts is adding to that vast volume every year. There are two reasons why we believe ephemeral passwords can help combat password fatigue. First, they require no management. In other words, there is no need to keep them around or remember them as new ones are always provisioned if needed (see Section 3 for details). Second, ephemeral passwords prevent the exposure of users' sensitive data as they are permanently unavailable after its

useful life; keeping the sensitive data permanently unreadable. Consequently, placing a shelf life of passwords is a viable solution for addressing this problem.

In this paper, we explore the design of a system for ephemeral passwords based on a Synthetic Aperture Multimodal Biometric Authentication method, called *SAMBA*. *SAMBA* borrows, by analogy, the "synthetic aperture" technique used in radio/optical astronomy [3, 8] whereby multiple cameras and sensors can be combined together in order to create a synthetic aperture that provides a greater image than any single sensor would ever be capable of. The idea of combining multiple sources of data in order to fuse together a single "bigger picture" has also been applied in personality assessment [13] and here we propose it as a method for verifying the identity of a user by fusing many smaller biometric samples before releasing an ephemeral password to this user. This password can be used to gain access to a Web account owned by the user. By using our system, users can request an ephemeral password every time they need one, use it, and then forget about it.

3. EPHEMERAL PASSWORDS

In a world where convenience is king, control over passwords lifetime is important. It safeguards people's protected information and also alleviate their password fatigue. Our proposed system for ephemeral passwords can help end users preserve some of that control. In other words, passwords are automatically generated when the users need them, are valid for only one login session or transaction, and are permanently unavailable after they are used. In what follows, we describe both how the release of ephemeral passwords should work, and our proposed authentication scheme. This scheme utilizes our Synthetic Aperture Multimodal Biometric Authentication (*SAMBA*) method.

3.1 Scenario: Releasing Ephemeral Passwords

Peter is a material scientist at a manufacturing company. He wants to pay his DIRECTV bill by sending money directly from his online Wells Fargo bank account. He opens his browser and then enters the URL of Wells Fargo's login page. While on that page, he sadly realizes that he cannot remember his password (or where he wrote it). Fortunately, he recently installed our system on his smart phone and his two wearable devices (watch, ring). So, he asks our system for an ephemeral password Wells Fargo can accept. Our system asks *SAMBA* to verify if this request is coming from Peter. If he is, then it releases a new password for him. Otherwise, the system immediately locks the smart phone. In the normal case, Peter gets his new password, uses it, pays his bill, leaves the website, and pretends this password never existed.

3.2 Proposed Scheme

The proposed scheme consists of five steps: registration, password request, identity verification with *SAMBA*, handshake, and password release. Figure 1 shows the proposed scheme. To facilitate presentation, we hide the registration step from Figure 1 as this step is performed offline and once. Any deviation from this decision will not affect the applicability our proposed scheme.

3.2.1 Registration

In this step the user registers with our system. This phase involves a few actions, such as;

1. Identification of a smart phone (primary) and set of wearable devices (peripheries) that will produce biometric data required by the system to verify the user's identity.
2. Binding between our system and a set of trusted Websites where the user has an active Web account. This binding guarantees the passwords that the system produces are accepted by these Websites.
3. Collection of multiple biometric samples or modalities, which are compared and fused to produce a confidence score (probability). We use these scores to verify the user's identity.

Once all the actions are performed, the user can start asking the system to release passwords his registered websites can accept.

