VU Security - 050125-1
WS 2013/2014

Willy Weisz

Forschungsplattform Computational Science Center

Informationen zur Lehrveranstaltung auf
http://www.csc.univie.ac.at/index.php?page=teaching

willy.weisz@univie.ac.at

für diese Lehrveranstaltung zu verwenden:
vusec@csc.univie.ac.at

universität wien

Ziele der LVA Security

Wissen über

- Sicherheitsthemen in der Informationstechnologie
- Bedrohungsszenarien für die Sicherheit
  - in einem Rechner
  - im Netz
- Strategien und Sicherheitsrichtlinien
- einige technische Lösungen

Literatur

- Da die Vorlesung „work in progress“ ist, wird die Liste der Literaturempfehlungen im Verlauf des Semesters erweitert werden.

Literatur

Urahn der Sicherheitsnormen in der IT:

Trusted Computer System Evaluation Criteria - TCSEC

(bekannt als „Orange Book)

DoD-5200.28-STD,December 1985

http://www.dynamoo.com/orange/fulltext.htm

Erstes der „Rainbow Series Books“

Literatur

Heute wird die Vertrauenswürdigkeit von Systemen differenzierter als durch eine eindimensionale Hierarchie dargestellt gesehen:

Common Criteria und

Common Evaluation Methodology

http://www.commoncriteriaportal.org

Literatur

siehe Sicherheitshandbuch des

http://www.bsi.bund.de/gshb/index.htm

http://www.bsi.bund.de/gshb/deutsch/index.htm

Auswirkungen

Sicherheit in der IT

- ist aufwendig,
- einschränkend,
- hinderlich,
- lästig,
- saugt Leistung ab,
- frustriert Betreiber von EDV wie Anwender.

Wieso also?

Ethische Forderungen

- Schutz der Privatsphäre
- Schutz des geistigen Eigentums
- Schutz des Individuums
- Schutz anvertrauter Geheimnisse

Wieso also?

Rechtliche Erfordernisse

- abgeleitet von den ethischen Forderungen
- Schutz des Informationseigentums
- Schutz von Staats- oder Geschäftsinteressen
- Durchsetzung von anderen gesetzlichen Vorschriften wie z.B.
  - Arztgeheimnis
  - Amtsgeheimnis

Vertrauen und Sicherheit

Sicherheit schafft Vertrauen

- in korrekte Verarbeitung
- in den Schutz der Informationen
  - vor Zerstörung
  - vor unerlaubter Veränderung
  - vor unerlaubter Einsicht

Vertrauen

Vertrauen erfordert Garantien (Strafandrohungen?) gegen Vertrauensbruch

- ideeller Art (Familie, Freundschaft)
- materieller Art (Bürgschaften usw.)
- rechtlicher Art (z.B. Haftungen)

Kann man einem System aus Hard- und Software „vertrauen“?

- woher kommt die „Garantie“?

Ein wenig Englisch

Da Englisch die „lingua franca“ der IT ist, ein paar Übersetzungen:

Vertrauen – trust

Sicherheit – security, aber auch safety

Bedrohung – threat

Richtlinie – policy

Schutz – protection

Weitere englische Fachausdrücke werden folgen.

Daten vs. Informationen

Daten in IT Systemen: Folge von Bits

Daten allein

- haben keinen Wert, aber
- ihr Verlust (Veränderung) kann Schaden sein.

Daten

- mit semantischer Deutung
- mit Verarbeitungsvorschriften (z.B. Programm)

sind Information.

Warum Informationen schützen?

- Informationen haben Wert
- Schutz personenbezogener Informationen (zum Teil) von Gesetzes wegen vorgeschrieben
- Verlust (unbefugte Veränderung) von Daten führt zu Informationsverlust ⇒ Verlust von Werten
- Vertrauensverlust des Benutzers
  - in Soft- und Hardware
  - in IT-Dienstleister

Informationen schützen Aufgabe des Benutzers

- Sicherheit auch Aufgabe des Benutzers
- Unsicherer Einsatz von Hard- und Software macht jede Sicherungsmaßnahme zunichte
- Sicherheitsbewusstsein muss zum Reflex werden

Ermittlung der Bedrohung

Bedrohungspotentiale sind vielfältig

- „Das Böse ist immer und überall“ (© EAV)

Bedrohung richtig einschätzen

- nicht überschätzen (kann teuer sein)
- aber auch nicht unterschätzen (wird sicher sehr teuer)

Bedrohungsanalyse (threat analysis) ist Voraussetzung für richtige Schutzmaßnahmen

Einige Bedrohungsbeispiele

Schadprogramme:

- können Daten (eventuell sogar Hardware) zerstören
- Systeme am Verarbeiten hindern (denial of service – DoS)
- Viren – Schadprogramme, die sich selbst (eventuell mit Änderungen) reproduzieren und verbreiten.
- Trojaner – Programme zum Ausspähen von Daten.
- Identitätsdiebstahl

Aufgaben

1. Nennen Sie Informationen, deren unrechtmäßige Kenntnis eine Bedrohung darstellen kann.
2. Nennen Sie Informationen, deren Verlust eine Bedrohung darstellen kann.
3. Nennen Sie Informationen, deren Verlust geringen, deren (unerkannte) Verfälschung eine großen Schaden anrichten kann.
4. Von welchen IT-Sicherheitsbedrohungen und -brüchen haben Sie zuletzt gelesen oder gehört?

Aufgaben

5. Was ist Datendiebstahl?

Was unterscheidet ihn von anderen Diebstählen?

Was müsste man sicherstellen, damit er sich nicht unterscheidet? Welchen Vorteil hätte das?

Aufgaben

6. Was sind die Bedrohungen in folgenden Fällen und die hinreichend sicheren wie auch ökonomisch günstigsten Sicherungs-maßnahmen für jeden der folgenden Fälle?

a. Am Beginn Ihrer Diplomarbeit haben Sie eine vollständige Literaturliste erstellt.

b. Sie stehen vor dem Abschluss einer lange vorbereiteten wissenschaftlichen Arbeit – eine frühere Publikation der Ergebnisse durch Andere macht sie wertlos.

TCSEC

Erste Einführung in Sicherheitskonzepte anhand von TCSEC (Orange Book)

Vorteil:

- Übersichtlichkeit wegen
  - Eindimensionalität
  - Hierarchie

TCSEC

Grundlegende Erfordernisse

- Sicherheitsrichtlinie – Security policy
- Verantwortlichkeit – Accountability
- Vertrauenswürdigkeit – Assurance
- Dokumentation – Documentation

TCSEC - Sicherheitsrichtlinie

Sicherheitsrichtlinie

- explizit formuliert
- klar definiert
- vom System erzwungen
- einige der Vorgaben:
  - Sicherheitsetikett – security label
  - Löschen der Information vor Zuteilung von Speicherobjekten
  - bestimmt Zugriffssteuerung – access control

TCSEC - Zugriffssteuerung

Zugriffssteuerung (soweit in TCSEC verwendet)

- auf Ermessensbasis
  discretionary access control – DAC
  - gesteuert durch Identität
  - „need to know“-Zugriffsrechte
- auf Ermächtigungsbasis
  mandatory access control – MAC
  - gesteuert durch Sicherheitseinstufung
  - hierarchisch
  - Objekte behalten Einstufung auch bei Export

TCSEC - Verantwortlichkeit

Erzwing- und überprüfbar

- Identifizierung – Identification
  - Zuordnung zu Individuum
- Authentisierung – Authentication
  - Nachweis der eigenen Authentizität
- Authentifizierung - Authentication
  - Überprüfen der behaupteten Authentizität
- Revision - Auditing

TCSEC - Vertrauenswürdigkeit

- Vorhandensein von Hard- und Software zur Erzwingung der Sicherheitsrichtlinie und der Verantwortlichkeit
- Garantie, dass vertrauenswürdige System-komponente wie vorgesehen funktioniert
- Vertrauensebenen
  - betriebliche (operational) Vertrauenswürdigkeit
  - Lebenszyklus-Vertrauenwürdigkeit – Life-cycle Assurance

TCSEC - Vertrauenswürdigkeit

Betriebliche Vertrauenswürdigkeit

- Systemarchitektur und -unversehrtheit (integrity)
- Vertrauenswürdige Verwaltung und Wiederherstellung
- Analyse von verdeckten Kanälen (covert channels)
  - parasitärer Kommunikationskanal
  - stiehlt Bandbreite
  - überträgt unbeabsichtigte und unerlaubte Information

TCSEC - Vertrauenswürdigkeit

Lebenszyklus-Vertrauenswürdigkeit

- Sicherheitstests
- Entwurfsspezifikation und -überprüfung
- Konfigurations-Management für sicherheits-relevante Komponenten (Überwachung von Änderungen)
- vertrauenswürdige Software-Distribution

Laufender Schutz der Vertrauenswürdigkeit

TCSEC - Dokumentation

- Entwurfsdokumentation
- Dokumentation der Sicherheitseinrichtungen
- Dokumentation der Systemverwaltung
- Dokumentation von Überprüfungsvorgängen

TCSEC - Referenzmonitor

Logische Einheit zur Durchsetzung der Zugriffssteuerung

- Zugriff auf Objekte nur über Referenzmonitor (reference monitor)
- Regeln genau definiert und richtig umgesetzt
- muss selbst geschützt sein
- seine Daten (z.B. Regelwerk, Log-Dateien) müssen ebenfalls geschützt sein
- überprüfte korrekte Implementierung

TCSEC - Sicherheitsklassen

D – Minimaler Schutz

- beurteilte Systeme, die jedoch
- keiner der höheren Sicherheitseinstufungen entsprechen

Aufgabe

7. Der ursprüngliche „Personal Computer“ unter MS-DOS, das keiner Evaluierung unterzogen wurde (und sicher nie bestanden hätte) war recht sicher.

a. Wie das?

b. Wodurch ist die Gefährdung entstanden?

TCSEC - Sicherheitsklassen

C – Ermessensbasierter Schutz
Discretionary Access Control – DAC

C1 ermessensbasierter Schutz

- Auseinanderhalten von Benutzern und Daten
- Benutzer authentifizieren sich
  - vor Beginn der Aktion
  - anhand geschützter Authentisierungsdaten
- Objektschutz
  - differenziert („ugo“ von Unix, ACLs)
- Szenarium: kooperierende Benutzer

TCSEC - Sicherheitsklassen

C2 kontrollierter ermessensbasierter Schutz

- feinkörniger als C1
  - Benutzer einzeln identifizierbar
  - individuelle Verantwortung durch z.B. login
- Revision sicherheitsrelevanter Aktionen
- Isolation von Ressourcen
- Systemdokumentation
- Benutzerhandbücher

TCSEC - Sicherheitsklassen

B – Ermächtigungsbasierter Schutz
Mandatory Access Control – MAC

B1 Labelled Security Protection

- Formlose Darstellung der Sicherheitsrichtlinie
- Sensitivitätsmarken für Objekte
  - werden auch mit Objekt exportiert
- MAC für ausgewählte Objekte
- Fehler müssen behoben oder umgangen werden

TCSEC - Sicherheitsklassen

B2 Strukturierter Schutz

- Sicherheitsrichtlinie ausformuliert und formal
- Alle Objekte mit DAC oder MAC
- Analyse verdeckter Speicherkanäle
- Verbesserte Test- und Überwachungsfunktionen
- Verstärkte Authentifizierungsmechanismen
- Trennung von Operator und Administrator
- .....

TCSEC - Sicherheitsklassen

B3 Sicherheitsdomänen

- Referenzmonitor-Anforderungen
- Trennung von sicherheitsrelevanten und anderen Komponenten
- Reduzierung der Komplexität
- Sicherheitsadministrator
- Audit sicherheitsrelevanter Ereignisse
- Eindringversuche
  - sofortige Entdeckung und Meldung

TCSEC - Sicherheitsklassen

B3 (Fortsetzung)

- vertrauenswürdige Wiederherstellung (recovery)
- Analyse zeitgesteuerter (timing) verdeckter Kanäle
- ...

TCSEC - Sicherheitsklassen

A Verifizierter Schutz

A1 Verifizierter Entwurf

- Funktionalität wie B3
- formalisierte
  - Entwurftechniken
  - Testtechniken
  - Verwaltungsprozeduren
  - Distributionsprozeduren

TCSEC - Sicherheitsklassen

über A1 hinaus

- formale Verifikation auf der Stufe des Quellcodes
- automatische Test-Generierung
- ...

TCSEC - Sicherheitsklassen

Meist anvisierter Schutz gut gesicherter Systeme:

- Evaluation für C2

TCSEC

Nachteil von TCSEC:

- strenge Hierarchie
  - nur Gesamtsicht
  - keine Bewertung einzelner Funktionalitäten
- keine Trennung von
  - Funktionalität (functionality)
  - Vertrauenswürdigkeit (Qualität) - Assurance
    - Korrektheit - Correctness
    - Wirksamkeit - Effectiveness

Nachfolger von TCSEC

Europa:

ITSEC – Information Technology Security Evaluation Criteria (1991)

Heutige Norm:

Common Criteria (CC)

mit

Common Criteria Evaluation Methodology

Common Criteria

1999 eingeführt

Derzeit Version 3.1 Release 4

3 Teile

- Einführung und allgemeines Modell
  Introduction and General Model
- Funktionale Sicherheitsanforderungen
  Security Functional Requirements
- Anforderungen an die Vertrauenswürdigkeit
  Security Assurance Requirements

Common Criteria

Web-Site: http://www.commoncriteriaportal.org

Unterteilung in

- Funktionsklassen – functional classes - nicht hierarchisch
- Vertrauenswürdigkeit (Qualität)
  - Wirksamkeit der Methoden
  - Korrektheit der Implementierung
  - beide sind zu prüfen

Common Criteria

Beispiele von Funktionsklassen:

- Kommunikation
- Schutz der Benutzerdaten
- Schutz der Sicherheitsfunktionen
- vertrauenswürdiger Pfad
- Identifizierung und Authentifizierung
- ...

