SSL Labs checking: Supplemental Material

Historical Timeline

- 1995 Netscape presents SSL 2.0
- 1996 Netscape fixes SSL and offers SSL 3.0 - This is still very good.
- 1999 TLS 1.0 - Further improvements and acceptance of this as a world wide standard. TLS stands for Transport Layer Security.
- 2002 BEAST attack flaw (Browser Exploit Against SSL/TLS) was theoretically established
- 2006 TLS 1.1 fixes the BEAST attack problem and adds more security and features.
- 2008 TLS 1.2 makes more improvements
- 2011 A practical application of the BEAST attack is demonstrated. Now it is a real, not merely theoretical problem.

Sample Letters

1. This was a form filled out on a website:

MRN-HRN : 0005301350
Email Address : (removed)
Subject : I am having technical problems with the website
Message : Please see attached link which tests sites for security :
https://www.ssllabs.com/ssltest/index.html

Most major Banks as well as most sites I deal with have an 'A' rating and Kaiser has been rated a'C'. It appears you have failed to take the necessary precautions to mitigate the beast attack leaving our medical records exposed. I would hope that every effort is made to strengthen the security surrounding our personal information. The site I have pasted above will provide you with all necessary information as to what caused your rating deficiency and what is needed to correct it.

Request Type : Contact the Web Manager

2. This was emailed to the IT person at my doctor's office.

I thought that perhaps this might help you push the people who are doing your patient record portal to upgrade their security. What I had suspected, that if they didn't know how to accept and store passwords it would be indicative of more pervasive failures has proven to be correct.

I've attached the report card from SSLLabs testing their SSL protocols. You can test for yourself at: https://www.ssllabs.com/ssltest/index.html

The significant findings are that the best protocol they offer is TLS 1.0. In 2006 (that is 7 years ago), this was superseded by TLS 1.1 which fixed security flaws. In 2008 that was superseded by TLS 1.2,which fixed more flaws. They will allow the use of weak keys, and they will allow using those weak keys with a weak cipher. This makes your patients vulnerable to a man in the middle attack.

There really is no excuse for them to have less than an A grade. All the banks and credit card companies I've tested do get an A grade. Even my site, gets an A grade and I pay less than $100/yr for hosting.

It just isn't that hard to do it right. If they can't do a simple SSL connection properly, then I do not think they can protect my data from hackers.

Please let me know if they fix anything based on this report. I'm doing a newsletter article on the SSL Labs test site and I've heard that lots of banks and credit unions have used it to improve their security. Finding it helped a medical records portal would be great.

Steve Shank

My Results

My banks and most of my financial services vendors did fine. My Doctors and my local Thriftway failed miserably. I have called as well as written them. So far, no improvement. However, many people are reporting having emailed their Credit Unions or Banks and been thanked and the fixes were implemented in a couple of days.

- **Banks:** Every bank I tested received an A grade as fully secure. I tested: Ally Bank, Capital One, Chase, USBank, and Bank of America
- **Other Financial resources I use:** Paypal: Misconfigured servers. Some A and some B, Vanguard: A, Dwolla: A
- **Stores and Vendors you might use:** Steveshank.com: A, Amazon.com: A, BestBuy.com: B, Lambs Thriftway (for customer loyalty card): F, Tunnelbear.com: A
- **My Medical Records:** Both my doctors failed to meet basic standards.