SESAME: Smartphone Enabled Secure Access to Multiple Entities

Ameya Sanzgiri Anandatirtha Nandugudi Shambhu Upadhyaya Chunming Qiao
Computer Science and Engineering, University at Buffalo, Buffalo, NY 14260
{ams76, ans25, shambhu, qiao}@buffalo.edu

***Abstract*—In this paper we present a smartphone based architecture to secure user access to web services which require password entry. Our architecture takes advantage of biometric sensors that are present in today's smartphones when authenticating a smartphone user in order to ensure that her identity cannot be masqueraded by anyone else. The user can then access web services using a complex password stored in her smartphone but without having to manually enter the complex password. As a result, the architecture overcomes many security limitations of today's password based authentication approaches, and in particular, resolves the current dilemma associated with the use of complex passwords. In addition, the proposed architecture not only works seamlessly with today's web services since it requires no changes to the existing authentication mechanisms used by the servers, but also can be extended to directly use a person's biometrics as credentials instead of passwords when accessing web services and cyber-physical devices in the future.**

I. Introduction and Motivation

Most Internet services like email, e-banking and social networking implement access control via a username password based authentication scheme. Recently, new classes of passwords such as Graphical, Haptic and Visual have been proposed to replace textual passwords which are plagued by human fallibility. While promising and efficient in standalone applications, these new class of passwords are not likely to be used in the foreseeable future, due to the requirement of new hardware, usage education and interoperability with current systems. Textual passwords thus are likely to remain at least for now as the only way to authenticate a user to web services. However, an adversary, by gaining knowledge of a user's password (e.g., by brute force attack), can compromise a user's access to such services. This concern can be largely alleviated by having users choose strong and complex passwords (which have a high information entropy) for authentication. In fact, some Service Providers have enforced password creation policies to make users choose such strong and complex passwords.

However, there are two inherent issues with users being forced to choose stronger (or complex) passwords. First, studies such as [1]–[4] have indicated that enforcing stricter password rules causes users (almost 50% according to [5]) to take shortcuts like writing down the *complex* password in clear text, either on paper or electronically, as a memory aid. Thus, it is easy for an adversary to get hold of the complex password [1], [6]–[8].

The second issue with complex passwords is the reuse or recycle of the same password for different services since remembering different passwords is burdensome. More than 34% of the people reused the exact password while almost 18% reused them with minor modifications [5]. The study in [9] also found that 41% of accounts from a university system could each be cracked in three seconds, using the knowledge of their expired passwords. A malicious entity can thus easily crack a user's password if she has the knowledge of password composition trends by the user or (and) if passwords are reused. To add to this, the risk of compromising her password either from shoulder surfing techniques [10] or key loggers on end systems always exists, especially in public places or systems [11], [12]. In shoulder surfing, an adversary is able to watch a user keying in her credential by visually recording the user's keystrokes. Keyloggers are programs or hardware devices that record all keyboard strokes.

Perhaps the most serious problem today is that current authentication systems have no mechanisms to recognize the identity of the person who enters the password; in other words, there is no way of verifying if the person presenting the credentials is actually the person that she is claiming to be. Since the communication channels can be secured using protocols such as https, SSL, TLS, the weakest link which controls a user's access to web services today is the human factor [13] due to the need of entering passwords. Hence, there is a clear need for a new system that secures the human computer interaction, especially for password entry in order to secure the end-to-end flow of data. One solution to the problem associated with passwords is to use biometrics as credentials to access web services. However, this would require an overhaul of the entire Internet and related web based services. Addressing these issues amounts to essentially finding the right answers to the following two important questions:

1. How do we build a system that overcomes the security limitations of passwords?
2. How do we incorporate biometric attributes seamlessly, i.e., without overhauling the entire Internet and the access mechanisms of its services.

The contribution of this paper which is also a summary of our solution methodology is as follows:

1. Incentivize the usage of strong passwords effortlessly.
2. Tie up a user's digital identity to physical identity.
3. Assimilate emerging technologies such as smartphones and cloud services into current technologies to realize a secure system.

