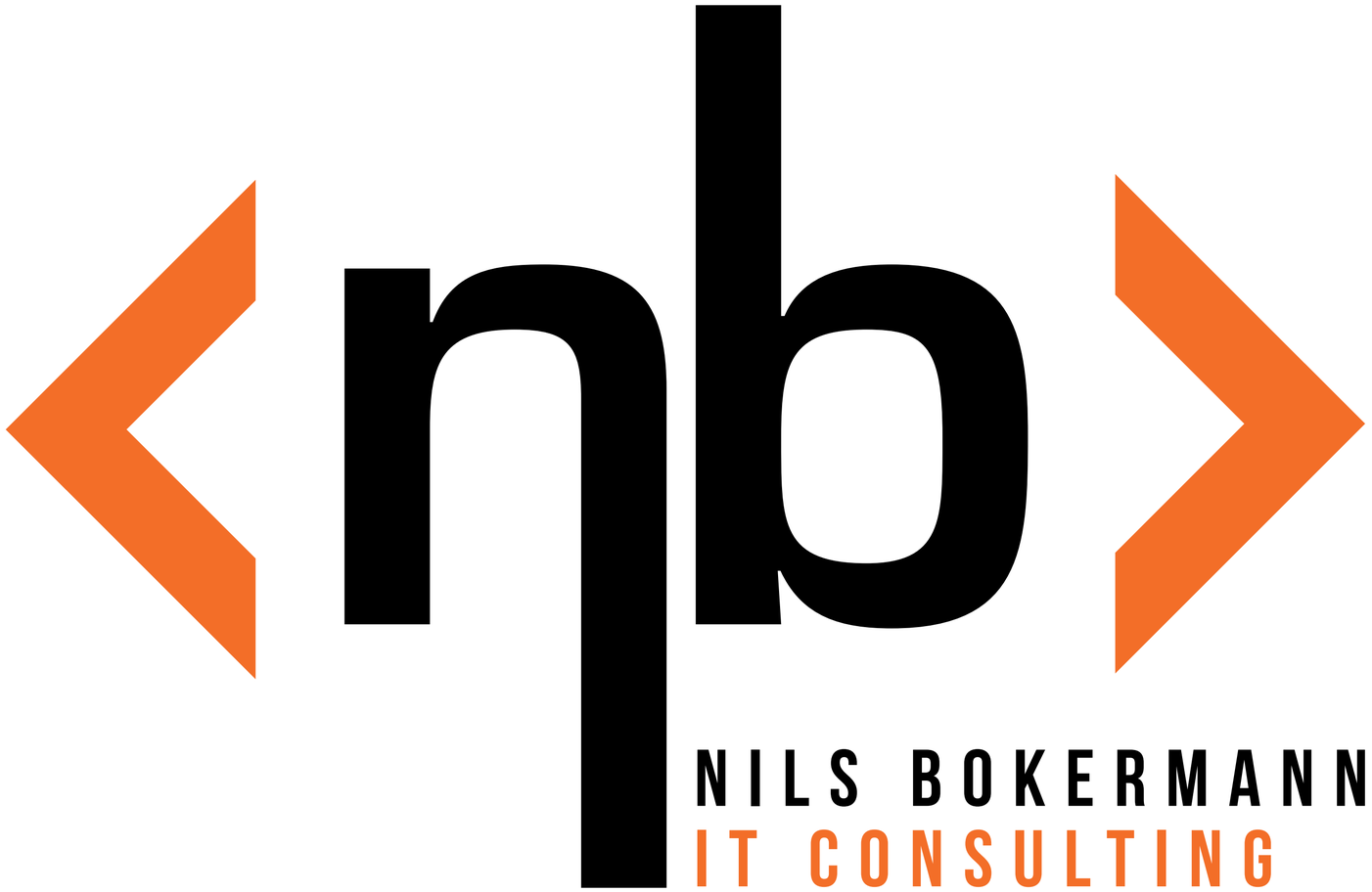


Wie sicher ist „Sicher“?

TLS und weiter?

JFS 2022 - Stuttgart

Über mich

Nils Bokermann

- freiberuflicher Softwareentwickler
- Chemiker ;-)

Schwerpunkte

- Entwicklung von Java Enterprise Anwendungen
- Ende zu Ende Verantwortlichkeit


info@bermuda.de


@sanddorn


xing.to/sanddorn

Agenda

- Netzwerkprotokoll
- TLS Life Hacking
- Use-Cases
- Zertifizierung (CA)

Alice und Bob

Client Hello

SessionId, Liste von unterstützen Algorithmen

Server Hello

SessionId, Gewählter Algorithmus

Certificate, Server Key Exchange, Server Hello Done

Zertifikat

Client Key Exchange

Premaster Secret

ChangeCipherSpec, Finished

ChangeCipherSpec, Finished

Zertifikat

Private Key

NILS BOKERMANN
IT CONSULTING

Vertrauensverhältnis

Was haben Alice und Bob erreicht:

- Gesicherte Verbindung zwischen den Endpunkten
- Nachträgliches Entschlüsseln quasi unmöglich

Was ist nicht erreicht:

- Validierung der Kommunikationspartner (Bob/Alice)
- Absicherung gegen Man-in-the-Middle Attack

