TLS Configuration Project

William Douglass

Here are the ten sites that I have chosen and a short description of them:

https://minesweeperonline.com/

It’s Minesweeper with lots of ads.

https://turnip.exchange/

A site where Animal Crossing: New Horizons players can invite people to their islands.

https://nookazon.com/

eBay but for Animal Crossing: New Horizons.

https://www.ebay.com

It’s eBay (for humans).

https://www.wikipedia.org

It’s Wikipedia.

https://www.taylorswift.com/

This is Taylor Swift’s official website.

https://vsaltykov.com/

This is the official website of Soviet/Russian artist Viktor Saltykov. He was somewhat popular with his band “Forum” in the late 80s and started a solo career in the 90s.

https://www.andreygubin.ru/

This is the official website of Russian pop artist Andrey Gubin, who was very popular from the 90s into the early 2000s. Personally, this site appears to not have left the style of the late 2000s and does not feel particularly official.

https://www.andreygubin.com/

This is a fan-run Andrey Gubin site that has more information about Andrey Gubin and looks more professional and official than the actual official website. It is a labor of love.

https://translit.ru/

Type with the Cyrillic writing system using the English equivalent.

| Subject, Common Name, Alternative Names | Validity Period | Cryptographic Key Type | Certificate Chain Details | Other Properties |
|---|---|---|---|---|
| minesweeper.com, minesweeper.com, www.minesweeper.com | 09-29-25 02:56 UTC to 12-28-25 02:56 UTC | RSA 2048 bits (e 65537) | Root issued by Internet Security Research Group.<br>1 Intermediate issued by Let's Encrypt.<br>All certificates use SHA256withRSA | Supports TLS 1.0 and 1.1 (results in a B)<br>TLS 1.0 and 1.1 use SHA w/ CBC mode exclusively<br>Protocol prevents downgrade attacks |
| turnip.exchange, turnip.exchange, *.turnip.exchange | 09-23-25 00:10 UTC to 12-22-25 01:08 UTC | EC 256 bits | Root issued by Google Trust Services LLC.<br>1 Intermediate issued by the above.<br>Root and Intermediate use SHA384withECDSA, leaf uses SHA256withECDSA | Supports TLS 1.0 and 1.1 (results in a B)<br>TLS 1.0 and 1.1 use SHA w/ CBC mode<br>Protocol prevents downgrade attacks |
| nookazon.com, nookazon.com, *.nookazon.com | 09-14-25 08:45 UTC to 12-13-25 09:39 UTC | EC 256 bits | Root issued by Google Trust Services LLC.<br>1 Intermediate issued by the above.<br>Root and Intermediate use SHA384withECDSA, leaf uses SHA256withECDAS | Supports TLS 1.0 and 1.1 (results in a B)<br>TLS 1.0 and 1.1 use SHA w/ CBC mode exclusively<br>Protocol prevents downgrade attacks |
| www.ebay.com, www.ebay.com, www.ebay.com, ... | 07-17-25 00:00 UTC to 07-17-26 23:59 UTC | RSA 2048 bits (e 65537) | Root issued by Sectigo Limited<br>1 Intermediate issued by the above.<br>Root and Intermediate use SHA384withRSA, leaf uses SHA256withRSA | Has HSTS with long duration (results in an A+)<br>Has CAA support<br>Does not support TLS 1.0 and 1.1 (very good) |
| *.wikipedia.org, *.wikipedia.org, *.wikipedia.org, … | 10-20-25 03:26 UTC to 01-18-26 03:26 UTC | EC 256 bits | Root issued by Internet Security Research Group.<br>1 Intermediate issued by Let's Encrypt.<br>Root and Intermediate use SHA256withRSA, leaf uses SHA384withECDSA | Has HSTS with long duration (results in an A+)<br>Has CAA support<br>Allows browsers without SNI support |
| taylorswift.com, taylorswift.com, taylorswift.com | 05-29-25 00:00 UTC to 05-28-25 23:59 UTC | RSA 2048 bits (e 65537) | Root issued by www.digicert.com<br>1 Intermediate issued by DigiCert Inc.<br>All certificates use SHA256withRSA | Does not support TLS 1.0 and 1.1<br>TLS 1.2 sometimes will use CBC mode but will prefer other suites.<br>Only works for browsers with SNI support |
| vsaltykov.com, vsaltykov.com, www.vsaltykov.com | 10-16-25 07:52 UTC to 01-14-26 07:52 UTC | RSA 4096 (e 65537) | Root issued by Internet Security Research Group.<br>1 Intermediate issued by Let's Encrypt.<br>All certificates use SHA256withRSA | Does not support TLS 1.0 and 1.1<br>TLS 1.2 contains a lot of suites, most are weak.<br>Only works for browsers with SNI support |
| andreygubin.com, andreygubin.com, www.andreygubin.com | 04-24-25 00:00 UTC to 04-24-26 23:59 UTC | RSA 2048 (e 65537) | Root issued by The USERTRUST Network.<br>1 Intermediate issued by Sectigo Limited<br>Root and Intermediate use SHA384withRSA, leaf uses SHA256withRSA | All simulated handshakes succeed<br>TLS 1.2 contains many suites with CBC mode but will prefer other suites.<br>Does not have HSTS |
| andreygubin.ru, andreygubin.ru, *.andreygubin.ru | 09-25-25 20:00 UTC to 12-24-25 20:59 UTC | EC 256 bits | Root issued by Google Trust Services LLC.<br>1 Intermediate issued by the above.<br>Root and Intermediate use SHA384withECDSA, leaf uses SHA256withECDSA | Supports TLS 1.0 and 1.1 (results in a B)<br>TLS 1.0 and 1.1 use SHA w/ CBC mode exclusively<br>Has OCSP stapling for revocation info. |
| translit.ru, translit.ru, www.translit.ru | 09-18-25 12:05 UTC to 12-17-25 12:05 UTC | RSA 2048 bits (e 65537) | Root issued by Internet Security Research Group.<br>1 Intermediate issued by Let's Encrypt.<br>All certificates use SHA256withRSA | Does not support TLS 1.0 and 1.1<br>CBC is not used in any of its TLS suites.<br>Has HSTS with long duration (results in an A+) |

