Netzsicherheit – Architekturen und Protokolle
Grundlagen PKI/PMI

Wiederholung Kryptographie

- Symmetrische Kryptographie
  - 1 Schlüssel für Ver- und Entschlüsselung
  - Schlüssel muss vor Kommunikation ausgetauscht werden
  - Schlüssel muss geheim gehalten werden
  - Schlüsselanzahl wächst quadratisch mit Anzahl der Kommunikationsteilnehmer
- Asymmetrische Kryptographie
  - Zwei zueinander inverse Schlüssel
  - Öffentlicher Schlüssel ist nicht geheim
  - Schlüsselanzahl wächst linear

- Nutzung der Schlüssel bei asymmetrischer Kryptographie
  - Öffentlicher Schlüssel des Partners notwendig, um
  - Daten für ihn zu verschlüsseln
  - Signaturen von ihm zu verifizieren
- Eigener privater Schlüssel notwendig, um
  - Daten von sich (=mit sich selbst als Absender) zu signieren
  - verschlüsselte Daten an sich zu entschlüsseln

Diskussion

Welches **neue** Problem hat man mit asymmetrischer Kryptographie?

Motivation: Authentifizierung

- Frage: woher bekommt man öffentlichen Schlüssel?
  - manueller Austausch?
  - via eMail oder Web-Site?

  → *Sichere Zuordnung Schlüssel/Kommunikationspartner?*
- Lösungsvorschlag: öffentliches Verzeichnis
  - Zuordnung: Name zu öffentlichem Schlüssel (ähnlich Telefonbuch)
  - Antworten auf Anfragen symmetrisch geschützt
  - Probleme des Ansatz?
- Wie erreicht man unabhängige, transportierbare Bindung von Authentifizierungsdaten? → PKI!

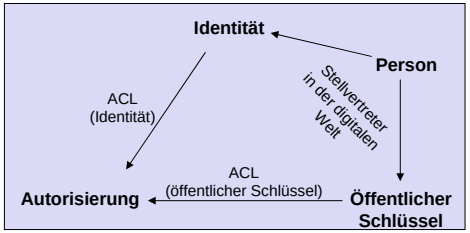
- Manueller Austausch bringt keinen Vorteil bzgl. des Schlüsselverteilproblems!
- Verzeichnisansatz bereits vorgeschlagen in
  - Whitfield Diffie, Martin E. Hellman: New Directions in Cryptography, in: IEEE Transactions on Information Theory 22 (6), November 1976, Seiten 644-654
- Probleme des Verzeichnisansatzes
  - Single Point of Failure: Bei Ausfall des Verzeichnisses keine Schlüssel-Anfrage mehr möglich
  - Schlechte Skalierbarkeit: Verzeichnis bei jeder Transaktion beteiligt
  - Authentizität der Zuordnung nicht transportierbar
  - Vertrauen in Verzeichnisdienstanbieter nötig (Bemerkung: Auch bei Verwendung einer PKI ist Vertrauen nötig, hier ist aber ein flexibleres Vorgehen möglich)
  - Verzeichnisdienstanbieter erfährt, wer mit wem kommunizieren will

Historisches

- Whitfield Diffie and Martin Hellman: "New Directions in Cryptography", IEEE Transactions on Information Theory, November 1976, pp. 644-654]
  - "Given a system of this kind, the problem of key distribution is vastly simplified. Each user generates a pair of inverse transformations, E and D, at his terminal. The deciphering transformation, D, must be kept secret but need never be communicated on any channel. The enciphering key, E, can be made public by placing it in a public directory along with the user's name and address. Anyone can then encrypt messages and send them to the user, but no one else can decipher messages intended for him."
- Loren Kohnfelder, "Towards a Practical Public-key Cryptosystem", 1978
  - Introduction of Certificates

Motivation: Autorisation

- Autorisierung über Zugangskontrolllisten (*Access-Control-List*)
  - der via Passwort/Ticket/PKK verifizierten Identität
  - des via Signatur (mit privatem Schlüssel) bestätigten öffentlichen Schlüssels



Problem: Zuordnung von Privilegien zu Personen lokal oder zentral gespeichert

Wie erreicht man eine unabhängige, transportierbare Bindung von Autorisationsdaten? → PMI!

