Netzwerk-Sicherheit

Verschlüsselung, Vertraulichkeit, Authentisierung

Jörn Stuphorn
stuphorn@rvs.uni-bielefeld.de

Stand der Veranstaltung

13. April 2005	Unix-Umgebung
20. April 2005	Unix-Umgebung
27. April 2005	Unix-Umgebung
4. Mai 2005	ARP, ICMP, ping
11. Mai 2005	IP-Adressen & Subnetzmasken
18. Mai 2005	Einführung in Bridging, Routing, ...
25. Mai 2005	IOS, Spanning-Tree
1. Juni 2005	IOS Befehle, Brigding, Routing
8. Juni 2005	Statisches Routing
15. Juni 2005	UDP-, MTU- und IP-Fragmentierung
22. Juni 2005	TCP-Verbindungen und -Datenfluss
29. Juni 2005	DHCP und NTP
6. Juli 2005	NAT und Firewalls
13. Juli 2005	***Verschlüsselung, Vertraulichkeit, Authentisierung***
20. Juli 2005	*Sichere Anwendungen*

Wofür Netzwerk-Sicherheit?

- Netzwerk bedeutet Verbindung mit anderem Nutzerkreis
- Nutzerkreis nicht zwangsläufig vertrauenswürdig
  - Große Firma
  - Globales Netz
  - Netzzugang auch für Unbekannte
- Zum Nutzerkreis können auch Angreifer zählen
- Im Internet wird es Angreifer geben

- Nachrichten die zwischen 2 Hosts ausgetauscht werden können abgehört, abgefangen und modifiziert werden
  - Viele lokale Netzwerke sind Broadcast basiert
  - Bestimmte Router im Internet werden von vielen Netzsträngen verwendet

- Es gibt keine globale Kontrolle über alle Netze und Benutzer des Internets

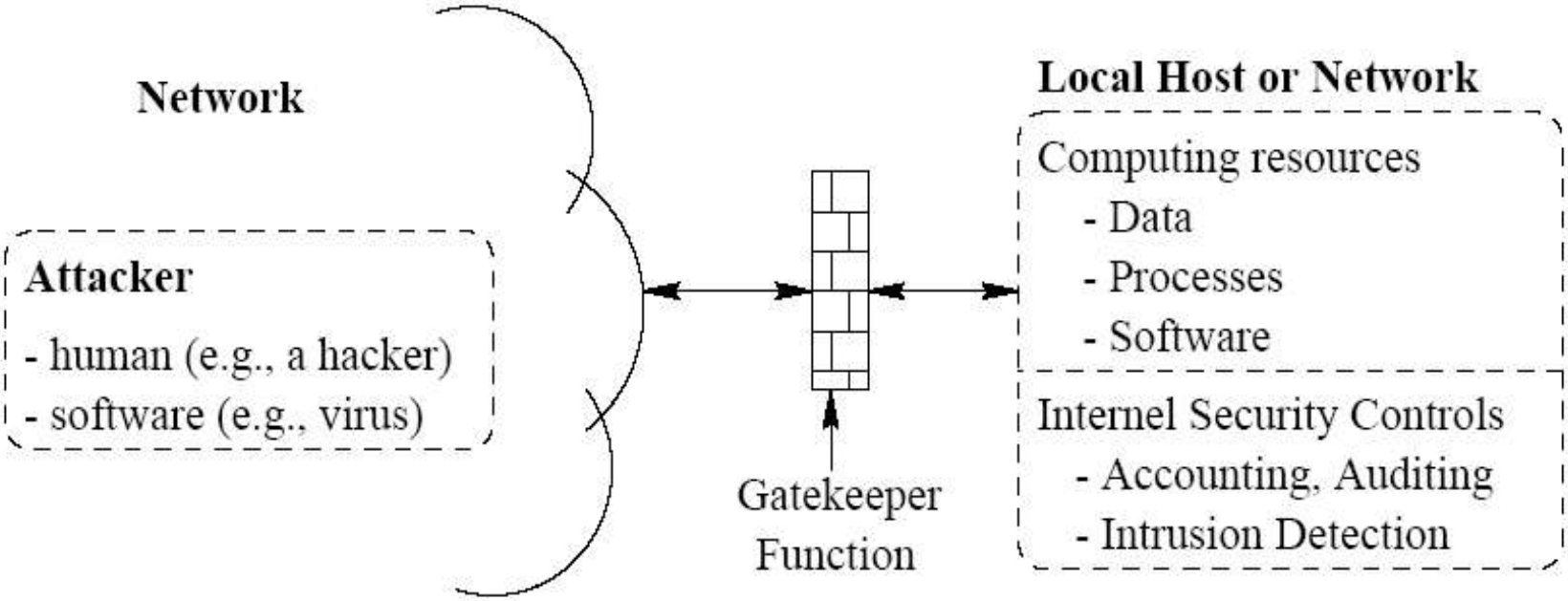
Wie erreiche ich Sicherheit?

