An Evaluation System For SSL Validation Schemes

Henning Perl, Sascha Fahl, Matthew Smith
Leibniz University Hannover, Germany, {perl, fahl, smith}@dcsec.uni-hannover.de

I. Introduction

While a lot of research is going into improving the CA system, there is currently no framework for comparing the merits and weaknesses of the different approaches. In this paper we suggest such a framework loosely following the design of the framework presented by Bonneau et al. [1] for evaluating web authentication schemes. Our findings are filed into one of two categories: deployability, or security. In each category, we describe a set of benefits, consisting of a mnemonic title and a description. In addition, we indicate where we borrowed a benefit from [1].

II. Benefits

A. Deployability Benefits

In this category deployment aspects are evaluated.

D 1 *No-User-Cost:* The cost for the user of the scheme is negligible. This means for instance that the system does not require special hardware which would need to be purchased by the end user. (c.f. [1, D2: *Negligible-Cost-per-User*].

D 2 *No-Server-Cost:* The total cost per user of the scheme is negligible for the server. As opposed to D 1 we only consider costs for the server here. We say that additional CPU or bandwidth costs are negligible, but addition recurring fees are not. A system has *Quasi-No-Server-Cost* if it is possible to enrol a server without costs but it is common to use a paid service. (c.f. [1, D2: *Negligible-Cost-per-User*].

D 3 *Server-Compatible:* On the server side, the system is compatible with SSL and X.509 certificates. Servers don't need to patch their web server or SSL library. (c.f. [1, D3: *Server-Compatible*])

D 4 *Browser-Compatible:* On the browser side, the system is compatible with SSL and X.509 certificates. The browser doesn't need to be patched. (c.f. [1, D4: *Browser-Compatible*]).

D 5 *Incrementally-Deployable:* The system can be deployed incrementally. The full benefit should only be awarded if early adopters already benefit from the system even if wide-spread adoption has not occurred yet. The benefit should not be granted if the benefit to adopters only kicks in once everybody has migrated, even if the technical migration can be executed in an incremental and backwards compatible way. A system is *Quasi-Incrementally-Deployable* if early adoption is beneficial and safe for the case that each client can securely acquire a list of servers that already offer the new service, i.e. no downgrade attacks are possible.

D 6 *Negligible-Communication-Overhead:* The total communication overhead between the client, the server, and (potentially) a third party is negligible. The system is plausible for mobile devices and settings with a low bandwidth connection.

D 7 *Negligible-Computational-Overhead:* The total computational overhead combined for the client, the server, and (in some cases) a third party is negligible. The system is plausible for mobile devices and settings with low processing power. The system has *Quasi-Negligible-Computational-Overhead*, if the computational overhead is negligible for the user.

D 8 *No-Additional-Infrastructure:* For the deployment, no additional infrastructure is necessary. The system either reuses the CA or DNS infrastructure or doesn't need any at all. We award a *Quasi-No-Additional-Infrastructure* if the systems reuses the CA or DNS infrastructure but requires those services to integrate the system.

D 9 *Trusted-Root-CA-support:* The system can validate trusted root-CAs that are distributed out-of-band with the clients, e.g. the Browser or OS.

D 10 *Custom-Root-CA-support:* The system can integrate custom root-CAs that are only trusted by clients that explicitly choose to trust them. This enables organizations to use the system to develop a closed PKI-infrastructure that can be combined with the public structure. A system has *Quasi-Custom-Root-CA-support* if user action is required to include custom root-CAs.

D 11 *Selfsigned-Certificate-support:* The system can validate certificates that are not signed by any third party.

D 12 *No-Out-Of-Band-Connection:* For the client to verify the server, the client only needs connectivity to the server, not to any other third party.We award *Quasi-No-Out-Of-Band-Connection*, if an out-of-band connection is only required in rare cases, e.g. if the certificate has just been issued or to download periodic updates.

B. Security and Privacy Benefits

S 1 *Built-In-Revocation*: The system has build in capability to revoke certificates. This can become necessary in the case when a server's private key was stolen. We allow for a short grace period bound by the network delay, before the compromised credentials must be revoked. The full benefit should only be awarded if the revocation mechanism is built into the system as an integral component.