Common Criteria

Funktionsklassen werden zu Schutzprofilen – Protection Profiles (PP) – zusammengefasst, z.B. für Firewalls, SmartCards

PPs benutzerseitig definiert

Produkt implementiert ein oder mehrere PPs

PPs können als Vorlage für das Sicherheitsziel – Security Target (ST) – dienen

ST dokumentiert die Sicherheitseigenschaften eines Produkts

Common Criteria

Vertrauenswürdigkeit

- Anforderungen zur Sicherstellung der Sicherheit – Security Assurance Requirements
  - Maßnahmen bei der Entwicklung
  - Maßnahmen bei der Evaluierung
  - CC enthalten Katalog von Maßnahmen
  - Maßnahmen in ST und PP dargestellt

Common Criteria

Vertrauenswürdigkeit

- Evaluierungsstufen – Evaluation Assurance Level (EAL)
  - numerische Bewertung des zu evaluierenden Produkts – Target Of Evaluation (TOE)
  - spiegelt die erfüllten Sicherheitsmaßnahmen wieder
  - Werte von 1 bis 7
  - höherer Wert heißt nicht unbedingt sicherer!!
    - nur dass das Vertrauen in die Implementierungsqualität der versprochenen Funktionen größer ist

Common Criteria

CC	ITSEC	ITSK	Bedeutung	TCSEC
EAL1	**E0-E1**	**Q0-Q1**	funktionell getestet	**D-C1**
EAL2	**E1**	**Q1**	strukturell getestet	**C1**
EAL3	**E2**	**Q2**	methodisch getestet und überprüft	**C2**
EAL4	**E3**	**Q3**	methodisch entwickelt, getestet und durchgesehen	**B1**
EAL5	**E4**	**Q4**	semiformal entworfen und getestet	**B2**
EAL6	**E5**	**Q5**	semiformal verifizierter Entwurf und getestet	**B3**
EAL7	**E6**	**Q6**	formal verifizierter Entwurf und getestet	**A**

Analyse

Erste Aktivität zur Herstellung von Sicherheit in der IT:

Analyse

- der Werte – assets – unserer IT
- der Bedrohungsszenarien – threat scenarios

Danach Suche nach möglichen Maßnahmen

  - z.B. Suche nach geeigneten PPs

Definition der geeigneten Maßnahmen, inkl. Kosten/Nutzen-Analyse

Bedrohungsanalyse

- Welche Werte haben wir?
- Welchen Verlust bringt ihre Zerstörung (inkl. unerlaubter Veränderung)?
- Wer kann Interesse an der Zerstörung haben?
- Welche Bedrohungsszenarien können wir erwarten?
  - Wovor haben wir uns zu schützen?
  - Vor wem müssen wir uns schützen?
  - Wie wahrscheinlich ist ein Angriff?

Bedrohungsanalyse

Folgerungen

- Können wir Angriffen entgehen?
  - Infrastrukturanalyse
  - Gegenmaßnahmen möglich?
    - Welche?
    - Welchen Schaden richten sie an?
      - Isolation des Systems
      - W(rite) O(nly) M(emory)
      - Kosten
      - Schlechte Ergonomie ⇒ Umgehungstaktiken werden entwickelt

Angriffsarten

- Ausspähen
  - Daten, Kommunikationsmuster, etc.
  - Zugangskriterien (Identitäten, Passworte)
- Zerstören
- Verändern
- Einschleusen
  - Falsche Daten
  - Programme (z.B. trojanische Pferde) oder Programmteile (z.B. Viren)

Angriffsarten

- Behinderungen
  - Zugriffsverhinderungen (denial of access)
  - Diensteverhinderungen (denial of service)
  - Überladungen des Systems (system overloading)
  - Systemabstürze
  - Überladung des Netzwerks (network overloading)
  - Konzertierte Aktionen
    - e-Mail-Bomben
    - gleichzeitige Zugriffe von sehr vielen Systemen aus

Angriffsarten

Überladungen können zum Entstehen von Sicherheitslücken führen

- System kann nicht mehr alle Sicherheitsmechanismen entfalten

OCTAVE von CERT

Operationally Critical Threat, Asset, and Vulnerability Evaluation

- Beispiel für Risikoanalyse und daraus folgende Strategie für die Planung von Sicherheitstechniken
- Frei erhältlich

`http://www.cert.org/octave`

Maßnahmen-Ebenen

- Physische – Bau, Umwelt, ...
- Organisatorische
- Hardware
- Programmtechnische

Physische Maßnahmen

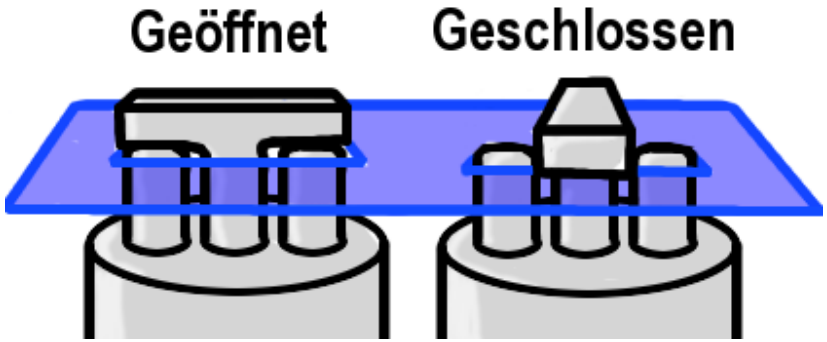
Gegen unerlaubten Zugriff auf Hardware

- Türen
- versperrbare Hardware
- versperrbare Racks
  - mit mechanischem Schloss
  - mit elektronischem Schloss
    - PIN, Karte oder Fingerabdruck (Thermopunkte)
    - ermöglicht Zutrittsprotokollierung
- Video-Überwachung

Physische Maßnahmen

Gegen Diebstahl

- versperrbare Türen
- Verankerung mit schwer- oder unbeweglichen Raumteilen oder Möbeln
- z.B. Kensington Lock



Physische Maßnahmen

Brandvorsorge

- Sprinkleranlage

Klimatisierung

- erfordert viel Fachwissen
- Reserven einplanen

Organisatorische Maßnahmen

Definition des Aufgabenbereichs von Mitarbeitern

Need-to-know-Prinzip, d.h. arbeiten mit

- minimalen Informationen
- ausreichenden Informationen

Erarbeiten eines Regelwerks

- Wer darf was womit tun?

Vermittlung des Regelwerks

- Verständlichkeit
- Verpflichtung der Mitarbeiter/Projektpartner

Organisatorische Maßnahmen

Protokollierung

- z.B. Zutritte, Aktionen im System
- Eventuell Video-Überwachung
- Abschreckung von „Übeltätern“
  - Protokolle vor Verfälschung und Zerstörung sichern ist extrem wichtig!
- Nachvollziehbarkeit
  - Insbesondere nach Auftreten von unerlaubten oder unvorhergesehenen Aktionen

Organisatorische Maßnahmen

Mitarbeiterauswahl

- Vertrauenswürdig
- Sicherheitsbewusst
- Ausgebildet
  - Schule, Universität usw.
  - Lokale Einschulung

Organisatorische Maßnahmen

Qualitätssicherung durch

- Prozessmodellierung
  - z.B. Capability Maturity Model Integration (CMMI) des Software Engineering Institute der Carnegy Mellon Universität http://www.sei.cmu.edu/cmmi
  - ISO 9000 ?? (Fragezeichen stehen für Aussagekraft der Zertifizierung)

Organisatorische Maßnahmen

8. Aufgabe:

Mehrere konkurrierende Hotels schließen schließen sich insofern zusammen, als ein Hotel, das den Zimmerwunsch eines Kunden nicht mehr erfüllen kann, diesen Wunsch an ein anderes weiter, das den Wunsch erfüllen kann.

Da jedoch Konkurrenz besteht, soll es keinem Hotel möglich sein, die Auslastung eines anderen einzusehen.

Hardware

Nur qualitativ hochstehende, verlässliche Hardware ermöglicht sicheren Betrieb

Nur hardware-unterstützte Sicherheit kann schützen

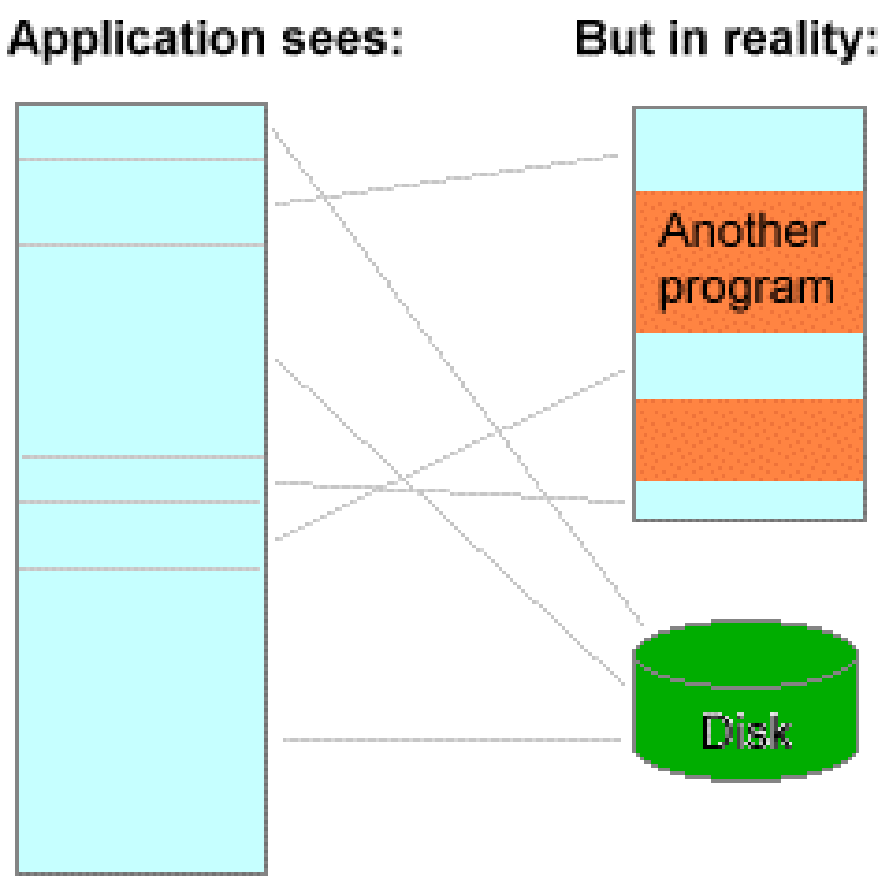
- Software allein ist zu verletzlich

Sicherheit durch Virtualisierung

Multi-User-Betriebssysteme benötigen Virtualisierung zur Sicherheit

- Für jeden Benutzerprozess
  - ein eigener virtueller Speicherraum,
  - den er nicht verlassen (überschreiten) kann.
- Virtuelle Adressen
  - werden über Systemtabellen auf reale Speicher-adressen abgebildet – kein direkter Speicherzugriff
  - kein Zugriff außerhalb des zugewiesenen virtuellen Speicherraums, da keine reale Adresse vorhanden

Dynamic Address Translation



- Einteilung des realen Speichers in gleich große Blöcke
- Zugriff auf Speicherstelle, die real innerhalb des Blocks: relativ zum Blockanfang adressiert
- Zugriff auf Speicherstelle, die real außerhalb des Blocks: Nachschlagen in Tabelle und adressieren relativ zu Blockanfang
- Reale Blöcke nicht unbedingt konsekutiv
- Reale Blöcke eventuell auf Platte ausgelagert
- Zugriff auf Adresse außerhalb des zugewiesenen virtuellen Adressraums → kein Tabelleneintrag

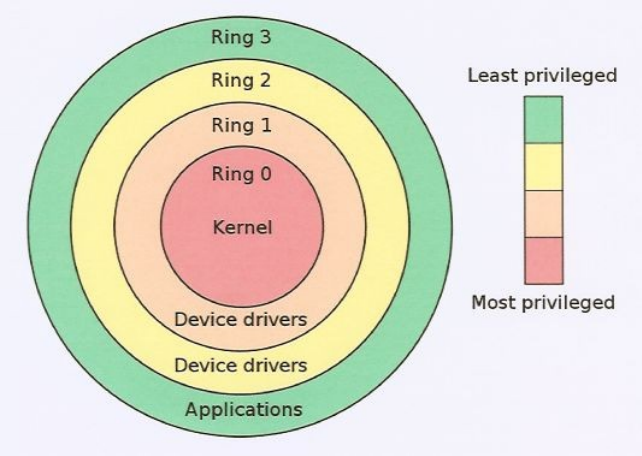
Hardware für Virtualisierung

Zugriff zum realen Speicher nur

- durch eigene Hardware (memory management)
- über Speichertabellen

Speichertabellenverwaltung durch spezielle Prozessorbefehle, die nicht allen Prozessen zur Verfügung stehen

Sicherheitsringe



- Innerer Ring mit höchsten Privilegien
- Privilegien sinken nach außen
- Informationsaustausch zwischen Ringen eingeschränkt auf vordefinierte Schnittstellen (⇔)
- x86-Architektur: Ring 0 erlaubt Ausführung von privilegierten Hardware-Befehlen
  ⇒ Kernel des Betriebssystems in Ring 0
- User-land-Prozesse laufen in Ring 3
- Linux und Windows nutzen nur Ring 0 und 3

Virtualisierung des Computers

Geht auf CTSS (Conversational Time Sharing System) zurück

- MIT, Cambridge,USA
- Ende 1950er/Anfang 1960er Jahre
- Aufteilung des Zentralrechners in „virtuelle Rechner“
- Hypervisor als Mini-Betriebssystem zur Zuteilung der Hardware zu den virtuellen Rechnern
- Portierung auf IBM/360-40, später IBM/360-67
  - Hypervisor wird CP (Control Program genannt)

Virtualisierung des Computers

1970/71 wird das Produkt von IBM unter der Bezeichnung VM (Virtual Machine) von IBM intern in ihren Labors für die Entwicklung von Betriebssystemen genutzt

Entwicklung eines schlanken, interaktiven Single-User-Betriebssystems CMS (Conversational Monitoring System) als Entwicklungsumgebung unter VM

Später VM/CMS als Produkt vermarktet

Virtualisierung des Computers

Jeder Benutzer erzeugt mit der Anmeldung einen eigenen virtuellen Rechner mit eigener Plattenumgebung

- permanenter zugeteilter Plattenbereich überlebt Abbau des virtuellen Rechners

Selbst der Absturz des Betriebssystems eines virtuellen Rechners ohne Einfluss auf andere virtuelle Rechner auf dem selben Zentralrechner

- ausgenommen, dass insgesamt mehr Rechenleistung für die weiter aktiven virtuellen Rechner bleibt

Virtualisierung des Computers

Auch bei den Kunden von IBM wurde VM zum Träger des Multi-User-Betriebssystem OS/370 und Nachfolger

Ursprünglicher Haupteinsatz: Testinstallationen neuer Betriebssystemversionen bei laufendem Betrieb

Ab 1990 z/VM auf den Rechnern der Serie Z

Virtualisierung des Computers

Ca. 1998 Versuch Unix unter VM zum Laufen zu bringen

- eher Spiellust als kommerzieller Weitblick
- jedoch erfolgreicher kommerzieller Beginn der IBM in der Unix-Welt
- Portierung unerwartet leicht

Virtualisierung des Computers

Virtualisierung durch Bereitstellung eines Teils der Hardware für die virtuellen Maschinen durch einen Hypervisor