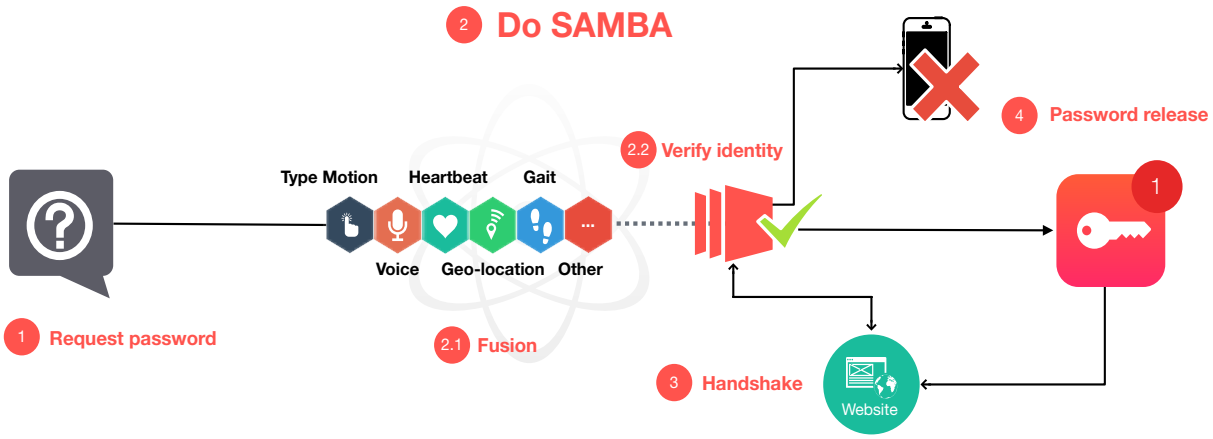

Figure 1. Proposed Scheme for SAMBA (Synthetic Aperture Multimodal Biometric Authentication).

3.2.2 Synthetic Aperture Multimodal Biometrics Authentication (SAMBA)

SAMBA is a new method for multimodal biometric authentication based on fusion [4, 17]. The SAMBA method uses biometric data collected from a set of wearable devices. *SAMBA* does not place any limitation on the number of devices from where it collects data and on the type of biometric data collected from these devices. As long as some of the biometric data overlap between different devices, a small subset of biometric samples can be used to efficiently verify a person's identity.

Inspired by SAPA [13], our system verifies a person's identity by fusing a set of small biometric samples. Our objective is to attach a probabilistic measure to the system, by converting the fused matching scores into confidence scores. These confidence scores are normalized (the sum of these scores is 1) and will represent the probability that a user is indeed that user by some level of confidence (e.g., the statement "I am 55% sure this is Peter" is correct 55% of the time). We hypothesize that as the number of biometric sensors grows, the level of confidence on a person's identity grows too.

SAMBA differs from traditional fusion in that the verification of a person's identity is performed by continuously fusing the input of many small biometric samples. This allows *SAMBA* to deal with varying numbers of biometric sensors installed on multiple wearable devices at any time.

3.2.3 Handshake

Implementing a 'one-time pass' type function where *SAMBA* releases an ephemeral password that a website can accept is non-trivial. The biggest issue is adoption. You could set up a token system akin to Apple Pay or FIDO's UAF Password-less Authentication [1], but you need vendors to support your architecture. Guaranteeing this support is easier said than done.

We address the above issue by initiating an automatic password reset. This initiation occurs during the authentication of our system to the registered website and involves the following steps:

1. Securely authenticate user requests for password resets, by using security question answers.
2. Establish a single-use and time-synchronized (e.g., 30 seconds) password that matches the website's password requirements. The shorter the lifetime of the password, the higher the security level provided.
3. Synchronize the ephemeral password with our system, so it is ready for release and its maximum validity period is enforced.

The primary driving force of this approach is the desire to provide a wrapper, or supplementary, mechanism that can be incorporated into existing authentication infrastructures, that does not require a complete overhaul of the cryptography systems by the service providers. We understand that this component is still very nascent and a naïve approach to using ephemeral passwords. Additional work is needed to develop the protocol and security capabilities, along with assessing the landscape of potential websites with which such a system would actually work. Other approaches might require the adoption of our technology by the websites the user is registered with, but this level of adoption is complex and typically requires very large partners to be involved for any progress to occur (for example, mobile payments at physical stores prior to Apple Pay).

