

Sicherheitsmanagement - Sicherheitsdienste

C.Stettler <cs@rogatec.ch>

Sicherheitsdienste

Allgemein

- Sicherheitsdienste werden implementiert durch Sicherheitsmechanismen

Identifikation / Authentifizierung

Dienst	Mechanismen
<ul style="list-style-type: none">▪ nur „legale“ Personen können in System einloggen▪ Person als „legal“ identifizieren▪ Sicherstellung, dass Person die ist, als die sie sich ausgibt	<ul style="list-style-type: none">▪ Benutzernamen / Passwort▪ Tokens (Smart Card)▪ Biometrie

Autorisation

Dienst	Mechanismen
<ul style="list-style-type: none">▪ identifiziert / authentifizierte Personen erhalten nur Zugang zu Systemen / Informationen / Daten, für die sie autorisiert sind▪ Logical Access Control	<ul style="list-style-type: none">▪ Access Control Lists▪ Klassifikation von Informationen → Multi Level Models mit verschiedenen Sicherheitsstufen▪ Rollenbasierter Zugriff (role based access control)

Vertraulichkeit (Confidentiality)

Dienst	Mechanismen
<ul style="list-style-type: none">▪ Sicherstellen, dass nicht autorisierte Personen keinen Zugriff auf Daten haben, die im Netzwerk übertragen werden (Lesen, Abfangen)	<ul style="list-style-type: none">▪ Verschlüsselung▪ symmetrische Verschlüsselung (DES, private key)▪ asymmetrische Verschlüsselung (public key)

Integrität

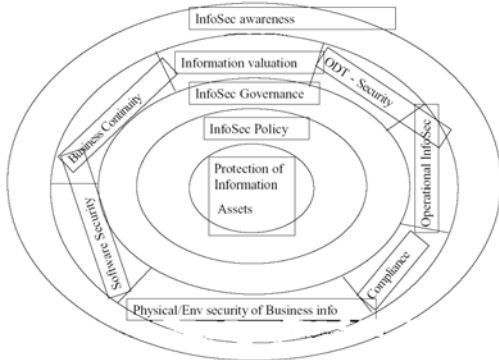
Dienst	Mechanismen
<ul style="list-style-type: none">▪ Sicherstellen, dass nicht autorisierte Personen im Netzwerk übertragene Daten nicht verändern können	<ul style="list-style-type: none">▪ MACs (Message Authentication Codes)▪ Checksums (Prüfsummen)▪ Message Digests (digitale Signaturen)

Unleugbarkeit (Non-Repudiation)

Dienst	Mechanismen
<ul style="list-style-type: none">▪ Sicherstellen, dass Person eine begangene Handlung abstreitet (Transaktionen)	<ul style="list-style-type: none">▪ digitale Signaturen (basierend auf public key Verschlüsselung)

C.Stettler <cs@rogatec.ch>

Information Security Framework



Risiko-Analyse

Allgemein

- Ziel von Sicherheit: Schutz der elektronischen Infrastruktur vor möglichen Bedrohungen
- Ziel Risiko-Analyse: Auswahl welche Systeme wie vor welchen Bedrohungen schützen

Risiko Management

- Prozess von Implementierung und Management der Kontrollmassnahmen zur Reduktion der identifizierten Bedrohungen

Risiko-Analyse

- Prozess zur Bestimmung der möglichen Bedrohungen und mögliche Schäden durch Bedrohungen an Systemen
- Hauptschritte
 - Risiko Analyse Methode wählen
 - Risiko Analyse durchführen
 - Resultate interpretieren
- Methodologien
 - formal – informal
 - detailliert – vereinfacht
 - high level – low level
 - quantitativ basiert – qualitativ basiert
 - automatisiert – manuell
 - diverse Kombinationen

Durchführung Risiko Analyse

- Systeme / Werte identifizieren
 - Hardware, Software, Daten, Personen, Dokumentation, Versorgung
- Schwachstellen / Gefährdungen bestimmen
 - Matrix Werte – Sicherheitskriterien
- Wahrscheinlichkeit des Eintretens der Gefährdungen bestimmen
 - wie oft / mit welcher Wahrscheinlichkeit tritt Gefährdungen auf
- Kosten berechnen
 - Annual Loss Expectancy (erwarteter Verlust / Jahr)

	Confidentiality	Integrity	Availability
Hardware			
Software			
Data			
People			
Documentation			
Supplies			

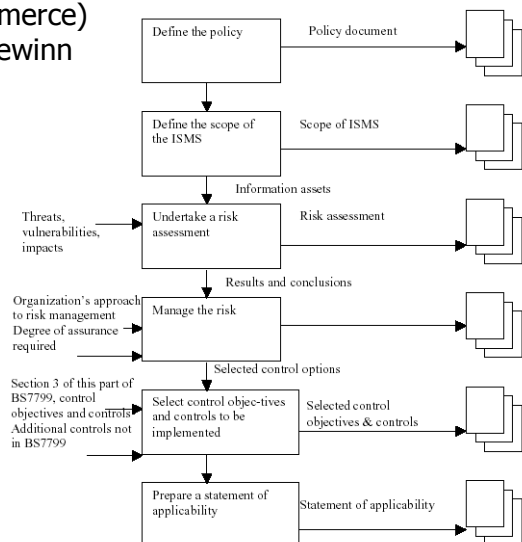
- Kosten jedes Vorfalls bestimmen
- Multiplikation mit erwartete Anzahl Vorfällen / Jahr
- Sicherheitskontrollen und Kosten bestimmen
 - Massnahmen zur Eindämmung der Bedrohung bestimmen
- Einsparungen pro Jahr bestimmen
 - Differenz Annual Loss Expectancy – Sicherheitskosten

Gründe für Risiko Analyse / Risiko Management

- Risikobewusstsein verbessern
- Basis für Entscheidungsfindung verbessern
- Ausgaben für Sicherheitsvorkehrungen anpassen
- Systeme / Werte und mögliche Bedrohungen identifizieren
- Kontrollmassnahmen zur Reduktion der Bedrohungen bestimmen

BS 7799: Code of Practice für Sicherheitsmanagement

- British Standard Institute, akzeptiert von vielen Ländern, in Zukunft ISO-Standard
- 10 Schlüssel-Kontrollen
- 109 detaillierte Sicherheitskontrollen
- Zertifizierung
 - international akzeptiert
 - nötig in Alltag (trust business partner / e-commerce)
 - ev. gesetzlich gefordert, bringt zusätzlichen Gewinn
 - keine Zertifizierung führt zu Verlust
 - Bestimmung des eigenen Sicherheitslevels
 - Vergleich mit anderen Firmen
 - Bestimmen von Lücken (Gap-Analyse)
 - genau bestimmtes Zertifizierungs-Prozedere
 - Zertifizierung gültig für 3 Jahre
- Schlüssel-Bereiche
 - Sicherheitspolitik
 - Sicherheitsorganisation
 - Wert-Klassifizierung und Kontrolle
 - Personensicherheit
 - physische Sicherheit /Umweltsicherheit
 - Computer-/Netzwerk-Management
 - System-Zugriffskontrolle
 - Systementwicklung / Wartung
 - Business Continuity Planning (Sicherstellung der Handlungsfähigkeit)
 - Einhaltung / Durchsetzung
- C:CURE
 - basiert auf BS 7799
 - Ziel: Vertrauenslevel für Organisationen und Partner bez. IT Sicherheit liefern