•Beispiele

  •für Passwort-Authentifizierung: pop, imap, smtp-auth

  •für Signatur: SSH (authorized_keys), SSL

•Speicherung der Privilegien:

  •lokal: auf dem Dienste-Server selbst

  •zentral: auf einem Privilegien-Server

Netzsicherheit – Architekturen und Protokolle
Grundlagen PKI/PMI

Digitale Zertifikate

Problemstellung

- Authentifizierung eines Sachverhaltes, den man nicht selbst überprüfen kann

→ man verlässt sich auf vertrauenswürdige Dritte, die ihn schon kontrolliert haben

Frage: was ist ein Zertifikat?

- ein digitales Dokument, in dem eine Instanz einen bestimmten Sachverhalt mittels digitaler Signatur bestätigt

→ erzeugt Vertrauen in den Sachverhalt

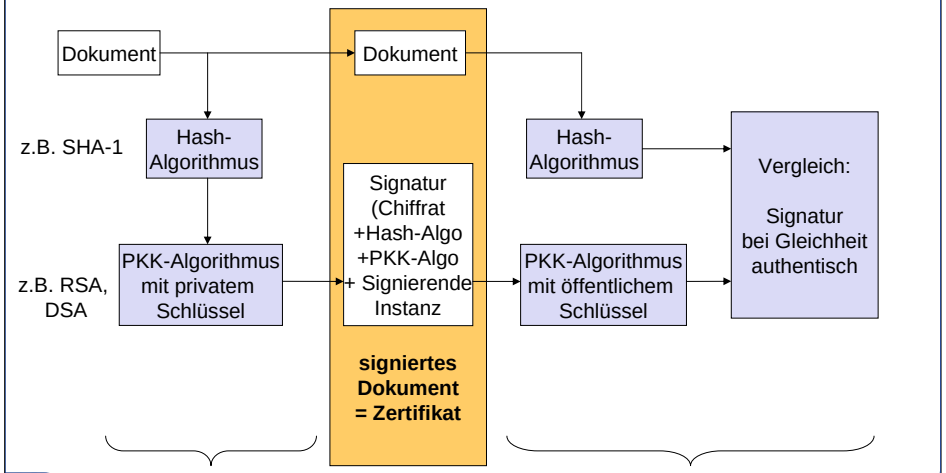
Frage: wer erstellt die Zertifikate?

- eine vertrauenswürdige Instanz: Certification Authority

•Ein Zertifikat ist ein digitales Dokument, in dem eine Instanz einen bestimmten Sachverhalt mittels digitaler Signatur bestätigt. Es ermöglicht somit die Authentifizierung dieses Sachverhaltes durch einer Instanz, die ihn selbst nicht prüfen kann.

•Certfification Authority: kann eine Institution, Behörde aber auch eine einzelne Person sein.

Digitale Signatur



•Statt der Anwendung eines Hashalgorithmus kann auch alternativ das gesamte Dokument mit dem privaten Schlüssel verschlüsselt werden.

•Dieses Verfahren hat jedoch zwei Nachteile:

•Die Anwendung asymmetrischer kryptographischer Verfahren ist deutlich aufwendiger als die Berechnung eines Hashwerts.

•Das Dokument muss bei diesem Verfahren zweimal übertragen werden (je einmal verschlüsselt und unverschlüsselt). Durch die Verwendung des Hashalgorithmus ergibt sich lediglich ein konstanter Overhead zu übertragender Daten (unabhängig von der Dokumentgröße).

•Der verwendete Hash-Algorithmus muss ein kryptographischer Hash-Algorithmus sein.

Klassifizierung von Zertifikaten

- Klassen von Zertifikaten
  - ID-Zertifikate
    - öffentlicher Schlüssel → eindeutiger Name (*Identität*)
    - Authentifikation von öffentlichen Schlüsseln
  - Attributzertifikate
    - Attributswerte → Identität
    - Autorisation zur Nutzung von Diensten
  - Autorisierungszertifikate
    - binden Privilegien → öffentlichen Schlüssel
    - Autorisation zur Nutzung von Diensten
- Zertifikate ersetzen zentrale globale Listen
  - öffentliches Verzeichnis mit (ID, öffentlicher Schlüssel) durch ID-Zertifikat
  - ACL auf ID-Basis durch Attributzertifikate
  - ACL auf Basis des öffentlichen Schlüssels durch Autorisierungszertifikate

•ID-Zertifikate sind die bekannteste Klasse, angewendet vor allem im Internet bei SSL/TLS für Internet-Banking, Internet-Shopping oder anderen sicheren Web-Zugriff. Auch alltägliche Dinge wie Personalausweis stellt ein ID-Zertifikat dar

•Wird inzwischen zunehmend auch für IMAP-SSL und andere TCP-basierte Dienste genutzt. Weitere Beispiele folgen in der Vorlesung noch!