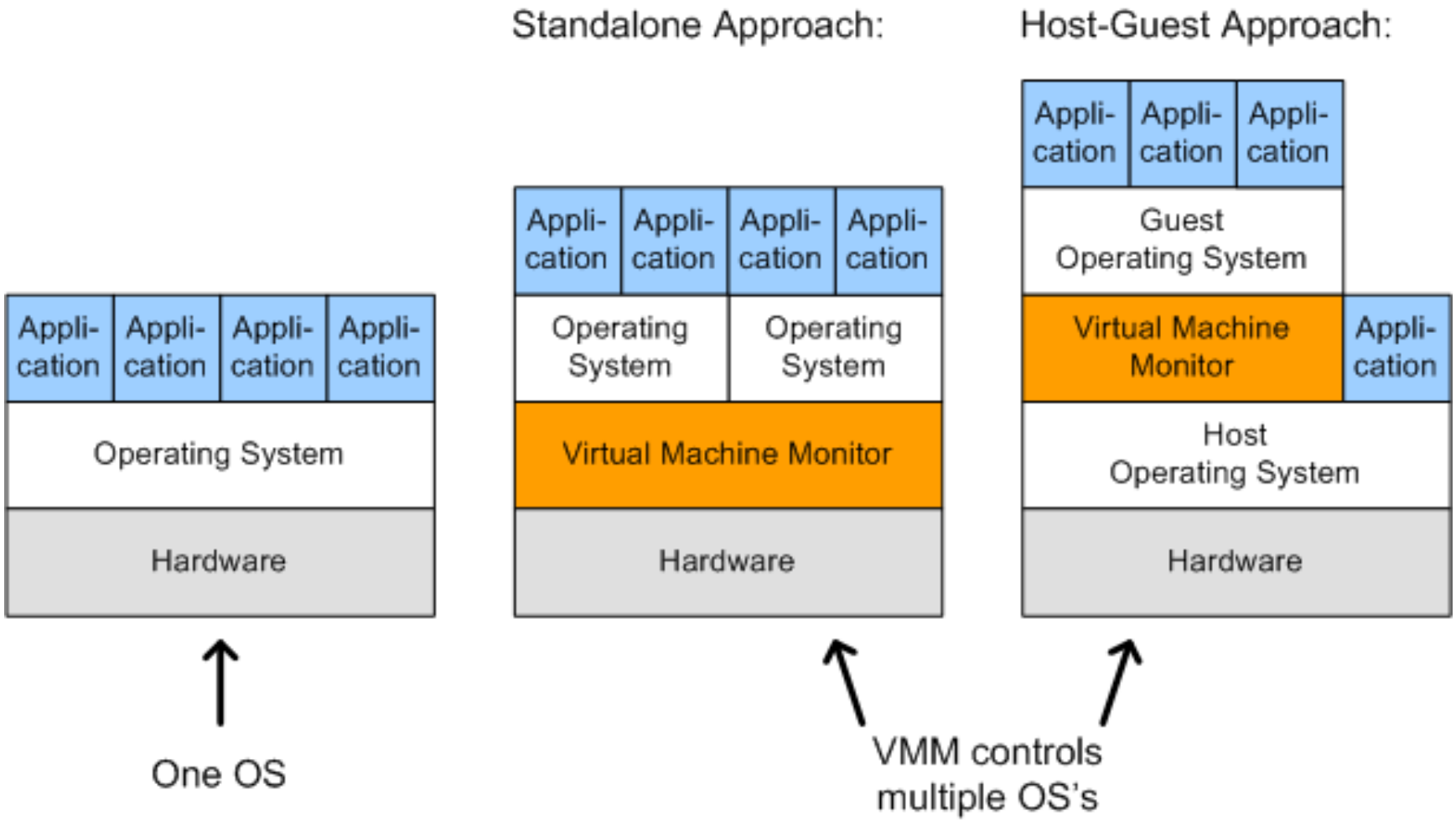
Gastsysteme teilen sich Hardware ohne voneinander zu wissen, außer dass weniger Hardware-Leistung dem einzelnen System zur Verfügung steht

Virtualisierung des Computers

Bereitsstellung als

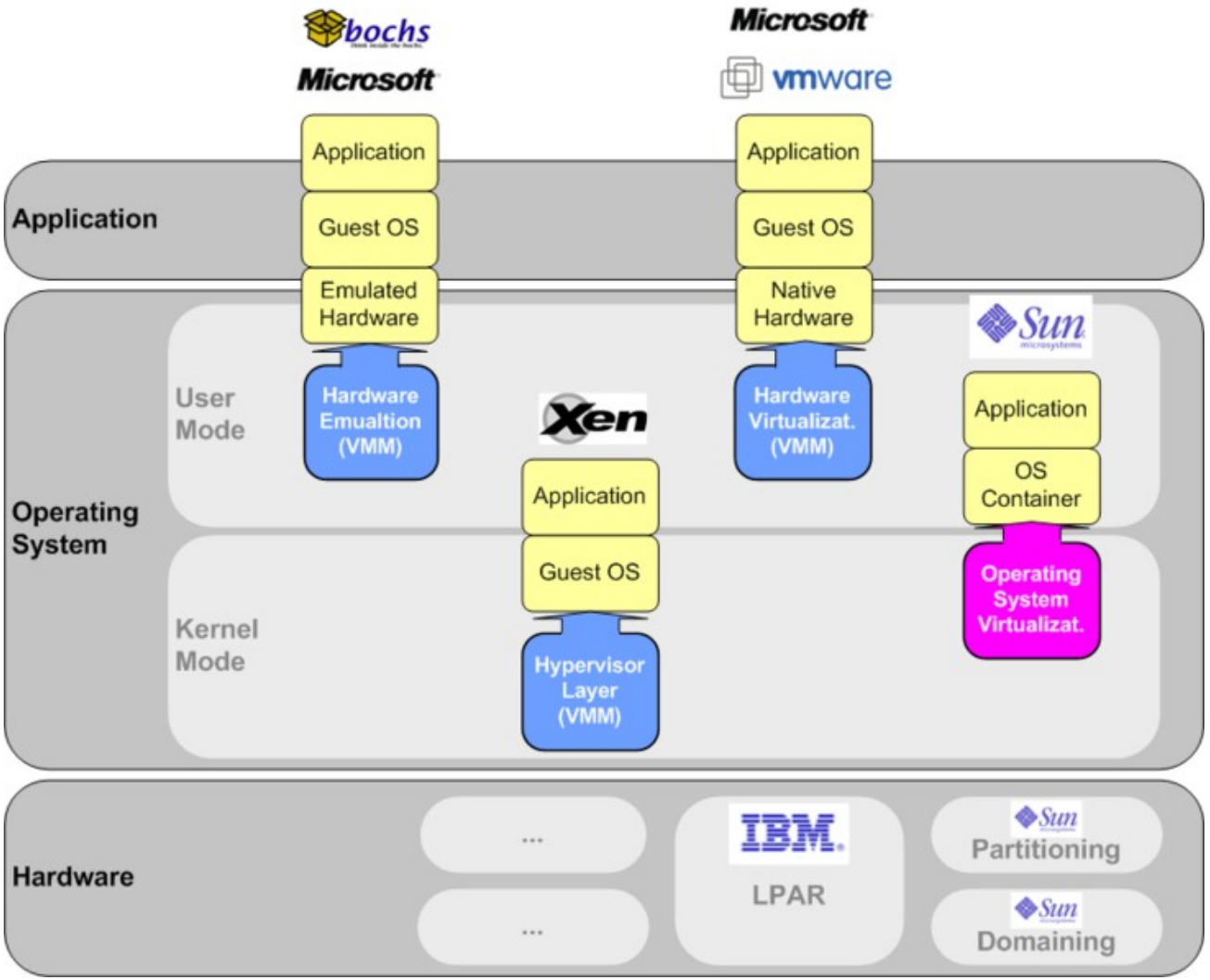
- Emulation der Hardware wie das unmodifizierte Gastsystem es benötigt
- Hardwarevirtualisation (native oder full virtualisation) – Gastsystem unverändert, jedoch für gleiche CPU wie Hardware
- Paravirtualisierung: abstrakte Hardware-Verwaltungsschicht, auf die das Gastsystem portiert werden muss
  - Virtualisierung nur wenn benötigt, sonst nativ

Virtualisierung des Computers



universität wien

Virtualisierung des Computers



Virtualisierung des Computers

Sicherheitüberlegungen

- Stand alone
  - Sicher, da keine Benutzer im Host-system
- Host-guest approach
  - Gefahr für Supervisor durch Benutzer im Host-System
  - falls sie Administrator-Privilegien erreichen

Virtualisierung - x86

Auf PC erste Entwicklungen 1998 durch Firma VMWare

- Einsatz mehrerer Betriebssysteme und Versionen gleichzeitig
  - Wirtsbetriebssystem (host operating system): Linux oder MS Windows
  - Gastsysteme (guest operating system): Linux und MS Windows, auch Intel-Mac/OS
- VMware xSphere Hypervisor (ESXi) hat eigenen Kernel (kein Trägerbetriebssystem)

Virtualisierung - x86

Bis auf die CPU sind alle virtuellen Rechner unter VMware gleich

⇒ Migration auf andere Rechner ohne großen Aufwand (wichtig für Nutzung von Ausweichrechnern)

Virtualisierung - Xen

Xen – Entwicklung der University of Cambridge, UK

Hardware wird nicht emuliert, sondern via Hypervisor dem Gastsystem zur Verfügung gestellt ⇒ sehr kleiner Overhead

- Läuft unterhalb des Betriebssystem-Kernels
- Hypervisor verteilt Betriebsmittel an Gastsysteme

Virtualisierung - Xen

- Domänen (domains) (= virtuelle Rechner)
  - privilegiert: Domäne 0 (dom0) hat volle Kontrolle über die Hardware und alle anderen Domänen
  - nicht privilegierte Domänen (domU)
    - von Domäne 0 mit Betriebsmitteln (resources) versorgt
    - können unter unterschiedlichen Betriebssystemen und deren Versionen betrieben werden
    - beeinflussen und stören einander nicht - außer Konkurrenz um Betriebsmittel

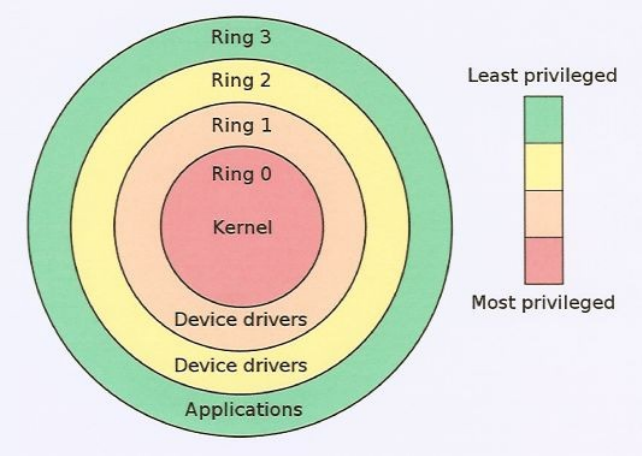
Virtualisierung - KVM

Virtualisierungs-Code im Linux-Kernel ab 2.6.20

Ladbarer Kernel-Modul kvm.ko

Benötigt Intel- oder AMD-Prozessoren mit Virtualisierungserweiterung (VT-x bzw. AMD-V)

Virtualisierung - x86



- Hypervisor in Ring 0
- Betriebssystem wandert in Ring 1
  ⇒ Anpassung des Gastsystems notwendig
- Weiterentwicklung der Hardware:
  Intel VT (Virtualization Technology)
  AMD-V (Virtualization)

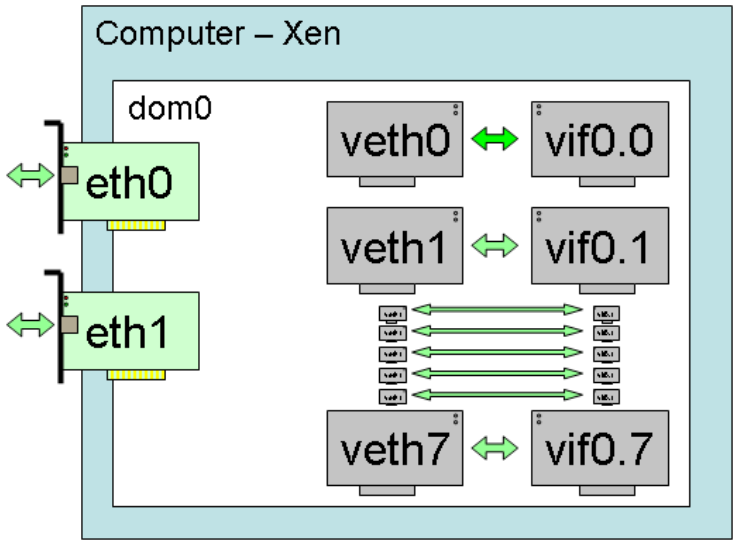
  Hardware-unterstützter Hypervisor in „Ring -1“
  ⇒ Gastsysteme weiter in Ring 0
  ⇒ Anpassung entfällt

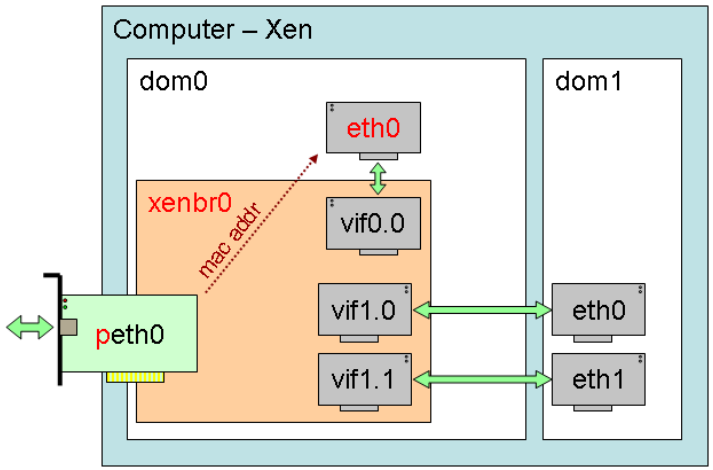
Virtualisierung - x86

Sicherheitsaspekte der Virtualisierung

- Trennung der virtuellen Rechner ab Kernel
- stabiler Gesamtbetrieb auch bei Verwendung instabiler Software in einem virtuellen Rechner
- Auftrennung von Benutzerbetrieb und Diensten in unterschiedliche virtuelle Rechner
- Gefährdete Dienste (bekannte Angriffsziele) können in eigenene virtuelle Rechner ausgelagert werden

Virtualisierung - Netzwerk





- Jede domX hat bis 7 eigene virtuelle Netzwerkkarten (Network Interface Card)
- Internes Netzwerk als bridge in dom0 ausgeführt – auch für mehr als eine physische Netzwerkkarte möglich (mehrere bridges)
- domU können öffentliche oder private IP-Adressen erhalten
- Sicherung von dom0 (via ihre ethX) ist essentiell!!!

