esse

ESSE Einführung in Security – VO 02: Kryptographie

Florian Fankhauser

24W

ESSE (Establishing Security) – IT Security Research Team
Research Group for Industrial Software (INSO)
https://establishing-security.at/

Agenda

- Kryptographie
- Chipkarten
- PKI-Bestandteile
- Zertifikate
- Vertrauensmodelle
- Gültigkeitsmodelle
- Bsp. für praktische Anwendung von Kryptographie (PGP/GPG, TLS)
- TLS-Sicherheit(sprobleme) in der Anwendung
- Ausgewählte Sicherheitsprobleme/-aspekte
- Literatur, Weblinks

Vertrauen

(Vergleiche Peter Steiner, *The New Yorker*)

Kryptographie: Einleitung 1/2

- Wissenschaft von der Geheimhaltung von Nachrichten

- Unverschlüsselter Text (Klartext, Plaintext)
- wird mittels einer Funktion, die durch einen Schlüssel (Key) parametrisiert wird,
- in den verschlüsselten Text (Ciphertext) umgewandelt.

- Komplexes, mathematisches Problem als Basis
- Einfache Berechnung eines Ergebnisses, allerdings schwierig diese Berechnung umzukehren

(Vergleiche Blieberger et al., Informatik)

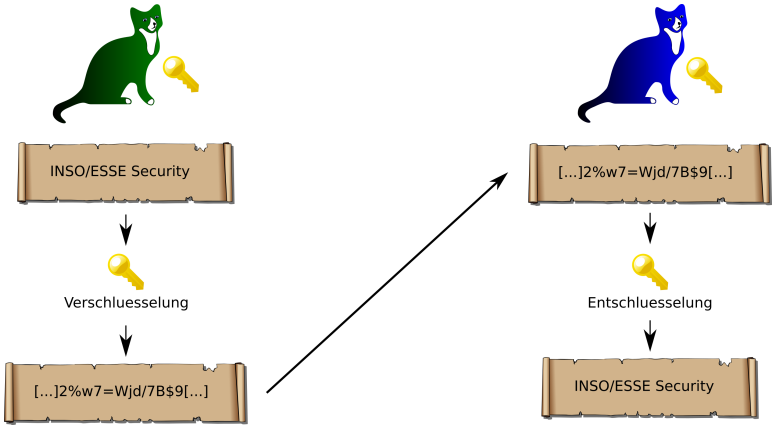
Kryptographie: Einleitung 2/2

- Schutzziele
  - Integrität → Signatur
  - Vertraulichkeit → Verschlüsselung
  - Authentizität → Signatur
- Unterscheidung in symmetrische und asymmetrische Kryptographie
  - Unterschiedliche Einsatzzwecke
  - Unterschiedliche Anforderungen an die Umgebung
- Kerckhoffs' Prinzip: Sicherheit darf nur von Geheimhaltung des Schlüssels abhängen. Nicht von der Geheimhaltung des Algorithmus!

Hash-Verfahren

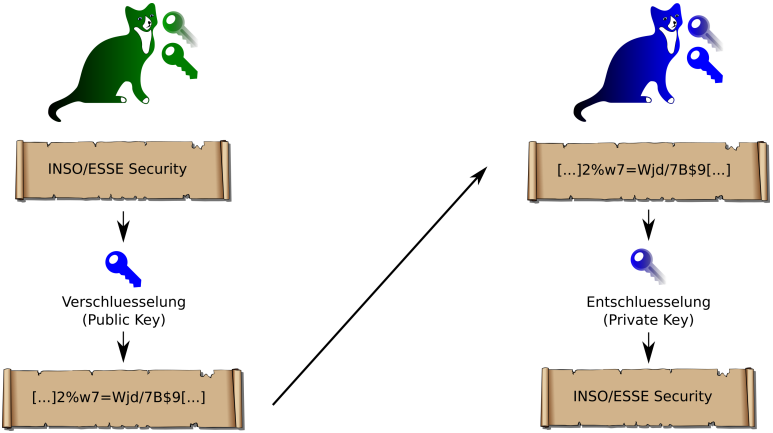
- Hash ist ein eindeutiger Fingerprint eines Dokuments
  - 2 Dokumente mit unterschiedlichen Inhalten dürfen (in der Praxis) nicht denselben Fingerprint erhalten
  - $\rightarrow$ Kollisionsresistenz
- Hash-Verfahren sind Einwegfunktionen
  - $y = f(x)$ ist mit wenig Aufwand zu berechnen
  - Umkehrfunktion $x = f^{-1}(y)$ nicht/schwer anwendbar
- Beispiele für Verfahren:
  - MD5, SHA-1 $\rightarrow$ gelten bereits als unsicher
  - SHA-2 Familie mit SHA-224, SHA-256, SHA-384 und SHA-512
  - SHA-3 Keccak Algorithmus wurde von NIST 2012 ausgewählt

Symmetrische Kryptographie



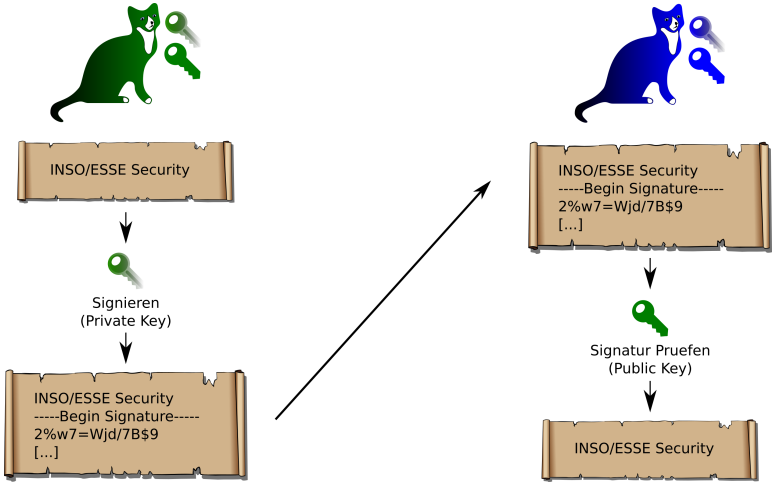
- Beispiele: Data Encryption Standard (DES), CCM-3DES, GCM-AES
- Problem ist Schlüsseltausch bei großer Anzahl an Teilnehmer:innen

Asymmetrische Kryptographie: Verschlüsselung



- Beispiele: OAEP-RSA, ElGamal

Asymmetrische Kryptographie: Signatur



- Beispiele: Rivest-Shamir-Adleman (RSA), ECDSA, ed25519

Hybridverschlüsselung

- Symmetrische Verschlüsselung → Nachteil Schlüsseltausch
- Asymmetrische Verschlüsselung → Nachteil Rechenintensiv
- Lösung: Kombination aus symmetrischer und asymmetrischer Verschlüsselung: Hybridverschlüsselung