•Attribut- und Autorisierungszertifikate bisher im Internet nahezu ungenutzt, eher in privaten Netzen.

•Z.B Führerschein als Autorisation in einem Attributszertifikat und weiterhin auch ID-Zertifikat

Welche Zertifikate aus der realen Welt passen in welche Klasse?

Personalausweis/Reisepass?

→ ID-Zertifikat (bindet Name an Bild)

(wenn man Zertifizierung des Alters auch noch berücksichtigt, eigentlich auch ein Attribut-Zertifikat)

Führerschein?

→ Attributzertifikat (hat auch ID-Charakter, da Bild enthalten ist)

Key-Card?

→ Autorisierungszertifikat, ID spielt keine Rolle, Rechte sind an Schlüssel gebunden, nicht an eine ID.

Kreditkarte?

Attributzertifikat (manche Geschäft verlangen auch einen Ausweis, d.h. ein ID-Zertifikat)

Fricard?

An der Universität für mehrere Zwecke benutzt

ID-Zertifikat (Identitätsfeststellung bei Prüfungen)

Attributzertifikat (Eigenschaft als Student oder Mitarbeiter)

Autorisierungszertifikat (Gebäudezugang)

Achtung! Wir bilden hier Analogien zur realen Welt – auch wenn die Fricard ähnliche Funktionen erfüllt wie ein ID-Zertifikat, heißt das nicht, dass die Fricard tatsächlich ein digitales Zertifikat enthält.

CAP-Prinzip

- Problem bei dezentraler Speicherung: **Konsistenz**
- ***CAP-Prinzip***: 2 der 3 Punkte sind bei verteilten Anwendungen realisierbar
  - C: strong **c**onsistency
    - Konsistenz der verteilten Daten
  - A: high **a**vailability
    - Hohe Verfügbarkeit der Daten
  - P: **p**artition-resilience
    - Ausfallsicherheit bei Netzwerkpartitionierung
- Beispiele? In welche Klasse fallen Zertifikate?

•Beispiele:

•CA ohne P: Bei verteilten Datenbanken ist Konsistenz bei hoher Verfügbarkeit nur realisierbar, wenn Partitionierung ausgeschlossen ist.

•CP ohne A: Bei verteilten Datenbanken ist Konsistenz bei Partitionierung nur realisierbar, wenn während der Dauer der Partitionierung Veränderungen geblockt werden können.

•AP ohne C: Bei redundanten DNS-Servern sind die Daten hoch verfügbar auch bei Partitionierung, allerdings sind die Daten evtl. nicht aktuell.

•Zertifikate fallen in die Klasse „AP ohne C“:

•Authentifikation der Daten ist hoch verfügbar, da sie von keinem zentralen Server oder Verzeichnis abhängt

•Authentifikation ist z.B. bei replizierten Servern immer noch möglich, auch wenn diese partitioniert sind

•Konsistenz der zertifizierten Daten ist nicht gesichert

•Literatur zum CAP-Prinzip

•Armando Fox, Eric A. Brewer; Harvest, Yield, and Scalable Tolerant Systems, in: Proceedings of the Seventh Workshop on Hot Topics in Operating Systems, 1999, S. 174-178.

CAP-Prinzip bei Zertifikaten

Problem

Zertifikate können ungültig werden, wenn die Informationen im Zertifikat nicht mehr zutreffen (z.B. ID stimmt nicht mehr, Privileg wird entzogen)

Lösungen

- Gültigkeitsdauer
- Offline-Prüfung durch Widerruflisten (*certificate revocation list – CRL*)
- Online-Prüfung (in welche CAP-Klasse fallen Zertifikate dann?)

•Widerruflisten: müssen nur periodisch aktualisiert werden, enthalten IDs von nicht mehr konsistenten Zertifikaten

•Online-Prüfung: Prüfender muss online sein und synchron Konsistenz des Zertifikates bestätigen lassen (z.B. durch CA)

•Zertifikate fallen dann in die Klasse „AC ohne P“:

•Authentifikation der Daten ist hoch verfügbar, da Widerrufinformation redundant auf Servern gespeichert werden kann

•Konsistenz der zertifizierten Daten ist gesichert, da synchron geprüft

•Bei Netzpartitionierung (zwischen Prüfendem und Server für Online-Prüfung) ist eine Prüfung nicht mehr möglich

