



openHPI – Sicherheit im Internet Offenes Internet, unsichere Transportwege

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

Offenes Internet, unsichere Transportwege

Internet als Netz der Netze **ist offen**, die Transportwege sind jedermann zugänglich und per se nicht geschützt

- Jeder mit Zugang zum Internet kann das Internet nutzen
- Technologien basieren in überwiegenden Teilen auf offenen, jedermann frei zugänglichen Standards
- Internet ist kein privates Netz, Daten passieren auf ihrem Weg zum Ziel meist mehrere "fremde" Netzwerke

Das ist eine Situation, die Hacker einlädt, **Daten** bei ihrem Transport durch das Internet

- abzuhören, zu stehlen, zu manipulieren und
- unter falschem Namen im Internet ihr Unwesen zu treiben

In dieser Kurswoche werden wir zunächst daran erinnern,

- wie **Daten** im Internet übertragen werden und welche **Zwischensysteme** zum Einsatz kommen
- und welche Gefahren in den "**besonders offenen**" drahtlosen Netzwerken – **WLANS** – drohen

Dann wollen wir verschiedene **Gefahren** und **Angriffsmöglichkeiten** vorstellen, die auf diesem Design des Internets basieren

- **Eavesdropping** – das **Abhören** von Nachrichten und Datenpaketen auf ihrem (offenen) Transportweg
- **Spoofing** – das **Vortäuschen** einer falschen (Absender-) Adresse kann auf vielen verschiedenen Ebenen für Angriffe oder zu deren Verschleierung genutzt werden
- ...

Unser Programm für Kurswoche 4: Offenes Internet, unsichere Transportwege

Verschiedene **Gefahren** und **Angriffsmöglichkeiten**, die auf dem Design des Internets basieren:

- Bei **Man-in-the-Middle** Angriffen schaltet sich ein Angreifer in einer Internetverbindung zwischen die beiden Nutzer und liest und manipuliert die vertraulich übertragenen Daten
- **Dienste** im Internet (wie WWW, Email, ...) sind beliebte Angriffsziele und bieten gewieften Angreifern **Einfallstore** in Serversysteme

Aufgrund seines großen Erfolgs und der Verbreitung ist das WWW eines der beliebtesten Angriffsziele im Web

- **Schwachstellen in Browsern** erlauben es Angreifern, die Rechner/Geräte der Internetnutzer anzugreifen
- **WWW-Server** können durch Angriffe so manipuliert werden, dass sie selbst zu Angriffswerkzeugen werden

Unser Programm für Kurswoche 4: Offenes Internet, unsichere Transportwege



Verschiedene **Gefahren** und **Angriffsmöglichkeiten**, die auf dem Design des Internets basieren:

In einem Exkurs stellen wir sogenannte **APT – Advanced Persistent Threats** vor als derzeit ausgefeilteste Angriffstechnik

- **Stuxnet**, mit dem iranische Uranzentrifugen angegriffen und zerstört wurden, fällt in diese Kategorie

Zum Ende der Kurswoche besprechen wir dann wirksame **Schutzmaßnahmen** gegen Angriffe auf die offenen Transportwege im Internet