- Zugriffssicherheit
  - Authentisierung
    feststellen der Identität des Benutzers
  - Autorisierung
    Zuordnung von Rechten zu einem Benutzer
  - Überwachung
    Überwachung der Verhaltensweise eines Benutzers
- Übertragungssicherheit
  - Vertraulichkeit
    Übertragung ist nur für Sender und Empfänger lesbar
  - Integrität
    Übertragung wird nicht verändert, Veränderung ist feststellbar
  - Unleugbarkeit
    Sender kann nicht leugnen die Nachricht gesendet zu haben
- Literaturempfehlung:
  - Andrew S. Tanenbaum, Computernetzwerke, 4. Auflage, Kapitel 8

Zugriffssicherheit

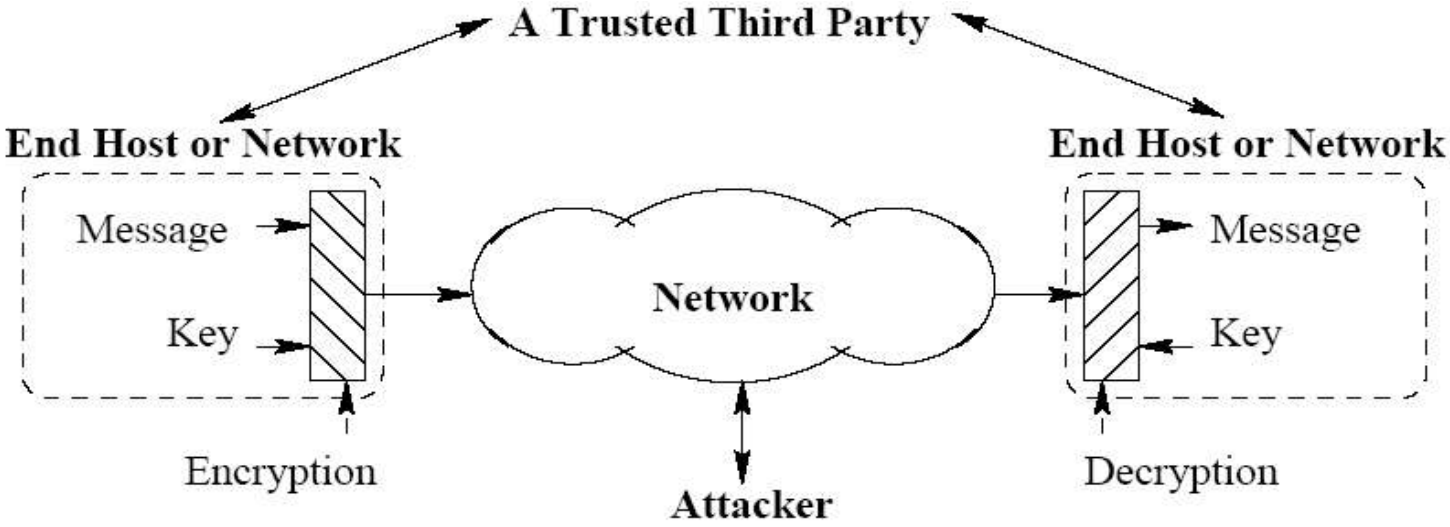
- **Authentisierung, Autorisation**

- Ein „gatekeeper“ schützt internes Netz vor Angriffen von außen
- Internes Netz besitzt Überwachungsfunktionen
  - Accounting (Aufzeichnung des Nutzungsverhaltens)
  - Auditing (Auswertung des Nutzungsverhaltens)



Übertragungssicherheit

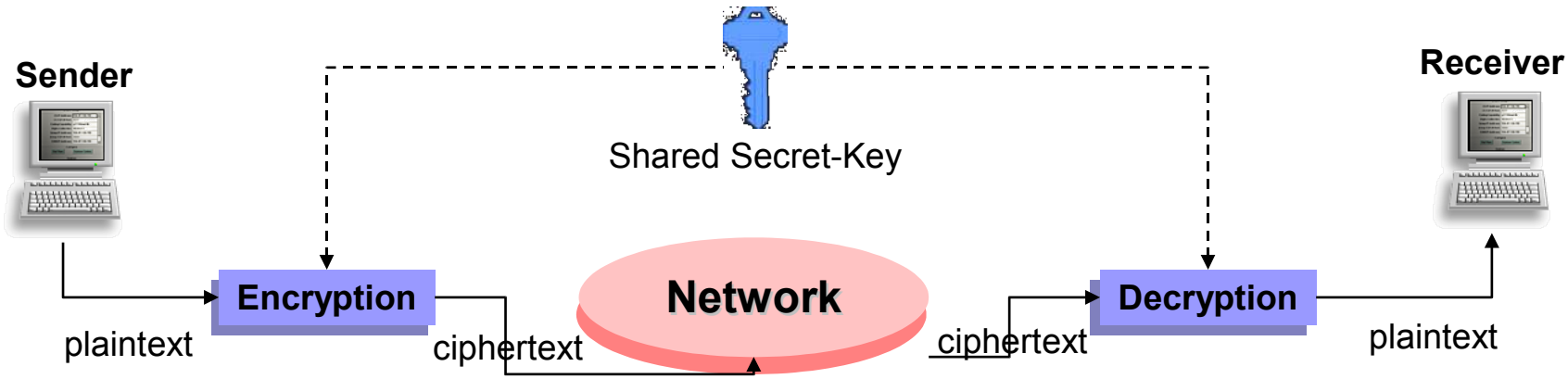
- **Vertraulichkeit (Confidentiality)**
- Der Sender
  - verschlüsselt die Übertragung mit einem Schlüssel
  - sendet die verschlüsselte Übertragung
- Der Empfänger
  - empfängt die verschlüsselten Informationen
  - benutzt einen entsprechenden Schlüssel um die Information zu entschlüsseln
- Verfahren ist sicher, wenn
  - die Schlüssel nur Sender und Empfänger bekannt sind
  - der Verschlüsselungsalgorithmus keine Schwächen hat