S 2 *OCSP-or-CRL-Compatibility*: The system can support revocation through OCSP or CRL.

S 3 *Resilient-To-DOS-Attacks*: The system does not rely on an infrastructure that is required for validation that can be knocked out through a denial of service. It is *Quasi-Resilient-To-DOS-Attacks* if an out-of-band connection is only needed from time to time or in special cases.

S 4 *User-Privacy-Preserving:* When using the system for server authentication, the information that the client requested a specific server does not leak to any third party.

S 5 *Secure-Key-Migration:* When a domain's owner changes keys this can be done in an automatic and verifiable way. The system has *Quasi-Secure-Key-Migration* if migration is possible but the process is indistinguishable from a MITMA for the client.

S 6 *Secure-Key-Migration-After-Credential-Theft:* When a domain's owner changes keys because a credential theft was detected, this can be done in an automatic and verified way. The system has *Quasi-Secure-Key-Migration-After-Credential-Theft* if migration is possible but the process is indistinguishable from a MITMA for the client.

S 7 *Secure-Domain-Migration*: The system allows the owner of a domain to change in a verifiable way. This benefit may not be awarded if this process leaves the previous owner the capability to impersonate the new owner for any amount of time. A system has *Quasi-Secure-Domain-Migration* if migration is possible but the process is indistinguishable from a MITMA for the client.

S 8 *First-Contact-Protection*: The system protects the connection fully from the very first connection from the client. The benefit should not be award if it is a "trust on first use" system. The system offers *Quasi-First-Contact-Protection* against an adversary if the incident is detectable after the fact. This benefit is evaluated according to the adversary capabilities in Section II-B1.

S 9 *Connection-Protection:* The system protects the adversary from eavesdropping on the connection. This is equivalent to server impersonation. The system offers *Quasi-Connection-Protection* against an adversary if the incident is detectable after the fact. This benefit is evaluated according to the adversary capabilities in Section II-B1.

1) Adversary Capabilities: For a more precise security analysis of benefits S 8 and S 9 we consider adversaries of different capability levels.

Lvl 1. *Active MITMA required:* The adversary only controls the connection between the client and the server.

Lvl 2. *Trusted CA certificate required:* Additionally, the adversary can sign any certificate using an arbitrary trusted root-CA (i.e. a "weakest link" attack).

Lvl 3. *Compromising user chosen third parties required:* Additionally, the adversary can compromise n third parties of his choice (i.e. n "strongest links" attack).

Defense against a first-level adversary is already covered by the current CA-PKI. The minimum improvement needed by any system is to protect against an attacker at level 2. Optionally a system also requires the attacker to successfully compromise or knock out n further third parties. Ideally this is combined with *trust agility*, meaning that the user can choose which n parties are used to validate the connection thus making it even harder for the attacker since he either has to know which n parties were chosen or compromise all possible third parties.

C. On Usability

We decided not to include usability benefits in the catalog for specific reasons. Even though the user experience of a SSL validation system may have a large impact on the security of the system e.g. through the way warning messages as well as safe connections are represented, we found it impossible to judge the various merits of the different systems objectively. While there might be differences in how helpful a system is when compiling information for a warning message, ideally a system should not show any false-positive warnings at all. Since all since can be theoretically be misconfigured and thus produce false-positives and both this and the quality of the warning messages are influenced more by implementation and deployment than the system itself, we decided not to score these aspects. In many cases the user interface will look the same as it looks today, with any other SSL system under the hood. Writing good warning messages is certainly a big challenge, with a whole bag of definitions on what "good" means in this context.

So in that sense, the usability of a SSL system is directly related to how easy it is to set up for a server administrator. We cover this as part of the deployability benefits. Finally, the debate of whether validation systems should block the connection if in doubt has been discussed by Sunshine et al. [2] and applies to all proposals as well.

References

[1] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. *Security and Privacy (SP), 2012 IEEE Symposium on.*

[2] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor. Crying wolf: An empirical study of SSL warning effectiveness. In *Proceedings of the 18th Usenix Security Symposium*, 2009.