Lokale Sicherheit

Lokale Sicherheit entscheidend beeinflusst durch:

- Qualität des Kernels und der Betriebsystem-komponenten
- Passworte, die wirklich schützen
  - Alle mit der Software gelieferten Originalpasswörter müssen sofort geändert werden (sind weltweit bekannt!!!)
- Anpassung der voreingestellten Zugriffs-berechtigungen auf Dateien an Sicherheits-richtlinie

Passwort - Kennwort

PIN – Personal Information Number

- rein numerisch (4 bis 6 Stellen üblicherweise)

Passwort/Kennwort

- meist bis zu 8 Zeichen
- Buchstaben, Ziffern, Interpunktionszeichen

Passphrase/Kennsatz

- Länger als Passwort

Passwortsicherheit

Passwort/Passphrase muss

- schwer zu erraten – für Andere
- leicht zu merken – für den Eigner

Es soll

- Groß- und Kleinbuchstaben
  - Großbuchstaben nicht (nur) am Wortanfang
- Ziffern (die eventuell Buchstaben ersetzen: z.B. 1 für l)
- Sonderzeichen

enthalten

Passwortsicherheit

Nicht leicht erratbar:

- Kein Name aus der persönlichen Umgebung
  - kann jedoch Teil eines komplexen Gebildes sein
  - kein Vorname (als einziger Bestandteil)
- Kein Begriff aus einer Cracker-Bibliothek
  - z.B. Ziffernfolge von 1 bis n (n < 9), Zeichenfolge auf einer Reihe der Tastatur
  - Überprüfen durch entsprechende Programme (z.B. CrackLib)

Zugriffsteuerung

4 Konzepte

- Ermessensbasiert DAC
- Ermächtigungsbasiert MAC
- Rollenbasiert RBAC
- Attributbasiert ABAC

Ermessensbasierte Zugriffsteuerung

Discretionary Access Control – DAC

Aus TSCEC:

„a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) to any other subject (unless restrained by mandatory access control)“

Ermessensbasierte Zugriffsteuerung

In heute üblichen Betriebssystemen:

- Zugriffsregeln zu Objekt (fast immer Datei oder Verzeichnis) vom „Eigentümer“ (owner) festgelegt
- meist 3 Subjektkreise: Eigentümer (des Objekts), Gruppe (der das Objekt zugeordnet ist), Andere
  - jeder mit eigenen Zugriffsrechten
- Zugriffsrechte:
  - Unix: lesen, schreiben (auch ändern und löschen), ausführen (Programm in Datei)
  - Windows: zusätzlich: ändern, Verzeichnisinhalt zeigen

Ermessensbasierte Zugriffsteuerung

Reicht nicht für alle Datenbankanforderungen

Ermächtigungsbasierte Zugriffsteuerung

Mandatory Access Control – MAC

aus TSCEC

"a means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity"

Ermächtigungsbasierte Zugriffsteuerung

Hochsicherheitsautorisierung

Zugriffsberechtigung

- Streng hierarchisch
  - auf Seiten des Objekts
  - auf Seiten des Subjekts/Zugriffswerbers
- Kein Ermessen des Objekteigners/Objekterstellers
- Meist zu restriktiv

Ermächtigungsbasierte Zugriffsteuerung

- Lesezugriff auf Objekte mit gleicher niedrigerer Einstufung (Read Down)
- Schreibzugriff auf Objekte mit gleicher oder höherer Einstufung (Write Up)
- Ersteller muss eventuell temporär seine Einstufung herabsetzen, um ein Objekt mit niedrigerer Einstufung zu schreiben.
- Bell und LaPadula-Modell
  http://www.albany.edu/acc/courses/ia/classics/belllapadula1.pdf

Rollenbasierte Zugriffsteuerung

Role-Based Access Control – RBAC

Größere Organisationen definieren Rechte nur für Funktionen/Rollen, nicht für Individuen

- Funktioniert auch bei Personalfluktuation
- Regelwerk bleibt bei Personalwechsel unverändert

Feinkörniger als DAC

- Ein Benutzer kann mehreren Rollen zugeteilt sein
  - zu jedem Zeitpunkt jedoch nur eine aktiv

Rollenbasierte Zugriffsteuerung

Flexibler als MAC

- Rollen können auch hierarchisch definiert werden
- Hierarchie nur in Regeln, nicht vom System erzwungen

RBAC unterstützt in

- Datenbanken
- derzeit nicht in (verbreiteten) Betriebssystemen

Attributbasierte Zugriffsteuerung

Attribute-based Access Control – ABAC

Objekte und Subjekte können Attribute haben

ABAC definiert Zugriffsrechte

- aufgrund der Attribute von Objekten und Subjekten
- durch Anwendung von Regeln

Rollen können als Attribute aufgefasst werden
⇒ ABAC kann RBAC-Regeln darstellen

Datenbanken

Datenbanken ermöglichen

- feinere Zugriffssteuerungen als Betriebssysteme
- Erzwingung der logischen Konsistenz der Informationen

Datenbanken erfordern

- Sicherstellung der Integrität (empfindlicher als sequentielle Dateien)
- aufwendigeren Sicherheitsapparat

Sicherheitsanforderungen für Datenbanken

- Physische Integrität
- Logische Integrität
- Verfügbarkeit
- Integrität der Informationselemente
- Authentifizierung
- Feinkörnige Zugriffssteuerungen
- Nachvollziehbarkeit

Physische Datenbankintegrität

- Raumsicherheit
- Redundante Rechenanlagen
- Redundante Plattenspeicher
  - RAID (Redundant Array of Independent Drives)
    - RAID 1: Spiegelung (Redundanz: ≥ 50% der Kapazität)
    - RAID 3/4: Verteilte Information, Parität auf dedizierter Platte (Flaschenhals)
    - RAID 5: Verteilte Information, Parität verteilt
    - RAID 6: wie 5 jedoch mit doppelter verteilter Parität
  - Ausfallsicherheit
    - Raid 1 – 5: 1 Platte
    - RAID 6: 2 Platten

Physische Datenbankintegrität

- Sicherung (Backup)
  - Datenbank-Software
    - ein Mal nach jeder Installation einer neuen Version
  - Datensicherung
    - regelmäßig
    - eventuell kontinuierlich
    - dislozierte Aufbewahrung

Logische Datenbankintegrität

- Schutz der Datenbankstruktur
  - korrumpierte Datenbank ist wegen der internen Vernetzung unbrauchbar
    - Gefährdung durch Plattenplatzüberlauf
      - Nicht in ein Dateisystem mit potentiell schnell wachsenden Dateien (z.B. Log-Dateien)
- Widerspruchsfreiheit
  - richtige Normalisierung wichtig
    - verhindert Widerspruch in den Daten
- Keine unvollständigen Änderungen zulassen
  - transaktionsorientiert

Schutz der Informationselemente

Schutz der Daten vor unberechtigtem Zugriff

- Nutzung der Zugriffsteuerung
  - Bewilligung zur Veränderung muss restriktiv gehandhabt werden
- Änderungen durch Datenbank überprüfen
  - Bedingungen, Plausibilität
- Änderungen protokollieren

Authentifizierung

Datenbanken haben eigene Benutzerstruktur

- keine Übernahme der Benutzeridentifizierung durch das Betriebssystem
- eigene Passwortüberprüfung
- auch Arbeitsplatz (z.B. Netzwerkadresse) kann über Zulassung entscheiden
- Einschränkung des zeitlichen Zugangs

Zugriffsteuerung in Datenbanken

- Welcher Benutzer darf
  - was sehen
  - was anlegen
  - was ändern
  - welche Regeln (neu)definieren
  - unter welcher Bedingung

  weil er es können *muss*?
- Restriktive Bewilligungen (need-to-know, need-to-do) vergeben!!!

Zugriffsteuerung in Datenbanken

- Körnigkeit der Bewilligung
  - Modul, Objekt, Tabelle, Informationselement
  - eventuell auch Werte(bereiche)
- Nutzung von Sichten (views)
  - Sichten schränken Blick (Zugriff) auf DB auf freigegebene Elemente ein
  - Sichten auf Ebene von Rollen oder Benutzer, eventuell sogar Arbeitsplatzadresse

Verfügbarkeit der Datenbank

Bei allen Sicherheitsüberlegungen:

eine Datenbank muss für erlaubte Zugriffe erreichbar sein!!!

- kein WOM (write-only memory)

Wegen der guten Sicherheitseinrichtungen von Datenbanken

- Angriffe meist über das Betriebsystem
- oder das Netz, z.B. durch Blockadeangriffe(Denial of Service, DoS)

Nachvollziehbarkeit

Nachvollziehbarkeit durch Protokollieren

- aller Änderungen der Zugriffsregeln
- aller Zugriffe auf Daten
  - welche Zugriffe
    - nur Änderungen oder auch Lesezugriffe?
  - welche Granularität?
  - wann?
  - von wo aus?

Angriffe über das Netz

Größte Gefahr für Computer-Systeme kommt aus dem Netz

- Zerstörung von Daten und Programmen
- Ausspähen
- Verfälschen von Informationen
- Blockieren von
  - Zugang zu Systemen
  - Systemen selbst (auch für lokalen Zugriff)

Maßnahmen

- Viren-/Trojaner-Scanner
  - Überprüfen beim Übertragen von Dateien
    - Verhindern des Abspeicherns
  - Überprüfen gespeicherter Dateien
  - Bereinigen
    - vor der ersten Ausführung
    - bei Infektion, wenn es noch geht
- Firewall

Internet-Protokoll

Zunächst einige Begriffe

- IP-Adresse
  - IP – Internet Protocol
  - Adressierung von Rechnern im Internet
  - IPv4 – Version 4
    - 32bit Adressen
    - übliche Darstellung
      - **4 mal 8 Bit**
      - **4 Dezimalzahlen 0 bis 255, getrennt durch Punkt**
    - bald zu kleiner Adressraum

Internet-Protokoll

- IP-Adresse
  - IPv6 – Version 6
    - 128bit Adressen
    - übliche Darstellung
      - **8 mal 16 Bit**
      - **8 Hexadezimalzahlen, getrennt durch Doppelpunkt**
    - Adressraum größer als je denkbar benötigt
  - Adressblöcke von zentraler Stelle (IANA) vergeben
    - IANA – Internet Assigned Numbers Authority
    - Endbenutzer erhalten IP-Adressen von
      - **ISP (Internet Service Provider) oder**
      - **übergeordneter RIR (Regional Internet Registry)**

Internet-Protokoll

- Netzwerkadressenunterteilung (IPv4 und IPv6)
  - CIDR – Classless Inter-Domain Routing
    - Führende Stellen: Netzwerk
    - Hintere Stellen: Host
  - Aufteilung durch Netzwerkmaske
    - VLSM – variable-length subnet masking
    - 32 bit Maske (für AND-Verknüpfung)
    - Netzwerkteil (führend): alle Bits 1
    - Host-Teil (hinten): alle Bits 0
  - CIDR-Schreibweise
    - A.B.C.D/n
    - n: Anzahl der Netzwerk-Bits (prefix)

Internet-Protokoll

- Öffentliche IP-Adressen
  - von überall im Internet ansprechbar
  - weltweit eindeutig
  - von RIR oder ISP vergeben

Internet-Protokoll

- Private IP-Adressen (IPV4)
  - nur im lokalen LAN (Local Area Network) bekannt
  - nicht weltweit eindeutig
  - frei verfügbar
  - Adressbereiche
    - 192.168.0.0 – 192.168.255.255 oder 192.168.0.0/16
    - 172.16.0.0 – 172.16.255.255 oder 172.16.0.0/16
    - 10.0.0.0 – 10.255.255.255 oder 10.0.0.0/8
- Insgesamt 588.513.792 reservierte Adressen in 11 Blöcken

Ports

Ports sind Schnittstelle zu Prozessen

- 16bit Zahl (0 – 65.535)
- Ports 0 bis 1.023
  - Öffnen für eingehende Verbindungen nur Administrator
  - Definition der Zuordnung durch IANA
- Ports 1.024 bis 49.151
  - Definition der Zuordnung durch IANA
- Ports 49.152 bis 65.535
  - nicht bei IANA registrierbar

Ports

- Server-seitiger Port fix
- Client-seitiger Port oft variabel ⇒ p > 49.151

- Port forwarding
  - Kommunikation zu einem bestimmten Port wird auf andern Rechner umgeleitet

- Port Scan
  - eine Art des Angriffs auf Server
  - Suche nach verwundaren Dienstprogrammen

Firewall

Sicherheitskomponente gegen Angriffe über das Netz

- Hardware-Komponenten
  - Router
    - Kopplung von Rechnernetzen
    - Weiterleitung von Datenpaketen zwischen Netzsegmenten
    - eventuell Zieladresse modifizieren
  - Rechner mit Weiterleit(Routing)-Funktionen
- Software-Komponenten
  - Regelwerk
  - Erzwinger der Regeln

Firewall

Firewall teilt das Datennetz in 3 Bereiche:

- externes Netz (Internet) – vor der Firewall
  - freier Netzwerkverkehr
  - ungeschützt
- internes Netz – hinter der Firewall
  - geschützt durch Firewall-Regeln
  - kein Zugang von außen initiierbar
  - Datenverkehr mit externem Netz nur von innerhalb des internen Netzes ausgehend

Firewall

- Demilitarisierte Zone (demilitarized zone – DMZ) – hinter der Firewall
  - kann auch vom externen Netz angesprochen werden
  - welche Datenpakete in welche Richtung weitergeleitet werden, bestimmen die Firewall-Regeln

Firewall-Konzept ist Teil der Sicherheitsrichtlinie

Firewall

Netzwerk-Firewall

- Überprüft Datenverkehr zwischen Netzwerk-segmenten (Ziel: Schadensvermeidung)
  - Externes Netz – meist Weitwegenetz (WAN – Wide Area Network) – nicht vertrauenswürdig
  - Internes Netz (LAN – Local Area Network – oder WLAN – Wireless LAN) – vertrauenswürdig
  - DMZ – Demilitarized Zone – Dienste für externes und internes Netz

Firewall

Personal Firewall

- am zu schützenden Rechner installiert
- überwacht nicht Verkehr zwischen Netzen
- kontrolliert nur Datenverkehr zu Programmen im Rechner

