

openHPI-Kurs: Wie funktioniert das Internet?
Internet als Angriffsziel

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut
Universität Potsdam

Erfolg des Internet macht es zum beliebten Angriffsziel

Internet und damit verbundenen Kommunikationstechnologien sind Schlüsseltechnologien der modernen Informationsgesellschaft

- Industrie und Wirtschaft machen reichlich Gebrauch von den Potenzialen der heutigen Kommunikationsmöglichkeiten; Popularität der vielen attraktiven kommerziellen und privaten Anwendungen macht das Internet zu einem globalen Markt

Kommerzielle Nutzung des Internets hat zu extremer Zunahme von Computer- und Cyber-Verbrechen geführt. Gefährdet sind:

- Computersysteme selbst
- Verbindungen und Systeme im Internet
- Abgeschlossene Intranets in Unternehmen

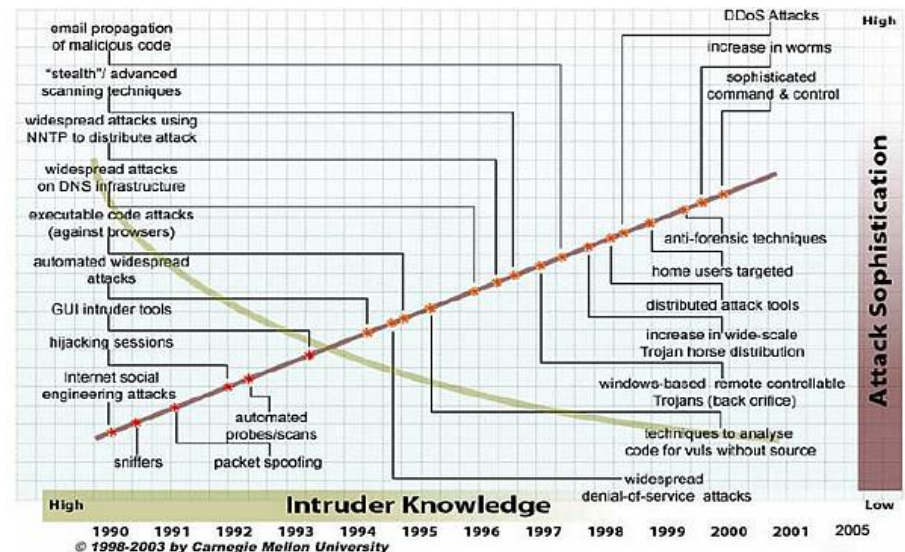
Internet ist ein einfaches Angriffsziel

Millionen miteinander verbundener Netzwerke bieten weltweit Milliarden von Zugangsstellen für Cyberkriminelle

Angriffe im Internet werden begünstigt durch

- Viele Design-Fehler in den Kommunikationsprotokollen
- Große Anzahl von Sicherheitslücken
- Einfacher Zugang zu Hacking-Tools
- Einfache Nutzung von Hacking-Tools
- ...

Ergebnis: Die Raffinesse der Angriffe steigt, während die von Angreifern erforderlichen Kenntnisse sinken



- Internet begann als Forschungsprojekt
 - kleine Forschungsgemeinschaft
 - überschaubares und vertrauenswürdiges Klientel
- Sicherheit war kein primärer Gesichtspunkt bei der Entwicklung von Internet-Protokollen
 - Typischer Satz in Internet-Standards/RFCs – Request for Comments:
"Sicherheitsfragen sind in diesem Memo nicht behandelt"
- Internet ist Verbund unabhängiger Rechnernetze, keine Internet-Behörde und keine staatliche Stelle kann das komplette Internet kontrollieren
- ...

Internet – viele Angriffspunkte

- Internet und internetbasierte Systeme bieten viele verschiedene Angriffspunkte und Risiken
 - bei den benutzten Computersystemen, z.B. PC, Laptop, Smartphone, Tablet, ...
 - bei der Anbindung an das Internet, in den Netzwerken und Zwischensystemen des Internets und
 - innerhalb von privaten Netzwerken, Unternehmen und Institutionen, die die Internet-Technologie in ihren Intranets nutzen
- Angriffe über das Internet sind einfach zu realisieren, mit relativ geringem Entdeckungsrisiko und schwer zu verfolgen
- Rasche Entwicklungszyklen bei Hardware- und Softwaretechnik hinterlassen Tausende von Schwachstellen und Angriffspunkten
 - **99% der Angriffe nutzen bekannte Schwachstellen aus !**

Verbesserte Chancen für Intrusion, also Einbrüche über das Internet

- Komplexität des Internet, seiner Protokolle und Anwendungen sowie Abhängigkeit vom Internet in Wirtschaft und Gesellschaft steigt ständig
- Angreifer sind gut vorbereitet und organisiert. Ihre Werkzeuge (Hacking Tools) sind immer ausgereifter, einfach zu bedienen und unterstützen massive Angriffe
- Vielfältiger Mangel an
 - Bewusstsein für Informationssicherheit
 - qualifiziertem Informationssicherheitspersonal, System- und Netzwerk-Administratoren
 - Regulierungen im globalen Internet und Machtmittel zur Durchsetzung gesetzlicher Vorgaben

Angriffspunkte beim IPv4-Protokoll

Internetprotokoll IPv4 ist äußerst erfolgreich bei der Kommunikation im Internet, hat jedoch auch Schwächen. So bietet IPv4 selbst z.B.

- keine Mechanismen zur Verschlüsselung
- keine Mechanismen zur Authentifizierung, also zur Feststellung der Identität des Senders

Deshalb kann beim Transport von IPv4-Paketen im Internet

- jeder beteiligte Rechner auf der Transportroute das Paket lesen und, schlimmer noch,
- das Paket manipulieren, bevor er es weiterschickt

Es ist leicht, IPv4-Pakete unter falschem Absender zu verschicken, indem im IP-Header eine falsche Absenderadresse angegeben wird

→ sehr beliebte Angriffsmethode **IP-Spoofing**

Angriffspunkte beim IPv4-Protokoll

Zum Beispiel: IP-Spoofing

Vortäuschung eines falschen Absenders, also das Versenden von IPv4-Paketen mit falscher Absender-IP-Adresse heißt → **IP-Spoofing**

Anwendungen:

- Überlistung von Sicherheitsüberprüfung durch Firewalls
- Erlaubt (fast) anonyme Angriffe auf Fremdsysteme, z.B.
 - Erzeugung von Überlast „**Denial of Service**“ (DoS)
 - unberechtigte Authentifizierung per IP-Adresse

Tools zum IP Spoofing:

■ Nmap, hping

Die genannten Applikationen sind zur Überprüfung der Netzwerksicherheit gedacht.

Jeglicher Angriff auf Geräte ohne Berechtigungen ist verboten und fällt unter den Straftatbestand der Computersabotage (§ 303b StGB)!

Maßnahmen für mehr Sicherheit

- Einsatz von **IPsec – Internet Protocol Security**
 - Protokollsuite zur Absicherung von IP-Kommunikation
 - Bietet für jedes IP-Paket **Verschlüsselungs-** und **Authentifizierungsmechanismen**
- Auch möglich: Verlagerung der Sicherheitsprüfung auf **höhere Schichten** im Protokollstapel
 - Auf der Transportschicht z.B.
 - bei TCP: Überprüfung der Sequenznummer
 - Auf der Anwendungsschicht z.B.
 - Paketfilter: Router filtert eingehende IP-Pakete aus externen Netzen, die vorgeblich aus internem Netz stammen
- Einsatz von → **VPN – Virtual Private Network**