Another Nail in the Coffin - SSL/TSL woes

Contributed by Michael Felt

Something we all use, but don't really know - TLS security

IMHO - a lot of SSL discussions are almost understood. I feel I know enough to know when I need to worry versus when I do not need to worry. But, my SSL coffin is still how the major browsers are really the ones who dictate what, when, how re: what elements of SSL is permitted.

Still miss my 40-bit encryption...

Not that I would want to rely on that on the open web - but I had a lot of firmware that was "web-enabled" and "secure" because it could only be accessed using https:// (aka SSL/TLS). Unfortunately, this hardware management interface was old enough that it was built to world standards - when France was still requiring 40-bit encryption as the "highest level permitted". Ultimately, I switched off the systems as they were unmanageable - but there was never a matter of security. These interfaces ran on a seperate VLAN, no router to WLAN area, etc..These systemsare in my SSL/TLS coffin.

A secure brand - that got lazy it seems

I know it is for the better security of "all of us", but I feel it is just one drop in the bucket. Starting next year Google (via Chrome v66) is withdrawing recongnitation of certificates signed by Symantec CA (subsideriaries). At issue is that Symantec did not monitor all of these subsidaries that CA signed ceritficates - that ultimately had their ROOT CA trust verified by Symantec ROOT CA's.

My move forward

I want to get to where I really understand how this circus called CA trust actually works - or better - how it is suppossed to work. To do so, I am going to become my personal CA. And since Mozilla and Google (rightfully) will not recognize me as a certified CA I am going to run into every problem imagineable (and also those unimageable).

And what about you?

Part A: That's your problem.

Part B: As I learn more - I'll write about it and share my insights. Especially those insights that are changes from what I thought I knew - but learned "is not quite accurate at 100%".