

TH Brandenburg
Online Studiengang IT Sicherheit
Fachbereich Informatik und Medien
Netzwerksicherheit
Prof. Dr. Michael Pilgermann

Einsendeaufgabe 2
Wintersemester 2023
Abgabetermin 15. November 2023

Gruppe 11
Mathias Baumbach (Matr-Nr. 20213703)
Mara Schulke (Matr-Nr. 20215853)

Zusammenfassung

Inhaltsverzeichnis

| | | |
|----------|---------------------------|----------|
| 1 | Durchführung | 2 |
| 1.1 | SSL Test I | 2 |
| 1.2 | SSL Test II | 6 |
| 1.3 | SSL Test III | 10 |
| 1.4 | Verschlüsselung | 13 |
| 1.5 | Steganographie | 14 |

Abbildungsverzeichnis

| | | |
|---|--|----|
| 1 | QualysSSL Test – nwsmooc.mooiin.org | 3 |
| 2 | QualysSSL Test – Recent Worst | 5 |
| 3 | QualysSSL Test – Browser Capabilities | 6 |
| 4 | QualysSSL Test – Browser Protocol Features | 8 |
| 5 | Google Chrome vs Firefox – 442 – Unsafe / Unsafe | 10 |
| 6 | Google Chrome vs Firefox – 444 – Safe / Unsafe | 10 |
| 7 | Google Chrome vs Firefox – 444 – Details | 11 |
| 8 | Google Chrome vs Firefox – 444 – Chrome Zertifikat | 11 |

1 Durchführung

1.1 SSL Test I

Aufgabenstellung

Testen Sie den Server `nwsmooc.moo.in.org` mit der SSL-Testseite von Qualys und erklären Sie die Ergebnisse (hinsichtlich Zertifikaten, TLS-Versionen, Handshakes und Details der Protokolle). Erklären Sie für eine weitere Webpräsenz, die als "Recent Worst" bewertet wird, was bei dieser nicht stimmt.

Hinweis: "Recent Worst" ist eine Liste auf der rechten Seite der Testseite. Zur besseren Nachvollziehbarkeit bitte Screenshots hinzufügen. Deren Inhalte sollen aber jeweils von Ihnen erklärt werden.

