ANGRIFF VON INNEN

Gefahren durch ARP-Spoofing

Das Hauptaugenmerk in Fachartikeln, die sich mit Angriffen auf Netze beschäftigen, liegt auf den Techniken eines Angreifers, der außerhalb des betrachteten Netzes lokalisiert ist. Vernachlässigt wird aber der im LAN sitzende Angreifer, obgleich einschlägige Statistiken bestätigen, dass dessen Anteil bei mehr als 70 Prozent liegt [1]. Aufgrund der fehlenden Sicherheitsmechanismen der für das LAN relevanten Protokolle ist es insbesondere über das Address Resolution Protocol [2] für einen internen Übeltäter einfach möglich, Angriffe durchzuführen, die derartige Schwächen ausnutzen und im Ausspähen und der Manipulation von Daten resultieren. Dieser Beitrag behandelt eine Reihe von Techniken und Werkzeugen, die einem Angreifer zur Verfügung stehen, und stellt diverse Gegenmaßnahmen vor.

Innerhalb eines Ethernet-LANs dient die MAC-Adresse (Media Access Control) als Kennung einer Netzkarte. Sie ist 6 Byte lang, für jede Netzkarte weltweit eindeutig und fest im ROM der Karte eingebrannt. Anwendungen, die auf den einzelnen Hosts im LAN ablaufen, verwenden zur Adressierung jedoch die ihnen jeweils bekannte IP-Adresse des Kommunikationspartners. Das Netzprotokoll ARP (Address Resolution Protocol) ist im TCP/IP-Referenzmodell innerhalb der Internetschicht einzuordnen. Mithilfe von ARP kann ein Host, der senden will und die IP-Adresse des Kommunikationspartners im selben Subnetz kennt, dessen MAC-Adresse ermitteln, um anschließend ein Ethernet-Frame mit den notwendigen Daten aufbereiten zu können.

Im optimalen Fall kann ein Host bereits ohne weitere Netzaktivität die MAC-Adresse seines gewünschten Kommunikationspartners ermitteln: Jeder Host führt eine ARP-Tabelle, in der eine gewisse Zahl von IP-MAC-Paaren vorgehalten werden kann. Diese Tabelle wird in der Regel dynamisch erzeugt.

Fehlt ein derartiger Eintrag für eine gewünschte IP-Adresse, muss der Host diese im Subnetz erfragen: Im regulären Betrieb lauscht jede Netzkarte nur auf Ethernet-Frames, die ihre eigene MAC-Adresse im Header tragen. Ethernet-Frames für andere Netzkarten werden nicht weiter berücksichtigt. Der Host nutzt nun die so genannte Ethernet-Broadcast-Adresse (in hexadezimaler Form: FF-FF-FF-FF-FF-FF), um mit einer Anfrage gleichzeitig die Netzkarten aller Hosts eines Ethernet-Segments zu adressieren. Eine Anfrage bezüglich der MAC-Adresse zu der IP-Adresse 192.168.1.3 würde also sinngemäß lauten: "Ich bin 192.168.1.2 mit MAC 12-34-56-78-9A-01, wer hat 192.168.1.3?".

Diese Anfrage wird als ARP-Request bezeichnet. Diesen Request nimmt jede Netzkarte beziehungsweise jeder Host zur Kenntnis. Empfängt ein Host einen ARP-Request, der seine IP-Adresse erhält, reagiert er mit einer Antwort, der ARP-Reply. Da zumindest innerhalb eines Ethernet-Segments eine IP-Adresse von maximal einem Host verwendet werden darf, kann theoretisch auch nur maximal ein Host mit einer ARP-Reply antworten. Durch diese ARP-Reply teilt er dem anfragenden Host seine MAC-Adresse mit: "Hier, ich bin 192.168.1.3 und habe MAC 12-34-56-78-9A-02!"

