

A NEW METHOD FOR SECURE USER AND SITE AUTHENTICATION

TECHNICAL FIELD

This invention relates to security and privacy. More particularly it relates to site and user authentication.

BACKGROUND OF THE INVENTION

Fake web sites are frequently used to trick users into revealing confidential information. Site "seals" with a logo which the user associates with security help give users a sense of comfort when visiting a legitimate web site. This is analogous to a Better Business Bureau sticker in a physical storefront. However, on the web it is trivial for a fake site to copy such a seal. Trying to detect sites with such counterfeit seals and to then take down these sites is a slow process. Another alternative, having seals which require a user to click on them to verify authenticity expects users to be far more proactive and careful than they have proven to be. A somewhat more secure alternative is to install a toolbar that examines each page the user downloads and checks whether the source is a known malicious site. The disadvantage of this approach is that the user has to download and install a toolbar. Another approach that has proven not to work is the use of the SSL infrastructure wherein users are expected to navigate a maze of locks, green bars and frequent cryptic error messages, in order to ascertain the legitimacy of a site. When combined with the rise of man in the middle (MITM) and man in the browser (MITB) attacks, it is safe to say that current site authentication techniques on the web simply do not work.

The converse problem of user authentication to a web site is even more challenging. Most techniques for authentication like passwords and one time passwords are considered vulnerable to MITM and MITB attacks. Exacerbating the situation is the notion of single sign on or federation; namely the notion that one site will vouch for the authenticity of the user to several other sites. A single key to open several doors is certainly convenient, but if that one key is weak, then the risk has just been amplified.

The innovation described herein seeks to use a single approach to greatly increase the security of both site and user authentication.

ADVANTAGES OF THE INVENTION

This invention may provide the following advantages:

- The ability to develop a site authentication “seal” technique that is not easily defeated by counterfeit web sites, and which does not require the user to download and install a toolbar or to click on the seal to check its genuineness.
- The ability to develop a new method of user authentication based on one time passwords which crucially does not require the provisioning of a per user secret, but rather only requires a per relying web site shared secret.
- The ability to use the new methods of site and user authentication to achieve more secure and convenient single sign on.

Additional objects, advantages, novel features of the present invention will become apparent to those skilled in the art from this disclosure, including the following detailed description, as well as by practice of the invention. While the invention is described below with reference to preferred embodiment(s), it should be

understood that the invention is not limited thereto. Those of ordinary skill in the art having access to the teachings herein will recognize additional implementations, modifications, and embodiments, as well as other fields of use, which are within the scope of the invention as disclosed and claimed herein and with respect to which the invention could be of significant utility.

SUMMARY

Our first innovation is to create a new method of site authentication that is not easily counterfeited. We achieve this by creating a pop-up window on the user's PC that is in communication with a security server, and where this communication channel is separate from the communication between the user's browser and whichever web site they are at. A legitimate web site embeds code in the web page which communicates to the security server from the user's desktop. The security server ensures the web site is not known to be malicious, and then signals both the web page on the user's browser, as well as the pop-up window to which it has a separate channel, that the web site is genuine. The 'signal' to the user can take the form of a visual cue conveying the concepts of "good site" or "bad site" or "do not know".

Our second innovation is to strengthen the security of the signaling mechanism described above by having the security server send a random image with the signal to both the pop-up window and the user's browser. The user who sees the image in both places gets further reassurance that the web site is safe.

Our third innovation ensures that counterfeiting the pop-up window is made very difficult by having the user select a personalization image which appears in the

pop-up window. An attacker who tries to pop-up a fake window is foiled as they cannot know the personalization image.

Our fourth innovation is to have the user authenticate to the security server and use the signaling mechanism described above to communicate assertions about the user's identity to the web site, thus enabling single sign on for the user.

Our fifth innovation is to have the security server provide the user with a fresh one time password for authentication into the web site, where the one time password is constructed using a secret shared between the web site and the security server, obviating the necessity of maintaining a per user shared secret which is a requirement for previous one time password mechanisms.