Antwort

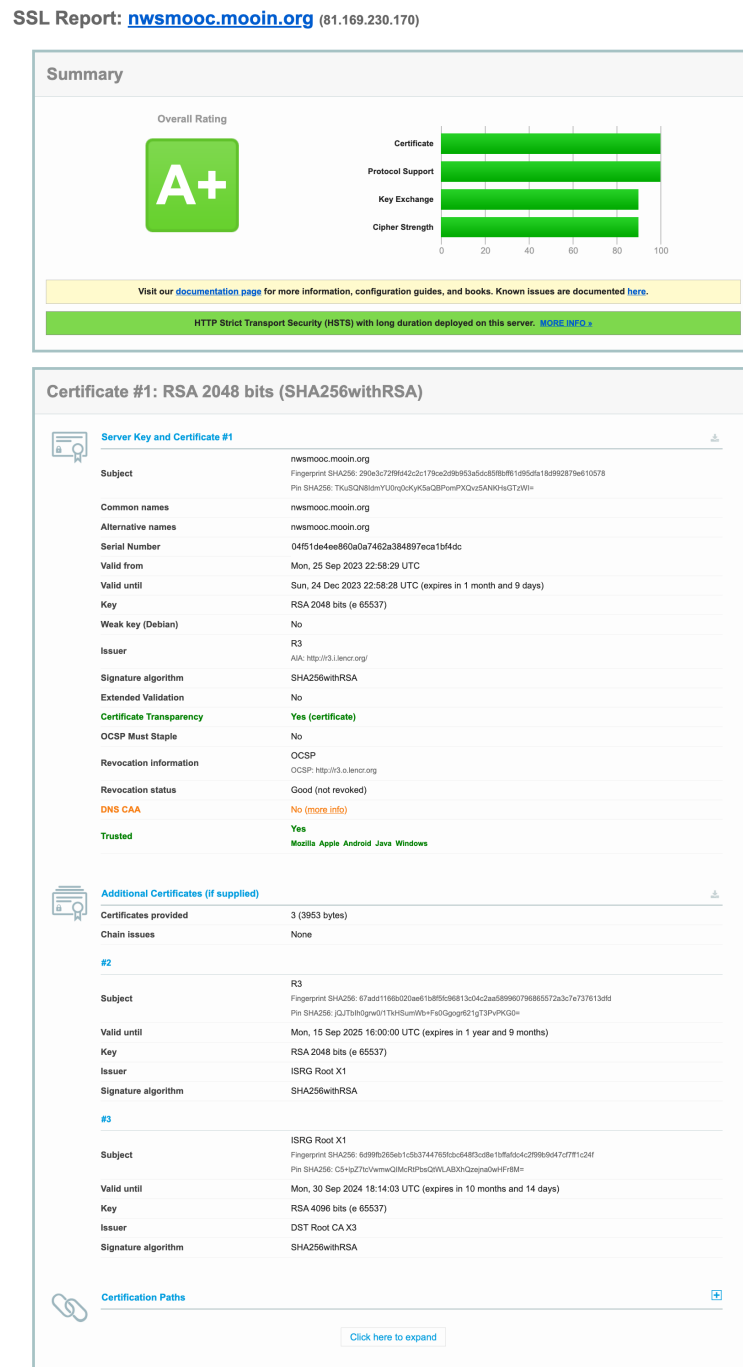


Abbildung 1: QualysSSL Test – nwsmooc.mooin.org

Der Web-Server hat insgesamt eine A+-Bewertung erhalten und ist dementsprechend auf dem aktuellen Stand / robust was die SSL-Konfiguration angeht. Das Zertifikat des Servers ist ein 2048-Bit RSA-Zertifikat, das mit SHA256+RSA signiert wurde. In dem Report von Qualys sind einige wichtige Eckdaten über das Zertifikat des Servers enthalten:

- Gültigkeit: Von 25. September 2023 bis zum 24. Dezember 2023
- Aussteller: R3
- Status: Das Zertifikat wurde nicht widerrufen.
- Vertrauenswürdigkeit: Ja – Mozilla, Apple, Android, Java und Windows vertrauen diesem Zertifikat.

Außerdem gibt der Bericht die Zertifikate weiter oben in der Zertifikats-Kette an:

- Zertifikat #2: Aussteller R3, RSA 2048 Bit, gültig bis 15. September 2025.
- Zertifikat #3: Aussteller ISRG Root X1, RSA 4096 Bit, gültig bis 30. September 2024.