Verschlüsselungsarten

- Klassische Verschlüsselungsmethoden
  - Permutation
    die Anordnung der Zeichen des „plaintext“ werden geändert
  - Subsitution
    die Zeichen des “plaintext” werden gegen anderes Alphabet getauscht

- Das Modul, das Verschlüsselung liefert heißt Chiffre (Cipher)
  - Stream cipher
    Verschlüsselung erfolgt bit-für-bit oder Byte-für-Byte
  - Block cipher
    Algorithmus fasst Bits zu Block bestimmter Größe
    Kompletter Block wird zu ciphertext Block verschlüsselt



Schlüsselarten

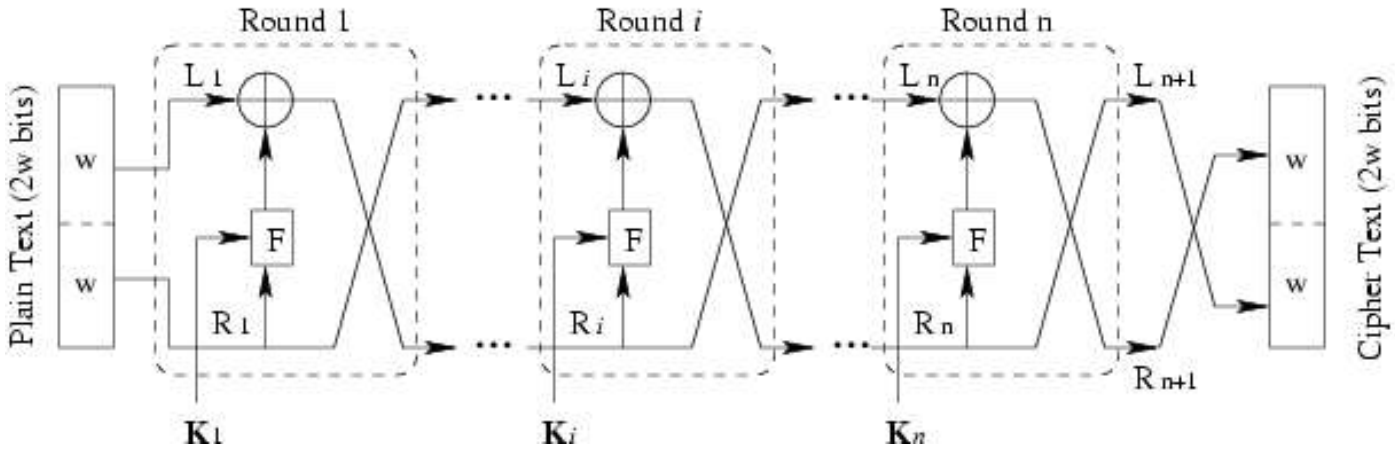
- Schlüssel werden benötigt für
  - Verschlüsselungsvorgang
  - Entschlüsselungsvorgang
- Chiffre mit symmetrischem Schlüssel
  - Sender und Empfänger besitzen den gleichen Schlüssel
  - Schlüsselaustausch muss über 2. Kanal erfolgen
  - Beide Parteien müssen dem 2. Kanal vertrauen
  - Verbreitetes Verfahren: AES, 3DES
- Chiffre mit unsymmetrischem Schlüssel
  public-key Verfahren
  - Unterschiedlicher Schlüssel für
    - Verschlüsselung und
    - Entschlüsselung
  - Verbreitetes Verfahren: PGP/GPG

Feistel Netzwerk Modell

- **Beispiel für Block-Chiffre Verfahren**

- Plaintext-Block (Länge 2w) wird in Chiphertext-Block (Länge 2w) verschlüsselt
- Der gleicher Verschlüsselungsvorgang (Round) wird mehrfach hintereinander ausgeführt (Chain)

- Operationen:
  - Der plaintext wird in 2 w-bit Blöcke gesplittet, L1 und R1
  - R1 wird mit geheimen Schlüssel K1 verschlüsselt
  - L1 XOR enc(R1) => R2
  - R1 wird zu L2