CobIT: Control Objectives for Information and related Technologies

- generell anwendbarer Standard für gute IT Sicherheit und Kontroll-Praktiken
- 392 spezifische Kontrollmechanismen für 34 IT-Prozesse (IT Sicherheit nur 1 davon)
- 21 Management Aktionen → müssen getroffen werden, um Sicherheit zu garantieren

GMITS: Guidelines for the Management of IT Security

- Ziel: ganzheitliches Management von IT Sicherheitsproblemen (technisch, physisch, prozedural, administrativ)
- Vereinheitlichung zwischen Organisationen
- Basis zur Unterstützung einer Organisation und Verbesserung der Situation
- 5 Teile von Konzepten / Modellen bis zu Schutzmassnahmen / Kontrolle

IT Produkt Evaluation

TCSEC: Trusted Computer System Evaluation Criteria

- Sammlung von Kriterien zur Bewertung von Software-Produkten
- verteilt verschiedene Klassen (A1, B3 – B1, C2, C1 D)
- US-Verteidigungsministerium als akkreditierte Stelle

ITSEC: Information Technology Security Evaluation Criteria

- Bewertung von Produkten und Systemen im kommerziellen Umfeld
- Unterscheidung Korrektheit und Effektivität
- 7 Kategorien: E0 – E6
- entwickelt und verbreitet in Europa

Common Criteria

- Verbindung von TCSEC und ITSEC
- Erstellung eines Protection Profiles aus Sicherheitsanforderungen

Identifikation und Authentifizierung

Grundlagen

- ein Computersystem muss zu jeder Zeit wissen, mit wem es kommuniziert, um
 - nur „legalen“ Benutzern Zugriff zu geben
 - zur Autorisation aufzufordern
 - Rechenschaft zu verlangen
- Wo wird es benützt?
 - In geschlossene Systemen (User im voraus bekannt)
 - In offenen Systemen (User im voraus unbekannt z.B. E-Commerce)
 - Wenn ein eindeutiger Identifier einem User zugeordnet werden muss (das passiert normalerweise bei einem Login)

Zweck von I & A

- Sicherstellen, dass nur „legale“ User Zugang zum System haben (autorisierte User)
- I&A einfacher in geschlossenen als in offenen Systemen

Ablauf

- 1. User identifizieren
 - User-id (nicht geheim)
 - Kann gestohlen (missbraucht) werden
 - Beweisen, dass die User-id diesem User gehört
- 2. Authentifizierung
 - verifizieren, dass die angegebene User-id der Person mit der id gehört
 - die (und nur die) diese mit geheimen Parametern beweisen kann
- geheime Parameter in vier Formen
 - etwas das der User **weiss**
 - etwas das der User **besitzt**
 - etwas das der User **ist**
 - **Kombination** dieser drei Punkte

Parameter

- Passwörter
 - Regeln
 - geheim halten
 - Passwortfile vertraulich aufbewahren
 - Sichere Übermittlung
 - Verschlüsselung der Passwörter vor dem abspeichern
 - Passwortfile verschlüsselt
 - Passwortfile geschützt gegen unautorisierten Zugang und Manipulation
 - PW während der Übermittlung schützen
 - Mindestlänge, regelmässiges Ändern des PW, nicht direkt vom User abgeleitet, möglichst random
 - PW-Authentifizierung weit verbreitet
 - User muss es nicht merken, wenn PW gestohlen (nicht Personenwagen mmhhh!)
- Physikalische Gegenstände
 - Magnetkarte, SmartCard, etc.
 - User merkt es, wenn es gestohlen wird
 - Gegenstand muss physikalisch vorhanden sein für Authentifikation
 - Magnetische Karte nicht sicher
 - SmartCard sicher (offline!)

- Kann immer noch gestohlen und weiterbenutzt werden
- Etwas, das der User ist
 - Biometrische Merkmale
 - Fingerabdruck, Retina, Stimme
 - Ersetzt PW
 - Kann nicht gestohlen werden
 - Teuer

Management von I&A

- User/Passwortfiles erstellen
- Neue User hinzufügen/entfernen
- PW ändern
- Passwortfiles sicher aufbewahren
- User-id's eindeutig
- Inaktive id's (?)
- Logfiles
- Multi-System Umgebungen
 - Login in mehrere Systeme
 - Verschiedene PW und Id's
 - Führt zu Problemen mit
 - Verschiedenen Passwortfiles
 - User verlässt das Geschäft (→ mehrere Files bearbeiten)
- Single Sign on System
 - Eine User-id und ein PW pro User
 - Risiko, da nur ein PW
 - Implementationen:
 - Synchronisation
 - Scripting
 - Trusted authentication server
 - Kerberos

Autorisation

- Ziel ist, dass der Computer nur zulässigen Users Zugang gewährt und nur zulässige und legitime Aktionen ausgeführt werden (dürfen) *von Solms & Eloff*
- Authorisation Policies
 - **Mandatory Access Control (MAC):** Baut auf einer durch Organisations- oder Systemrichtlinien festgelegten Zugriffskontrolle auf

Bei der benutzerbezogenen Zugriffskontrolle, dem MAC-Modell, werden die Ressourcen anhand ihrer Sensitivität kategorisiert. Im Einzelfall bedeutet dies, dass das Modell Informationen in die klassischen Geheimhaltungsstufen »Vertraulich«, »Geheim« und »Streng Geheim« einstuft. Die Benutzer dürfen abhängig von ihrer Kompetenz im Unternehmen auf diese kategorisierten Informationen zugreifen. Leider können explizit privilegierte »High-Level«-Benutzer dadurch alle untergeordneten Daten einsehen, die überhaupt nicht in ihren Verantwortungsbereich fallen.

- **Discretionary Access Control (DAC):** Baut auf einer benutzerbestimmbaren Zugriffskontrolle auf

Hinter dem DAC-Modell steht die Idee, die Ressourcen anhand ihrer funktionalen Kriterien zu klassifizieren. Verschiedene Ressourcen-Gruppen werden für verschiedene Benutzer freigegeben. Mitarbeiter der Kreditabteilung würden beispielsweise den Zugriff auf alle für die Kreditvergabe relevanten Daten erhalten. Weil aber ein Benutzer dadurch einen unbeschränkten Zugriff auf alle Daten mit einem bestimmten funktionalen Kriterium besitzt, darf er auch Informationen einsehen, auf die er nicht zwingend angewiesen ist. Das Modell schaltet mehr Daten frei, als es eigentlich notwendig wäre.