BRIEF DESCRIPTION OF DRAWINGS

Figure 1 depicts the main components of the system in accordance with the present invention.

Figure 2 shows the system augmented with user authentication, in this case achieved using out of band authentication, in accordance with the present invention.

PREFERRED EMBODIMENT(S) OF THE INVENTION

We will first describe the preferred embodiment for site authentication and then describe how the system can be augmented to also perform user authentication. As shown in Figure-1 the system consists of the following components:

- A security server.

- A pop-up window on the user's desktop.
- A browser on the user's desktop.
- The web site the user is browsing.

There are three distinct phases of operation: (i) the set-up and personalization of the pop-up window which is a one time process, (ii) the start-up of the pop-up window which happens at periodic intervals (akin to logging into a computer at each use), and (iii) The wake-up process when the user browses to a web site that can authenticate itself to the user using the security server.

For set-up the user visits a web site hosted at the security server and selects a personalization image. This image is stored locally on the user's PC using cookies, FLASH storage or similar local storage options. This is in general a one time event per user per PC, and only need be repeated if the user wants to change the personalization image, or the local storage is deleted for some reason.

Start-up occurs at periodic events. For instance this could happen once a day before the user begins browsing the web. The user can initiate the process manually, via a bookmark or bookmarklet, or by using the user's default web page mechanism. Alternately, there could be wake-up code which is triggered by the user visiting a web site that uses the system. Once the pop-up has been started it will be on the user's desktop occupying a relatively small amount of space. Typically the user will position the pop-up at a convenient location on their screen. The act of starting up the pop-up also results in the security server planting a local session object (for instance in a session cookie) on the user's PC.

A web site that wishes to participate in the system will embed on the page code to access the system. Typically this will be in the form of Javascript code within an iFrame. The code will reach out to the security server, an act that transfers to the security server, the previously planted session object. The security server checks the REFERRER or ORIGIN tag of the request from the iFrame against a known whitelist or blacklist of permitted/prohibited sites. It then responds to the iFrame and simultaneously signals the pop-up it is in communication with. The signal consists of two parts, first an indication of whether the web site is "good", "bad", or that the security server "does not know". The second part of the signal is a random image that is sent (if the site is legitimate) to the pop-up and to the iFrame. For a legitimate web site the user's pop-up will have a visual cue (e.g. a green light) that the web site is "good" and will show a random image. The iFrame will also show a similar visual cue and critically will also show the same random image. If the web site was on a black list the pop-up will show a visual cue (e.g. a red light) that indicates the site is "bad".

Attackers trying to defeat the system by creating a fake pop-up are thwarted because they will not know the personalization image. And, an attacker who tries to display the visual cue in the iFrame will not succeed as they do not know the random image that is sent to the pop-up. Finally, a counterfeit web site will not be able to manipulate the REFERRER or ORIGIN tag as it is inspected by the browser.

The communication between the pop-up and the security server can be implemented in a variety of ways. One approach would be to have the pop-up repeatedly make XHR requests with long time outs. Consequently whenever the

security server has a need to send a message to the pop-up and simply opens to the currently open XHR request.

The system described above can be extended to communicate assertions about the user from the security server to the web server. We assume that the user, preferably during start-up, uses some method of authenticating to the security server. For instance the user could prove possession of credentials issued previously or use an out of band authentication technique to prove possession of a phone number. Once this has happened the security server is in a position to respond to requests for identity assertions from the web site. One way to achieve this would simply be for the web site to send the security server an assertion request, for instance via the request in the iFrame, and the security server can simply respond with the assertion. This request response could use the format of standards such as OpenID or SAML. This marries site authentication to user authentication (something that federation protocols like OpenID and SAML do not address) which provides significant security benefits.

