TwoKind Authentication: Usable Authenticators for Untrustworthy Environments

Katelin Bailey Linden Vongsathorn Apu Kapadia Chris Masone Sean W. Smith

Department of Computer Science
Dartmouth College
Hanover, NH 03755, USA

ABSTRACT

The ease with which a malicious third party can obtain a user's password when he or she logs into Internet sites (such as bank or email accounts) from an insecure computer creates a substantial security risk to private information and transactions. For example, a malicious administrator at a cybercafe, or a malicious user with sufficient access to install key loggers at a kiosk, can obtain users' passwords easily. Even when users do not trust the machines they are using, many of them are faced with the prospect of accessing their accounts with a single level of privilege. To address this problem, we propose a system based on two modes of authentication—*default* and *restricted*. Users can signal to the server whether they are in an untrusted environment so that the server can log them in under restricted privileges that allow them to perform basic actions that cause no serious damage if the session or their password is compromised.

1. INTRODUCTION

In today's Internet, authenticating users are faced with significant security risks. Because people routinely access Internet sites from untrustworthy computers, their passwords have the potential to be easily compromised, either by the administrator of the computer, or by somebody with sufficient privileges to install or replace applications. Current authentication mechanisms such as one-time passwords [4] (such as RSA SecurID [3]) and privileged "trading passwords" (such as those used by eTrade [1]), and even PKI, do not fully solve the problem. One-time passwords limit the damage caused by stolen passwords, but allow full-scale damage in a hijacked session. In systems that employ PKI, the users' passwords may not be at risk, but malicious programs can hijack a user's session and do damage to the user's account after they have logged in. eTrade-style trading passwords are required by server policy, where the set of privileges is assumed to be low by default (this method follows the principle of least privilege [5]). Users are required to re-enter the trading password while executing privileged actions such as trades. Such systems are less usable since the default mode of access is that of high privilege—requiring users to enter a high-security password each time they want to access archived email would be a nuisance. To mitigate the effects of password theft and session hijacking, we propose *TwoKind authentication*, a solution based on two modes of authentication—*default* and *restricted*. To signal untrustworthy environments to the server, users employ their restricted authenticator to limit the privileges of the session, thereby allowing usable access under normal circumstances, but restricted access from untrusted computers. TwoKind authenticators include passwords and PKI-based keys; for the purpose of exposition, we will focus on TwoKind passwords since they are the most common form of authentication today.

Apu Kapadia is a Post-doctoral Research Fellow at the Institute for Security Technology Studies (ISTS), Dartmouth College.

2. APPROACH

In a password-based TwoKind authentication system, the restricted password limits the actions one can perform, and therefore limits the damage that can be caused by man-in-the middle attacks (stolen passwords or hijacked sessions). These passwords are used to signal to the server that the user is in one of two possible situations; a *safe* situation where they are confident in the security of the computer and its Internet connection, and an *unsafe* situation where the user is not confident in the security of the computer or connection. For example, a traveler in a foreign country can use a restricted "travel password" at an untrusted cybercafe. Since the user assumes that the environment is untrusted, the loss of the restricted password is assumed to be likely. The amount of damage that can be done with this password or session, however, is limited by the low privileges associated with that password. In contrast to other authentication methods, TwoKind authentication addresses the concerns of "everyday users," whose default mode of access is that of high privilege—consider the nuisance caused by a system that requires users to enter a high-security password each time they want to access archived email. With a restricted password, users can signal to the server when their connection is insecure, in which case only low-privilege actions are permitted. For example, a restricted email session might allow only reading and sending new messages. A restricted banking session might allow only viewing account balances and recent transactions. In summary, (1) users have a means to signal to the server that the connection is not trusted, and (2) the loss of a user's restricted password, or a hijacked session, allows malicious parties to perform only low-privileged actions in the user's account.

3. EVALUATION

While it seems evident that TwoKind authentication would be useful to users who desire such a mechanism, it is unclear whether everyday users in general can be instructed to assess the trustworthiness of their environment and use the correct form of TwoKind authentication. We propose a user study to evaluate the *effectiveness* of our approach.