(www.networkcomputing.de)

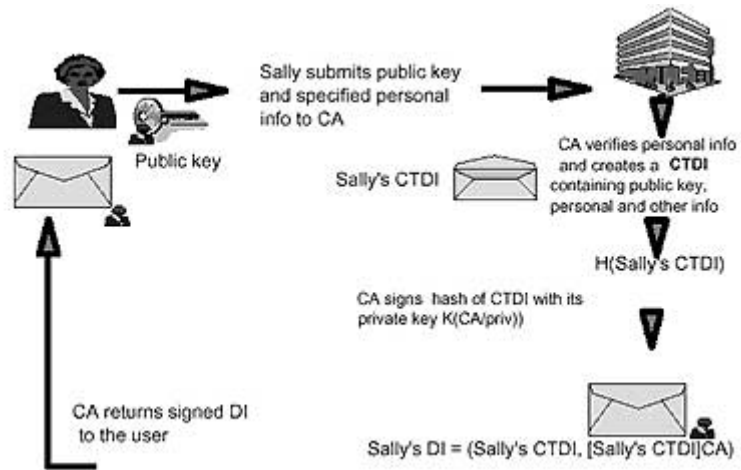
- Subjekte und Objekte
 - Objekt: irgendeine Komponente einer Computer-Umgebung
 - Subjekt: fordert einen Service von einem Objekt
- DAC-Policy-Modelle
 - Directory list
 - Zugangskontroll-Liste (Access control list)
 - Zugangskontroll-Matrix (Access control matrix)
(Grafiken auf Folien 7/8)
- MAC-Policy-Modelle
 - Militär-Sicherheits-Modelle (Military Security Model)
 - Ein Subjekt bekommt nur Zugang zu einem Objekt, wenn folgende zwei Bedingungen wahr sind:
 - $\text{security_class}(\text{subject}) \geq \text{security_class}(\text{object})$
 - $\text{compartment}(\text{object}) \supseteq \text{compartment}(\text{subject})$ [Superfolien von Bauknecht...]
 - Bell&Lapadula-Modell
 - weit referenziertes Modell
 - Nachfolger des Military Security Models
 - für Subjekt und Objekt
 - angepasste Klassifikationshierarchie
 - erlaubter Informationsfluss

- star-property
 - Subjekt S_i kann nur Schreibrecht auf Objekt O_j haben, wenn $C(S_i) \leq C(O_j)$
- Simple security property
 - Subjekt S_i kann nur Leserecht auf Objekt O_j haben, wenn $C(S_i) \geq C(O_j)$
- Kerberos
 - Siehe AAI
- Kerberos in multi-domain Umgebungen
 - Es besteht die Möglichkeit, ein Ticket auf einem entfernten Server für einen entfernten Server anzufordern. Ansonsten gleiches Prinzip
- Multilevel Sicherheit in Netzwerken
 - Allgemeine Verwendung
 - Obligatorische Zugangskontrolle
 - Kennzeichnend (labelling)
 - Vertrauen
 - Multilevel Sicherheitsnetzwerk
 - Einfache Sicherheitseigenschaft
 - *-property

Verbindlichkeit

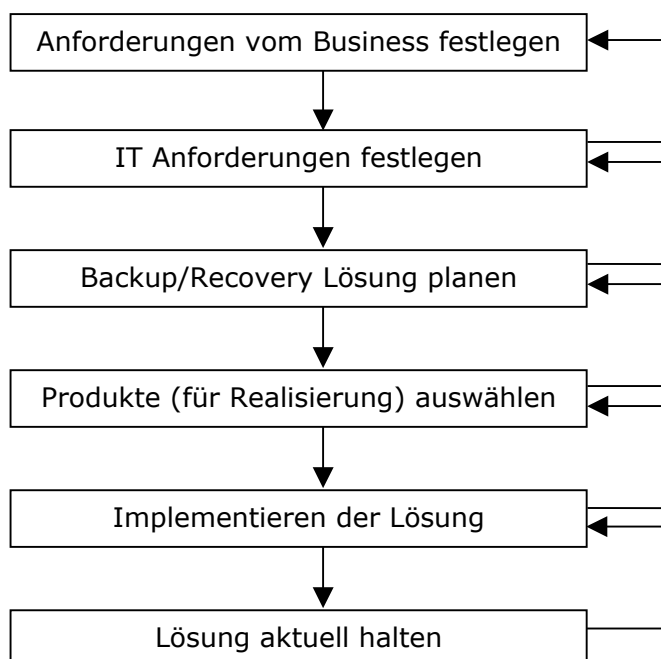
- Begriff: Ein User soll nicht abstreiten können, etwas nicht gemacht zu haben, das er gemacht hat.
- Realisierung durch
 - Konventionelle Unterschriften
 - Digitale Unterschriften
 - Verschlüsselung
- Private Key (symmetrische Verschlüsselung)
 - Probleme:
 - Schlüsselverteilung
 - Teilnehmer müssen vorher Kontakt gehabt haben, damit sie in den Besitz des Schlüssels kommen (kein wirklich offenes System)
 - Verweigerung möglich (man kann niemanden zwingen)
- Publik Key (asymmetrische Verschlüsselung)
 - Jeder Teilnehmer hat ein eindeutiges Paar von Schlüsseln
 - Sein privater Schlüssel (nur für den Besitzer)
 - Ein öffentlicher Schlüssel (in einem öffentlichen Directory aufbewahrt)
- **Forward Public Key Encryption (FPKE)**
 - Sally verschlüsselt die Nachricht mit dem öffentlichen Schlüssel von Peter und Peter entschlüsselt diese dann mit seinem privaten Schlüssel
 - Die Nachricht ist während der Übertragung sicher
 - Teilnehmer müssen vor der Übertragung nicht in Kontakt treten
 - Vertraulich
 - Keine Verweigerung, keine Probleme mit Schlüsselverteilung
 - Ablauf:
 - PKE ist langsam
 - Zufälligen DES Schlüssel s generieren
 - Nachricht unter DES mit s verschlüsseln
 - Schlüssel mit Empfängers öffentlichem Schlüssel verschlüsseln
 - Verschlüsselte Nachricht und Schlüssel schicken
- **Inverse Public Key Encryption (IPKE; Digital Signature)**
 - Nachricht während der Übertragung nicht sicher (jedermann kann den öffentlichen Schlüssel finden und entschlüsseln)
 - Vertraulichkeit nicht erzwungen
 - Verschlüsselung einer Nachricht mit dem eigenen privaten Schlüssel
- **Enveloped Public Key Encryption (EPKE)**
 - EPKE folgt aus Ziel: Vertraulichkeit UND keine Verweigerung erzwingen (enforce confidentiality and non-denial)
 - Nachricht während der Übertragung sicher
- Public Key Algorithmen
 - Bekanntester: RSA (Rivest, Shamir, Adleman)
 - Herz der Informationssicherheit in E-Commerce
- Digitale Signatur erstellen
 - PKE ist langsam
 - Zuerst die Nachricht hashen (@Stedi: let's smoke that shit!)
 - Nachricht mit dem privaten Schlüssel verschlüsseln
- Clear Text Digital Identity (CTDI)
 - Persönliche Info des Besitzers
 - Besitzers öffentlicher Schlüssel