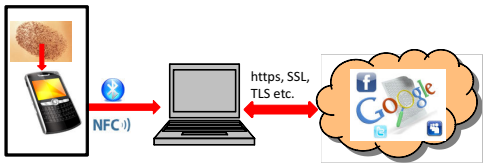


Fig. 1: Overview of SESAME

The remainder of this paper is organized as follows. We discuss the main idea of the proposed Smartphone Enabled Secure Access to Multiple Entities (SESAME) architecture in Section II. Section III describes protocols for SESAME, including a basic prototype implementation on Android phone, and integration with Cloud-based authentication with biometrics. Section IV discusses the various aspects of our design such as its capability to defend against Man in the Middle (MITM) and Denial of Service (DoS) attacks, as well as what happens if the smartphone is lost and compares it with other similar architectures. Section V concludes the paper.

II. Main Idea

Figure 1 presents an overview of SESAME which consists of a user accessing web services on a Host Terminal via a smart device. Here the Host Terminal is used to view the web content while the smart device is used for authentication purposes. The flow of information from the Host Terminal to the web server is securely processed via Internet protocols. Similarly, the authentication mechanisms and schemes at the web server are unchanged. SESAME mainly addresses the interaction between a user and the Host Terminal for accessing services. Specifically, we address the problem of inputting credentials via a Host Terminal to access a service. Incidentally, addressing this specific problem also addresses the limitation of memorizing textual passwords. SESAME provides an avenue that is complimentary to textual passwords and their usage, mainly providing a way to better support its use while removing their limitations. A user during the registering process for a web service, chooses a strong password. She then stores her credentials for the service (username and strong password) on a smart device by manually entering this information. Whenever she has to access the web service, she will securely transfer the credentials from her smart device to a Host Terminal or a cloud service which will then forward her credentials to the appropriate Service Providers. The Service Provider authenticates the user and delivers the service to the Host Terminal.

A. Description of the Architecture

1) Integrating Biometrics using Smart Devices: In SESAME, the ubiquitous smart devices play a crucial role. Smart devices in addition to possessing the processing capability and memory that rival modern computers also have optimized modules to efficiently use their limited energy, thus providing longer standby time. Many smartphones like the Motorola Atrix, come equipped with biometric sensors like fingerprint readers as well as features such as face-unlock, to authenticate the use of the smartphone. This has resulted in a paradigm shift from the traditional password based authentication on computers to the use of biometric attributes for accessing personal data stored on smart devices. With the use of smart devices, the need for setting up dedicated Biometric authentication is not required, hence circumventing its major drawback. With such a secure system already in place, SESAME proposes to extend the existing authentication schemes present in the smart devices to access web based services. By leveraging on smartphone authentication mechanisms, users can now authenticate themselves to web services via their smart device. Such a system provides an inimitable access to Internet services for each individual. By this we mean, only the owner has access to the credentials stored on the smartphone since the authentication of the device is tied to her unique biometric attributes and no other person can imitate these attributes.

2) Wireless Communication: Once we have the passwords stored on the smart device, the stored passwords need to be transferred securely to a host, so that the host can authenticate the user. This can be achieved by transferring credentials via the wireless medium using Bluetooth (BT) or Near Field Communication (NFC) which were selected for SESAME. Smartphone manufacturers already plan on integrating NFC with their smartphones, many of which are already equipped with Bluetooth. SESAME uses either or both of these mediums to transfer user credentials. The new standards of Bluetooth provides a mechanism for encrypting all its data transfers which initially were vulnerable to DoS and MITM attacks. Another desirable aspect of Bluetooth is its short range communication (more than NFC's very short communication range) and SESAME utilizes this short range to monitor the physical proximity of the user. This way a user and her smart device are *virtually leashed* to the Host Terminal. If the user moves away from the Host Terminal, the virtual leash is broken, thus alerting the Host Terminal to lock the computer or log off the user.

Similarly, due to advantages such as a very short communication range and resistance to eavesdropping, NFC is already used in financial transactions such as payments. In the current Android implementation, NFC transfers occur only when the device is unlocked (achieved only by an authenticated user). Further, NFC data rates can also transfer a user's credentials to the host device without any delay.

3) Cloud Services: Cloud services can be integrated into SESAME architecture seamlessly. The Host Terminal can also communicate with the Service Provider via a cloud service. This model has many benefits as the Host Terminal can offload the interaction with the Service Provider to the cloud. The Host Terminal simply acts as a gateway between the user interactions and the Service Provider. This makes SESAME more scalable as there would be no changes required at Host Terminal to include the services for any new Service Provider, or if an existing Service Provider changes the authentication or user interaction schemes. The model described here is one of the ways SESAME can leverage the cloud services.

