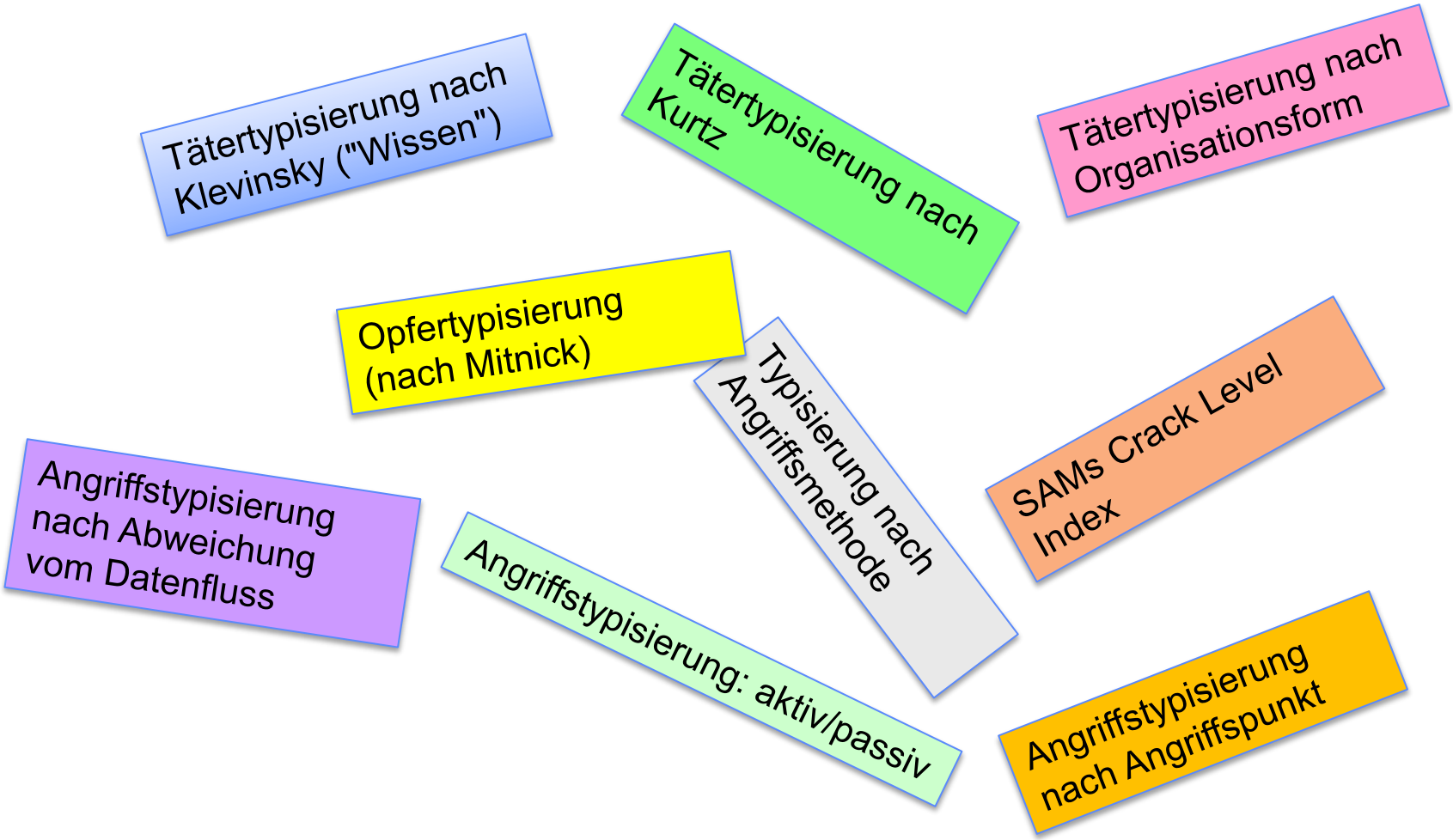
Modul 3: Opfer, Angreifer und Angriffe

- **Opfer, Angreifer und Angriffe**
  - Typisierungen und Kategorienbildungen
- **Beispiele von Angriffen auf Netze und Protokolle**
- **VorlesungsAddon: Social Engineering**

Opfer, Täter und Angriffe: Eine Vielzahl von Typisierungen und Kategorienbildungen



Opfertypisierung (nach Mitnick*)

- Unkenntnis des wahren Wertes von Informationen
  - Empfangspersonal
  - Sekretäre
  - Kundendienst
- Spezielle Privilegien
  - Systemadministratoren
  - Technischer Kundendienst
  - Wartungspersonal
- Hersteller, Lieferanten oder externe Dienstleister
  - Hersteller von Computer-Hardware und -Software
  - Entsorger
- Besondere Abteilungen
  - Personal
  - Buchhaltung

* Mitnick, K; Simon, W.: The Art of Deception – Controlling the Human Element of Security, 2. Auflage, Indiana 2003

Tätertypisierung nach Klevinsky ("Wissen")

- **First-Tier Hackers.**
  - **Sehr detailliertes Wissen über Netzprotokolle und OSI-Modell.**
  - **Harter Kern der Szene, verzichtet auf große Publicity.**
  - **Besitzt Fähigkeit neue Schwachstellen zu finden.**
  - **Schreiben automatisierte Werkzeuge, die zum Ausnützen der Schwachstellen benötigt werden.**
- **Second-Tier Hackers.**
  - **Wissensstand eines Systemadministrators.**
  - **Erfahrung im Umgang mit mehreren Betriebssystemen.**
  - **Verständnis von Arbeitsweise des TCP/IP-Protokolls.**
  - **Wissen Sicherheitslücken auszunützen.**
- **Third-Tier Hackers.**
  - **Haben Verlangen in die Systeme einzudringen.**
  - **Geringes technisches Wissen.**
  - **Verfügen über Werkzeug.**
  - **Leicht zu identifizieren, aber unberechenbar.**

Tätertypen nach verschiedenen Rollen:

- Cyberkriminelle
- Hacker
- Malware-Schreiber
- Botnetz-Betreiber
- Spammer
- Domain-Squatter
- Hacktivisten gegen Regierungen
- Regierungen gegen ihre Bürger
- Industriespionage
- Cyberterrorismus
- Cyberkrieg