- Ablauf
  - Verschlüsselung der zu verschlüsselnden Daten mit einem neu erstellten symmetrischen Schlüssel
  - Verschlüsselung des soeben erstellten symmetrischen Schlüssels mittels des öffentlichen Schlüssels
  - Asymmetrisch verschlüsselten symmetrischen Schlüssel an das symmetrisch verschlüsselte Dokument anhängen

Probleme und Lösungen bei Kryptographie

- Vielzahl an Problemen und Lösungen in der Kryptographie
- Kryptographische Verfahren sind komplex → Complexity is the worst enemy of security (B. Schneier)
  - Komplexität kryptographischer Protokolle und PKIs
  - Implementierungsfehler (Zufallszahlen) → siehe Debian/OpenSSL
  - → es gibt sehr viele Möglichkeiten für Fehler!
- Alterung von Algorithmen/Schlüssellängen
  - Angreifer:in kann Daten ohne Kenntnis des privaten Schlüssels entschlüsseln (z. B. mittels Brute-Force)
  - Erfordert regelmäßige Umschlüsselung von Daten unter Verwendung neuerer Algorithmen/längerer Schlüssel

Probleme und Lösungen – Private Schlüssel

- Sichere Verwahrung des privaten Schlüssels → Sicherer Schlüsselspeicher
  - Kompromittierung: Schutzziele verletzt
  - Chipkarte
  - Hardware Security Module (HSM)
- Verlust des privaten Schlüssels → Verlust der verschlüsselten Daten
  - Oft Backup des privaten Schlüssels erforderlich → zusätzliche organisatorische Maßnahmen
  - Wenn nur für Signaturen eingesetzt → gegebenenfalls kein Backup erforderlich

Probleme und Lösungen – Private/Öffentliche Schlüssel und Übergreifendes

- Integrität/Authentizität für Schlüssel
  - Angreifer:in kann Schlüssel manipulieren → Man in the Middle
  - Zertifikate enthalten eine digitale Signatur
- Schlüssel enthält keine Informationen zum Besitzer/zur Besitzerin
  - Zuordnung zu einer Person schwierig
  - Verwendung von Zertifikaten mit zusätzlichen Informationen zum Besitzer/zur Besitzerin des Schlüssels
- Übergreifende Festlegungen für die Verwendung der PKI erforderlich
  - Prüfung von Zertifikaten

Chipkarten

- Speicherkarten
  - Keine Sicherheitsmerkmale für eine Zugriffskontrolle vorhanden
- Prozessorkarten
  - Betriebssystem der Karte regelt Zugriff auf Daten
  - Möglichkeit Zugriff über Personal Identification Number (PIN) zu regeln
  - Anwendung z.B. mit kryptographischen Schlüsseln
  - Gut: Privater Schlüssel verlässt die Chipkarte nicht
- Kontaktbehaftet vs. kontaktlos
- Beispiele für Einsatzgebiete: Gesundheitskarte, Subscriber Identity Module (SIM), Bankomatkarte

Chipkarten – Beispiele für Angriffe

- Side Channel (“Seitenkanal”) Angriffe (Stromverbrauch, Rechenzeit,...)
  - Oswald und Paar: Breaking Mifare DESFire MF3ICD40 (Stromverbrauch)
- Physikalisch (Temperatur, Spannung, ...)
- Man in the Middle
  - z.B. über Kartenterminal
- Social Engineering
  - Diebstahl
  - Ausspionieren der PIN

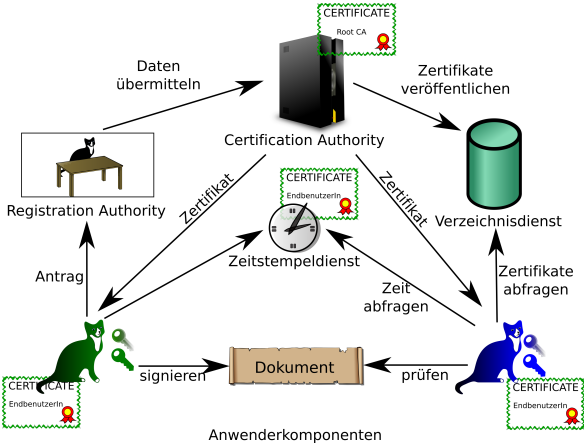
Kartenterminals

- Zum Lesen und Schreiben von Daten
- Unterschiedliche Sicherheitsklassen
  - Sicherheitsklasse 1: Keine besonderen Sicherheitsmerkmale
  - Sicherheitsklasse 2: Gerät enthält PIN-Pad
  - Sicherheitsklasse 3: PIN-Pad und Display
  - Sicherheitsklasse 4: PIN-Pad, Display und eigenes Sicherheitsmodul zur Authentisierung des Geräts
- Physikalische Schutzmaßnahmen gegen Manipulationen erforderlich

PKI-Bestandteile

- Registration Authority (RA)
- Certification Authority (CA)
- Verzeichnisdienst (DIR)
- Time Stamping Authority (TSA)
- Sperrinformationen (CRL/OCSP)
- Anwenderkomponenten
- Zertifikate
- Organisatorische Festlegungen

PKI-Bestandteile – Übersicht



(Vergleiche BSI: *Grundlagen der elektronischen Signatur*)

Registration Authority (RA)

- Registrierung neuer Anwender:innen
  - Überprüfung der Identität
  - Weiterleitung an CA zur Ausstellung von Zertifikaten für die PKI
  - z.B. Extended Validation Certificate (EV)
- Sperre von Zertifikaten/Benutzer:innen
- Definierte Protokolle für Zertifikatsantrag und -austausch
  - Certificate Management Protocol (CMP)
  - Public Key Cryptography Standards #10 (PKCS#10)
- Kompromittierung bei fehlender/fehlerhafter Überprüfung z.B. Let's Encrypt (1, 2)

Beispiel einer Registration Authority – ID Austria

- In .at gibt es unterschiedlichste RAs für die ID Austria
- Details sind auf

  `https://www.oesterreich.gv.at/id-austria/registrierungsbehoerden.html`

  zu finden

- Beispiele
  - Bezirkshauptmannschaften
  - Gemeinden
  - Magistrate
  - Landespolizeidirektionen
  - Finanzämter

Certification Authority (CA)

- Zuständig für Ausstellung und Verwaltung der Zertifikate
  - Endbenutzer:innen-Zertifikate werden durch CA-Zertifikat signiert
  - Erstellung/Signatur von Sperrinformationen
  - Optional auch Schlüsselerzeugung für Endbenutzer:innen
  - Optional Personalisierung von Chipkarten
  - Optional Versand der Informationen an Endbenutzer:innen (PIN-Brief, Zustellung Chipkarte,...)
- Besondere Anforderungen für sichere Betriebsumgebung
  - Speicherung und Zugriff auf private Schlüssel!
- Kompromittierung des privaten Schlüssels einer CA $\rightarrow$ alle ausgestellten Zertifikate und damit signierten Dokumente unsicher

