TU Braunschweig
Institut für Betriebssysteme
und Rechnerverbund

Verteilte Systeme

Prof. Dr. Stefan Fischer

Kapitel 10: Sicherheit

Überblick

- Das Sicherheitsproblem
- Sicherheitsdienste und -mechanismen
- Kryptographie u. Anwendungen
  - Vertraulichkeit
  - Authentifizierung
  - Integrität
- Zugriffssteuerung
  - Firewalls
  - Virtual Private Networks

Grundbegriffe

- **Angriffe**:
  Jede Handlung, die die Sicherheit der Informationen einer Organisation gefährdet
- **Sicherheitsmechanismen**:
  Ein Mechanismus zur Entdeckung, Verhinderung oder Beseitigung eines Sicherheitsangriffs
- **Sicherheitsdienste**:
  Ein Dienst, der die Sicherheit eines DV-Systems und des Informationsaustauschs einer Organisation erhöht. Der Dienst wirkt Sicherheitsangriffen entgegen und verwendet einen oder mehrere Sicherheitsmechanismen.

Sicherheitsdienste

- Informationssicherheitsdienste sind prinzipiell nichts anderes als Nachbildungen von Funktionen zur Absicherung physischer Dokumente (sehr viele Vorgänge beruhen auf Dokumenten und deren Integrität).
- Herausforderungen:
  - Unterscheidung von Kopien: normalerweise machbar bei physischen Kopien
  - Veränderung an gedruckten Dokumenten hinterlässt Spuren
  - Prüfverfahren beruhen meist auf der physischen Beschaffenheit eines Dokuments

  → Wie sieht das bei elektronischen Dokumenten aus?

Sicherheitsmechanismen

- Es gibt keinen Mechanismus, der alle diese Dienste erbringen kann.
- Aus diesem Grund wurden eine Reihe von Sicherheitsmechanismen entwickelt.
- Der bei weitem wichtigste ist jedoch die Kryptographie (s.w.h).

Angriffe

- Zur besseren Beurteilung und Abwehr von Angriffen teilt man sie in verschiedene Kategorien ein, die jeweils ein Abweichen vom normalen Datenfluss anzeigen:

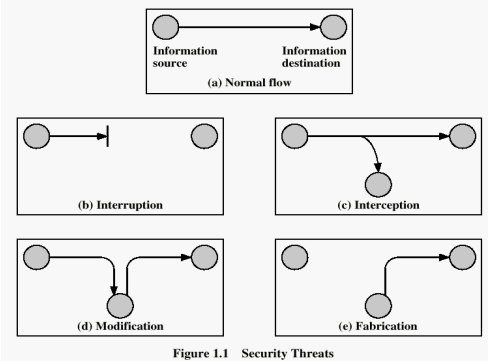
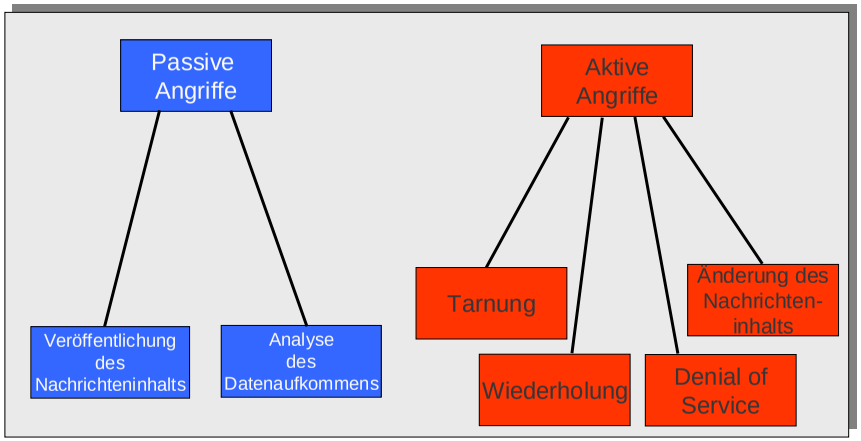


Figure 1.1 Security Threats

Angriffstypen

- Unterbrechung:
  - Bestandteil des Systems wird zerstört oder unbrauchbar gemacht.
  - Angriff auf die Verfügbarkeit
- Abfangen:
  - Ein nicht berechtigter Dritter erhält Zugriff auf einen Systemteil.
  - Angriff auf die Vertraulichkeit
- Modifikation:
  - Ein nicht berechtigter Dritter verschafft sich nicht nur Zugriff auf einen Systemteil, sondern manipuliert ihn auch.
  - Angriff auf die Integrität
- Fälschung:
  - Ein nicht berechtigter Dritter schleust gefälschte Objekte in ein System ein.
  - Angriff auf die Authentizität

Einteilung in passive und aktive Angriffe



Kategorien von Sicherheitsdiensten

- Basierend auf diesen Angriffen bzw. den Angriffszielen wollen wir nun noch einmal versuchen, verschiedene Kategorien von Sicherheitsdiensten zu finden:
- Die folgende Kategorisierung wird weitgehend verwendet:
  - Vertraulichkeit
  - Authentifizierung
  - Integrität
  - Nicht-Anfechtbarkeit
  - Zugriffssteuerung
  - Verfügbarkeit