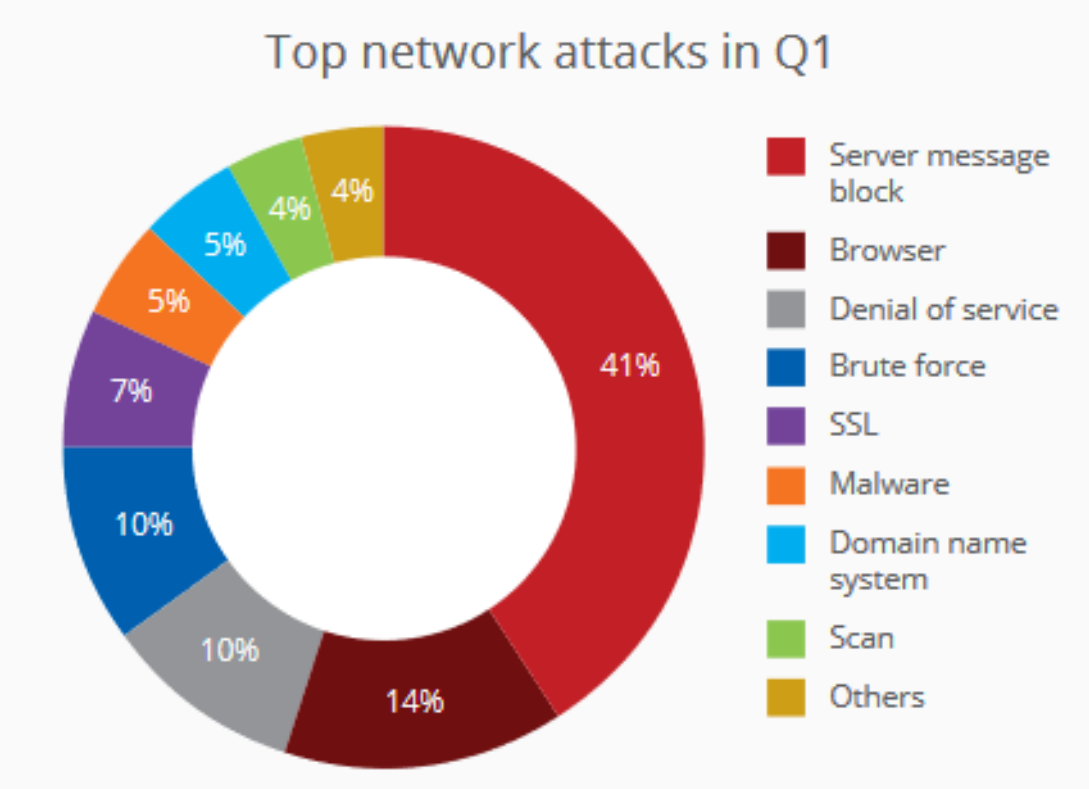
nach: Philipp Schaumann, https://sicherheitskultur.at/Angreifer_im_Internet.htm#class

Angriffstypisierung: aktiv/passiv

- **Passive Angriffe**
  - Analyse des Nachrichtenaufkommens
  - Abhören von Teilnehmer-Identitäten
  - Mitlesen von Nachrichten

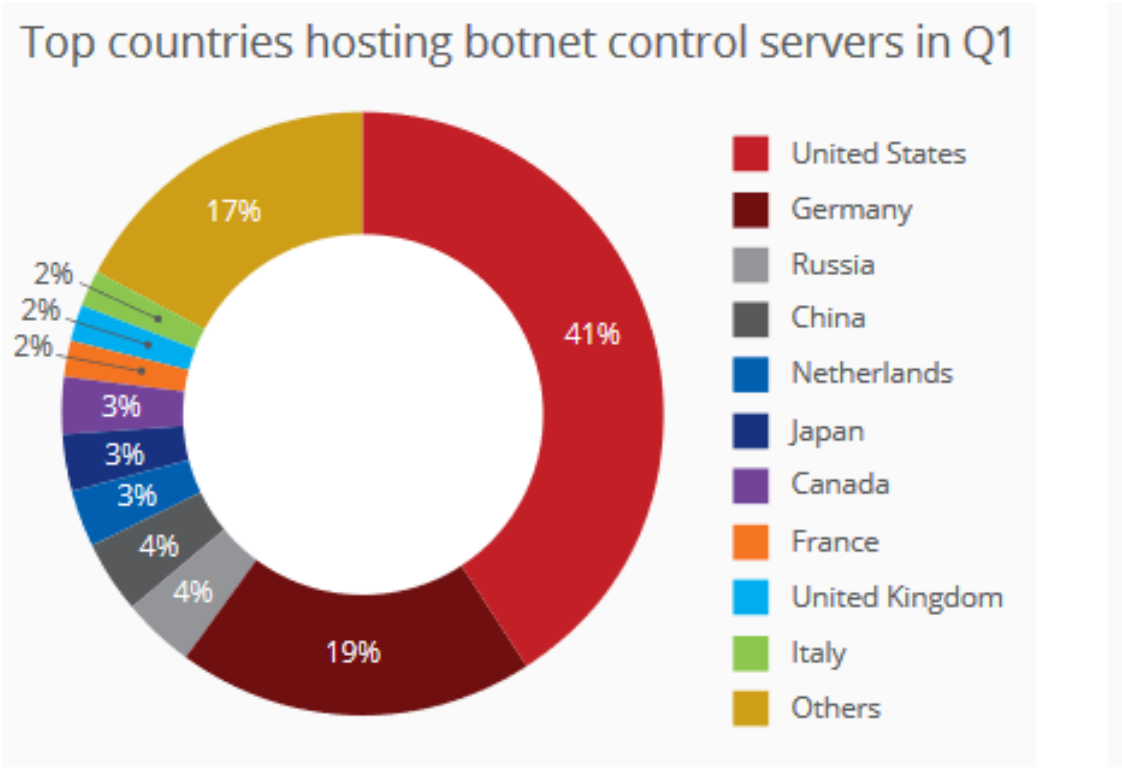
- **Aktive Angriffe**
  - Tarnung (Spoofing)
  - Denial of Service
  - Verändern von Nachrichten
  - Viren, Würmer, Trojanische Pferde

