

Softwaresicherheit

x.509 Certificate Validation:
challenges, pitfalls, bugs

Julian Hinxlage, Edgar Schkrob und Johannes Theiner

Fachbereich Technik
Abteilung Elektrotechnik und Informatik

21.11.2019

2022-01-20

- Vorstellung Thema
- Vorstellung Gruppe

Übersicht

Grundlagen

Validierung von Extensions

Weitere Probleme

nicht technische Probleme

Fazit

2022-01-20

└ Übersicht

Übersicht

Grundlagen
Validierung von Extensions
Weitere Probleme
nicht technische Probleme
Fazit

Grundlagen

Allgemein

- ▶ Standard der ITU-T
- ▶ auch bekannt als ISO/IEC 9594-8
- ▶ wird in TLS, SSL, HTTPS, und S/MIME angewendet
- ▶ Vertrauenswürdige Zertifikatsstellen vorausgesetzt

2022-01-20

└ Grundlagen
└ Allgemein
└ Allgemein

Allgemein

- ▶ Standard der ITU-T
- ▶ auch bekannt als ISO/IEC 9594-8
- ▶ wird in TLS, SSL, HTTPS, und S/MIME angewendet
- ▶ Vertrauenswürdige Zertifikatsstellen vorausgesetzt

Zertifikatsstruktur

- ▶ Version
- ▶ Seriennummer
- ▶ Algorithmen-ID
- ▶ Aussteller
- ▶ Gültigkeit
- ▶ Inhaber
- ▶ Inhaber-Schlüsselinformationen
- ▶ Eindeutige ID des Ausstellers
- ▶ Eindeutige ID des Inhabers
- ▶ Erweiterungen
- ▶ Signatur

2022-01-20

└ Grundlagen
└ Zertifikatsstruktur
└ Zertifikatsstruktur

Zertifikatsstruktur

- ▶ Version
- ▶ Seriennummer
- ▶ Algorithmen-ID
- ▶ Aussteller
- ▶ Gültigkeit
- ▶ Inhaber
- ▶ Inhaber-Schlüsselinformationen
- ▶ Eindeutige ID des Ausstellers
- ▶ Eindeutige ID des Inhabers
- ▶ Erweiterungen
- ▶ Signatur

Zertifikatsstruktur

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1 (0x1)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=AT, ST=Steiermark, L=Graz, O=TrustMe Ltd

Validity

Not Before: Oct 29 17:39:10 2000 GMT

Not After : Oct 29 17:39:10 2001 GMT

2022-01-20

└─ Grundlagen
└─ Zertifikatsstruktur
└─ Zertifikatsstruktur

Zertifikatsstruktur

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1 (0x1)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=AT, ST=Steiermark, L=Graz, O=TrustMe Ltd

Validity

Not Before: Oct 29 17:39:10 2000 GMT

Not After : Oct 29 17:39:10 2001 GMT

Zertifikatsstruktur

Subject: C=AT, ST=Vienna, L=Vienna, O=Home, OU=Web Lab, CN

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:c4:...

2022-01-20

└─ Grundlagen
└─ Zertifikatsstruktur
└─ Zertifikatsstruktur

Zertifikatsstruktur

Subject: C=AT, ST=Vienna, L=Vienna, O=Home, OU=Web Lab, CN
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:c4:...

Zertifikatsstruktur

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Alternative Name:

email:xyz@anywhere.com

Netscape Comment:

mod_ssl generated test server certificate

Netscape Cert Type:

SSL Server

Signature Algorithm: md5WithRSAEncryption

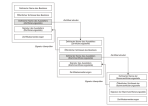
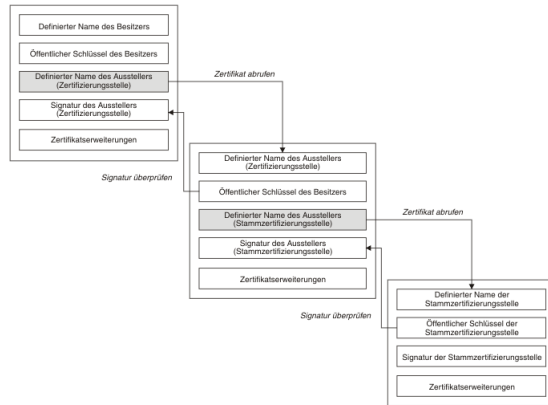
2022-01-20

└─ Grundlagen
└─ Zertifikatsstruktur
└─ Zertifikatsstruktur

Zertifikatsstruktur

Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Alternative Name:
email:xyz@anywhere.com
Netscape Comment:
mod_ssl generated test server certificate
Netscape Cert Type:
SSL Server
Signature Algorithm: md5WithRSAEncryption