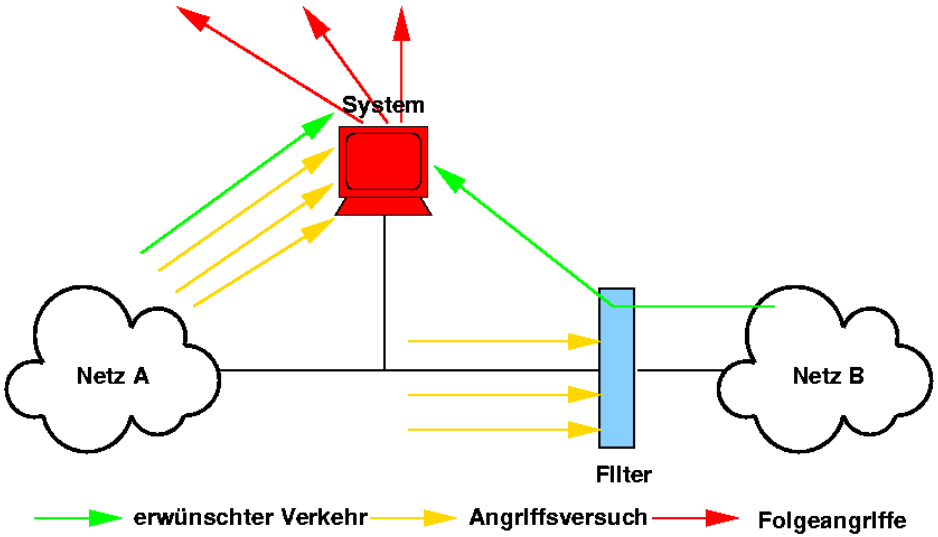
Firewall

Server vor Firewall

- ungeschützt
- kann zu Folgeangriffen genutzt werden

Internes Netz B

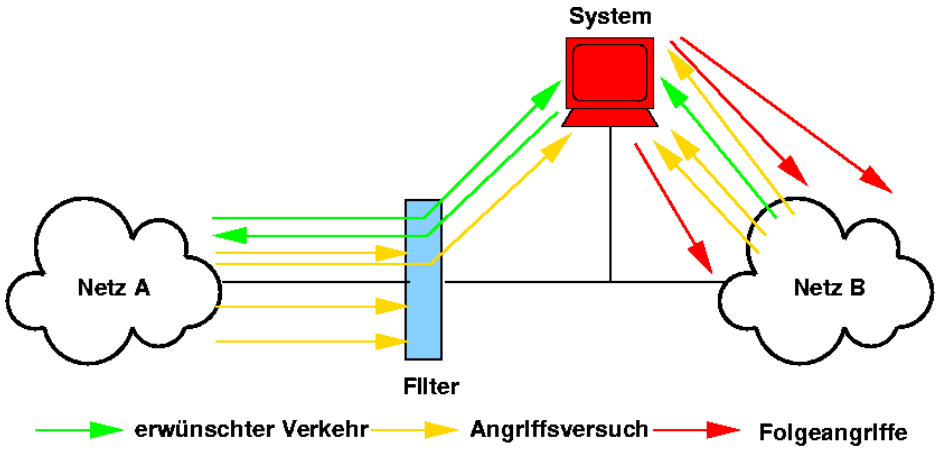
- geschützt



Firewall

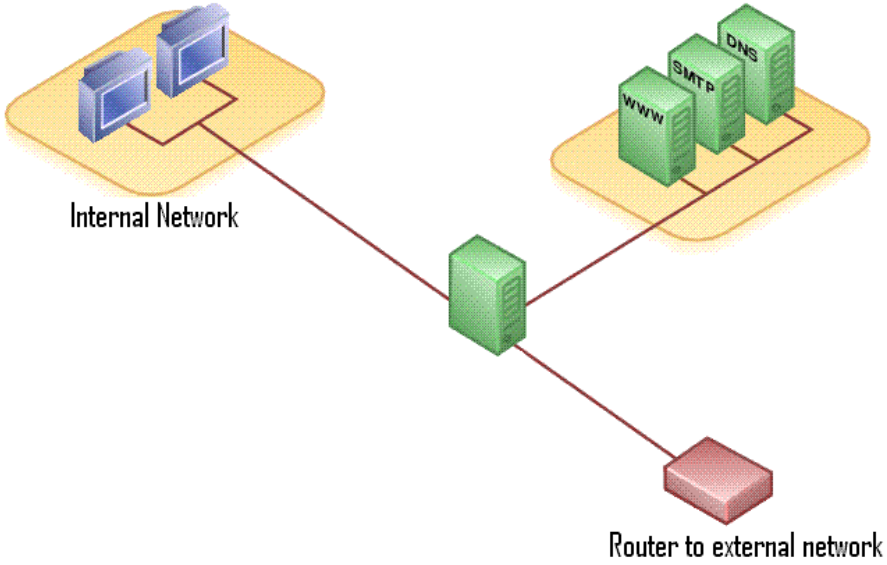
Server und internes Netz

- vor meisten Angriffen geschützt
- kein Schutz vor Angriffen über Server-Dienste

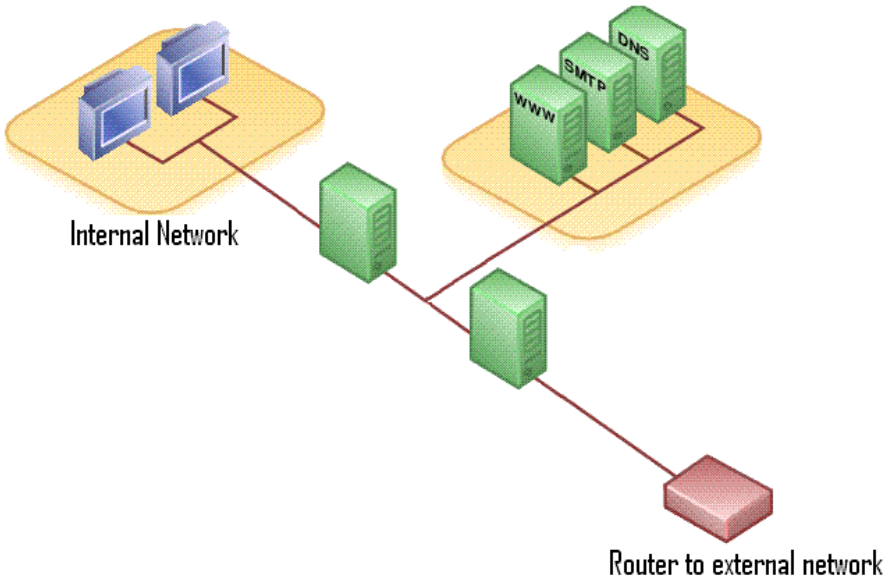


Firewall

Einstufiges Firewall-Konzept



Firewall

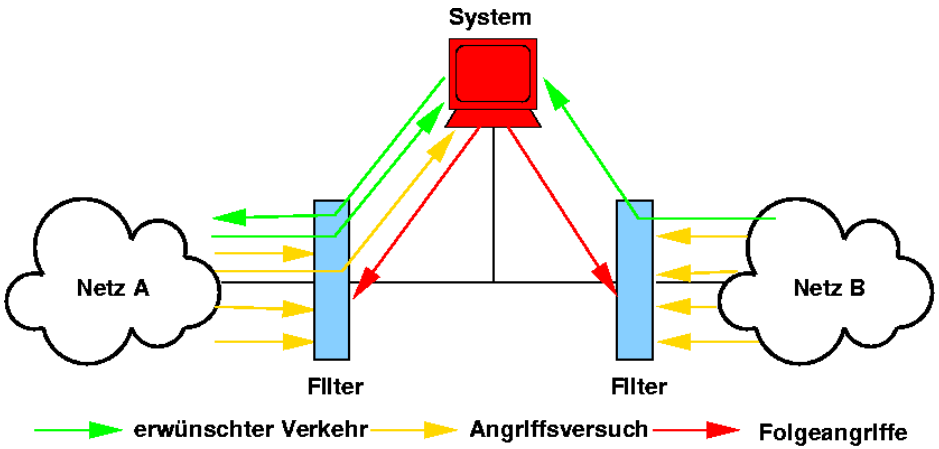


Zweistufiges Firewall-Konzept

Perimeternetz als DMZ

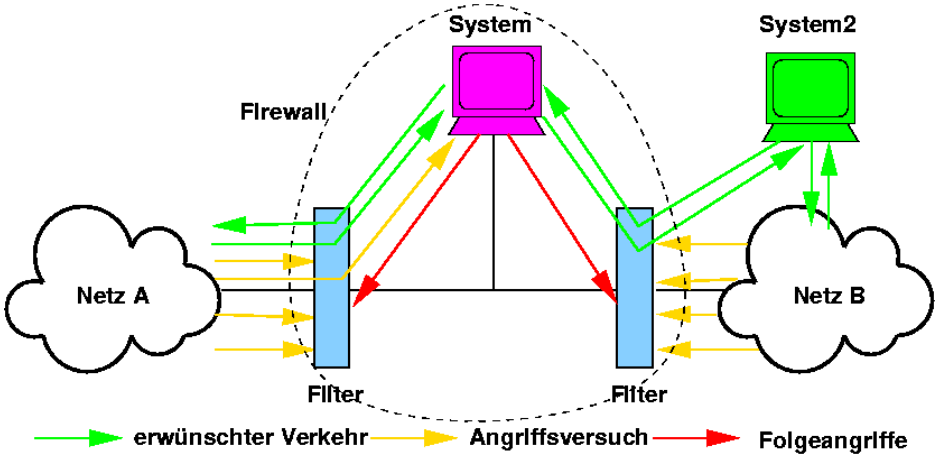
- zwischen 2 Routern
- Optimal: Router von unterschiedlichen Marken
  - nicht gleiche potentielle Sicherheitslücken

Firewall



- Folgeangriffe über kompromittierten Server blockiert
- Eventuell auch Dienste für internes Netz nicht verfügbar

Firewall



System 2

- Dienste wie System nur für internes Netz
- Dienste nach außen gehen über System
- Bei Kompromittierung von System in DMZ stehen Dienste innerhalb des internen Netzes sicher zur Verfügung

Firewall

Paketfilter

- überprüft und steuert Weiterleitung von Datenpaketen anhand der IP-Adressen und Ports von Quelle und Ziel der einzelnen Pakete

Stateful Packet Inspection

- überprüft paketübergreifend
- erkennt logische Datenströme

Firewall

Network Address Translation – NAT

- auch Masquerading genannt
- IP-Adressen werden automatisch und transparent durch andere ersetzt
- alle Systeme des internen Netzes haben nach außen eine gemeinsame IP-Adresse
- auch Systeme in Netzen mit privaten IP-Adressen können in externes Netz kommunizieren (z.B. Cluster)

Network Address Port Translation – NAPT

- Auch Port-Adressen umgesetzt

Virtuelles Privates Netz

Virtual private network – VPN

Problem:

Lokale Netzwerke können gut abgesichert werden

Kein Zugang von Rechnern über das Internet in das abgesicherte Netz

Wunsch:

Zugriff auf Betriebsmittel wie für Rechner im LAN, aber nur für Berechtigte

Virtuelles Privates Netz

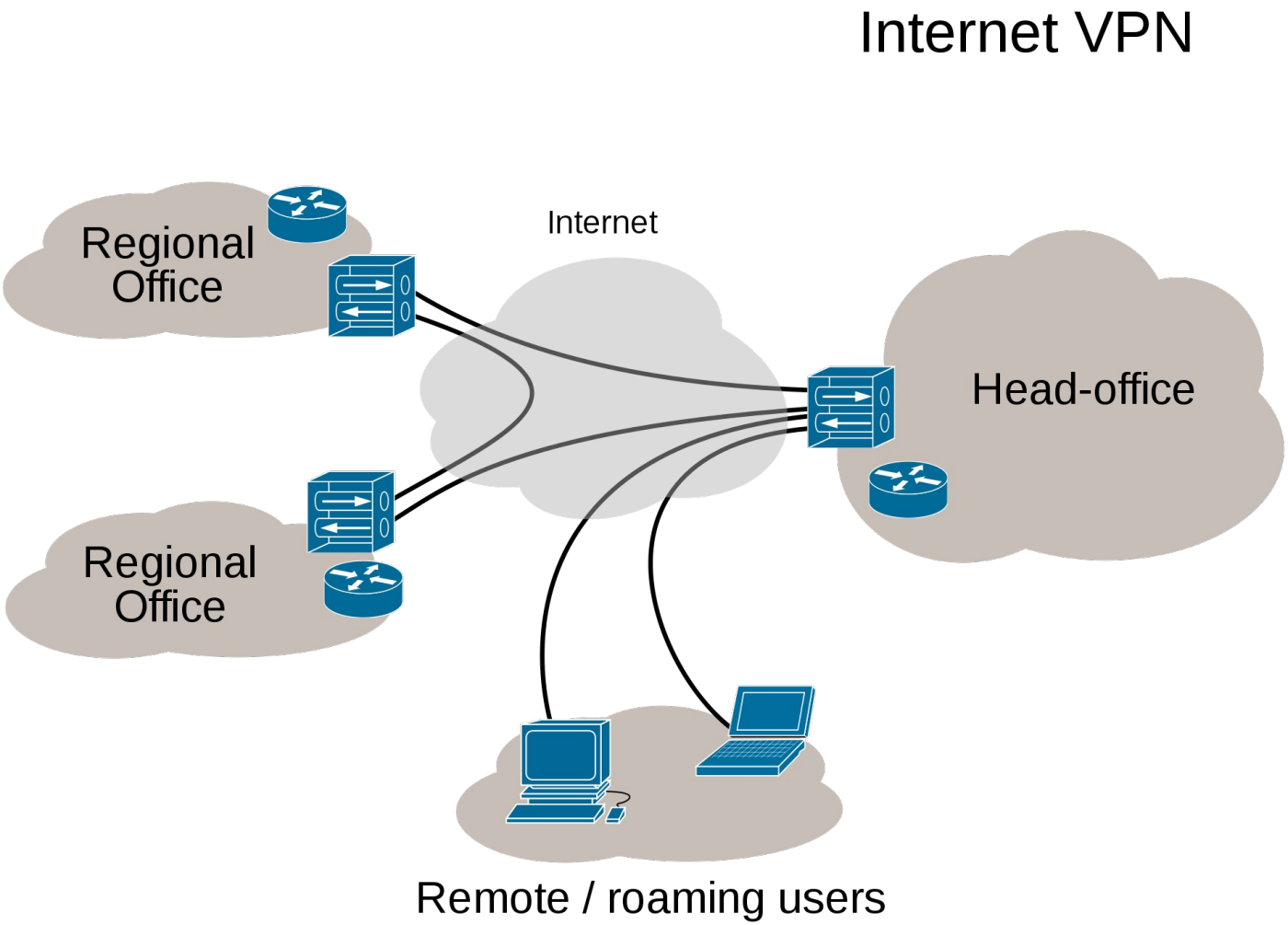
Anwendungen:

Organisationen, die über mehrere Standorte verteilt sind, die über Internet verbunden sind

Mobile Mitarbeiter, die mit ihren Mobilen Rechnern oder Smartphones auf Informationen im Organisationsnetz zugreifen müssen

Mitarbeiter, die von zu Hause aus Zugriff auf das Organisationsnetz benötigen

Virtuelles Privates Netz



Virtuelles Privates Netz

Anmeldung an VPN-Server, der die Zugriffsberechtigungen prüft

Aufbau eines „Tunnels“, in dem der entfernte Rechner eine „lokale Adresse“ bekommt ⇒ VPN

Datenpakete des VPN werden in Datenpakete des realen Netzes verpackt

Vertraulichkeit der Kommunikation durch verschlüsselung der Daten im Tunnel

Kryptographie

Sichere Datenkommunikation benötigt

- Abhörsicherheit
- Schutz vor Manipulation der Datenpakete

Zur Erfüllung beider Forderungen wird Kryptographie (Verschlüsselung) eingesetzt.