3.2.4 Password release

This step involves the release of the password requested by the user. Once the previous steps have been completed, the system enforces the known password validity period and notifies the user of its expiration. Within this valid period, the user gain access to the website of interest.

We now discuss the design principles that guided the conception of SAMBA and describe its architecture.

4. SAMBA SYSTEM

SAMBA is a system for generating ephemeral passwords that a user's trusted websites can accept. An attack [19] against *SAMBA* can only succeed if an attacker can comprise all of the diverse components upon which the system is built. In what follows, we describe the *SAMBA* system's design principles and architecture.

4.1 Design Principles

The *SAMBA* system is guided by three design principles:

Fusion of multiple types (or modalities) of biometrics. We seek to build a system that will verify the identity of a user by fusing many smaller biometric samples before releasing an ephemeral password to this user. This is a system that is as accurate as the union of its inputs. A successful attack must subvert all of the combined system's sensors registered by a user.

Efficient match and non-march identity determination. The use of rolling time windows helps us collect relevant biometric samples in a given time period. Combining multiple rolling windows of biometric data (under a varying number of sensors) with overlapping properties can assist us in multiple ways. First, it keeps biometric samples within a given time window. Second, it can significantly increase the level of confidence on a person's identity before releasing the needed passwords. Lastly, it can increase the efficiency of a match and non-match determination of a person's identity. We accomplish all of this via synthetic aperture measurements [3, 8, 13] and fusion [4, 17].

Support future innovation in biometrics. The *SAMBA* system must be extensible to allow inclusion of new types of biometric data. These data can come either from newly installed sensors on existing devices or new devices with a set of new sensors.

4.2 SAMBA's Architecture

Figure 2 shows the proposed architecture of the *SAMBA* system. This architecture will implement the idea of ephemeral passwords, which are time-synchronized and single-use passwords.

The architecture is composed of two types of devices: the wearable device(s) and the mobile device. Each of these devices contains an application layer, which is responsible for using remote sensors. The sensor services on both types of devices are primarily responsible for both accessing the sensor data, establishing Bluetooth connectivity, and exchanging biometric data. At both sides of the architecture are instances of the *SAMBA* system. The instance on the mobile device is the primary *SAMBA*. This instance is responsible for overseeing the key functional pieces of *SAMBA*: collecting biometric samples from wearable devices, producing its own biometric samples, verifying the user's identity, authenticating with the registered websites, and releasing an ephemeral password. The *SAMBA* peripheries are responsible for producing biometric samples the primary *SAMBA* can use for further processing.