—

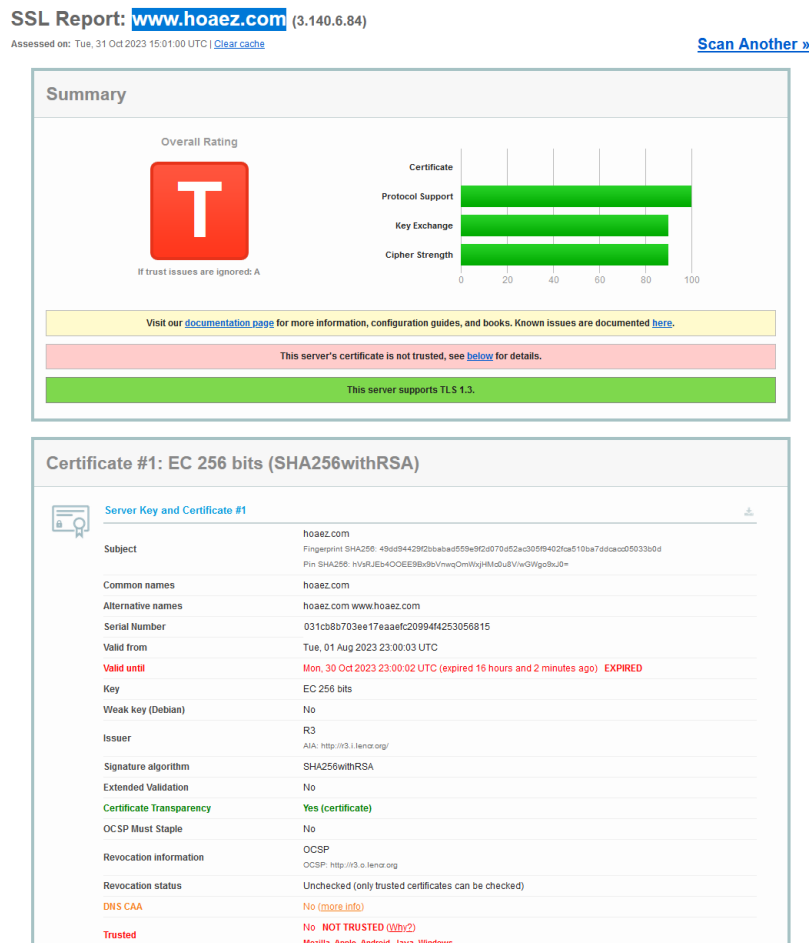


Abbildung 2: QualysSSL Test – Recent Worst

Der Server www.hoaez.com hat lediglich eine Gesamtbewertung von T erhalten, was bedeutet, dass dem Zertifikat des Servers nicht vertraut werden kann (e.g. da es abgelaufen ist, oder durch eine Misskonfiguration). Um dennoch einen Report erstellen zu können, hat Qualys die Vertrauenswürdigkeit bis auf weiteres ignoriert.

Unter der Zusammenfassung gibt es einen Abschnitt, der Details zum Zertifikat des Servers liefert. Diese deuten explizit darauf hin, dass das Zertifikat (zum Test-Zeitpunkt seit 16 Stunden) abgelaufen und somit nicht mehr gültig ist. Es ist anzunehmen, dass durch eine Erneuerung des Zertifikates, alle Probleme behoben werden können und der Server wieder eine ausreichend gute Bewertung erhalten würde.

Das Zertifikat an sich ist verwendet Elliptic-Curve mit 256 Bits und wurde ebenfalls mit SHA256+RSA signiert.

Dieser Report ist ein gutes Beispiel dafür, als Administrator im Idealfall auf sich-selbsterneuernde Zertifikate zu setzen, um einem Vertrauensverlust der Nutzer (durch eine Warnmeldung des Browsers) entgegen zu wirken.

1.2 SSL Test II

Aufgabenstellung

Führen Sie den Client-Test von Qualys aus und erklären Sie die Ergebnisse. (Siehe <https://clienttest.ssllabs.com:8443/ssltest/viewMyClient.html>)

Antwort

Wir haben den Client-Test mit der Mozilla Firefox Version 119.0.1 durchgeführt und folgendes Ergebnis erhalten:

The screenshot displays the Qualys SSL Labs 'SSL/TLS Capabilities of Your Browser' test results. The user agent is identified as Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0. The results are as follows:

- Protocol Support:** Your user agent has good protocol support. Your user agent supports TLS 1.2 and TLS 1.3, which are recommended protocol version at the moment.
- CVE-2020-0601 (CurveBall) Vulnerability:** Your user agent is not vulnerable. For more information about the CVE-2020-0601 (CurveBall) Vulnerability, please go to [CVE-2020-0601](https://cve-2020-0601). To test manually, click [here](#). Your user agent is not vulnerable if it fails to connect to the site.
- Logjam Vulnerability:** Your user agent is not vulnerable. For more information about the Logjam attack, please go to weakdh.org. To test manually, click [here](#). Your user agent is not vulnerable if it fails to connect to the site.
- FREAK Vulnerability:** Your user agent is not vulnerable. For more information about the FREAK attack, please go to www.freakattack.com. To test manually, click [here](#). Your user agent is not vulnerable if it fails to connect to the site.
- POODLE Vulnerability:** Your user agent is not vulnerable. For more information about the POODLE attack, please read [this blog post](#).

