# ARP-Spoofing “Man-in-the-Middle” in der Theorie

Autor: Gerrit Haake Datum: 05.12.2017

### Fallbeschreibung

Anna (im folgenden PC-A), Benni (im folgenden PC-B) und Corinna (im folgenden PC-C) befinden sich im gleichen Netzwerk. Anna möchte sich mit Benni über das LAN verbinden und Daten austauschen. Corinna will die Daten abfangen, ohne das Anna es mitbekommt.

### 1. Ausgang

* 3 PCs
* PC-A und PC-B neutrale Netzwerkbenutzer
* PC-C ist der Angreifer (Man-in-theMiddle)

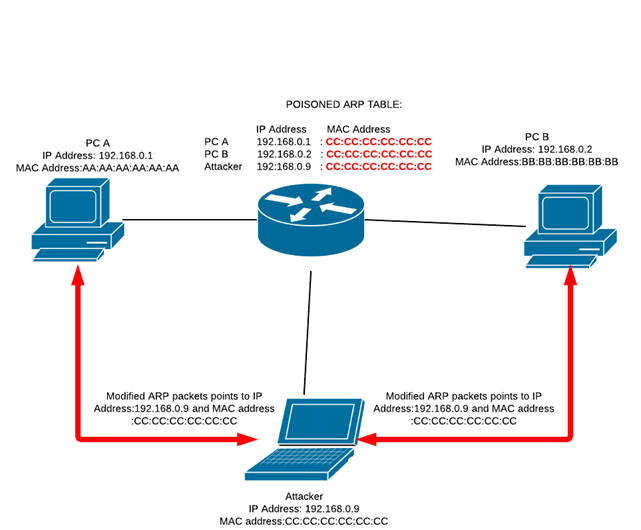
### 2. Anfrage von Daten

* PC-A sendet ein Paket an alle PCs des Netzwerks über einen Broadcast.
* PC-A versucht sich mit PC-B zu verbinden.

### 3. ARP-Spoofing

* PC-C gibt sich für PC-B
* Antwortet also, obwohl die Anfrage nicht ihm zugeordnet war.
* Damit das Ganze nicht auffällt, leitet PC-C die Packete anschließend von seiner IP auf die IP des PC-B transparent weiter.

### 4. Angriff erfolgreich durchgeführt



ARP-Spoofing

Die obere Grafik zeigt den zuvor beschriebenen Angriff. Die ARP-Tabelle wurde “infiziert” und die Daten werden alle über den PC-C geleitet. Nun kann PC-C unverschlüsselte Pakete auslesen und somit an Passwörter, E-Mailadressen und weitere Daten erhalten, die über nicht-verschlüsselte Verbindungen vesendet wurden.

## Gegenmaßnahmen

### Gegenmaßnahme 1: SSL verwenden

SSL oder generell verschlüsselte Verbindungen sind in der Regel vor MITM angriffen sicher. Dennoch besteht die Möglichkeit zwischen dem Ziel und dem Angreifer eine verschlüsselte Verbindung aufzubauen und dann die Daten unverschlüsselt zum Client weiterzuleiten.

### Gegenmaßnahme 2: statische ARP-Einträge

Die Einträge in der ARP-Tabelle können, beispielsweise über Windows mit der Shell und dem Befehl arp -s manuell gesetzt werden. Somit kann man sich vor ARP-Spoofing schützen.

### Gegenmaßnahme 3: Layer-3-Switche

ARP-Requests in andere Segmente werden vom Switch geprüft. Arbeitet dieser auf der Netzwerkschicht (Layer 3), wird neben der MAC-Adresse auch die IP-Adresse mit vorhergehenden Einträgen abgeglichen. Fallen dabei Unstimmigkeiten oder häufige Neuzuordnungen auf, schlagt der Switch Alarm.

### Gegenmaßnahme 4: Programme

Es gibt einige Programme die das Netzwerk überwachen und auffällige ARP-Vorgänge aufspüren.

Bekannte Tools sind: - Arpwatch - ARP-Guard - XAarp

### Fazit

1. Das Mitschneiden von Daten in einem öffentlichen Netzwerk ist möglich und einfach.
2. Es sollten keine wichtigen oder persönlichen Daten in öffentlichen Netzwerken eingeben werden.
3. Auf Webstites auf denen relevante Zugansdaten eingegeben werden ist darauf zu achten, dass im Browser https:// und nicht http:// vor der Website steht (Sichere Verbindung).
4. Meldung wie “Die verschlüsselte Seite versucht Daten über eine unsichere Verbindung zu versenden” sollten beachtet werden.