E) Sicherheit: IP-Spoofing und ARP Spoofing

1. Allgemeine Beschreibung

IP-Spoofing

IP-Spoofing bezeichnet in Computernetzen das Versenden von IP-Paketen mit gefälschter Absender-IP-Adresse. Die Kopfdaten jedes IP-Pakets enthalten dessen Quelladresse. Dies sollte die Adresse sein, von der das Paket gesendet wurde. Indem der Angreifer die Kopfdaten so fälscht, dass sie eine andere Adresse enthalten, kann ein Angreifer das Paket so aussehen lassen, als ob das Paket von einem anderen Computer gesendet wurde. Dies kann von Eindringlingen dazu genutzt werden, Sicherheitsmaßnahmen wie z. B. IP-adressbasierte Authentifizierung im Netzwerk auszutricksen.

ARP-Spoofing

ARP-Spoofing oder auch ARP Request Poisoning (Anfrageverfälschung) bezeichnet das Senden von gefälschten ARP-Paketen. Beim ARP-Spoofing wird das gezielte Senden von gefälschten ARP-Paketen dazu benutzt, um die ARP-Tabellen in einem Netzwerk so zu verändern, dass anschließend der Datenverkehr zwischen zwei Rechnern in einem Computernetz abgehört oder manipuliert werden kann.

2. Themenbereich (Praktische Relevanz)

Das Thema ist im Bereich Sicherheit von Rechnernetzwerken angesiedelt.

IP-Spoofing lässt sich jedoch nur beschränkt zum Einbruch in andere Systeme verwenden, da die Antwortpakete des attackierten Rechners an die gespoofte Absenderadresse im IP-Header zurückgeschickt wird und daher den wirklichen attackierenden Absenderhost nicht erreichen, ausser die Pakete werden vom Angreifer in einem ungeswitchten Netzwerk gesnifft.
Dieses Verhalten lässt sich jedoch auch als „Waffe“ benutzen, wenn mit gespooften Paketen SYN-Flooding betrieben wird. Hier wird der Ziel Host der Attacke als gespoofte IP verwendet, dieser erhält dann alle Antwortpakete und dessen Verbindung wird dadurch möglicherweise lahmgelegt.

ARP-Spoofing lässt sich dazu verwenden den Datenverkehr zwischen 2 Hosts A und B abzuhören. Dazu werden gefälschte ARP-Nachrichten verschickt mit den jeweiligen IP Adressen von Host A und B und der eigenen (Angreifer) Hardware Adresse. Der Angreifer fungiert unbemerkt als Proxy zwischen Host A und B, dies nennt man einen Man-In-The-Middle-Angriff. Während ein reines Abhören des Netzwerkverkehrs mit Hilfe eines Sniffers nur in ungeswitchten Netzwerken funktioniert, ist dieser Angriff auch in geswitchten Netzwerken erfolgreich.

3. Technische Details

Protokollinsformationen IP

Internet Protokoll (IP): RFC 791 http://tools.ietf.org/html/rfc791
Internet Protokoll (IPv6): RFC 2460 http://tools.ietf.org/html/rfc2460