Kryptographie

Literatur

Populärwissenschaftlich und sehr gut:

Simon Singh, The Code Book, The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 1999

Der Klassiker:

Bruce Schneier, Applied Cryptography, Second Edition, 1996

Kryptographie

Literatur

Douglas R. Stinson, Cryptography: Theory and Practice, Second edition, 2002

Kryptographie

Verschlüsselung

- Ersetzt
  - Originaltext – auch Klartext (plaintext) genannt –
  - durch unverständlichen Geheimtext (ciphertext),
  - die eineindeutig abbildbar sind
- hat 2 Komponenten
  - Algorithmus – heute meist nicht geheim
  - Schlüssel für den Algorithmus – zumindest teilweise geheim

Kryptographie

Verschlüsselung

- Mechanisch
- Skytala

Kryptographie

Verschlüsselung

- elektromechanisch
  - z.B. Enigma

Kryptographie

Verschlüsselung

$(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$

- Algorithmisch

$K \in \mathcal{K}$

- Erfordert entsprechende Rechenleistung

$e_k \in \mathcal{E}$

$d_k \in \mathcal{D}$

- Erst durch Computer möglich

$e_k : \mathcal{P} \rightarrow \mathcal{C}$

$d_k : \mathcal{C} \rightarrow \mathcal{P}$

$d_k(e_k(x)) = x \quad \forall x \in \mathcal{P}$

Kryptosysteme

Kryptosystem: $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$

Schlüsselraum: $K \in \mathcal{K}$

Menge der Klartexte: $\mathcal{P}$

Menge der Geheimtexte: $\mathcal{C}$

Menge der Verschlüsselungsfunktionen: $e_K \in \mathcal{E}$

Menge der Entschlüsselungsfunktionen: $d_K \in \mathcal{D}$

Verschlüsselungsfunktion (Chiffre): $e_K : \mathcal{P} \rightarrow \mathcal{C}$

Entschlüsselungsfunktion: $d_K : \mathcal{C} \rightarrow \mathcal{P}$

Umkehrbarkeit: $d_K(e_K(x)) = x \quad \forall x \in \mathcal{P}$

Beispiele

Verschiebechiffre (z.B. Cäsar-Chiffre)

- e(x) : x + k (mod n) n ... Alphabetlänge

Vigenère Chiffre

- e(x) : $x_i + k_i$ (mod n)

Affine Chiffre

- e(x) : ax + k (mod n)

Vigenère-Quadrat

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Kryptanalyse

Kryptanalyse: Versuch der Entschlüsselung ohne Kenntnis von Schlüssel und/oder Algorithmus

- heute nur mehr Suche nach Schlüssel – Algorithmus meist offengelegt

Brute-Force

- alle Schlüssel durchprobieren
- Erfolg hängt von Geschwindigkeit der Versuchsdurchführung ab

Kryptanalyse

Statistische Methoden

- Sprachabhängige Wahrscheinlichkeitsverteilung von
  - Buchstaben
  - Buchstabenkombinationen
  - Abwehr: Verschlüsselung größerer Buchstabenfolgen als „ein Zeichen“ → Buchstabenmuster entspricht nicht mehr dem der Sprache des Klartextes

Sprach- und Kontextabhängige Methoden

- wahrscheinliche Klartextinhalte

Kryptologie - Kryptanalyse

Ziel der Kryptologie

- Finden sicherer Algorithmen und Schlüsselräume

Kryptanalyse

- Präventiv: Erkennen von Schwachstellen und „unsicheren“ Schlüsselteilräumen
- Destruktiv: Entschlüsseln ohne Schlüsselkenntnis

Schlüsselverteilung

Problem:

- Sichere Schlüsselverteilung
  - abhörsicher (nur an berechtigte Empfänger)
  - verfälschungssicher
    - Gefahr der Man-in-the-middle-Attacke

Nur über sichere Kanäle

Pro Kommunikationspaar ein Schlüssel

- Frage: wie viele werden für ***n*** Teilnehmer benötigt?

Man-in-the-middle-Attacke

Alice schickt Nachricht an Bob

Eve

- fängt Nachricht ab
- verschickt andere Nachricht an Bob,
- Bob erkennt Veränderung nicht,
- verändert Bobs Antwort so, dass Alice nicht merkt, dass ihre Nachricht Bob nicht erreicht hat

Man-in-the-middle-Attacke

Im Falle von Verschlüsselung:

- Eve fängt Schlüssel von Alice ab,
- schickt Bob ihren eigenen Schlüssel
- Entschlüsselt Alices Nachricht und
- Verschlüsselt sie mit Schlüssel ihrer Kommunikation mit Bob

Symmetrie

Symmetrische Verfahren

- Ver- und Entschlüsselung verwenden gleichen geheimen Schlüssel oder 2 Schlüssel, sich voneinander ableiten lassen
- analog zum mechanischen Schloss
  - gleiches Profil schließt und öffnet
- seit Beginn der Kryptographie verwendet
- bis 1976 einzige (denkbare) mögliche Methode

Symmetrie

Asymmetrische Verfahren

- Schlüssel sind verschieden,
- aber gekoppelt
- längste Zeit nicht denkbar

Sichere Schlüsselvereinbarung

Sichere Schlüsselvereinbarung über unsicheren Kanal:

Whitfield Diffie und Martin Hellman, New Directions in Cryptography, IEEE Transactions in Information Theory, 22 (6), 644-654, November 1976

http://www-ee.stanford.edu/~hellman/publications/24.pdf

Sichere Schlüsselvereinbarung

Mechanisches Analogon:

Alice hat 2 gleiche Schlüssel

Alice steckt einen Schlüssel in Kästchen, das sie mit Vorhängschloss verschließt und sendet es Bob

Bob hängt sein Vorhängschloss daran und schickt es an Alice zurück

Alice nimmt ihr Schloss ab und schickt Kästchen an Bob

Bob öffnet Kästchen und entnimmt den Schlüssel

Jetzt kann unter Nutzung eines Vorhängschlosses, zu dem nun beide einen Schlüssel haben, vertraulich kommuniziert werden.

Sichere Schlüsselvereinbarung

Aufgabe:

Formulieren Sie mathematisch, warum eine algorithmische Verallgemeinerung des mechanischen Analogons für eine sichere Schlüsselvereinbarung im Allgemeinen nicht funktioniert.

Welche mathematische Eigenschaft macht das mechanische Analogon möglich?

Sichere Schlüsselvereinbarung

Problem:

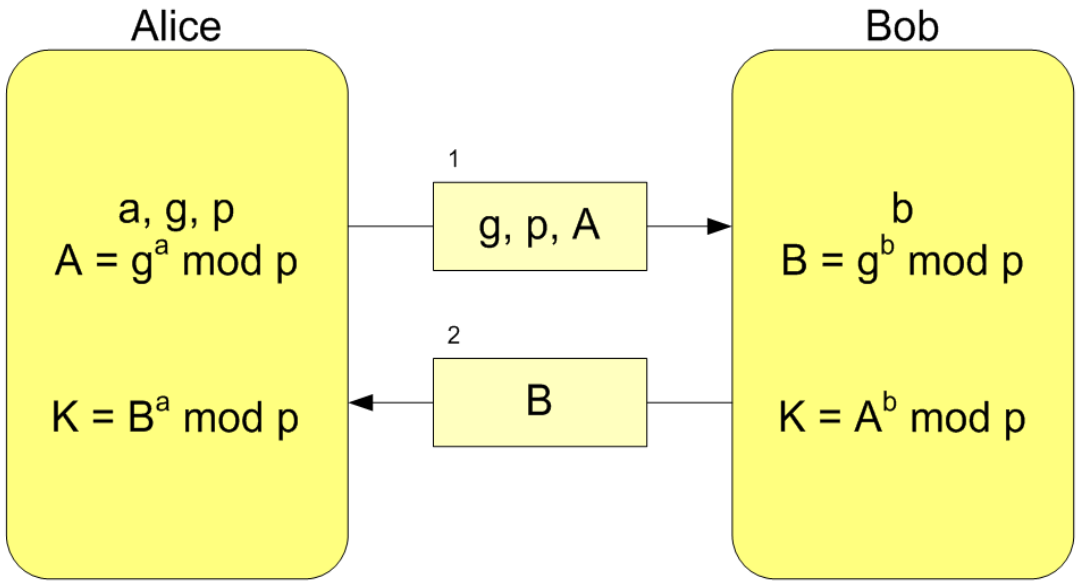
Mechanisch: Reihenfolge bei Entschlüsselung unerheblich

Algorithmisch: meist kommt es auf die Reihenfolge der Schritte an (nicht kommutativ)

Benötigt: Schlüssel über kommutative Funktion erreichbar

Diffie-Hellman-Merkle-Algorithmus zur Schlüsselvereinbarung 1976 veröffentlicht

Diffie-Hellman-Merkle-Algorithmus



$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

p Primzahl $2 \leq g \leq p-2$ $a,b,g \in \mathbb{Z}$ A, B öffentliche Schlüssel K geheimer Schlüssel

g,p,A,B über unsicheren Kanal austauschbar

Kommuntative Eigenschaft: $g^{ab} \bmod p \equiv g^{ba} \bmod p$

Geheimnis: Problem g^{ab} oder a und b zu finden, wenn g^a und g^b bekannt

Problem der Berechnung der diskreten Logarithmen a und b

Diffie-Hellman-Merkle-Algorithmus

Diffie-Hellman-Merkle vereinbart asymmetrisch

- geheimen Schlüssel für symmetrische Verschlüsselung
- für laufende Kommunikationssitzung

Nicht gegen Man-in-the-middle-Attacken geschützt

- zusätzliche Authentifizierung benötigt

Diffie-Hellman-Merkle-Algorithmus

Aufgabe:

Durch das Sammeln genügend großer Mengen an verschlüsselten Informationen während langer Sitzungsdauern kann mittels geeigneter kryptanalytischer Verfahren der geheime Schlüssel enttarnt werden (abhängig vom Verschlüsselungsalgoritmus und der Schlüssellänge).

Was muss man tun, um die Verschlüsselung längerer Kommunikations-sitzungen sicher zu gestalten?

Symmetrische Kryptosysteme

Mehrere Verfahren bekannt

- Einige haben sich als nicht sicher genug erwiesen
- Verbreitete Verfahren - FIPS-Normen
  - DES – IBM-Entwicklung: LUCIFER
    - 64 Bit davon 56 Bit Schlüssel
  - 3DES DES 3mal angewandt
  - AES Advanced Encryption Standard (Rijndael)
    - Nachfolger von DES als NIST-Norm (USA)
    - Block- und Schlüssellängen: 128, 192, 256
    - Keine erfolgreichen Attacken bisher gefunden

Symmetrische Kryptosysteme

- Patentiertes Verfahren (bis 2011)
  - IDEA International Data Encryption Algorithm
  - Patent galt auch in Österreich

Kryptographie mit öffentlichen Schlüsseln

Ronald L. **R**ivest, Adi **S**hamir, Leonard **A**dleman
1978

RSA-Algorithmus

- basiert auf Problem der Faktorisierung der Produkte großer Primzahlen

RSA-Algorithmus

p, q Primzahlen, $N = p \cdot q$

Eulersche φ-Funktion: $\varphi(N) = (p-1) \cdot (q-1)$

wähle $1<e<\varphi(N)$ ggT$(e,\varphi(N))=1$ d.h. e, φ(N) teilerfremd

berechne d: $e \cdot d \equiv 1 \pmod{\varphi(N)}$

Verschlüsseln: $C \equiv K^e \pmod{N}$

Entschlüsseln: $K \equiv C^d \pmod{N}$

e, N bilden öffentlichen Schlüssel

d, N bilden privaten Schlüssel

RSA-Algorithmus

Damit d nicht von e und N ausgehend leicht (schnell) berechnet werden kann,

- müssen p und q
  - unbekannt bleiben,
  - große Primzahlen (weitere Eigenschaften?) sein
  - nicht nahe beieinander liegen, um eine effiziente Fermat-Faktorisierung zu verhindern.
- darf e eine effiziente Exponentiation erlauben
  - kurze Bit-Länge, wenige 1-Bits
- aber nicht zu klein sein
  - 3 ist schlecht, 0x10001 = 65537 ist gut
  -

Asymmetrische Verschlüsselung

Daten mit öffentlichem Schlüssel des Leseberechtigten verschlüsseln

- Nur er kann mit seinem geheimen Schlüssel entschlüsseln
- Nur ein Schlüsselpaar für Kommunikation Aller mit einem Empfänger notwendig
  - n Schlüsselpaare für Gruppe von n Teilnehmern
  - statt $O(n^2)$ wie bei symmetrischer Verschlüsselung

Asymmetrische Verschlüsselung

Herstellung eines Teils des Schlüsselpaares bei Kenntnis des anderen zu aufwendig, daher

- Verlust des einen ⇒ Verlust des Paares
- Öffentlichen Schlüssel verteilen oder auf System mit regelmäßiger Datensicherung übertragen
- Kryptosysteme, die zur effizienten Entschlüsselung p und q (und daraus abgeleitete Werten) gemeinsam mit dem privaten Schlüssel nach PKCS#1-Norm abspeichern (openSSL, Java, .Net), ermöglichen die Rekonstruktion des öffentlichen Schlüssels aus dem privaten – kein Sicherheitsproblem.

RSA Privater Schlüssel

```
RSAPrivateKey ::= SEQUENCE {
    version           Version,
    modulus             INTEGER,  -- n
    publicExponent    INTEGER,  -- e
    privateExponent   INTEGER,  -- d
    prime1            INTEGER,  -- p
    prime2            INTEGER,  -- q
    exponent1           INTEGER,  -- d mod (p-1)
    exponent2           INTEGER,  -- d mod (q-1)
    coefficient       INTEGER,  -- (inverse of q) mod p
    otherPrimeInfos   OtherPrimeInfos OPTIONAL
}
```

Asymmetrische Verschlüsselung

Sichere Verwahrung des privaten Schlüssels

- äußerste Vorsicht vor Verlust
- nur Besitzer zugänglich
- Zugriffsberechtigung: nur für Eigner und nur lesend
- privaten Schlüssel nur verschlüsselt aufbewahren
- am besten immer bei sich haben

Asymmetrische Verschlüsselung

Nachteil

- Verschlüsselung ca. 1000mal rechen-aufwendiger als symmetrische Verschlüsselung

⇒ hybride Verfahren:

  - symmetrische Verschlüsselung der Daten
  - asymmetrische Verschlüsselung des Schlüssels der symmetrischen Verschlüsselung mit öffentlichem Schlüssel des berechtigten Lesers der Daten
    - Schlüssel meist viel kürzer als Datensatz
  - Mitabspeichern des verschlüsselten Schlüssels

Asymmetrische Kryptosysteme

Gebräuchliche asymmetrische Verfahren

- DSA
- RSA
  - RSA-Norm PKCS#1 (Public Key Cryptography Standard)
  - RFC 3447 der IETF (Internet Engineering Task Force)
- ElGamal
- Elliptische Kurven

Verteilung des öffentlichen Schlüssels

Öffentlicher Schlüssel publizierbar

- über unsichere Kanäle
- im Internet

Problem

- gesicherte Zuordnung zu Benutzer/System
- Identifizierung des legitimen Besitzers des privaten Schlüssels

Identifizierung des Schlüsseleigners

Verteilung des öffentlichen Schlüssels problemlos

Jedoch: Wer ist der rechtmäßige Besitzer des privaten Schlüssels?