A final innovation allows us to significantly strengthen the binding between the user, the security server acting as an Identity Provider and the web site which is the Relying Party. First, we assume that the security server and the web site have a priori agreed on a shared secret (the system is easily extended to use public key cryptography). Second, as shown in Figure-2, we assume that the user has used some method, for instance out of band authentication, to authenticate to the security server. When the user is at a web site that requests authentication, and the web site communicates this request to the security server, the security server calculates a one time password as a function of the secret shared with the web site and some

other information, and displays it to the user in the pop-up window. The user enters (perhaps by cutting and pasting) this one time password into the web site, which confirms authenticity by re-computing the one time password. This system has all the security properties of one time passwords, yet has the tremendous advantage that it does not require a shared secret with each user, and it is only the security server and the web sites that need shared secrets for the purpose of generating one time passwords. The actual one time password can be constructed based on a time stamp or a counter based OTP algorithm (in the way we use these algorithms the time or counter value needs to be communicated by the security server to the web site; or potentially computed deterministically using some agreed upon formula).

CLAIMS

What is claimed is:

1. A method of authenticating a user on a network, comprising:
receiving, by a security server, a request of a network site for authentication of the user;
calculating, by the security server in response to the receipt of the authentication request, a one-time-password based on a secret shared by the security server and the network site but not by the user, and not associated with any particular user, wherein the one-time-password is independently calculable by the network site based on the shared secret; and
transmitting, by the security server, the calculated one-time-password to authenticate the user to the network site.
2. The method of claim 1, wherein:
the user is represented on the network by a user network device executing code embedded in a web network page that is (i) associated with the network site and (ii) displayed by the user network device; and
the authentication request is received from the user network device in accordance with the execution of the embedded web network page code.
3. The method of claim 1, wherein:
the user is represented on the network by a user network device which displays a web network page associated with the network site; and
the calculated one-time-password is transmitted, by the security server to the user network device for display presentation on a pop-up window displayed by the user network device and entry by the user onto the displayed web network page.

4. The method of claim 3, further comprising:
receiving, by a security server from the user network device, an identifier of the user network device and an identifier of the network site; and
transmitting, by the security server to the user network device in response to the receipt of the identifiers, an indication of legitimacy of the network site that will cause display of a corresponding legitimacy indicator on both the displayed web network page and the displayed pop-up window.
5. The method of claim 4, further comprising:
determining, by the security server, the legitimacy of the network site based on the received network site identifier.
6. The method of claim 5, further comprising:
storing, by the security server on the user network device, a local session object;
wherein the received user network device identifier includes the stored local session object; and
wherein the received network site identifier includes a network address of the network site included presented in the displayed web network page.
7. The method of claim 4, wherein:
if the transmitted indication indicates that the network site is legitimate, the corresponding legitimacy indicator includes a first type visual cue in a first state; and
if the transmitted indication indicates that the network site is illegitimate, the corresponding legitimacy indicator includes the first type visual cue in a second state.
8. The method of claim 7, wherein:
the first type visual cue is a light;
the first state is green; and
the second state is red.

9. The method of claim 7, further comprising:

if the transmitted indication indicates that the network site is legitimate, the corresponding legitimacy indicator also includes a second type visual cue in the form of a random image.

10. An article of manufacture for authenticating a user on a network, comprising:
processor readable storage medium; and

logic stored on the storage medium, wherein the stored logic is configured to be readable by a processor and thereby cause the processor to operate so as to:

receive a request of a network site for authentication of the user;

calculate in response to the receipt of the authentication request, a one-time-password based on a secret shared by a security server and the network site but not by the user, and not associated with any particular user, wherein the one-time-password is independently calculable by the network site based on the shared secret; and

transmit the calculated one-time-password to authenticate the user to the network site.

11. The article of manufacture of claim 10, wherein:

the user is represented on the network by a user network device executing code embedded in a web network page that is (i) associated with the network site and (ii) displayed by the user network device; and

the authentication request is received from the user network device in accordance with the execution of the embedded web network page code.

12. The article of manufacture of claim 10, wherein:

the user is represented on the network by a user network device which displays a web network page associated with the network site; and

the calculated one-time-password is transmitted to the user network device for display presentation on a pop-up window displayed by the user network device and

entry by the user onto the displayed web network page.