Zertifikatskette



2022-01-20

└ Grundlagen
└ Zertifikatskette
└ Zertifikatskette

Validierung von Extensions

Key Usage

- ▶ die Nutzung des Schlüssels wird limitiert
- ▶ mehrere Werte können angenommen werden
- ▶ z.b. kann ein Zertifikat nur eingesetzt werden um andere Zertifikate zu signieren

2022-01-20

└ Validierung von Extensions
└ Key Usage
└ Key Usage

Key Usage

- ▶ die Nutzung des Schlüssels wird limitiert
- ▶ mehrere Werte können angenommen werden
- ▶ z.b. kann ein Zertifikat nur eingesetzt werden um andere Zertifikate zu signieren

KCI Attacke

- ▶ KCI steht für Key Compromise Impersonation
- ▶ es ist eine Man in the middle Attacke
- ▶ über Client Zertifikat konnte ein Server Zertifikat ausgestellt werden
- ▶ möglich da die Key Usage Validierung nicht richtig implementiert war

2022-01-20

└ Validierung von Extensions
└ Key Usage
└ KCI Attacke

KCI Attacke

- ▶ KCI steht für Key Compromise Impersonation
- ▶ es ist eine Man in the middle Attacke
- ▶ über Client Zertifikat konnte ein Server Zertifikat ausgestellt werden
- ▶ möglich da die Key Usage Validierung nicht richtig implementiert war

Critical Extensions

- ▶ Zertifikate mit unbekannten "critical" Erweiterungen sind ungültig
- ▶ Bekannte "critical" Erweiterungen müssen überprüft werden

2022-01-20

└ Validierung von Extensions
└ Critical Extensions
└ Critical Extensions

Critical Extensions

- ▶ Zertifikate mit unbekannten "critical" Erweiterungen sind ungültig
- ▶ Bekannte "critical" Erweiterungen müssen überprüft werden

Hostname Validation

- ▶ Hostname des Antragstellers
- ▶ Domain bei Webserver Zertifikaten
- ▶ E-Mail-Adresse bei E-Mail Zertifikaten
- ▶ nicht in allen Anwendungsgebieten einheitlich

2022-01-20

└ Validierung von Extensions
└ Hostname Validation
└ Hostname Validation

Hostname Validation

- ▶ Hostname des Antragstellers
- ▶ Domain bei Webserver Zertifikaten
- ▶ E-Mail-Adresse bei E-Mail Zertifikaten
- ▶ nicht in allen Anwendungsgebieten einheitlich

Basic Constraints

- ▶ gibt an, ob ein Zertifikat ein CA Zertifikat ist
- ▶ Anzahl der darauf folgenden Zertifikate

2022-01-20

- └ Validierung von Extensions
 - └ Basic Constraints
 - └ Basic Constraints

Basic Constraints

- ▶ gibt an, ob ein Zertifikat ein CA Zertifikat ist
- ▶ Anzahl der darauf folgenden Zertifikate

Name Constraints

- ▶ Limitierung von CA Zertifikaten
- ▶ welche Art von Zertifikate dürfen in der Kette folgen

2022-01-20

- └ Validierung von Extensions
 - └ Name Constraints
 - └ Name Constraints

Name Constraints

- ▶ Limitierung von CA Zertifikaten
- ▶ welche Art von Zertifikate dürfen in der Kette folgen

Weitere Probleme

Validity Dates

- ▶ enthält Felder "notBefore" und "notAfter"
- ▶ bei fehlerhafter Prüfung könnten abgelaufene Zertifikate genutzt werden

2022-01-20

- └ Weitere Probleme
 - └ Validity Dates
 - └ Validity Dates

Validity Dates

- ▶ enthält Felder "notBefore" und "notAfter"
- ▶ bei fehlerhafter Prüfung könnten abgelaufene Zertifikate genutzt werden

Certificate Chain Validation

- ▶ alle Schritte müssen für alle Zertifikate in der Kette ausgeführt werden
- ▶ Root Zertifikate sind selbst signiert

2022-01-20

- └ Weitere Probleme
 - └ Certificate Chain Validation
 - └ Certificate Chain Validation

Certificate Chain Validation

- ▶ alle Schritte müssen für alle Zertifikate in der Kette ausgeführt werden
- ▶ Root Zertifikate sind selbst signiert

Certificate Revocation

- ▶ Liste von für ungültig erklärten Zertifikaten
- ▶ muss angefragt werden, wenn ein Zertifikat überprüft wird
- ▶ stellt weitere Anforderungen an die Infrastruktur