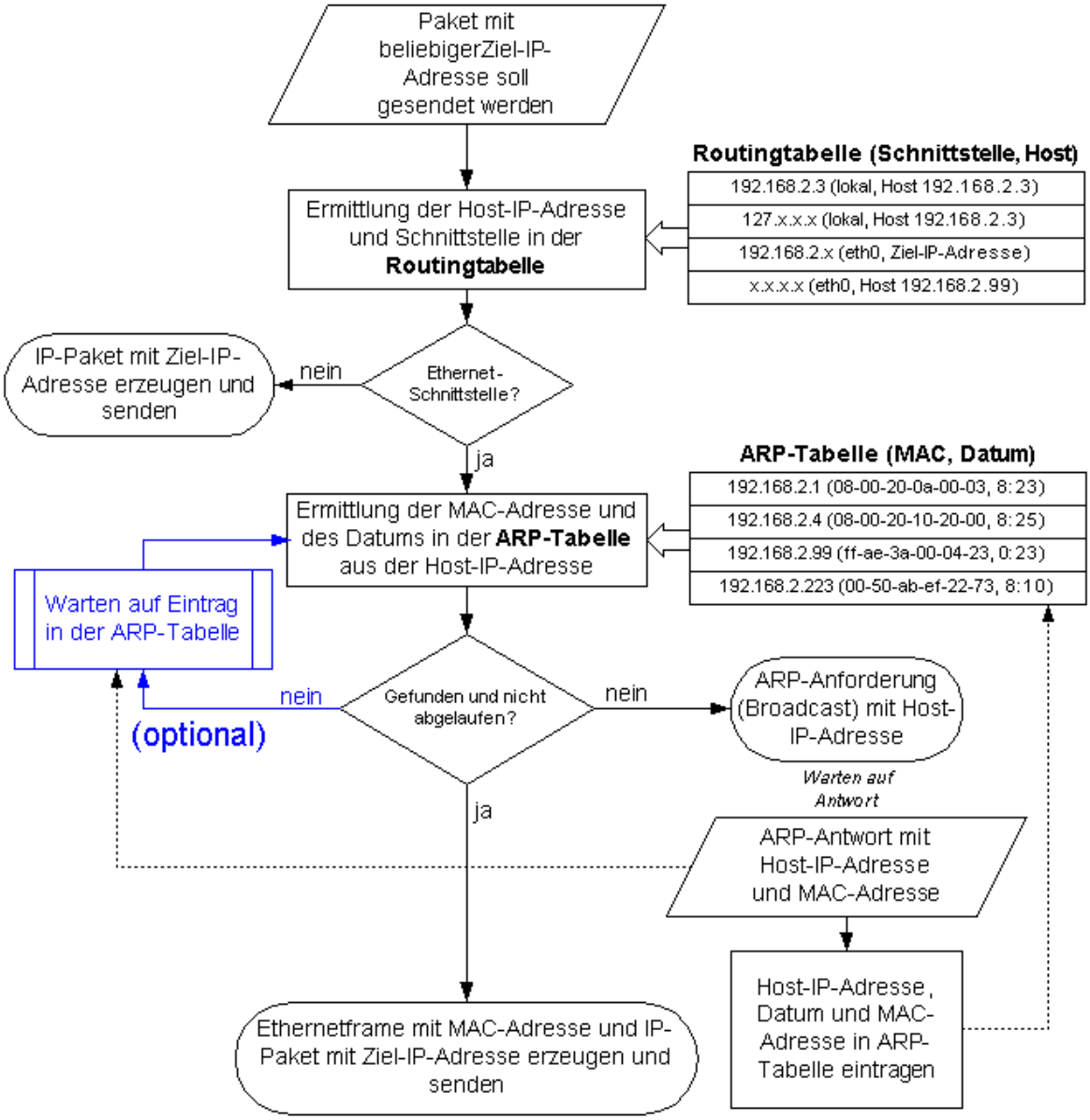
IP bildet die erste vom Übertragungsmedium unabhängige Schicht der Internetprotokoll-Familie. Das bedeutet, dass mittels IP-Adresse und Subnetzmaske (subnet mask) für IPv4, bzw. Präfixlänge bei IPv6, Computer innerhalb eines Netzwerkes in logische Einheiten, so genannte Subnetze, gruppiert werden können. Auf dieser Basis ist es möglich, Computer in größeren Netzwerken zu adressieren und Verbindungen zu ihnen aufzubauen, da logische Adressierung die Grundlage für Routing (Wegewahl und Weiterleitung von Netzwerkpaketen) ist.

Protokollinformationen ARP

Address Resolution Protocol (ARP): RFC 826 http://tools.ietf.org/html/rfc826

Das ARP ist für die Auflösung der MAC-Adressen im lokalen Netzwerk zuständig. Sollen Daten über Netzwerkgrenzen hinweg gesendet werden, wird das Internet Protokoll (IP) verwendet. IP-Implementierungen sind in der Lage, zu erkennen, dass ein Paket nicht für das lokale Subnetz bestimmt ist und senden es an einen lokalen Router, der sich um die Weiterleitung des Pakets kümmert. Dieser Router hat wiederum eine lokale MAC Adresse, die über ARP ermittelt werden kann.