Verzeichnisdienst (DIR)

- Zugriff auf öffentliche Zertifikate
  - Zertifikate zur Prüfung von Signaturen bzw. zum Verschlüsseln erforderlich
- Beliebige Schnittstellen möglich
  - Lightweight Directory Access Protocol (LDAP), Online Certificate Status Protocol (OCSP),...
- Zugriff auf Zertifikat muss eindeutig sein
  - Suche nach Name des Besitzers/der Besitzerin ist oft nicht eindeutig
  - Festlegung eindeutiger Identifizierungsmerkmale, um Zertifikate beim Dienst zu finden

Sperrinformationen

- Vertraulichkeit des privaten Schlüssels erforderlich
  - Wenn nicht gegeben, kann dem privaten Schlüssel nicht mehr vertraut werden
  - Auch sämtliche mit diesem Schlüssel signierte Dokumente nicht mehr vertrauenswürdig
  - Sperre des zu einem Schlüssel gehörenden Zertifikats erforderlich
  - Dem Schlüssel selbst ist nicht anzusehen, ob er gesperrt ist
- Anwendung muss Sperrstatus eines empfangenen Zertifikats prüfen
- Protokolle zum Verteilen von Sperrinformationen:
  - Certificate Revocation List (CRL)
  - Online Certificate Status Protocol (OCSP)

Zeitstempeldienste (TSA)

- Service stellt signierte Zeitstempel aus
  - Dient als Nachweis, dass Daten zu diesem Zeitpunkt existierten
- Ablauf
  - Client sendet Hash-Wert des Dokuments an TSA
  - TSA fügt Zeitstempel ein und signiert diese Kombination
  - Client fügt diese Information zum Dokument hinzu
- Integrität der zeitlichen Information kann durch Signatur des TSA sichergestellt werden

Anwenderkomponenten

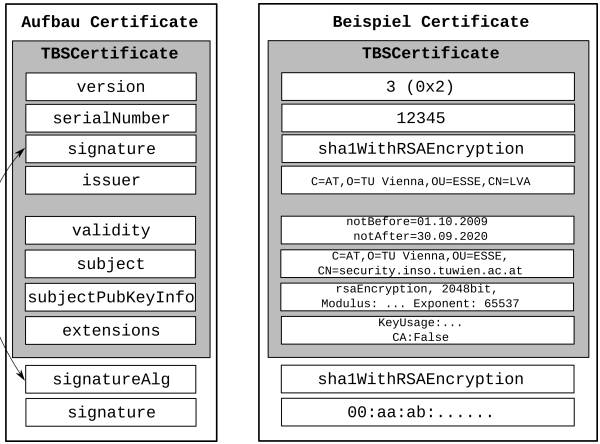
- Verwendung von PKI-Funktionalitäten
  - Abfrage von Zertifikaten aus dem Verzeichnisdienst
  - Signatur- und Pfadvalidierung
  - Signaturerstellungseinheit
  - Kryptographische Algorithmen
- Anwendungen
  - Mail-Client-Applikation
  - XML- oder Web-Service-Client-Applikation
    - XML Security: XMLDSig für Signaturen und XMLenc für Verschlüsselungen
    - WS-Security (basiert auch auf XML Security)
  - Virtual Private Network (VPN), TLS/SSL,...

Zertifikate

Zertifikate als Entität für die Vertrauensstellung

- Zuordenbarkeit eines Public Keys zu einer Identität
- Bestätigung wird durch Zertifizierungsstelle (CA) durchgeführt
- Zertifikat ist im Rahmen der PKI öffentlich
- Zusätzliche Angaben vorhanden
  - Zeitliche Gültigkeit (heute oft nur mehr maximal 1 Jahr)
  - Informationen zum Aussteller (CA)
  - Vorgesehener Einsatzzweck (KeyUsage und ExtendedKeyUsage)
  - ...
- Beispiele für Standards:
  - X.509, Card Verifiable Certificate (CVC)

Bestandteile X.509v3-Zertifikat



(Vergleiche BSI: *Grundlagen der elektronischen Signatur*)

Beispiel Zertifikat Codiert (PEM)

-----BEGIN CERTIFICATE-----
MIIEGTCCAwGgAwIBAgIJAMWHerzo+JcmMA0GCSqGSIb3DQEBCwUAMGExCzAJBgNV
BAYTAkFUMQ8wDQYDVQQIEwZWaWVubmExHzAdBgNVBAoTFkVTU0UgTFZBIFNlY3Vy
aXR5IFdTMDgxIDAeBgNVBAMTF1NlY3VyaXR5IExWQSBFeGFtcGxlIENBMB4XDTA4
MTAxNTE5MjYyNVoXDTExMTAxNTE5MjYyNVowYTELMAkGA1UEBhMCQVQxDzANBgNV
BAgTBlZpZW5uYTEfMB0GA1UEChMWRVNTRSBMVkEgU2VjdXJpdHkgV1MwODEgMB4G
A1UEAxMXU2VjdXJpdHkgTFZBIEV4YW1wbGUgQ0EwggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQC/YzHFYRO9G0EnAp2t9FdXfi7bOBs06oIILGtYz2X8vHz7
JfBQTyTJzN0nPIVP66TjGg2a8asv+iMQQX5TK3WX7qEXUbbv2Xfu68dhaW+DbaGo
5b0rFmUF9NDHVV+lBccLmyfw1oOzY3b47vjX+o566ZGbaaOYYKh+xbx2KxTHK4RR
9zbGpDsIwwMXcgMrd88Fopk2x0SJcC697SRho62WkUpRnNl86b4yS/9PLDKNLoDz
dFbIZ3MnG53fRlSperm5EXNhtnkwWpiWmZbghFppUURSYhPj1EnE0VAhJtztSUA
Rk6DaSUAoMPihWLESiUGyb7E2LsaaGOJ5FPqHTMBAgMBAAGjgdMwgdAwHQYDVR0O
BBYEFHIsRBfTziYpfT7kXSJ01gMC5TWoMIGTBgNVHSMEgYswgYiAFHIsRBfTziYp
fT7kXSJ01gMC5TWooWWkYzBhMQswCQYDVQQGEwJBVDEPMA0GA1UECBMGVmllbm5h
MR8wHQYDVQQKExZFU1NFIExWQSBTZWN1cml0eSBXUzA4MSAwHgYDVQQDExdTZWN1
cml0eSBMVkEgRXhhbXBsZSBDQYIJAMWHerzo+JcmMAwGA1UdEwQFMAMBAf8wCwYD
VR0PBAQDAgEGMA0GCSqGSIb3DQEBCwUAA4IBAQCJA1+x6uPrp4o0vQAbMaRNA+ll
sR3n/ZVdi+wh+YPD162Ls6s0DDl50CUguGV+txdb75zn0isRtP3XUTXiEEj5TCih
vc7tMY50ag9sLTKYHbWJbjTIBss66OFTRDN7M2IZz5L3zTCvZx+dtt8Sf2p/B9+9
PhKCN9+ymOhSCNJ/yG/dVH8RoflkiRHmGP2Jqjkshs68Qtylt3kkSwj7LUaDY8pR
5iF257rX6ilOvaaFAIVj0Y7VpSnJ6Ns5Tq0WMDwm2VgxO1S2SNXELjeOVttR14uH
Q+uK9xQTrrp8GWNdt+5Nns/7CgQJPQ05z4l6blWMGG0S59bP7ayyIAweMirH
-----END CERTIFICATE-----

