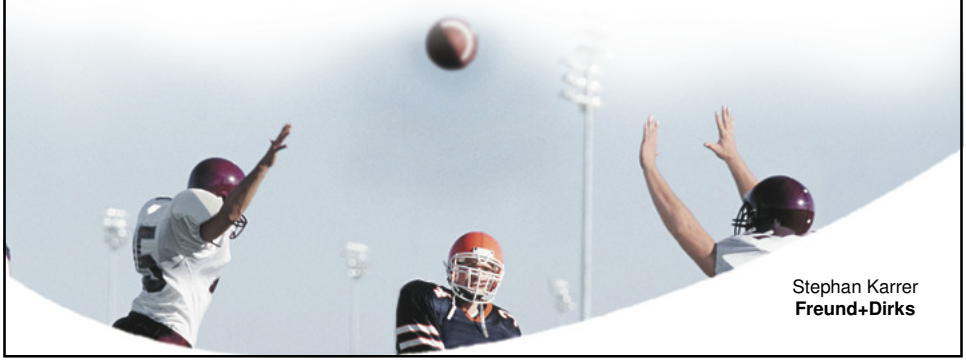
Freund+Dirks
Empowering IT-Professionals

Netzwerk-Grundlagen Sicherheitsaspekte



Stephan Karrer
Freund+Dirks

Freund+Dirks
Empowering IT-Professionals

Allgemeine Bedrohungen bei der Vernetzung von IT-Systemen

- Anzapfen von Kommunikationskanälen (wire tapping)
  - Abhören (passiv)
    → Verlust der Vetraulichkeit
  - Fälschen, Löschen oder Wiedereinspielen von Nachrichten
    → Verlust der Integrität
- Überlasten der Kanäle und Empfänger
  → Verlust der Verfügbarkeit
- Erweiterung der Menge der potentiellen Zugreifer (Subjekte)
  → Unerlaubte Nutzung
- Zusätzliche Verbreitungsmöglichkeiten lokaler Bedrohungen

Freund+Dirks
Empowering IT-Professionals

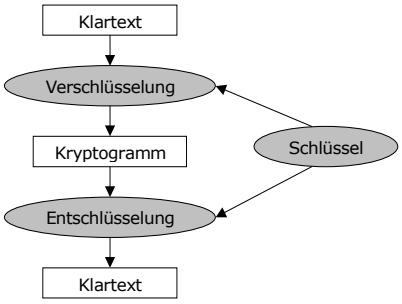
Ausflug zur Kryptografie

Kryptografische Verfahren ermöglichen:

- Geheimhaltung von Daten (Vertraulichkeit)
- Erkennung von Manipuationen (Integrität)
- Sichere Authentisierungsverfahren

Freund+Dirks
Empowering IT-Professionals

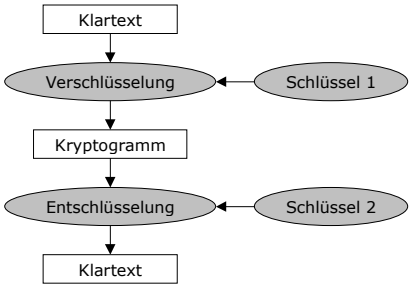
Symmetrisches Verschlüsselungssystem (Ein-Schlüssel-System)



- Sender und Empfänger benötigen den Schlüssel
- Es existieren Block- und Stromchiffren
- Sicherer Kommunikationskanal ist für den Schlüsselaustausch notwendig
- Beispiele: DES, Triple DES, AES, Blowfish, RC2, RC4, ...

Freund+Dirks
Empowering IT-Professionals

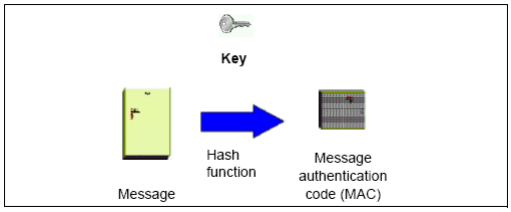
Asymmetrisches Verschlüsselungssystem (Zwei-Schlüssel-System, Public Private Key System)



- Trennung von Authentizität und Vertraulichkeit durch getrennte Schlüssel
- Häufige Anwendung: Systeme mit öffentlichen und privaten Schlüsseln
- Ermöglicht z.B: Digitale Signatur, Senden von vertraulichen Nachrichten unter Verwendung öffentlicher Schlüssel, Vertraulichkeit und Authentizität über einen unsicheren Kanal
- Nachteil ist schlechtere Performanz, deswegen hauptsächlich in Kombination mit symmetrischen Verfahren zum Schlüsselaustausch eingesetzt
- Beispiele: Diffie-Hellmann, RSA, Elgamal, ...

Freund+Dirks
Empowering IT-Professionals

„One Way Ciphers“



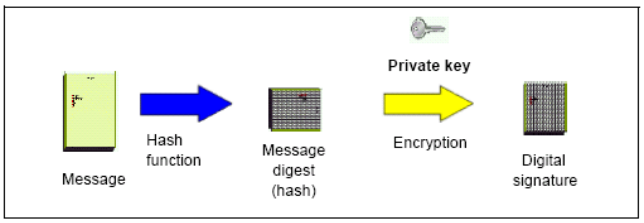
Quelle: IBM

Heute üblich sind kryptografische Hash-Funktionen (auch kryptografische Prüfsummen oder Message-Digest-Funktionen genannt)

Bsp: MD5, SHA-1, ...