Das folgende Flussdiagramm stellt den Zusammenhang von IP-Routing mit ARP dar:



Gegenmassnahmen IP-Spoofing

Paketfilter sind eine mögliche Gegenmaßnahme gegen IP-Spoofing. Das Gateway zu einem Netzwerk sollte eine eingehende Filterung vornehmen: Von außen kommende Pakete, die Quelladressen von innenliegenden Rechnern haben, werden verworfen. Dies verhindert, dass ein externer Angreifer die Adresse einer internen Maschine fälschen kann. Idealerweise sollten auch ausgehende Pakete gefiltert werden, wobei dann Pakete verworfen werden, deren Quelladresse nicht innerhalb des Netzwerks liegt; dies verhindert, dass IP-Adressen von externen Maschinen gespooft werden können und ist eine bereits lange bestehende Forderung von Sicherheitsfachleuten gegenüber Internetdienstanbietern: Wenn jeder ISP konsequent ausgehende Pakete filtern würde, die laut ihrer Quelladresse nicht aus dem eigenen Netz stammen, wäre massenhaftes IP-Spoofing (häufig in Verbindung mit Denial of Service-Attacken) ein wesentlich geringeres Problem als es heute im Internet ist.

Einige Protokolle auf höheren Schichten stellen eigene Maßnahmen gegen IP-Spoofing bereit. Das Transmission Control Protocol (TCP) benutzt beispielsweise Sequenznummern, um sicherzustellen, dass ankommende Pakete auch wirklich Teil einer aufgebauten Verbindung sind. Die schlechte Implementation der TCP-Sequenznummern in vielen älteren Betriebssystemen und Netzwerkgeräten führt jedoch dazu, dass es dem Angreifer unter Umständen möglich ist, die Sequenznummern zu erraten und so den Mechanismus zu überwinden. Alternativ könnte er versuchen, zum Man in the Middle zu werden.

Dass sich ein Wurm aber auch innerhalb eines einzigen UDP-Pakets verbreiten kann, hat im Jahr 2003 SQL Slammer bewiesen. Dieser benutzte damals kein IP-Spoofing, wäre damit aber wahrscheinlich besser durch Firewalls mit Anti-Spoofing-Funktionalität gekommen.

Hätte eine Firewall z. B. eine Regel, die den MS-SQL-Dienst (UDP Port 1433) von einer IP-Adresse A.A.A.A zu B.B.B.B erlaubt, müsste der Wurm auf dem Rechner C.C.C.C seine eigene Absender-Adresse nur auf A.A.A.A fälschen um die Firewall zu passieren. Da nur ein einziges Paket notwendig ist und das User Datagram Protocol (UDP) keinen Zustand hat, würde auch eine Stateful Firewall keinen Schutz bieten.

Defending Against Sequence Number Attacks: RFC 1948 http://tools.ietf.org/html/rfc1948

Defeating Denial of Service Attacks which employ IP Source Address Spoofing:
RFC 2827 http://www.ietf.org/rfc/rfc2827.txt

Manipulation von ARP-Tabellen

Im Gegensatz zu einem Hub kann bei einem Switch grundsätzlich die Kommunikation zwischen zwei Stationen von keiner der anderen Stationen abgehört werden. Zu diesem Zweck pflegt der Switch eine Tabelle, die die MAC-Adressen der beteiligten Stationen den verschiedenen Ports zuordnet. Datenpakete beziehungsweise Ethernet-Frames, die an eine bestimmte MAC-Adresse adressiert sind, werden nur an den Port weitergeleitet, an dem der betreffende Rechner angeschlossen ist.

Doch nicht nur der Switch pflegt eine Tabelle mit MAC-Adressen, sondern auch die beteiligten Rechner. Mit ARP-Anfragen können diese ARP-Tabellen am beteiligten Rechner gefüllt werden. Ziel des ARP-Spoofings ist es, die ARP-Tabellen zu manipulieren (ARP-Cache-Poisoning). Dazu schickt ein Angreifer eine ARP-Antwort an das Opfer, in der er seine eigene MAC-Adresse als die des Routers ausgibt, der für das betreffende Subnetz als Standard-Gateway fungiert. Sendet das Opfer anschließend ein Paket zum eingetragenen Standard-Gateway, landet dieses Paket in Wirklichkeit beim Angreifer. Auf die selbe Weise wird der ARP-Cache des Routers so manipuliert, dass Ethernet-

Frames, die eigentlich an das Opfer adressiert wurden, in Wirklichkeit beim Angreifer landen. Auf einschlägigen Internet-Seiten sind eine Reihe von Tools verfügbar, die diese Angriffsmethode ermöglichen.

MAC-Flooding ist eine Angriffsmethode, die die Funktionsweise eines Switches beeinflusst. Switches erlernen angeschlossene MAC-Adressen dynamisch. Die MAC-Adressen werden in der Switching-Tabelle gespeichert. Der Switch weiß dadurch, an welchen Ports die entsprechenden MAC-Adressen angeschlossen sind.

