DuD
Datenschutz und Datensicherheit

ARP Poisoning

Dirk Fox

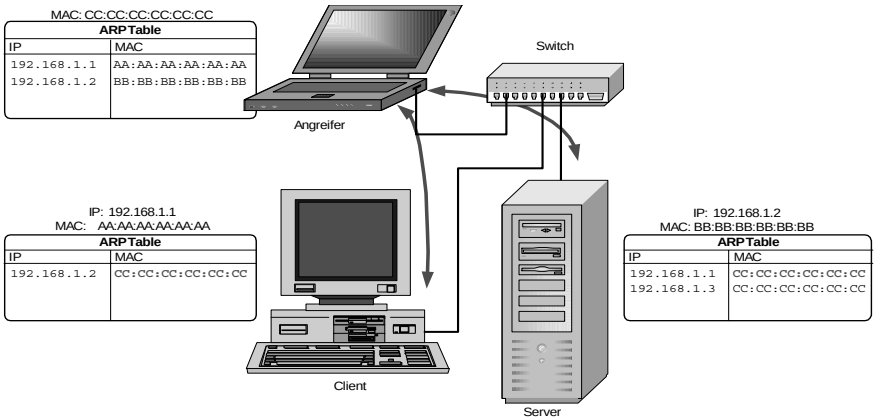
Hintergrund

Dass das „Anzapfen“ von Kommunikationsverbindungen in Behörden- und Unternehmensnetzen technisch keine Herausforderung darstellt, hat sich inzwischen herumgesprochen: Es genügt ein PC oder Laptop mit Netzwerkkarte, der mit einem – im Internet frei verfügbaren – so genannten „Sniffer“-Programm alle auf dem jeweiligen Kabelsegment übertragenen Datenpakete mitliest. Das Sniffer-Programm versetzt dazu die Netzwerkkarte in den „promiscuous“-Betrieb, in dem alle Datenpakete unabhängig von der Empfängeradresse an das Programm wietergegeben werden. Dank ausgereifter Programmfunktionen lassen sich auf Knopfdruck komplette E-Mails rekonstruieren oder durch clevere Filterung besonders interessante Daten wie z. B. die Passwörter aller E-Mail-Postfächer aus dem Datenverkehr herausklauben.

Als Schutz vor solchen Angriffen gilt bei vielen Administratoren noch heute die so genannte „strukturierte Verkabelung“ eines geswitchten Netzes, in dem durch einfache „Schalter“ (Switch) jedes Kabelsegment nur noch genau einem Rechner zugeteilt wird. Das entzieht einem Abhörangriff die Grundlage: Der PC eines Angreifers würde an jedem Netzanschluss nur für ihn selbst bestimmte Datenpakete empfangen – normalerweise also keine. Tatsächlich aber lässt sich dieser Schutz durch ARP Poisoning aushebeln.

Adressierung

Häufig ist von den „eindeutigen IP-Adressen“ die Rede, mit denen Computer im Internet weltweit identifiziert werden können. Auf der Ebene des lokalen Netzes aber erfolgt die technische Adressierung eines Datenpakets bei der Zustellung an einen ganz bestimmten PC über eine weltweit eindeutige Produktnummer der Netzwerkkarte, der so genannten MAC (Media Access Control) Adresse. Für die Eindeutigkeit dieser auch „physikalische Adresse“ genannten Nummer sorgt ein international standardisiertes Nummerierungssystem, dessen erste 24 Bits von insgesamt 48 eindeutig den Hersteller der Karte bezeichnen.[1]



Für die netzinterne Zuordnung eines an eine bestimmte IP-Adresse gerichteten Datenpakets muss den Netzkomponenten (Router, Server etc.) bekannt sein, welcher MAC-Adresse die IP-Adresse zugeordnet ist. Dazu werden mit dem Address Resolution Protocol (ARP) die Adresspaare (IP-Adresse und zugehörige MAC-Adresse) abgefragt (ARP-Request). Mit den Antworten füllt die Netzwerkkomponente eine Tabelle, mit deren Hilfe bei weiteren eingehenden Paketen die Zuordnung unmittelbar erfolgt.[2]

Protokollschwäche

So weit, so gut. Leider aber besitzt ARP eine inhärente Schwäche: Empfängt eine Netzkomponente ARP-Antwortpakete, wird der Inhalt in die Tabelle ungeprüft übernommen – auch ohne dass zuvor ein ARP-Request verschickt wurde. Das erlaubt simple Fälschungsangriffe, bei denen ein Angreifer die Zuordnungstabelle einer Netzkomponente so modifiziert, dass Kommunikationsverbindungen über seinen eigenen Rechner „umgeleitet“ werden.

Ein solcher Angriff ist in der Abbildung dargestellt. Mit Hilfe falscher ARP-Pakete hat der Angreifer die Server-Tabelle so gefälscht, dass IP-Pakete für den Client an ihn geschickt werden; und dem Client-PC hat er seine MAC-Adresse als die des Servers untergeschoben. Damit geht jedes vom Server an den Client adressierte Datenpaket physikalisch zunächst an den Angreifer, der es mitliest und anschließend an den Client weiterleitet.

Da die Zuordnungstabelle beim nächsten Booten gelöscht wird, hinterlässt der Angriff keine Spuren. Schlimmer noch: Gegen ihn ist bislang kein Kraut gewachsen, da die Zuordnungstabellen nur mit erheblichem Aufwand fest voreingestellt werden können. Insbesondere in Netzen mit dynamischer IP-Adressvergabe (DHCP) müssen auch die Zuordnungstabellen dynamisch erstellt werden.

Ausblick

ARP Poisoning ist inzwischen fester Bestandteil zahlreicher im Internet frei verfügbarer Hacking-Tools und auch für technische Laien kinderleicht zu bedienen. Vor Angriffen dieser Art in internen Netzen hilft eingeschränkt eine kontrollierte Zuordnung der Netzanschlüsse (kein DHCP, feste MAC-Adresskonfiguration im Switch) und wirksam allein die Verschlüsselung aller Kommunikationsdaten.

[1] Die MAC-Adresse findet sich unter Windows bei den Eigenschaften der Netzwerkverbindung; mit dem Konsolenbefehl „ipconfig /all“ lässt sie sich auslesen.

[2] Der Inhalt der ARP-Tabelle kann mit dem Konsolenbefehl „arp –a“ angezeigt werden.