Vertraulichkeit

- engl.: *confidentiality*
- = Schutz der übertragenen bzw. gespeicherten Daten vor passiven Angriffen
- Kann auf verschiedenen Ebenen realisiert werden
  - Kompletter Datenaustausch zwischen zwei Benutzern bis auf
  - Nachrichtenebene
- Anderer Aspekt: Schutz des Datenflusses vor Analyse

Authentifizierung

- engl. *authentication*
- Überprüfung einer Nachricht auf ihre Echtheit: kommt sie wirklich von dem, der behauptet, sie geschickt zu haben
- Bei einer einzelnen Nachricht:
  - Authentifizierung für diese Nachricht
- Bei einer länger andauernden Beziehung:
  - Zusätzlich muss verhindert werden, dass jemand die authentifzierte Identität übernehmen kann

Integrität

- engl. *integrity*
- Auch hier verschiedene Ebenen
  - Schutz vor Änderung einzelner Nachrichten
  - Schutz einer ganzen Verbindung durch Verhindern von
    - Änderungen an einzelnen Nachrichten
    - Vertauschung
    - Verdoppelung
    - Einfügung
    - Wegfall von Nachrichten

Nicht-Anfechtbarkeit

- engl. *non-repudiation*
- Hindert den Sender bzw. den Empfänger einer Nachricht daran, die Übertragung der Nachricht zu leugnen
  - Wenn eine Nachricht abgeschickt wird, kann der Empfänger beweisen, dass die Nachricht tatsächlich vom angegebenen Sender stammt.
  - Der Sender kann beweisen, dass der Empfänger die Nachricht erhalten hat.

Zugriffssteuerung

- engl. *access control*
- Die Möglichkeit, den Zugriff auf Host-Systeme und Anwendungen zu beschränken und zu steuern
- Dazu muss typischerweise eine Einheit, die versucht Zugriff zu erhalten, zunächst identifiziert und authentifiziert werden.
- Anschließend können die Zugriffsrechte sehr genau zugeschnitten vergeben werden

Verfügbarkeit

- engl. *availability*
- Ein System kann benutzt werden, wenn es benötigt wird.
- Kann durch eine Vielzahl von Angriffen in Frage gestellt werden.
- Es gibt automatische Gegenmaßnahmen, oft können aber auch nur physische Gegenmaßnahmen helfen.

Kryptographie

- Kryptologie umfasst zwei Gebiete
  - Kryptographie:
    grob gesagt die Wissenschaft vom Datenschutz durch Verschlüsselung
  - Kryptanalyse:
    die Kunst, ohne Kenntnis des Schlüssels an die geheimen Daten zu kommen
- Kryptologie ist schon seit Tausenden von Jahren Gegenstand von Untersuchungen
- Trotzdem ist diese Wissenschaft immer noch sehr geheimnisumwittert – warum?

Wichtige Begriffe

Klartext:

die zu verschlüsselnde Botschaft

Geheimtext:

Der verschlüsselte Text

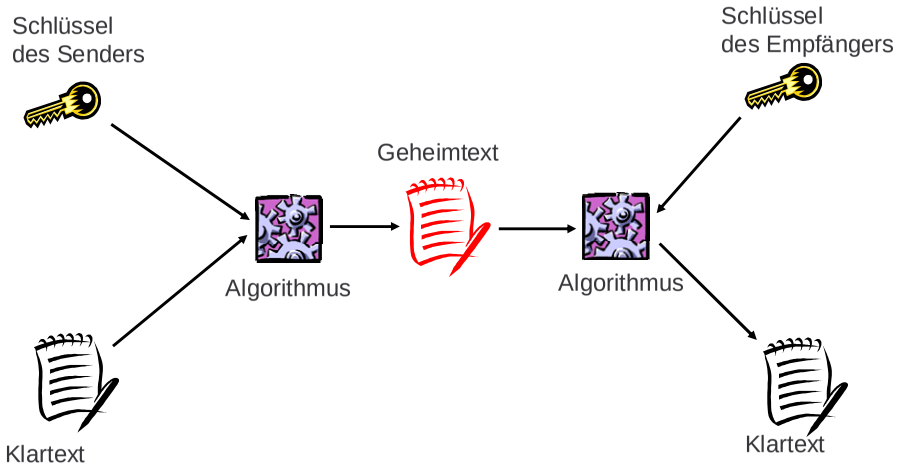
Verschlüsselung, Codierung, Chiffrierung:

Überführung des Klartext in den Geheimtext

Entschlüsselung, Decodierung, Dechiffrierung:

Überführung des Geheimtext in den Klartext

Prinzip der Verschlüsselung



Geheime Schlüsselverfahren

- Die Kommunikationspartner A und B besitzen einen gemeinsamen geheimen Schlüssel K_c.
- K_c wird sowohl für Ver- als auch für Entschlüsselung eingesetzt.
- Bis Mitte der 70er Jahre des 20. Jhdts. kannte man nur geheime Schüsselverfahren
- Wir wollen uns zunächst eines der einfachsten Verfahren anschauen, die Caesar-Chiffrierung.

