

Überblick über Sicherheitsprobleme

Teil II: Sicherheitsprobleme im Netzwerk

von Stefan Heimann

Inhaltsverzeichnis :

<i>Abbildungsverzeichnis</i>	4
0. Einleitung.....	5
1. Überblick über die Entstehung des Internet.....	5
1.1. Die Entstehung des ARPANET.....	5
1.2. Der Übergang zum NFSNET.....	6
1.3. Das Internet.....	6
1.4. Fazit zur Entstehungsgeschichte.....	7
2. Grundarten von Netzwerkg Angriffen.....	7
2.1. Sniffing (Netz-Spionage).....	8
2.2. Denial-of-Service (DoS).....	9
2.3. Spoofing (Maskerade).....	9
2.4. Man-in-the-Middle.....	10
3. Sicherheitsschwächen der Internet-Protokolle und deren Implementationen.....	10
3.1. ARP (Address Resolution Protocol).....	11
3.1.1. Funktionsweise des ARP.....	11
3.1.2. Schwächen des ARP.....	11
3.1.2.1. ARP-Spoofing.....	11
3.1.2.2. ARP-Man-in-the-Middle.....	11
3.1.2.3. ARP-Sturm : DoS.....	12
3.1.2.4. ARP-Broadcast-Sturm : DoS.....	12

Überblick über Sicherheitsprobleme

3.2.IP (Internet Protocol).....	13
3.2.1.IP-Fragmentierung.....	13
3.2.2.IP-Strict-Source-Routing.....	13
3.2.3.Schwächen des IP.....	14
3.2.3.1.IP-Spoofing.....	14
3.2.3.2.Source-Routing-Angriffe : DoS.....	14
3.2.3.3.Ping-of-Death : DoS.....	14
3.2.3.4.Tiny-Fragment-Angriffe.....	14
3.2.3.5.Overlapping-Fragment-Angriffe (Teardrop).....	15
3.3.ICMP (Internet Control Message Protocol).....	15
3.3.1.Ping-Flooding : DoS.....	15
3.3.2.Smurf (ICMP-Sturm) : DoS.....	15
3.3.3.ICMP-Destination-Unreachable (Typ 3) : DoS.....	16
3.3.4.ICMP-Fragmentation-Needed-And-DF-Set (Typ 3, Code 4) : DoS.....	16
3.3.5.ICMP-Source-Quench (Typ 4) : DoS.....	16
3.3.6.ICMP-Redirect (Typ 5) : Man-in-the-Middle.....	16
3.4.TCP (Transmission Control Protocol).....	17
3.4.1.Syn-Flooding : DoS.....	17
3.4.2.Land : DoS.....	18
3.4.3.Out-of-Band (OoB) : DoS.....	18
3.4.4.TCP-Sequenznummer-Angriff (Sequenznummernraten) : Spoofing.....	19
3.4.5.TCP-Hijacking : Man-in-the-Middle.....	19
3.4.6.TCP-Man-in-the-Middle.....	20
3.5.UDP (User Datagram Protocol).....	21
3.5.1.UDP-Flooding : DoS.....	21
3.5.2.UDP-Spoofing.....	21
3.6.DNS (Domain Name Service) und DNS-Spoofing.....	21
A: Quellenangaben.....	23

Abbildungsverzeichnis:

Abbildung 1 : Sniffing.....	8
Abbildung 2 : Denial-of-Service.....	8
Abbildung 3 : Spoofing.....	9
Abbildung 4 : Man-in-the-Middle.....	10
Abbildung 5 : IP.....	12
Abbildung 6 : ICMP.....	15
Abbildung 7 : TCP.....	17
Abbildung 8 : TCP-Sequencenumber-Attack.....	18
Abbildung 9 : TCP-Hijacking.....	19
Abbildung 10 : TCP-Man-in-the-Middle.....	20

0. Einleitung

Nachdem der erste Teil den Begriff Sicherheit mit seinen grundlegenden Aspekten geklärt hat und einen Überblick über die Sicherheit von Hosts gegeben hat, wird der zweite Teil sich nun mit den Sicherheitsproblemen von Netzwerken beschäftigen.

Anhand der Entstehungsgeschichte des Internet soll zuerst verdeutlicht werden, warum die heute verwendeten Netzwerkprotokolle und deren frühe Implementationen fast gar keinen Sicherheitskriterien genügen, die im ersten Teil vorgestellt wurden.

Danach werden die Grundarten von Netzwerkangriffen erläutert, wobei jede eine Verletzung eines bestimmten Sicherheitsmerkmals darstellt.

Schließlich werden die bekanntesten Sicherheitsschwächen der verbreitetsten Netzwerkprotokolle bis zur Darstellungsschicht nach dem ISO/OSI-Referenzmodell vorgestellt, angefangen bei dem Ethernet-Protokoll ARP auf der physikalischen Schicht bis hin zu den Transportprotokollen des Internet.

1. Überblick über die Entstehung des Internet

1.1. Die Entstehung des ARPANET

Das US-amerikanische Militär stellte zur Zeit des kalten Krieges in den späten 50'er Jahren fest, daß es zum einen sehr auf die Unterstützung durch Computersysteme, welche bereits mittels einfacher Netzwerke miteinander verbunden worden waren, angewiesen war und daß zum anderen diese Computersysteme und deren Kommunikation sehr anfällig für Angriffe waren, denn die Zerstörung von nur einem Teil des Netzes, durch Bombenangriffe, Atomschläge, andere Angriffe oder auch Naturkatastrophen, hätte die Zerstörung des gesamten Netzes zur Folge gehabt und damit die Unterbrechung aller Kommunikation. Ein weiteres Problem war die Zentralisierung von Kommunikationseinrichtungen für Kommando- und Kontrollstrukturen. Solche Zentren boten ein ideales Angriffsziel.

Um auch weiterhin eine führende Rolle in der Technologie zu besetzen, wurde 1957 die Advanced Research Projects Agency (ARPA), später in Defense Advanced Research Projects Agency (DARPA) umbenannt, von dem Department of Defense (DoD) gegründet. Die ARPA sponserte viele Forschungen auf dem Gebiet der Netzkommunikation und 1962 wurde erstmals eine Arbeit zur theoretischen Lösung der oben beschriebenen Probleme von der RAND Corporation veröffentlicht. In dieser Arbeit wurde die Theorie von paketvermittelnden Netzwerken entwickelt. Man ging von den Prämissen aus, daß dieses Netzwerk keine zentrale Behörde zur Verwaltung haben dürfe, denn diese wäre ein Angriffspunkt gewesen, und daß das Netzwerk selbst unzuverlässig sei. Es sollte demnach von der Gestaltung her auch dann noch arbeiten, wenn Teile von ihm zerstört wären. Eine große Datenmenge sollte in mehrere Datenpakete aufgeteilt werden, wobei jedes Datenpaket quasi dynamisch und unabhängig von den anderen einen Weg durch das Netz finden sollte. Verlorene oder zerstörte Pakete sollten nochmals übertragen werden.

1967 wurden die Spezifikationen für einen Interface Message Processor (IMP) entwickelt. Die IMP's sollten die inneren Knoten des Netzes darstellen. Jeder Host sollte an einen IMP angeschlossen werden und die IMP's sollten miteinander über ein gemeinsames Protokoll kommunizieren, um die Pakete an den jeweiligen Ziel-Host weiter zu übertragen. Die

Überblick über Sicherheitsprobleme

Zwischenschaltung der IMP's war nötig, weil Computersysteme von verschiedenen Herstellern verbunden werden sollten und dadurch Inkompatibilitäten bestanden.

1969 nahm das ARPANET mit vier IMP's seinen Dienst auf. An das Netz waren das Militär und Forschungseinrichtungen für militärische Forschung angeschlossen.

