Covert Channels Can Be Useful! – Layering Authentication Channels to Provide Covert Communication*

Mohammed H. Almeshekah, Mikhail J. Atallah, and Eugene H. Spafford

Purdue University CERIAS
656 Oval Drive, West Lafayette, IN 47907, USA.
{malmeshe,matallah,spaf}@purdue.edu
http://www.cerias.purdue.edu

Abstract. This paper argues the need for providing a covert back-channel communication mechanism in authentication protocols, discusses various practical uses for such a channel, and desirable features for its design and deployment. Such a mechanism would leverage the current authentication channel to carry out the covert communication rather than introducing a separate one. The communication would need to be oblivious to an adversary observing it, possibly as a man-in-the-middle. We discuss the properties that such channels would need to have for the various scenarios in which they would be used. Also, we show their potential for mitigating the effects of a number of security breaches currently occurring in these scenarios.

Keywords: Authentication, Server Impersonation, Back-channels, Phishing

1 Introduction

Whereas many current research efforts in improving authentication seek to develop stronger credentials and better management of these credentials, we are not aware of a facility for giving users and their service providers a login flexibility beyond the usually implied "this username requests to access to the system." Service providers (such as banks, brokerages, etc) provide all-or-nothing access: A customer who merely wants to check her balances and positions (i.e., read-only access) cannot do so without implicitly obtaining the authority to carry out transactions (including money transfers), and the authority to administer the account (including changing the physical address of record, the email address of record, etc). Ideally, in this situation, there should be three levels of access: One that allows only viewing account balances, another that also allows

* This is a preprint of the paper in "Proceedings of the 21st International Workshop on Security Protocols," F. Stajano and J. Anderson, eds.; published and ©in 2013 by Springer-Verlag. The final version appears at http://springerlink.com.

currying out transactions, and the highest one that also allows account administration. Compromising the credentials of the read-only level would not give the adversary full control over the user's account, and would limit the damage done during the time it takes for the victim and bank to realize that a phishing attack has happened. Contrast this to the current deployed systems, where a victim of phishing would grant the adversary all of these privileges at once, even if the victim wanted "read-only" access (e.g., because the phishing email containing a link to a phishing site invited the victim to "view an important message").

A customer who knows she is "taking a risk" by logging in from a public place, with possibilities of shoulder-surfing and/or of hidden CCTV cameras, should really be given the option of a degraded form of login (the "read-only" kind). The question then arises, why is such a 3-level login facility not provided by financial institutions, even though the liability from a phishing attack often falls more on them than on the imprudent customer? The obvious answer is that no customer would want to memorize three passwords for each institution they do business with. Customers are having enough of a hard time managing their current passwords where the ratio is one-to-one. We argue that there is a way to have the benefits of the 3-level access, without the burden of increasing the number of passwords users have to manage.

2 Preliminary Solution

This section presents a simple first step towards achieving the goal of conveying extra information to the server, beyond the all-or-nothing access that is implicit in every login made in currently deployed systems. In what follows, for convenience we use financial institutions in our examples, but this entails no loss of generality as the discussion applies equally well to any service provider.

2.1 A Simple Proposal

We propose a login mechanism such that:

1. The interface is similar to those currently deployed, namely, with two fields, one for entering a username and the other for entering a password, and
2. What is entered in the password field does not tax the user's memory significantly more than in currently deployed systems, and
3. What a shoulder-surfer or eavesdropper observes when the user enters her credentials reveals no information as to what covert message is being sent, other than the usually implied "this username wants to login."

To achieve the second requirement, we propose that the user enters, in the password field, the regular password (the same thing users enter today) followed by a space, and then followed by a word that conveys the secret message to the bank. In the 3-level access example we discussed, this could be one of three words $\{w_1, w_2, w_3\}$ that are (i) trivially memorizable by the user, and (ii) have

a natural total ordering in that particular user's mind. For example, the three words could be the names of the 3 first dogs of that customer, or of three soccer teams, or of three makes of cars. Accidental mis-typing (that results in a word that is outside the pre-agreed set) would result in a failed login, with the necessity to re-enter username, etc. The only constraint on these three words is that the edit distances among them should be greater than one typographic error. This is essential so that mis-typing one of them does not accidentally result in sending another one. A shoulder-surfer (or a ceiling CCTV camera) that captures what the user entered would of course be able to replay it, but would not get a higher access level.

The above simple scheme does not reveal to a shoulder-surfer the nature of the secret message being sent to the bank through the memorizable word. Even a shoulder-surfer who is a customer of the same bank (and we should assume such an adversary) may not know that the covert message pertains to a choice of access-level, because the bank customer may have chosen to use the covert-messaging facility for something completely different than access-level selection. We discuss below the possibilities of sending other covert messages to the bank.

