SSL Failings

Steven M. Bellovin
http://www.cs.columbia.edu

Problem Areas

- Trust model
- Cognitive

Ancient Trust Model

On the Continent it is frequently the case that the signatures of messages involving, for instance, money payments or delivery of valuable documents, purport to be certified by the telegraph operator transmitting the despatch. When we consider, however, the poor pay accorded in many countries to such operators, we cannot but feel that they are exposed to temptations which a prudent man would guard himself against, by declining to accept a guarantee which the Telegraph Company would not back up by an admission of their own liability in the event of a fraud occurring.

--Robert Slater, 1876

Today's Trust Model

To the extent permitted by applicable law, Relying Party Agreements shall require Relying Parties to indemnify VeriSign for:

- The Relying Party's failure to perform the obligations of a Relying Party,
- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

Verisign's CPS, 2009

Follow the Money

"A commercial certificate authority can be trusted to protect you from anyone from whom they won't take money"

-- Matt Blaze

Cognitive Issues

- Users don't understand certificates
- Users don't understand PKI
- Users don't know how many CAs their browsers trust
- Users don't understand the consequences of failures
- But it doesn't matter much, because users rarely look at the little lock or the green EV icon
- We can't fix these problems