Scott Christensen

10/11/16

C.S. 465

Project 6 TSL Report

|  |  |  |  |
| --- | --- | --- | --- |
| TLS Results |  |  |  |
|  |  |  |  |
| Name | Key Exchange Method | Authentication Algorithm | Symmetric Encryption Algorithm-  Key Size-Mode |
| Google.com | ECDHE | RSA | AES-128-GCM |
| Facebook.com | ECDHE | ECDSA | AES-128-GCM |
| Amazon.com | ECDHE | RSA | AES-128-GCM |
| Youtube.com | ECDHE | RSA | AES-128-GCM |
| Microsoft.com | ECDHE | RSA | AES-256-GCM |
| Blizzard.com | ECDHE | RSA | AES-128-GCM |
| MTGSalvation.com | ECDHE | ECDSA | AES-128-GCM |
| Yahoo.com | ECDHE | RSA | AES-128-GCM |
| Twitter.com | ECDHE | RSA | AES-128-GCM |
| Byu.edu | ECDHE | RSA | AES-256-GCM |

After collecting the results from each of these websites, I found out some pretty interesting things. I thought it was interesting just how common a lot of the methods and algorithms were across various sites. All of the sites I observed used ECDHE for their Key Exchange method, nearly all of them used RSA for their Authentication Algorithm, and nearly all of them used AES- 128 bit key-GCM for their symmetric encryption. There were a few of them that used ECDSA for their Authentication and some that used a larger AES key size it their Symmetric Encryption.

Some questions that I have after doing this report include things about the individual algorithms themselves that I’m not familiar with, such as what is ECDSA? What is ECDHE? What is GCM? But I also have questions about why so many sites use these same algorithms. Is each of these algorithms just super secure and there is no reason to change? Or are these algorithms merely the standard everyone tries to reach as a bare minimum for the scale of their organization? These are things I’d really like to know.