Towards Improving Usability of Authentication Systems Using Smartphones for Logical and Physical Resource Access in a Single Sign-On Environment

G. Carullo, F. Ferrucci, F. Sarro[1]

Abstract The design of authentication methods raises crucial questions on how to solve conflicts between security and usability goals, that are at opposite ends of a "see-saw". As a matter of fact, the usability of security systems has become a major issue in research on the efficiency and user acceptance of security systems. An authentication is more strong as more tokens are involved in authentication process. The main disadvantage is that users need to purchase and keep with them several tokens and cards. To address the above issues, we propose a two factors authentication scheme that allows users to employ their smartphones as unique authentication token providing access to both online and physical resources in a user-friendly and secure manner.

Introduction

Most of the Internet services serve users carrying out human-oriented processes and often requiring authentication mechanisms for different reasons, such as privacy, access to logical or physical resources, and so on. Thus, the design of usable yet secure authentication methods raises crucial questions concerning how to solve conflicts between security and usability goals. As a matter of fact, the usability of security systems has become a major issue in research on the efficiency and user acceptance of security systems [1]. As an example, conventional static password-based authentication systems are widely used in several applications, but users often employ authentication keys easy to remember and to guess or the same username-password couple for different services. These typical user behaviors strongly reduce the security of an already weak authentication mechanism. In many security-oriented environments this low level of safety is not acceptable, thus it is important to improve the quality and robustness of the adopted access control me-

[1] University of Salerno, Fisciano (SA), Italy, {fferrucci, fsarro}@unisa.it

chanisms. To this end, the National Institute of Standards and Technology (NIST) proposed several guidelines to ensure that a certain desired security level is met using “tokens” [2]. Tokens are physical or logical items that the claimant possesses and controls and may be used to authenticate claimant's identity. The NIST categorization of tokens is: *something you know*, like password or Knowledge-based Authentication (KBA), *something you have*, like an ID badge, a cryptographic key, or a digital certificate, and *something you are*, like a voice print, facial pictures, and other aspects involved in biometric-recognition. An authentication process gets stronger as more tokens are involved. For example, a “two factor authentication” checks at least two tokens, such as something that the user know and something that he/she has. However, this kind of authentication requires that users need to purchase and keep with them several tokens and cards to access online and physical resources, thus impacting on usability of the authentication systems.

To address these issues, in this paper we propose an authentication scheme that allows users to employ their smartphone as unique authentication hardware token providing access to both online and physical resources. In particular, we intend to achieve several goals: increasing security level enforcing a two factor authentication; reducing hardware complexity by using only one hardware token; improving usability and being applicable in real-world scenarios; being easy to use by non-expert users to discourage bad practices (e.g., writing passwords on notes or reusing the same password) that may decrease the security level; being backward compatible to be usable even in environments that cannot be upgraded for either technical or policy reasons; it should not require additional specialized hardware.

The rest of the paper is organized as follows. We first give some technical details needed to understand the proposed authentication scheme and then describe the proposed solution providing architectural details and a sample use-scenario. Security threats and countermeasures are also discussed followed by related work. Final remarks and future work close the paper.

Technical background

We provide a brief explanation of Single Sign-On (SSO) mechanism [3] and of one of its implementation, namely the Shibboleth System [4]. SSO is an authentication mechanism whereby a single action of user authentication and authorization allows him/her to access all systems where he/she has access rights, without the need to enter multiple passwords. Thus, SSO both splits the complexity of architecture security and helps security workers to reduce the gap between security and usability. Several protocols can be used to manage SSO, such as Shibboleth and OpenID [5]. We chose Shibboleth because of its flexibility, robustness, and widespread usage. It works as follows: when a user visits web resources protected by a Service Provider (SP), he/she needs either to have a valid Shibboleth session (i.e.,

he/she is already authenticated) or to authenticate himself/herself. In the latter case, the SP redirects the user's browser to the Where Are You From (WAYF), which presents the user with a list of organizations whose users may access to the resources. The user chooses one of the listed organizations and he/she is redirected to his/her Identity Provider (IdP). The user can log in submitting his/her credentials to the IdP accordingly to the sign-on method the home organization chose. If the user is successfully authenticated, he/she will be associated to specific attributes, such as his/her username, roles that he/she covers, etc.. Thus, the IdP component sends the browser back to the original resource web site and sends to the SP a message that contains the authentication statement and the user's attributes. Thus, the SP processes the message and, if the provided credentials match the service's access control policy, a new Shibboleth session is instantiated for the client. The browser requests again the protected resource and the user can access to it.