Die ARP-Tabelle sieht dann wie folgt aus (das C-Flag gibt an, dass der Eintrag komplett ist):

```
# arp
Address          HWaddress          Flags
192.168.1.2      12-34-56-78-9A-01    C
192.168.1.3      12-34-56-78-9A-02    C
```

Mit der jetzt bekannten MAC des Empfängers kann der sendende Host nun das erste in einen Ethernet-Frame gekapselte IP-Paket versenden. Die neue MAC-Adresse speichert der sendende Host in seiner ARP-Tabelle ebenso wie der Empfänger das IP-MAC-Adressen-Paar des Senders, sofern es ihm zuvor nicht ohnehin bekannt gewesen war. Hosts, die einen ARP-Request aussenden, gehen davon aus, dass der ARP-Reply korrekt ist, eine Authentifizierung der Daten findet nicht statt.

ARP-Tabellen sind wie Caches aufgebaut: Wird ein Eintrag für eine gewisse Zeit (abhängig von der Implementierung, in der Regel jedoch wenige Minuten) nicht verwendet, so wird er ungültig und aus der Tabelle gelöscht. Ebenso sind es die am seltensten verwendeten Einträge, die als Erstes überschrieben werden.

ARP ist ein zustandsloses Protokoll. Empfängt ein Host ein ARP-Reply, so evaluiert er es, unabhängig davon, ob er nun tatsächlich einen ARP-Request gesendet hat oder nicht. Dieses Verhalten stellt eine Schwäche des ARP dar, wurde aber aus Performanzgründen in dieser Form realisiert.

SCHWACHPUNKTE UND MÖGLICHE ANGRIFFSPUNKTE VON ARP Sniffing, also das Lauschen am Netz, ist nach Meinung von vielen Administratoren in Ethernet-Segmenten, die über einen Switch verbunden sind, also eine stern-

förmige Topologie mit einem dedizierten Strang für jeden Host aufweisen, nicht möglich: Durch die Funktion des Switches sieht der Host nur die Datenpakete, die für ihn gedacht sind. Dem Switch ist hierbei bekannt, an welchen der an seinen Ports angeschlossenen Hosts er einen Ethernet-Frame in Abhängigkeit von der MAC-Adresse senden muss. Die beiden folgenden Angriffe werden als "Spoofing" (Vortäuschung) bezeichnet.

Die erste Methode ist als Denial of Service bekannt: Der Angreifer sendet an einen Host eine gefälschte ARP-Reply, bei der er die IP-Adresse des Routers des Subnetzes mit einer nicht existenten MAC-Adresse assoziiert. Diese Information übernimmt der Host. Frames dieses Hosts, die das Segment danach eigentlich verlassen müssten, landen aber somit im Daten-Nirwana: Der Host ist isoliert.

Der für die Vertraulichkeit kommunizierter Daten folgenschwerste Angriff ergibt sich durch einen Man-in-the-Middle-Angriff. Hierbei gelingt es einem Angreifer im LAN, die MAC-Adresse seines Hosts mit einer IP-Adresse eines anderen Hosts zu assoziieren. Dieser Angriff soll an folgendem Beispiel verdeutlicht werden, bei dem Angreifer M die Kommunikation zwischen den Hosts A und B belauschen möchte. Die IP-Adresse des Beteiligten x sei dabei IP-x, die korrespondierende MAC-Adresse MAC-x. Durch vorheriges Beobachten des Netzes kennt Angreifer M die IP-MAC-Paare von A und B. M sendet eine ARP-Reply mit der IP-Adresse von B, aber seiner MAC-Adresse an A. Wie oben erwähnt, ist das ARP-Protokoll zustandslos, A ist sich nicht bewusst, dass er keinen ARP-Request mit der Frage nach der MAC-Adresse von B per Broadcast in das Subnetz gesendet hat und übernimmt, nicht an der Authentizität des ARP-Requests zweifelnd, das Paar (IP-B, MAC-M) in seine ARP-Tabelle. Eine äquivalent gefälschte ARP-Reply (IP-Adresse von A, eigene MAC-Adresse von M) sendet M an B. Bild 1a stellt die Situation ohne Spoofing, Bild 1b nach erfolgreichem ARP-Spoofing durch M dar.