1970 wurde das neue Network Control Protocol (NCP) vorgestellt, das dann zur Kommunikation zwischen den IMP's eingesetzt wurde. Ein Jahr später wurden die heute immer noch gebräuchlichen Protokolle FTP und Telnet entwickelt.

Probleme traten 1973 auf, als man versuchte, ARPANET-ähnliche Netze durch das ARPANET zu verbinden, denn die inneren Knoten dieser Netze benutzten nicht das NCP. Dieses Problem wurde als „internet problem“ bekannt. Daher entschloß man sich dazu, ein neues Protokoll, das Transmission Control Protocol (TCP), zu entwickeln, das dieses Problem lösen sollte. Zu dem damaligen Zeitpunkt sollte das TCP noch die Aufgaben von IP mit übernehmen. Erst 1977 wurden die verschiedenen Aufgaben unter dem Protokollpaar TCP/IP aufgeteilt. Zur gleichen Zeit wurde das transportunzuverlässige User Datagram Protocol (UDP) entwickelt. Bis 1983 wurde das ARPANET vollständig auf TCP/IP umgestellt.

1.2. Der Übergang zum NFSNET

In den 80' er Jahren entstanden eine Reihe weiterer Netze, denn auch Wissenschaftler, die nicht auf dem Gebiet der militärischen Forschung tätig waren, wollten die Vorzüge der Vernetzung zum wissenschaftlichen Austausch nutzen. 1981 wurde das Computer Science Network (CSNET) gegründet, das Universitäten miteinander verbinden sollte und ausschließlich TCP/IP verwendete, gegründet. 1983 zog sich das US-Militär aus dem ARPANET zurück und gründete sein eigenes Netz, das MILNET.

1984 sah man sich mit dem wachsenden Problemen bei der Namens- und Adressverwaltung in Netzen konfrontiert, so daß der Domain Name Service (DNS) entstand.

Der Anfang vom Ende des ARPANET war die Gründung des NFSNET, finanziert durch die National Science Foundation (NSF). Das NFSNET sollte den Zusammenschluß von vielen Netzen realisieren und war damit der erste backbone.

1.3. Das Internet

Nachdem das NSFNET nach und nach alle Aufgaben des ARPANET übernommen hatte, wurde 1990 das ARPANET aufgelöst. Zu diesem Zeitpunkt waren auch kommerzielle Organisationen daran interessiert, das NSFNET zu kommerziellen Zwecken zu nutzen. Die Entwicklung des WWW 1989 förderte dieses Interesse, denn auch für private Nutzer wurde das weltumspannende Netz nun interessanter. Die kommerzielle Nutzung des Netzes entsprach jedoch nicht den Interessen der NSF, so daß diese 1991 Restriktionen gegen die Übertragung von Paketen mit kommerziellen Inhalt erließ, doch das NSFNET sollte als backbone schließlich durch die Entstehung weiterer backbones 1994 abgelöst werden. Dieses Jahr ist gleichzeitig das offizielle Entstehungsjahr des Internet.

1995 zieht sich die NSF als backbone vollständig aus dem Internet zurück. Gleichzeitig erhalten kommerzielle Onlinedienste wie zum Beispiel America Online (AOL), die bisher nur E-Mails und News mit dem Internet austauschen konnten, vollwertigen Zugang mit echten Gateways, wodurch

Überblick über Sicherheitsprobleme

deren Benutzer nun die volle Anzahl an Diensten des Internet nutzen konnten.

1.4. Fazit zur Entstehungsgeschichte

Die Öffnung des Internet für kommerzielle Dienste bietet der stark steigenden Anzahl von Nutzern neue Möglichkeiten, ihre Computersysteme zu nutzen. Bevor solche Dienste wie WWW das Internet für ein breites Spektrum und eine große Anzahl von Nutzern interessant werden ließ, dienten die Vorgänger des Internet zur Kommunikation und Kooperation zwischen wissenschaftlichen Einrichtungen und Universitäten und wurden auch von solchen unterhalten. Da die Anzahl der Vermittlungsknoten überschaubarer war und die Nutzergruppe eigentlich nur aus wissenschaftlichen oder staatlichen Angestellten und Studenten bestand, war es recht einfach, bei Mißbrauch von Netzen Strafen zur Abschreckung durchzusetzen, denn ein Mißbrauch konnte den Verlust der Arbeitsstelle oder der Nutzungsrechte nach sich ziehen. Zudem waren die Ergebnisse der Wissenschaft ohnehin dazu bestimmt, der Öffentlichkeit zu dienen.

Das heutige Internet besteht aus einer unüberschaubar großen Menge an Nutzern und Hosts. Fast jeder kann sich an dieses Netz über viele verschiedene Provider anschließen. Firmen nutzen das Internet zunehmend, um kommerzielle Dienste anzubieten oder auch zur Kommunikation. Damit ist es nicht nur sehr viel schwieriger geworden, Täter im Internet zurückzuverfolgen und sie zu bestrafen, da teilweise die rechtliche Grundlage dazu fehlt, sondern auch sehr viel wahrscheinlicher für diese Täter, lohnende Beute zu machen oder Schaden mit schwerwiegenden Folgen anzurichten.

Während sich das Internet und deren Nutzung geändert hat, haben sich seine Protokolle, die hauptsächlich dafür gestaltet worden waren, um Verfügbarkeit und Übertragungsintegrität zu gewährleisten, und um eine einfache Kommunikation zu ermöglichen, nicht geändert. Sie enthalten keine Elemente, um solche Sicherheitskriterien wie Vertraulichkeit, Authentizität oder Datenintegrität zu gewährleisten, welche für kommerzielle Zwecke und ernsthafte Nutzung erforderlich wären. Erst der einheitliche Einsatz von Protokollen und Diensten, die solche Sicherheitskriterien im Design erfüllen, werden ein gewisses Grundmaß an Sicherheit in vernetzten Systemen gewährleisten.

2. Grundarten von Netzwerkangriffen

Nachfolgend werden nun die bekanntesten und verbreitetsten Arten von Netzwerkangriffen vorgestellt. Jeder dieser kann dazu dienen, ein bestimmtes Sicherheitsmerkmal zu verletzen. Dabei kann man noch einmal grob unterscheiden zwischen passiven und aktiven Angriffen.

Passive Angriffe sind dadurch gekennzeichnet, daß der Datenverkehr eines Netzes beobachtet, nicht jedoch modifiziert wird. Dadurch ist es auch sehr schwer, passive Angriffe zu entdecken. Da keines der im dritten Kapitel vorkommenden Protokolle eine Verschlüsselung seiner Pakete vorsieht, jene also im Klartext übertragen werden, kann jeder, der ein solches Paket mitliest, sowohl die eigentlichen Daten als auch Protokollinformationen, wie zum Beispiel Absender und Empfänger, erhalten. Dieses Mitlesen von Paketen ist besonders leicht bei Netzwerktopologien durchzuführen, bei denen der Datenverkehr nicht getrennt wird, wie zum Beispiel bei der Bustopologie, so daß jeder an das Netz angeschlossene Kommunikationspartner alle Daten, die über das Netz übertragen werden, mitlesen kann, insbesondere auch solche Daten, die eigentlich nicht für diesen bestimmt sind. Diese Eigenschaft wird jedoch auch von Netzwerkadministratoren zur

Überblick über Sicherheitsprobleme

Analyse oder Verbesserung des Netzwerkes genutzt. Bei elektromagnetischen Übertragungsmedien ist das Mitlesen des Datenverkehrs auch ohne Anschluß ans Netz möglich.