13. The article of manufacture of claim 12, wherein the stored logic is further configured to cause the processor to operate so as to:

receive, from the user network device, an identifier of the user network device and an identifier of the network site; and

transmit, to the user network device in response to the receipt of the identifiers, an indication of legitimacy of the network site that will cause display of a corresponding legitimacy indicator on both the displayed web network page and the displayed pop-up window.

14. The article of manufacture of claim 13, wherein:

the stored logic is further configured to cause the processor to operate so as to:

store, on the user network device, a local session object; and

determine the legitimacy of the network site based on the received network site identifier;

the received user network device identifier includes the stored local session object; and

the received network site identifier includes a network address of the network site included in the displayed web network page.

15. The article of manufacture of claim 13, wherein:

if the transmitted indication indicates that the network site is legitimate, the corresponding legitimacy indicator will include a first type visual cue in a first state and a second type visual cue in the form of a random image; and

if the transmitted indication indicates that the network site is illegitimate, the corresponding legitimacy indicator will include the first type visual cue in a second state.

16. A system for authenticating a user on a network, comprising:

a communications port configured to receive a request of a network site for authentication of the user; and

a processor configured to calculate, in response to the receipt of the authentication request, a one-time-password based on a secret shared by a security server and the network site, but not by the user, and not associated with any particular user, and to direct transmission of the calculated one-time-password to authenticate the user to the network site;

wherein the one-time-password is independently calculable by the network site based on the shared secret.

17. The system of claim 16, wherein:

the user is represented on the network by a user network device executing code embedded in a web network page that is (i) associated with the network site and (ii) displayed by the user network device; and

the authentication request is received from the user network device in accordance with the execution of the embedded web network page code.

18. The system of claim 16, wherein:

the user is represented on the network by a user network device displaying a web network page associated with the network site; and

the calculated one-time-password is transmitted to the user network device for display presentation on a pop-up window displayed by the user network device and entry by the user onto the displayed web network page.

19. The system of claim 18, wherein:

the communications port is further configured to receive, from the user network device, an identifier of the user network device and an identifier of the network site; and

the processor is further configured to direct transmission, to the user network device in response to the receipt of the identifiers, of an indication of legitimacy of the network site that will cause display of a corresponding legitimacy indicator on both the displayed web network page and the displayed pop-up window.

20. The system of claim 19, wherein:

the processor is further configured to direct storage of a local session object on the user network device, and determine the legitimacy of the network site based on the received network site identifier;

the received user network device identifier includes the stored local session object; and

the received network site identifier includes a network address of the network site included in the displayed web network page.

21. The system of claim 19, wherein:

if the transmitted indication indicates that the network site is legitimate, the corresponding legitimacy indicator includes a first visual cue in a first state and a second visual cue in the form of a random image; and

if the transmitted indication indicates that the network site is illegitimate, the corresponding legitimacy indicator includes the first visual cue in a second state.

22. A method of authenticating a user on a network, comprising:

receiving, by a first user agent on a user network device from a network site, a request of the network site for the user to be authenticated;

transmitting, by the first user agent to a security server, the network site request;

receiving, by a second user agent on the user network device from the security server in response to transmission of the network site request, a one-time-password calculated based on a secret shared by the security server and the network site, but not by the user, and not associated with any particular user,;

transferring the one-time-password from second user agent to first user agent; and

transmitting, by the first user agent to the network site, the one one-time-password to authenticate the user to the network site;

wherein the one-time-password is independently calculable by the network site based on the shared secret.

23. The method of claim 22, further comprising:
transmitting, by the first user agent to the network site, a request of the user to be authenticated by the network site;
wherein the network site request is received in response to the transmitted user request.
24. The method of claim 22, wherein:
the first user agent is a web network page that is associated with the network site and displayed on the user network device; and
the second user agent is a pop-up window displayed on the user network device.
25. The method of claim 24, wherein:
the web network page has embedded code; and
the transmission of the network site request by the first user agent to the security server is based on execution of the embedded web network page code by the user network device.