Abbildung 3: QualysSSL Test – Browser Capabilities

Im Kopf der Ergebnisseite wird eine Zusammenfassung der Bewertung ausgegeben. Es wird zunächst die Protokoll-Unterstützung mit grün/gut bewertet – in unserem Fall ob TLS 1.2 und TLS 1.3 unterstützt wird. Danach folgen spezifische Schwachstellentests:

- **Curveball / CVE-2020-0601** - Schwachstelle im Windows-OS bei der Validierung von digitalen Zertifikaten die potentiell angreifbar für MitM macht.
- **Logjam** - Sicherheitslücke im Diffie-Hellman-Schlüsselaustausch, welcher bei verschlüsselten Verbindungen wie TLS verwendet wird. Ermöglicht den Schlüsselaustausch zu manipulieren und verschlüsselte Verbindungen zu entschlüsseln.

- **FREAK (Factoring RSA Export Keys)** – Sicherheitslücke, die Angreifern es ermöglichte Verschlüsselung von HTTPS-Verbindungen zu umgehen.
- **POODLE (Padding Oracle On Downgraded Legacy Encryption)** - Schwachstelle in SSLv2/3 die es ermöglichte die Verschlüsselung zu umgehen.

Keine der Schwachstellen sind auf unserem Client vorhanden.





| Protocol Features | | | |
|---|---------|--|-------------|
|  Protocols | | | |
| TLS 1.3 | | | Yes |
| TLS 1.2 | | | Yes |
| TLS 1.1 | | | No |
| TLS 1.0 | | | No |
| SSL 3 | | | No |
| SSL 2 | | | No |
|  Cipher Suites (In order of preference) | | | |
| TLS_AES_128_GCM_SHA256 (0xc1301) Forward Secrecy | | | 128 |
| TLS_CHACHA20_POLY1305_SHA256 (0xc1303) Forward Secrecy | | | 256 |
| TLS_AES_256_GCM_SHA384 (0xc1302) Forward Secrecy | | | 256 |
| TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) Forward Secrecy | | | 128 |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) Forward Secrecy | | | 128 |
| TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc039) Forward Secrecy | | | 256 |
| TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc038) Forward Secrecy | | | 256 |
| TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc03c) Forward Secrecy | | | 256 |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc03d) Forward Secrecy | | | 256 |
| TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) VIEAK | | | 256 |
| TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) VIEAK | | | 128 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) VIEAK | | | 128 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) VIEAK | | | 256 |
| TLS_RSA_WITH_AES_128_GCM_SHA256 (0xc01c) VIEAK | | | 128 |
| TLS_RSA_WITH_AES_256_GCM_SHA384 (0xc01d) VIEAK | | | 256 |
| TLS_RSA_WITH_AES_128_CBC_SHA (0xc01f) VIEAK | | | 128 |
| TLS_RSA_WITH_AES_256_CBC_SHA (0xc01e) VIEAK | | | 256 |
| (1) When a browser supports SSL 2, its SSL 2-only suites are shown only on the very first connection to this site. To see the suites, close all browser windows, then open this exact page directly. Don't refresh. | | | |
|  Protocol Details | | | |
| Server Name Indication (SNI) | | Yes | |
| Secure Renegotiation | | Yes | |
| TLS compression | | No | |
| Session tickets | | No | |
| OCSP stapling | | Yes | |
| Signature algorithms | | SHA256/ECDSA, SHA384/ECDSA, SHA512/ECDSA, RSA_PSS_SHA256, RSA_PSS_SHA384, RSA_PSS_SHA512, SHA256/RSA, SHA384/RSA, SHA512/RSA, SHA1/ECDSA, SHA1/RSA | |
| Named Groups | | x25519, secp256r1, secp384r1, secp521r1, ffdhe2048, ffdhe3072 | |
| Next Protocol Negotiation | | No | |
| Application Layer Protocol Negotiation | | Yes | h2 http/1.1 |
| SSL 2 handshake compatibility | | No | |
| Mixed Content Handling | | | |
|  Mixed Content Tests | | | |
| Images | Passive | | No |
| CSS | Active | | No |
| Scripts | Active | | No |
| XMLHttpRequest | Active | | No |
| WebSockets | Active | | No |
| Frames | Active | | No |
| (1) These tests might cause a mixed content warning in your browser. That's expected. (2) If you see a failed test, try to reload the page. If the error persists, please get in touch. | | | |
| Related Functionality | | | |
| Upgrade Insecure Requests request header (more info) | | | Yes |

