Christopher LaJon Morgan

Oct 26, 2013

Project 7 TLS CS 465

**Connect to booklist.byu.edu**

Looks like booklist uses DH for its key exchange algorithm.

**Connect to Five secure websites**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Westmark.org | Chase.com | Gmail.com | LearningSuite | Facebook.com |
| Key Exchange Method | RSA | RSA | RSA | DH | RSA |
| Key Size | 2048 | 1024 | 2048 | 2048 | 2048 |
| Cipher Suite | RC4-SHA | RC4-SHA | RC4-SHA | DHE-RSA-AES256-SHA | RC4-SHA |
| Session resumption? | NO | YES | YES | YES | YES |
| Protocol | TLSv1/SSlv3 | TLSv1/SSlv3 | TLSv1/SSlv3 | TLSv1/SSlv3 | TLSv/SSlv31 |

Westmark is a private credit union in Idaho. They are very stringent when I comes to security. This makes a lot of sense give that one incident could put them completely out of business. They have no capital to make up for such a mistake and also everyone would leave to a larger bank just around the corner. Westmark is known to block all third party apps, just as one example. Therefore, it was interesting to note that don’t do session resumption, just one more feather in their hat.

It was also interesting to notice that every private entity is using RC4 but the only private entity is using DHE-RSA-AES256. Another interesting point to me was that Chase.com was the only site with a 1024 bit key. I wonder why that is the case. Given just these five sites its really curious to me.