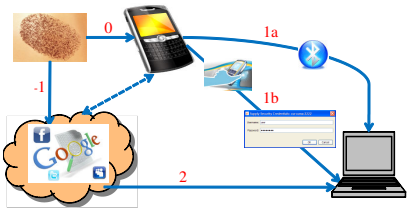
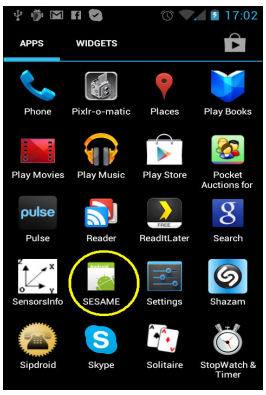


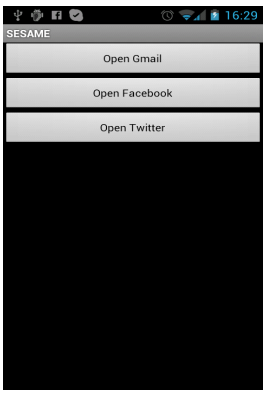
Fig. 2: Operation of SESAME

B. The SESAME Framework

In our architectural framework, a user (U) stores the credentials to access a service (S) provided by a Service Provider (SP) on her smartphone. The stored credentials on the smart device are encrypted using the user's biometric attributes. To access the service provided by the SP on a Host Terminal, User launches an application installed on her smartphone, chooses the service, and initiates data transfer by tapping her smartphone against the Host Terminal's NFC reader thus establishing a *secure* communication channel between them. The service credentials stored on the smart device are decrypted using User's biometric attribute and is transferred to the Host Terminal over the secure communication channel. After receiving the credentials, the Host Terminal contacts the SP using the medium (like web browser) through which the user desires to access the service and supplies the transferred credentials using appropriate network protocols. Once authenticated, the user can use the service on the Host Terminal. This process is illustrated in Figure 2 where the numbered links shows the sequence of operations. It is important to note that, SESAME encourages the use of strong passwords by virtually eliminating the requirement of memorizing passwords using symbolic links, mnemonic symbols or passphrases. SESAME, thus facilitates strong password usage by involving the smart device in the *memorization* of passwords, which reduces the burden on the human. By encrypting data on the smartphone, the architecture ensures that there is no unauthorized access to the credentials stored.



(a) Installed app on the phone



(b) Interface to access web services

Fig. 3: Concept in Action (a) and (b)

III. Protocol Development

A. Current Internet Services

Figure 3 illustrates the working instance, implemented on a Google Nexus S smartphone running Android ICS 4.0.3. The Host Terminal's OS is Ubuntu Linux. Note that in this implementation, the BT radios of the phone and laptop are paired with each other due to lack of NFC enabled devices. A Python process listens to incoming RFCOMM communication over the BT radio. A user who wishes to access her GMail account (for example) on the Host Terminal, configures the SESAME app (circled in 3(a)) on her phone with her GMail credentials, which are then encrypted on the phone. To access her GMail service, she unlocks her phone, launches the SESAME app, authenticates herself to decrypt her stored credentials. She then presses the "Open Gmail" button on the app as shown in Figure 3(b). The stored credentials are transferred over BT to the Host Terminal. The Python process opens the web browser on the Host Terminal which initiates a secure https connection with GMail's web service. The process then supplies the user's credentials to the web service for authentication. After successful authentication, the user uses the GMail service as she would on any other system. The prototype monitors the physical proximity of the user via the BT connection. This is achieved by the phone sending "presence beacons" over the BT channel every 30 seconds (which is configurable) to the laptop. In case the Host Terminal does not receive any presence beacons for two consecutive cycles (60 seconds) it logs off the user session on the Host Terminal.