- CA unterschreibt CTDI
- Zertifikat erstellen und ausstellen



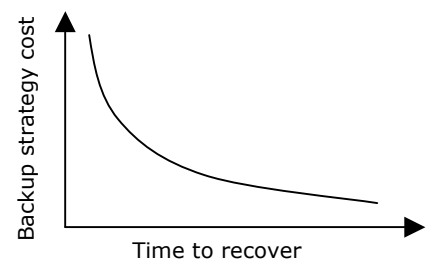
Notfallplanung

- Was ist ein Disaster/Katastrophe?
An extended service interruption of the information systems services of an organisation which can not be corrected within an acceptable predetermine time frame, and which necessitates the use of an alternative site or alternative equipment for recovery.
- Welche Arten von Disaster gibt es?
 - Spezieller Raum
 - Feuer
 - Überschwemmung
 - Stromausfall
 - Gebäude
 - Explosion
 - Bombardierung
 - Feuer
 - Umgebung
 - Erdbeben
 - Verseuchung
 - Flugzeugabsturz
 - Natürliches Disaster
 - Wasser/Feuer
 - menschliche Vandalen
 - nicht autorisierter Zugriff und Gebrauch
- Entscheidungskriterien
 - Umfang des Disasters
 - Recovery-Geschwindigkeit
 - Umfang der Recovery
 - ➔ alle drei Punkte hängen von den Kosten ab!
- Strukturierte Vorgehensweise (Phasen)

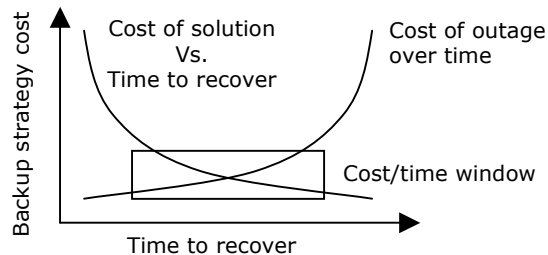


- Phase 1 – Business-Anforderung
 - Risikoanalyse
 - Physikalische Sicherheit
 - Datensicherheit
 - verärgerte Mitarbeiter
 - Backup und Recovery Systeme
 - Verwundbarkeit der Infrastruktur
 - IT Center lokalisieren
 - Key skills
 - Mit welchen Risikotypen ist die UG verwundbar?
 - Welchen Ausfall kann der kritische Businessprozess aushalten?
 - Versuchen alle Businessprozesse als sehr wichtig zu klassifizieren
 - Steps in Analysis
 - Businessprozess identifizieren
 - Wirkung eines Ausfalles bestimmen
 - Kosten
 - lost business
 - Legale Auswirkung
 - Bestimmen des maximal akzeptierbaren Ausfalls
 - Recovery Priorität
 - high critical
 - medium critical
 - low critical
- Phase 2 – IT-Anforderungen
 - Prozesstypen
 - Applikationen, die den Business-Prozess (BP=Business-Prozess?) machen
 - IT Systems Management Infrastruktur, die für den Betrieb und Support der BP notwendig ist
 - Inventur (für Applikationen und Daten)
 - maximal akzeptable „downtime“
 - maximal akzeptabler Datenverlust
 - Data currency when service is resumed (???)
 - Hardware Kapazitätsanforderungen
 - Netzwerkanforderungen
 - zu pflegende Service Levels
 - Service level agreements
 - verfügbare Applikationen
 - nicht verfügbare Applikationen
 - Ordnung der Applikationsrecovery
 - maximaler Ausfall einer Applikation
 - maximaler Ausfall einer Netzwerkverbindung
 - maximaler Datenverlust
 - Information Gathering (Informationssammlung?)
 - Senior Management
 - BP Besitzer
 - Applikationsbesitzer
 - Systemsupport/Programmierung
 - Applikationssupport
 - Systemprogrammierung
 - Netzwerk
 - Operations
 - Informationssicherheit

- Phase 3 – Backup/Recovery Lösung
 - Umfang der Recovery
 - Annahme, welche Typen von Disaster included/excluded sind
 - Sequenz, in welcher Applikationen recovered werden
 - maximale Recoverytime pro Applikation
 - zu wiederherstellende (recovered) Daten
 - Data currency of the data once recovered
 - Teststrategie
 - Wo wird getestet?
 - Welche Ressourcen werden benötigt?
 - Kann das Netzwerk getestet werden?
 - Müssen noch andere Nutzlast/Daten entfernt werden während dem Test?
 - Daten Backup und Recovery Prozesse
 - Online Kopien
 - Wachsen der Kopien
 - Copy DBMS log data
 - Datentransfer und sichere Speicherung
 - Managing and operating the alternate site (alternate site = jene Seite, wo die Backups gespeichert werden)
 - Cold site
 - Anlage hat Strom und ist gekühlt
 - Keine Operationen auf der alternate site
 - Hot site
 - Installierte und bereite Systeme
 - Unbemannt, wird ferngesteuert
 - Personal auf beiden Seiten
 - Beschreibung der Recovery Konfiguration
 - Distanz zwischen den Beiden Seiten (prime <-> alternate)
 - Issues (Probleme)
 - Verbindungsbandweite
 - Verbindungskosten
 - Businessverlagerung
 - Real-time remote update
 - Kombination von in-house und disaster Backup
 - Entscheidungskriterien
 - Disaster-Kosten
 - Startkosten
 - Betriebskosten
 - Kosten im Falle eines Disasters
 - Disasterabsicherung (in welchem Mass)
 - Recoverygeschwindigkeit
 - Vollständigkeit
- Phase 4 – Produktewahl für die Realisierung
 - Kosten
 - Hardware
 - Software
 - Netzwerk
 - Alternate site
 - Implementierungsaufwand
 - Wartungsaufwand



Cost of DR Strategy vs. Outage



- Phase 5 – Implementierung der Lösung
 - Installieren der alternate recovery Anlage
 - Anzahl erlaubter Teilnehmer
 - Support Services
 - Is cold site included?
 - Netzwerktauglichkeit
 - Physische Sicherheit
 - Entwickeln und Implementieren der technischen Möglichkeiten/Verfahren für den Support der Recovery Lösung
 - Daten-Backup Verfahren
 - Speicher-Verfahren ausser Haus
 - Data Recovery Verfahren
 - Change Management Verfahren
 - Application design rules
 - Human resources Verfahren
 - Recoveryplan entwickeln
 - Disaster erkennen und Plan ausführen
 - Recovery Team und Mitglieder
 - Hauptaufgabe und Verantwortungen
 - Inhaber des Plans (?)
 - Pflege des Plans
 - Test des Plans
 - Develop Recovery Teams und Rollen
 - PL
 - Koordinator
 - Vorstand
 - Alternate site manager
 - Zuhörer
 - Management-Team
 - Administrationsteam
 - Info- und Helpdesk-Team
 - Hardware-Team
 - Ausser Haus Speicher-Team
 - Netzwerk-Team
 - Software-Team
 - Operations-Team
 - Applikationssupport-Team
 - Business Users-Team

