Secure Web Authentication with Mobile Phones

Min Wu MINWU@LCS.MIT.EDU
Simson Garfinkel SIMSONG@LCS.MIT.EDU
Rob Miller RCM@LCS.MIT.EDU
MIT Computer Science and Artificial Intelligence Laboratory, 200 Technology Square, Cambridge MA, 02139 USA

1. Introduction

People increasingly rely on public computers (*e.g.*, Internet kiosks) to do business over the Internet. But accessing today's web-based email, online auctions, or banking sites invariably requires typing a username and password to prove one's identity to the remote service. This creates a significant security vulnerability since the user's password can be captured by the computer and later reused by a hostile party; attacks of this sort have happened in England [7] and in the US [3; 8].

In this paper we present a solution to this problem using a mobile phone as a hand-held authentication token, and a security proxy which allows the system to be used with unmodified third-party web services. Our goal is to create a system that is both secure and highly usable.

2. Authentication Protocol

In our model, a user (U) that wishes to use an Internet kiosk (K) to access a remote service (R) requiring authentication would instead connect to the trusted security proxy (P). The proxy mediates all aspects of the user's communication with the remote service, stores U's username and password and can use credentials to log in to R. P also stores a mobile phone number for each user.

Figure 1 illustrates the authentication process, which has eight steps: (1) The user directs K's browser to contact P. (2) U types her username into K, which sends it to P. (3) P randomly chooses a word from a dictionary and displays it as a "session name" on K's browser. (4) The same word is sent to M in an SMS message. This SMS message contains a link that directs M's built-in WAP browser to contact a dynamically-generated page on P. This page presents U with a choice to allow or deny the session. (5) U looks at the session name displayed on K and (6) verifies that the same session name is displayed on M. (7) If the session names match, U chooses "yes" to allow the session. (8) Once authenticated, P operates like a traditional web proxy, with the exception that P maintains the user's web cookies in a secure "cookie jar" so that the cookies, which

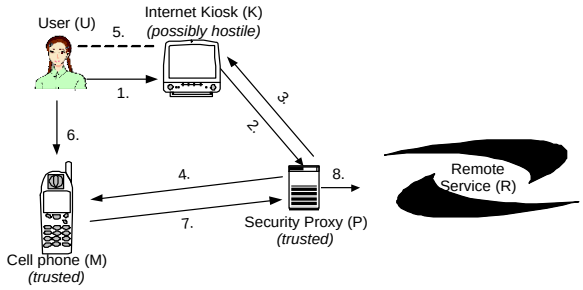

Figure 1. Authentication Protocol

may contain authentication information (*e.g.*, a stored password), are never provided to K.

If U chooses to disallow the session, U is asked if fraud has taken place. Fraud might result if a keystroke logger recorded U's username and a replay attack is taking place. In this case, U can select an option on M that will lock her account until further notice.

When U finishes using R, she can terminate the session either by closing K's browser or by revisiting the approval page on M and disallowing the session. Being able to terminate the session from the cell phone is useful for those cases when the user walks away from the kiosk but forgets to log out. The proxy will also expire the user's session after a short idle time.

3. Threat Model and Enhancements

Our system is designed to address what we consider the two most likely security threats: (1) K remembers connection information for replay attack at a later time; (2) P receives two simultaneous connections from different kiosks, each claiming to be the same user.

We address both of these through the use of a unique *session name* (SN) for each user's session that is displayed, and a *nonce* (N) that is transmitted to M with both the SMS message and the WAP page. SN is an easy way for the user to verify that the session displayed on K matches the

session displayed on M; N prevents forged replies from an attacker who knows SN but does not have possession of M.

Security of the system depends on the security of messages sent by SMS and WAP, which are encrypted with A5 [2; 5]. Only M can receive the short message containing SN and N. As a result, only M can obtain the proper WAP page from P, and only M can acknowledge the choices on the page. When P receives "yes" with SN and N, it knows that the session named SN is indeed initiated and approved by M.

The security of this system also depends upon the fact that U is in possession of M. We believe that this is a reasonable assumption: when people lose their mobile phones, they are typically reported lost and deactivated. Once deactivated, M will no longer be able to receive SMS messages destined for U.

Some services require users to periodically type their passwords during a session when switching from one area of the service to an area of higher security. The proxy can observe such password requests and satisfy them directly — optionally by receiving specific authorization from the user's mobile phone. In the event that new confidential information needs to be provided, the user could type "SECRET" in a form and have this request satisfied through request by P to M. Ross *et al.* have developed a system [10] for intercepting other confidential information through a web proxy and displaying that information on a small-screen hand-held device.

4. User Interface Design

This work was motivated to find a solution to the "hostile host" problem that was both secure and usable. Security and usability are often seen at odds with one another; we believe that by applying design principles, we can build systems that are both secure and usable. (1) *Minimize user input:* Our system requires only that the user know the URL of the proxy and their username. By assuming possession of M, we even eliminate the necessity of the user to remember a password! (2) *Make relevant security decisions on the user's behalf when possible:* Instead of being deployed by a third-party, our proxy could be deployed by a service such as E*Trade. Detecting that a user is stationed at a public-access kiosk (and possibly hostile host), the system could avoid prompting the user for a password, and instead use mobile phone authentication. (3) *Provide the user with clear instructions when they are needed:* The system provides step-by-step instructions on both K and M. Likewise the SMS message and WAP screens, while brief, have been carefully written to be free of technical jargon and understandable. (4) *Make the system's security-relevant decisions visible to the user; when appropriate, give the user the ability to override the system's actions:* The user is always aware as to the current state of the authentication process. When the user disallows authentication at M, the user is given the choice whether or not to disable her username.

5. Related Work

RSA Mobile [4] is an SMS-based authentication system that requires the user to type a one-time password sent to their mobile phone into the computer's web browser in order to log in. This solution is less optimal than ours, as the user could easily make a mistake when typing an unfamiliar password. RSA Mobile could be made to work with unmodified web services through the use of a security proxy, but this functionality is not currently available. Fujitsu [1] and Pohlmann [9] describe similar systems.

Clarke *et al.* [6] describe an alternative mechanism for using untrusted kiosks that avoids the wireless network and instead creates a cryptographically secure channel between the PDA and the remote server using a video camera attached to the PDA and encrypted graphic displayed on the kiosk screen.

References

[1] "mPollux SMS Security Option" *Fujitsu SDA*, 2003.

[2] "GSM calls even more secure - thanks to new A5/3 Algorithm" *ETSI*, 2002.

[3] "Keystroke Logger Captures Passwords At Copy Shop: Experts Advise Caution" *Associated Press*, 2003.

[4] "RSA Mobile: two-factor authentication for a mobile world" *RSA Security*, 2002.

[5] Biryukov, A. *et al.* "Real Time Cryptanalysis of A5/1 on a PC" http://cryptome.org/a5.ps

[6] Clarke, D. *et al.* "The Untrusted Computer Problem and Camera-Based Authentication" *Proceedings of the International Conference on Pervasive Computing*, 2002.

[7] Leyden, J. "Crooks harvest bank details from Net kiosk" *The Register*, 2003.

[8] McCullagh, D. "Ex-student accused of spying on campus" *CNET*, 2003.

[9] Pohlmann, N. "Authentication via Mobile Phone — Breaking the Ground" *Business Briefing Global Security Systems*, 2002.

[10] Ross, S. J. *et al.* "A Composable Framework for Secure Multi-Modal Access to Internet Services from Post-PC Devices" *Third IEEE Workshop on Mobile Computing Systems and Applications*, 2000.