Caesar-Verschlüsselung

- Dies ist eine der ältesten Verschlüsselungsmethoden, angeblich erfunden von Julius Caesar.
- Es wird einfach jeder Buchstabe des Klartextes durch den im Alphabet 3 Plätze (bzw. allg. n Plätze) weiter hinten stehenden ersetzt:
  - A → D
  - B → E
  - ....
  - Z → C
- Was ist der Schlüssel?
- Zum Ausprobieren: http://willy.chemie.uni-konstanz.de/fotos/caesar.htm
- Es gibt eine große Menge historischer Verfahren (einfache Substitution, Vigenère, Enigma, …)

Modernere Verschlüsselungsverfahren

- Wir wollen uns nun mit einigen Verfahren beschäftigen, die „etwas“ moderner sind:
  - Erst Mitte der 1970er Jahre entwickelt
  - Bit- statt zeichenweise Verschlüsselung
  - Nutzung von Konfusion und Diffusion
  - Bis heute gibt es ausser Brute-Force keinen bekannten Angriff gegen diese Verfahren
- Insbesondere gehen wir ein auf
  - Data Encryption Standard (DES)
  - RSA (Rivest, Shamir, Adleman)

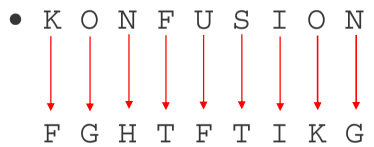
Bitweise Verschlüsselung

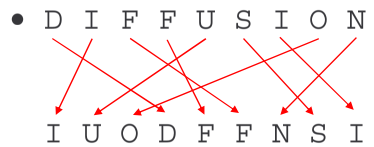
- Bisherige Verfahren: zeichenorientiert
- Mit Computern kann man auf bitweise Verschlüsselung übergehen:
  - Häufigkeitsanalysen werden schwierig: wie sieht die Verteilung des 3. Bits aller Bytes eines Textes aus?
- Typischerweise wird die bitweise XOR-Operation verwendet, um Schlüssel und Klartext zu verknüpfen
  - XOR ist einfach in Hardware zu implementieren
  - XOR ist leicht umkehrbar (einfach erneute Anwendung)

⊕	0	1
0	0	1
1	1	0

Konfusion und Diffusion

- Konfusion
  - Verschleierung des Zusammenhangs zwischen Klartext und Geheimtext
  - Also Ersetzen eines Zeichens durch ein anderes
- Diffusion
  - Verteilung der im Klartext enthaltenen Information über den Geheimtext
  - Das Prinzip der Transposition, die Positionen der Zeichen werden vertauscht





Verschärfung: Lawineneffekt

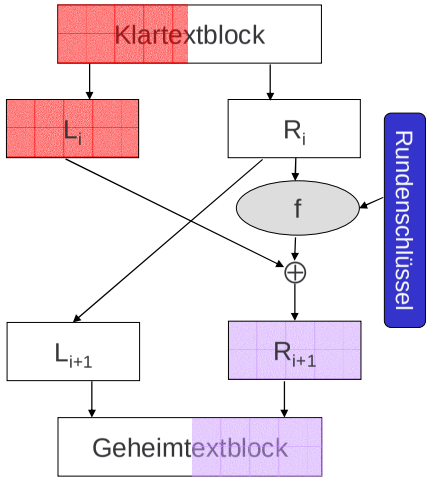
- Lawineneffekt
  - Jedes Bit des Geheimtextes soll von jedem Bit des Klartextes und des Schlüssels abhängen.
- Die einfachen Verfahren arbeiten nur mit Konfusion.
- Ziel: Änderung eines Schlüssel- bzw. Klartextbits führt bei jedem Geheimtextbit mit 50% Wahrscheinlichkeit zu einer Änderung
- Sonst können statistische Verfahren angewandt werden

Strom- vs. Blockchiffrierung

- Stromchiffrierung
  - Es wird eine Bitfolge erzeugt, mit der der Nachrichtenstrom verschlüsselt wird – optimalerweise genauso lang wie der Strom.
- Blockchiffrierung
  - Es werden Gruppen von Bits zusammengefasst und gemeinsam verschlüsselt, oft jede Gruppe mit demselben Schlüssel
  - Einfaches Beispiel: einfache Substitution wie bei Caesar
- Heute nutzen praktisch alle sehr guten Verfahren die Blockchiffrierung.

Feistel-Netzwerke

- Heute die zentrale Komponente gängiger Kryptoverfahren
- Entworfen von Horst Feistel (IBM) Anfang der 70er Jahre
- Verschlüsselung besteht aus mehreren Runden
- Einfaches Prinzip mit einer sehr hilfreichen Eigenschaft – das Dechiffrieren wird einfach
- Warum?