- Phase 6 – Lösung aktuell halten
 - Wartung
 - neue Applikationen Entwickeln
 - aktuelle Hardware-Konfiguration ändern
 - Netzwerkänderungen
 - organisationale Änderungen
 - Systemänderungen
 - Änderungen der alternate site
 - Revision
 - Test
 - entdecken von Fehlern und Problemen
 - trainieren der Mitarbeiter
 - wachsen der Erkenntnis

Kapitel 14: Internet Layer Sicherheitsprotokolle

Sinn: Sicherheitsdienste für Netzwerke und Internet Layer anbieten. Die Technologie, die diese Dienste ermöglicht, ist Layer 3 tunneling.

Als Ipv6 von der IETF standardisiert wurden, beschloss man, eine passende Architektur für deren Sicherheit zu entwickeln (Ipssec WG). Diese enthält ein IP Security Protocol (IPSP) und ein Internet Key Management Protocol (IKMP) und ist sowohl auf Ipv6 oder Ipv4 anwendbar.

Beim Datenaustausch zwischen zwei Ipssec Modulen wird die Sicherheit durch den Authentication Header (AH) und ein Encapsulating Security Payload (ESP) gewährleistet.

Der AH komprimiert die Authentifikationsdaten eines IP Pakets. Genauer gesagt, wird ein Message Authentication Code (MAC)

- vom sendenden Ipssec Modul errechnet
- ans IP Paket angehängt
- vom erhaltenden Ipssec Modul verifiziert

Das ESP benutzt IP Verkapselung um den Inhalt eines IP Pakets kryptographisch zu verschlüsseln, wobei

- das sendende Ipssec Modul das IP Paket inkapselt und
- das erhaltende Ipssec Modul das IP Paket entkapselt

Diese Ipssec Mechanismen (AH, ESP) können sowohl mit manuellem oder automatisiertem Key Management verwendet werden.

Es wurden, im Gegensatz zu den grundlegenden IPSec Mechanismen, dem IETF Ipssec WG viele Key Management-Protokoll Vorschläge zugeschickt:

- Modular Key Management Protocol (MKMP)
- Photuris Key Management Protocol
- Oakley Key Determination Protocol

MKMP:

- von IBM entwickelt
 - Protokoll für Austausch zwischen A und B:
 - o $A \rightarrow B: N_a, MAC_K(N_a, N_b)$
 - o $B \rightarrow A: N'_b, MAC_K(N'_b, N_a)$
- K: "master secret" (Key?)
 N_a, N_b : "nonce" (Knoten?)

Photuris KMP:

- von Qualcomm
- Dieses Protokoll kombiniert einen Schlüsselaustausch mit einer Authentifikation der öffentlichen Parameter unter Verwendung von RSA Digitalen Signaturen
- Zusätzlich liefert es eine Vorstellung eines Cookie-Austausches zur Verhütung gegen ressourcenblockierende Attacken

Oakley KDP:

- von der University of Arizona
- Wie Photuris KMP
- Im Gegensatz zu seinen Vorgängern sind die verwendeten kryptographischen Algorithmen verhandelbar

Die IETF hat 1996 das Oakley Protokoll zum verbindlichen Key Management Protokoll für das Internet erklärt. Der Hauptgrund für diese Entscheidung war die innewohnende Eigenschaft von Oakley und dessen verwandten Protokollen (z.B. Photuris), PFS (Perfect Forward Secrecy) zu gewährleisten.

Mögliche Implementierungen:

1. Integration des IPsec Protokolls in eine natürliche IP Implementierung



2. „Bump-in-the-stack“-implementation (BITS)

3. „Bump-in-the-wire“-implementation (BITW)

Es wird angenommen, dass in der langen Frist viele Verkäufer IP Stacks anbieten werden, welche die IPsec Protokolle implementieren und beinhalten. Cisco und Windows 2000 beinhalten z.B. Implementierungen für IPsec. Momentan sind die meisten Implementierungen BITS oder BITW.

Kapitel 15: Transport Layer Sicherheitsprotokolle

Transport Layer Sicherheitsprotokolle für das Internet:

- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS)

SSL Facts:

- Version 3.0 in allen grösseren Browsern implementiert
- Basis der Wireless Transport Layer Security (WTLS)

Using SSL:

- Die kommunizierenden Parteien können sich gegenseitig durch Verwendung von Public Key Kryptographie authentisieren
- Vertraulichkeit und Echtheit des Datenverkehrs werden geschützt
- SSL schützt nicht vor
 - o Traffic analysis Attacken
 - o Attacken gegen die TCP Implementierung
- Beide Parteien (z.B. Server und Client) müssen wissen, dass der andere auch SSL verwendet
- Das SSL Protokoll muss auf beiden Seiten einer SSL Session die Statusinformation initialisieren und beibehalten
- Elemente einer SSL Session State Information
 - o Session ID
 - o Peer Zertifikat
 - o Kompressionsmethode
 - o Master secret (z.B. 48 bytes werden zwischen client und server geteilt)
- Eine SSL Session kann für verschiedene Connections verwendet werden
- Elemente einer SSL Connection State Information
 - o Server und Client schreiben MAC secrets (z.B. message authentication keys)
 - o Initialisierungsvektor
 - o Sequenznummer

- Das SSL Record Format Protocol stellt
 - o Fragmentierung
 - o Komprimierung und Dekomprimierung
 - o Verschlüsselung und Entschlüsselung
 zur Verfügung.
- Jeder SSL Record beinhaltet
 - o Inhaltstyp
 - o Versionsnummer des Protokolls
 - o Länge
 - o MAC
- Mit dem SSL Handshake Protokoll können Client und Server
 - o Eine Kompressionsmethode auswählen
 - o Den Server authentisieren
 - o Optional den Client authentisieren
- Key exchange Algorithmen
 - o RSA
 - o Fortezza
 - o Diffie-Hellman
- Proxy-Server gelten als “man-in-the-middle”
- End-to-end Sicherheitsprotokolle, wie SSL, wurden als Schutz gegen „men-in-the-middle“ erstellt
- Folglich ist die Zusammenarbeit zwischen diesen Protokollen und proxy-basierten Firewalls nicht einfach
- Ein Protokoll kann durch eine Firewall „proxiiert“ oder „getunnelt“ werden
 - o Proxiert: Proxy Server hat Kenntnis vom Applikationsprotokoll
 - o Getunnelt: Proxy Server hat nicht Kenntnis vom Applikationsprotokoll
- Mit dem Tunnel Protokoll kann der Client (z.B. Browser) HTTP benutzen, um sich mit dem HTTP proxy server zu verbinden
- Deshalb gibt der Client den passenden Hostnamen und Portnummer an
- Der Gebrauch von SSL zur Sicherung von HTTP Datenverkehr beeinflusst die Nützlichkeit von Proxy Servern fürs Caching negativ
- Der grösste Nachteil von SSL ist, dass es keinerlei Support für die Sicherung von UDP-basierten Applikationen gibt

Kapitel 16: Application Layer Sicherheitsprotokolle

2 Möglichkeiten, Application Layer zu sichern

- Nimm ein gegebenes Applikationsprotokoll und füge ihm die benötigten Sicherheitsfeatures bei
→ security-enhanced application protocols
- Füge einem Sicherheitssystem ein standardisiertes API bei, das von vielen Applikationsprotokollen gebraucht werden kann, um die verlangten Sicherheitsfeatures einzubauen
→ authentication and key distribution systems

Security-enhanced application protocols:

- Terminal access (z.B. Telnet, Rlogin...)