Abbildung 4: QualysSSL Test – Browser Protocol Features

Es folgt eine Detailauflistung der Protokoll-Features, die ergänzt ist um eine Auflistung der unterstützten Cipher Suites in Reihenfolge der Präferenz (von oben nach unten). Dabei werden viele kryptographische Verfahren als grün/gut bewertet, einige aber als weak. Dies ist z.B. auf die Duldung von SHA (anstatt SHA256) zurückzuführen, oder weil der CBC-Modus (Cipher Block Chaining) erlaubt wird. CBC hat bekannte Schwächen, beispielsweise auf Angriffe wie den sogenannten "Padding Oracle Attack". Die Ermöglichung von CBC in Verbindung mit älteren Authentifizierungsalgorithmen wie SHA1 wird hier vermutlich als unsicher (auf englisch: weak) angesehen.

Unter der Überschrift **Protocol Details** wird als gut/grün hervorgehoben, dass TLS compression deaktiviert ist. Dies war ein Feature in älteren TLS-Versionen und sollte Daten komprimieren vor der Verschlüsselung, war jedoch angreifbar und wurde daher in Folgeversion deaktiviert. Ebenfalls deaktiviert sein sollte die SSL 2 handshake compatibility – dies ist die bereits erwähnte POODLE Schwachstelle. Die letzte farbliche Hervorhebung in diesem Abschnitt lautet **Session tickets – No**. Warum die Deaktivierung von Session-Tickets als weak gekennzeichnet wurde, konnten wir nicht 100% feststellen. Der Blog der Betreiber-Webseite beschreibt diesen Eintrag hauptsächlich aus Sicht eines Web-Server/-Seiten Betreibers so, „dass session tickets ein alternativer Session-Management Mechanismus sei, welcher separate Encryption Keys verwendet, die selten rotiert werden und lieber nicht verwendet werden sollten, wenn man die Implementation nicht genau im Detail versteht.“ (vgl. <https://blog.qualys.com/product-tech/2013/06/25/ssl-labs-deploying-forward-secrecy>, abgerufen am 09.11.2023). Es erschien uns eher als Vorteil denn als Nachteil dass dieses Feature im Firefox deaktiviert sei.

Den Abschluss der Ergebnisseite bildet der Abschnitt **Mixed Content Handling**, in dem die Kompatibilität mit diversen Webtechnologien (z.B. CSS, Frames usw.) getestet wird.

1.3 SSL Test III

Aufgabenstellung

Rufen Sie die Test-Webseiten <https://aaacertificateservices.comodoca.com:442/> sowie <https://aaacertificateservices.comodoca.com:444/> mit Firefox und mit Google Chrome auf. Erklären Sie, was passiert. Sind die Resultate bei allen vier Tests so wie erwartet?

Antwort

Um das Verhalten der beiden Browser näher zu betrachten haben wir uns dazu entschieden, die Tests simultan durchzuführen, um zu veranschaulichen, wann die beiden Browser sich anders verhalten. Als erstes haben wir den Server auf dem Port 442 getestet:

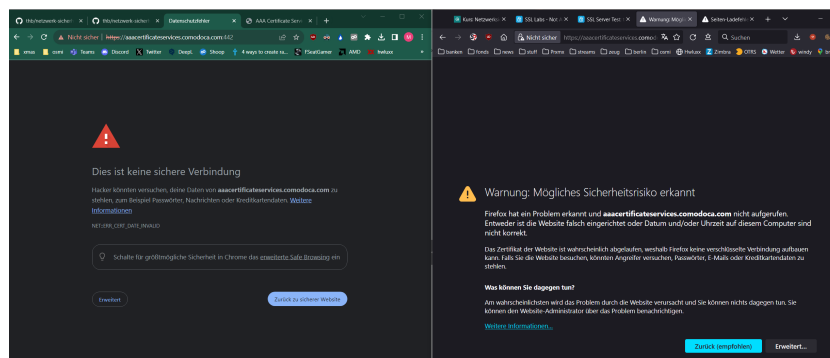


Abbildung 5: Google Chrome vs Firefox – 442 – Unsafe / Unsafe

Bei diesem Web-Server / Port erkennen beide Browser direkt ein abgelaufenes Zertifikat und warnen den Nutzer davor, diese Webseite zu verwenden (da die Identität des Servers nicht sicher gestellt werden konnte).