Feistel-Netzwerke (II)

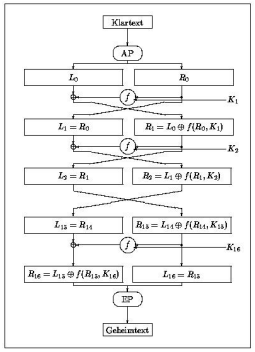
- Es gilt:
  - $L_{i+1} = R_i$ und $R_{i+1} = L_i \oplus f_{s,i}(R_i)$
- Damit folgt bei Kenntnis des Schlüssels und f
  - $L_i = L_i \oplus f_{s,i}(R_i) \oplus f_{s,i}(R_i)$ (Umkehrbarkeit von XOR)
    $= R_{i+1} \oplus f_{s,i}(R_i)$
- Das heißt, durch erneutes Anwenden der Funktion f lässt sich von der Stufe i auf i-1 zurückrechnen.
- Dies geht bis L_0 und R_0.
- Das heisst, f muss nicht umkehrbar sein! Es genügt, dass f ohne Schlüssel nicht berechenbar ist.
- Man kann also beliebig komplexe Funktionen wählen.

Geschichte von DES

- DES = Data Encryption Standard
- Ergebnis einer öffentlichen Ausschreibung des amerikanischen National Bureau of Standards (NBS) Mitte der siebziger Jahre zum Entwurf eines **einheitlichen sicheren Verschlüsselungsalgorithmus**
- Bester Vorschlag von IBM (Feistel, Coppersmith et al.)
- Modifiziert von 128 auf 56 Bit Schlüssellänge unter Mitarbeit der berühmten NSA (National Security Agency)
- Deswegen immer wieder Bedenken wegen möglicher Unsicherheit, die nur die NSA kannte
- Bis heute kein Angriff außer Brute-Force bekannt

Der DES-Algorithmus

- DES kodiert Datenblöcke: 64 Bits werden in einem Schritt verschlüsselt.
- Die Schlüssellänge ist ebenfalls 64 Bit, wobei jedes 8. Bit ein Kontrollbit ist $\Rightarrow$ 56 Bit effektive Schlüssellänge
- DES führt 16 Verschlüsselungsschritte aus.
- Eine Runde ist ein Feistelnetzwerk und besteht aus Bit-Permutationen und Verteilungen.



Sicherheit von DES

- DES ist heute wegen seiner kurzen Schlüssellänge in kurzer Zeit mittels Brute-Force zu brechen
- Neuere Analyseverfahren wie differenzielle und lineare Analyse werden ebenfalls ständig weiterentwickelt und stellen eine Gefährdung dar
- Deswegen wird DES ersetzt durch neuere Verfahren mit längeren Schlüsseln wie z.B. Triple DES

Verteilung geheimer Schlüssel

- großes Problem: wie tauschen die beiden Kommunikationspartner ihre(n) Schlüssel aus, bevor sie kommunizieren können?
- Über dieselbe Leitung geht es offensichtlich nicht – extreme Unsicherheit!
- Andere Verfahren:
  - Telefon
  - Brief
  - Kurier
  - Persönliches Treffen
- Frage nach Sicherheit und Anwendbarkeit?

Verteilung geheimer Schlüssel (II)

- Traut man zum Schlüsseltausch einem Kanal nicht, wählt man eine Kombination aus mehreren.
- Beispiel: 64-Bit-Schlüssel in 4 Teile teilen, je einen Teil über jeden Kanal
- Frage: wie teilt man den Schlüssel?
  - Warum ist eine Aufteilung in 4 16-Bitblöcke nicht gut?
  - Besser: Schlüssel = Summe von vier 64-Bit-Zahlen, von denen drei zufällig sind
  - Warum ist das besser?

Schlüsselverteilzentren

- Populäre Variante: Schlüsselverteilzentren (*key distribution centers*, KDC), die On-Demand einen Sitzungsschlüssel für die Kommunikationspartner generieren können
- Vorteil: schnell, flexibel
- Nachteile:
  - Mit dem Schlüsselcenter muss auch zunächst ein vertraulicher Schlüssel etabliert werden
  - Der Schlüsselcenter muss 100% vertrauenswürdig sein

Asymmetrische Verfahren

- Wegen der versch. Nachteile Suche nach neuen Verfahren zur Schlüsselverteilung
- Sensationelle Neuerung Mitte der siebziger Jahre
  - Etablierung eines geheimen Schlüssels ohne dass die Kommunikationspartner sich kennen müssen
  - Basiert auf zwei unterschiedlichen Schlüsseln, die miteinander mathematisch zusammen hängen (deshalb asymmetrisch, alle bisherigen Verfahren waren symmetrisch)
  - Entwickelt von Diffie und Hellman 1976

Die Idee von Diffie-Hellman

- In asymmetrischen Schlüsselverfahren besitzt jeder Partner in einer Zweier-Kommunikationsbeziehung zwei Schlüssel:
  - Ein privater Schlüssel, der geheim gehalten werden muss
  - Ein öffentlicher Schlüssel, der jedem zur Verfügung steht
- Es ist praktisch unmöglich, den einen Schlüssel aus dem anderen abzuleiten, obwohl die beiden voneinander abhängig sind.
- Authentizität und Integrität müssen für den öffentlichen Schlüssel garantiert sein, jedoch nicht die Vertraulichkeit.