Figure 1: information about the validity period, key type, certificate chain, and other properties that I found interesting.

| Subject, Common Name, Alternative Names | Authentication Algorithm | Symmetric Encryption Details (Algorithm, Key Size, Mode) | Hashing Algorithm | Cryptographic Guarantees |
|---|---|---|---|---|
| minesweeper.com,<br>minesweeper.com,<br>www.minesweeper.com | RSA | AES, 256, GCM | SHA384 | Forward Secrecy, Confidentiality and Integrity |
| turnip.exchange,<br>turnip.exchange,<br>*.turnip.exchange | ECDSA | AES, 128, GCM | SHA256 | Forward Secrecy, Confidentiality and Integrity |
| nookazon.com,<br>nookazon.com,<br>*.nookazon.com | ECDSA | AES, 128, GCM | SHA256 | Forward Secrecy, Confidentiality and Integrity |
| www.ebay.com,<br>www.ebay.com,<br>www.ebay.com, ... | RSA | AES, 128, GCM | SHA256 | Forward Secrecy, Confidentiality and Integrity |
| *.wikipedia.org,<br>*.wikipedia.org,<br>*.wikipedia.org, | ECDSA | AES, 128, GCM | SHA384 | Forward Secrecy, Confidentiality and Integrity |
| taylorswift.com,<br>taylorswift.com,<br>taylorswift.com | RSA | AES, 128, GCM | SHA256 | Forward Secrecy, Confidentiality and Integrity |
| vsaltykov.com,<br>vsaltykov.com,<br>www.vsaltykov.com | RSA | AES, 256, GCM | SHA384 | Forward Secrecy, Confidentiality and Integrity |
| andreygubin.com,<br>andreygubin.com,<br>www.andreygubin.com | RSA | AES, 256, GCM | SHA384 | Forward Secrecy, Confidentiality and Integrity |
| andreygubin.ru,<br>andreygubin.ru,<br>*.andreygubin.ru | ECDSA | AES, 128, GCM | SHA256 | Forward Secrecy, Confidentiality and Integrity |
| translit.ru,<br>translit.ru,<br>www.translit.ru | RSA | AES, 128, GCM | SHA256 | Forward Secrecy, Confidentiality and Integrity |

Figure 2: information about the validity period, key type, certificate chain, and other properties that I found interesting.

Summary:

Of all the websites I tested, they preferred the use of AES in GCM mode, with the key size being either 128 or 256. These sites do not always use this encryption algorithm, with notable appearances from ChaCha20 and ECDSA. These websites all had a grade of at least a B. These websites getting a B supported TLS 1.0 and TLS 1.1, both of which are very old and insecure. Interestingly, these sites either appear to be older or were made by individuals simply wishing to provide a unique service, not companies who have to more seriously consider security. Of the six websites getting an A, half had an A+, mostly resulting from the long-term HTTP Strict Transport Security (HSTS) deployments each had. Of all the sites, only wikipedia.org not have a tag saying “This site works only in browsers with SNI support”. However, delving deeper into the report shows that older browsers such as Android 2.3.7 without SNI support were not simulated because of this, indicating that wikipedia.org more likely than not only works for browsers with SNI support despite the lack of such a statement on the SSL report.

Something else I would like to discuss regards the websites that are effectively made by and for other Russian speakers. I had the assumption that because of their national origin, the protocols for these sites may be different. While my dataset only has three of these, I found this assumption to be incorrect and any “sketchiness” to be a result of factors presumably not related to national origin. The first that came to mind was the official website for Andrey Gubin. As previously mentioned on the first page, this site seems to have never left the style of the late 2000s, and I believe this to be related to the fact that Gubin has not performed live since the late 2000s, meaning there is little reason to update the official website, which has not been updated since 2023 and the news it lists having not been updated since 2015. Its SSL report reflects this, with its continued support of TLS 1.1 and 1.0. In contrast, the fan site appears to be more official, and is a reflection of owner’s continued interest and love for Andrey Gubin. Its news is more up to date the site has a modern look. Its SSL report also reflects this, with the site not having support for the weaker TLS 1.1 and 1.0 protocols. One last comparison that I will end with regards Viktor Saltykov’s official website, which is very modern and up to date with his still active career. Once again, the SSL report for his official website reflects this, supporting modern TLS protocols while dropping support for older protocols.

Questions:

What exactly is SNI support? From my limited research, it appears that SNI allows an IP address to have multiple certificates at once, allowing multiple servers hosted on the same IP address to have different certificates rather than one shared certificate. What is the point of this?

Why do some servers not have a preference for which TLS suite they use? In most cases where there is no preference, the SSL report shows that the list contains all suites labeled in green. However, would it be better to have a preference so the server has control over the order of suites it attempts to use? Additionally, how important is this preference in TLS?

Did we cover what ChaCha20 is (I may have forgotten if we did)? How does it compare to AES?

Reviewed by: Sulaiman Mohyuddin