Beispiel CA-Zertifikat

```
Data: Version: 3 (0x2)
      Serial Number: 86:d2:8b:36:17:e4:6b:70
      Signature Algorithm: sha256WithRSAEncryption
      Issuer: C=AT, ST=Vienna, O=ESSE LVA, CN=ESSE
      Validity
          Not Before: May  3 06:31:41 2010 GMT
          Not After : May  2 06:31:41 2015 GMT
      Subject: C=AT, ST=Vienna, O=ESSE LVA, CN=ESSE
      Subject Public Key Info:
          Public Key Algorithm: rsaEncryption
          RSA Public Key: (2048 bit)
              Modulus (2048 bit):
                  00:e3:f3:94:d1:e6:93:26:23:99:00:d8:e6:13:40:.....
              Exponent: 65537 (0x10001)
      X509v3 extensions:
          X509v3 Subject Key Identifier:
              EA:89:8D:B4:94:AC:77:D8:ED:ED:DC:11:B8:13:A4:9A:B6:4B:61:B2
          X509v3 Authority Key Identifier:
              keyid:EA:89:8D:B4:94:AC:77:D8:ED:ED:DC:11:B8:13:A4:9A:B6:4B:61:B2
              DirName:/C=AT/ST=Vienna/O=ESSE LVA/CN=ESSE
              serial:86:D2:8B:36:17:E4:6B:70
          X509v3 Basic Constraints:
              CA:TRUE
          X509v3 Key Usage:
              Certificate Sign, CRL Sign
```

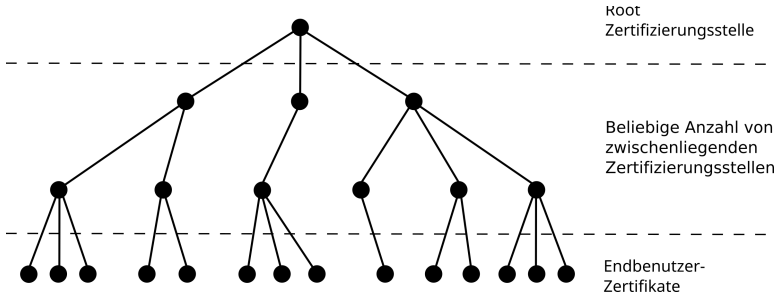
Beispiel Endbenutzer:innen-Zertifikat

```
Data: Version: 3 (0x2)
      Serial Number: c5:87:7a:bc:e8:f8:97:29
      Signature Algorithm: sha256WithRSAEncryption
      Issuer: C=AT, ST=Vienna, O=ESSE LVA IntroToSec WS11, CN=IntroToSec LVA Example CA
      Validity
            Not Before: Oct 15 19:36:18 2009 GMT
            Not After : Oct 15 19:36:18 2012 GMT
      Subject: C=AT, ST=Vienna, O=ESSE LVA IntroToSec WS11, CN=IntroToSec LVA Example Mail Zertifikat
      Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
               Modulus (2048 bit):
                  00:e0:0f:1d:bc:67:11:1e:e0:3d:6d:45:ba:56:ef:...........
               Exponent: 65537 (0x10001)
      X509v3 extensions:
            X509v3 Basic Constraints:
               CA:FALSE
            X509v3 Subject Key Identifier:
               97:57:A1:60:C5:AD:0A:08:56:D3:D1:9C:D1:71:18:D6:4C:DD:E8:3A
            X509v3 Authority Key Identifier:
               keyid:72:2C:44:17:D3:CE:26:29:7D:3E:E4:5D:22:74:D6:03:02:E5:35:A8
            X509v3 Key Usage:
               Digital Signature, Non Repudiation, Key Encipherment
            X509v3 CRL Distribution Points:
               URI:http://server.invalid/ca.crl
            X509v3 Extended Key Usage: critical
               E-mail Protection
```

Beispiel Endbenutzer:innen-Zertifikat für TLS-Server

```
Data: Version: 3 (0x2)
    Serial Number: 86:d2:8b:36:17:e4:6b:71
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=AT, ST=Vienna, O=ESSE LVA, CN=ESSE
    Validity
        Not Before: May  4 06:49:30 2010 GMT
        Not After : May  3 06:49:30 2012 GMT
    Subject: C=AT, ST=Vienna, O=ESSE LVA, CN=www.server.invalid
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (2048 bit)
            Modulus (2048 bit):
                00:ee:69:ea:6e:29:55:f1:92:5f:42:4d:a3:4a:28:.....
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Subject Key Identifier:
            79:8D:89:83:E9:C7:C4:DC:6E:F3:21:84:5D:20:C7:DB:9A:4C:BB:2E
        X509v3 Authority Key Identifier:
            keyid:EA:89:8D:B4:94:AC:77:D8:ED:ED:DC:11:B8:13:A4:9A:B6:4B:61:B2
        X509v3 Basic Constraints:
            CA:FALSE
        X509v3 Key Usage:
            Digital Signature, Non Repudiation, Key Encipherment
        X509v3 Extended Key Usage: critical
            TLS Web Server Authentication
        X509v3 CRL Distribution Points:
            URI:http://server.invalid/ca.crl
```