Advanced Encryption Standard

- **Beispiel für symmetrische Block-Chiffre**
- Nachfolger von DES (Data Encryption Standard)

- Block-basierte Chiffre (Rijndael Algorithmus)
  - Blocklänge und Schlüssellänge unabhängig voneinander
  - Mit Werten von 128, 192 oder 256 Bit
  - Jeder Block wird in eine 2D Tabelle mit vier Zeilen geschrieben
  - Zellen der Tabelle 1 Byte groß
  - Variable Anzahl an Spalten je nach Blockgröße (min: 4, max: 8)
  - Jeder Block wird nacheinander Transformationen unterzogen
  - AES wendet verschiedene Teile des Schlüssels nacheinander an

  - Die Anzahl dieser Runden (r) variiert abhängig von
    - Schlüssellänge (k)
    - Blockgröße (b)

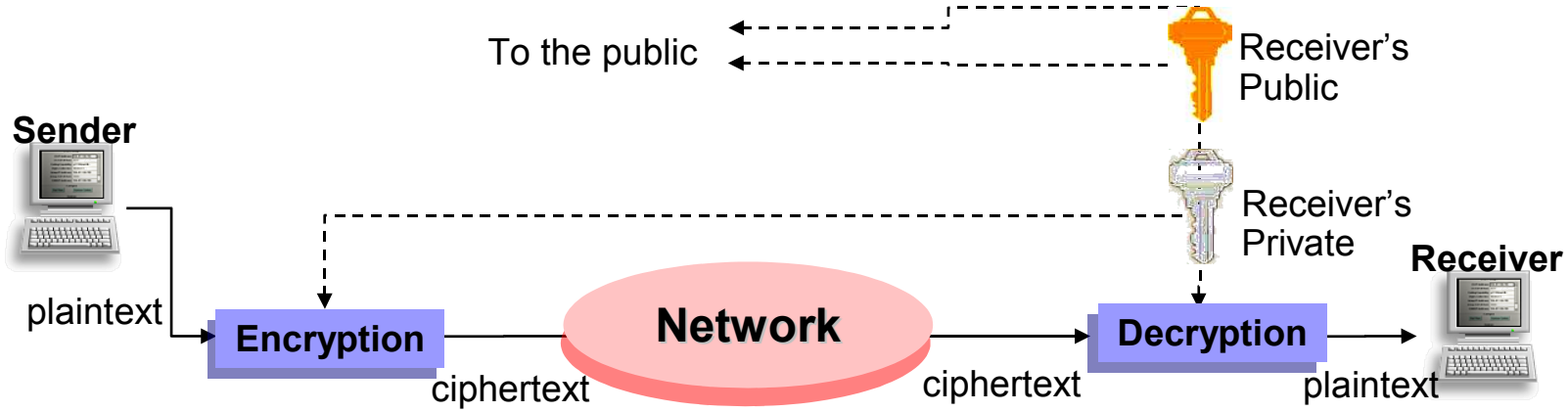
r	b = 128	b = 192	b = 256
k = 128	10	12	14
k = 192	12	12	14
k = 256	14	14	14

Ablauf von AES

- Schlüsselexpansion
- Vorrunde
  - KeyAddition ()
- Verschlüsselungsrunden (wiederhole solange runde<r)
  - Substitution()
  - ShiftRow()
  - MixColumn()
  - KeyAddition()
- Schlussrunde
  - Substitution()
  - ShiftRow()
  - KeyAddition()

Public-Key Verfahren

- 2 Schlüssel für jeden Empfänger
  - öffentlicher Schlüssel
  - privater Schlüssel
- Vorteile
  - öffentlicher Schlüssel kann problemlos über unsicheren Kanal übertragen werden
  - Empfänger benötigt nur 1 Schlüssel für alle Nachrichten
- Nachteile
  - Überprüfung, ob Schlüssel authentisch ist, ist notwendig
  - Algorithmus komplex