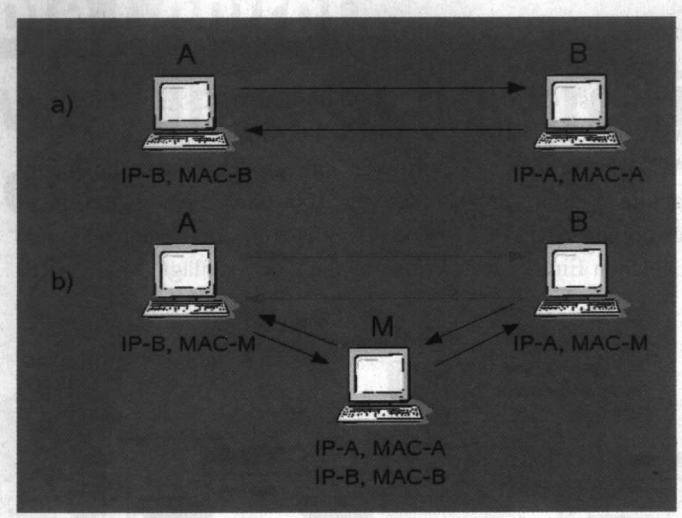

Bild 1. Oben: Situation vor dem Spoofing, unten nach dem Eingriff

Sämtliche Kommunikation zwischen A und B verläuft nun über M. Sofern dieser keine Daten verwirft, fällt diese Situation weder A noch B auf. Sind A und B keine gewöhnlichen Hosts im Netz, sondern beispielsweise A ein PC und B der Router des Subnetzes, so ergibt sich die pikante Situation, dass M den gesamten Datenverkehr von A, also auch den in das Internet mitlesen kann. Dieses Mitlesen erstreckt sich von Passwörtern bis hin zu persönlichen Daten. Auch vermeintliche sichere Verbindungen über SSL (Secure Socket Layer), das bei sicheren Webseiten wie etwa bei Onlinebanking eingesetzt wird, oder auch SSH (Secure Shell), für eine verschlüsselte Sitzung auf einem Server, sind unter gewissen Umständen für einen Angreifer einsehbar.

WERKZEUGE Obwohl die eigentlichen Angriffe auf Netzebene stattfinden, ist die Durchführung auch für Laien (Stichwort "Script-Kiddies") kein Problem: Es finden sich ausreichend viele kostenlose Programme dafür im Internet.

ARPoison ist eine Anwendung für die Kommandozeile unter Unix. Es erlaubt dem Benutzer die Erzeugung und das Versenden von gefälschten ARP-Replies.

dsniff ist eine Sammlung von Werkzeugen zum ARP-, aber auch DNS-Spoofing und bietet beispielsweise zusätzlich die Möglichkeit, einen Man-in-the-Middle-Angriff auf HTTP-Sitzungen durchzuführen.

Ettercap darf als das Schweizer Messer unter den Sniffing- und Spoofing-Werkzeugen bezeichnet werden: Neben den aufgeführten Funktionen obiger Programme ist es in der Lage, einen Man-in-the-Middle-Angriff auf SSH1- und HTTPS-Verbindungen erfolgreich durchzuführen. Dieses bedeutet, dass selbst kryptografisch abgesicherte Verbindungen wie sie bei Onlinebanking verwendet werden, verwundbar sind. Ein Angreifer ist in der Lage, PINs und TAN abzugreifen und Konten zu manipulieren. Das HTTPS-Verbindungen zugrunde liegende SSL-Protokoll wird von vielen anderen Anwendungen (wie etwa SAP) verwendet. Somit ist es einem internen Mitarbeiter einer Firma möglich, sogar auf Gehaltsbuchungen zuzugreifen und sie zu manipulieren.