Identifizierung des Eigners:

- Web of Trust oder
- X.509 PKI (Public Key Infrastructure)

Web of Trust

Basiert auf kryptographischen Schlüsseln nach openPGP (z.B. GnuPG)

- Zuordnung zu Eigner in „Zertifikat“ mit
  - öffentlichem Schlüssel
  - Namen und e-Mail-Adresse(n) des Eigners
- Zertifikat kann in öffentlichen Server geladen werden
- Zertifikat kann nicht gelöscht werden, nur widerrufen
- Zertifikat kann vom Eigner widerrufen werden (revocation), z.B. bei Verlust des privaten Schlüssels
  - privater Schlüssel benötigt
  - sollte gleich erstellt werden (nicht veröffentlicht)

Web of Trust

Netzwerk aufgebaut auf Vertrauen

A bestätigt, dass der öffentliche Schlüssel S_B ***B*** gehört, da

- ***B*** es ihm bestätigt hat, z.B. durch telefonische Durchgabe einer „Kurzfassung“ (fingerprint) oder durch persönliche Übergabe (auf Floppy oder CD)
- und eventuell zusätzlich ***B*** eine von ***A*** mit S_B verschlüsselte Nachricht entschlüsselt oder ihm eine signierte Nachricht zukommen lässt.

Bestätigung: „Zertifikat“ wird unterschrieben

Web of Trust

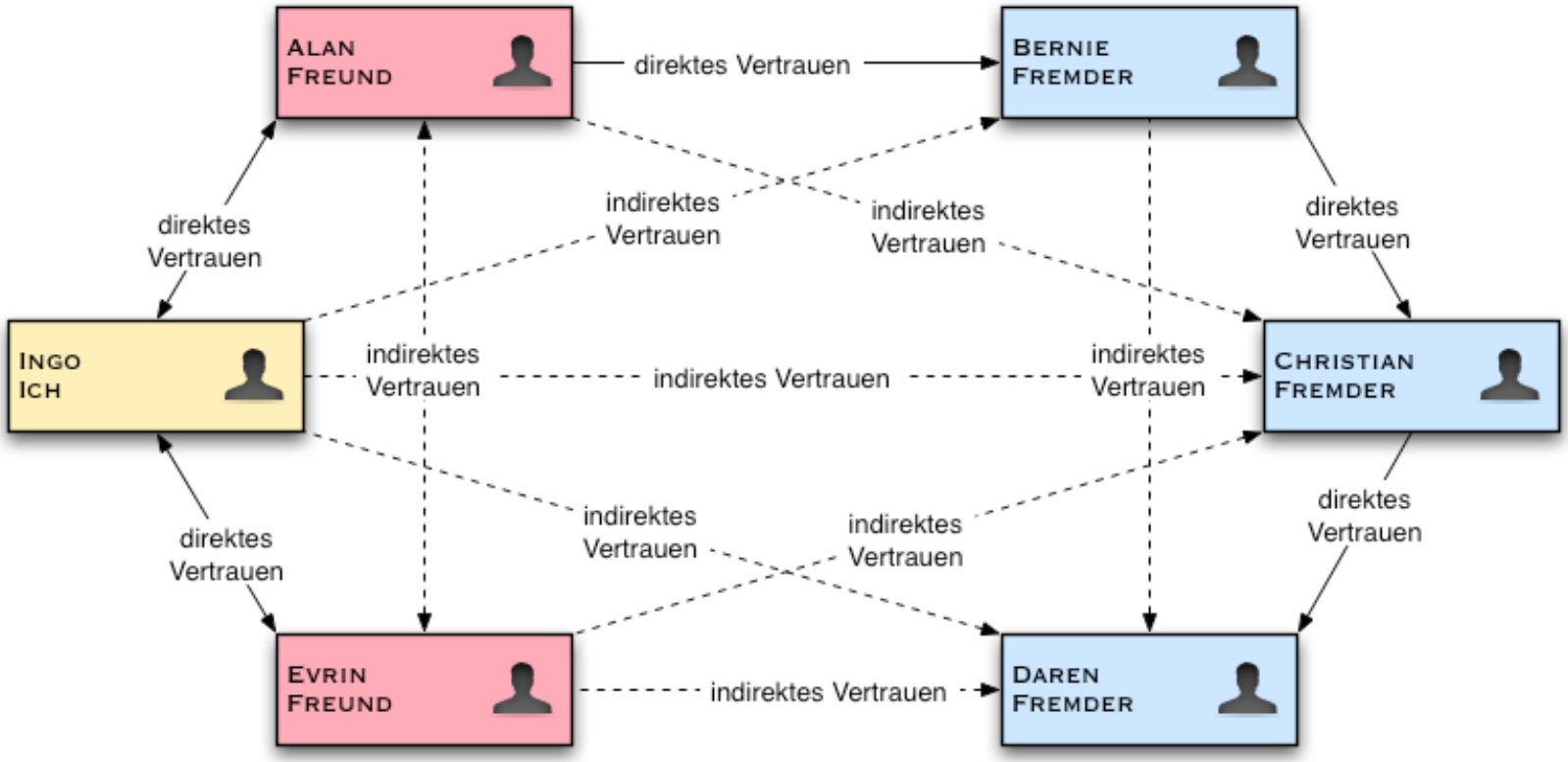
B unterschreibt den Schlüssel S_c von ***C***

- ***A*** kann die Unterschrift von S_c überprüfen
- je nach Vertrauen, das ***A*** in ***B*** hat, wird er vertrauen, dass die Identität von ***C*** laut Zertifikat zu S_c von ***B*** korrekt überprüft wurde.

A vertraut ***B*** direkt

A vertraut ***C*** indirekt

Web of Trust


ALAN FREUND
direktes Vertrauen
BERNIE FREMDER
direktes Vertrauen
indirektes Vertrauen
indirektes Vertrauen
direktes Vertrauen
INGO ICH
indirektes Vertrauen
indirektes Vertrauen
indirektes Vertrauen
CHRISTIAN FREMDER
direktes Vertrauen
indirektes Vertrauen
indirektes Vertrauen
direktes Vertrauen
EVRIN FREUND
indirektes Vertrauen
DAREN FREMDER

Web of Trust

Je mehr Unterschriften das Zertifikat von ***C*** hat, desto wahrscheinlicher ist,

- dass das von ***B*** dabei ist und
- dass daher ***A*** ***C*** vertraut.

Frage:

Kann ***A***,
der das Zertifikat von ***B*** „überprüft“ hat,
sicher sein,
dass ***B*** ebenso genau das Zertifikat von ***C*** überprüft hat,
wie das von ***B***?

Indirektes Vertrauen ist fragwürdiger als direktes.

Web of Trust

- Schlüssel in Server kann nicht gelöscht werden
  - Widerruf möglich
- Unterschriften zu Schlüssel können nicht gelöscht werden
  - Widerruf möglich

Daher bleiben Informationen zu e-Mail-Adressen des Eigners und seine Kontakte zu Signatoren auf immer einsehbar.

- kann ein Problem des Schutzes der Privatsphäre werden

X.509 PKI

X.509 PKI

- Zertifikate nach ITU-Norm X.509
  - Weltweit eindeutige Identität
    - DN Distinguished Name nach nach ITU X.500
      z.B. C=AT,O=Austrian Grid,OU=univie,CN= Willy Weisz
      oder DC=at,DC=austriangridca,O=UniVie,CN=Willy Weisz
    - Aufteilung des Namensraums
- Glaubenwürdiger Dritter: Zertifizierungsstelle
  - CA Certification Authority
  - agiert als Notar
  - kein Web of Trust

Zertifizierungsstelle

Policy

- beschrieben in CP und CPS
  - Certification Policy Zertifizierungsrichtlinie
  - Certification Practice Statement beschreibt Implementierung (keine genauen Interna)
- Basis für Vertrauen
  - sollte vor Vertrauen auf Zertifikate studiert werden

Zertifizierungsstelle

Zertifikat

- öffentlicher Schlüssel in Hülle
- Hülle
  - Identifikation des Zertifikatinhabers
    - zeitlicher Gültigkeitsbereich
  - Verwendungszweck der kryptographischen Schlüssel
  - Identifikation der Zertifizierungsstelle
  - Digitale Signatur durch CA

Zertifizierungsstelle

Zertifikat verliert seine Gültigkeit durch

- Ablauf der Gültigkeitsperiode
- Widerruf
  - initiiert von
    - Inhaber (z.B. bei Änderung der Identifikationsdaten)
    - Zertifizierungsstelle bei Missbrauchverdacht
  - durchgeführt von Zertifizierungsstelle

Zertifizierungsstelle

Widerruf von Zertifizierungstelle:

- Widerrufliste (Certification Revocation List - CRL)
  - regelmäßig (z.B. alle 30 Tage)
  - oder – früher – bei Bedarf erstellt
  - von Stelle, die Zertifikate anerkennt (relying party), in regelmäßigen Abständen (verzögert) abgerufen
- Interaktiv von Relying Party abgerufen
  - Online Certification Status Protocol (OCSP)
  - Stand der aktuellen CRL

Zertifizierungsstelle

Erstellung des Zertifikats

- Signierrechner
  - Offline (zu keinem Zeitpunkt im Netz)
  - Online mit Signieren in HSM (Hardware Security Module)
    - Zertifiziert nach FIPS 140-n (*n* derzeit 2, 3 in Vorbereitung)
    - Privater Schlüssel der CA kann HSM nicht aktivierbar verlassen (spezieller Verschlüsselungsalgorithmus des HSM)
      - kann nur in HSM wieder aktiviert werden

Hausaufgabe

Wozu unterschreiben Sie ein Dokument?

Was sagt die Unterschrift dem Empfänger?

Was sagt die eigenhändige Unterschrift dem Empfänger und einem Dritten?

Warum hat ein Unterschrift nur einen begrenzten rechtlichen Wert? Was muss man tun, um die Unterschrift rechtlich verbindlich zu machen?

Digitale Signatur

Sicherstellen, dass Informationen

- nicht nachträglich verändert wurden
- vom angegebenen Sender stammen.

Digitale Signatur

- Erstellung mit privatem Schlüssel
- Prüfung mit öffentlichem Schlüssel (Zertifikat)

Digitale Signatur

Mögliche Verfahren

- Information wird zusätzlich verschlüsselt
  - Vergleich Klartext mit entschlüsseltem Geheimtext
  - zu aufwendig
- eine kurze Information, die das Original vertritt wird verschlüsselt
  - Kurzinformation muss Einwegfunktion des Originals sein (Hash = Durcheinander)
  - zweites Original zu gleichem Hash schwer zu finden (nicht ableitbar)

Digitale Signatur

Hash-Algorithmen

- MD5 – zu unsicher
  - erfolgreiche Angriffe bekannt
- SHA-Serie
  - SHA-1 160 bit lang
    - Norm: FIPS 180-1
    - Noch sicher genug (bis ca. 2010)
  - SHA-2-Serie
    - Norm: FIPS 180-2
    - SHA-224, SHA-256, SHA-384 und SHA-512
      - Zahl gibt die Länge an

Digitale Signatur

Neuer Algorithmus von NIST ausgeschrieben

→ SHA-3

Einreichungsende des Wettbewerbs: 31.10.2008

64 Hash-Verfahren eingereicht

Entscheidung am 3. Oktober 2012:

- Sieger Keccak <http://keccak.noekeon.org/>

Digitale Signatur

Signatur von e-Mails mit privatem Schlüssel zu

- OpenPGP-„Zertifikat“: PGP/MIME
- X.509-Zertifikat: S/MIME

Mail-Clients können (teilweise)

- e-Mails signieren
- die Überprüfung durchführen

Digitale Signatur & Verschlüsselung

Digitale Signatur und Verschlüsselung können beide auf selbe Information angewandt werden

- Signatur des Originals
  - ???
- Verschlüsselung (Original plus Signatur)
  - Vertraulichkeit
- Signatur des verschlüsselten Originals
  - ???

Digitale Signatur & Verschlüsselung

Hausaufgabe:

Was bestätigt die erste Signatur laut vorhergehender Folie?

Was bestätigt die zweite Signatur (nach der Verschlüsselung)?

HTTPS

Sichere Web-Seiten-Übertragung

- erstellt sichere Kommunikation
  - symmetrische Verschlüsselung der ausgetauschten Daten
  - mit Sitzungsschlüssel
- authentifiziert Web-Server
  - unter Verwendung von X.509-Zertifikat
- kann auch Client authentifizieren
  - Server-Konfiguration
  - mit X.509 Zertifikat und privaten Client-Schlüssel
  - mit UserID/Passwort

SSL und TLS

Sichere Datenübertragung im Internet

- Protokoll angesiedelt in der Darstellungsschicht (6) des OSI-Models
- in Transportschicht des TCP/IP Stapels (über TCP)
- SSL (Secure Sockets Layer)
  - Versionen 1.0 bis 3.0
- TLS (Transport Layer Security)
  - Nachfolger von SSL 3.0
  - Versionen 1.0 (=SSL 3.1), 1.1 und 1.2
  - IETF RFC 2246, 4346, 5246

SSL/TLS

2 Schichten

Untere Schicht

- SSL Record Protocol
  - Symmetrische Ende-zu-Ende Verschlüsselung mit Sitzungsschlüssel (im Handshake ausgehandelt)
  - Sicherstellung der Nachrichtenintegrität durch kryptographische Prüfsumme (Hash)