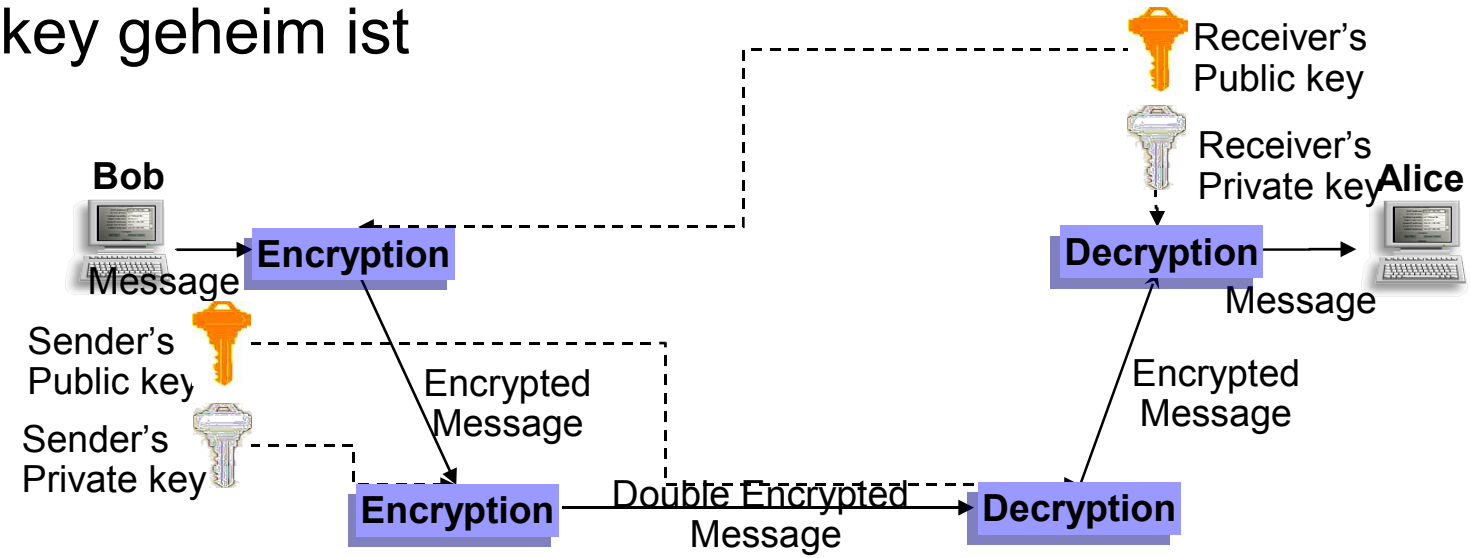


Verwendung von public-key

- Authentisierung
  - Bob verschlüsselt Nachricht mit eigenem private key
  - Bob sendet die verschlüsselte Nachricht an Alice
  - Alice entschlüsselt Nachricht mit Bob's public key
    - Alice weiß, dass Nachricht von Bob stammt
    - Jeder kann Nachricht entschlüsseln, da Bob's public key bekannt ist
- Vertraulichkeit
  - Bob verschlüsselt Nachricht mit Alice's public key
  - Bob sendet die verschlüsselte Nachricht an Alice
  - Alice entschlüsselt Nachricht mit eigenem private key

Verwendung von public-key

- Authentisierung und Vertraulichkeit
  - Bob verschlüsselt Nachricht mit
    - Alice's public key
    - eigenem private key
  - Bob sendet die verschlüsselte Nachricht an Alice
  - Alice entschlüsselt Nachricht mit
    - Bob's public key
    - eigenem private key
  - Alice weiß, dass Nachricht von Bob stammt
  - Nur Alice kann Nachricht entschlüsseln, da Alice's private key geheim ist



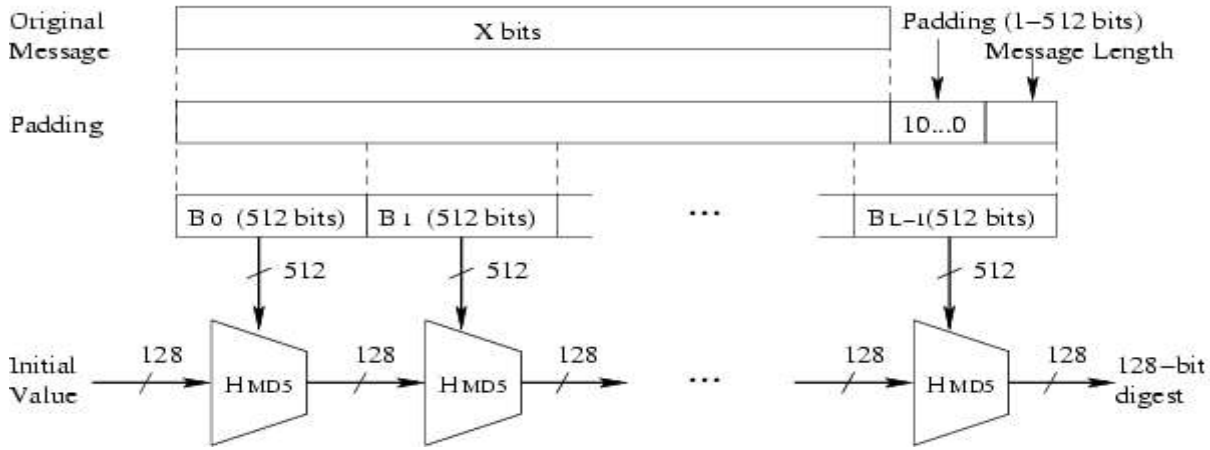
Hashing und Authentisierung

- Abbildung einer Nachricht variabler Länge auf einen Hashwert fester Länge
- Hashing ist nicht umkehrbar
  - Hashwert kann aus Nachricht berechnet werden
  - Die Nachricht kann anhand des Hashwertes nicht rekonstruiert werden
- Hashing kann einen Digest (Auszug) der Nachricht erzeugen
  - Message Authentication Code (MAC)
- Der Empfänger kann anhand des Digest feststellen, ob Nachricht authentisch ist
  - Empfänger erhält Digest, den Sender erzeugt hat
  - Empfänger erzeugt Digest der empfangenen Nachricht
  - Empfänger vergleicht Digest des Senders mit eigenem Digest