Absicherung von Identitäten

Client Hello

SessionId, Liste von unterstützen Algorithmen

Server Hello

SessionId, Gewählter Algorithmus

Certificate, Server Key Exchange, Server Hello Done

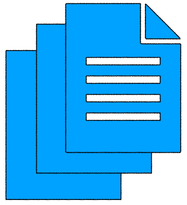
Zertifikatskette

Client Key Exchange

Premaster Secret

ChangeCipherSpec, Finished

ChangeCipherSpec, Finished



CA Certificate

Zertifikat

Private Key

NILS BOKERMANN
IT CONSULTING

Vertrauensverhältnis

Was haben Alice und Bob erreicht:

- Alice kann Bobs Identität verifizieren

Was haben Alice und Bob nicht erreicht:

- Keine Absicherung gegen Verlust von Bob’s Private Key
- Identitätsverifikation gilt nur für den Zeitpunkt der Zertifikatsausstellung

Validieren von Zertifikaten 1

CRL

Client Hello

SessionId, Liste von unterstützen Algorithmen

Server Hello

SessionId, Gewählter Algorithmus

Certificate, Server Key Exchange, Server Hello Done

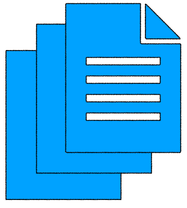
Zertifikatskette

Client Key Exchange

Premaster Secret

ChangeCipherSpec, Finished

ChangeCipherSpec, Finished



CA Certifikate

Zertifikat

Private Key

NILS BOKERMANN
IT CONSULTING

Vertrauensverhältnis

Was haben Alice und Bob erreicht:

- Verifikation des Zertifikats.

Was haben Alice und Bob nicht erreicht:

- CRL wird regelmäßig, aber nicht ständig aktualisiert.

Validieren von Zertifikaten 2

Serial Number

Gültig/Ungültig

Client Hello

SessionId, Liste von unterstützen Algorithmen

Server Hello

SessionId, Gewählter Algorithmus

Certificate, Server Key Exchange, Server Hello Done

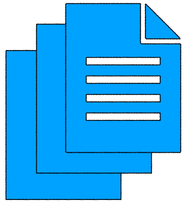
Zertifikatskette

Client Key Exchange

Premaster Secret

ChangeCipherSpec, Finished

ChangeCipherSpec, Finished



CA Certifikate

Zertifikat

Private Key

Vertrauensverhältnis

Was haben Alice und Bob erreicht:

- Verifikation des Zertifikats.

Impact auf Alice:

- Alice gibt möglicherweise Information über die besuchten Seiten preis.

Validieren von Zertifikaten 3

Signed Response

OCSP Request

Client Hello

SessionId, Liste von unterstützen Algorithmen

Server Hello

SessionId, Gewählter Algorithmus

Certificate, Certificate Status, Server Hello Done

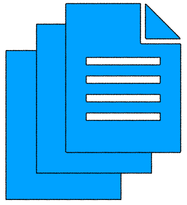
Zertifikatskette

Client Key Exchange

Premaster Secret

ChangeCipherSpec, Finished

ChangeCipherSpec, Finished



CA Certificate

Zertifikat

Private Key

Vertrauensverhältnis

Was haben Alice und Bob erreicht:

- Wie OCSP

Was hat die Zertifizierungsstelle erreicht:

- Abwicklung des OCSP-Traffic über Bob

Implikation für Bob

- Möglich Öffnung des Webservers auf die OCSP-Adresse.

Und was macht mein Browser?

- Umgang der Browser höchst unterschiedlich
- Viele Browser basieren auf eigenen Revoke-Listen
- **https://www.ssl.com/blogs/how-do-browsers-handle-revoked-ssl-tls-certificates/**

Life-Session OpenSSL

- Zertifikat aus einem Webserver laden
- Zertifikats-Chain herunterladen
- OCSP-Anfrage an die Zertifizierungsstelle

Use Cases

- Welche Fälle gibt es zu unterscheiden:
  - Klassische Web-Seite (Viele Alices)
    - Welcher Sicherheitsanforderung gibt es für die Seite?
  - öffentliche API
  - API Bereitstellung mit namentlich bekannten Nutzern (typischer interner Fall)

Zertifizierungsstellen

- Sectigo:
  - **https://sectigo.com**
  - Vertrieb über **www.psw-group.de**
  - Revocation über die Webseite
  - Installation „klassisch“

Zertifizierungsstellen 2

- Let’s encrypt
  - https://letsencrypt.org
  - Non-Profit CA
  - Steuerung über ACME-Protokoll
  - Installation über Certbot oder Webserver

Eigene CA/SubCA?

- Verteilung der Root-Zertifikate?
- Sicherheitsanforderung für die Zertifizierungsstelle.
- Personeller Aufwand

Fragen?

- https://github.com/sanddorn/TLS-Hands-on


nils.bokermann@bermuda.de


@sanddorn


xing.to/sanddorn

NILS BOKERMANN
IT CONSULTING

Literatur und weitere Informationen

- TLS 1.2: https://datatracker.ietf.org/doc/html/rfc5246/
- OCSP Stapling: https://datatracker.ietf.org/doc/html/rfc6961
- https://www.ssl.com/blogs/how-do-browsers-handle-revoked-ssl-tls-certificates/
- IETF PKI Certificate and CRL: https://datatracker.ietf.org/doc/html/rfc5280
- ITU-T X.509: https://www.itu.int/t/aap/recdetails/1334
- https://github.com/sanddorn/TLS-Hands-on