- Secure Telnet (STEL)
- Secure Shell (SSH)
- File Transfer (z.B. FTP)
- Email (z.B. POP3)
 - SMTP/POP3 auf SSL
 - Secure messaging schemes
 - Pretty Good Privacy (PGP)
- WWW Transaktionen (z.B. HTTP)
- Domain Name System (DNS)

Authentifikations- und Schlüsselverteilungssysteme

- Kerberos
 - Secure European System for Applications in a Multi-vendor Environment (SESAME)
- SPX

Design-Anforderungen für Kerberos

- Single sign-on (Password wird nur einmal, für das anfängliche Login verwendet)
- Public Key Kryptographie wird nicht verwendet

In der Kerberos Architektur muss jede Sicherheitsdomäne eine sichere Umgebung betreiben, welche ein Key Distribution Center (KDC) verwaltet. Die KDC hat eine Datenbank mit einem Geheimschlüssel K_p für jedes P.

Mankos von Kerberos:

- Man ist auf die Verlässlichkeit der KDC angewiesen
- Schlechte Skalierbarkeit

SESAME

- Basiert auf Authentisierungsservice von Kerberos
- Benutzt Privilege Attribute Certificates (PACs) um den Einheiten Sonderrechte zu verteilen
 - PAC
 - Digital unterzeichnetes Statement über die Sonderrechte einer Einheit

Kapitel 17: Message Sicherheitsprotokolle

2 Möglichkeiten, Nachrichten sicher durch ein Computernetzwerk zu senden

- Verwende ein gesichertes Nachrichtentransferprotokoll
 - application layer security protocol
- Verwende ein gegebenes (unsicheres) Nachrichtentransferprotokoll und sichere die Nachricht bevor sie verschickt wird
 - message security protocol

Pretty Good Privacy

- Kryptographische Algorithmen, die in ein plattformunabhängiges Software-Paket integriert sind (von Zimmermann)
- Im Gegensatz zu anderen secure messaging schemes kann PGP off-line verwendet werden
- Falls ein UA MIME-kompatibel ist, können die Funktionalitäten von PGP mit denen von MIME verbunden werden

Unterschiede PGP und MIME

- Sie verwenden unterschiedliche Nachrichtenformate
- Verschiedene Handhabung der Public Keys und Public Key Zertifikate (web of trust vs. PKI)

Kapitel 18: Schlussfolgerungen und Ausblick

Fragen

- Welches Sicherheitsprotokoll ist das Beste?
- Welches Layer eignet sich am besten, um die Kommunikation zu sichern?

→ Diese Fragen sind schwierig zu beantworten

End-to-end Argument

- Sicherheitsfunktion kann nur dann vollständig und korrekt implementiert werden, wenn das Wissen über die Applikation am Endpunkt des Kommunikationssystems vorhanden ist

Lecture 1 – Introduction to Information Security

Sicherheit in der Informationstechnik:

Computersicherheit -> Netzwerksicherheit -> Internet-Sicherheit

Methode:

Identifikation des Risikos -> Risikoeinschätzung -> Risiko-Lösung -> Risikoüberwachung

Gefahren:

- Verlust/Ausstieg der IT-Anlagen
- unerlaubter Zugriff auf IT
- unerlaubte Änderung der IT
- Fälschung von Objekten
- Person leugnet, eine Aktion zu machen

Software kann bösartig zerstört werden oder versehentlich geändert/gelöscht werden:

- Löschen von Software
- Logische Bombe (Ändern des Programs, die Datei am 1. Juli zu löschen)
- Trojanisches Pferd; Trapdoor (versteckter Einstieg möglich)
- Informations-Leck (Information wird unauthorisierten Personen zugänglich gemacht)

Verteidigungsmethoden:

- Verschlüsselung
- Authentifizierung (public key, one-way, two-way)
- Digitale Signaturen + DI's
- Sicherheitsprotokolle (SET, SSL, SHTTP)
- MAC (message authentication codes)
- Beschränkung des Zugriffs (Firewalls, Rechtevergabe)
- Sensibilisierung der Personen
- Organisatorische Massnahmen
- Paketfilter / Application Gateways
- Email-Sicherheit (PGP, S/MIME)
- One-Time-Passwords

Ziel: ISO-Standard:

- Identifikation und Authentifizierung
- Authorisation
- Vertraulichkeit
- Integrität
- Unleugbarkeit

Architektur & Sicherheitsaspekte

RSD (Rapid Secure Development):

Nutzungsszenario -> Dienste -> Gefahren -> Massnahmen -> Realisierung mit Rückkopplung (Überprüfung & Validierung)

= systematische Vorgehensweise und hilft, keine wesentlichen Sicherheitsprobleme zu übersehen, bietet aber keine vollautomatische sichere Internet-Nutzungskonzeption

Weitere Massnahmen:

- Angriffserkennung
- Katastrophenplanung (Backup)
- Dokumentationen: Überblick, Benutzerhandbuch, Topologie, Problemlösungen (auch für Unerfahrene lesbar)
- Schulung der Mitarbeiter (Fehlerverriingerung durch richtiges Verhalten und Wissen)
- Bewusstseinsbildung (Aufmerksamkeit auf Gefahren und Risiken; Verantwortungsbewusstsein)
- Geschäftsgrundsätze - Policies

Topologie:

Internet (offenes Netzwerk basierend auf TCP/IP):

- Weltweit
- Interaktion mit Kunden
- Nutzung (Informationsnachfrage, -angebot, e-Commerce)

Intranet (geschlossenes TCP/IP-Netzwerk, Teilnehmer definiert):

- Wer nimmt teil?
- Nutzung

Extranet- Trusted Third Parties:

- Interaktion zwischen Unternehmen
- Häufig über Internet → Sicherheitsprobleme

Probleme:

- Technisch: Unterschied zwischen Inter-, Intra- und Extranet nicht existent (alle TCP/IP)
- Organisatorisch: Sicherheit- und Datenschutzfragen erfordern Trennung der Netze