Anwendung asymm. Verfahren

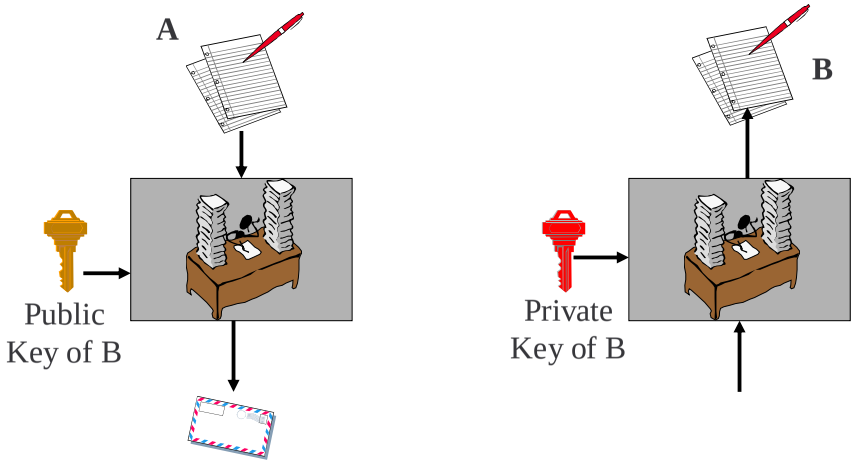
- Asymmetrische Schlüsselverfahren können nach diesem Prinzip drei unterschiedliche Anwendungen haben:

1. Schlüsselaustausch für symmetrische Verfahren
2. Verschlüsselung und Entschlüsselung „normaler“ Nachrichten
3. Digitale Signaturen

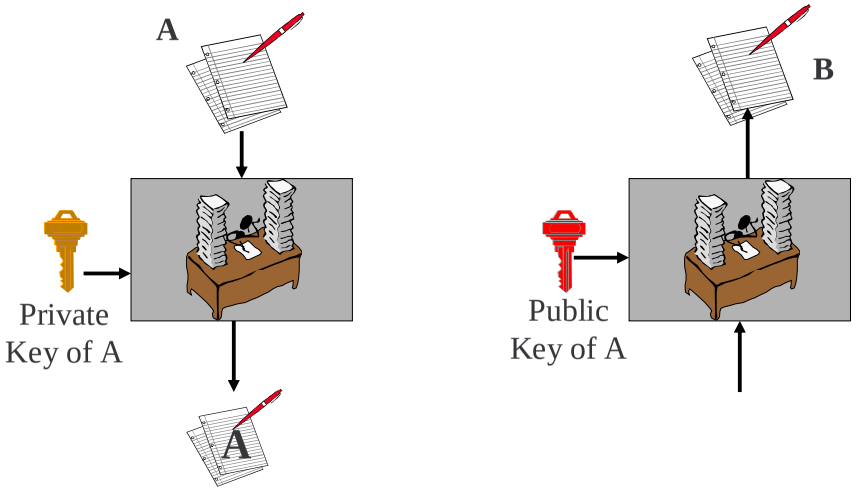
Generelles Verfahren

- Annahme: A will mit B kommunizieren
- Zunächst erzeugt jeder ein asymmetrisches Schlüsselpaar.
- Wenn B an A eine Nachricht schicken will, verschlüsselt er diese mit dem öffentlichen Schlüssel von A.
- Wenn A diese Nachricht bekommt, entschlüsselt sie die Nachricht mittels ihres privaten Schlüssels.

Ver- und Entschlüsselungsprozess



Prozess des digitalen Signierens

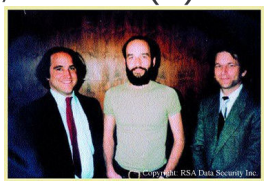


Unterschied Symmetrisch-Asymmetrisch

Symmetrisch	Asymmetrisch
Derselbe Algorithmus mit demselben Schlüssel wird für Ver- und Entschlüsselung verwendet.	Je ein Algorithmus und Schlüssel für Ver- und Entschlüsselung.
Sender und Empfänger besitzen jeweils denselben Schlüssel.	Sender und Empfänger müssen je jeweils einen der zusammengehörigen Schlüssel besitzen.
Der Schlüssel muss geheim gehalten werden.	Einer der beiden Schlüssel muss geheim gehalten werden.
Es muss unmöglich oder zumindest sehr schwer sein, eine Nachricht ohne weitere Infos zu entschlüsseln.	Es muss unmöglich oder zumindest sehr schwer sein, eine Nachricht ohne weitere Infos zu entschlüsseln.
Kenntnis des Algorithmus plus mitgelesene Nachrichten dürfen nicht ausreichen, um den Schlüssel zu bestimmen.	Kenntnis des Algorithmus plus mitgelesene Nachrichten plus Kenntnis des einen Schlüssels dürfen nicht ausreichen, um den anderen Schlüssel zu bestimmen.

RSA

- Diffie-Hellman leistet nur den Schlüsselaustausch, man kann keine geheimen Nachrichten verschicken bzw. digital signieren
- Der erste Algorithmus, der die von Diffie und Hellman postulierten Eigenschaften erfüllte, wurde 1977 von Rivest (R), Shamir (S) und Adleman (A) entwickelt.