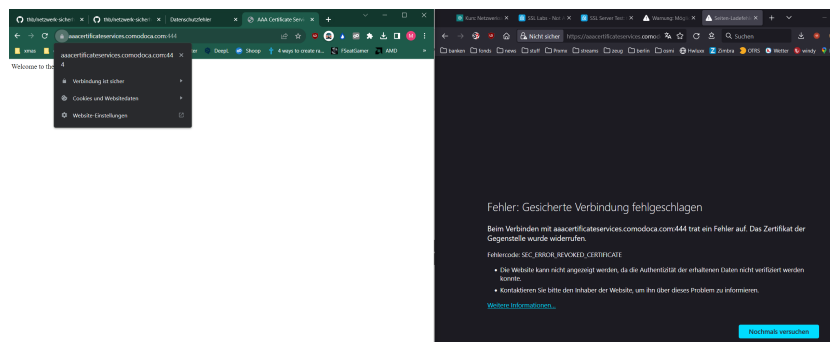


Abbildung 6: Google Chrome vs Firefox – 444 – Safe / Unsafe

Bei dem zweiten Test (also dem Server auf Port 444) verhalten sich die Browser interessanterweise unterschiedlich: Chrome zeigt dies als sichere Verbindung an, obwohl Firefox warnt und angibt, dass das Zertifikat widerrufen worden sei.