MD5

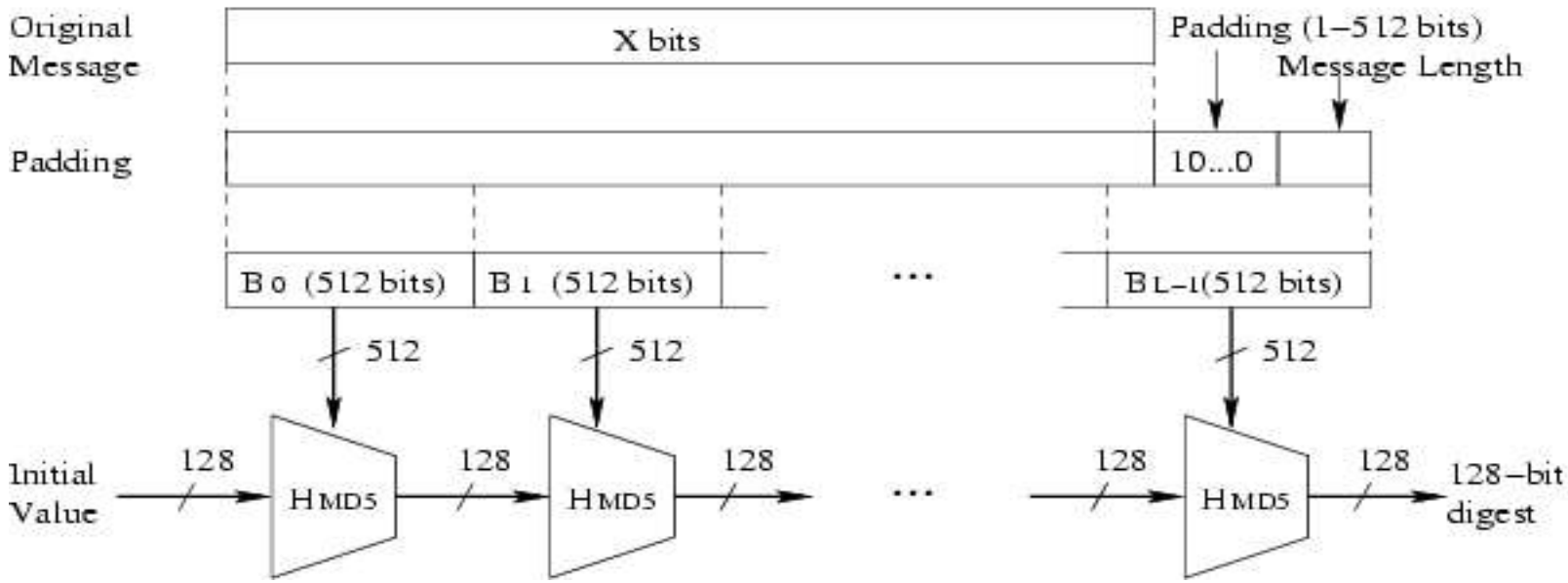
- Message Digest 5
- ehemals weit verbreitetes Hashingverfahren
- Inzwischen sind Methoden bekannt, gezielt gleiche MD5 Hashes für unterschiedliche Dateien zu erzeugen

- **Bemerkung:**
  - Es wird für jeden Hashalgorithmus möglich sein, für unterschiedliche Dateien den gleichen Hashwert zu erzeugen,
  - es sei denn, der Hashwert ist gleich lang, wie das optimal komprimierte Original.



MD5

- Message Digest 5
- Die Nachricht wird in 512bit Blöcke geteilt
- MD5-Algorithmus verbindet
  - 128bit Wert mit
  - 512bit Nachrichtenblock
- letzter Block wird durch „Padding“ auf 512bit gefüllt
- Ergebnis: 128bit Digest der Nachricht



Digitale Signatur

- Wenn sich Sender und Empfänger nicht vertrauen
  - Sender kann gesendete Nachricht nicht leugnen
- Überprüfung von Sendedatum und -zeit
- Authentisierung des Nachrichtenkontextes

- Digitale Signatur enthält (u.a.)
  - Digest der Nachricht
  - User ID
  - Timestamp

- Vorgang:
  - Sender erzeugt Nachricht mit angefügter Signatur
  - Nachricht wird verschlüsselt (symmetrisch oder asymmetrisch)
  - Nachricht wird gesendet, empfangen und entschlüsselt
  - Inhalt der Signatur wird überprüft

Sicherheitsimpelemtierung

- Sicherheit kann durch Implementation auf unterschiedlichen Layern gewährleistet werden
- Application Layer
  - ssh
  - Kerberos
- Transport Layer
  - SSL
- Network Layer
  - IPsec