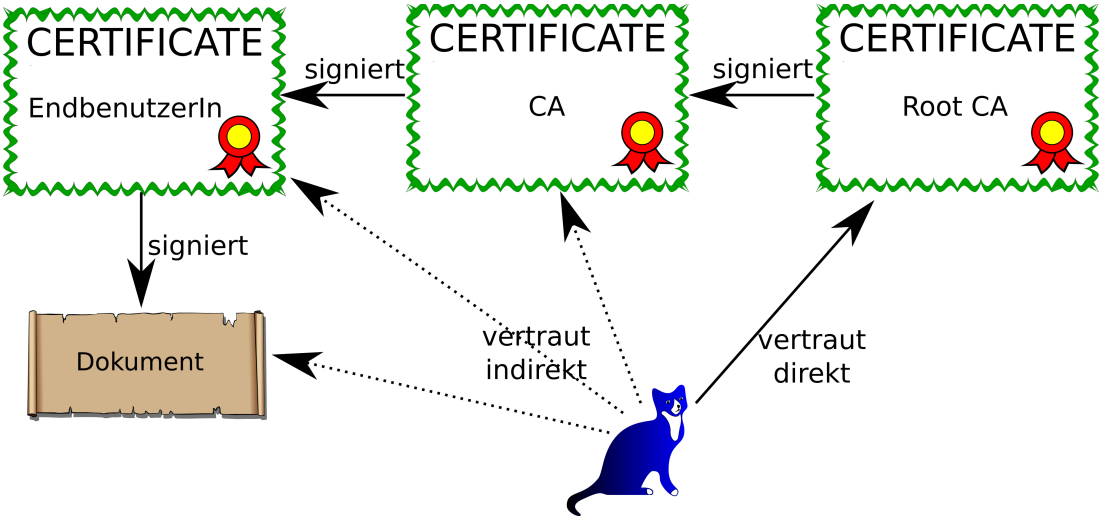
Vertrauensmodell – Hierarchische Struktur



- Hierarchischer Aufbau → Vertrauensstellung über eine Root-CA
- Zwischenliegenden Zertifizierungsstellen wird indirekt vertraut
- Verwaltung großer Infrastrukturen möglich

(Vergleiche Adams und Lloyd: *Understanding PKI*)

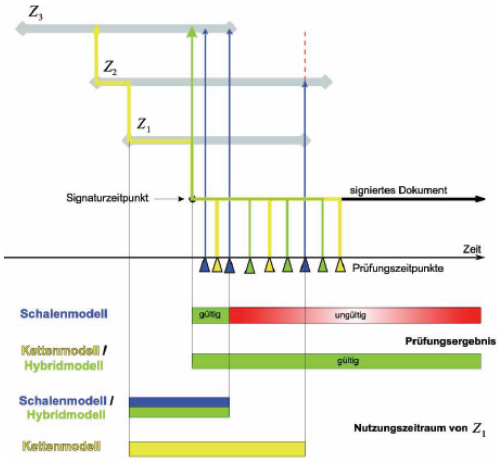
Zertifikatskette



Gültigkeitsmodelle bei Signaturen

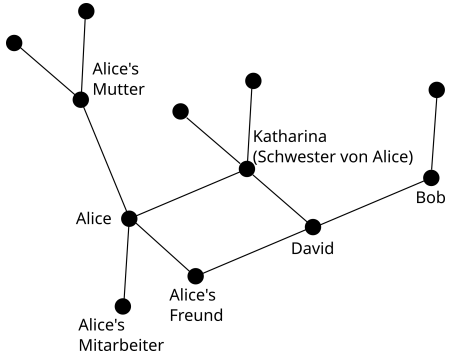
- Festlegung der Regeln für die Überprüfung einer Signatur
- Berücksichtigung des gesamten Zertifikatspfads
- Unterschiedliche Modelle vorhanden
  - Schalenmodell → Zum Zeitpunkt der Prüfung alle Zertifikate im Pfad gültig
  - Kettenmodell → Zum Zeitpunkt der Erstellung der Signatur war jeweils das signierende Zertifikat gültig
  - Hybridmodell → Zum Zeitpunkt der Erstellung der zu prüfenden Signatur waren alle Zertifikate im Pfad gültig

Gültigkeitsmodelle Beispiel



(Vergleiche BSI: *Grundlagen der elektronischen Signatur*)

Vertrauensmodell – Web of Trust



- Direkte Vertrauensstellung, Beispiel: Pretty Good Privacy (PGP)
- Kommunikationsteilnehmer:in muss Zugehörigkeit des Schlüssels zur Identität des Kommunikationspartners/der Kommunikationspartnerin überprüfen
  - Indirekte Vertrauensstellung möglich

    (Vergleiche Adams und Lloyd: *Understanding PKI*)

PGP / GPG

- PGP=Pretty Good Privacy
  - Entwickelt durch Phil Zimmermann (1991)
  - Früher als Freeware erhältlich, mittlerweile proprietär
- GPG=GNU Privacy Guard
  - Open Source Variante
  - Basiert auf dem OpenPGP-Standard (RFC4880)
- Inkludieren von Informationen zu Benutzer:innen
  - Namen, E-Mail, Photo

Transport Layer Security (TLS)

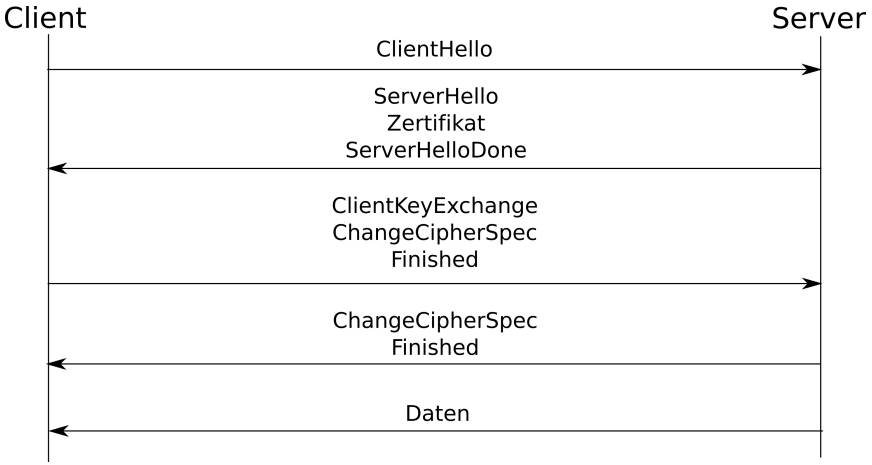
- HTTPS $\rightarrow$ “HTTP over TLS”
- TLS ist der Nachfolger von SSL (Secure Sockets Layer)
- TLS 1.3: RFC 8446 (August 2018)
- TLS 1.0 und 1.1 seit 2020 in großen Webbrowsern nicht mehr unterstützt
- Verwendung für
  - Authentifizierung (einseitig oder beidseitig)
  - Verschlüsselung der Kommunikation
- Verschlüsselung nur zwischen zwei Komponenten auf Layer 4 möglich
  - Vertraulichkeit für Ende zu Ende über mehrere Stationen muss auf höheren Ebenen sichergestellt werden

Cipher Suiten bei TLS

- Cipher Suiten legen kryptographische Methoden für die Kommunikation fest
  - Kommunikationspartner handeln sich eine gemeinsame Cipher Suite aus