Bei **aktiven Angriffen** wird der Datenverkehr modifiziert. Es können hierbei Daten unrechtmäßig erstellt, geändert oder gelöscht werden, wozu in den meisten Fällen ein Zugang zum Netz erforderlich ist. Diese Art von Angriffen ist durch die Modifikationen leichter zu entdecken, bietet aber gleichzeitig mehrere und schwerwiegendere Möglichkeiten, Schäden zu verursachen.

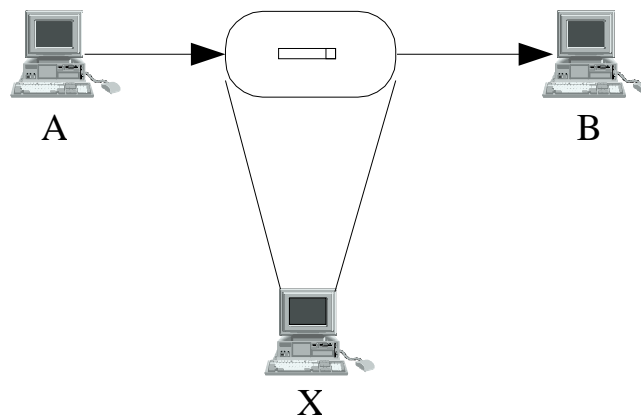


Abbildung 1 : Sniffing

2.1.Sniffing (Netz-Spionage)

Beim Sniffing wird der Datenverkehr beobachtet, um Daten, im Falle eines Angriffes unerlaubt, mitzulesen oder eine Datenverkehrsanalyse durchzuführen, was ihn zum klassischen passiven Angriff macht. Das unerlaubte Mitlesen von Daten dient dazu, geheime Daten, zum Beispiel Paßwörter, zu erhalten, während die Datenverkehrsanalyse eingesetzt wird, um mögliche Angriffspunkte, wie zum Beispiel Server, zu ermitteln. Sniffing kann also auch zur Vorbereitung eines anderen, aktiven Angriffes genutzt werden. Es stellt als unerlaubte Handlung eine Bedrohung des Sicherheitsmerkmals Vertraulichkeit dar.

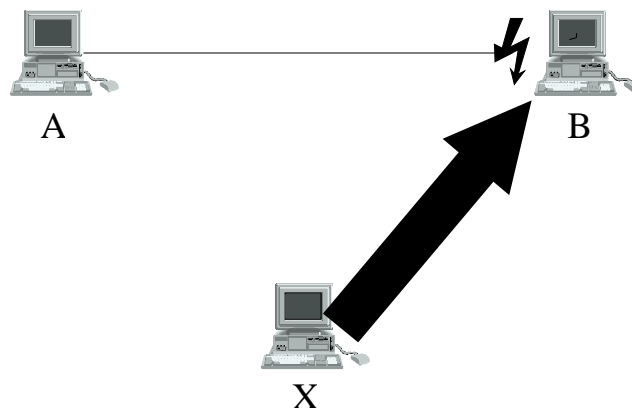


Abbildung 2 : Denial-of-Service

2.2. Denial-of-Service (DoS)

Bei einer Denial-of-Service-Attacke werden Betriebsmittel unrechtmäßig ge- oder verbraucht, so daß eine rechtmäßige Nutzung jener behindert wird oder gar nicht mehr möglich ist. Eine Art der Sabotage also, die durch Überlastung oder vollständigen Verbrauch dazu führt, daß einer oder mehrere Dienste kaum oder gar nicht mehr die an sie gesandten Aufträge erfüllen können. Der Angreifer sendet dabei meist entweder so viele Aufträge an einen Host, daß dieser mit der Bearbeitung der Aufträge voll beschäftigt ist, oder Aufträge, die durch die Ausnutzung einer Schwäche dafür sorgen, daß ein Dienst durch einen schweren Fehler ausgeschaltet wird.

Die Weiterentwicklung dieser Angriffsmethode ist die Distributed-Denial-of-Service-Attacke (DDoS), bei der mehrere zum Teil unfreiwillige Hosts dazu benutzt werden, ein Ziel anzugreifen. Entweder existieren mehrere Angreifer, die sich abgesprochen haben, oder ein Angreifer sucht sich nicht ausreichend geschützte Hosts, installiert dort ein Programm, auch Zombiecode genannt, und startet die DDoS-Attacke, indem er ein Signal an die korrumpierten Hosts sendet, die dann jeder für sich eine DoS-Attacke auf das gemeinsame Ziel durchführen.

DoS ist eine recht verbreitete Form des Angriffs und kann, je nach Abhängigkeit von den Diensten oder dem Dienst, störende oder fatale Auswirkung für den Angegriffenen haben. Solche Angriffe werden zum einen durchgeführt, um einfach Schaden anzurichten, zum anderen, um durch die Blockierung oder Ausschaltung eines Dienstes andere Angriffe starten zu können. Auf jeden Fall stellt eine DoS-Attacke einen Angriff auf die Verfügbarkeit dar.

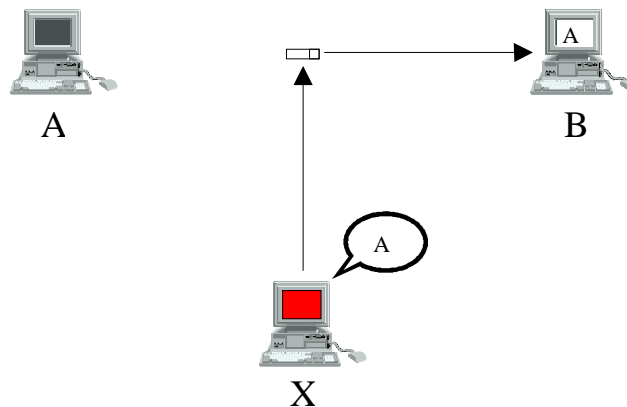


Abbildung 3 : Spoofing

2.3. Spoofing (Maskerade)

Beim Spoofing werden Daten, die zur Identifikation oder Authentikation verwendet werden, ver- oder gefälscht, um die eigene Identität zu verschleiern oder eine falsche Identität vorzutäuschen. Speziell bei Netzwerkprotokollen sind diese Daten meist unverschlüsselt im Protokollkopf enthalten, und ein speziell geschriebenes oder verändertes Programm kann ohne Probleme einen Protokollkopf mit falschen Daten produzieren. Diese Tatsache kann einerseits mißbraucht werden, um einer eventuellen Rückverfolgung zu entgehen oder einen einfachen Filter zu umgehen, wobei die Daten, die zur Identifikation herangezogen werden, dann zufällig gewählt werden können. Andererseits können diese Daten gezielt gewählt werden, um bestimmte Rechte, die mit einer bestimmten Identität verbunden sind, unrechtmäßig zu erwerben. Spoofing untergräbt also die Identifikation oder Authentikation.

Überblick über Sicherheitsprobleme

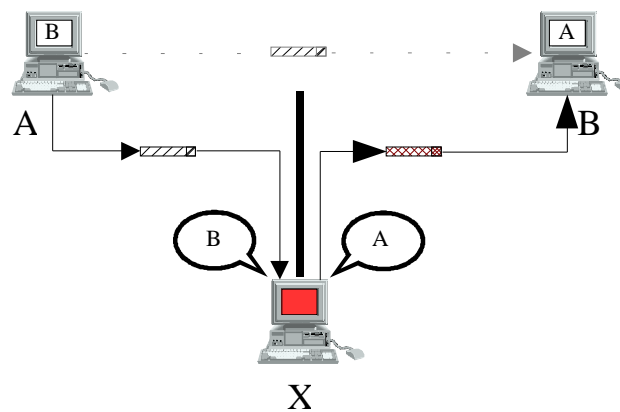


Abbildung 4 : Man-in-the-Middle

2.4. Man-in-the-Middle

Die Man-in-the-Middle-Angriffsmethode bezeichnet eine Angriffsmethode, bei der die Kommunikation oder der Datenverkehr zwischen zwei Kommunikationspartnern ohne deren Wissen manipuliert, umgeleitet oder unterbrochen wird. Die Übernahme eines einzigen Kommunikationsendpunktes wird auch Hijacking genannt.