B. Future Internet Services

In this section, we describe how SESAME can be integrated to leverage the services of the Cloud and how in the future, Service Providers can integrate SESAME to register and authenticate users based on their biometrics. Figure 4 illustrates how SESAME can leverage the services of the cloud. The initial workings of the protocol for this scenario are similar to the ones described in Section III-A, the key difference is the usage of the Cloud Service in the authentication process and the service delivery to the Host Terminal. Service is delivered either directly to the Host Terminal or via a Cloud Service. The interaction between the Cloud Service and Host Terminal can be realized in a number of methods and each of these methods realizes an instance of the SESAME architecture. We discuss two such possible instances of SESAME- *Authentication and Service Delivery via Cloud Service* (Alt 1) where the Cloud Service interacts with the SP and delivers the service to the Host Terminal, and *Authentication via Cloud Service and Service Delivered directly to Host Terminal* (Alt 2), where the user interacts with SP directly. The SESAME protocol in these scenarios is illustrated in Figure 4 where the first seven steps leading up to the successful BT/NFC connection between the Device and Host Terminal are not shown.

Further extension to the future architecture can be made by replacing the password based authentication with the use of

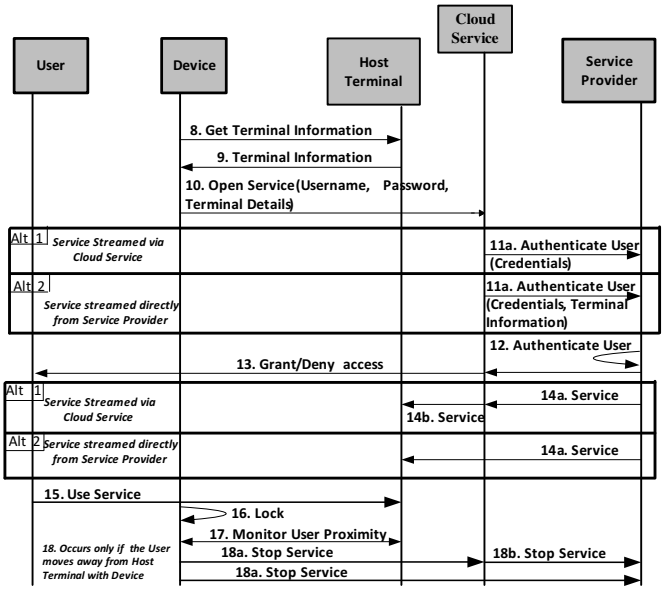


Fig. 4: Website Access Authentication via Cloud Service

only username and Biometric Hash (BH). This architecture would require the SP to support the use of BH as the authentication scheme.

IV. Discussion

SESAME is an architecture that bolsters textual password based authentication schemes for accessing Internet based services. SESAME realizes scalability and configurability without any major changes to the current Internet architecture or web services' authentication schemes. Further, there is no overhead on the user's part other than establishing the login credentials for the various web services and storing it securely on the smart device. Below, we discuss some aspects of SESAME.

A. Security Analysis

SESAME's design engineers the philosophy of building a secure system using insecure components and is resilient against shoulder surfing and key logging attacks.

a) MITM attacks for BT/NFC: The use of NFC to transfer credentials precludes attacks such as eavesdropping by using secure communication channels. Further, by using NFC for the pairing of the device and Host Terminal, we eliminate the MITM attacks. NFC's communication range makes it resilient against these attacks.

b) DoS Attacks: There have been no reports of DoS attacks targeting NFC. Bluesmack, the only known DoS attack against BT exploited a specific make of devices. With newer standards, Bluetooth is also resilient to such attacks. Smart devices could present a vulnerability to DoS attacks that aim at accelerating energy consumption. However, the authors of [14] have demonstrated the ineffectiveness of such attacks, since modern smart devices have many modules that are optimized to conserve energy.

B. Unavailability of Smart Device

The design of SESAME ensures that even if the smart device is unavailable or lost, a user can still access the service. Since SESAME augments current authentication schemes, resetting of password is transparent and for a low cost. A user can simply reset her password (if she has chosen a strong password and cannot remember it) with the appropriate SP. In case the smart device is lost or ends up in the hands of an adversary, SESAME protects unauthorized access to the user's data. All of the user's data stored on the phone is encrypted using the user's biometric attribute. It would be very difficult for the adversary to decrypt this data, since it would require the physical presence of the user. For the futuristic scenario where Biometric Hash (BH) replaces the password, the user would have to reset her account using the security answers and registering a new BH with the Service Providers. For current architectures, after resetting her account the user can choose a new password and store it on the replacement device. If the smart device is lost, the user does incur the cost (which is low) of having to reset her password.

