Sicherheit auf der Sicherungsschicht (OSI-Schicht 2)

Allgemeine Problematik des Schichtenmodells

Werden die Daten auf einer Schicht (z.B. Schicht 2) kompromittiert, werden durch die Kapselung auch die Daten aller darüberlegenden Schichten manipulierbar (wenn sie nicht zusätzlich gesichert sind.)

Wiretapping

Unter Wiretapping wird das Mitschneiden in einem drahtgebundenen Netzwerk verstanden. Ein Gerät hat dabei physikalischen Zugriff auf Netzwerkmedium und kann den Datenverkehr mitschneiden. Das Gerät wird TAP-Device genannt. Bekannte Angriffe

Cache Poisoning

Ein Switch leitet (beim normalen Forwarding) einen eingehenden Rahmen nur an den Switch-Port weiter, an dem auch das Ziel (bzw. die Ziel-MAC-Adresse) angeschlossen ist. Ein Angreifer muss somit dafür sorgen, dass die Rahmen an ihn weitergeleitet werden, damit er den Datenverkehr mitlesen kann. Beim Cache Poisoning wird die MAC-Address Tabelle (ARP-Table) eines Angriffsziel mit falschen Informationen manipuliert. Damit wird vorgetäuscht, dass eine IP-Adresse unter einer bestimmten MAC-Adresse, nämlich die des Angreifers, zu erreichen ist. Dazu hat ein Angreifer zwei Möglichkeiten

1. ARP bietet die Möglichkeit, dass Systeme ihre MAC-Adresse von sich aus bekannt geben (gratious arp). Ein Angreifer sendet nun gefälschte ARP-Pakete in denen er eine nicht zulässige Zuordnung zwischen MAC-Adresse und IP-Adresse bekannt gibt.
2. Ein Angreifer kann alle Anfragen (ARP-Request) mit einer gefälschten Antwort (ARP-Response) beantworten.

MAC Address Flooding

Wie oben beschrieben besitzt ein Switch eine Zuordnungstabelle (Source Address Table) für die Zuordnung zwischen MAC-Adresse und Switch-Port. Ein angekommener Ethernet-Rahmen wird ausgelesen und in der Zuordnungstabelle wird ein Eintrag für die Ziel-MAC-Adresse des Rahmens gesucht. Wenn ein Eintrag vorhanden ist, wird der Rahmen gemäß des Eintrags weitergeleitet. Wenn allerdings kein Eintrag in der Tabelle vorhanden sendet der Switch den Rahmen an alle Ports weiter. Wenn ein Angreifer nun die Tabelle des Switches mit falschen Angaben überflutet, hat der Switch für echte Zuordnungen keinen Speicherplatz in der Tabelle und sendet Rahmen für die keine Zuordnung vorhanden ist an alle Ports weiter.

Mögliche Verteidigungen

Um Angriffen auf der zweiten OSI-Schicht entgegen zu wirken, ist es sinnvoll den ARP-Verkehr im Netzwerk zu untersuchen. Während eines Angriffes ist der ARP-Verkehr stark erhöht. Ein mögliches Werkzeug für eine Angriffserkennung ist ArpWatch. Das Programm überwacht die ARP-Tabelle und meldet Unregelmäßigkeiten Um den Angriff Cache Poisioning zu verhindern kann man am Switch die maximale Anzahl von MAC-Adressen die pro Port gelernt werden können beschränken. Eine weitere Möglichkeit ist die Einführung einer Authentifizierung auf Schicht 2 (IEEE 802.1X), so dass ein Switch nur dann Daten weiter leitet, wenn sich ein Teilnehmer erfolgreich authentifiziert hat.