== Title:

Evaluating certificate trust model enhancements for HTTPS

== Classification:

Covers both "transparency and alternative certification, distribution or confirmation of key information" and "creation, reporting and use of revocation information"

== Speaker:

Jeremy Clark (Carleton University)

== Abstract:

Internet users today depend daily on HTTPS to provide secure communication with the websites they intend to visit. Over the years, attacks against HTTPS and its certificate trust model have improved, while the number of browser-trusted (and thus, by default, user-trusted) certificate authorities (CAs) have proliferated and the validation put into certificate issuance has eroded. We provide a comparative evaluation of the most prominent among current proposals to enhance security aspects of the CA-Browser trust model. In particular, we examine proposals the community finds important and/or tractable for:

(i) detecting certificate substitution attacks even when the substituted certificate is browser-trusted;

(ii) detecting 'SSL stripping:' man-in-the-middle attacks that aim to downgrade any potential HTTPS connection to HTTP;

(iii) enhancing the robustness and reliability of certificate revocation mechanisms; and,

(iv) exposing the hidden nature of intermediate CA certificates.

Instead of focusing on the specifics of each proposal, we deconstruct their underlying concepts into a set of 16 primitives that can be combined in different ways to address these security issues. Primitives that offer a certain enhancement will typically trade off aspects of security, privacy, deployability and usability; thus, we also provide an evaluation framework of 19 properties that each primitive either fulfills, partially fulfills, or does not fulfil. Building on this contextual review, classification, and comparative evaluation, we provide a summary of important open problems and future research directions.

This is joint work with Paul C. van Oorschot and will appear at the 2013 IEEE Symposium on Security and Privacy.