2022-01-20

- └ Weitere Probleme
 - └ Certificate Revocation
 - └ Certificate Revocation

Certificate Revocation

- ▶ Liste von für ungültig erklärten Zertifikaten
- ▶ muss angefragt werden, wenn ein Zertifikat überprüft wird
- ▶ stellt weitere Anforderungen an die Infrastruktur

Redirection

- ▶ bei Weiterleitungen muss das Zertifikat des Ziels überprüft werden
- ▶ wurde bei der CA StartEncrypt missachtet

2022-01-20

└ Weitere Probleme
└ Redirection
└ Redirection

Redirection

- ▶ bei Weiterleitungen muss das Zertifikat des Ziels überprüft werden
- ▶ wurde bei der CA StartEncrypt missachtet

StartEncrypt

- ▶ Kontrolle über Domain wird häufig über eine vorhandene Datei bewiesen
- ▶ Datei konnte sich hinter einer Weiterleitung befinden
- ▶ gültige Zertifikate wurden ausgestellt

2022-01-20

└ Weitere Probleme
└ Redirection
└ StartEncrypt

Pfad der Datei konnte in diesem Fall geändert werden

Datei konnte auch bei Dateihostern wie Dropbox gehostet werden um dort Zertifikate zu erhalten

StartEncrypt

- ▶ Kontrolle über Domain wird häufig über eine vorhandene Datei bewiesen
- ▶ Datei konnte sich hinter einer Weiterleitung befinden
- ▶ gültige Zertifikate wurden ausgestellt

Weak Algorithm

- ▶ Signaturverfahren sowie Hashfunktion wichtig
- ▶ unterschiedliche Schlüssellängen
- ▶ längere Zeit wurde die gebrochene Hashfunktion md5 verwenden
- ▶ die Wahl des richtigen Verfahrens ist wichtig und für die Sicherheit von Zertifikaten essenziell

2022-01-20

- └ Weitere Probleme
 - └ Weak Algorithm
 - └ Weak Algorithm

Weak Algorithm

- ▶ Signaturverfahren sowie Hashfunktion wichtig
- ▶ unterschiedliche Schlüssellängen
- ▶ längere Zeit wurde die gebrochene Hashfunktion md5 verwenden
- ▶ die Wahl des richtigen Verfahrens ist wichtig und für die Sicherheit von Zertifikaten essenziell

Verwendung von Bibliotheken

Viele Bibliotheken sind:

- ▶ sind kompliziert aufgebaut
- ▶ haben schlechte Standardwerte

2022-01-20

- └ Weitere Probleme
 - └ Verwendung von Bibliotheken
 - └ Verwendung von Bibliotheken

Verwendung von Bibliotheken

Viele Bibliotheken sind:

- ▶ sind kompliziert aufgebaut
- ▶ haben schlechte Standardwerte

[1]

nicht technische Probleme

Verbindungssicherheit

HTTPS & SSL doesn't mean "trust this." It means "this is private." You may be having a private conversation with Satan.

— Scott Hanselmann <https://twitter.com/shanselman/status/187572289724887041>

2022-01-20

- └ nicht technische Probleme
 - └ Verbindungssicherheit
 - └ Verbindungssicherheit

oder: Ein Zertifikat hat keine Aussage darüber, ob der Gesprächspartner vertrauenswürdig ist. Nur das er derjenige ist für den er sich ausgibt.

Verbindungssicherheit

Why is it a good idea to look for a small padlock icon in the browser window when visiting a web shop?

- ☒ Because it shows that the web shop is a secure site.
- ☐ Because it shows that the web shop has good offers.
- ☐ Because it makes shopping faster.

2022-01-20

└ nicht technische Probleme
└ Verbindungssicherheit
└ Verbindungssicherheit

Verbindungssicherheit

Why is it a good idea to look for a small padlock icon in the browser window when visiting a web shop?

- ☒ Because it shows that the web shop is a secure site.
- ☐ Because it shows that the web shop has good offers.
- ☐ Because it makes shopping faster.

Verbindungssicherheit

Why is it a good idea to look for a small padlock icon in the browser window when visiting a web shop?

- ☒ Because it shows that the web shop is a secure site.
- ☐ Because it shows that the web shop has good offers.
- ☐ Because it makes shopping faster.

