CERIAS

The Center for Education and Research in Information Assurance and Security

Layering Authentication Channels to Provide Covert Communication

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

The Problem and Motivation

Service providers (such as banks) provide *all-or-nothing access*: A customer who merely wants to check her balances (i.e., read-only access) cannot do so without implicitly obtaining the authority to carry out sensitive transactions (including money transfers and changing the physical address of record. Ideally, in this situation, there should be three levels of access: One that allows only viewing account balances, another that also allows 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.

Why is such a multi-level login facility is not provided by financial institutions?

No customer would want to memorize three passwords for each institution they do business with as they 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.

Preliminary Solution

We propose a login mechanism such that:

1. The interface is similar to those currently deployed (username and password),
2. What is entered in the password field does not tax the user's memory, 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.

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, 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.

Improved Authentication Process:

- Accidental mis-typing (that results in a word that is outside the pre-agreed set) would result in a failed login.
- 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.
- It does not reveal to a shoulder-surfer the nature of the secret message being sent to the bank.

Desiderata for a Better System

Obliviousness

An electronic eavesdropper should neither learn nor be able to re-use the recorded client responses.

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. 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).

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.

Conveying Other Messages

Conveying Duress

One 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”. 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). 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).

Indirectly Exposing Phishing

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. The user can 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”. 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.

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 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).

Conclusion

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 \cite{fix_econ_fed_id}. 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 \cite{nstic}. 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).