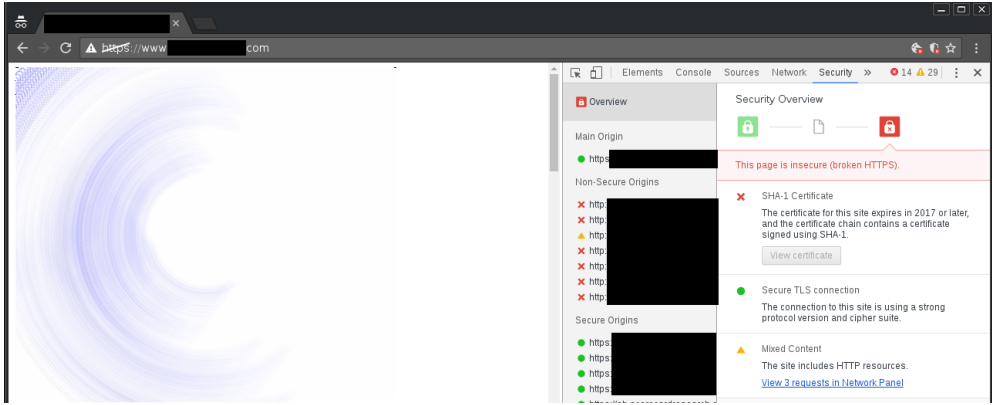
- Teile einer Cipher Suite
  - Schlüsselaustausch (RSA, DHE, ECDHE, ...)
  - Authentifizierung (RSA, DSS, ...)
  - Verschlüsselung (3DES, AES, ...)
  - Hashfunktion (SHA256, ...)
  - Beispiel: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

TLS – Kommunikationsablauf

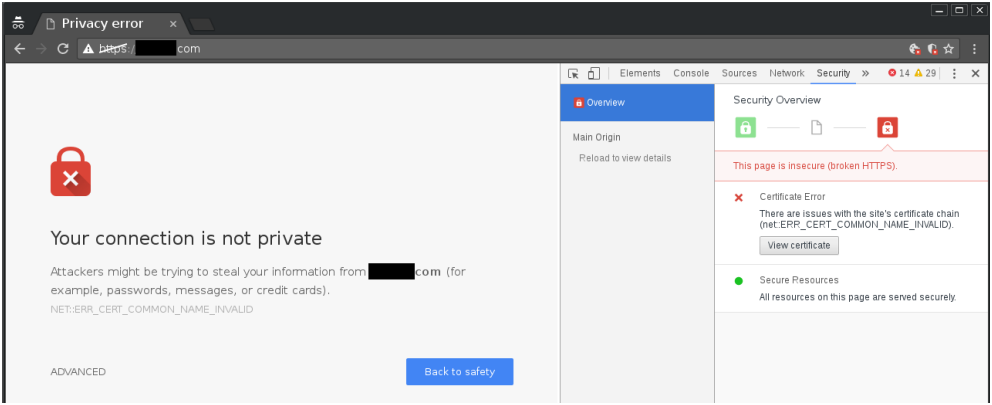


TLS-Sicherheit(sprobleme) in der Anwendung

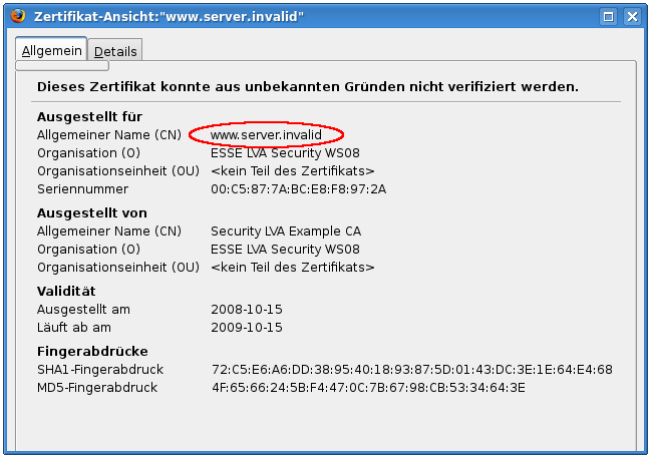
SHA-1 als Hashing-Algorithmus ist veraltet – Chromium



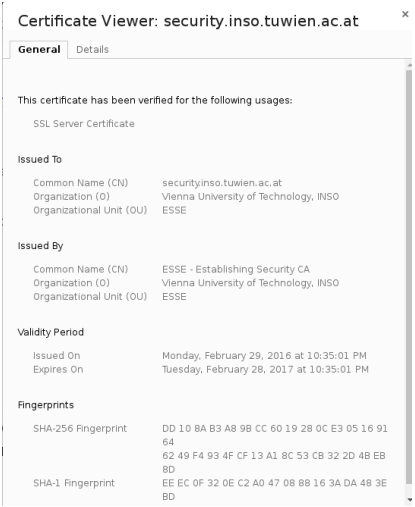
DNS-Name des Servers stimmt nicht mit Zertifikat überein – Chromium



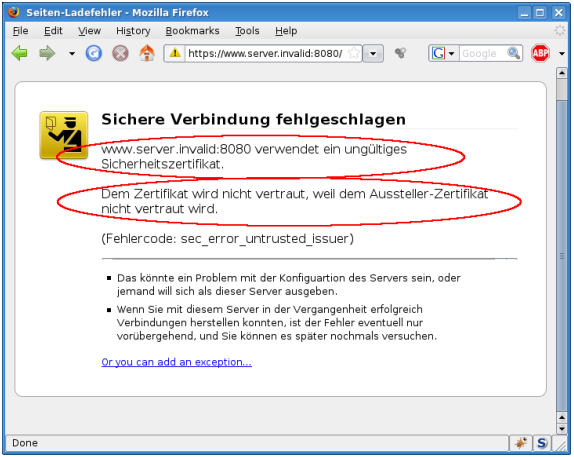
Betrachtung der Zertifikatsinformationen – Firefox



