



SSL Bashing

– Issues of X.509 in web security

Tobias Limmer

Computer Networks and Communication Systems
Dept. of Computer Sciences, University of Erlangen-Nuremberg, Germany

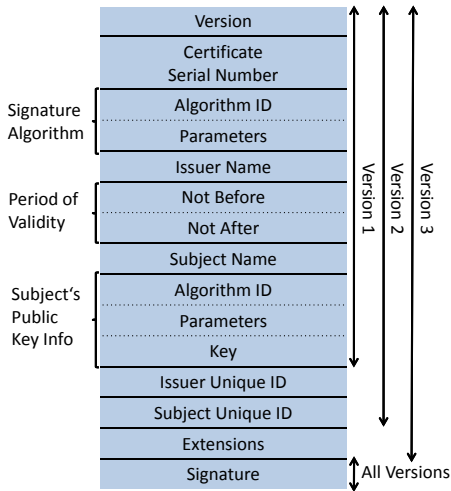
10.1.2010



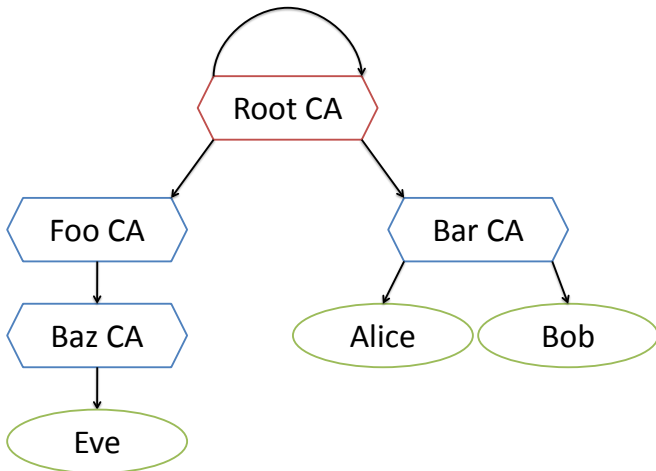
Overview

- Data sources:
 - Dan Kaminsky's talk at the 26C3
 - J. Sunshine et al., *Crying Wolf: An Empirical Study of SSL Warning Effectiveness*. In Proceedings of the 18th Usenix Security Symposium, August 2009.
- Talk structure:
 - Introduction
 - X.509 PKI problems
 - SSL implementation problems

X.509 certificate



X.509 PKI (Public Key Infrastructure)



Getting An X.509 Certificate for your Website

- Domain Validation:
 - 1 Register domain in DNS, also include a canonical email address in the record
 - 2 Generate public/private key
 - 3 Provide public key to a Certificate Authority with the domain name
 - 4 CA sends mail to email address in DNS record
 - 5 User clicks on link in email
 - 6 Receive certificate
- Many CAs perform better validation
- But: Security is only as strong as the weakest part!

Problems of our X.509 PKI

- Accepted Root CAs are regarded equally, no matter how much effort is spent in authentication
- Who 'accepts' Root CAs?
 - The software vendors! Microsoft, Mozilla, Apple, ...
- Not all information within X.509 certificates is authenticated by CAs
 - Scrubbing only performed by a few CAs
- Certificate Revocation:
 - Done by using CRLs (Certificate Revocation Lists)
 - Has anybody ever downloaded a CRL for your webbrowser? Or email client?

Problems of our X.509 PKI

- Delegation in X.509
 - Case: We want to issue our own certificates for *.i7.informatik.uni-erlangen.de
 - This is only possible with the *name constraints* extension.
 - not supported in many SSL libraries yet
 - Is being done anyway with intermediate certificates that may sign arbitrary certificates
- Root CA attack using vulnerabilities of MD5 by Stevens and Sotirov in 2008
- MD2 is still supported by all SSL implementations except GnuTLS
 - Preimage attack soon possible
 - Proposed attack: Use some known MD2 signature from root CA for signing an own CA certificate (we can modify the certificate's content to match the hash)
 - We need a MD2 signature: Verisign's root certificate is self-signed with MD2

Solving these PKI problems for the web

- Kaminsky suggests hierarchy as used for DNS:
 - One root that delegates to different registries for top-level domains, which in turn allow only providers to register domains
- Switch offline verification to online verification
- Standardize authentication process
- But: no mature suggestions available yet

SSL Browser Implementation Issues

- Passive security indicators (e.g. lock in status bar) were shown to be ineffective
- Many web browsers now display „active“ warnings requiring user action
- At least 44% of 380,000 SSL-enabled websites trigger browser warnings
 - Caused by domain mismatch, expired and non-authenticated certificates
 - Users get used to warning dialogs!
- Survey with 100 participants in a laboratory study conducted
- Used Firefox 2, Firefox 3 and MS Internet Explorer 7 SSL warnings

Browser Warnings: Firefox 2

You are being redirected to Cameo.

Please [click here](#) if



Browser Warnings: Firefox 3



Secure Connection Failed

cameo.library.cmu.edu uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is unknown.

(Error code: sec_error_unknown_issuer)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

[Or you can add an exception...](#)

Browser Warnings: Internet Explorer 7



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

-  [Click here to close this webpage.](#)
-  [Continue to this website \(not recommended\).](#)
-  [More information](#)

Redesigned Warning for Firefox 3



Secure Connection Failed

The website responding to your request failed to provide verifiable identification.

What type of website are you trying to reach?

- Bank or other financial institution
- Online store or other e-commerce website
- Other
- I don't know

Continue

You are seeing this warning because the response contained a [self-signed certificate](#).



High Risk of Security Compromise

Your connection to *cameo.library.cmu.edu* is either being intercepted by another party or someone is impersonating *cameo.library.cmu.edu*.

An attacker is attempting to steal information that you are sending to *cameo.library.cmu.edu*. We advise you to contact this company by telephone or using a different computer that does not yield this warning.

Get Me Out of Here!

Why was this site blocked?

[Ignore this warning](#)

Survey

- Users should go about „each task in the way you would if you were completing it with the computer you usually use“
- Participants were told that survey is about information retrieval in the Internet
- 4 tasks:
 - Google search
 - Retrieve last two digits of participant's bank account
 - Get price of book from Amazon
 - Get call number of book from local library

Survey Results

	FF2	FF3	IE7	Single-Page	Multi-Page
Bank	18 (90%)	11 (55%)	18 (90%)	9 (45%)	12 (60%)
Library	19 (95%)	12 (60%)	20 (100%)	16 (80%)	19 (95%)

Table 5: Number (and percentage) of participants in each condition who ignored the warning and used the website to complete the library and bank tasks.

Survey Results

- Multi-Page warning was circumvented by 5 users (clicked on „other“ for bank page)
- Firefox 3 warning page:
 - was mistaken as „server down“ error page (2 users)
 - 7 out of 14 participants not understanding the warning chose not to continue (too difficult to circumvent!)
 - some participants tried to switch browser :-)

Conclusion

- Too many users vulnerable to MITM attacks, regardless of warning design
- Best way: avoid warnings altogether and make decisions for users
 - Some Add-Ons already available: Perspectives, ForceHTTPS
 - Improve X.509 PKI somehow?

The end

Thanks for your attention!

Questions?