Top Netzangriffe im Q1/2018



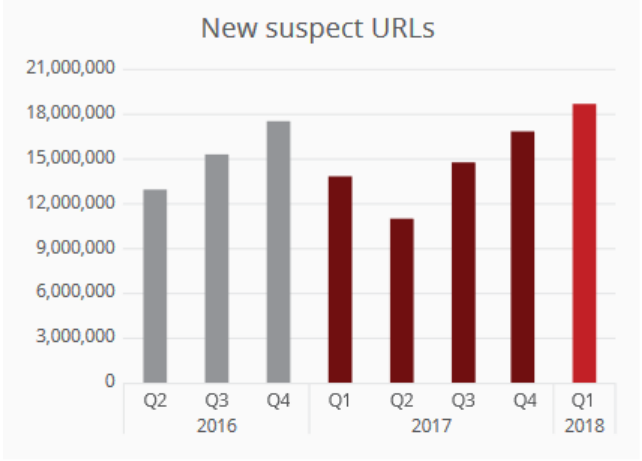
aus: McAfee Labs Threats Report, June 2018

Top Länder, die Bot-Netze hosten (Q1/2018)

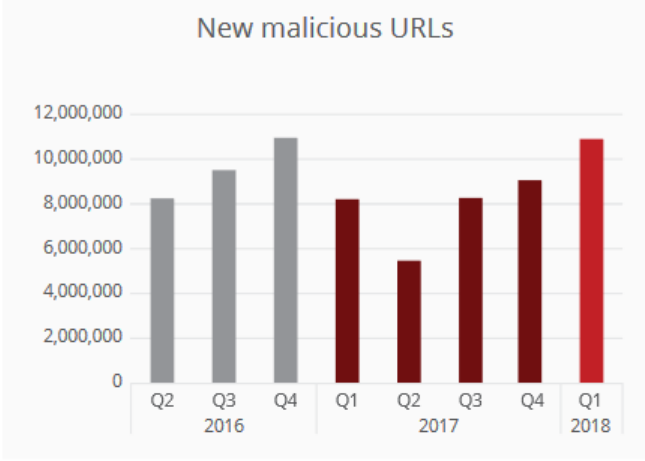


aus: McAfee Labs Threats Report, June 2018

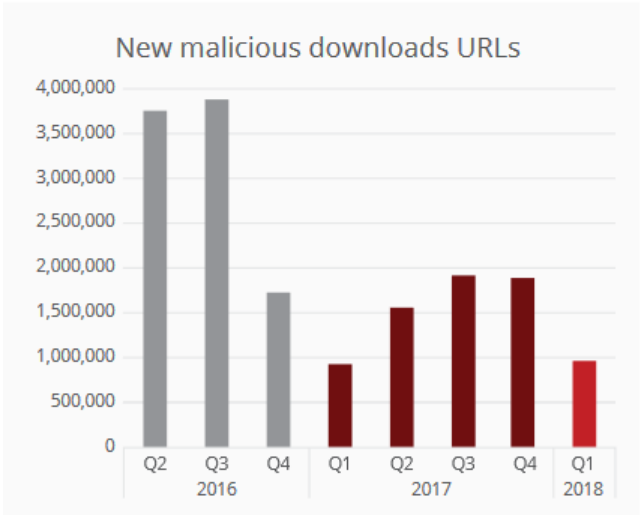
Web: Verdächtige und gefährliche URLs

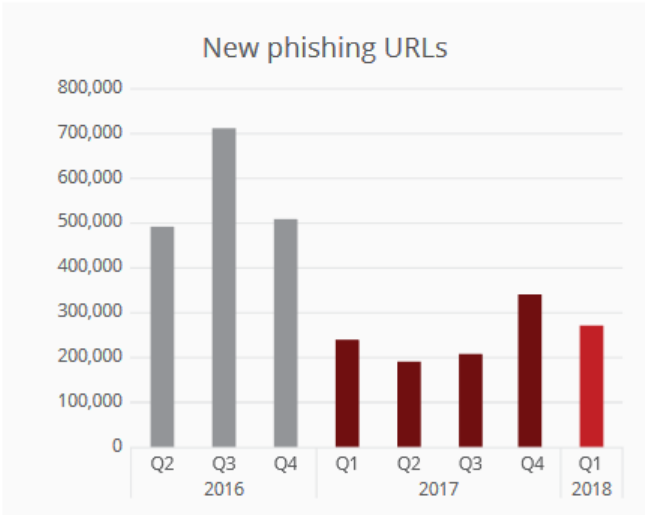


Source: McAfee Labs, 2018.



Source: McAfee Labs, 2018.





aus: McAfee Labs Threats Report, June 2018

Interaktive Websites

- **Größe des Datendiebstahls:**

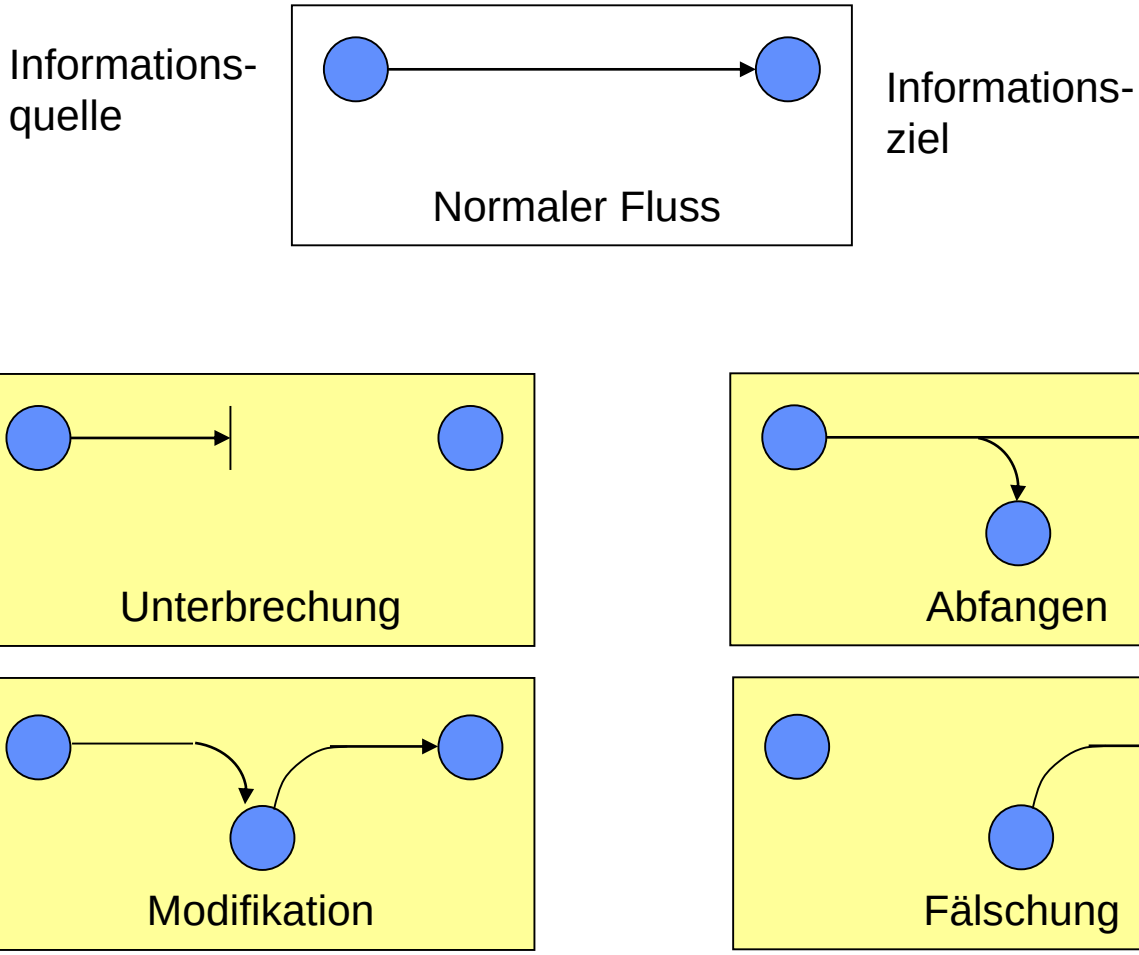
  World's Biggest Data Breaches
  http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