Taking a mandatory Cyber Awareness Course. The correct answer to this question is: The traffic between the browser and the webshop is encrypted. But the option does not exist. cc @troyhunt

2022-01-20

└ nicht technische Probleme
└ Verbindungssicherheit
└ Verbindungssicherheit

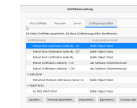
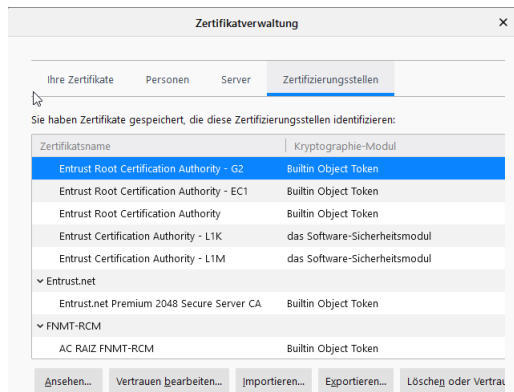
Verbindungssicherheit

Why is it a good idea to look for a small padlock icon in the browser window when visiting a web shop?

- ☒ Because it shows that the web shop is a secure site.
- ☐ Because it shows that the web shop has good offers.
- ☐ Because it makes shopping faster.

Taking a mandatory Cyber Awareness Course. The correct answer to this question is: The traffic between the browser and the webshop is encrypted. But the option does not exist. cc @troyhunt

Vertrauen in die Zertifikatskette



2022-01-20

- └ nicht technische Probleme
 - └ Vertrauen in die Zertifikatskette
 - └ Vertrauen in die Zertifikatskette

Zertifikatsspeicher des Brower

Die ersten Einträge sehen harmlos aus
letzter Eintrag nicht unbedingt

So hat Kazakhstan 2014 über Antrag bei Browserherstellern versucht ein Root Zertifikat hinzuzufügen um MITM bei eigenen Bürgern durchzuführen. 2019 über ISPs die Bürger zwingen, sonst kein Internetzugriff. Apple, Google und Mozilla haben das Zertifikat inzwischen blockiert und aktuell ist diese Praxis nicht aktiv

IDN homograph attack



2022-01-20

- └ nicht technische Probleme
 - └ IDN homograph attack
 - └ IDN homograph attack

IDN homograph attack

Apple Inc. (US) | https://www.apple.com

Beim Darstellen von Namen etc. drauf achten das einige Zeichen aus unterschiedlichen Alphabeten sich sehr ähnlich sehen.

IDN homograph attack

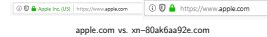


apple.com vs. xn-80ak6aa92e.com

2022-01-20

- └ nicht technische Probleme
 - └ IDN homograph attack
 - └ IDN homograph attack

IDN homograph attack



Beim Darstellen von Namen etc. drauf achten das einige Zeichen aus unterschiedlichen Alphabeten sich sehr ähnlich sehen.

IDN homograph attack



apple.com vs. xn-80ak6aa92e.com

Unterschiedliche Domains, gleiche Darstellung

2022-01-20

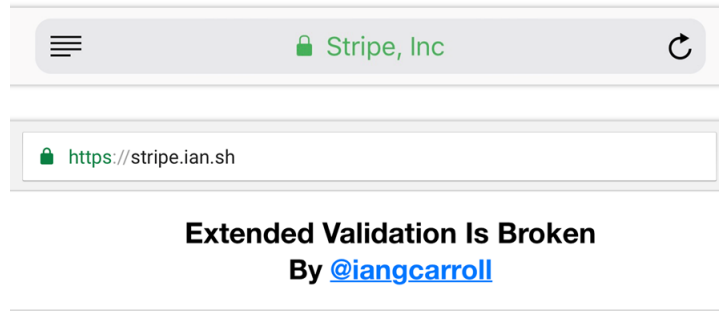
- └ nicht technische Probleme
 - └ IDN homograph attack
 - └ IDN homograph attack

IDN homograph attack



Beim Darstellen von Namen etc. drauf achten das einige Zeichen aus unterschiedlichen Alphabeten sich sehr ähnlich sehen.

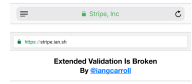
Extended Validation



2022-01-20

- └ nicht technische Probleme
 - └ Extended Validation
 - └ Extended Validation

Extended Validation



Extended Validation Zertifikate sind eine Erweiterung von x.509. Diese Zertifikate erhält man nur mit Unternehmensregistrierung von einigen wenigen CAs. Da mehrere Firmen den selben Namen tragen können (unterschiedliche Standorte) können auch mehrere Zertifikate erstellt werden. [2]

Fazit

Fazit

- ▶ Libraries zum validieren verwenden
- ▶ positive Indikatoren vermeiden
- ▶ Alternative: SSH

2022-01-20

└─Fazit

└─Fazit

Fazit

- ▶ Libraries zum validieren verwenden
- ▶ positive Indikatoren vermeiden
- ▶ Alternative: SSH

Danke für die Aufmerksamkeit

Literatur I

- [1] M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh und V. Shmatikov, „The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software,“ Techn. Ber., 2012.
- [2] I. Carroll, „Extended Validation Is Broken,“ (29. Apr. 2018), Adresse: <https://stripe.ian.sh/> (besucht am 06.11.2019).