Weitere Funktionen sind:

- Angriffe auf PPTP (Point-to-Point-Tunneling-Protocol): Dieses Protokoll wird beispielweise von Microsoft-Produkten verwendet, um ein vermeintlich sicheres VPN (Virtual Private Network) aufzubauen.
- Passwortsammler für nahezu alle gängigen Protokolle.
- Passive Recherche im LAN (Scanning): Zur Ermittlung von Topologie, angeschlossenen Servern etc.

Ettercap ist für alle gängigen Betriebssysteme und auch Microsoft Windows verfügbar.

GEGENMASSNAHMEN Die obigen Ausführungen haben gezeigt, wie leicht die Sicherheit im LAN kompromittierbar ist, die beschriebenen Werkzeuge machen deutlich, dass sich dieser Missbrauch auch durch technisch wenig versierte Zeitgenossen (oder auch ausreichend verärgerte Mitarbeiter) durchführen lässt.

Welche Gegenmaßnahmen kann ein Netzverantwortlicher ergreifen?

Eine präventive Methode ist die des Static ARP. Hierbei wird für jeden Host die Zuordnung IP-MAC-Adresse festgelegt und in der ARP-Tabelle als "statisch" gekennzeichnet (in der obigen ARP-Tabelle käme bei einem solchen Eintrag in der Spalte "Flags" ein "M" hinzu). Diese Einträge werden durch ARP-Requests und -Replies nicht mehr automatisch verändert. Diese Maßnahme bedeutet jedoch einen immensen Verwaltungsaufwand, der in großen Netzen nicht mehr zu realisieren ist. Außerdem können bei den Microsoft Windows Versionen 9x, NT und 2000 statisch gesetzte ARP-Einträge durch entsprechende ARP-Anfragen trotzdem verändert werden.

Eine simple Lösung zur Detektion ist das Programm ARPwatch [3], das ein LAN-Segment beobachtet und eine eigene Tabelle der IP-MAC-Zuordnungen führt. Tritt eine ARP-Reply mit einer bekannten IP-Adresse, aber anderen MAC-Adresse, als in der internen Tabelle aufgelisteten auf, alarmiert ARPwatch den Systemadministrator per E-Mail.

Auch das Intrusion Detection System Snort verfügt über den Präprozessor arpspoof, der in seiner Funktionalität ARPwatch entspricht. Ihm muss der Administrator hingegen eine gültige ARP-Tabelle vorgeben.

Gegen die obigen Maßnahmen sprechen Fehler bei der Realisierung (statisches ARP bei Microsoft Windows) oder ein zu hoher Aufwand der Administration, falls der Netzadministrator feste Paare von IP- und MAC-Adressen vorgeben muss. Diese Vorgehensweise ist in mittleren und großen Unternehmen mit mehreren 100 oder 1000 Hosts nicht mehr zu realisieren. Am besten in kleinen Netzumgebungen schlägt sich ARP-watch. In modernen Netzen kommt als K.o.-Kriterium allerdings DHCP (Dynamic Host Configuration Protocol) hinzu, das zur dynamischen Vergabe von IP-Adressen an Hosts verwendet wird. ARPwatch würde mit der Meldung einer Vielzahl falscher Angriffe reagieren.

