Michael Christensen
CS 465
November 1, 2013

Project 7 – TLS

Website	**Key Exchange Method**	**SSL-Session Protocol**	**Key Size**	**Size of Encryption**	**Cipher Suite Chosen**	**Supports Session Resumption/ Renegotiation?**	**Session-ID /Master-Key Length**	**Certificate Issuer**	**Certificate Subject**	**Depth of Certificate Chain**
Mail.google.com	ECDHE_ECDSA	TLSv1.2	2048 bit server public key	128 bit with RC4	ECDHE-RSA-RC4-SHA	Yes	64 bytes / 96 bytes	Google Internet Authority G2	Google Inc	2 (Google Internet Authority → Geotrust → Equifax)
Gradebook.byu.edu (redirects to cas.byu.edu)	DHE_RSA	TLSv1.0	2048 bit server public key	256 bit with AES_256_CBC	DHE-RSA-AES256-SHA	Yes	64 bytes / 96 bytes	Digicert HA CA-3	BYU	1 (Digicert High Assurance CA → Digicert High Assurance EV Root CA)
Chase.com	RSA	TLSv1.2	1024 bit server public key	128 bit with RC4	RC4-SHA	Yes	64 bytes / 96 bytes	Verisign International Server CA	JPMorgan Chase	1 (Verisign International Server CA → Class 3 Public Primary Certification Auth)

Facebook.com	ECDHE-RSA	TLSv1.2	2048 bit server public key	128 bit with AES128_CBC	ECDHE-RSA-AES128-SHA	Yes	64 bytes / 96 bytes	Verisign Class 3 Secure Server CA	Facebook, Inc.	2 (Verisign Class 3 Secure Server CA → Verisign Class 3 Public Primary CA → Class 3 Public Primary CA
Wellsfargo.com	RSA	TLSv1.0	2048 bit server public key	128 bit with RC4	RC4-SHA	No	64 bytes / 96 bytes	Verisign Class 3 Secure Server CA	Wells Fargo and Company	3 (Verisign Class 3 Secure Server CA → VeriSign Class 3 Public Primary CA → Class 3 Public Primary CA → Pclass 3 Public Primary CA

Summary:

I noticed that the common method for method authentication across all of these sites was SHA1 (which is the one column of data I didn't include in the table above since the values for each were the same). In addition, the size of the server public keys, session ids, and master keys were the same for every connection. I am more surprised about the differences in Key Exchange methods between the five. Wells Fargo, with which I most of my banking, only uses RSA, while Facebook and Gmail use some form of Ephemeral Elliptic Curve Diffie-Hellamn, with Facebook using RSA signatures and Gmail using ECDSA signatures, which is based on the DSA standard for signatures. Another difference is in the mode of encryption; Gmail, Chase, and Wellsfargo use a block cipher (128 bit RC4), while Facebook uses 128 bit CBC, and BYU goes even further to use a 256 bit CBC. I suppose Gmail, Chase, and Wellsfargo use RC4 because of its speed, since a block cipher scheme takes longer to encrypt information. However, I am surprised that BYU chooses to use such a large key size (twice that of the other websites), since the other websites take care of much more private information, in my opinion.