

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.

OBJECTIVES OF THE INVENTION

This invention has the following objectives:

- 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.
- 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.
- 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 DISCLOSURE OF THE INVENTION

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

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