C. Comparisons with Similar Architectures

The idea of using portable devices to control access to physical spaces has been studied before [15], [16], however the concepts presented in these papers were for securely facilitating physical access and did not extend to the cyber-domain. Subsequently, the authors provide a simplistic authentication protocol that uses "digital keys" from an external entity. The "Grey Project" [17]–[19] also presented an access-control system based on smartphones that helps in authenticating a person while providing access control to physical resources such as a door. However, the suggested architecture is subject to masquerading by anyone with a legitimate user's device and the need for intervention by the owner of the service. In the architectures proposed in [20], [21], an authentication challenge to a registered device is sent via a trusted module, whenever an attempt to access a web service occurs in order to allow the user to either accept or deny the access using the registered device. The architecture requires the said web services to be integrated with it (meaning that existing servers need to be enhanced). It is also more for preventing fraud than for letting a user authenticate to a webserver using a smart device. Our work differs from both these architectures in three aspects. First, SESAME uses the smart device as a means of tying a user's digital identity to her physical identity, by using biometrics to encrypt her digital credentials on the smart device as well as to provide access to them. Second, by removing the need for a human to memorize passwords SESAME encourages the use of complex passwords. Third, SESAME does not require trusted modules or integration with web services.

EtherTrust [22] and the work in [23] proposed a cloud service based authentication scheme for a web service via NFC on a user's registered smartphone. The RFID reader component on the Host Terminal contacts a central key server via the smartphone's Internet connection to retrieve the requisite password. This however requires the smartphone to have Internet connectivity and in addition, the user to store all her passwords on the central server. In SESAME, all passwords

are stored on the user's smartphone which many users may find it convenient rather than using a third party facility. Another related architecture is BioLink [24], which provides access to web services via biometric authentication. However, it requires the use of a dedicated fingerprint reader attached to the Host Terminal which is circumvented in SESAME by using a smart device, thus allowing access to a user on any Host Terminal.

D. Strengths

SESAME abstracts the user from having to choose and change her passwords regularly in cases where such policies are enforced by a SP (such as enterprise security). Since SESAME encourages the use of strong passwords, such schemes might not be necessary in the first place. In fact by using SESAME, Service Providers can themselves send complex passwords to users, who can then store them on their smart device. In the future, the use of biometric hash to register and authenticate users will eliminate such policies. Similarly, since in the SESAME architecture all passwords are stored on a portable device, it also addresses the case of a "roaming" user requiring access to her credentials. Another strength of SESAME is that it can be adapted to simplify reservations and control access in Cyber Physical Systems (CPS) such as hotel room reservations, car services, smart grid security, etc. This architecture of SESAME is however beyond the scope of this paper.

V. Conclusions

In this paper, we have identified two main problems with textual password based authentication schemes and designed a smartphone based solution called SESAME that addresses them by incentivizing the usage of strong passwords effortlessly. By using biometrics, SESAME secures the weakest link which is the human computer interaction in present day's web service authentication. Our architecture eliminates all the shortcomings of textual passwords while augmenting simplicity. In addition to this, we have developed a working prototype that validates our design and also designed protocols which open an avenue for the integration of biometrics with web based authentication schemes and cyber-physical systems such as access to hotel rooms and rental cars. Our future work includes the implementation of a variety of SESAME apps and evaluating performance of the protocols by real experimentation.

VI. Acknowledgment

Shambhu Upadhyaya likes to thank the U.S. Department of Defense (Grant No. H98230-11-0463) for the support provided to him. Usual disclaimers apply.

References

[1] A. Adams, M. Sasse, and P. Lunt, "Making passwords secure and usable." *People and Computers*, pp. 1–20, 1997.

[2] P. Inglesant and M. Sasse, "The true cost of unusable password policies: password use in the wild." in *Proceedings of the 28th international Conf. on Human factors in computing systems*. ACM, 2010, pp. 383–392.

[3] R. Shay and E. Bertino, "A comprehensive simulation tool for the analysis of password policies." *International Journal of Information Security*, vol. 8, no. 4, pp. 275–289, 2009.

[4] J. Stanton, K. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors." *Computers & Security*, vol. 24, no. 2, pp. 124–133, 2005.