Die erste Möglichkeit, eine Man-in-the-Middle-Angriffsmethode durchzuführen, sieht den Zugang zu einem Vermittlungsknoten zwischen den beiden Endknoten vor, so daß die Daten, die diesen Knoten passieren, von dem Angreifer manipuliert werden können.

Die zweite Möglichkeit besteht darin, die beiden Kommunikationspartner in dem Glauben zu lassen, die Kommunikation fände nur zwischen ihnen statt, während in Wirklichkeit der Datenverkehr zum Angreifer umgeleitet wird, der dann die Rolle des jeweils anderen Kommunikationspartners übernimmt.

Bei der dritten Möglichkeit wird der Datenverkehr zwischen den beiden Angriffszielen entweder einseitig oder beidseitig unterbunden.

Die Man-in-the-Middle-Angriffsmethode stellt wohl die schwierigste Angriffsmethode dar. Wird sie jedoch erfolgreich durchgeführt, stellt sie die schwerwiegendste Art der Manipulation dar. Beide Kommunikationspartner werden dabei nicht nur geschädigt, sondern verdächtigen sich unter Umständen gegenseitig und kommen nicht auf die Idee, daß sie beide Opfer sind.

3. Sicherheitsschwächen der Internet-Protokolle und deren Implementierungen

Dieser Abschnitt zeigt die bekanntesten Sicherheitsschwächen der verbreitetsten Protokolle von der netznahen, physikalischen Schicht bis zur Darstellungsschicht. Ein grundlegendes Problem in bezug auf Sicherheit resultiert daraus, daß bei den meisten Protokollen der Wille aller Beteiligten zur Kooperation vorausgesetzt wird. Ein unkooperatives Verhalten wird unrealistischer Weise ausgeschlossen.

3.1. ARP (Address Resolution Protocol)

3.1.1. Funktionsweise des ARP

Das Address Resolution Protocol wird zur Zuordnung von IP-Adressen auf physikalische Adressen im Ethernet verwendet. Dies ist notwendig, da Kommunikationspartner im Ethernet technisch gesehen nur über diese physikalischen Adressen, die durch die Hardware fest vergeben sind, miteinander kommunizieren können. Das Netz bleibt trotzdem durch die Vergabe von logischen Adressen, also den IP-Adressen, flexibel.

Um eine Zuordnung der logischen IP-Adresse zur physikalischen Ethernet-Adresse durchzuführen, sendet ein Host, der die Ethernet-Adresse des Empfängers benötigt, ein ARP-Paket, welches die eigene Ethernet-Adresse und die IP-Adresse des Empfängers enthält, per Broadcast. Diese Anfrage wird **ARP Request** genannt. Zusätzlich enthält das Paket meist auch die eigene IP-Adresse, damit der Empfänger nicht per Broadcast antworten muß, wenn ihm das Adreßpaar des Fragenden bekannt ist. Die Antwort, der **ARP Reply**, ist ein Paket, das die Ethernet-Adresse des gesuchten Empfängers enthält.

Die ermittelten Adreßpaare werden für bestimmte Zeit in dem sogenannten ARP-Cache aufbewahrt, um die Anzahl der ARP Request zu senken.

3.1.2. Schwächen des ARP

Ethernet wurde zuerst bei physikalischen und logischen Bustopologien eingesetzt, doch heute wird es, dank der stark gefallen Preise für Switches, mehr und mehr bei logischen Sterntopologien eingesetzt, die eben durch diese Switches realisiert werden. Logische Sterntopologien haben den Vorteil, daß Sniffing zur Datenspionage kaum möglich ist, während dies wiederum bei logischen Bustopologien ein Problem darstellt, sollten die Daten unverschlüsselt über das Netz versendet werden.

3.1.2.1. ARP-Spoofing

Da es bei ARP grundsätzlich keine Möglichkeit gibt, die Angaben im Header zu verifizieren, so wie bei allen Protokollen, die noch vorgestellt werden, kann ein Angreifer diese Daten für unterschiedliche Zwecke fälschen.

3.1.2.2. ARP-Man-in-the-Middle

Ein Angreifer kann die Zuordnung der IP-Adresse zur Ethernet-Adresse manipulieren, indem er fälschlicher Weise auf einen ARP Request verzögert antwortet, so daß die Antwort des tatsächlich gefragten Hosts mit der des Angreifers überschrieben wird. Ebenso ist es möglich, daß der gesuchte Host, weil er abgeschaltet ist oder als Folge einer gezielten DoS-Attacke, nicht antworten kann.

Teilweise verarbeiten Hosts auch die ARP Requests und ARP Replies anderer Hosts und speichern

Überblick über Sicherheitsprobleme

die Angaben im ARP-Cache, um die Anzahl von ARP Requests zu verringern. Dann besteht die Möglichkeit für einen Angreifer, selbst einen ARP Request, am besten mit gleichzeitigem Einsatz von ARP-Spoofing, mit der gewünschten IP-Adresse zu senden und wie oben beschrieben mit der eigenen Ethernet-Adresse darauf zu antworten, womit nach und nach die ARP-Caches verändert werden können. In allen Fällen werden Pakete nun zum Angreifer umgeleitet.

3.1.2.3.ARP-Sturm : DoS

Dieser Angriff nutzt die Tatsache aus, daß es keine Beschränkungen für die maximale Anzahl von zu senden ARP Requests gibt. Daher kann ein Angreifer die Netzlast in einem Ethernet erheblich steigern, indem er so viele ARP Requests wie möglich sendet, ohne die Antworten abzuwarten.

3.1.2.4.ARP-Broadcast-Sturm : DoS

Als Weiterentwicklung des ARP-Sturmes in einem Netz mit Routern kann ein Paket mit einer nicht existenten IP-Adresse per Broadcast verschickt werden. Infolgedessen senden alle Router ein ARP Request, um das Paket weiterverschicken zu können, worauf der Angreifer, mit Angabe einer Ethernet-Broadcastadresse, ein ARP Reply sendet. Die Router sind nun damit beschäftigt, das Paket an alle anderen Host und vor allem sich gegenseitig zu schicken, was zu einem Teufelskreis führt.