Eigenschaften von RSA

- Blockchiffrieralgorithmus
- Klar- und Geheimtextblöcke werden als große ganze Zahlen aufgefasst, ebenso der Schlüssel
- Die Schlüssellänge ist variabel (typisch heute: 1024, 2048 Bit).
- RSA basiert auf den Eigenschaften von Primzahlen und modularer Arithmetik.
- Insbesondere wird ausgenutzt, dass es schwer ist, das Produkt zweire großer Primzahlen zu faktorisieren.

RSA in Kürze

Schlüsselerzeugung:

Wähle p, q	p und q sind Primzahlen, $p \neq q$
Berechne $n = p \times q$	
Berechne $\phi(n) = (p-1)(q-1)$	
Wähle eine Ganzzahl e	$ggt(\phi(n), e) = 1; 1 < e < \phi(n)$
Berechne d	$d \equiv e^{-1} \bmod \phi(n)$
Öffentlicher Schlüssel:	$KU = \{e,n\}$
Privater Schlüssel:	$KR = \{d,n\}$

Verschlüsselung:

Klartext:	M < n
Geheimtext:	$C = M^e \bmod n$

Entschlüsselung:

Geheimtext:	C
Klartext:	$M = C^d \bmod n$

Sicherheit von RSA

- Der vielversprechendste Angriff auf RSA (außer Brute Force) besteht in der Faktorisierung von n.
- Wenn es gelingt, aus n p und q abzuleiten, dann kann man $\phi(n)$ berechnen und damit d.
- Allerdings ist Faktorisierung ein hartes Problem, das mit zwei Stoßrichtungen angegangen wird
  - Einsatz von immer mehr Computer-Power
  - Immer verfeinerte Algorithmen

Sichere Protokolle und Anwendungen

- Die Ideen und Lösungen der Kryptographie wurden inzwischen auf vielfältige Art und Weise in Kommunikationsprotokolle und Anwendungen umgesetzt, bspw.:
  - IPsec
  - Secure Socket Layer/Transport Level Security
  - PGP – Email-Sicherheit
  - SET – sichere Transaktionen

Firewalls

- Vergleich mit Burgtor / Burggraben einer mittelalterlichen Burg:
  - Erlaubt Eintritt nur an bestimmter Stelle
  - Verhindert, dass Angreifer an weitere Verteidigungsanlagen herankommt
  - Sorgt dafür, dass System nur an einem bewachten Punkt verlassen werden kann
- Grenze zwischen unsicherem und vertrauenswürdigem Netz
- Meist: zwischen Internet und Intranet

Firewalls - Aufgaben

- Durchlass von akzeptablem Netzverkehr
- Verkehr ist akzeptabel, wenn er der Sicherheitspolitik des Betreibers genügt
- Die Sicherheitspolitik ist eine Menge von Filterregeln
- Je mehr Möglichkeiten die Angabe von Filterregeln bietet, desto feiner kann Netzverkehr beschrieben und unterschieden werden
- Aber: desto schwieriger wird es auch, unerwünschten Verkehr garantiert zu beschränken

Was ein Firewall kann...

- Den Datenverkehr analysieren, z.B.
  - Filterregeln basierend auf IP-Adresse und/oder Portnummer
  - Filterregeln basierend auf den Inhalten der Pakete (also Auswertung höherer Schichten)
- Nicht akzeptablen Verkehr beschränken (=verwerfen)
- Den Netzverkehr protokollieren
- Zusätzlich evtl. Analyse und Intrusion Detection

Was ein Firewall nicht kann...

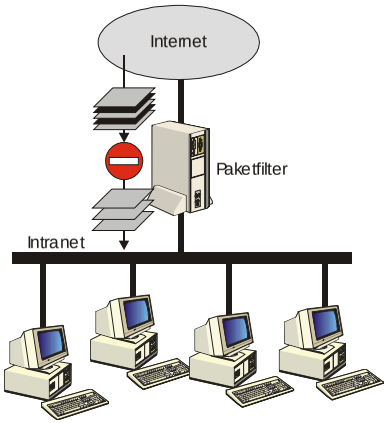
- Kein Schutz gegen bösartige „Insider“
- Kein Schutz gegen Verkehr, der gar nicht durch Firewall geht (z.B. Modemzugang)
  - Zusätzliche Netzzugänge sollten daher vermieden werden oder ebenfalls über Firewall geroutet sein
  - Speichermedien (CD-ROM, Disketten, ...) sind wahrscheinliche Mittel, um relevante Informationen zu transportieren
- Kein Schutz gegen unbekannte Bedrohungen
- Kein wirklicher Schutz gegen Viren / Würmer / Trojanische Pferde
  - Denn diese stellen „reguläre“ Daten dar, die übertragen werden
- →Firewalls können nur funktionieren, wenn sie Teil einer betreiberweiten Sicherheitsarchitektur sind!