2.2 Conveying Other Messages

Once financial institutions make such a login facility available, its possible uses include many other scenarios other than the 3-level access used above to introduce the rationale for such a mechanism. Some customers may not care at all about 3-level access: Such customers might decide to never click on an email link, therefore never fall prey to phishing. They might also never take any risk when logging in from public places. Such a customer may set her account up so that the trivially memorizable word(s) that comes after the password covertly convey to the bank different courses of action(s) that the bank is supposed to take following the login. The scheme can also be extended to provide k-level access, with $k > 3$, although the costs in storage and user memory increase accordingly.

Conveying Duress One such possibility is conveying to the bank one of the following two messages: (i) "this is a normal login and I request full access"; or (ii) "I am under duress, pretend that access is granted but call the police immediately and inform them that I am under duress." As discussed in [1, 2], if the user is under duress then the adversary will demand to know, under threat of violence, how the user conveys both messages (i) and (ii). As explained in [2], there is a way for the user to appear to comply while giving the adversary what will trigger message (ii) only (if the adversary attempts to use it). For example, the agreement with the bank could be that "bulldog" is the word for message (i), and any other dog breed is for message (ii). Typos result in denied access (no accidental police-calling because of a typo). An adversary who is given wrong information, such as poodle for message (i) and any non-poodle dog for message (ii), has no way to tell whether a signal will be sent to the bank or not.

Indirectly Exposing Phishing There is no way for the victim of an ongoing phishing attack, made possible as a result of the user's unwisely clicking on a link in a phishing email from the "bank," to directly inform the bank of this fact. However, the user can unwittingly (and indirectly) alert the bank to this fact if one of the few covert messages in her repertoire is "I am doing this login because you solicited it in an email to me." If such a covert message is sent to the bank's server it indirectly alerts the bank of the high likelihood of an unfolding phishing attack. Because the bank knows whether it solicited a conniption or not – many banks never send email-embedded links as a matter of policy – it can conclude whether the user has fallen for a phishing attack. As a result of that, an active man-in-the-middle attack resulting from the successful phish only compromises a degraded version of the login that (indirectly) alerts the bank. The bank can call the customer and ask for a change of password and provide advice so as to avoid a repeat occurrence of the episode. This is not a sure-fire defense and several things can still go wrong but it provides an improvement over the current situation where the bank is oblivious of such an attack, even though it may stand to suffer damages from it more than the customer; in some countries financial institutions are required to charge-back the customers accounts when they fall prey to a phishing attack if the customers acted in good faith.

Phishing is characterized by the discrepancy between what the user thinks (that the bank sent an email urging access via a provided link) and the bank's state (that it sent no such link). Providing a way for users to express their state serves to indirectly alert the bank and prompt it to take some precautionary measures. Such measures can include contacting the user to verify a sensitive transaction and/or giving the user limited access thus minimizing the damage caused by an adversary. Furthermore, the bank can direct the adversary to a honeypot account and alert the user, using out-of-band communication channels, so that the adversary can be monitored and possibly identified for prosecution.

A more sophisticated system can be designed following the same structure in [2] where a third party monitoring user logins is only alerted if the user signals a solicited login as a result of a phishing attack. Such a third party would learn nothing about the identities and activities of the users during normal logins and will only be alerted in case of phishing. We can imagine such a security and business model of combatting phishing led by third-party companies.

2.3 Using other channels than the password field

The password field is not the only channel for conveying a covert message to the server; we next give examples of other authentication channels that can be used for that purpose.

Biometrics Some biometrics can be used as the communication channel depending on how much control the user has on the selection of the biometric and its mode of use. For example, when using an iris scan the user has limited choice, but when using fingerprints the user may send a covert message by the choice of

finger to use. Furthermore, for a given finger the user may be able to convey a message through the tilt of the finger relative to the fingerprint reader.

Multi-factor Authentication Two-factor authentication has been widely adopted, especially in financial institutions. It increases security but remains vulnerable to server impersonation and other sophisticated attacks such as those used by the Zeus malware [6]. Not only is our proposal still relevant in a world of multi-factor authentication, but the multiplicity of factors provides a new mechanism for covert communication. The choice by the user of which factors to use can be used as the covert communication mechanism. For example, if three factors are available and a minimum of two are required, then the user's choice of which factor to leave out sends a covert message to the server.

2.4 Channel capacity

Psychological and user-acceptance considerations dictate that covert messages be encoded in unary: If three bits can be sent then three (and not the usual 2^3) distinct covert messages can be sent to the server. In fact we argue that, even if $k > 3$ bits can be sent (e.g., by the user's choosing of $k - 1$ out of k possible factors to authenticate), in practice it will not be practical for the typical user to send more than a very small number of bits (possibly as low as 3, but that number is best determined experimentally with user studies).

