Verteilte Systeme

TLS

by

Dr. Günter Kolousek

TLS

- Transport Layer Security
  - $\rightarrow$ IETF
- Geschichte
  - SSL 1.0 (Secure Sockets Layer) von Netscape
  - SSL 3.1
  - TLS 1.0 (wie SSL 3.1)
  - TLS 1.1 (Detailverbesserungen)
  - TLS 1.2 (Detailverbesserungen, aktuell)
  - TLS 1.3 (Sicherheit und Performance)
- Implementierungen
  - OpenSSL, GnuTLS, LibreTLS, BoringSSL, mbed TLS, Botan, cryptlib, SChannel (Microsoft),…

Aufgaben und Verwendung

- Aufgaben
  - Authentifizierung
  - Geheimhaltung
  - Integrität
- Verwendung
  - https
  - imaps, pop3s
  - smtp mittels starttls
  - snmptls
  - (ftps)

Struktur

- Im Schichtenmodell zwischen Anwendungsschicht und Transportschicht
  - entspricht ISO/OSI Schicht 5
- Transportprotokoll: TCP
- Verwendung vieler kryptographischer Algorithmen

Struktur – 2

- TLS-Protokolle $\rightarrow$ 2 Schichten:
  - TLS Handshake Protocol, TLS Change Cipher Spec. Protocol, TLS Alert Protocol, TLS Application Data Protocol
  - TLS Record Protocol
- TLS Handshake Protocol
  - Authentifizierung der Kommunikationspartner auf Basis asymmetrischer Verschlüsselung
    - in der Regel nur Server, aber auch zweiseitig möglich
  - Schlüsselaustausch mittels DH
    - bevorzugt mittels elliptische Kurven (ECDHE)
    - bis TLS 1.2 auch mit RSA
- TLS Record Protocol
  - Ende-zu-Ende Verschlüsselung mittels symm. Verschlüsselung (z.B. AES)!!!
  - Sicherung der Integrität und Authentizität mittels MAC

Zertifikate

- $\rightarrow$ Foliensatz *security*
- Zertifikatstypen
  - selbst zertifiziert vs. zertifiziert durch CA
    - CA … Certificate Authority (Zertifikatsstelle)
  - $\rightarrow$ Validation Level
  - Secured Domain
    - single-name Zertifikate: beinhalten nur einen ”Host” und die Root-Domäne
    - wildcard Zertifikate: beinhalten alle single-level Subdomänen und die Root-Domäne

Zertifikatstruktur

- Version, Seriennummer, Algorithmen-ID
- essentielle Daten
  - Zertifikatsinhaber (Subject)
  - öffentlicher Schlüssel (& Algorithmusinfo) des Zertifikatsinhabers (Subject Public Key Info)
  - Aussteller (Zertifikatsstelle, Issuer)
  - Ausstellungszeitraum (Validity)
- signiert mit privaten Schlüssel des Ausstellers (& Algorithmusinfo)
- Zertifikatsformate
  - `.cer`, `.crt`, … DER (Abstract Syntax Notation One, ASN.1) oder Base64 kodiertes Zertifikat
  - `.der` … DER kodiertes Zertifikat
  - `.pem` … Base64 kodiertes Zertifikat
  - `.csr` … DER oder Base64 kodierte Zertifizierungsanfrage

CA

- trusted third party, für denjenigen
  - der Zertifikat ausgestellt bekommt
  - der Zertifikat überprüft
- strikte hierarchische Struktur der CAs
- durch CA ausgestellte Zertifikate $\rightarrow$ Browser!
  - Browser beinhalten eine Menge an Root-Zertifikaten
- X.509: Standard der ITU-T
  - ITU: Internationale Fernmeldeunion
  - -T: Telecommunication
  - z.B.: V.24 (serielle Schnittstelle, ähnlich wie RS-232), JPEG (Bildkompression), H.264 (Videokompression), E.164 (Telefonnummernschema)
- Beispiele:
  - Let's Encrypt, CAcert
  - Comodo, GlobalSign, GoDaddy, Verisign,…

Zertifikatskette

- certificate chain
- Zertifikate der zweiten Ebene durch Wurzel signiert
  - schon notwendig, da private Schlüssel der Root-CA nicht ”online” (besonders Schutzbedürfnis!)
- Zertifikate der dritten Ebene durch zweite Ebene signiert
- …
- Verifikation mittels gesamter Liste

Validation Levels

- Problem vieler ”lax” ausgestellten ”HTTPS-Zertifikate”
  - $\rightarrow$ Preisdruck…
- Validation levels für HTTPS-Websites
  - Domain validation (DV)
  - Organization validation (OV)
    - zusätzlich zur Domäne: Organisation muss rechtlich existieren
  - Extended validation (EV)
    - zusätzlich zur Domäne: Feststellung der Identität und Adresse sowie Sicherstellung, dass Person befugt ist (rechtlich bindende Dokumente werden vorgelegt)

Domain Validation

- $\rightarrow$ Let's Encrypt
- Zertifikat validiert Domäneneigentum (Zugriff)
  - Domäne ist registriert und Admin kann den Zertifikationsrequest bestätigen (z.B. per E-Mail oder, dass spezielle DNS Records gesetzt werden)
- Dauer zwischen einigen Minuten und einigen Stunden
- Anzeige: "Connection Not Secure" (oder ähnliches)

Organization Validation

- Zertifikat validiert Domäneneigentum + Organisationinformationen im Zertifikat wie Name, Stadt, Land
- Validierung ähnlich DV, jedoch müssen zusätzliche Dokumente bzgl. der Organisation vorgewiesen werden
- Dauer: einige Tage
- Anzeige der Organisationsinfos in den Details

Extended Validation

- Zertifikat validiert Domäneneigentum + Organisationsinformationen (wie OV)
  - die legale Existenz der Organisation
- Validierung ähnlich OV, jedoch werden zusätzliche Schritte und Überprüfungen
- Dauer: einige Tage bis einige Wochen
- Anzeige: Vollständiges Schloss

Alternativen?

- ETS
  - Enterprise Transport Security
    - ursprünglicher Name eTLS (auf Druck der IETF umbenannt)
  - standardisiert von ETSI (European Telecom Standards Institute)
    - unter Mitwirkung des GCHQ (britischer Geheimdienst)…
    - aber wer genau in der Arbeitsgruppe ist? $\rightarrow$ nicht bekannt!
  - kompatibel zu TLS 1.3
    - hebelt aber die Ende-zu-Ende Verschlüsselung aus!!!
  - Anwendungsfälle
    - für Unternehmen: Sicherheitsaudits, Schutz vor Schadsoftware und vor ”ungesetzlicher Datenexfiltration” (Verlust)
    - für Regierungen: gesetzliche Datenexfiltration?!