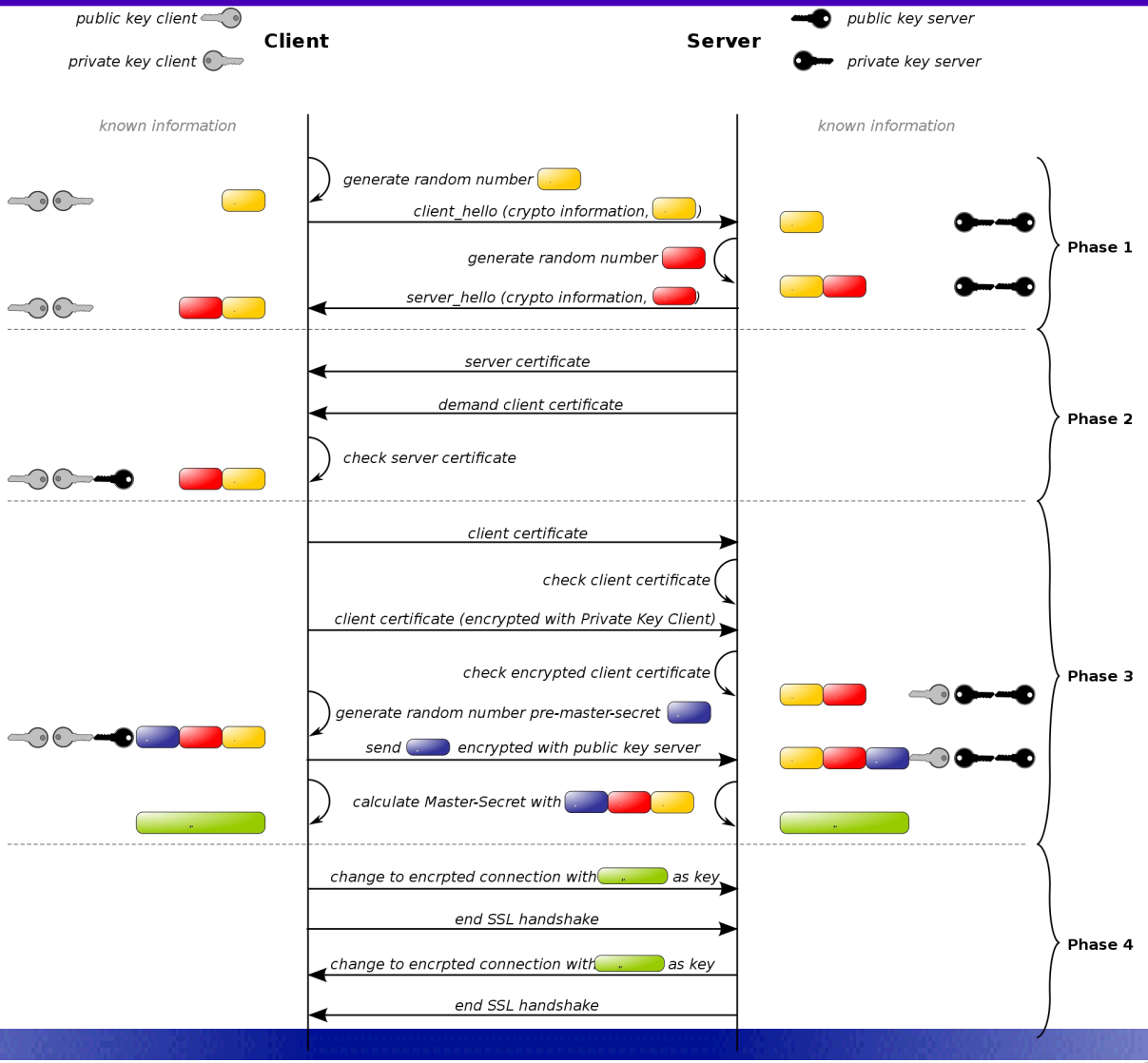
SSL/TLS

2 Schichten

Obere Schicht

- SSL Handshake Protokoll
- SSL Change Cipher Specification Protokoll
- SSL Alert Protokoll
  - Diverse Mitteilungen: Fehler und Warnungen
- SSL Application Data Protocol
  - Zerlegung der Daten
  - Kompression und eventuell Verschlüsselung

SSL und TLS



Fehler im SSL/TLS-Protokoll

Im November 2009 veröffentlicht

- Folge einer nicht durchdachten Optimierung beim Neuaushandeln der Verschlüsselung
- Erlaubt Man-in-the-Middle-Angriff (MitM)
  - Nicht trivial
  - Aber es gibt sinnvolle Angriffsszenarien

Darstellung in:

`http://www.g-sec.lu/practicaltls.pdf`

Angriff über SSL/TLS-Protokoll

Vorgangsweise:

1. Klient sendet TLS-Handshake zum Server
2. MitM hält den Datenstrom auf und handelt seinerseits TLS-Verbindung aus
3. MitM sendet Strom mit seinen Anforderungen (oft mit „ignore what comes now“ beendet), jedoch als „nicht abgeschlossen“ an den Server
4. Innerhalb seiner verschlüsselten Session initiiert MitM eine Neuaushandlung (renegotiation)

Angriff über SSL/TLS-Protokoll

5. und reicht dabei die TLS-Handshake-Daten einschließlich der initialen Anforderungen (die eventuell lt. 3. ignoriert werden) an den Server weiter.
6. Entsprechend der Normvereinbarung werden alle Anforderungen der Kommunikation, die einen Abschluss der Folge schickt, zugeordnet – auch über Neuverhandlungen hinweg.

Angriff über SSL/TLS-Protokoll

7. Falls der Server wegen einer der Teilanforderungen eine Authentisierung des Klienten verlangt, so geschieht dies im Zuge der Neuverhandlung.
8. Die weitere Kommunikation verläuft für den Klienten normal weiter.

Das Problem liegt darin, dass für den Server anhand des Protokolls nicht erkennbar ist, dass mit der Neuaushandlung ein Partnerwechsel stattgefunden hat – ebenso für den Klienten.

Behebung im SSL/TLS-Protokoll

Das Problem kann nur dadurch behoben werden, dass sich in Zuge einer Neuaushandlung beide Partner vergewissern, dass sie ein gemeinsames Geheimnis, eine Kennung der zu verlassenden Session, kennen.

Im Angriffsfall ist die Kennung der Session mit dem MitM dem Klienten unbekannt, und der Angriff wird erkannt.

Korrektur des Fehlers

Erweiterung des Verbindungsprotokolls

- Einführung einer Session-Kennung
- Überprüfung der beidseitigen Kenntnis der Session-Kennung bei der Neuaushandlung
- Neudefinition der Kennung für die session nach der Neuaushandlung
- IETF RFC 5746

Hardware Security Token

Hardware zum Speichern kryptographischer Schlüssel

- Eigner trägt ihn bei sich
- Kryptographische Funktionen im Token
  - Schlüsselpaar in Token erstellt
  - privater Schlüssel nur in Token-Speicher
    - erst nach PIN-Eingabe aktiviert
    - nicht auslesbar
  - Prozessor für Ver- und Entschlüsselung im Token

Hardware Security Token

2-Faktoren-Authentifizierung:

- Haben:
  - einen physischen Schlüsselbehälter mit verschlüsseltem privaten Schlüssel
    - Diebstahl ist physischer Verlust – wie bei mechanischem Schlüssel
- Wissen
  - Pin darf nur dem Besitzer des Hardware Token bekannt sein

Nur wenn beide Faktoren vorhanden sind, kann der private Schlüssel verwendet werden

Hardware Security Token

3-Faktoren-Authentifizierung:

- zu Haben und Wissen kommen
- biometrische Daten (z.B. Fingerabdruck)
- derzeit kaum in Verwendung

SmartCard

SmartCard

- Prozessor-/Speicher-Chip auf Plastikkarte
- Kartenleser im Computer
  - PIN-Eingabe über Tastatur und Programm
  - Gefahr des Mitlesens durch anderen lokalen Benutzer
    - z.B. Trojaner, der Daten über das Netz weiterleitet
  - Diebstahl des „Wissens“ bleibt unbemerkt
    - gestohlene SmartCard kann verwendet werden

SmartCard

SmartCard

- Besser: Kartenleser mit eigener numerischer Tastatur
  - sicherer Pfad für PIN-Eingabe
    - nicht über Computer
  - von Trojaner nicht auspähbar
  - kann auch Computer-Tastatur mit eingebautem Kartenleser sein
    - PIN-Eingabe geht direkt auf Kartenleser nicht über den Computer Computer

Hardware Security Token

Secure USB Token

- enthält SmartCard-Chip
- Format eines USB-Sticks
- direkt an USB-Eingang des Computers angeschlossen
  - PIN-Eingabe über Computer
  - gleiche Sicherheitsstufe wie SmartCard ohne eigene PIN-Eingabetastatur

SmartCard mit Magnetstreifen

Überbleibsel einer alten Technologie

- erste Bank- und Kreditkarten hatten Information auf Magnetstreifen
- Magnetstreifen kopierbar
  - Skimming, ein Man-in-the-Middle-Angriff
- Wird oft auf Schlüsselkarten von Hotels kopiert
  - Schlüsselkarten haben andere Magnetisierungsstärke
  - Sollten nicht für Geldgeschäfte verwendbar sein
  - Unterschied wird jedoch oft nicht berücksichtigt

PKI-Anwendung: Grid Computing

Grid Computing:

- Verarbeitungsleistung steht im Netz zur Verfügung (Grid wie das Stromnetz)
- Benutzer kann entfernte Resourcen nutzen,
  - nachdem er sich lokal (PC, lokale Workstation) angemeldet hat,
  - ohne explizite Neuanmeldung am entfernten System (Single Sign On – SSO)
- Zukunft
  - keine explizite Angabe des Zielssystems
  - nur Leistungsanforderung wird abgesetzt

Rechtedelegation

SSO erfordert

- Identifizierung und Authentifizierung ohne Login am entfernten System
- Rückverfolgung auf Identität am Ausgangsrechner
- Rechtezuteilung am Zielsystem aufgrund der Identität am Ausgangsrechner

=> Delegation von Rechten (und Identität) - Proxy

Proxy

Benötigt wird

- Identifizierungs/Authentifizierungs-Algorithmus
- Absicherung gegen Identitätsdiebstahl

Lösung:

- Generierung eines Schlüsselpaares
  - das zum Zielsystem weitergeleitet wird
  - dessen öffentlicher Schlüssel Teil eines X.509-Zertifikats ist
  - das eine begrenzte Lebensdauer hat

Proxy

Proxy-Zertifikat

- wird mit dem privaten Schlüssel des Eigners signiert (Eigner fungiert als CA für den Proxy)
- subjectName des Proxy enthält den des Originalzertifikats
- wird gemeinsam mit dem privaten Schlüssel an das Zielsystem übertragen
  - wo der Proxy nur für den dort definierten „Eigner“ zugreifbar ist
    - „Eigner“ am Zielsystem über subjectName des Proxy-Zertifikats bestimmt (z.B. über gridmap file bei der Globus Middleware)

Proxy

Proxies sind transitiv

- Proxy kann für weitere Delegation ein weiteres Proxy generieren
  - signiert mit dem privaten Schlüssel des vorhergehenden Proxy
- So kann ein Job/Prozess im Grid
  - im Auftrag des Ausgangsnutzers
  - einen weiteren Job auf einem weiteren entfernten System starten
  - und seine Rechte delegieren

Proxy

Proxy ist verwundbarer als eigener privater Schlüssel

- Hat einen nicht verschlüsselten privaten Schlüssel
  - notwendig, da keine Passwort-Eingabe am entfernten System möglich
- Vertrauenswürdigkeit eines entfernten Systems
  - muss vorab geklärt werden

Virtuelle Organisationen - VO

Virtuelle Organisation

- Organisationsform im Grid
  - Teilnehmer (reale Organisationen) bringen Verbraucher und Betriebsmittel (Resources) ein
  - Administrationsdomänen bleiben erhalten
  - Zugriffsrechte
    - im Rahmen der VO
    - entsprechend den Regeln der einzelnen Administrationen

Virtuelle Organisationen - VO

Virtuelle Organisation

- temporär
  - z.B. für die Dauer eines Projekts
- dynamisch veränderbar, z.B.
  - Zu-/Abgang von Teilnehmern
  - Funktions-/Rollendefinitionen innerhalb der VO

Mehrere VOs mit gleichem oder überlappenden Ressourcen/Benutzer-Pool

Berechtigungen in der VO

Hängen ab von

- Berechtigungen in der Teilnehmerorganisation
  - z.B. Spital: Arzt, Pflegepersonal, Techniker, Administratoren
- Berechtigungen innerhalb der VO
  - z.B. Projektleiter, Administrator, Arbeitspaketleiter, Koordinator
  - unabhängig von der Hierarchie der Teilnehmer-organisationen

Berechtigungen in der VO

Berechtigungen in der VO

- mehrdimensionale Vorgaben
- dynamisch wegen der Dynamik der VO

=> Identitätsbasierte (ermessensbasierte) Berechtigung (DAC) nicht sinnvoll handhabbar

=> attributbasierte Berechtigungen

Berechtigungen in der VO

Attribute für Berechtigungen in der VO

- aus den Teilnehmerorganisationen
- aus der VO

Zugriffssteuerung muss

- alle Attributquellen befragen
- mehrdimensionales Regelwerk berücksichtigen

=> Zugriffsteuerung aufgrund von Richtlinien (policies)

Attributautoritäten

Informationen über Attribute/Rollen werden von Attributautoritäten (Attribute Authorities - AA)

- der einzelnen Organisationen
- der VO

veröffentlicht und signiert werden.

Gleiches gilt für Attribute der Betriebsmittel

Autorisierung aufgrund von Richtlinien

Richtlinie (Policy) = Satz von Regeln, die auf Identitäten und Attributen von Verbrauchern und Betriebsmitteln beruhen

Kann die Bewilligung durch Dritten erfordern

- z.B. durch den Patienten zur Freigabe seiner Gesundheitsakte an den Arzt oder die Versicherung
- Der Dritte muss ebenfalls authentifiziert werden,
- seine Attribute berücksichtigt werden.

Autorisierungsarchitektur

Für jeden Verbraucher und jedes Betriebsmittel einer Anforderung muss

- eine vollständige Richtlinie oder ein Satz von Richtlinien durch eine *Source of Authority* (SOA), auch als *Policy Administration Point* (PAP) bezeichnet, definiert werden,
- eine daraus abgeleitete Entscheidung, anzunehmen oder abzulehnen, abgeleiten werden.

Autorisierungsarchitektur

Ein Klientenagent (z.B. Web-Portal) sammelt alle ihm zugänglichen Authentisierungsdaten und Attribute

- vom Anforderer
- von *Policy Information Points* (PIP), z.B. ihm zugänglichen AAs

und sendet diese mit der Anforderung an das Betriebsmittel

Autorisierungsarchitektur

Dort übernimmt der *Policy Enforcing Point* (PEP) die Anforderung mit allen beigefügten Informationen.

Der PEP übergibt zuerst einmal die Anforderung an einen *Policy Decision Point* (PDP), der

- optimal beim Betriebsmittel angesiedelt ist,
- aber auch übergeordnet angesiedelt sein kann.

Autorisierungsarchitektur

Der PDP

- wendet die Regeln der Policy an
- unter Berücksichtigung aller Identitäts- und Attributinformationen
- kann eventuell von PIPs, z.B. AAs, weitere Informationen anfordern,
- entscheidet über die Anforderung
- reicht die Entscheidung - *annehmen* oder *ablehnen* – an den PEP zurück.

Autorisierungsarchitektur

Der PEP schließlich

- setzt die Entscheidung des PDP zwingend um oder
- trifft eine Standardentscheidung, wenn der PDP keine Entscheidung treffen konnte, und setzt diese zwingend um.
  - Standardentscheidung muss vorab vorgegeben sein.
  - Unentscheidbarkeit darf es nicht geben.

Attributsammlung

Attributsammlung durch

- den Agenten des Anforderers
- den PDP

Sammlung durch den Agenten des Anforderers

- skaliert besser
- leichter realisierbar, insbesondere in Bezug auf Attribute, die in der Organisation des Anfordernden vorhanden sind.

Attributsammlung

Attribute oft in unterschiedlichen Datenbanken vorhanden.

Daher Bedarf nach

- genormten Protokollen zum Transport der Attribute,
- Entwicklung von *Plugins* für Datenbanken, um diese Protokolle zu bedienen.

Attributsammlung

Vorhandene Protokollnormen

- X.509 Attributzertifikate im ASN.1-Format
  - IETF RFC 5755
  - http://www.ietf.org/rfc/rfc5755.txt
- die XML-kodierte Security Assertion Markup Language (SAML)
  - der OASIS (Organization for the Advancement of Structured Information Standards)
    - http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

Attributsammlung

Signierte Attribut-Informationen können

- als eigenständige Informationsblöcke übertragen
  oder
- in Proxies als *Extensions* eingebaut werden.