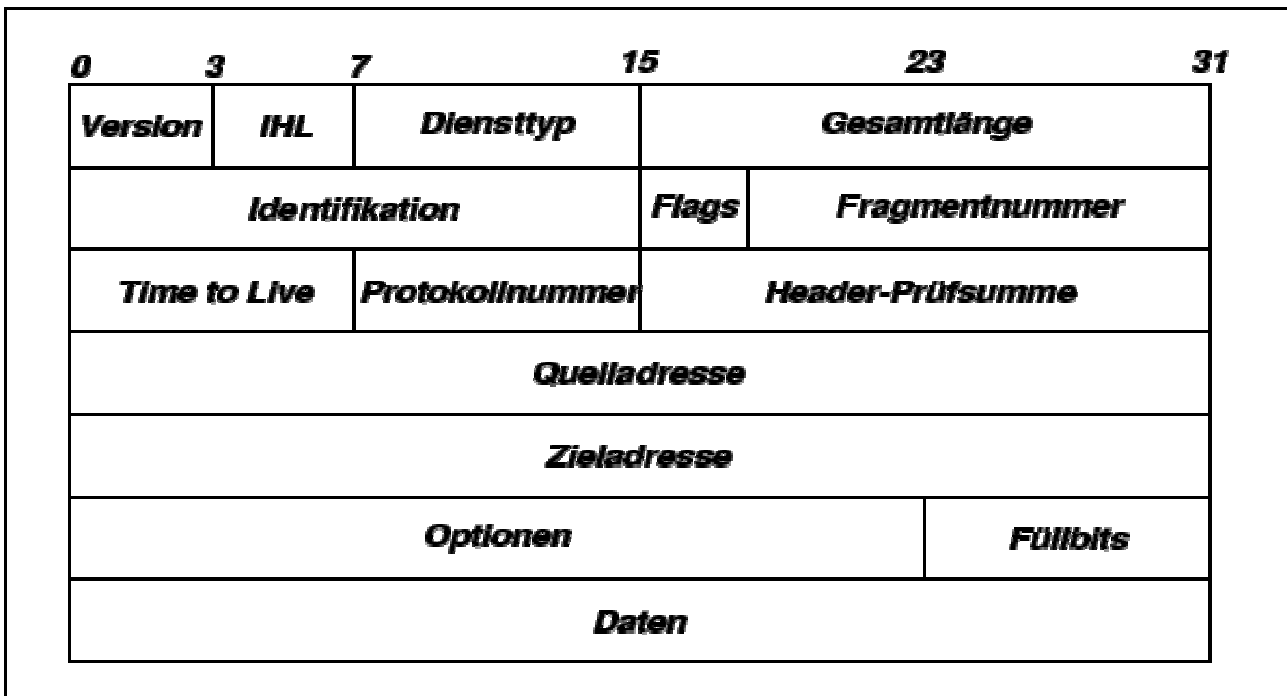


Abbildung 5 : IP

3.2.IP (Internet Protocol)

Nun folgen die bekanntesten Angriffe durch oder mit dem Internet Protocol. Dazu noch zwei kurze Wiederholungen zu IP–Fragmentierung und IP–Strict–Source–Routing.

3.2.1.IP–Fragmentierung

IP erlaubt Pakete inklusive Header mit einer maximalen Größe von 64 KByte oder 65.536 Byte. Es ist jedoch gut möglich, daß ein schichtmäßig darunterliegendes Protokoll nur kleinere Pakete verschicken kann, wie dies zum Beispiel bei Ethernet der Fall ist, denn bei Ethernet können maximal 1.500 Bytes pro Paket übertragen werden. Daher können IP–Pakete in Fragmente, jedes mit einem Header versehen, aufgeteilt werden, welche dann beim Empfänger zu dem ursprünglichen IP–Paket defragmentiert werden. Um dies zu bewerkstelligen, benötigt man Identifikationsnummer, den Fragmentabstand bzw. Fragmentnummer (offset) und die Länge der einzelnen Fragmente.

Fragmente werden anhand der Identifikationsnummer einander zugeordnet und bilden zusammen das eigentliche Paket. Bei jedem Fragment außer beim letzten wird zudem das „more fragments“-Flag gesetzt, welches zum einen eine Fragmentierung beim ersten Fragment und zum anderen anzeigt, daß weitere Fragmente folgen.

Die Fragmentnummer oder offset dient zur Ordnung der einzelnen Fragmente, denn die Fragmente müssen nicht in der richtigen Reihenfolge beim Empfänger eintreffen, und gibt somit die Position innerhalb des eigentlichen Paketes an. Zusammen mit der Länge kann so festgestellt werden, ob noch Fragmente fehlen und beim letzten Fragment, wie groß das eigentliche Paket ist.

3.2.2.IP–Strict–Source–Routing

Strict–Source–Routing ist eine Option des IP, welches die vollständige Route als Abfolge von IP–Adressen, die das betreffende Paket zu durchlaufen hat, vorschreibt. Diese vorgeschriebene Route muß strengstens eingehalten werden.

Diese Option wird aber so gut wie gar nicht verwendet, weshalb sie im allgemeinen zu ignorieren ist.

3.2.3.Schwächen des IP

3.2.3.1.IP-Spoofing

Einer der grundlegendsten Angriffe durch IP ist IP-Spoofing, bei dem die Source-Address ver- oder gefälscht wird, um Rückverfolgung zu entgehen oder sich als anderer, vertrauenswürdiger Host auszugeben. Letzteres ist vor allem dann gravierend, wenn die IP-Adresse zur Authentikation verwendet wird, wie bei den bekannten r-Kommandos unter Unixsystemen. Ein Problem beim Spoofing ist jedoch, daß die Antworten für den Angreifer, der Spoofing einsetzt, unsichtbar sind, wenn er jene nicht zu sich umleiten bzw. abfangen oder sniffen kann.

3.2.3.2.Source-Routing-Attacke : DoS

Wird die Source-Routing-Option von Routern berücksichtigt, ist es möglich, Sicherheitsmaßnahmen zu umgehen, beispielsweise abgesicherte Vermittlungsknoten. Ebenso kann das Problem der unsichtbaren Antworten beim Spoofing abgeschwächt werden, denn die Antwort wird ebenfalls unter Verwendung von Source-Routing verschickt, was es leichter macht, diese Antworten zu sniffen oder umzuleiten bzw. abzufangen.

3.2.3.3.Ping-of-Death : DoS

Ping-of-Death nutzt eine fehlerhafte Implementierung bei der Fragmentierung aus. Ältere Versionen von MS Windows 95 erlaubten es, ein Ping zu senden, dessen Gesamtgröße die zugelassenen 64 KByte überstieg. Dies führte bei vielen Systemen beim Zusammensetzen der Fragmente zu einem bufferoverflow und damit zum Absturz. Es gab keine Fehlerbehandlung oder auch nur Erkennung, wenn die Fragmentnummer und die Länge des letzten Fragmentes ein zu großes ursprüngliches Paket ergaben. Heutzutage sind die meisten Systeme einem solchen Angriff gegenüber immun.

3.2.3.4.Tiny-Fragment-Attacke

Diese Attacke wird dazu benutzt, spezielle Sicherheitsmaßnahmen, die statisch Nutzinformationen wie TCP-Header überprüfen, zu umgehen. Dazu werden die Pakete geschickt fragmentiert, so daß die Information über mehrere Fragmente verteilt ist. Die Taktik, einen Angriff durch viele kleine Schritte zu verbergen, wird auch manchmal Salami-Taktik genannt. Einige Paketfilter überprüfen zum Beispiel nur das erste Fragment, welches in diesem Falle wenig aussagekräftig ist, wenn ein TCP-Header und dessen Port-Informationen auf mehrere Fragmente verteilt und nicht analysiert bzw. erkannt werden kann. Hier hilft es, Pakete erst dann weiterzusenden, wenn das komplette Paket übermittelt, zusammengesetzt und überprüft wurde.

3.2.3.5.Overlapping-Fragment-Attacke (Teardrop)

Eine weitere Möglichkeit, verdächtige Informationen zu verstecken, ist die Overlapping-Fragment- oder Teardrop-Attacke. Hierbei wird ausgenutzt, daß oft nicht überprüft wird, ob durch die Fragmentnummer-Angabe (offset) sich Pakete überschneiden. Wird ein Paket durchgelassen, wenn die ersten Fragmente keine verdächtigen Header-Informationen enthalten, so können diese durch spätere Fragmente, die die verdächtigen Informationen enthalten, durch Wahl einer entsprechenden Fragmentnummer (offset) überschrieben werden. Auch hier hilft es ein Paket erst vollständig zusammensetzen und dann zu analysieren.