Lösung:

- Klassifikation von Netzen nach Aufgaben und Sicherheitsanforderungen
- Ziel: Abschottung der identifizierten Netze durch organisatorische und technische Massnahmen
- Area Konzept: Identifikation von Subnetzen gleicher Sicherheitsanforderungen anhand Anwendungen, Netzelementen, Endsystemen und Organisation
- Virtual Private Networks: Absicherung des Datenaustauschs zwischen Netzen hoher Sicherheitsanforderungen über unsichere Netze (für Intranets über verschiedene Standorte, Extranets, Remote Access), realisiert mit kryptographischen Massnahmen

Kryptographische Hilfsmittel:

- Symmetrische Verfahren (private key)
- Attacken auf Kryptosysteme
- Algorithmen
- Brute Force Attack Vergleich
- Asymmetrische Verfahren (public key)
- Bedingungen und Prinzipien asymmetrischer Kryptosysteme

Symmetrische Verfahren:

$f_k: M \rightarrow C$, $f_k^{-1}: C \rightarrow M$

c soll unter Kenntnis von k und m effizient berechenbar sein, m soll unter Kenntnis von c und k zurückgewonnen werden

Attacken auf Kryptosysteme:

m: Klartext, c: Chiffre, k: Schlüssel

- Known Cyphertext Attack (c bekannt, m+k nicht)
- Known Plaintext Attack (c+m bekannt, k nicht)
- Chosen Plaintext Attack (freies m mit Kenntnis von c, k unbekannt)

Symmetrische Algorithmen:

- DES (56bit): 1977, Brute Force: 2^{56} Versuche
- 3DES (2x56bit): 3 DES Verschlüsselungen in Folge, Brute Force: $2^{(2 \cdot 56)}$ Versuche
- IDEA (128bit): 90er Jahre, Brute Force: 2^{128} Versuche

Brute-Force-Attack:

Bei 40bit ca. 1 Tag, bei 128 bit 10^{23} Jahre = sicher

Annahme: 10 Millionen Versuche pro Sekunde

Amerikanische Exportrestriktion aber 40 bit

Asymmetrische Kryptosysteme:

m: Klartext

f_e : Verschlüsselungsfunktion

g_d : Entschlüsselungsfunktion

e, d: Schlüsselerzeugung

f: Chiffre

Bedingung für asymmetrische Kryptosysteme:

- Zusammenhang zw. e und d
- wenn e und c bekannt, darf m nicht berechenbar sein
- wenn m, e und c bekannt, darf d nicht berechenbar sein

-> 2 letzten Punkte sind nicht lösbar, wenn e und d einen Zusammenhang haben

Lösung: Verwendung mathematisch schwer lösbarer Probleme wie z. B.

Primzahlfaktorisation

Signaturen:

- Verwendung von Hashsummen
- ElGamal, MD5 etc.

Sicherheitsmanagement

Fehlende Sicherheit:

- betriebswirtschaftliche Auswirkungen
- volkswirtschaftliche Auswirkungen
- Auswirkungen für Mensch und Umwelt

aber:

Sicherheit = Kosten ohne Produktivität:

- mangelndes Sicherheitsbewusstsein bei Führung
- Probleme mit Kompetenzvergabe
- vertagte Investitionen
- Angst vor Prestigeverlusten

Grundbedrohungen:

- Vertraulichkeit, Abhörsicherheit und Anonymität
- Integrität
- Verfügbarkeit
- Verbindlichkeit

3 Ebenen: strategische, taktische und operative Ebene

Informationsmanagement:

Informationssicherheit mit Sicherheitsmanagement planmässig herstellen, überwachen und erhalten

Sicherheitsmanagement:

Erreichung der strategischen Sicherheitsziele, Verhindern der realen Schäden

Strategische Ebene:

- Grundsatzentscheidungen basierend auf Unternehmenspolitik
- Rahmenbedingungen
- definiert organisatorische Elemente

Informationssicherheitspolitik:

- Grundsätze
- Erfüllung von Gesetzen
- Voraussetzungen für interne Revision
- Möglichkeit im Schadensfall allfällige rechtliche Schritte abzustützen

Taktische Ebene:

- Anwendung Grundsatz
- Feststellung momentaner Bedrohungssituation und Identifikation der Schutzobjekte
- Risikoanalyse
- Suche nach adäquaten Massnahmen und Bewertung
- Auswahl und Realisierung durch Management
- Kontrolle

Operative Ebene:

Personelle und organisatorische Massnahmen:

- Ausbildung
- Handbuch
- Rollenkonzept
- Beachtung von Interessens- und Befugniskonflikten
- Protokollierung
- Mehr-Augen-Prinzip
- Auditing/Revision

Technische Massnahmen:

- Zugriffskontrolle
- Verschlüsselung
- Digitale Unterschriften
- Integritätssicherung
- Authentisierung
- Verkehrserzeugung
- Routingkontrolle
- Notarisierung

Bauliche Massnahmen:

- Zugangskontrolle
- Feuer-/Wasserschutz
- Katastrophenplanung
- Ausweichlösungen
- Evakuierungspläne
- UPS (unterbrechungsfreier Strom und Überspannungsschutz)

Gefahren Internet:

- Neue Bedrohungen, die unsichtbar sind und von weltweit kommen (jeder Rechner kann jeden erreichen)
- Datenschutz- und Urheberrechtproblematik verschärft
- hohe Komplexität:
 - Daten könnte beim Transport mitgelesen werden
 - kein Schutz gegen Verfälschung/Verlust/Duplizierung
 - Fälschung von Absendererkennungen möglich

Sicherheitsmanagement – Authentifizierungs- & Autorisierungsinfrastrukturen

C.Stettler <cs@rogatec.ch>

Einführung

Sicherheit

- mit Aufkommen von eCommerce und eBusiness zunehmend wichtig
- vor allem in Netzwerken und verteilten Systemen (Internet)
- Sicherheit umfasst viele Aspekte

Sicherheitsdienste

- Authentifikationsdienste
- Zugriffskontrolldienste
- Datenvertraulichkeitsdienste
- Datenintegritätsdienste
- Verbindlichkeitsdienste

Authentifikation / Autorisierung

- Authentifikation bei eCommerce /eBusiness nicht primär („Hauptsache, er kann zahlen“)
- Autorisierung ist entscheidend

Autorisierungsverfahren/-systeme

- auf Basis von Authentifikation (Zugriffsregelung über Username / Password)
- anonyme Verfahren (Ticketing-Systeme, anonyme Zahlungssysteme)

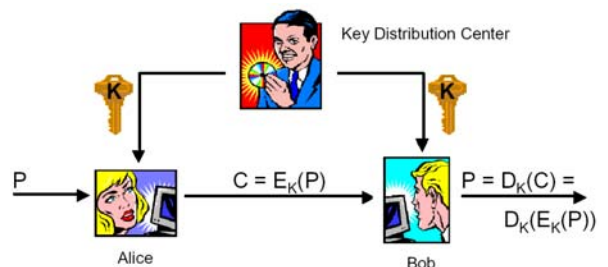
Authentifikations- und Autorisationsinfrastruktur