2.5 Credentials-sharing

It is ill-advised to share access credentials (such as a password) with others, yet people do it all the time for the sake of convenience. For example, doctors or managers share their passwords with a nurse or secretary so they can avoid the inconvenience of using a (possibly unwieldy) patient-management or enterprise-resource-planning software system. For password-based systems, a service provider can gain a competitive advantage by offering those customers who choose to share their access credentials the ability to share lower forms of access credential (e.g., "read-only" with their tax-accountants).

3 Desiderata for a Better System

The scheme that implements the covert channel needs to have more sophisticated features than the simple ones discussed above. We discuss these features in the following paragraphs.

3.1 Obliviousness

An electronic eavesdropper should neither learn nor be able to re-use the recorded client responses (even for, e.g., repeating the low form of "read-only" login that

the user executed). Achieving this means that the server, upon receiving a login request, must use a nonce that affects what the user's client software sends to the server. A replay would then be useless because at the next login the server will generate a different nonce and will expect a different response. The simple scheme's user interface would still be used, but it would need to be processed by client software (that would use it together with the nonce received from the server to generate the response sent to the server). Such obliviousness is best implemented within, for example, the WWW browser itself, as using plugins would imply a lack of mobility, but this assumes the client is running trusted software.

3.2 Resistance to Server Compromise

An adversary who gets a copy of the information stored in the server's credentials file (e.g., /etc/passwd/) should not gain more information than in currently deployed systems. In the scheme discussed earlier, where a password is followed by an easy-to-memorize word, neither the password nor the easy-to-memorize words are vulnerable to a dictionary attack. This is of more importance with the latter as they are likely to be dictionary words (because they need to be trivially memorizable by the user).

3.3 Resistance to Persistent Adversaries

The scheme should assume that the adversary is persistent in seeking access to the user's account, and the adversary will continuously try until he succeeds unless specifically prevented by the underlying scheme. In the case of an attack involving coercion the adversary can demand all the possible login credentials and try them until he succeeds. In phishing attacks, the adversary might launch a number of different attacks through a different number of vectors, e.g., a phishing email, a Facebook message, and an IM message.

4 Further Remarks

A grand vision for authentication has been sought for a number of years, of users having a small number of identities to login to the many heterogeneous service providers, with full control on the user side [3]. Such a vision has been articulated in the National Strategy for Trustworthy Identities in Cyberspace (NSTIC), with cell phones serving as a central hub for client online identities [7]. Such a mechanism addresses many of the security and privacy problems associated with online identities, but it does not render unnecessary what we are proposing: A cell phone hub would become a more tempting target for evildoers, and would benefit from what we propose (especially in cases of physical coercion against the phone's owner).

The features and properties of a covert communication channel as we describe deserves further investigation along many dimensions, including:

1. *Cryptographic:* How to best achieve the desired obliviousness and resistance to server compromise, without degrading the ability and performance of the necessary credentials-checking at login time?
2. *Psychological:* Which parameters of such a system would be acceptable to users, and (if acceptable) would not cause too many errors and false alarms after deployment?
3. *Risk analysis and Economics:* Would such a system decrease the overall risk to the service provider, and by how much. What is its effect on the liability insurance rates of the service provider? Are here any hidden and costly unintended consequences?

Many questions will need answering, but we believe that the overall outcome of such investigations will be favorable to our general approach along all of the above-mentioned dimensions.

Acknowledgments Portions of this work were supported by National Science Foundation Grants CNS-0915436, CNS-0913875, Science and Technology Center CCF-0939370; by an NPRP grant from the Qatar National Research Fund; and by sponsors of the Center for Education and Research in Information Assurance and Security. The statements made herein are solely the responsibility of the authors.

References

1. Clark, J. & Hengartner, U. Panic Passwords: Authenticating Under Duress, In Proceedings: The 3rd Conference on Hot Topics in Security, USENIX Association, (2008).
2. Stefanov, E. & Atallah, M. Duress Detection for Authentication Attacks Against Multiple Administrators. In Proceedings: The 2010 ACM Workshop on Insider Threats, ACM, pp. 37-46, (2010).
3. Can we fix the security economics of federated authentication?, In Proceedings: The 19th international conference on Security Protocols, Springer-Verlag, pp. 33-48, (2011).
4. Molloy, I., Li, J. & Li, N. Dynamic Virtual Credit Card Numbers, In Proceedings: Financial Cryptography, pp. 208-223, (2007).
5. Phishing Activity Trends Report - 1st Quarter 2012 Anti-Phishing Working Group, July (2012), `http://www.apwg.org`.
6. Trend Micro, How ZeuS/ZBOT Bypasses Two-Factor Authentication, October (2010), `http://community.trendmicro.com/t5/Web-Threat-Spotlight/ZeuS-ZBOT-Variant-Bypasses-Two-Factor-Authentication/ba-p/16514`.
7. The White House, National Strategy for Trusted Identities in Cyberspace (NSTIC), (2011).