- **Animation,+Statistiken von Angriffen, Werbung in eigener Sache:**

  Kaspersky CYBERBEDROHUNG ECHTZEITKARTE
  https://cybermap.kaspersky.com/de/

- **Norse Attack Map:**
  http://map.norsecorp.com/

Angriffstypisierung nach Abweichung vom Datenfluss

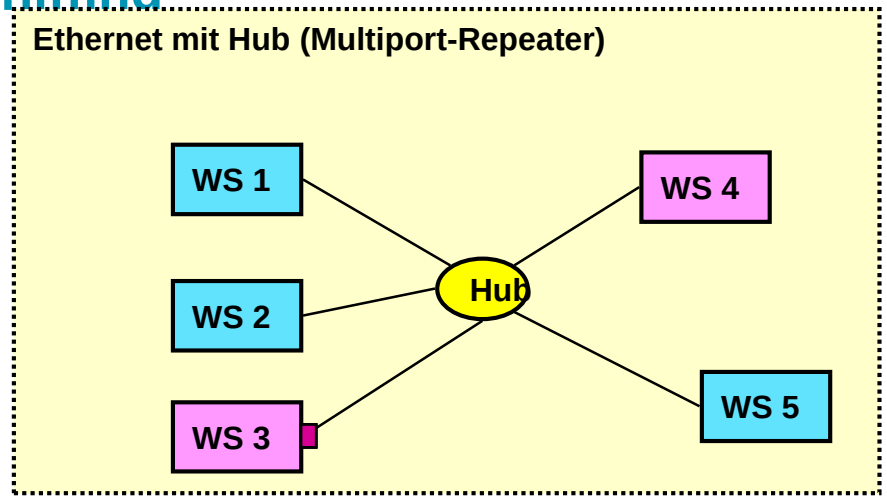


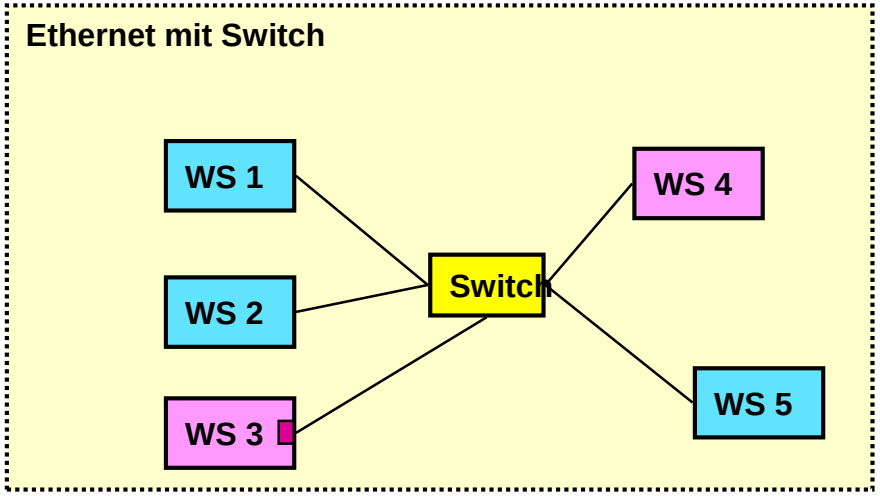
Klassifikation von Angriffen im Netz

	Unterbrechung	Abfangen	Modifikation	Fälschung
Anwendung (5/6/7)	Vielzahl von anwendungsspez. Angriffen			
Transport (4)	SYN-Flooding		Sequence Number Guessing	
IP (3)	Ping of Death Smurf (Ping-Flooding)		IP-Spoofing	
Datenüber-tragung (1/2)		Ethernet-Sniffing		ARP-Spoofing
Medium (0)				