3.1 Proposed user study

The user study requires subjects to participate in a game designed to measure their risk-taking habits in the context of TwoKind authentication. Subjects are given several tasks in which they must log in to a Facebook-style program [2], which we call *Green Book*. The subject always has the option not to complete a task. To log in, the subject is given two passwords—a *high-privilege password*, which provides access to all the functions within the program, and a *low-privilege password*, which provides access to a limited set of functions. Some of the tasks can be completed only by logging in with a high-privilege password. There are two different environments in which the subject will be asked to complete tasks—*safe* and *unsafe*. While a user can use either of their passwords in both these environments, there may be times when this is undesirable, e.g., if the user is logging in to a risky environment with their high-security password.

The subject is given a certain number of points for each successfully completed task. If a subject logs in to an unsafe environment, they will lose a set number of the points with some probability. The amount they lose would be determined by the password they had used—more points would be lost for use of the high password. At the end of the game, the subject is given a certain amount of monetary compensation directly related to their score. We will present the users with each of the four permutations of the two different variables: safe and unsafe environments, and high and low-privilege tasks. By presenting the subject with scenarios in which they must decide whether to risk accumulated points, we hope to determine their willingness to risk compromise, and whether the use of TwoKind authentication reduces their probability of compromise.

The study will feature *Green Book*, a social-networking website similar to the popular Facebook. Users will have several attributes, e.g., friends, groups, profile, current status, etc. In high-security mode, the users can modify all of these attributes. In low-security mode, they can modify only their status, groups, and profile. These three were chosen as low-security actions because they are easily reversible and do not involve modifying the user's social network. Figure 1 shows a screenshot of our application.

3.2 Analysis

Instead of measuring how often subjects complete their tasks, we predict that the majority of users will follow certain patterns. For example, certain users may risk their high-privilege passwords 10% of the time, while other users might be less risk-averse. Defining these patterns of behavior would give insight into the way and the extent to which people understand security and interpret risk. If subjects do fall into categories, an interesting second step to the user study would be to increase the subjects' stress during study (e.g., by imposing time limits for completing tasks) and to observe the changes in how many people fall into which groups, or to observe when the whole system broke down and users stopped being able to cope with the complexity of the model.

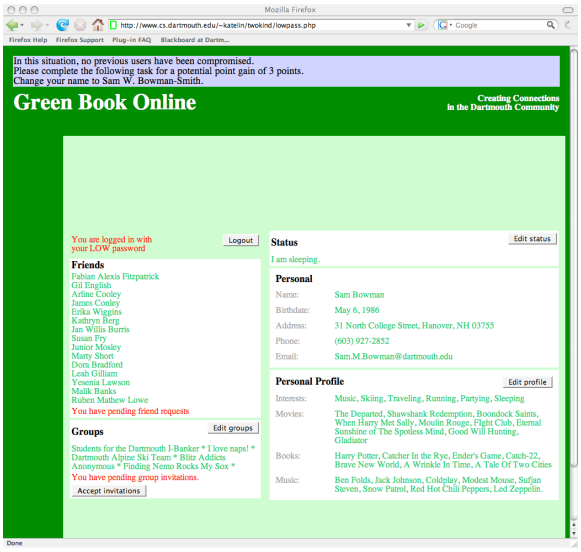

Figure 1: Screenshot of *Green Book*

4. CONCLUSIONS

We believe that the TwoKind method is a feasible and useful authentication method which is an improvement to the current practice of using a single high-privilege password, or repeatedly requiring high-privilege passwords for certain actions. In our opinion, the benefits of having the ability to restrict privileges based on the environment would outweigh the costs of having to remember two passwords or carry two authenticators (such as PKI tokens), if the users both understand and utilize the method. We hope to validate the effectiveness of TwoKind authentication through our proposed user study.

5. ACKNOWLEDGMENTS

We would like to thank Sara Sinclair, Denise Anthony, and Peter Gutmann for their helpful comments. This research was supported in part by the NSF, under Grant CNS-0448499, the Bureau of Justice Assistance, under grant 2005-DD-BX-1091, and the Women in Science Project at Dartmouth College. The views and conclusions do not necessarily reflect the views of the sponsors.

6. REFERENCES

[1] eTrade Trading Passwords. https://www.etradeaustralia.com.au/EStation/hep_aec_connecting.asp.

[2] Facebook. http://www.facebook.com.

[3] RSA SecurID. http://www.rsa.com/node.aspx?id=1156.

[4] Leslie Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24(11):770–772, November 1981.

[5] Jerome H. Saltzer and Michael D. Schroeder. The protection of information in computer systems. *Communications of the ACM*, 17(7), July 1974.