The proposed approach

The authentication scheme we proposed extends Shibboleth capabilities to grant online and physical resources access using a smartphone as unique hardware token (something you have) with a password or others tokens established by the IdP (usually something you know). This allows us to be backward-compatible, enabling a wide usage of the solution without changing the existing IdP. Moreover, since usability is our main goal, off-the-shelf smartphones combined with an SSO mechanism lets us significantly improve system usability. Indeed, the user does not need to remember more than one password and he/she does not need to carry multiple tokens to authenticate to different systems. To perform physical access, session data are transferred from the smartphone to the authentication terminals using an optical recognition system based on 2D bar-codes called QR-codes. This lets us to expose a smaller attack surface to possible eavesdroppers that may stay close to the user while he/she enters his/her credentials. Fig. 1 shows some snapshots of the client-side software that runs on smartphones using Google Android, but that can be easily ported to other mobile phone operating systems. The *Login* functionality (Fig. 1.a) lets users to authenticate themselves in case of the SP is already configured to communicate directly with a certain IdP. Otherwise users can exploit the embedded web browser clicking on *Custom login* to start the Shibboleth-process. All configurations can be done touching *Configure*. After a successful authentication, the application shows the main menu (Fig. 1.b) and through it users can load the QR-code needed to access physical resources (*Get QR-code*), can reconfigure their SP (*Configuration*), or can surf the Internet to access logical resources (*Navigate*).

In the sequel we detail how the authentication scheme works showing how the involved components interact each other and providing an example of usage.

a) b)

Fig. 1. Some application snapshots

Architecture details

To authenticate users through a mobile phone, only two requirements must be satisfied: users have to use a smartphone both connected to the Internet and with a working SIM card, while the IdPs need to use an LDAP server [6] to store users' IMEI (International Mobile Equipment Identity) and IMSI (International Mobile Subscriber Identity) which are unique identifiers associated to mobile phone and SIM card, respectively. Fig. 2 shows the architecture underlying the proposed authentication scheme. The smartphone software application, needed for starting the authentication process, is composed by two modules: the *Authentication Module* and the *Android Session Handler*. The first one transparently manages the HTTP communication with the configured SP and the relative IdP accordingly to the Shibboleth protocol (1-2), by letting the user to authenticate himself/herself via HTTPS. If the application is configured to use a statically known SP, the authentication process is carried on automatically: the mobile application will send a first request to an ad hoc protected resource on the *Service Provider First Access* to start the identification and the user has only to input his/her credentials that will be checked by the IdP (3). If the application is not configured to use a specific SP, the user can exploit the web browser embedded in the application to connect to his/her preferred SP and log in using his/her credentials. For simplicity, we suppose that the mobile application is configured to interact with our SP, but it can be statically changed or be chosen at run time via our embedded web browser.

Until the session expires, the user can request to the smartphone application a QR-code, representing his/her current Shibboleth session that can be then exploited for physical access. Indeed, The *Android Session Handler* generates the QR-code that contains the Shibboleth cookie, needed to associate users to a valid Shibboleth session and the IMEI and IMSI identifiers. When a user wants access

to a restricted physical environment, he/she only has to show the QR-code displayed on his/her mobile phone to the webcam (4) of the *Authentication Terminal* that is located in the building that he/she wants access to. The *Webcam Capture Module* captures the QR-code and communicates it to the *QR-code Recognition Module*, also running on the *Authentication Terminal*. This module decodes the data stored in the QR-code and sends it to the *HTTPS Session Handler*. Notice that QR-code changes mirroring Shibboleth-cookie, so a certain QR-code is valid only until the session expires. The *HTTPS Session Handler* transforms the received data into web cookies and tries to access to the resource protected by the *SP Physical Access* (5). The *SP Physical Access* requests IMEI and IMSI to the IdP (6) and compares them to the ones provided by the *Authentication Terminal*. If they match and the received cookies represent a valid Shibboleth session, it grants access to the requested resource. Organization's access policies can be easily plugged into the *SP Access Control Module* (7) to check other attributes before granting access, such as time or other information relative to the user that is trying to access to protected resources. The final page redirection is handled by the *Authentication Terminal* (8) that can, for example, unlock a door to let the user enter the building.