Angriffsbeispiel: Ethernet-Sniffing

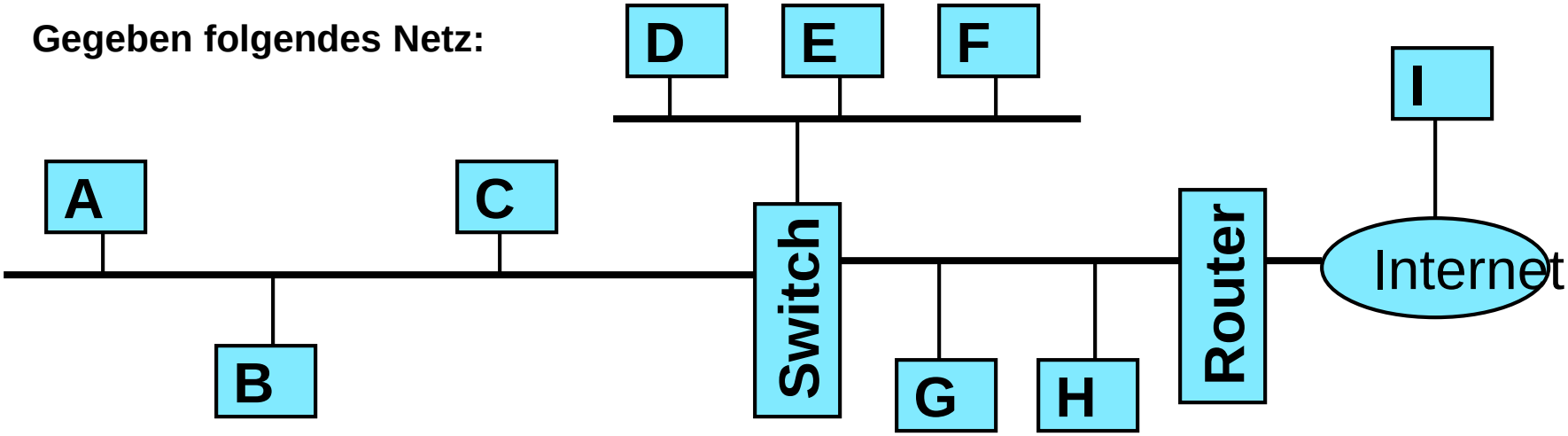
- Alle Station erhalten alle Paket von WS 03
- Ethernetkarte filtert Pakete
- Filter der Ethernetkarte kann abgeschaltet werden "promiscuous mode"
- Sniffing im Switched Ethernet erschwert
- Abwehr:
  - Schutz des Mediums
  - Ethernetkarte ohne "promiscuous mode" (*aber* Problem Laptop)
  - Segmentierung der Netze durch Switch/Router
  - Verschlüsselung





Angriffsbeispiel: Ethernet-Sniffing

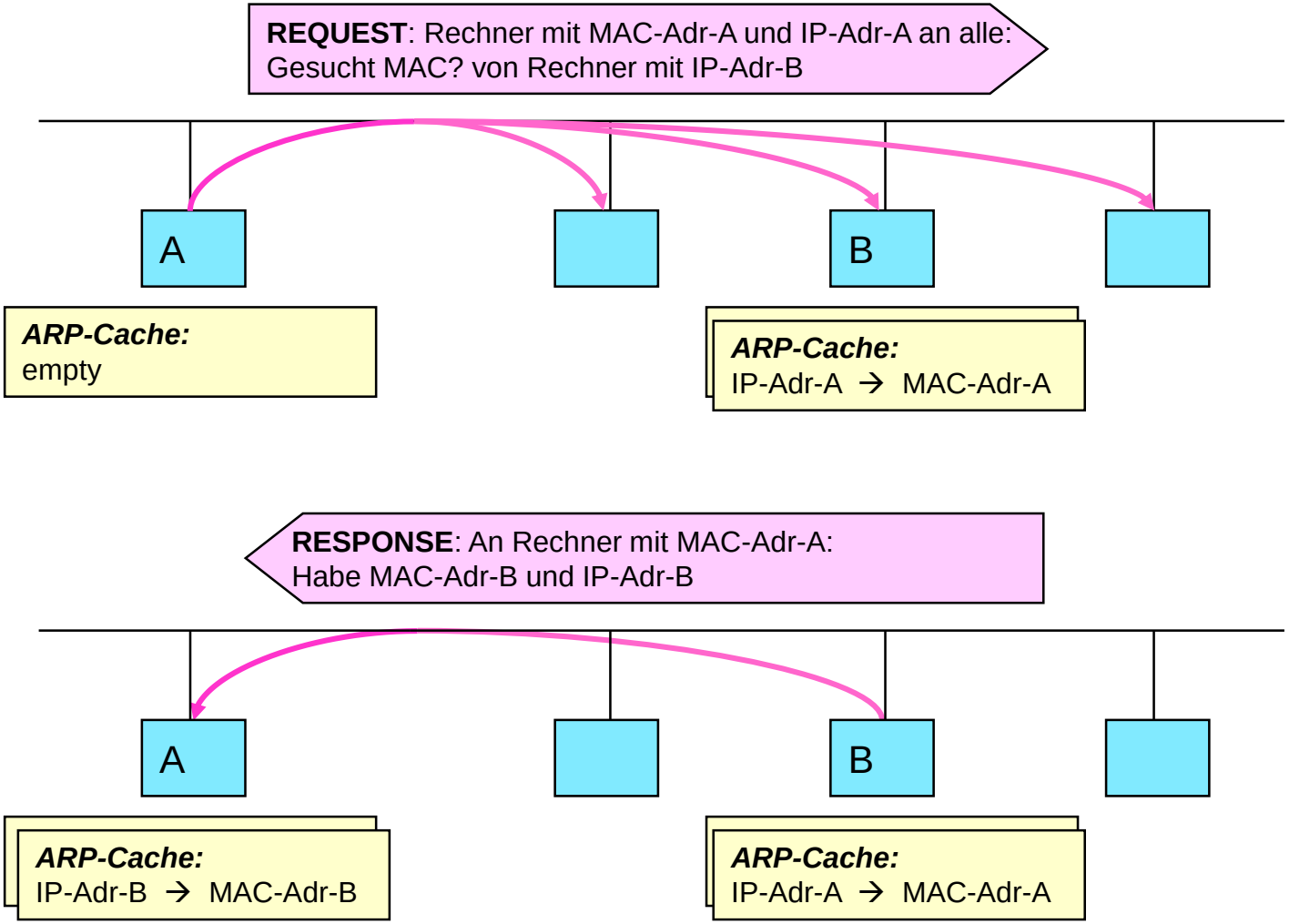
Gegeben folgendes Netz:



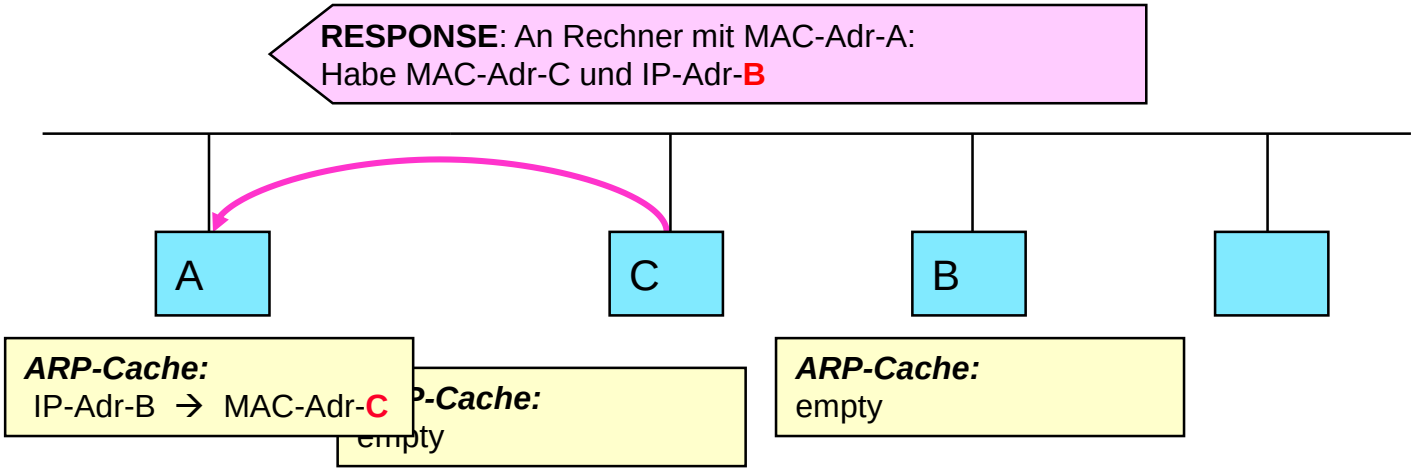
Szenarien:

- **B greift an. Welche Paket kann er sniffen?**
- **G greift an. Welche Paket kann er sniffen?**
- **Wie wirken sich Repeater, Brücken, Switches, Router, Firewalls auf den Angriff aus?**
- **Funktioniert Angriff auch von außerhalb des Firmennetzes?**

Wiederholung: ARP-Protokoll

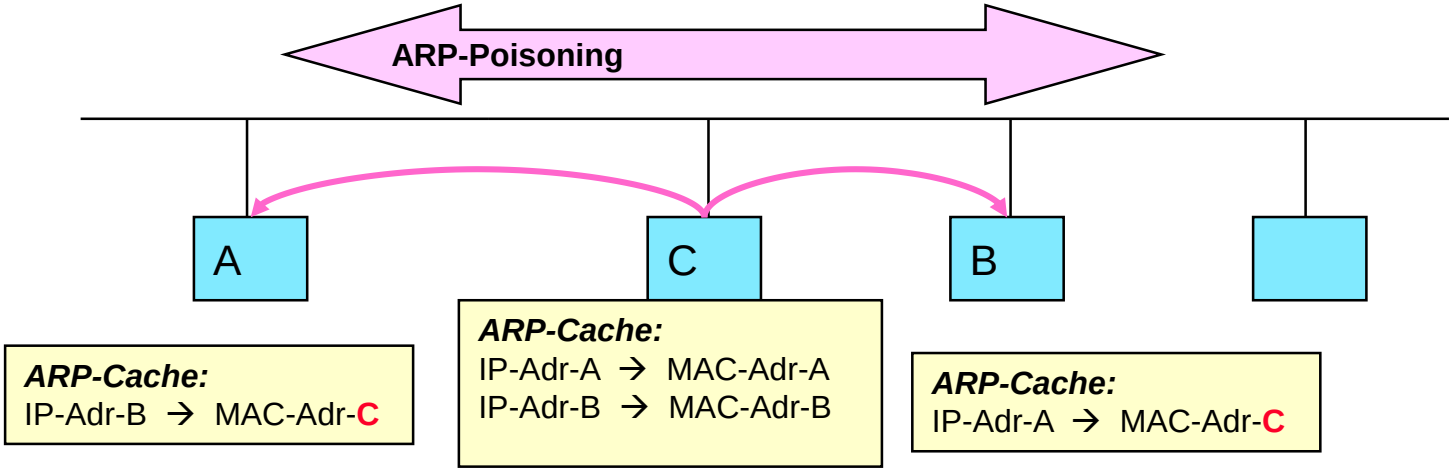


ARP-Poisoning



Angriffsbeispiel: ARP-Spoofing

- ARP-Caches der angegriffenen Rechner werden mit ARP-Responses präpariert.
- Pakete, laufen nun über Angreifer und können dort gesnifft / manipuliert werden.



Maßnahmen gegen ARP-Spoofing

- **Erkennen des ARP-Spoofings:**
  - periodische Abfrage der ARP Caches aller Maschinen durch ein Network Management System
- **Erschweren/Verhinderung des ARP-Spoofings:**
  - Gratuitous ARP (RFC3220) abschalten
  - Proxy ARP (RFC 1027) abschalten
  - statische Einträge in den ARP Cache
  - Benutzung eines dedizierten ARP-Servers
  - Einrichtung von Subnetzen
  - Nutzung von VPNs
- **Einsatz von Tools wie ArpWatch oder XArp: Monitoring der Änderungen der Zuordnung von Ethernetadressen und IP-Adressen**
  - Erstmaliges Erscheinen einer neuen Ethernetadresse
  - Wechseln der Zuordnung von der üblichen auf eine neue Zuordnung
  - Alarmiert Systemadministrator bei Auffälligkeiten per E-Mail

Angriffsbeispiel: Ping of Death

NT Versions Affected:

3.51, 4.0

Problem:

Large packet pings (PING -l 65527 -s 1 hostname) otherwise known as 'Ping of Death' can cause a blue screen of death on 3.51 systems:

STOP: 0X0000001E

KMODE_EXCEPTION_NOT_HANDLED - TCPIP.SYS

-OR-

STOP: 0x0000000A

IRQL_NOT_LESS_OR_EQUAL - TCPIP.SYS

NT 4.0 is vunerable sending large packets, but does not crash on receiving large packets.

Angriffsbeispiel: SYN-Flooding Attacke

- 1. Multiple TCP connection requests (SYN) are sent to the target computer with an unreachable source IP address.
- 2. On receiving the connection request, the target computer allocates resources to handle and track the new connection, then responds with a "SYN-ACK" to the unreachable address.
- 3. A default-configured Windows NT 3.5x or 4.0 computer will retransmit the SYN-ACK 5 times, at 3, 6, 12, 24, and 48 seconds. After the last retransmission, 96 seconds are allowed to pass before the computer gives up on receiving a response, and deallocates the resources that were set aside earlier for the connection. The total elapsed time that resources are in use is 189 seconds.