Validierung (Grundlage)

- Validierung eines Zertifikates
  - syntaktische und semantische Prüfung seiner Gültigkeit
- Vorraussetzung für den Validierenden
  - vertraut einer Menge von CAs
  - ist im Besitz der Zertifikate dieser CAs
  - hat die Integrität und Authentizität dieser Zertifikate geprüft
- Ablauf: der Prüfende verifiziert, ob das zu prüfende Zertifikat
  - zeitlich noch gültig ist
  - widerrufen wurde
  - alle Parameter für die Anwendung gültig sind (z.B. Sicherheitsrichtlinie)
  - aufgrund des eingesetzten Vertrauensmodells als vertrauenswürdig gilt
    - z.B. ausgestellt durch eine vertrauenswürdige CA
  - eine gültige Signatur hat

Netzsicherheit – Architekturen und Protokolle
Grundlagen PKI/PMI

Infrastrukturen

- Kerndienste des Management von Zertifikaten
  - Registrierung, Zertifizierung, Publizierung
  - Widerruf, Re-Zertifizierung
- Infrastrukturen zum Management von Zertifikaten
  - ID-Zertifikaten
    - Public Key Infrastructure (PKI)
  - Attributzertifikaten
    - Privilege Management Infrastructure (PMI)
  - Autorisierungszertifikate: ?
    - (bisher kein Begriff geprägt, jedoch starke Parallelen zur PMI vorhanden)

•Widerruf: nur vor Ablauf der Gültigkeitsdauer

•Re-Zertifizierung: nach Ablauf der Gültigkeitsdauer oder nach Widerruf

X.509 Standard

- PKI und PMI
  - X.509
    - Authentifizierung und Autorisation für X.500 Standard
  - X.500
    - Globales verteiltes Verzeichnis, Internet-Telefonbuch
  - PKI wesentlich durch X.509-Standard geprägt
  - PMI ebenfalls, jedoch noch relativ neu, daher wenig verbreitet
  - PKI-/PMI-Architektur dennoch von X.509 unabhängig, daher
    - erst neutrale Einführung
    - dann Vorstellung der X.509-spezifischen Formate

Alternative Standards

- Weitere Standards
  - SDSI/SPKI (nicht behandelt)
    - zu X.509 alternative Architekturen und Formate
    - unvollendete Standardisierung, dennoch interessante Konzepte
  - PGP (wird anschließend behandelt)
    - ID-Zertifikatsystem, das mit minimaler Infrastruktur auskommt

Netzsicherheit – Architekturen und Protokolle
Grundlagen PKI/PMI

Was ist eine Public Key Infrastruktur?

- Public Key Infrastructure (PKI)
  - ist eine Infrastruktur zum Management von ID-Zertifikaten
  - ermöglicht somit Authentifikation öffentlicher Schlüssel
- Bausteine einer PKI
  - Organisatorische Bausteine
    - Zertifizierungsrichtlinie (Certification Policy)
    - Dokumentation interner Abläufe (Certification Practice Statement)
    - Zugrundeliegendes Vertrauensmodell
  - Technische Bausteine
    - Zertifikatsformat (z.B. X.509), das das Vertrauensmodell unterstützt
    - Managementprotokolle zur technischen Umsetzung der PKI-Dienste

Wie und von wem werden diese Bausteine eingesetzt und umgesetzt?

•Zertifizierungsrichtlinie: Welcher Sachverhalt wird für welche Anwendung wie zertifiziert?
  •Beispiele
    •https://www.verisign.com/repository/vtnCp.html
    •http://www.dfn-pca.de/certification/policies/
•Dokumentation interner Abläufe
  •soll Vertrauen in die CA stärken (Stichpunkt: Transparenz/Berechenbarkeit)
  •Beispiel: https://www.verisign.com/repository/summary.html
•Managementprotokolle
  •z.B. entwickelt durch die IETF PKIX Working Group
  •Beispiele OCSP,… - später in der Vorlesung

PKI-Modell

Eine PKI besteht aus folgenden Elementen

- Benutzer (subject, end entity)
  - Mensch, Maschine oder Prozess
  - meldet sich bei der PKI an (*enrollment*) und lässt sich ein Zertifikat ausstellen
  - will andere öffentliche Schlüssel authentifizieren

Zertifizierter Benutzer

- Registration Authority (RA)
  - Implementiert administrative Aspekte der PKI
  - Schnittstelle zwischen Benutzer und CA
  - Entkopplung (CA i.d.R. offline)
  - evtl. direkt Teil der CA