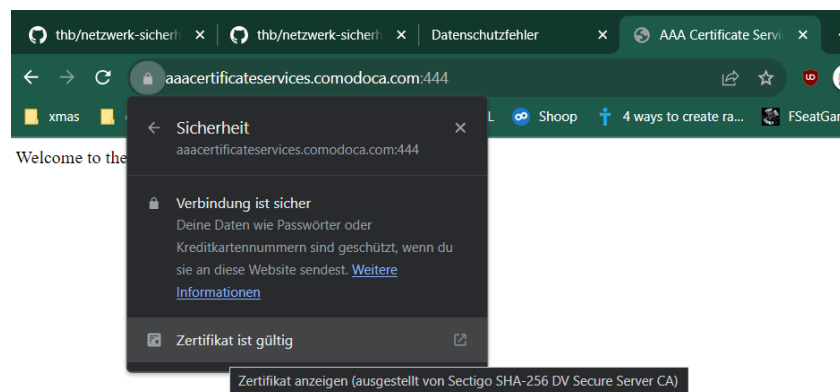


Abbildung 7: Google Chrome vs Firefox – 444 – Details

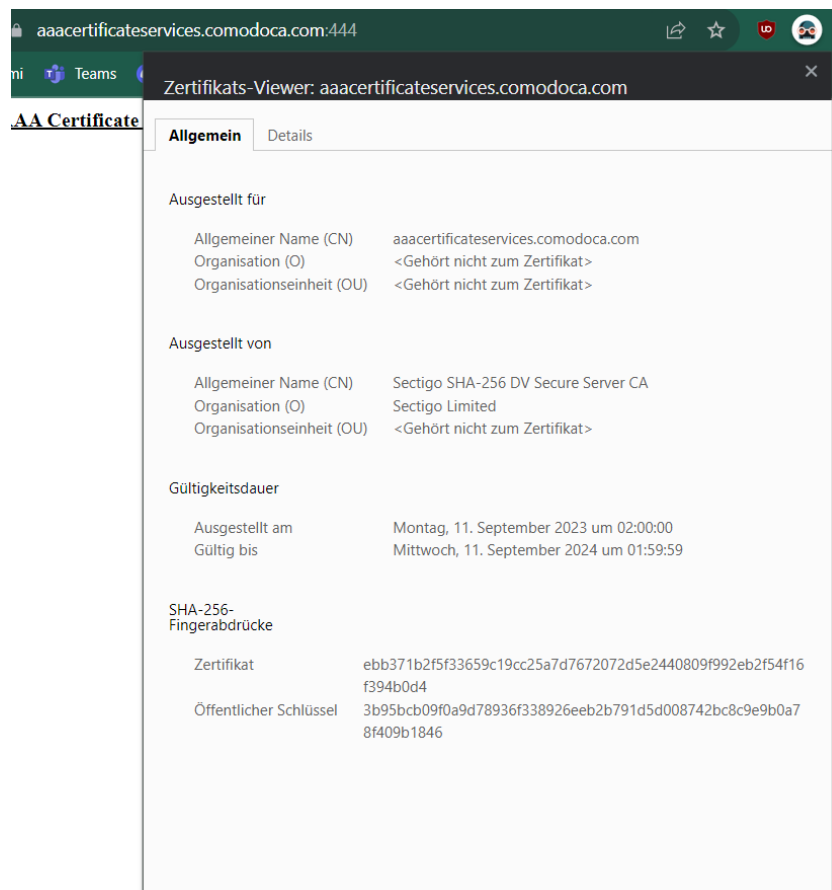


Abbildung 8: Google Chrome vs Firefox – 444 – Chrome Zertifikat

Auch bei näherer Betrachtung des Zertifikats im Chrome-Certificate-Viewer, lässt sich keine Spur von dem Widerruf finden.

Die unterschiedlichen Verhaltensweisen der Browser könnten mehrere Gründe haben:

1. **CRL und OCSP:** Chrome und Firefox verwenden wahrscheinlich unterschiedliche Methoden zur Überprüfung des Widerrufsstatus eines Zertifikats. Chrome überprüft möglicherweise nicht den Widerrufsstatus oder konnte den Certificate Revocation List (CRL) oder Online Certificate Status Protocol (OCSP) Server nicht erreichen. Wenn der Server nicht erreichbar ist, kann Chrome die Verbindung unter bestimmten Bedingungen zulassen.
2. **Caching:** Es könnte ein Caching-Problem vorliegen, bei dem Chrome das Zertifikat oder seinen Status zwischengespeichert hat und keinen Live-Check durchführt, um zu sehen, ob das Zertifikat widerrufen wurde.
3. **Widerrufsinformationen:** Es ist auch möglich, dass Firefox aktualisierte Widerrufsinformationen hat, die Chrome nicht hat. Dies kann passieren, wenn die Widerrufsinformationen kürzlich aktualisiert wurden und Chrome das Update noch nicht erhalten hat.
4. **Browser-Konfiguration:** Die Sicherheitseinstellungen des Browsers könnten unterschiedlich konfiguriert sein. Zum Beispiel könnte Chrome so eingerichtet sein, dass es mit bestimmten Arten von Zertifikatsfehlern fortfährt, die Firefox nicht zulässt, oder umgekehrt.
5. **Certificate Pinning:** Chrome könnte das Zertifikat für diese Seite gepinnt haben, was die normale Überprüfung der Vertrauenskette umgehen würde, die sonst zu einer erkannten Widerrufsstatus führen könnte.

Da wir allerdings beide Browser kontrollieren und beide Browser zum Zeitpunkt des Tests auf dem neusten Stand waren und wir den Web-Server vorher noch nie verwendet haben, deutet dies auf eine Diskrepanz bei den CRL / OCSP Abfragen hin – wahrscheinlich, da unterschiedliche Informationen verwendet werden.

In einem solchen Fall, sollte immer dem Browser mit Sicherheitsbedenken vertraut werden.

1.4 Verschlüsselung

Aufgabenstellung

Installieren Sie VeraCrypt auf Ihrem Rechner. Hierzu erhalten Sie zusätzlich eine VeraCrypt-Datei. In der Datei ist ein normaler und ein versteckter Container zu finden, die jeweils eine Datei enthalten. Das Passwort für den normalen Container ist der Exponent e des RSA-Schlüssels vom nwsmooc.mooiin.org-Server. Dokumentieren Sie Ihre Vorgehensweise mit Screenshots und geben Sie anschließend das im versteckten Container gefundene Kennwort an.

Hinweis: Zur Bedienung von VeraCrypt können Sie sich beispielsweise hier ein Video ansehen: <https://youtu.be/atb2pdx394>.