[5] S. Komanduri, R. Shay, P. Kelley, M. Mazurek, L. Bauer, N. Christin, L. Cranor, and S. Egelman, "Of passwords and people: Measuring the effect of password-composition policies." in *Proc. of the 2011 annual Conf. on Human factors in computing systems*. ACM, 2011, pp. 2595–2604.

[6] A. Brown, E. Bracken, S. Zoccoli, and K. Douglas, "Generating and remembering passwords." *Applied Cognitive Psychology*, vol. 18, no. 6, pp. 641–651, 2004.

[7] B. Ives, K. Walsh, and H. Schneider, "The domino effect of password reuse." *Communications of the ACM*, vol. 47, no. 4, pp. 75–78, 2004.

[8] D. Feldmeier and P. Karn, "Unix password security-ten years later." in *Advances in Cryptology CRYPTO89 Proc.* Springer, 1990, pp. 44–63.

[9] Y. Zhang, F. Monrose, and M. K. Reiter, "The security of modern password expiration: an algorithmic framework and empirical analysis." in *Proceedings of the 17th ACM Conf. on Computer and communications security*, ser. CCS '10. New York, NY, USA: ACM, 2010, pp. 176–186.

[10] B. Laxton, K. Wang, and S. Savage, "Reconsidering physical key secrecy: Teleduplication via optical decoding." in *Proceedings of the 15th ACM Conf. on Computer and communications security*. ACM, 2008, pp. 469–478.

[11] M. Backes, M. Durmuth, and D. Unruh, "Compromising reflections-or-how to read lcd monitors around the corner." in *Security and Privacy, 2008. SP 2008. IEEE Symposium on*. IEEE, 2008, pp. 158–169.

[12] F. Tari, A. Ozok, and S. Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords." in *Proceedings of the second symposium on Usable privacy and security*. ACM, 2006, pp. 56–66.

[13] M. Sasse, S. Brostoff, and D. Weirich, "Transforming the weakest linka human/computer interaction approach to usable and effective security." *BT technology journal*, vol. 19, no. 3, pp. 122–131, 2001.

[14] S. Salerno, A. Sanzgiri, and S. Upadhyaya, "Exploration of attacks on current generation smartphones." *Procedia CS*, pp. 546–553, 2011.

[15] A. Beaufour and P. Bonnet, "Personal servers as digital keys." in *Proceedings of the Second IEEE International Conf. on Pervasive Computing and Communications (PerCom'04)*, ser. PERCOM '04. Washington, DC, USA: IEEE Computer Society, 2004.

[16] F. Zhu and M. W. Mutka, "The master key: A private authentication approach for pervasive computing environments." in *Fourth IEEE International Conf. on Pervasive Computing and Communications (PerCom06*, 2006, pp. 212–221.

[17] L. Bauer, S. Garriss, and M. K. Reiter, "Efficient proving for practical distributed access-control systems." in *Computer Security—ESORICS 2007: 12th European Symposium on Research in Computer Security*, ser. Lecture Notes in Computer Science, vol. 4734, Sep. 2007, pp. 19–37.

[18] L. Bauer, L. F. Cranor, M. K. Reiter, and K. Vaniea, "Lessons learned from the deployment of a smartphone-based access-control system." in *SOUPS '07: Proc. of the 3rd Symposium on Usable Privacy and Security*, Jul. 2007, pp. 64–75.

[19] L. Bauer, S. Garriss, and M. K. Reiter, "Distributed proving in access-control systems." in *Proc. of the 2005 IEEE Symposium on Security and Privacy*, May 2005, pp. 81–95.

[20] "Smartphone-based authentication:apps." 2011. [Online]. Available: http://www.msec.be/wiscy/ws2011/talks/talk_boukayoua.pdf

[21] "The Authentication Revolution: Phones Become the Leading Multi-factor Authentication device." 2012. [Online]. Available: http://www.phonefactor.com

[22] "Ethertrust, trust your digital life." 2012. [Online]. Available: http://wwww.ethertrust.com

[23] J. K. W. Michael T. Lundy, "Utilizing a mobile device to operate an electronic locking mechanism." US Patent US 8 037 511, October 11, 2011. [Online]. Available: http://www.google.com/patents/US8037511

[24] "Biolink Idenium." 2012. [Online]. Available: http://biolinksolutions.com/biometric-authentication-active-directory/