Secure Web Authentication with Mobile Phones

Min Wu, Simson Garfinkel, Robert Miller
MIT Computer Science and Artificial Intelligence Lab, 32 Vassar Street, Cambridge MA 02139
{minwu, simsong, rcm}@csail.mit.edu

As computing becomes pervasive, people increasingly rely on public computers to do business over the Internet. But accessing today's web-based services invariably requires typing a username and password to authenticate – a significant vulnerability, since the password can be captured by the public computer and later reused by a hostile party. We introduce 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 an authentication system that is both secure and highly usable.

Figure 1 illustrates the authentication process. A user who wishes to use an Internet kiosk to access a remote service requiring authentication would instead connect to a trusted security proxy (step 1). The proxy stores the user's passwords and can use them to log in to the remote service. It also stores a mobile phone number for each user, to which a short text message (SMS) is sent to complete the authentication. Once the user responds to this message, the user's connection from the kiosk is authenticated (step 2). The proxy then operates as a traditional web proxy and mediates all aspects of the user's communication with the remote service, but preventing long-term authenticators (*e.g.*, cookies) from touching the kiosk (step 3).

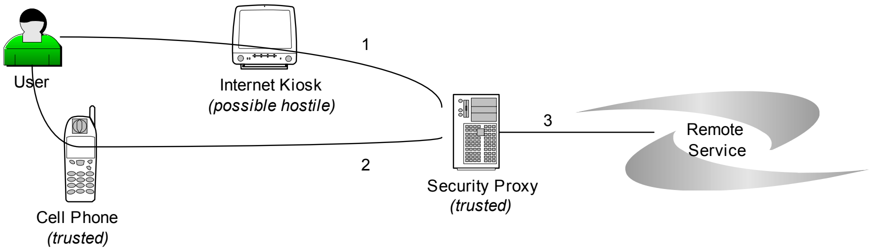

Figure 1: Authentication Process

A one-time, human-readable session name is displayed in the browser and on the mobile phone, designed to prevent replay attacks and forged sessions. However, if the user blindly approves sessions without checking the session name, an attacker can trick the user into approving a wrong authentication session.

We ran a user study to determine how our approach compares, in terms of security and usability, to other techniques that use a mobile phone for authentication. Four login techniques were studied, two that send a one-time password in the text message (either 8 random digits or 2 random words), and two based on our approach (either visually checking the session names shown on the kiosk and the mobile phone, or actively choosing the correct session name from a list of choices on the mobile phone). Subjectively, users rated logging in by checking as the easiest of the four techniques (rated 4.45 out of 5), followed by logging in by choosing (4.20/5). Typing a one-time password was least preferred (3.55/5), because it forces switching between the mobile phone and the keyboard, and because typos caused more errors. To measure the security, we simulated attacks during the user study to try to trick the user into approving wrong sessions. Logging in by checking was easily spoofed: for one attack, users were tricked 36% of the time. However, logging in by choosing was secure, with zero error rate over a total of 47 attacks.

By asking the user to choose and approve a correct session name from her mobile phone, we provide a mobile authentication solution that is both secure and easy to use. Our solution can be deployed as a good backup to password login. When a user forgets her password, she can still log in using her mobile phone instead.