DEFENDING WEB BROWSERS AGAINST MAN-IN-THE-MIDDLE ATTACKS

BACKGROUND

Computer network communications are often secured through the use of encryption and decryption keys and certificates issued by certificate authorities, such as those used by the Hypertext Transfer Protocol Secure (HTTPS) which employs the Transport Layer Security (TLS) or the Secure Sockets Layer (SSL) protocols. In accordance with such protocols, a certificate that is provided by a computer server to a web browser is validated by the web browser by tracing the certificate to a root certificate authority, typically along a chain of intermediate certificate authorities, and authenticating digital signatures provided by each certificate authority along the chain. Web browsers are supported in this task by consulting lists of "trusted" root certificate authorities that are maintained by the web browser, the operating system of the computer that hosts the web browser, or both. Unfortunately, existing systems are vulnerable to malicious actors that manipulate such lists, such as in support of man-in-the-middle attacks.

SUMMARY

In one aspect of the present disclosure a computer network security method is provided, including configuring a web browser with a capability of determining whether a root certificate authority appears in a first list of trusted root certificate authorities that is maintained by an operating system of a host computer that hosts the web browser, configuring the web browser with a capability of determining whether the root certificate authority was included in the first list at the time that the operating system was installed on the host computer or was thereafter included in the first list by the operating system, configuring the web browser with a capability of determining whether the root certificate authority appears in a second list of trusted root certificate authorities that is provided to the web browser by an administrator, configuring the web browser to determine whether a certificate meets predefined invalidation criteria; and

configuring the web browser to cease to communicate with a party that provided the certificate to the web browser responsive to the web browser determining that the certificate meets the predefined invalidation criteria.

In an example the computer network security method further includes configuring the web browser to validate the certificate and thereafter determine whether the certificate meets the predefined invalidation criteria.

In an example the predefined invalidation criteria includes one or more of the following criteria:

- the certificate's root certificate authority does not appear in the first list,
- the certificate's root certificate authority was not included in the first list at the time that the operating system was installed on the host computer, or was not included in the first list by the operating system after the operating system was installed on the host computer, and
- the certificate's root certificate authority does not appear in the second list.

BRIEF DESCRIPTION OF THE DRAWINGS

Aspects of the invention will be understood and appreciated more fully from the following detailed description taken in conjunction with the appended drawings in which:

Fig. 1A is a simplified conceptual illustration of a system for defending web browsers against man-in-the-middle attacks, constructed and operative in accordance with an embodiment of the invention;

Fig. 1B is a simplified flowchart diagram of an exemplary method for use with the system of Fig. 1A, operative in accordance with an embodiment of the invention; and

Fig. 1C is a simplified conceptual illustration of a reporting system for use with the system of Fig. 1A, operative in accordance with an embodiment of the invention.

DETAILED DESCRIPTION

Reference is now made to Fig. 1A, which is a simplified conceptual illustration of a system for defending web browsers against man-in-the-middle attacks, constructed and operative in accordance with an embodiment of the invention, and additionally to Fig. 1B, which is a simplified flowchart diagram of an exemplary method for use with the system of Fig. 1A, operative in accordance with an embodiment of the invention. In the system of Fig. 1A and method of Fig. 1B, a web browser 100 is configured to incorporate the functionality of conventional web browsers, such as those based on the Google™ Chromium™