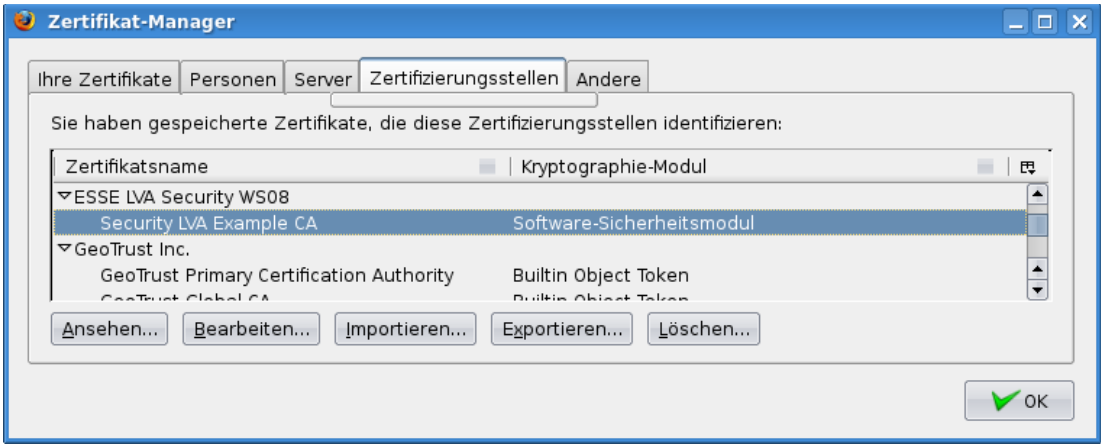
Betrachtung der Zertifikatsinformationen – Chromium



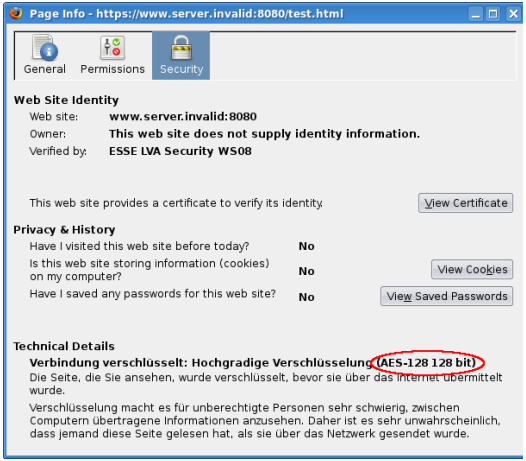
Fehlermeldung über fehlendes CA-Zertifikat – Firefox



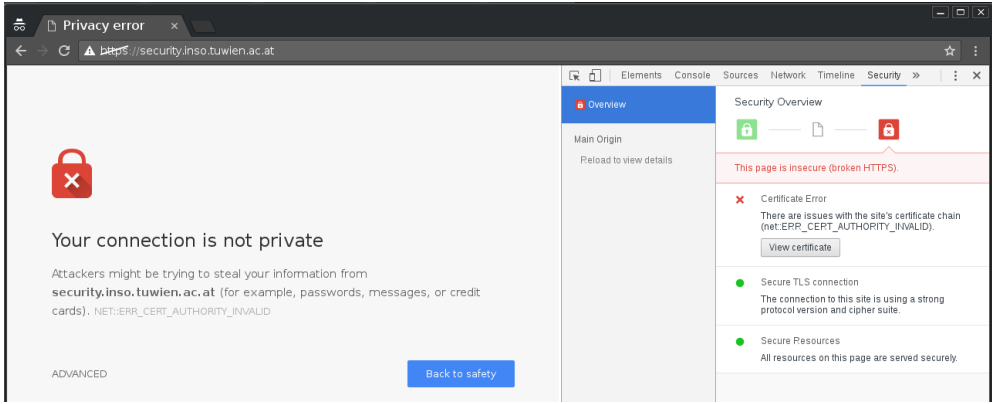
Import des CA-Zertifikats – Firefox



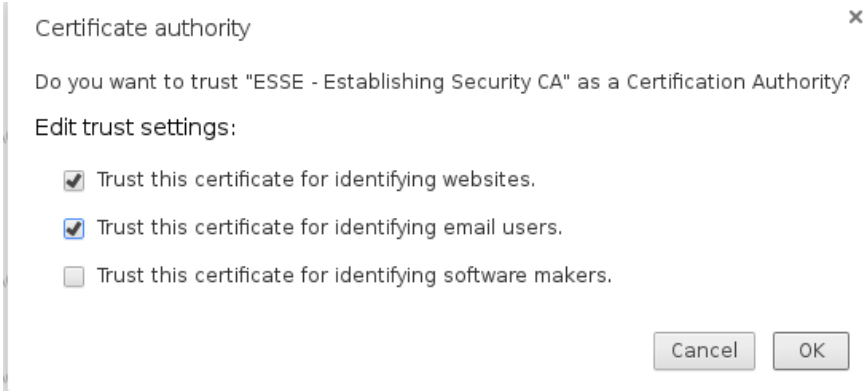
Erfolgreiche Überprüfung des Zertifikats – Firefox



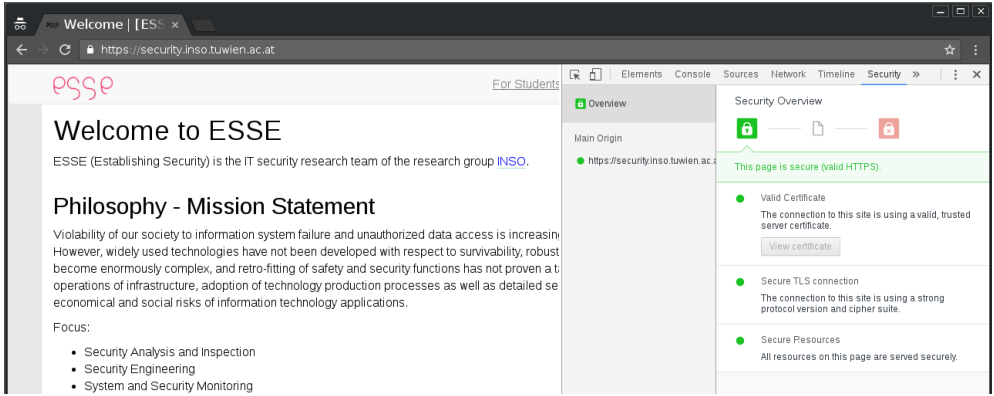
Fehlermeldung über fehlendes CA-Zertifikat – Chromium