Application Layer Sicherheit

- Secure Shell Protocol (SSH)
  - Wird ältere Methoden für entfernten Zugriff ersetzen
    - telnet
    - ftp
    - rcp
  - Unterstützt viele (nahezu alle) Verfahren mit Public-Key Algorithmus
  - Unterstützt viele Authentisierungsverfahren
  - ssh Client und Server benutzen digitale Signaturen um ihre Identität zu verifizieren
  - Die gesamte Kommunikation zwischen Client und Server ist verschlüsselt

Application Layer Sicherheit

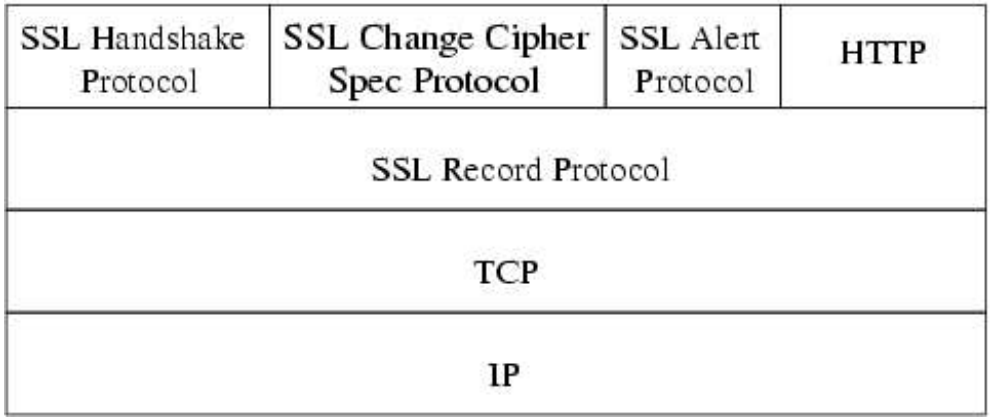
- Secure Shell Protocol (SSH)
  - Sicheres Arbeiten mit entferntem Host über unsicheres Netz
  - ssh bietet Protokolle für
    - sicheres Anmelden auf einem entfernten Host
    - Weitere Dienste zum arbeiten mit entferntem Host
- Hauptkomponenten:
  - SSH-TRANS
    - Transport Layer Protocol
    - Serverauthentisierung
  - SSH-USERAUTH
    - Authentisiert einen Nutzer von der Client-Seite gegenüber Server
  - SSH-CONNECT
    - Verbindungsprotokoll
    - multiplexing des verschlüsselten Tunnels auf mehrere logische Kanäle

Application Layer Sicherheit

- Kerberos
  - Netzwerk Authentisierungs Protokoll
  - Verwendet Verschlüsselung mit symmetrischen Schlüssel
  - Authentisiert Benutzer für Netzwerk Dienste
    - z.B. als Authentisierung für WAP-Verschlüsselung
- Aufteilung
  - Authentication Server
  - Ticket Granting Server
  - 2 Arten von Erlaubnisse (Tickets) an Benutzer
    - Ticket-Granting Ticket
      einmal per Nutzer-Login
    - Service-Granting Ticket
      einmal per Service
  - Das Nutzerpasswort wird nicht übertragen und daher nicht 'sniffbar'.

Transport Layer Sicherheit

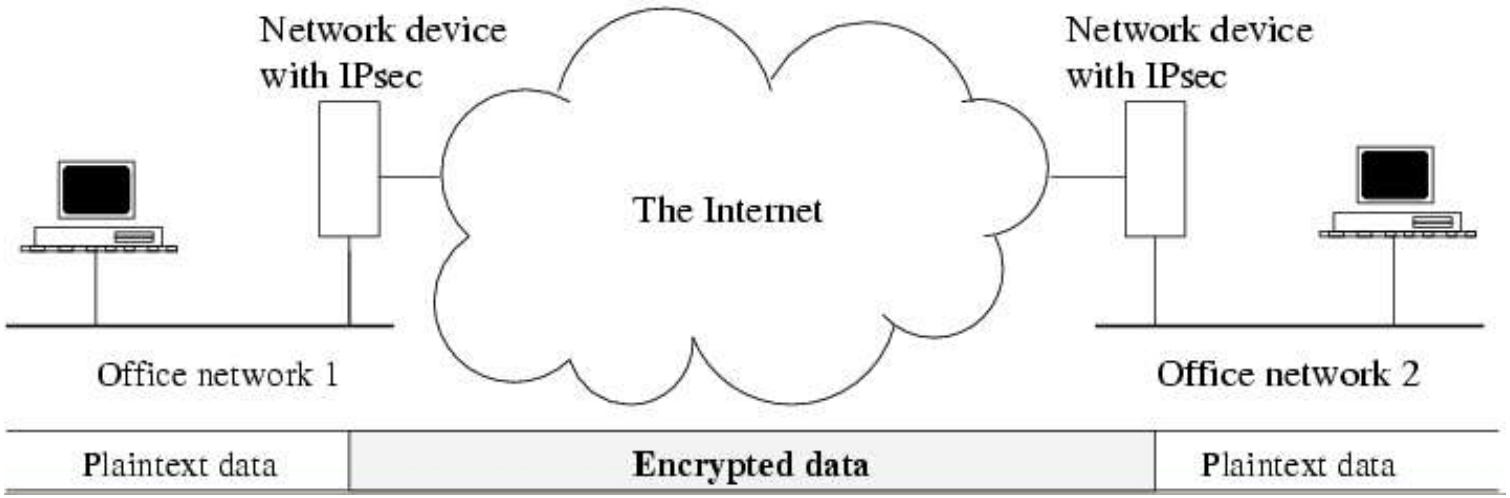
- Secure Sockets Layer (SSL) Protokoll
  - verschlüsselter Datenaustausch zwischen Client und Server
  - Verwendet TCP für Datenkommunikation
  - Unabhängig von Anwendungen des Application-Layers