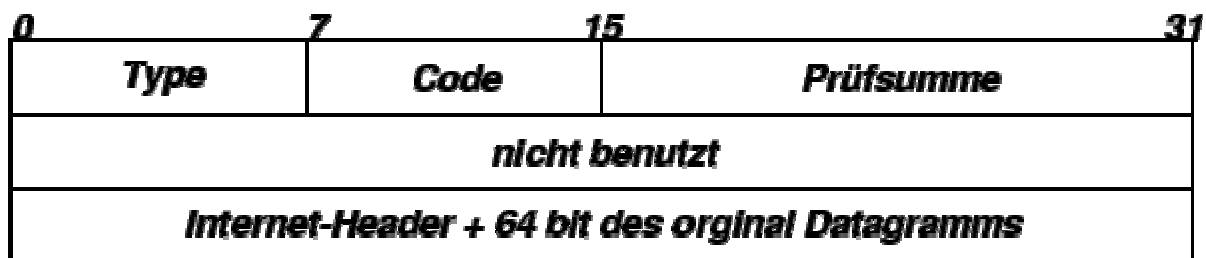


Abbildung 6 : ICMP

3.3.ICMP (Internet Control Message Protocol)

Durch das ICMP werden Status und Kontrollmeldungen zwischen Hosts ausgetauscht. Es ist ein integraler Bestandteil vom IP, obwohl es wie ein Transportprotokoll auf IP aufsetzt. Durch die Felder Typ und Code im ICMP-Header wird die Bedeutung der Nachricht angezeigt.

3.3.1.Ping-Flooding : DoS

Während beim normalen Ping in einigen Abständen ein Echo Request (Typ 8 Code 0) als Anfrage und als Antwort ein Echo Reply (Typ 0 Code 0) gesendet wird, werden beim so genannten Ping-Flooding so viele Echo Requests wie möglich gesendet, wodurch der angegriffene Host mit der Beantwortung der übermäßig vielen Anfragen voll beschäftigt wird.

3.3.2.Smurf (ICMP-Sturm) : DoS

Setzt man gezielt Spoofing beim Ping-Flooding ein, kann der Angreifer die Anzahl der Echo Requests noch erheblich steigern. Dazu startet der Angreifer ein Ping-Flooding auf eine Broadcastadresse und spooft die Source-Address mit der Adresse des anzugreifenden Hosts. Natürlich kann als Source-Address ebenfalls eine Broadcastadresse angegeben werden.

3.3.3.ICMP–Destination–Unreachable (Typ 3) : DoS

Um einen Host vom Netz gezielt abzukoppeln, sendet der Angreifer ein ICMP–Paket mit der Destination–Unreachable Nachricht und gespoofter Adresse des anzugreifenden Hosts. Ein Host, der solch eine Nachricht erhält, wertet entweder den mitgeschickten Datenteil aus und kappt die entsprechende Verbindung oder kappt alle Verbindungen zu dem angegriffenen Host, wenn der Datenteil nicht ausgewertet wird, was vor allem bei älteren Implementationen der Fall war. Werden solche ICMP–Pakete auch von einem Vermittlungsknoten ausgewertet, sendet dieser für eine bestimmte Zeit, bei Erhalt eines Paketes mit der entsprechenden IP–Adresse, gleich selbst ein ICMP–Destination–Unreachable für diese IP–Adresse.

3.3.4.ICMP–Fragmentation–Needed–And–DF–Set (Typ 3, Code 4) : DoS

Diese Nachricht wird verschickt, wenn eine Fragmentierung nötig wäre, weil das zu vermittelnde Paket zu groß ist, jedoch durch das gesetzte Don't–Fragment–Flag (DF) untersagt ist. Ein Angreifer kann die Netzlast merklich erhöhen, indem er durch das Senden von ICMP–Fragmentation–Needed–And–DF–Set Nachrichten immer kleinere Pakete fordert.

3.3.5.ICMP–Source–Quench (Typ 4) : DoS

Ist der Puffer eines Hosts überlastet, sendet dieser den Sender oder Sendern von Paketen ICMP–Source–Quench Nachrichten, um dessen oder deren Übertragungsrate zu senken bis die gewünschte Übertragungsrate, mit der der Host arbeiten kann, erreicht ist. Wenn ein Angreifer ständig ICMP–Source–Quench Nachrichten verschickt, kann er dadurch den Datenverkehr sehr verlangsamen, indem er dabei die IP–Source Adressen spooft. Mit dieser Angriffsmethode lassen sich auch gezielt Vermittlungspfade ändern.

3.3.6.ICMP–Redirect (Typ 5) : Man–in–the–Middle

Die ICMP–Redirect Nachricht soll der Performancesteigerung im Netz dienen und kann von einem Host abgeschickt werden, wenn dieser eine bessere Route zu einem Empfänger gefunden hat. Zum Beispiel soll ein Vermittlungsknoten B ein Paket, das er von Vermittlungsknoten A erhalten hat, an den Empfänger weiterleiten. Ist B überlastet oder Vermittlungsknoten C besser geeignet, solche Pakete zum Empfänger zu vermitteln, kann B durch ein ICMP–Redirect A mitteilen, daß Pakete für bestimmte Hosts oder Netze direkt an C zu schicken sind.

Dies kann von einem Angreifer mißbraucht werden, um den Netzwerkverkehr zu sich umzuleiten, indem er ICMP–Redirects mit gespoofter Source–IP–Address verschickt. Dies kann als Vorbereitung für weitere Angriffe benutzt werden.

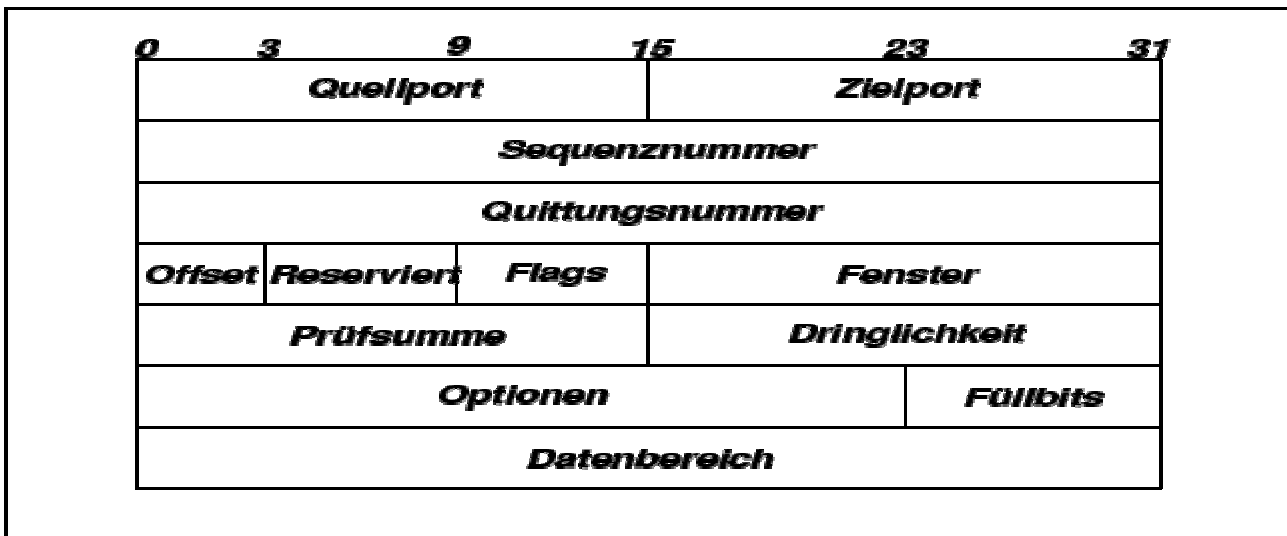


Abbildung 7 : TCP

3.4.TCP (Transmission Control Protocol)

Das TCP ist das verbindungsorientierte Protokoll der Transportschicht, welches eine zuverlässige Übertragung garantiert, und wird von den meisten Internetdiensten genutzt. Zuverlässige Übertragung heißt, daß das TCP Übertragungsfehler wie Reihenfolgenvertauschung, Verlust von Paketen und Verdoppelung von Paketen behandelt, die die unteren Schichten nicht abfangen können. Die Kommunikationsendpunkte werden jeweils durch die IP Adresse und die Portnummer, die dem Dienst bzw. dem Client-Programm zugeordnet ist, identifiziert.