Wenn nun eine angeschlossene Station mit Hilfe eines geeigneten Tools eine Vielzahl von Paketen mit unterschiedlichen Quell-MAC-Adressen sendet, speichert der Switch diese MAC-Adressen in seiner Switching-Tabelle. Sobald der Speicherplatz für die Switching-Tabelle gefüllt ist, sendet ein Switch sämtliche Pakete an alle Switch-Ports. Durch dieses "Fluten" der Switching-Tabelle mit sinnlosen MAC-Adressen kann ein Switch nicht mehr feststellen, an welche Ports tatsächliche Ziel-MAC-Adressen angeschlossen sind. Diese Angriffsmethode wird verwendet, um das Mitlesen von Paketen in geswitchten Netzen zu ermöglichen. Es sind frei verfügbare Tools auf einschlägigen Seiten im Internet verfügbar, die auf einem Switch über 155.000 MAC-Adress-Einträge innerhalb einer Minute erzeugen können.

ARP-Spoofing erkennen

ARP-Spoofing zu erkennen oder zu verhindern ist nicht einfach. Dazu gibt es mehrere Möglichkeiten. Eine davon ist, das ARP ganz außen vor zu lassen und mit statischen Tabellen zur Umsetzung von IP-Adressen zu Hardware-Adressen zu arbeiten. Diese Möglichkeit ist nicht sehr effizient, weil die ARP-Tabellen ständig aktualisiert werden müssen. Besser ist es, am Grundproblem anzusetzen: Jede ARP-Antwort, ob angefordert oder nicht, ob sinnvoll oder nicht, wird von fast allen Betriebssystemen akzeptiert. Hier kann es helfen, das Verarbeiten von ARP-Antworten Programmen mit größerer Intelligenz zu überlassen. Diese überwachen, wer die Antworten wann schickt und welche Informationen die Antworten enthalten. Offensichtlich gefälschte ARP-Pakete lassen sich so erkennen und verwerfen. Dieser Ansatz wird zum Beispiel von ArpWatch implementiert. XArp, welches als graphische Benutzeroberfläche für Windows und Linux verfügbar ist, verwendet zusätzlich weitergehende Inspektionsmodule um Angriffe zu erkennen und aktive Validierung der ARP-Mappings.

4. Anwendungsinformationen

a) Hinweise zu verfügbaren Open Source-Werkzeugen, mit denen das Thema praktisch angewandt oder zumindest getestet werden kann

Implementierung der ARP-Spoofing-Attacke von Felix von Leitner:
http://www.fefe.de/arprelay/

ARP-Spoofing unter Windows:
http://www.oxid.it/cain.html

Sniffer für Switched LANs:
http://ettercap.sourceforge.net/

Überwachen des IP-MAC-Mappings für Unix:
ftp://ftp.ee.lbl.gov/arpwatch.tar.gz

Neuere Version von ArpWatch:
http://freequaos.host.sk/arpwatch/

Intelligente Überwachung des ARP-Verkehrs mit aktiven und passiven Methoden. GUI-basiert und verfügbar für Windows und Linux:
http://www.chrismc.de/development/xarp

b) Hinweise auf vergleichbare Werkzeuge

Unter Unix und Windows kann der ARP-Cache mit arp (oder arp -a) angezeigt und manipuliert werden. Mit dem Zusatzprogramm arping können manuell Anforderungen versendet werden.

5. eigene Ergänzungen

http://www.my-proxy.com/content/security-tech/introduction-ip-spoofing.html

Pakete mit lokalen Source-IP Adressen (vom Internet ankommend) verwerfen

Ein Auszug aus einer Server Firewall Konfiguration für eth0 (Internet Interface):

```
# First contact
/sbin/iptables -A INPUT -i lo -s 127.0.0.1/255.0.0.0 -j ACCEPT
/sbin/iptables -A INPUT -i eth0 -s 192.168.0.0/255.255.0.0 -j LOG
/sbin/iptables -A INPUT -i eth0 -s 192.168.0.0/255.255.0.0 -j DROP
```

1. Zeile: Alle auf dem lokalen Interface ankommenden Pakete mit der Source-IP Address 127.0.0.1/8 akzeptieren.

2. + 3. Zeile: Alle auf dem externen Interface ankommenden Pakete mit einer für lokale Netzwerke definierten Source-IP Address (hier am Beispiel 192.168.0.0/16) loggen und auf der nächsten Zeile verwerfen.