



openHPI – Sicherheit im Internet Abhören im Internet - Eavesdropping

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

Eavesdropping – Abhören im Internet

Eavesdropping, dt. Abhören

- Abhören der über ein offenes Netzwerk gesendeten Datenpakete mit dem Ziel, vertrauliche Informationen zu erlangen und zu sammeln

Wie ist das überhaupt möglich ?

- Datenpaket wird beim Transport vom Absender zum Empfänger über mehrere Zwischensysteme geleitet
- Diese Zwischensysteme können abgehört werden
- Programme zum Abhören heißen **Sniffer**

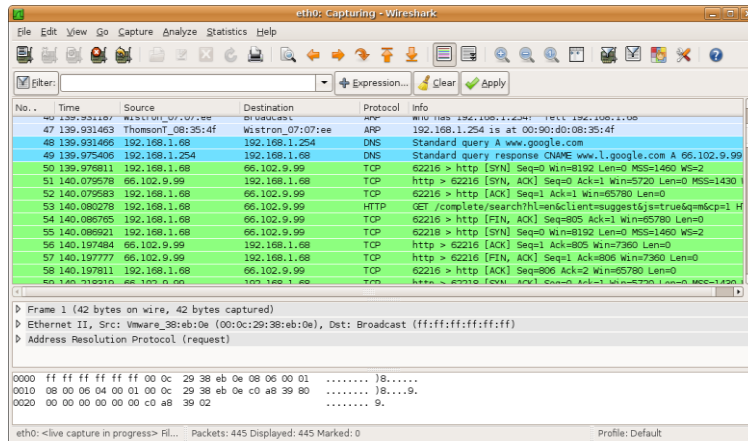
Sniffer – Programm, das an der Leitung Netzwerkpakete abfängt

- Eigentlich zur **Diagnose von Netzwerkproblemen** gedacht und nicht als Angriffswerkzeug ...
- Verschiedene **Betriebsmodi** von Sniffern
 - **Direkter Modus**
 - Zeigt nur die Datenpakete an, die an das adressiert sind an das (Zwischen-)System, auf dem der Sniffer installiert ist, und die dieses wieder verlassen
 - **Promiscuous Modus**
 - Zeigt alle Datenpakete an, die über das Zwischensystem geleitet werden, auf dem der Sniffer installiert ist
 - Wird Sniffer an strategischen Stellen im Internet installiert, sieht er alle Datenpakete, die im Netzwerk verschickt werden ...

Sniffer fängt **massenweise Daten** ab, aber das **Durchsuchen** ist sehr aufwendig

- Idee: Filterung, z.B.
 - nach Absender oder Empfänger
 - Protokoll oder Port
 - nach bestimmten Inhalten
 - ...
- Spezialisierte Lauschprogramme
 - suchen in den Datenpaketen gezielt nach bestimmten Inhalten (Mustern) , wie z.B. Passwörter oder Nutzernamen, z.B.
 - Cain & Abel

Populärster Sniffer: Wireshark



Eavesdropping | Sicherheit im Internet | Prof. Dr. Christoph Meinel

5

Verschiedene Angriffsszenarien (1/2)

■ Sniffing von HTTP-Passwörtern

- HTTP (für Datentransport im WWW zuständig) versendet Passwörter im Klartext
- Sniffer kann Klartextpasswörter und Nutzernamen direkt aus entsprechenden Datenpaketen auslesen ...

■ Sniffing von Sitzungsschlüsseln

- Webseiten verwenden Sitzungsschlüssel, um sich an eingeloggte Nutzer zu erinnern und sie wiederzuerkennen

<http://bank.de/ueberweisung?sitzung=geheimnis1534>

- Sitzungsschlüssel kann aus HTTP-Paketen ausgelesen werden
- Damit kann Angreifer dann die Sitzung ohne weiteres Login übernehmen

Eavesdropping | Sicherheit im Internet | Prof. Dr. Christoph Meinel

6

■ **Ausspähen besuchter Webseiten**

- HTTP-Anfragen zeigen die besuchten Webseiten
- Neugierige Angreifer können alle besuchten Seiten sehen, einschließlich z.B. eingegebener Suchbegriffe in Google
- möglich ist es auch, den Inhalt der besuchten Seiten zu sehen

■ **Mitlesen von Email**

- Email Protokoll SMTP ist unverschlüsselt
- Angreifer kann Inhalt von Emails komplett mitlesen

■ ...

Schutzmaßnahmen gegen Abhören im Internet

■ **Verschlüsseln** von Nachrichten und Verbindungen

- HTTPS anstatt HTTP verwenden
- Daten können zwar abgehört aber nicht mehr verstanden werden
- Abhören von gut verschlüsselten Verbindungen bei richtiger Umsetzung nahezu unmöglich

■ **Starke Authentifizierung – Mehrfaktor-Authentifizierung**

- Abgefangene Zugangsdaten können allein nicht zum Einloggen verwendet werden
 - Mehrfaktor-Authentifizierung erfordert z.B. den Besitz einer Smart-Karte als zweiten Faktor zur PIN
- Abgehorchte Passwörter sind damit nutzlos