Der Verbindungsaufbau wird beim TCP durch einen Three-Way-Handshake etabliert. Zuerst sendet der Client ein TCP-Paket mit gesetztem SYN-Flag. Der Host sendet, wenn die Verbindung zugelassen wird, eine Antwort mit gesetztem SYN- und ACK-Flag, um den Verbindungsaufbau zu bestätigen. Beim dritten Schritt bestätigt wiederum der Client den endgültigen Verbindungsaufbau mit gesetztem SYN-Flag. Der weitere Datenaustausch verläuft als Vollduplexverbindung.

Um die zuverlässige Übertragung zu gewährleisten, wird jedes Paket durch eine Sequenznummer identifiziert, die beim Verbindungsaufbau zufällig gewählt werden soll. Der ordentliche Empfang von Paketen wird durch die Quittungsnummer bestätigt, die immer die nächste noch nicht erhaltene Sequenznummer angibt. Die Quittungsnummer wird dabei immer um die empfangene Datenmenge erhöht, wodurch deren Empfang bestätigt wird.

3.4.1.Syn-Flooding : DoS

Eine Verbindung, die zwar vom Clienten initiiert aber noch nicht durch den dritten Schritt vollständig aufgebaut wurde, wird halboffene Verbindung genannt. Der sogenannte Backlog-Wert gibt die maximale Anzahl von gleichzeitig halboffenen Verbindungen für den Server an. Ist dieser Wert erreicht, nimmt der Server keine weiteren Verbindungsanfragen an, bis eine halboffene Verbindung entweder durch den Clienten endgültig aufgebaut oder durch Zeitüberschreitung abgebrochen wird.

Überblick über Sicherheitsprobleme

Syn-Flooding ist eine DoS-Attacke, bei der so viele Verbindungsanfragen wie möglich an den angegriffenen Server geschickt werden, ohne jemals vollständig etablieren zu werden. Ist der Backlog-Wert im Verhältnis zur Übertragungsrate und dem Zeitüberschreitungswert zu klein gewählt, ist der Server durch die massiven Verbindungsanfragen für rechtmäßige Clients blockiert.

3.4.2.Land : DoS

Bei der Land-Attacke bringt man den Server, sofern er nicht gegen diese Art von Attacke geschützt ist, dazu, sich selbst zu blockieren. Dazu schickt ein Angreifer Pakete mit gesetztem SYN-Flag und gespooften IP-Adressen zum anzugreifenden Server. Die Besonderheit dieses Angriffs besteht darin, daß die Source- und Destination-Adresse identisch und gleich der des Servers, die Portadressen jedoch verschieden sind. Der Server antwortet so auf seine vermeintlich eigenen Pakete. Noch schlimmer wird es, wenn der Server sein Antwortpaket mit gesetztem SYN- und ACK-Flag als Verbindungsaufbau interpretiert.

3.4.3.Out-of-Band (OoB) : DoS

Dieser Angriff macht sich eine fehlerhafte Implementation von NETBEUI seitens Microsoft zunutze. Werden Daten, die nicht der Norm entsprechen, an Port 135 oder 139 geschickt, führt das bei älteren, ungeschützten Microsoftsystemen zum Absturz.

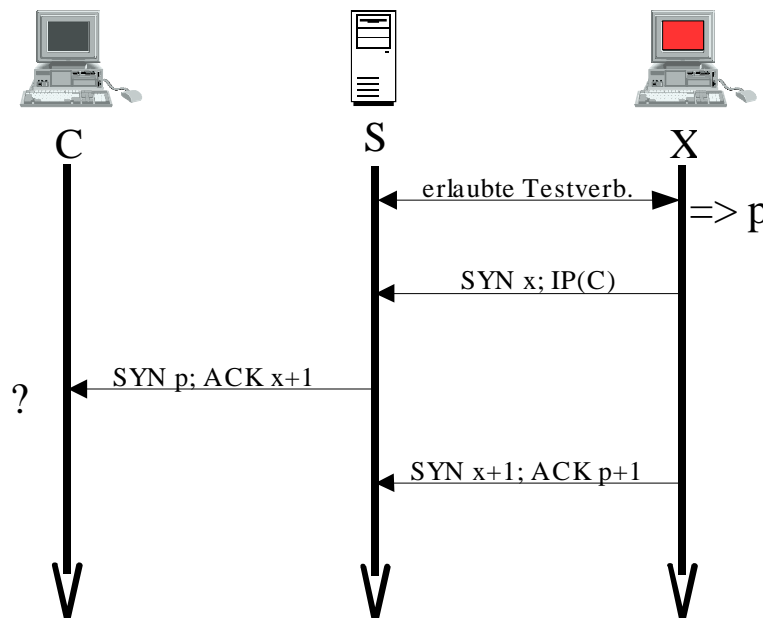


Abbildung 8 : TCP-Sequence-Number-Attack

Überblick über Sicherheitsprobleme

3.4.4. TCP-Sequenznummer-Attack (Sequenznummernraten) : Spoofing

Wie weiter oben erwähnt, sollte die Sequenznummer beim Verbindungsaufbau zufällig gewählt werden. Bei vielen Systemen wird die Sequenznummer jedoch quasi deterministisch gewählt und kann über die letzte Sequenznummer erraten werden. Diesen Umstand kann sich ein Angreifer zunutze machen, um unerlaubte Verbindungen aufzubauen. Dazu baut er eine erlaubte, harmlose Testverbindung zum anzugreifenden Server auf, um so die Sequenznummer für den nächsten Verbindungsaufbau zu raten. Dann initiiert er eine für ihn unerlaubte Verbindung mit gespoofter Source-Adresse. Die Antwort des Servers kann der Angreifer nicht sehen. Zum endgültigen Etablieren der Verbindung sendet der Angreifer die Rückantwort mit der aus der Testverbindung geratenen Sequenznummer. Auch wenn für den Angreifer weiterhin die Schwierigkeit besteht, daß die Antworten des Servers unsichtbar sind, so kann er doch zum Beispiel bei den r-Kommandos einen Befehl an den Server schicken. Dieser Befehl könnte dem Angreifer dann Tür und Tor zum Server öffnen. Dazu ist noch zu bedenken, daß die Rückmeldungen des Servers bei vielen Befehlen bekannt sind oder erraten werden können, wodurch es möglich ist, auf die Datenmenge der Antworten zu schließen.

