Thomas Hart
CS465
Project 6 – TLS

Results Table

	Website	Key Exchange Method	Authentication Algorithm	Symmetric Encryption Algorithm	Key Size	Mode	Signature
1	facebook.com	None	Poly1305	ChaCha Stream Cipher	256	None	SHA256
2	instragram.com	None	Poly1305	ChaCha Stream Cipher	256	None	SHA256
3	amazon.com	ECDHE	RSA	AES	128	GCM	SHA256
4	zionsbank.com	ECDHE	RSA	AES	256	GCM	SHA384
5	chase.com	ECDHE	RSA	AES	128	GCM	SHA256
6	stackoverflow.com	ECDHE	RSA	AES	128	GCM	SHA256
7	netflix.com	ECDHE	RSA	AES	256	GCM	SHA384
8	battle.net	ECDHE	RSA	AES	256	GCM	SHA384
9	steampowered.com	ECDHE	RSA	AES	256	GCM	SHA384
10	gmail.com	ECDHE	RSA	AES	256	GCM	SHA384

Comparisons

The signatures in all these methods are consistently SHA256 AND SHA384. Besides that, there were three consistent choices between websites. The first was unique to social media websites Facebook and Instagram. They used ChaCha and Poly 1305 as AEAD methods. They have no block cipher mode because this is a stream cipher. The second method was Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) as the key exchange method, RSA as the authentication algorithm, AES as the symmetric encryption algorithm, mostly with 128-bit keys (except for battle.net – 256-bit key), and GCM as the cipher mode. The third option was the same as the previous, except ECDHE and RSA were not defined explicitly. These also had 256-bit keys across the board. Note that the ones without ECDHE and RSA did list TLS at the beginning like so: TLS_AES_256_GCM_SHA384. Although they do not explicitly say ECDHE and RSA in the cipher suite, these are the default for the newest versions of TLS, so they are implied and reflected in the table.

Cryptographic Guarantees

For Facebook.com, Poly1305 guarantees authentication, meaning senders and receivers know that the entity they are communicating with is who they say they are. The ChaCha stream cipher guarantees confidentiality, meaning eavesdroppers won’t be able to tell what the actual messages say because they are encrypted. It is even more secure with a 256-bit key, as opposed to a 128-bit key.

Amazon.com is guaranteed safety of the encryption/decryption key through ECDHE, authentication through RSA, confidentiality through AES, and message integrity through GCM (the receiver knows the message has not been tampered with).

Battle.net also has confidentiality through AES and message integrity through GCM.

Questions

I’m curious why social media websites use ChaCha20 and Poly1305. Are there particular needs of a social media website that are different than other websites? I also read in the TLS article that Amazon is cheap by using the method they are. Why is that, or is that information outdated? Other prestigious sites like Facebook got a B ranking on the SSL Labs test. What makes it rate that low?