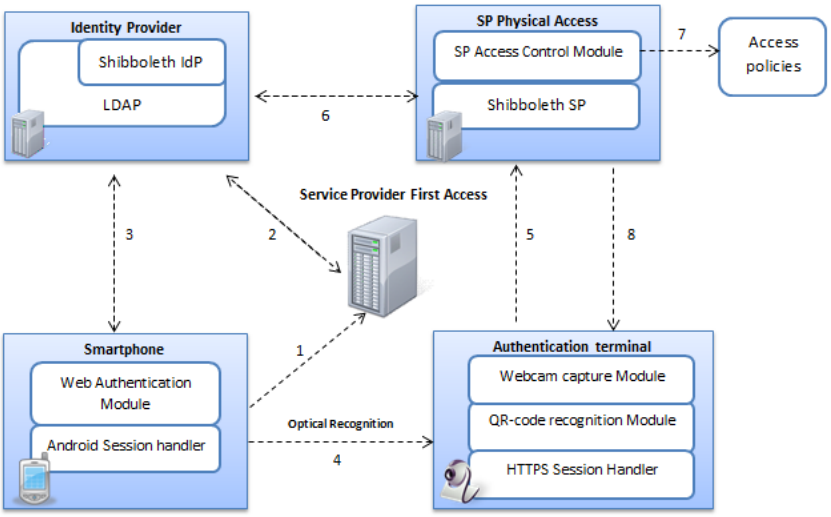

Fig. 2. The proposed protocol

Example

The proposed authentication system is very flexible and can be applied within several organizations' information systems in which a physical access is required to protected resources (e.g., laboratories, documentation), such as higher-education institutions, consulting firms or governmental buildings access. As an example, in Fig. 3 a scenario where several consulting firms provide different ser-

vices to many other organizations is depicted. The workers of a firm can access to all (or to a part of) the resources of a certain organization in agreement with its access policies. For example, *Worker2* of *FirmA* is a legal counselor of both organizations 1 and 2 thus he/she can access to their documents, while *Worker1* is a computer technician and can access only to the organization's laboratory. The access will be denied to any unauthorized person, such as an intruder or a person who works for a consulting firm which is not related to another organization and cannot access to its resources (e.g., *Worker3*). The scenario highlights several advantages of our proposal for both end-users and organizations: (i) users can manage their identities in a simple way enjoying a higher protection; (ii) it is globally available; (iii) organizations can easily integrate the system into their existing Shibboleth-based solutions, saving costs for upgrade; (iv) it enables a finer-grained control on user accesses.

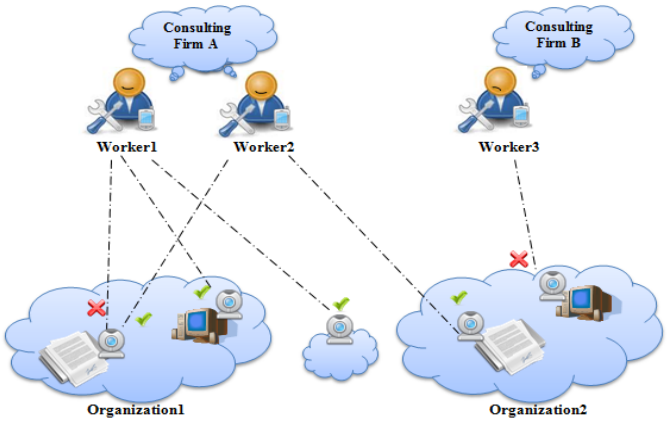

Fig. 3. A consulting firm sample scenario

Security evaluation

In this section a security evaluation of the proposed authentication scheme is discussed showing how the solution resolves possible threats. Threats related to the *password authentication* (usually adopted by IdPs) concern attackers trying to guess or steals user's password via social engineering or using malicious software such as keystroke logger. To avoid such threats a two-factor authentication was exploited, thus attackers require both tokens in order to reconstruct the necessary information. Moreover, passwords are not shown as plaintext, while it is up to the user to look at the permissions during the installation of a new keyboard and to be sure of what he/she is installing; otherwise to completely avoid the problem, the software keyboard installation function can be completely disabled. There are several threats related to the *user device*: (i) attackers might steal a mobile phone (or IMEI and IMSI) to impersonate a valid user; (ii) attackers might try to guess IMEI

and IMSI; (iii) attackers might install on the mobile phone a malicious software that tries to steal Shibboleth Session. In the first case, the two-factor authentication allowed us to prevent the attack. In addition, IMEI and IMSI are hard to guess, so we prevent the second threat too. To thwart brute force attacks, up to three unsuccessful authentications are allowed, after that the access is denied to the user. Moreover, no application has permission to read or write the user's private data or other application's files, to perform network access, etc., thus Shibboleth's cookie is accessible only inside our application. To prevent threats related to the *internet connection* (i.e., attackers might try to spoof sensitive information over the network or to mount a man-in-the-middle attack) it was secured with TLS. Finally, concerning threats related to the *QR-code authentication*, attackers staying close to the screen which displays the QR-code might try to steal information or to guess QR-code. These attacks are hard since, on the one hand, it is not feasible for a person to recognize information stored into a QR-Code and, on the other hand, brute force attacks are not allowed as we explained before.