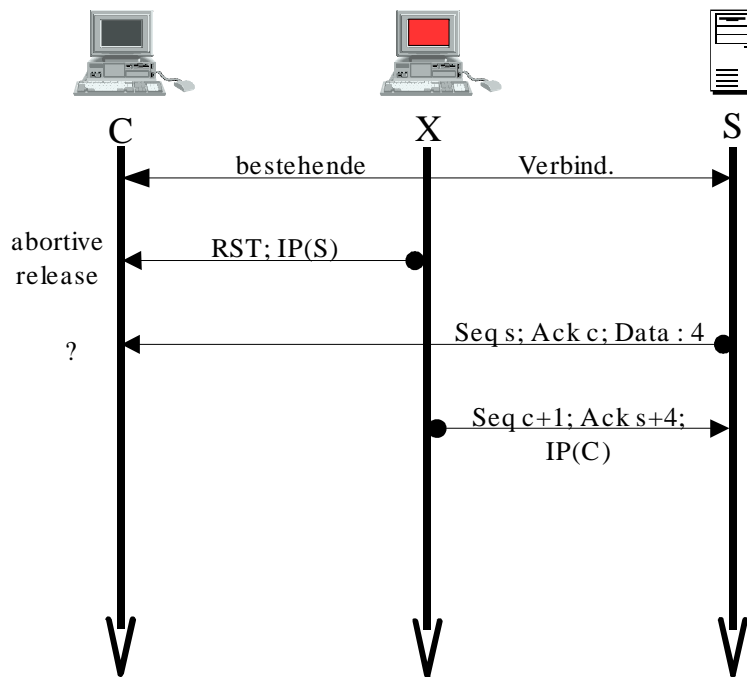


Abbildung 9 : TCP-Hijacking

3.4.5. TCP-Hijacking : Man-in-the-Middle

Das TCP-Hijacking zielt darauf ab, eine bereits bestehende Verbindung zwischen zwei Hosts an einem Ende zu übernehmen. Dies kann genutzt werden, um Authentikationsmechanismen zu umgehen.

Hat der Angreifer nicht die Möglichkeit, die Verbindung zu sniffen, müssen die Sequenznummern über das Sequenznummernraten, das weiter oben beschrieben wurde, ermittelt werden. Der

3.5.UDP (User Datagram Protocol)

Das UDP ist im Gegensatz zum TCP ein verbindungsloses, unzuverlässiges Transportprotokoll. Unzuverlässig deshalb, da es nicht garantiert, daß die Datenpakete ihr Ziel erreichen und wenn, gibt es ebenso keine Garantie für den Empfang der Pakete in der korrekten Reihenfolge. Eine Fehlerkontrolle ist ebensowenig vorgesehen. Der Vorteil des UDP ist ein kleinerer und einfacherer Header, was zu einer Erhöhung des Datendurchsatzes führt. Es verwendet wie das TCP Portnummern zur Adressierung.

Benutzt wird dieses Protokoll unter anderem vom alten NFS (Network File System) und dem DNS (Domain Name Service).

3.5.1.UDP-Flooding : DoS

Wie bei jedem anderen der bereits vorgestellten Protokolle, ist auch beim UDP möglich, einen Host oder einen UDP-Dienst durch das massive Verschicken von Paketen zu blockieren oder zum Absturz zu bringen.

3.5.2.UDP-Spoofing

Beim UDP ist es noch einfacher als beim TCP, Pakete zu fälschen, da keine Möglichkeit zur Identifikation existiert, denn das UDP verwendet keine Sequenz- bzw. Quittungsnummern. Eine Identifikation kann also nur über IP-Adressen erfolgen. Dies ist vor allem bei der Benutzung durch das NFS kritisch.

3.6.DNS (Domain Name Service) und DNS-Spoofing

Der Domain Name Service ist ein hierarchisch strukturierter Dienst und bietet die Möglichkeit, IP-Adressen auf Domain-Namen und umgekehrt abzubilden. Dies macht es für den Menschen sehr viel einfacher, die verschiedenen Dienste im Internet oder in anderen internetbasierten Netzen zu nutzen. Jeder DNS-Server hält die Zuordnungen für eine begrenzte Zeit im DNS-Cache, da sich die Zuordnungen auch ändern können. Befindet sich eine gefragte Zuordnung nicht im Cache, wird eine Anfrage an einen anderen DNS-Server, meistens einer, der in der Hierarchie höher steht, gesendet. So wird die baumartige Hierarchie solange durchlaufen bis die Zuordnung gefunden wird.

Eine in jüngster Zeit ausgenutzte Schwachstelle dieses Systems sind die sogenannten Root-DNS-Server, welche die höchste Ebene der Hierarchie bilden. Würden diese Root-DNS-Server durch (D)DoS-Attacken für längere Zeit erfolgreich blockiert, könnten die Caches der darunterliegenden DNS-Server nicht mehr erneuert werden und das Internet könnte blockiert sein.

Ein weiterer Angriff mittels DNS erlaubt es, den Cache eines ungeschützten DNS-Servers zu verändern, was benutzt werden kann, um den Datenverkehr von Hosts, die auf diesen DNS-Server

Überblick über Sicherheitsprobleme

zugreifen, umzuleiten. Ungeschützt ist ein DNS-Server dann, wenn er Änderungen des DNS-Caches von nicht vertrauenswürdigen DNS-Servern oder Hosts, die sich als solche ausgeben, zulässt. Eine Möglichkeit, diesen Angriff durchzuführen, besteht darin, daß der vermeintliche DNS-Server des Angreifers einen gefälschten DNS-Eintrag enthält. Wenn er Datenverkehr zu sich selbst umleiten will, wird in dem gefälschten Eintrag der Name des anzugreifenden Servers der IP-Adresse des Angreifers zugeordnet. Der Angreifer fordert nun vom anzugreifenden DNS-Server Einträge zur eigenen Seite. Der angegriffene DNS-Server fragt nach diesen Einträgen beim vermeintlichen DNS-Server des Angreifers nach. Ist der angegriffene DNS-Server ungeschützt, akzeptiert er ebenfalls den gefälschten Eintrag.

A: Quellenangaben

[Hans-Joachim Mück, Carsten Benecke, Stefan Kelm 2000] :
Bericht 224 : „Sicherheit in vernetzten Systemen“

Internet :

<http://www.tecchannel.de/internet/682/5.html> [Peter Klau 2001]

<http://www.computerbetrug.de/netzwerk/angriffe.php>

[http://www.computec.ch/dokumente/
denial-of-service/
denial-of-service/denial-of-service.html](http://www.computec.ch/dokumente/denial-of-service/denial-of-service/denial-of-service.html) [Marc Ruef 2000]
[ip-fragmentierung/ip-fragmentierung.txt](http://www.computec.ch/dokumente/ip-fragmentierung/ip-fragmentierung.txt) [mr.gentleman]
[tcp-ip-angriffe/tcp-ip-angriffe.html](http://www.computec.ch/dokumente/tcp-ip-angriffe/tcp-ip-angriffe.html)
[tcp-ip/arp_rarp_und_proxy_arp/arp_rarp_und_proxy_arp.html](http://www.computec.ch/dokumente/tcp-ip/arp_rarp_und_proxy_arp/arp_rarp_und_proxy_arp.html) [Marc Ruef 2000]
[allgemein/konzeption_und_realisierung/dip.html](http://www.computec.ch/dokumente/allgemein/konzeption_und_realisierung/dip.html) [Klaus Bauer 1999]

<http://library.succurit.com/unsorted/german/icmp.txt> [Marc Ruef 2000]

http://www.sans.org/rr/firewall/DNS_spoof.php

<http://www.all.net/journal/netsec/1995-08.html> [Dr. Frederick B. Cohen & Associates 1996]

<http://mitglied.lycos.de/rapidwien/KOMPLETT.PDF> [Helmut Wimmer 1997] : „Zur Konvergenz von Technologie und Denken; Hypertext und Internet“

http://www.mt.haw-hamburg.de/home/martini/OPN_sicherheit.pdf [Prof. Dr. Nils Martini 2002] : „Sicherheit im Internet“

http://www.id.ethz.ch/aktuell/veranstaltungen/IDForum/000616_folien/sicherheitsaspekte.pdf [Prof. B. Plattner] : „Sicherheitslücken in den Internetprotokollen“

RFC 792 (u.a. ip-source-querch)