Architektur von Firewalls

- Ein Firewall kann aus verschiedenen logischen Komponenten bestehen:
  - Paketfilter
  - Circuit Level Gateway
  - Application Gateway (Proxy Server)
- Realisierung in
  - Routern
  - Bastion Hosts
- Die einzelnen Komponenten müssen jedoch nicht unbedingt physikalisch auf verschiedenen Rechnern laufen

Paketfilter

- Analysieren Netzverkehr auf der Transport- und Netzwerkschicht
  - Filterung anhand IP-Adresse, Portnummer und Protokoll
- Als Paketfilter werden meist Router verwendet
- Paketfilter arbeiten sehr schnell
- Paketfilter sind transparent für den Benutzer

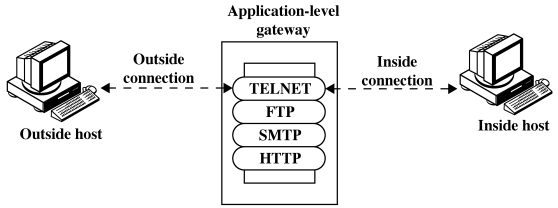


Vor- / Nachteile von Paketfiltern

- Vorteile
  - Zugriff auf Netzdienste geschieht völlig transparent
  - Die meisten Router unterstützen die Angabe von Filterregeln, sodass keine teure Zusatzhardware nötig ist
- Nachteile
  - Konfiguration sehr schwierig
  - Nachweis, ob das System wirklich nur gewünschten Verkehr durchlässt, ist oft schwer zu erbringen

Proxy Server

- = Application Gateways
- Erlauben Zugriff auf Dienste des Internet
- Zugriffe laufen nicht direkt, sondern mit dem Proxy Server als „Mittelsmann“ ab
- Kontrolle kann auf der Anwendungsebene stattfinden; d.h., evtl. können einzelne Anwendungskommandos verboten werden



Warum Proxy Server?

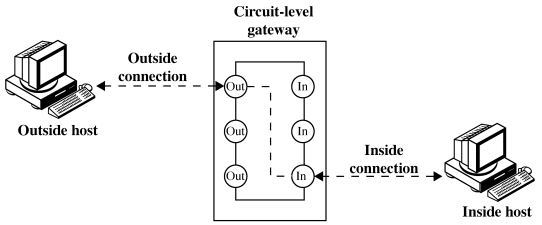
- Direkter Zugang zu Diensten im Internet bedenklich
- Einfache Lösung: nur ein gesicherter Rechner / Bastion Host wird ans Internet angeschlossen
- Aber: alle Benutzer müssten sich auf diesem Rechner einloggen, um die Dienste zu nutzen
- Proxy Server ermöglicht die Benutzung dieses gesicherten Rechners, aber ist transparent für den Benutzer

Vor- / Nachteile von Proxy Servern

- Vorteile
  - Transparenter Zugriff auf viele Dienste
  - Erlauben/Verbieten bestimmter Aktionen kann auf Anwendungsebene geschehen
  - Protokollierung wird einfacher
- Nachteile
  - Für viele Dienste ist keine Proxy-Funktionalität vorhanden
  - Installation von Proxy-Modulen für Dienste kann Sicherheitslücken öffnen
  - Z.T. müssen die Anwendungen Proxy-Funktionalität besitzen, um überhaupt einen Proxy-Dienst zu nutzen (also sind nicht alle Dienste transparent)
  - Proxy Server können ebenfalls nicht (oder nur teilweise) feststellen, ob die übertragenen Nutzdaten „böse“ sind (also Viren, Würmer oder trojanische Pferde beinhalten)

Circuit Level Gateway

- Es werden zwei TCP-Verbindungen aufgebaut.
- TCP-Segmente werden von einer zur anderen übergeben.
- Es findet keine Kontrolle auf Anwendungsebene statt.
- Sicherheit besteht in der Auswahl der zuzulassenden Verbindungen.
- Anwendung: für sichere Verbindungen nach draußen, geringerer Overhead als beim Application Gateway



Bastion Host

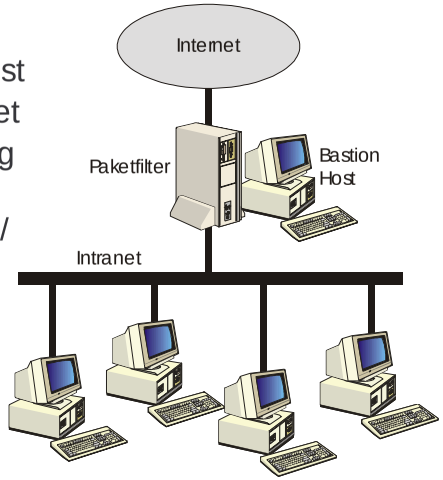
- Bastion Host repräsentiert das Intranet nach außen
- Bastion Host ist den Angriffen aus dem Internet ausgesetzt
- → Sicherheit äußerst wichtig
  - Konfiguration sollte möglichst einfach und übersichtlich sein
  - Jeder unnötige Dienst sollte entfernt werden
  - Es muss mit Angriffen gerechnet werden
  - Regelmäßiger Test auf Sicherheitslöcher mit entspr. Werkzeugen (etwa SAINT, Nessus, u.a.)
  - Entfernung aller Entwicklungs- und Installationswerkzeuge (Compiler, Make-Tools, etc.)