Antwort

ÜBERARBEITEN

Um das zur Verfügung gestellte VeraCrypt File öffnen zu können, soll der Exponent e des RSA-Schlüssels der Webseite nwsmooc.mooiin.org verwendet werden. Diesen Exponenten kann man sich ganz einfach ausgeben lassen, in dem man sich im Mozilla Firefox Browser jene Webseite öffnet und auf das Schlosssymbol drückt, um sich das Zertifikat anzusehen.

Im Abschnitt „Öffentlicher Schlüssel – Informationen“ bekommt man diesen einfach ausgegeben (Siehe Abbildung XXX). Wir merken an dieser Stelle an, dass wir diesen Exponenten zunächst auch blind getestet hatten, da in der Praxis fast immer die Zahl 65537 als Exponent verwendet wird. Für das RSA Verfahren werden große Primzahlen bevorzugt verwendet und der Algorithmus muss dabei unterschiedliche Operationen bei der Bearbeitung basierend auf dem Binärkode tätigen. 6553710 ist binär kodiert 10000000000000001 (?????????????) was es zu einer effizienten Zahl für den Algorithmus macht (Einsen werden multipliziert, Nullen potenziert).

Mounted man mit VeraCrypt die bereitgestellte Datei und gibt als Passwort 65537 an, erhält man Zugriff auf die Datei. (siehe Abbildung XXX)

Der Inhalt des Textfiles „Datei-angezeigter-Container.txt“ lautet: „Das Zugangskennwort für den versteckten Container lautet: VerSteCon0815“

Wir konnten uns an das Modul Digitaler Selbstschutz erinnern, in dessen Reportinhalt VeraCrypt bereits vorkam, und haben den Container gecloned und ein 2. Mal gemounted, wobei wir dieses Mal das Passwort VerSteCon0815 eingegeben haben.

Damit konnten wir Zugriff auf den versteckten Container und seinem Inhalt „Datei- versteckter-Container.txt“ erhalten.

Der Text dieser Datei lautet:

Das gesuchte Kennwort lautet: HiddenVolumeVeraCrypt

Die anderen Einstellungen entsprechen den Default-Einstellungen

Für mooin.jpg: Luminance Interval = 5 Header Position = bottom CharSet = UTF8

Für mooin.bmp (Oben beim "Media's encoding format" auf "BMP" wechseln): Image quality: 96,975 Aktivieren Sie zusätzlich zu "Compressed Data" jeweils auch "Encrypted Data" mit AES256. Dort muss der Key in beide Kästchen eingetragen werden. Über die SilentEye-Aufgabe erhalten Sie über mooin.bmp übrigens schon vorab eine Aufgabensammlung zur Klausurvorbereitung.

1.5 Steganographie

Aufgabenstellung

Installieren Sie SilentEye auf Ihrem Rechner und untersuchen Sie die bereitgestellten Beispieldateien. mooin.jpg enthält ein verstecktes Kennwort, mooin.bmp eine Datei. Die notwendigen Einstellungen können Sie der Aufgabe mit VeraCrypt entnehmen. Dokumentieren Sie Ihre Vorgehensweise mit Screenshots und geben Sie das gefundene Kennwort an.

Hinweis: Sollte es Schwierigkeiten geben, wenn Sie beide Dateien nacheinander untersuchen, dann schließen Sie SilentEye zwischendurch.

Antwort

ÜBERARBEITEN

SilentEye ist eine Open-Source-Software, die zur Steganographie verwendet wird, um zusätzliche Informationen in Bildern und Audiodateien zu verstecken oder auszulesen.

Um mooin.jpg zu untersuchen, öffnen wir die Datei mit dem Programm SilenteYe und verwenden die Einstellungen aus der Lösung der Aufgabe 1.4.

Dadurch kann der verborgene Bereich des Bildes erfolgreich entschlüsselt werden und gibt als dekodierte Message den Text “Kennwort: SteganographieInNWSMOOC” frei.

Mit diesem Kennwort und den bereitgestellten Einstellungen für das zweite Bild, lässt sich auch dessen versteckter Inhalt sichtbar machen und entschlüsseln. Wir können an dieser Stelle die Datei AufgabensammlungSS16.pdf extrahieren und abspeichern.