Московский авиационный институт
(Национальный исследовательский
университет)

Институт: «Информационные технологии и прикладная математика»
Кафедра: 806 «Вычислительная математика и программирование»
Дисциплина: «Криптография»

Курсовой проект

Тема: Аутентификация с асимметричными алгоритмами шифрования

Студент: Чекменев Вячеслав Алексеевич

Группа: М8О-307Б-20

Дата:

Москва, 2023

Инструменты:

1. Firefox
2. Wireshark

Условие:

Провести сравнительный анализ в отношении безопасности и корректности настройки веб-серверов с учетом их организационной и государственной принадлежности.

Ход работы:

1. Выбираем сервера для анализа, в моем случае это:

- akorda.kz (ASTANA, ICON OF JAVA – NAGOOR BABU)
- jut.su (SF, California, based anime website)
- avito.ru (Moscow)
- pomofocus.io (London, UK)
- pikcoffeeroasters.com (GUNZENHAUSEN, bayern)

2. Собранные сведения:

Хост: akorda.kz
Версия TLS 1.3: Алгоритмы шифрования: TLS_AES_128_GCM_SHA256
Версия TLS 1.0: Алгоритмы шифрования: Connection not encrypted
Версия сертификата: v3
Валидность сертификата: 05 Oct 2023
Удостоверяющий центр: The USERTRUST Network
Время установки соединения: 65 мс

Хост: jut.su

Версия TLS 1.3: Алгоритмы шифрования: TLS_AES_128_GCM_SHA256

Версия TLS 1.0: Алгоритмы шифрования: Connection not encrypted

Версия сертификата: v3

Валидность сертификата: 10 Jul 2023

Удостоверяющий центр: ISRG Root X2

Время установки соединения: 55 мс

Хост: avito.ru

Версия TLS 1.3: Алгоритмы шифрования: TLS_AES_128_GCM_SHA256

Версия TLS 1.0: Алгоритмы шифрования: Connection not encrypted

Версия сертификата: v3

Валидность сертификата: 18 Mar 2029

Удостоверяющий центр: GlobalSign

Время установки соединения: 70 мс

Хост: pomofocus.io

Версия TLS 1.2: Алгоритмы шифрования: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Версия TLS 1.0: Алгоритмы шифрования: Connection not encrypted

Версия сертификата: v3

Валидность сертификата: 19 Jul 2023

Удостоверяющий центр: ISRG Root X1

Время установки соединения: 40 мс

Хост: pikcoffeeroasters.com

Версия TLS 1.2: Алгоритмы шифрования: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Версия TLS 1.0: Алгоритмы шифрования: Connection not encrypted

Версия сертификата: v3

Валидность сертификата: 06 Jul 2023

Удостоверяющий центр: ISRG Root X1

Время установки соединения: 75 мс

Вывод:

Большинство сайтов используют одинаковые методы шифрования, такие как TLS_AES_128_GCM_SHA256 и TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256. Это указывает на распространенность и применение надежных алгоритмов шифрования для обеспечения безопасности соединений.

Большая часть сайтов поддерживает протокол TLS 1.2 или даже 1.3, что является хорошей практикой, так как TLS >= 1.2 считается достаточно безопасным и широко распространенным протоколом.

Интересно отметить, что сайты из разных стран могут использовать одинаковые удостоверяющие центры (УЦ), такие как ISRG Root X1. Это указывает на то, что независимо от географического расположения, некоторые УЦ предоставляют услуги сертификации для сайтов по всему миру.

У большинства сайтов срок действия сертификата составляет не более 2 лет с момента выпуска. Это говорит о том, что владельцы сайтов следят за обновлением своих сертификатов и обеспечивают их актуальность для обеспечения безопасного соединения с посетителями.

Интересно отметить, что сайты из разных стран могут использовать одинаковые удостоверяющие центры (УЦ), такие как ISRG Root X1. Это указывает на то, что независимо от географического расположения, некоторые УЦ предоставляют услуги сертификации для сайтов по всему миру.

Некоторые сайты все еще разрешают подключение с использованием устаревшего и небезопасного протокола TLS 1.0. Однако радует подход большинства сайтов, которые отказываются устанавливать соединение с этим устаревшим протоколом, тем самым обеспечивая повышенную безопасность своих посетителей. Такой подход должен быть приветствован и побуждать другие сайты к переходу на более безопасные протоколы, такие как TLS 1.2 и TLS 1.3.