  - Vier Protokolle:
    - SSL Handshake Protocol
      Authentisierung, Aushandeln des Algorithmus, Schlüsselaustauch
    - SSL Change Cipher Spec Protocol
      Aktualisiert verwendete Cipher für die Verbindung
    - SSL Alert Protocol
      Übertragung von SSL-bezogenen Warnungen
    - SSL Record Protocol

Network Layer Sicherheit

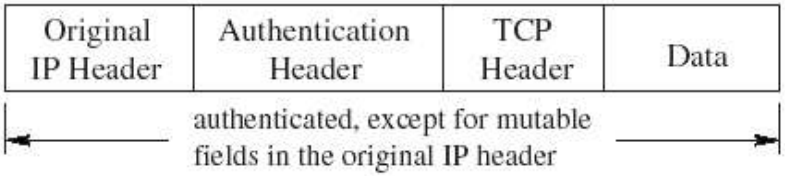
- IPsec – IP Security
  - Protokolle für
    - Authentisierung und
    - Vertraulichkeit
- Anwendung:
  - 2 Büros sind über Internet verbunden
  - 2 Gateways erzeugen sicheren Kanal über das Internet
  - Anwendungsinformation wird über sicheren Kanal übertragen
  - Auch VPN (virtual private network) genannt



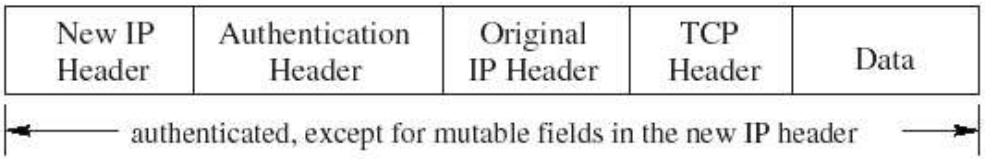
Network Layer Sicherheit

- 2 Protokolle
  - AH: Authentication Header
  - EPS: Encapsulating Security Payload
- 2 Modes:
  - Transport Mode
  - Tunnel Mode

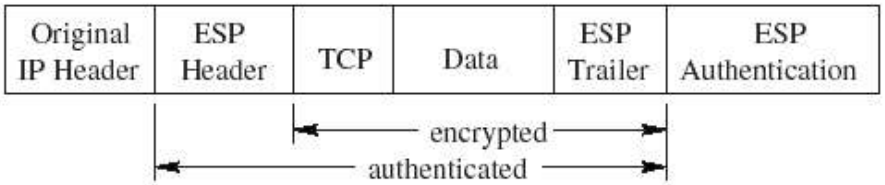
AH: Transport Mode



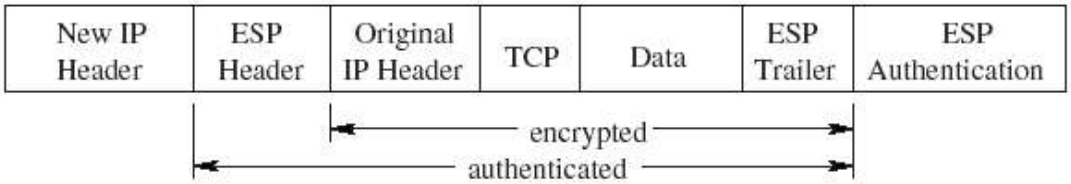
AH: Tunnel Mode



ESP: Transport Mode



ESP: Tunnel Mode



System Sicherheit

- Firewalls
  - blockt ungewünschten Verkehr von außen nach innen
  - hindert internen Nutzer an Zugriff auf unerwünschten externen Dienst
  - 3 Arten:
    - Packet filter (z.B. iptables)
    - Application gateway / Proxy Server
    - Circuit-level Gateway
- Auditing & Intrusion Detection
  - Unix/Linux protokolliert
    - Netzwerkereignisse und
    - Nutzeraktivität
  - Ein Eindringling kann durch Auswertung der Loginformationen entdeckt werden
    - Kontrolle aktiver Nutzer
    - Überprüfung von Netzwerkdiensten
    - „Tripwire“: Erkennnen von Änderungen in den Systemdateien
    - „Honey-Pot“: Datei, die für Angreifer interessant ist und Zugriff bremst