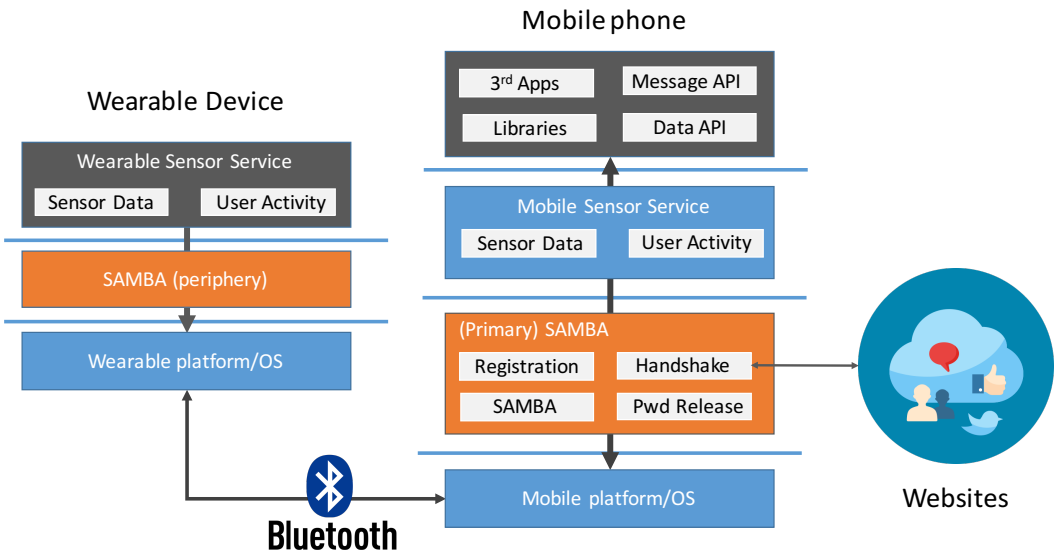

Figure 2. The architecture of the SAMBA system

5. RELATED WORK

There has been an exhaustive amount of work dedicated to solving usability issues related to authentication, and no shortage of novel approaches. However, replacing the password has been exceptionally difficult [2], likely because any one solution does not provide the technological simplicity, transparency, and understandability that password authentication provides. Given that there are a number of competing authentication schemes and mechanisms, here we focus on the most relevant to our proposed system.

Traditional Biometrics. Traditional biometrics, such as fingerprints or iris scanning, have become extremely popular and have seen recent wide-spread adoption in the mobile world. Apple, Samsung, and many other hardware vendors have incorporated fingerprint scanners into their mobile devices for fast and convenient authentication. This method of authentication has also been extended by allowing local biometric authentication to serve as the authentication mechanism to third parties, such as Apple and Android pay with multiple banks. However, while these approaches are becoming rather robust solutions, biometrics have the inherent problem that once information is compromised, it cannot ever be changed. If an attacker steals a set of fingerprints, the credentials can be revoked for authentication purposes, but the rightful user can no longer use them to access the secured system.

Behavioral Biometrics. Various behavioral biometrics have been proposed, from keystroke dynamics (e.g., how do you type your password?) to gait and user location. However, any no single method has been demonstrated to be usable at scale. A massive issue with any *single* behavioral biometric is the massive variability inherent to human behavior that provides a noisy authentication signal. For example, no user wants to be locked out of their system because they are typing in their password or are writing an email while holding their morning coffee. Similarly, movement patterns related to gait are fairly consistent, unless you have an injury, or some other environmental constraint alters your biomechanics in some way. Because of the variability in human behavior, any single approach is prone to failure due to a correct rejection problem – a serious issue that would definitely not help ameliorate security fatigue.

Biometric Fusion. The idea to fuse multiple modalities of Biometrics together is not unexplored. Both the methods for accomplishing biometric fusion [10] and the susceptibility of these systems to attacks [12, 14] is of interest to the security community, but thus far it has been difficult to apply these rules to a working system at scale. Google recently announced an attempt in this direction with their new Trust API [7], which will incorporate numerous bits of information about a user to create an identity for authentication purposes. The position we take here is that a system that can seamlessly incorporate signals across device sensors and be integrated into existing authentication systems would be ideal as an initial step towards future adoption of implicit authentication.

6. CONCLUSION

Here we presented *SAMBA*, our approach to ephemeral passwords to ameliorate password fatigue. Our proposed system combines our Synthetic Aperture Multimodal Biometrics Authentication (*SAMBA*) method with a lightweight scheme and architecture for "single-use password" release and consumption. Between sensors and data becoming exceedingly cheap and advancements in machine learning techniques, we believe that the current state of technology is ripe for the development of ephemeral passwords. The ability to simply use passive information about a user to provide an authentication mechanism is ideal from the perspective of solving security fatigue, as it removes the need for actively dealing with passwords. Of course, implicit authentication comes with drawbacks, as users are not immediately comfortable with a mysterious system that dictates whether they are able to authenticate or not, so future work is needed to develop a method for making the "synthetic aperture" more transparent to users. Despite these challenges, we argue that this approach, in one form or another, is likely the future of password-less authentication.