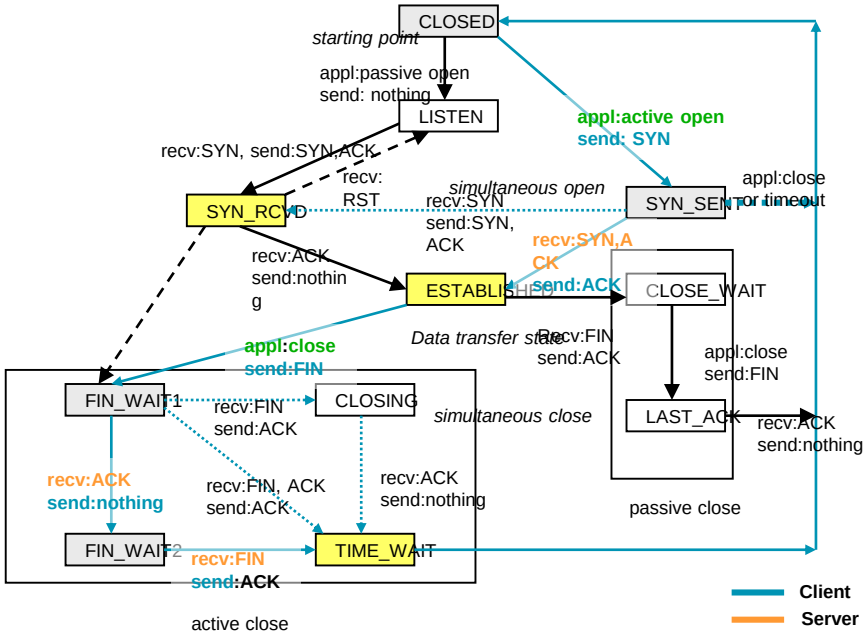
Quellen:

- thE_iNviNciblE@gmx.de: Kid2elite.de.vu - Hacking , Cracking , Exploits und mehr
- Mikrosoft: Internet Server Unavailable Because of Malicious SYN Attacks, http://support.microsoft.com/default.aspx?scid=142641

Erkennen von SYN-Flooding Attacken

- **netstat -n -p tcp**

Prot	Local Address	Foreign Address	State
TCP	127.0.0.1:1030	127.0.0.1:1032	ESTABLISHED
TCP	127.0.0.1:1032	127.0.0.1:1030	ESTABLISHED
TCP	10.57.8.190:21	10.57.14.154:1256	SYN_RECEIVED
TCP	10.57.8.190:21	10.57.14.154:1257	SYN_RECEIVED
TCP	10.57.8.190:21	10.57.14.154:1258	SYN_RECEIVED
TCP	10.57.8.190:21	10.57.14.154:1259	SYN_RECEIVED
TCP	10.57.8.190:21	10.57.14.154:1260	SYN_RECEIVED
TCP	10.57.8.190:2	10.57.14.154:1261	SYN_RECEIVED
TCP	10.57.8.190:21	10.57.14.154:1262	SYN_RECEIVED
TCP	10.57.8.190:21	10.57.14.154:1263	SYN_RECEIVED
TCP	10.57.8.190:21	10.57.14.154:1264	SYN_RECEIVED
TCP	10.57.8.190:21	10.57.14.154:1265	SYN_RECEIVED
TCP	10.57.8.190:21	10.57.14.154:1266	SYN_RECEIVED
TCP	10.57.8.190:4801	10.57.14.221:139	TIME_WAIT



Gegenmaßnahmen: SYN-Flooding Attacke

Problem:

- **Begrenzter Pufferbereich für (halboffene) Verbindungen.**

Gegenmaßnahme: SYN-Cookies (http://cr.yp.to/syncookies.html , 2005)

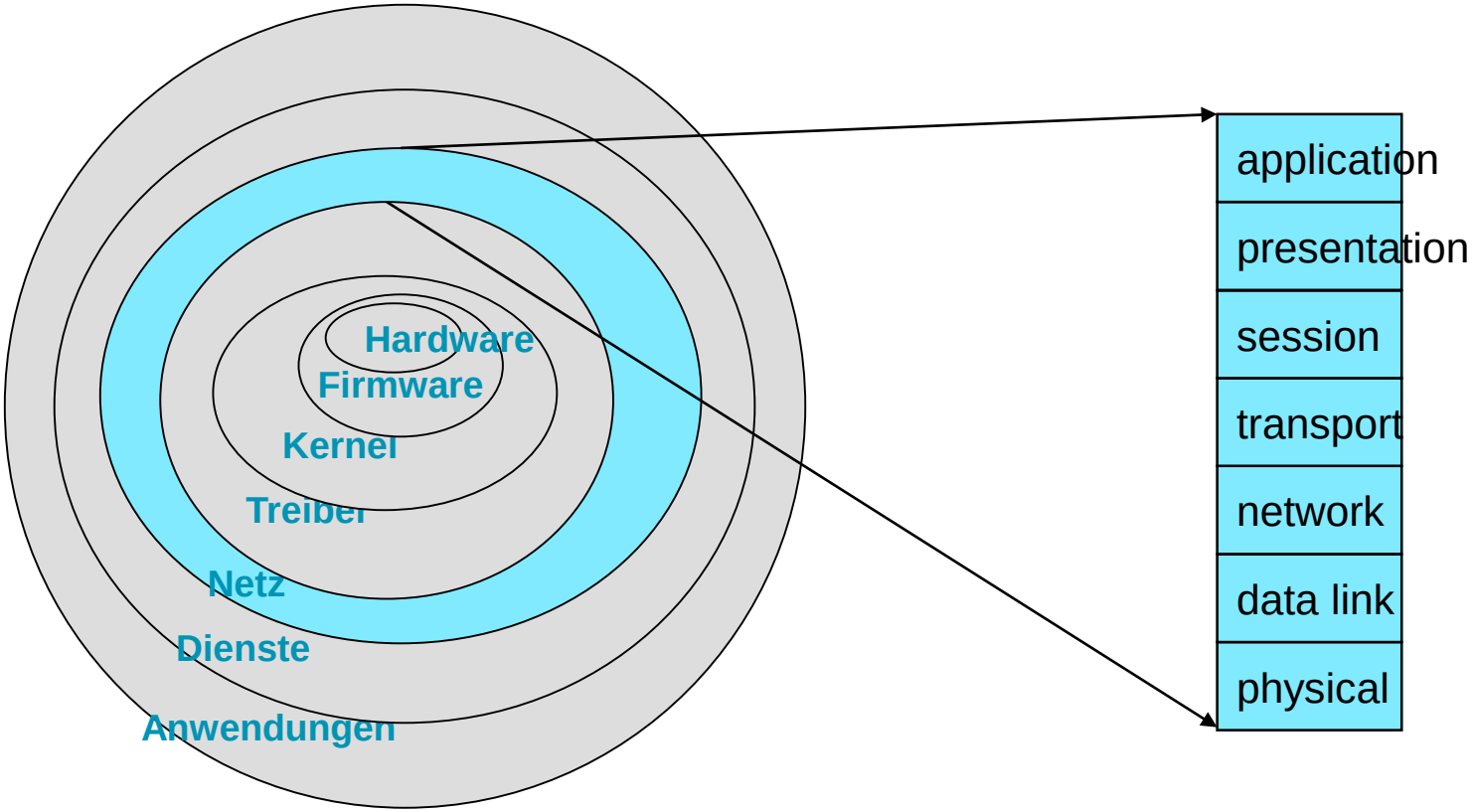
- **Server speichert keinerlei Informationen über ein erhaltenes SYN-Paket**
- **Server sendet Hashwert über wesentliche Infos aus dem SYN-Paket versteckt in der Server-Initial-Sequence-Number als SYN-Cookie an den Client**
- **Nimmt der Client die Verbindung an, kann der Server anhand der im SYN-Cookie enthaltenen Informationen feststellen, dass er mit diesem Client bereits gesprochen hat und die Verbindung herstellen.**