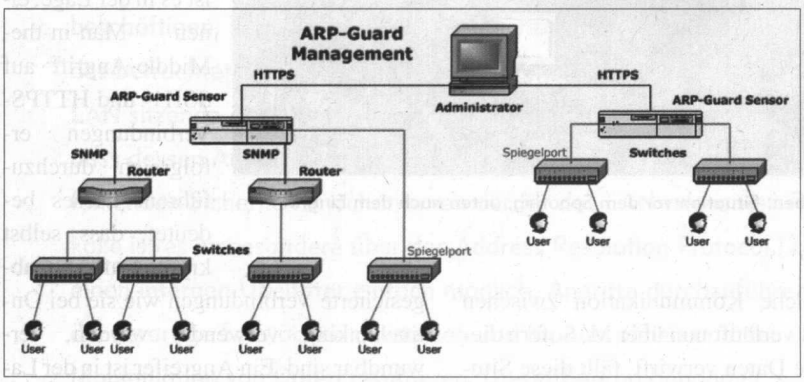

Bild 2. Die Sensoren von ARP-Guard erkennen einen Wechsel der IP-MAC-Beziehung

Die Gefahr durch ARP-Spoofing und die Lücke in Produkten zur Erkennung will ISL (Internet Sicherheitslösungen) mit dem Produkt ARP-Guard [4] schließen. Das ARP-Guard-System besteht aus Sensoren zur Detektion von ARP-Spoofing-Angriffen und einem Managementsystem zur Auswertung und Weiterverarbeitung der Sensormeldungen. Das Managementsystem benachrichtigt im Angriffsfall automatisch die eingetragenen Sicherheitsbeauftragten oder Netzadministratoren. ARP-Guard-Sensoren analysieren ARP-Meldungen in einzelnen Netzsegmenten. Dazu werden an jeden LAN-Switch über den verfügbaren Spiegel-Port die ARP-Guard-Sensoren angeschlossen. ARP-Guard-LAN-Sensoren lassen sich auf separaten PCs oder Workstations oder auch auf bereits vorhandenen, aber nicht ausgelasteten Rechnern einsetzen. Jeder ARP-Guard-Sensor kann bis zu acht LAN-Switches überwachen. Für größere Netze werden ARP-Guard-LAN-Sensoren kaskadiert und auf getrennte Netzsegmente verteilt. Auch für noch größere Netze, in denen eine flächendeckende Überwachung mit LAN-Sensoren zu kostenaufwändig wäre, hat das Unternehmen eine Lösung entwickelt, die darauf beruht, bestehende SNMP-fähige Router als Sensor zu verwenden. Über einen SNMP-Sensor werden die ARP-Tabellen von bis zu mehreren 100 Routern überwacht und alle relevanten Veränderungen durch das Management gemeldet.

Die einzelnen ARP-Guard-Sensoren sind über verschlüsselte IP-Verbindungen mit dem ARP-Guard-Managementsystem verbunden. Das Managementsystem analysiert die Meldungen und bereitet sie für den Netzadministrator auf, der per SMS oder E-Mail benachrichtigt wird. Darüber hinaus erfolgt eine Protokollierung aller Veränderungen an ARP-Tabellen, die der Administrator über ein Web-Frontend abruft. Über dieses Web-Frontend kann der Administrator das System konfigurieren. Ebenso ist ARP-Guard DHCP-fähig und berücksichtigt IP-MAC-Wechsel, die aufgrund der dynamischen Vergabe von IP-Adressen entstehen. Das ARP-Guard-System ist auch gegenüber ARP-Spoofing-Angriffe geschützt.

FAZIT Für interne Angreifer ist es leicht, Kommunikationsverbindungen im LAN zu attackieren und Daten wie beispielsweise Passwörter oder Bankdaten zu erlauschen oder zu verändern. Sowohl die Werkzeuge als auch Gegenmaßnahmen sind frei im Internet verfügbar. Aufgrund der Brisanz des Themas sollte jedoch im Unternehmensbereich die professionelle Hilfe von Sicherheitsfirmen in Anspruch genommen werden.

(Dr. Thomas Demuth/mw)

Quellen:

[1] http://www.kpmg.com/about/press.asp?cid=469
[2] http://www.ietf.org/rfc/rfc826.txt
[3] http://www-nrg.ee.lbl.gov/nrg.html
[4] https://www.arp-guard.com/