7. REFERENCES

[1] Balfanz, D. (2014). UAF Protocol Specification. Retrieved from https://fidoalliance.org/specs/fido-uaf-protocol-v1.0-rd-20140209.pdf

[2] Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2015). Passwords and the Evolution of Imperfect Authentication. *Communications of the ACM*,*58*(7), 78-87.

[3] Curlander, J. C., & McDonough, R. N. (1991). *Synthetic Aperture Radar*. John Wiley & Sons New York, NY, USA.

[4] Dantcheva, A., Velardo, C., D'Angelo, A., & Dugelay, J.-L. (2010). Bag of Soft Biometrics for Person Identification. *Multimedia Tools and Applications*, *51*(2), 739–777.

[5] de Joode, D. (2012). *Does password fatigue increase the risk on a phishing attack?* Tilburg University. Retrieved from http://ilk.uvt.nl/downloads/pub/papers/hait/dejoode2012.pdf

[6] Florencio, D., & Herley, C. (2007). A Large-scale Study of Web Password Habits. In *Proceedings of the 16th International Conference on World Wide Web,* 657–666.

[7] Google Developers (2016). *Bridging the physical and digital. Imagine the possibilities. ATAP – Google I/O 2016*. Video File. Retrieved from: https://youtu.be/8LO59eN9om4?t=295.

[8] Harger, R. O. (1971). Synthetic Aperture Radar Systems: Theory and Design. *Synthetic Aperture Radar Systems: Theory and Design., by Harger, R. O.. New York, NY (USA): Academic Press, 232 P.*

[9] Hayday, G. (2002). Security nightmare: How do you maintain 21 different passwords. Silicon.com, 11 December 2002.

[10] Khan, H., Hengartner, U., & Vogel, D. (2015). Usability and Security Perceptions of Implicit Authentication: Convenient, Secure, Sometimes Annoying. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)* (pp. 225-239).

[11] Peterson, A. (2016). Why changing your password regularly may do more harm than good. Retrieved May 31, 2016, from https://www.washingtonpost.com/news/the-switch/wp/2016/03/02/the-case-against-the-most-annoying-security-measure-virtually-every-workplace-uses/

[12] Poh, N., Bourlai, T., Kittler, J., Allano, L., Alonso-Fernandez, F., Ambekar, O., ... & Ganster, H. (2009). Benchmarking Quality-Dependent and Cost-Sensitive Score-Level Multimodal Biometric Fusion Algorithms. *Information Forensics and Security, IEEE Transactions on*, *4*(4), 849-866.

[13] Revelle, W., & Laun, G. (2004). Synthetic Aperture Personality Assessment. In *annual meeting of the Society of Multivariate Experimental Psychology*. Retrieved from http://personality-project.org/revelle/publications/sapa.mpa.key.pdf

[14] Rodrigues, R. N., Ling, L. L., & Govindaraju, V. (2009). Robustness of multimodal biometric fusion methods against spoof attacks. *Journal of Visual Languages & Computing*, *20*(3), 169-179.

[15] Roesner, F., Gill, B. T., & Kohno, T. (2014). Sex, Lies, or Kittens? Investigating the Use of Snapchat's Self-Destructing Messages. In *Financial Cryptography and Data Security,* 64–76.

[16] Ross, B., Jackson, C., Miyake, N., Boneh, D., & Mitchell, J. C. (2005). Stronger Password Authentication Using Browser Extensions. In *Usenix Security,* 17–32.

[17] Ross, A., & Jain, A. (2003/9). Information fusion in biometrics. *Pattern Recognition Letters*, *24*(13), 2115–2125.

[18] Shein, E. (2013). Ephemeral Data. *Communications of the ACM*, *56*(9), 20–22.

[19] Syverson, P. (1994). A Taxonomy of Replay Attacks [Cryptographic Protocols]. In *Computer Security Foundations Workshop VII, 1994. CSFW 7. Proceedings,* 187–191.