Firewall-Konfigurationen

- Oftmals bestehen Firewalls aus Kombinationen dieser Komponenten, die auf verschiedene Art und Weise angeordnet werden
- Bekannte Konfigurationen:
  - Dual-Homed Firewall
  - Screened-Host Firewall
  - Screened-Subnet Firewall

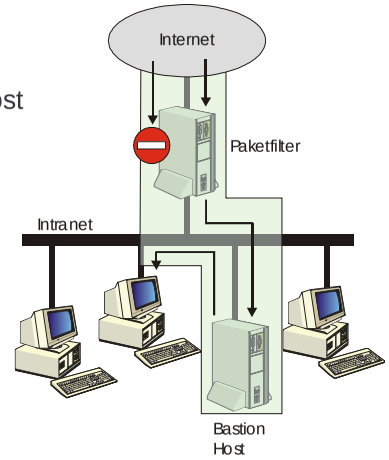
Dual-Homed Host Firewall

- Dual-Homed Host = Rechner, der mit zwei Netzwerken verbunden ist
- Hier: Internet und Intranet
- Keine direkte Verbindung zw. Inter- und Intranet
- Kommunikation nur von / zu Bastion Host möglich
- Oft in einem Rechner vereint
- Proxy-Funktionalität
- Aber: „Single Point of Failure“



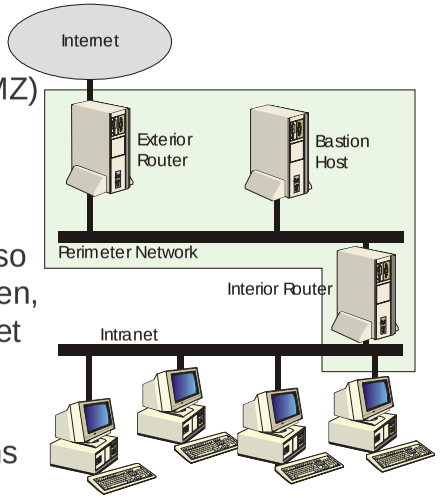
Screened Host Firewall

- Bastion Host hat nur noch Verbindung zum Intranet
  - Ist also kein Dual-Homed Host mehr
- Zusätzlicher Router als Paketfilter am Übergang Internet / Intranet
- Wird der Paketfilter überlistet, ist der Angreifer im Intranet
- „Single Point of Failure“



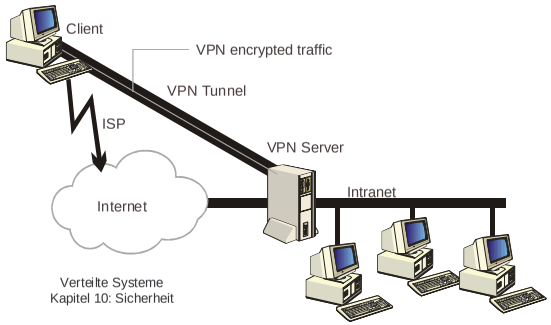
Screened Subnet Firewall

- Zwei Paketfilter/Router, dazwischen liegt die DeMilitarisierte Zone (DMZ) = Perimeter Network
- Bastion Host liegt in der DMZ
- Angreifer müssen nun also DREI Systeme überwinden, um Zugriff auf das Intranet zu bekommen
- → Lösung des „Single Point of Failure“-Problems



Virtual Private Network

- Gesicherte Verbindung über IP
  - aufbauend auf beliebiger IP-Verbindung (etwa über Modem, ISDN, DSL, DFN-Infrastruktur, ...)
  - also keine dedizierte Leitung notwendig → günstiger
- Darauf verschlüsselter VPN-Tunnel zwischen VPN-Client und Server



IPSec für VPN

- IPsec (secure Internet Protocol) wird als Tunneling-Protokoll verwendet
- Optional in IPv4, integriert in IPv6
- Schlüsselaustausch über Internet Key Exchange (IKE)
- Authentifizierung über Authentication Header (AH)
  - MD5 oder SHA-1
- Verschlüsselte IP-Pakete mittels Encapsulating Security Payload (ESP) Header
  - DES oder 3DES
  - Transportprotokoll-Header und -Daten verschlüsselt

PPTP für VPN

- Point-to-Point Tunneling Protocol (PPTP): Microsofts Äquivalent zu IPsec
  - Authentifizierung (PAP/CHAP)
  - Datenverschlüsselung (RSA RC4 Cipher)
  - Optional Datenkompression
  - PPTP tunnelt eine PPP-Verbindung

Weitere Protokolle zur Realisierung von VPN

- Transport Layer Security (TLS, RFC2246)
  - Ursprung in SSL (Secure Socket Layer)
  - Verschlüsselt TCP-Verbindungen
- Layer 2 Tunneling Protocol (L2TP, RFC2661)
  - Tunnelt PPP über UDP (oder andere nicht-IP Protokolle)
  - Daher alle Protokolle möglich, die über PPP übertragen werden können
  - Security: L2TP mit IPsec möglich (Internet Draft)

Literatur

- S. Fischer, U. Walther: *Linux Netzwerke*, SuSE Press, 2000.
- W. Stallings: *Network Security Essentials*, Prentice Hall, 2000.
- D. Chapman, E. Zwicky: *Building Internet Firewalls*, O'Reilly, 1995.
- R. Oppliger: *Internet and Intranet Security*, Artech House, 1997.
- ... und Clifford Stoll: Cuckoo's Egg – for fun ☺