- Infrastruktur, die Authentifikations-/Autorisationsdienste anbietet
- ev. nur Vereinfachung der Umsetzung der Dienste → API nötig
- Ansätze
 - PKI-basiert → asymmetrische Kryptosysteme
 - Passwort-basiert → benutzerspezifische Passwörter
 - elektronische Zahlungssysteme

PKI-basierte Ansätze

symmetrisches Kryptosystem

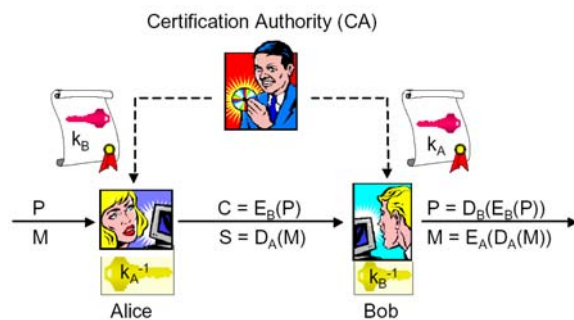
- nur einen Schlüssel für Ver- / Entschlüsselung
- Single / Secret Key Cryptosystem
- Key Distribution Center verteilt Schlüssel
- Einigung auf einen Schlüssel als Problem
→ wie sicher übermitteln ?



asymmetrisches Kryptosystem

- jeder Benutzer hat zwei Schlüssel
 - privater Schlüssel (private key)
 - öffentlicher Schlüssel (public key)
- „Public Key Cryptosystem“
- Certificate Authority (CA) vergibt Schlüssel
- CA speichert Zertifikate in zentralem Verzeichnisdienst (LDAP)

- Benutzer können Zertifikate und Statusinformationen aus Verzeichnisdienst holen
→ Gültigkeit des Zertifikates validieren
- Schlüssel stehen in mathematisch eindeutiger Beziehung
- Berechnung des einen Schlüssels aus dem anderen nicht mit vertretbarem Aufwand
- Basis für Sicherheit: Faktorisierungsproblem → zu komplex für heutige Rechner
- Sicherstellung Authentizität und Integrität der öffentlichen Schlüssel nötig
- Public Key Zertifikate bestätigen Zusammengehörigkeit öffentlicher Schlüssel – Benutzeridentität
- verschiedene Modell und Ansätze (meist X.509)
 - Version, Seriennummer, Signatur-Algorithmus-Identifikator, Aussteller, Gültigkeit, Subjekt, Subjekt Public Key Informationen, Erweiterungsfelder, digitale Signatur von CA
- Varianten
 - Codierung von Autorisierungsinformationen in Erweiterungsfelder der Zertifikate → bei statischen Informationen
 - Verwendung von speziellen Attributzertifikaten → bei dynamischen Informationen
 - Verwaltung von Autorisierungsinformationen in DB → bei dynamischen Informationen
- Aufbau / Betrieb von öffentlicher PKI und Einsatz von Public Key Zertifikaten sehr schwierig



Passwort-basierte Ansätze

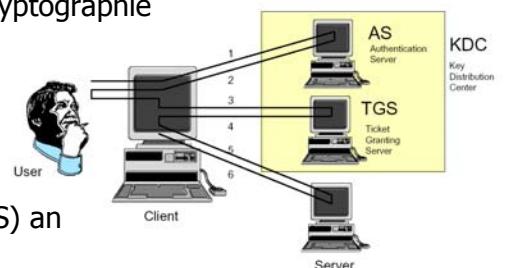
Beispiele

- Kerberos
- Microsoft .NET Passport
- Liberty Alliance Project

Kerberos

- Ziel: Single Sign On
- Ticketing System → bewusster Verzicht auf asynchrone Kryptographie
- Ablauf

- Client kontaktiert Authentication Server (AS) mit User-Passwort
- Client erhält Master Ticket von AS
- Client fordert mit Master Ticket spezifisches Service-Ticket bei Ticket Granting Server (TGS) an
- Client erhält Service Ticket
- Client benutzt Service auf gewünschtem Server unter Vorweisen des Service Tickets



- Tickets
 - können von Client nicht dechiffriert, nur weitergeben werden
 - Client muss Beweis mitliefern, dass er rechtmässiger Besitzer des Tickets ist -> Authentifikator (chiffrierter Zeitstempel)

- User Passwort
 - wird nicht übermittelt → kein Sniffen möglich
 - AS sendet Client einen String, Client verschlüsselt String mit Passwort, AS entschlüsselt (kennt das Passwort)
- Verifial Password Guessing
 - Hacker fängt chiffrierten String ab
 - Passwörter raten, testen, ob String Sinn macht
 - User-Passwort meist schlecht

MS .NET Passport

- Verwendung von SSL zwischen User und Passport Server → PKI ! → viel einfacher als Kerberos
- Ablauf
 - Client besucht Site mit .NET Passport
 - Site leitet User an zentralen Passport Server weiter
 - User logt bei Passport Server ein → erhält Cookies
 - Passport Server leitet User auf ursprüngliche Site zurück

Erweiterung → AAI

- Privilegien direkt in Ticket integrieren (Windows 2000)
- Privilegien in Privilege Attribute Server speichern

Vergleich

Ansatz	Vorteile	Nachteile
PKI-basiert	<ul style="list-style-type: none"> ▪ einfache Authentifikations- / Autorisationsprotokolle („Offline“) ▪ Zertifikate als intuitiv verständliche Technologie (digitale Identitätskarte) ▪ flexibler Einsatz / Erweiterbarkeit 	<ul style="list-style-type: none"> ▪ noch keine Standardisierung / Profilierung (→ Attributzertifikate) ▪ meist Zusatzhardware erforderlich (Smart Cards, USB-Tokens)
Passwort-basiert	<ul style="list-style-type: none"> ▪ Umgang mit Passwörter intuitiv verständlich ▪ keine Zusatzhardware nötig ▪ kein Bedarf nach Standardisierung / Profilierung ▪ Effizienz 	<ul style="list-style-type: none"> ▪ komplexe Authentifikations- / Autorisationsprotokolle (Kerberos ...) ▪ Initialaufwand für Passwortverteilung ▪ Big-Brother-Eigenschaft (AS weiss alles) ▪ Verwundbarkeit der Authentifikations- / Autorisationsserver („Online“)

Ausblick

- PKI-Ansätze überzeugen aus theoretischer Sicht (speziell digitale Signaturen für Verbindlichkeitsdienste)
- PKI-Ansätze in Praxis mit erheblichen Problemen
- heute meist Passwort-basiert oder Mischform
- bei Biometrische Verfahren noch Fragen bez. Leistungsfähigkeit, Skalierbarkeit, Benutzbarkeit, Unterstützungsmöglichkeiten (sind sehr teuer, wenn sie gut sein sollen)