Related Work

Several works in the literature have focused on using smartphones as hardware token for authentication systems providing logical or physical resources access. However, to the best of our knowledge, our approach is the first that aims to grant both logical and physical resources access in an SSO environment taking into account also usability issues. In the following, we outline a selection of previous research works. Concerning authentication systems to grant access to physical resources, in [7] the authors exploit mobile phones to control admittance services. In particular, they propose to use Near Field Communication (NFC) [8], which is a low-power and short-range wireless interface, to enable SIM cards as security tokens, while the authentication process is carried out via GSM. However, NFC is not available on most of existing mobile phones thus limiting the applicability of this approach. With the same aim Tsai and Hung [9] proposed to use digital keys on Bluetooth-enabled mobile phones together with an SMS-based authentication. The authentication relies on NFC showing the same limitation of [7]. As for secure access to logical resources, Hallsteinsen *et al.* [10] proposed the use of both mobile phones and computers exploiting GSM network and SMS-based communication to perform authentication based on Java Middlet. Thanh *et al.* [11] describe a SIM-based authentication system involving Bluetooth and specialized hardware, such as USB dongle, card readers, and GPRS/3G PC card, to access directly to the information stored in the SIM card. As we said, the use of additional hardware can impact on system usability. Moreover, many of these works provide on-line authentication, thus the mobile phone used as token needs constant access to GSM or similar networks, whereas our system accesses to the network only when the first log in occurs (until timeout expiration).

Conclusions and future work

In this paper, we proposed a novel approach for authentication systems, for both logical and physical resources, based on SSO. We showed how to turn a smartphone into a user-friendly and secure authentication token. The proposed approach avoids some security weakness, such as the possibility of shoulder surfing attacks, guessing attacks, and more other common attacks. The solution can be easily integrated into all already existing Shibboleth-based services. Let us stress that since we use Shibboleth, all organizations can easily add their additional access policies into our solution. As future work we plan to evaluate the usability of our system on a wide scale and exploit the obtained experimental results to formulate metrics that allow us to better control security and usability aspects. On the implementation side, we want improve the portability of our system, by realizing the smartphone client on different operating systems, and its usability, by providing a flexible interface to automatically interact with custom IdP pages.

ACKNOWLEDGMENTS. We wish thank Prof. E. Feustel for his valuable suggestions and insightful comments.

References

1. Ben-Asher, N., Meyer, J., Moller, S., Englert, R. (2009) An Experimental System for Studying the Tradeoff between Usability and Security, Procs. Int. Conf. on Availability, Reliability and Security: 882-887.
2. NIST U.S. Department of Commerce (2008) Electronic Authentication Guideline Information Security, Special Publication 800-63-1.
3. Pashalidis A., Mitchell C. (2003) A Taxonomy of Single Sign-On Systems, Information Security and Privacy, Lecture Notes in Computer Science, 2727/2003, 21: 249-264.
4. Scavo T., Cantor,S. (2005) Shibboleth architecture technical overview, available at http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-tech-overview-latest.pdf
5. Recordon, D., Reed, D. (2006) OpenID 2.0: a Platform for User-Centric Identity Management, Procs. Procs. Second ACM Workshop on Digital Identity Management: 11-16.
6. Koutsonikola, V., Vakali, A. (2004) LDAP: Framework, Practices, and Trends, IEEE Internet Computing, (8) 5: 66-72.
7. Noll, J., Calvet, J.C., Myksvoll, K. (2006) Admittance Services through Mobile Phone Short Messages, Procs. Int. Conf. on Wireless and Mobile Communications: 29-31.
8. NFC Forum (2008) http://www.nfc-forum.org
9. Tsai, C.-S., Hung, C.-I. (2010) An enhanced secure mechanism of access control, Procs. Int. Conf. on Communication Systems, Networks and Applications:119-122.
10. Hallsteinsen, S., Jorstad, I., Thanh, D.V. (2007) Using the Mobile Phone as a Security Token for Unified Authentication, Procs. Int. Conf. Systems and Networks Communication: 68.
11. Thanh, D.V., Jonvik, T., Jorstad, I. (2006) Enhancing Internet Service Security Using GSM SIM Authentication, Procs. Global Telecommunications Conference, IEEE: 1-5.