Behandlung in einem RFC:

Although SYN cookie implementations exist and are deployed, the use of SYN cookies is often disabled in default configurations, so it is unclear how much operational experience actually exists with them or if using them opens up new vulnerabilities. Anecdotes of incidents where SYN cookies have been used on typical web servers seem to indicate that the added processing burden of computing MD5 sums for every SYN packet received is not significant in comparison to the loss of application availability when undefended. For some computationally constrained mobile or embedded devices, this situation might be different.

- **RFC 4987: TCP SYN Flooding Attacks and Common Mitigations, Aug 2007**

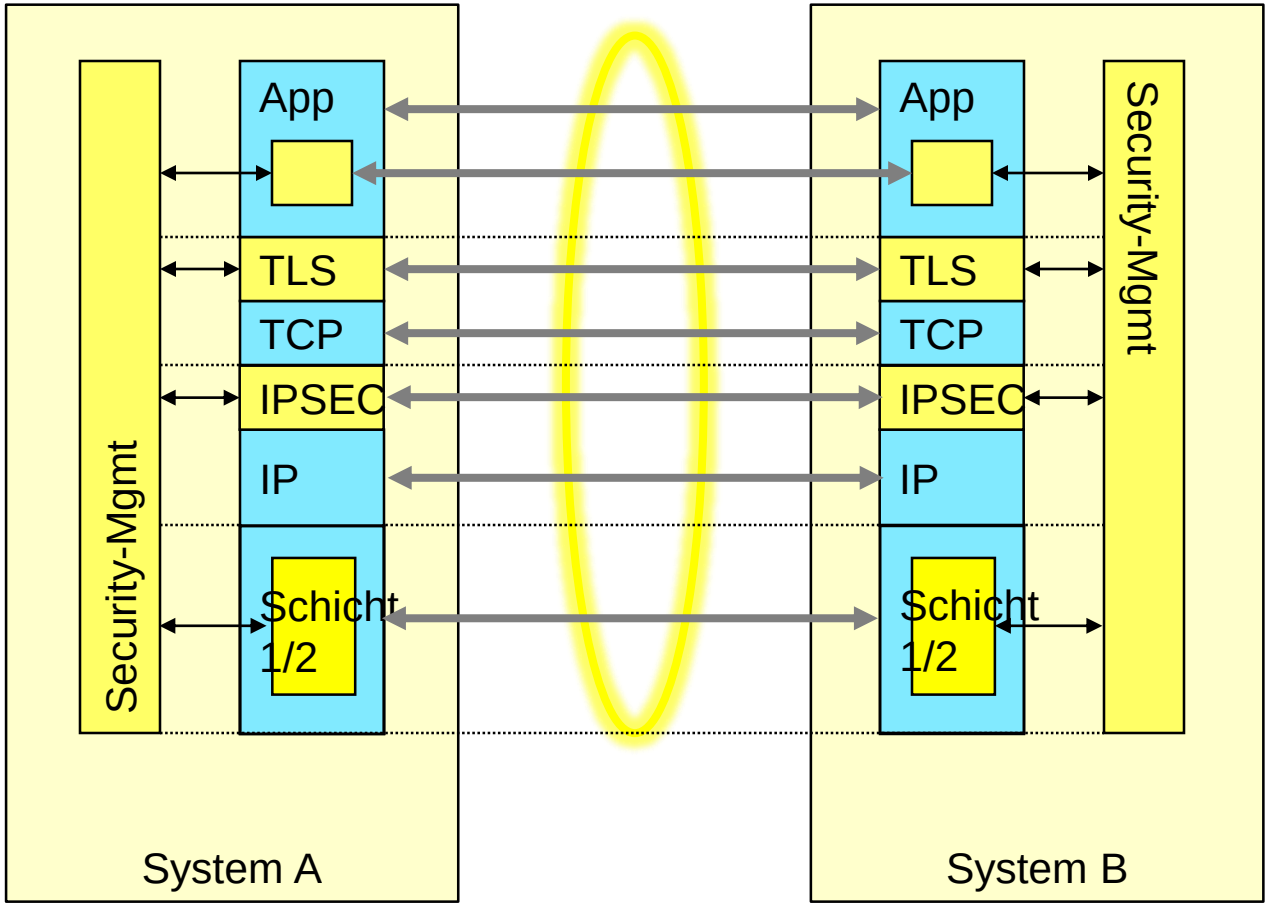
Zwiebelmodell der Schutzmechanismen (Privilegierung)



Zwiebelmodell der Schutzmechanismen

- Zuordnung von Angriffen zu Schichten
- Zuordnung von Gegenmaßnahmen zu Schichten

Sicherheit im Internet-Protokollstack



Ebenen der Sicherheit

- **sichere Applikationen, z.B. eCash, PGP. ("ich vertraue der Applikation")**
- **sichere Ende-zu-Ende-Verbindung ("ich vertraue dem sicheren Transport bis hin zu meiner Anwendung")**
- **sichere IP-Verbindung ("ich vertraue der Übermittlung über das Internet")**

- **Voraussetzung: Sicherheit in den Systemen**