2022-01-20

└─Fazit

└─Literatur

Literatur I

- [1] M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh und V. Shmatikov, „The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software,“ Techn. Ber., 2012.
- [2] I. Carroll, „Extended Validation Is Broken,“ (29. Apr. 2018), Adresse: <https://stripe.ian.sh/> (besucht am 06.11.2019).

Literatur II

- [3] X. Zheng, „Phishing with Unicode Domains,“ (14. Apr. 2017),
Adresse:
<https://www.xudongz.com/blog/2017/idn-phishing/>
(besucht am 26.10.2019).

2022-01-20

└─Fazit

└─Literatur

Literatur II

[3] X. Zheng, „Phishing with Unicode Domains,“ (14. Apr. 2017),
Adresse:
<https://www.xudongz.com/blog/2017/idn-phishing/>
(besucht am 26.10.2019).

Literatur III

- [4] T. Hunt, „The Decreasing Usefulness of Positive Visual Security Indicators (and the Importance of Negative Ones),“ (7. Mai 2018), Adresse:
<https://www.troyhunt.com/the-decreasing-usefulness-of-positive-visual-security-indicators-and-the-importance-of-negative-ones/>
(besucht am 02.11.2019).

2022-01-20

└─Fazit

└─Literatur

Literatur III

- [4] T. Hunt, „The Decreasing Usefulness of Positive Visual Security Indicators (and the Importance of Negative Ones),“ (7. Mai 2018), Adresse:
<https://www.troyhunt.com/the-decreasing-usefulness-of-positive-visual-security-indicators-and-the-importance-of-negative-ones/>
(besucht am 02.11.2019).

Literatur IV

- [5] R. Housley, R. Laboratories, W. Polk u. a., „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,“ RFC 3280, 25. Okt. 2020.
- [6] D. Cooper, NIST, S. Santesson u. a., „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,“ RFC 5280, 2008.

2022-01-20

└─Fazit

└─Literatur

Literatur IV

- [5] R. Housley, R. Laboratories, W. Polk u. a., „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,“ RFC 3280, 25. Okt. 2020.
- [6] D. Cooper, NIST, S. Santesson u. a., „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,“ RFC 5280, 2008.

Literatur V

- [7] C. Cimpanu, „Apple, Google, and Mozilla block Kazakhstan’s HTTPS intercepting certificate,“ (21. Aug. 2019), Adresse: <https://www.zdnet.com/article/apple-google-and-mozilla-block-kazakhstans-https-intercepting-certificate/> (besucht am 12.11.2019).
- [8] C. Hlauschek, M. Gruber, F. Fankhauser und C. Schanes, „Prying open Pandora’s box: KCI attacks against TLS,“ Techn. Ber., 2015.

2022-01-20

└─Fazit

└─Literatur

Literatur V

- [7] C. Cimpanu, „Apple, Google, and Mozilla block Kazakhstan’s HTTPS intercepting certificate,“ (21. Aug. 2019), Adresse: <https://www.zdnet.com/article/apple-google-and-mozilla-block-kazakhstans-https-intercepting-certificate/> (besucht am 12.11.2019).
- [8] C. Hlauschek, M. Gruber, F. Fankhauser und C. Schanes, „Prying open Pandora’s box: KCI attacks against TLS,“ Techn. Ber., 2015.

Literatur VI

- [9] R. Eikenberg, „Gratis-CA StartEncrypt beginnt mit Sicherheitsproblemen,“ (2. Juli 2016), Adresse: <https://www.heise.de/security/meldung/Gratis-CA-StartEncrypt-beginnt-mit-Sicherheitsproblemen-3252904.html> (besucht am 13.11.2019).

2022-01-20

└─Fazit

└─Literatur

Literatur VI

[9] R. Eikenberg, „Gratis-CA StartEncrypt beginnt mit Sicherheitsproblemen,“ (2. Juli 2016), Adresse: <https://www.heise.de/security/meldung/Gratis-CA-StartEncrypt-beginnt-mit-Sicherheitsproblemen-3252904.html> (besucht am 13.11.2019).