Freund+Dirks
Empowering IT-Professionals

Digitale Signatur



Quelle: IBM

Geeignete Kombination der Mechanismen ergibt interessante Möglichkeiten

Freund+Dirks
Empowering IT-Professionals

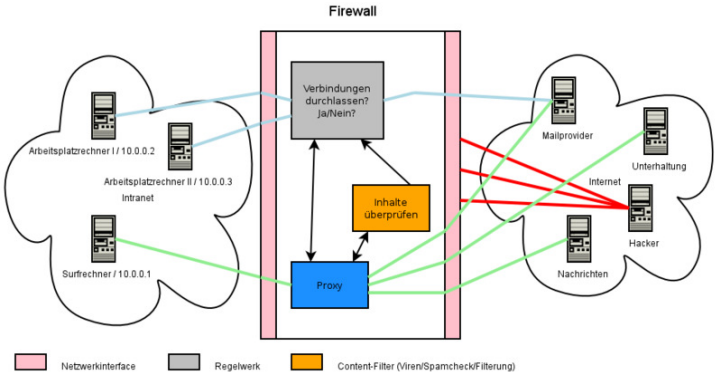
Eine Public-Key-Infrastruktur sollte im Minimum bereitstellen

- Digitale Zertifikate: Digital signierte elektronische Daten, die sich zum Nachweis der Echtheit von Objekten verwenden lassen
- Certification Authority: Organisation, welche die Bereitstellung von Zertifikaten übernimmt
- Registration Authority: Organisation, bei der Personen und Maschinen Zertifikate beantragen können
- Certificate Revocation Lists: (Sperrliste) Listen mit zurückgezogenen, abgelaufenen und für ungültig erklärten Zertifikaten
- Verzeichnisdienst: ein durchsuchbares Verzeichnis welches ausgestellte Zertifikate enthält (meist ein LDAP-Server)
- Validierungsdienst

Freund+Dirks
Empowering IT-Professionals

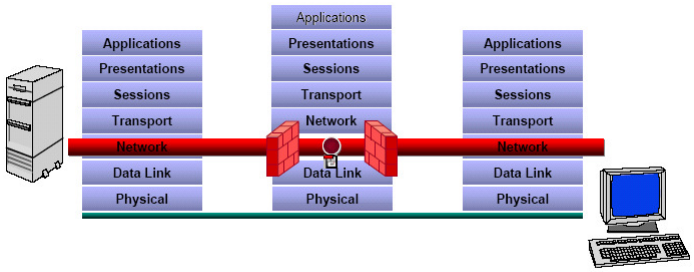
Ein paar Definitionen: Firewall

Firewall *Eine oder mehrere Komponente, die den Zugriff und den Datenverkehr zwischen 2 Netzen einschränkt und überwacht (oft zwischen Internet und Intranet)*



Freund+Dirks
Empowering IT-Professionals

Paketfilter: üblicherweise ein Router mit zusätzlichen Filtern

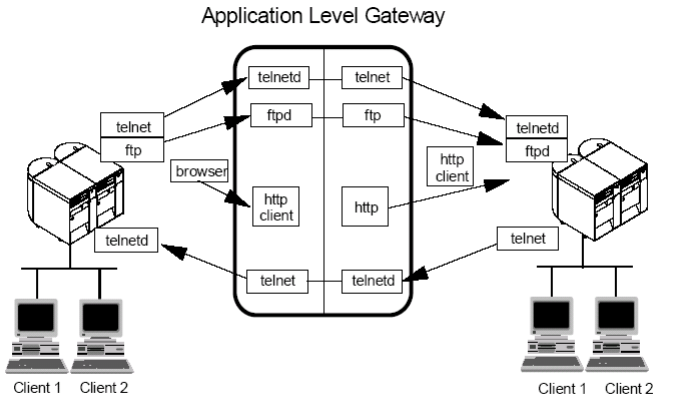


Quelle: Wolthusen

Screening Router, sofern er ein inneres Netz schützt.

Freund+Dirks
Empowering IT-Professionals

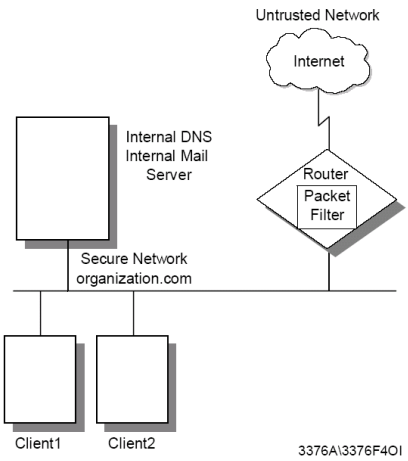
Proxy-System / Application Level Gateway



Quelle: IBM

Freund+Dirks
Empowering IT-Professionals

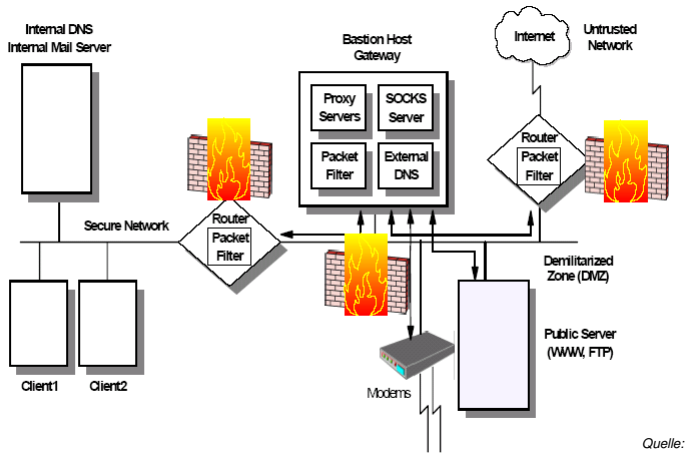
Einfacher Überwachungsrouter (screening router, screened subnet)



Quelle: IBM

Freund+Dirks
Empowering IT-Professionals

Screened Subnet Firewall



Quelle: IBM