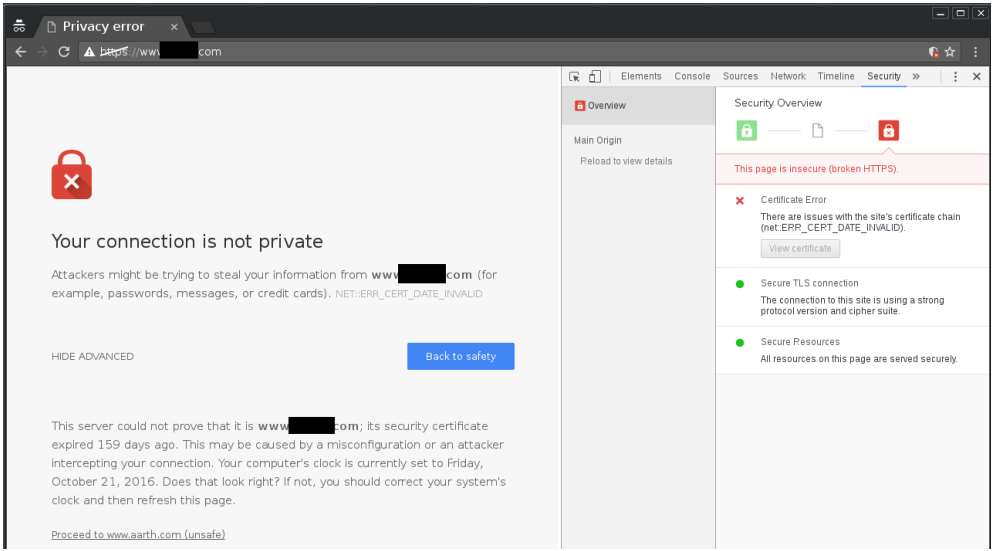
Import des CA-Zertifikats – Chromium



Erfolgreiche Überprüfung des Zertifikats – Chromium



Abgelaufenes Zertifikat – Chromium



TLS-Fehler sind (k)ein Sicherheitsrisiko!

(abgelaufenes Zertifikat in der Praxis)

TLS-Fehler Überall ;)

(abgelaufenes Zertifikat in der Praxis)

Weitere ausgewählte Sicherheitsprobleme/-aspekte

- Browser kennzeichnen HTTP only Webseiten
- Let's Encrypt
- Auch die aktuellen Spezifikationen von TLS 1.2 tragen Altlasten mit sich
- Hlauschek, Gruber, Fankhauser, Schanes: *Prying Open Pandora's Box: KCI Attacks against TLS* – `https://www.kcitls.at/`
- Vertrauen in CAs
- Lenovo Superfish Adware Vulnerable to HTTPS Spoofing
- Zertifizierungsstellen: WoSign und StartCom verlieren Apples und Mozillas Vertrauen
- Fefes Blog (Hyundai-Firmware und Probleme mit (a)symmetrischen Schlüsseln)

Literatur, Weblinks 1/7

- Florian Fankhauser, Christian Schanes, und Christian Brem. Sicherheit in der Softwareentwicklung.
  In *Softwaretechnik - Mit Fallbeispielen aus realen Entwicklungsprojekten*, Kapitel 13, Seiten 589–646. Pearson Studium, München, 1. Auflage, 2009
- Ronald Eikenberg. Heise Newsticker: Android-Apps mit SSL-Lücken, 2013.
  `https://heise.de/-2062942`
- Gerd Baron und Peter Kirschenhofer. *Einführung in die Mathematik für Informatiker*.
  Springer-Verlag, Wien, 2. Auflage, 1996.
  ISBN 3-211-82797-8.
  Band 3

Literatur, Weblinks 2/7

- Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C.*
  John Wiley & Sons, Inc., 1996.
  ISBN 0-471-11709-9
- Bruce Schneier. *Secrets & Lies: IT Sicherheit in einer vernetzten Welt. Übers. aus dem Amerikan. von Angelika Shafir.*
  dpunkt.verlag GmbH, Heidelberg, 2004.
  ISBN 3-527-50128-2
- Carlisle Adams und Steve Lloyd. *Understanding PKI: Concepts, Standards, and Deployment Considerations.*
  Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2. Auflage, 2002.

Literatur, Weblinks 3/7

- David Oswald und Christof Paar. Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World.
  In Bart Preneel und Tsuyoshi Takagi, (Hrsg.), *Cryptographic Hardware and Embedded Systems - CHES 2011*, Band 6917 von *Lecture Notes in Computer Science*, Seiten 207–222. Springer Berlin Heidelberg, 2011.
  ISBN 978-3-642-23950-2.
  doi: 10.1007/978-3-642-23951-9{_}14
- Andrew S. Tanenbaum. *Computernetzwerke*.
  Pearson Studium, München, 4. Auflage, 2003.
  ISBN 3-8273-7046-9
- Johann Blieberger, Bernd Burgstaller, und Gerhard H. Schildt. *Informatik*.
  Springer-Verlag, Wien, 3. Auflage, 2005.

Literatur, Weblinks 4/7

- Zertifizierungsstellen: WoSign und StartCom verlieren Apples und Mozillas Vertrauen
- Gezinkte Primzahlen ermöglichen Hintertüren in Verschlüsselung
- Zertifikats-Klau: Fatale Sehschwäche bei Comodo
- Certificate Transparency: Google setzt Symantec die Pistole auf die Brust
- Sennheiser-Software spielt Angreifern mächtige Werkzeuge in die Hände
- Bruce Schneier. Cryptography Is Harder than It Looks.
  IEEE Security Privacy, 14(1):87–88, Jan 2016.
  ISSN 1540-7993.
  doi: 10.1109/MSP.2016.7

Literatur, Weblinks 5/7

- Auguste Kerckhoffs. La cryptographie militaire.
  Journal des sciences militaires, IX, Januar–Februar 1883
- Bruce Schneier: Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure
- Christiane Rütten. Schwache Krypto-Schlüssel unter Debian, Ubuntu und Co., Mai 2008.
  `https://heise.de/-207332`
- openclipart.org als Quelle einiger Grafiken/Grafikbestandteilen

Literatur, Weblinks 6/7

- Clemens Hlauschek, Markus Gruber, Florian Fankhauser, und Christian Schanes. Prying Open Pandora's Box: KCI Attacks against TLS.
  In *9th USENIX Workshop on Offensive Technologies (WOOT 15)*, Washington, D.C., August 2015. USENIX Association.
  https://www.usenix.org/conference/woot15/workshop-program/presentation/hlauschek
- Signal Technical information
- BSI verschickt privaten PGP-Schlüssel

Literatur, Weblinks 7/7

- Ahmed Tanvir Mahdad, Cong Shi, Zhengkun Ye, Tianming Zhao, Yan Wang, Yingying Chen, und Nitesh Saxena. EarSpy: Spying Caller Speech and Identity through Tiny Vibrations of Smartphone Ear Speakers. 2022. doi: 10.48550/arXiv.2212.12151
- `https://web.archive.org/web/20231023093525/https://notes.valdikss.org.ru/jabber.ru-mitm/`, `https://blog.fefe.de/?ts=9bcc63d0`
- `https://cabforum.org/network-security-requirements/`
- `https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/`

Zusammenfassung

- Grundlagen zu Kryptographie (Verschlüsselung, Signatur)
- Bestandteile einer Public Key Infrastructure
- Aufbau und Verwendung von Zertifikaten
- Vertrauensmodelle
- Anwenderkomponente anhand von Firefox/Chromium
- Herausforderungen und ausgewählte Lösungen bei Kryptographie
- Ausblick: Viele weitere Details und zusätzliche Aspekte, z.B. Elliptic Curve Cryptography (ECC)

Vielen Dank!

https://establishing-security.at/