RA

•Administrative Aspekte bei RA

- •Verifiziert die Identität der beantragenden Instanz (z.B. durch Personalausweis)
- •Verifiziert den Besitz des privaten Schlüssels
- •Prüft die Parameter des Schlüsselpaares

PKI-Modell (2)

- Certification Authority (CA)
  - Implementiert Zertifizierung
  - folgt technischen Standards, die Formate spezifizieren
  - erzeugt durch Signatur Zertifikate
  - Schutz dieses Signaturschlüssels
  - Erstellung von Widerruflisten

CA

- Speicher/Verzeichnis (directory)
  - für ausgestellte Zertifikate, gültige und historische
  - Abruf von Zertifikaten über diverse Protokolle möglich
  - Publizierung der Gültigkeit von Zertifikaten über Widerruflisten

Widerruf von ID-Zertifikaten

Eine CA kann ein Zertifikat (evtl. vom Benutzer ausgelöst) vor Ablauf seiner Gültigkeitsdauer widerrufen, wenn

- das Zertifikat nicht mehr benutzt wird
- der private Schlüssel nicht mehr nutzbar ist
- der zu einem Zertifikat gehörige private Schlüssel sicher oder eventuell kompromittiert wurde
- Angaben in dem Zertifikat nicht mehr stimmen
- Parameter des Schlüsselpaares nicht mehr adäquat sind

•Privater Schlüssel nicht mehr nutzbar, wenn
  •Crash der Festplatte, Zerstörung der Chip-Karte
  •Vergessen des Passwortes, das den Schlüssel sichert
  •Diebstahl des Rechners
•Kompromittierung des privaten Schlüssels
  •Entdeckung eines Trojanischen Pferds
  •Entdeckung eines Überwachungsgerätes
•Angaben in Zertifikat stimmen nicht mehr
  •Namensänderung
  •Wechsel der Abteilung, Verlassen der Firma
•Parameter nicht mehr adäquat
  •Algorithmus gebrochen
  •Schlüssellänge zu gering

Anforderungen an eine PKI

Anforderungskatalog

- Sicherheit interner Abläufe
- Sicherheit der Signaturschlüssel der CA
- Effizienz: Validierung eines Zertifikates
- Skalierbarkeit
- Komfort: vertretbarer Aufwand für Benutzer
- Vertrauenswürdigkeit

•Anforderungen an eine PKI
  •Sicherheit interner Abläufe
  •Registrierung, Prüfung von Identität und Schlüsselpaar
  •Zusammenspiel der Komponenten
  •Prozesse im Fehlerfall
•Sicherheit des Signaturschlüssel der CA
  •Rechner ohne Netzwerkanschluss
  •Physikalische Zugangsbeschränkung (CA-Rechner in einem Safe)
  •Aufwendige Authentifikation (z.B. via Smartcards, evtl 4-Augen-Prinzip)
•Effizienz: Validierung eines Zertifikates
  •Komplexität
  •Rechenaufwand, Zeitaufwand
•Skalierbarkeit
  •Abläufe
  •Formate und Protokolle
•Komfort: vertretbarer Aufwand für Benutzer
  •Entfernung zur nächsten Registrierungsstelle
  •Zeitlicher Aufwand bei Registrierung/Zertifizierung
•Vertrauenswürdigkeit

Was fehlt?

- Vertrauen, Vertrauenswürdigkeit
  - bereits mehrfach erwähnt, aber was ist das?
  - Wie wird Vertrauen in einer PKI hergestellt?
    - z.B. Vertrauen in die Gültigkeit eines Zertifikats

→ nächste Vorlesungseinheit

•Vertrauen ist an Kontext gebunden. Vertrauen einer Person gegenüber ist in einem anderen Kontext vielleicht nicht gegeben.

Literatur

Historisch

- Loren Kohnfelder: Towards a practical public-key cryptosystem. Bachelor Thesis, MIT, Cambridge, 1978.

Aktuelles Buch

- Carlisle Adams, Steve Lloyd: Understanding PKI, Addison Wesley, 2003

Aktuelle Online-Dokumente

- PKI-Forum: CA-CA Interoperability; 2001
  - guter Überblick über das Thema, dabei recht kurz gefasst
- The Open Source PKI Book, online verfügbar

•CA-CA Interoperability: http://www.apectelwg.org/apecdata/telwg/23tel/estg/estg_11.pdf

•Open Source PKI Book: http://ospkibook.sourceforge.net/