Micha Borrmann, Sebastian Schreiber

Wer zählt, gewinnt

Wiederentdeckung eines 20 Jahre alten IP-Header-Eintrags

Eine fast in Vergessenheit geratene Funktion des Internet-Protokolls TCP/IP ermöglicht heimliche Lastmessungen auf Internet-Servern, versteckte Port-Scans und das Aufspüren versteckter Rechner hinter einem NAT-Router.

Die IP-ID ist regulärer Bestandteil des IP-Headers und wurde bereits 1981 mit RFC 791 eingeführt. Diese ID soll IP-Pakete eines Rechners voneinander unterscheiden, damit der Empfänger fragmentierte Pakete richtig zuordnen kann. Im Lauf der Jahre ist die IP-ID fast in Vergessenheit geraten, auch weil Fragmentierung mittlerweile kaum mehr auftritt. Die meisten Internet-Provider verbieten das Zerlegen von Paketen in ihren Backbones über das „Don't Fragment"-Bit, um keine Bandbreite für fast leere Frames zu verschwenden.

Doch in letzter Zeit hat die IP-ID eine wahre Renaissance erlebt, verrät sie doch einiges über den Absender. Das kommt daher, dass die meisten Betriebssysteme die IP-ID für jedes neue Paket um eins erhöhen – oder einen anderen konstanten Wert. Sendet man an einen Internet-Server zwei Ping-Pakete, kann man aus der Differenz der IP-IDs der Antworten Rückschlüsse über dessen anderweitige Aktivitäten ziehen. Weiß man beispielsweise, dass das Betriebssystem des Zielrechners die IP-ID immer um eins erhöht und die zweite IP-ID um 17 größer ist als die des ersten Antwortpakets, hat der Server zwischen den beiden Pings 16 andere Pakete verschickt.

Das klingt zunächst unspektakulär, lässt sich jedoch durch regelmäßige Ping-Pakete schon zu einer Art heimlicher Lastmessung ausnutzen. Der Abstand zwischen den IP-IDs zweier Messungen vermittelt einen Eindruck davon, wie viel der Ziel-Server gerade zu tun hat. Die Grafik rechts illustriert das Ergebnis einer solchen Messung auf www.heise.de und www.stern.de über einen Zeitraum von 48 Stunden (Freitag 00:00 bis Samstag 24:00). Es ist gut zu sehen, dass Freitags deutlich mehr Surfer heise online und die Web-Seiten des Stern besuchen als am Samstag und dass die Rushhour bei den Servern auf die Mittagszeit fällt.

Anstelle von Ping-Paketen kann man übrigens auch jedes beliebige andere IP-Paket verwenden, das eine Antwort des angespochenen Rechners provoziert – also beispielsweise einen regulären Abruf einer Web-Seite. Am einfachsten bekommt man IP-ID-Sequenzen mit dem Unix-Tool hping2 (siehe Softlink) zu sehen:

```
# hping -c 3 -p 80 192.168.0.1
HPING (eth0 192.168.0.1): NO FLAGS are set
len=46 ip=192.168.0.1 id=1351
len=46 ip=192.168.0.1 id=1352
len=46 ip=192.168.0.1 id=1353
```

Dieser Aufruf führt einen so genannten TCP-Ping auf dem Web-Server-Port 80 durch. Der hier angesprochene Linux-Rechner zählt die IP-ID tatsächlich sequenziell hoch (die hping-Ausgabe wurde zugunsten der Übersichtlichkeit gekürzt).

Hinter dem Router

Mit einem NAT-Router können sich mehrere Rechner eine Internet-Verbindung so teilen, dass nach außen nur eine IP-Adresse sichtbar ist. Manche Internet-Provider wie T-Online verbieten jedoch in ihrem Nutzungsvertrag die parallele Nutzung eines Flatrate-Zugangs durch mehrere Personen. Da bei Verbindungen nach außen immer nur die externe IP-Adresse des Routers in Erscheinung tritt, war man lange Zeit überzeugt, dass ein solcher Missbrauch schon technisch gar nicht nachweisbar wäre.

Doch wie der amerikanische Sicherheitsexperte Steven Bellovin zeigte, wurde dabei die Rechnung ohne die IP-ID gemacht [1]. NAT-Router verändern diese nämlich bei den weitergeleiteten Paketen nicht. Sind in einem Netz hinter einem NAT-Router zwei Rechner gleichzeitig aktiv, versendet er beispielsweise Pakete mit den IP-IDs

30, 31, 4989, 32, 33, 4990, 4991

Die 30er stammen von dem einen System, die jenseits der 4000 vom anderen. Trägt man die IP-IDs gegen die Zeit auf, ergeben sich zwei Geraden. Für die Grafik auf Seite 213 oben haben wir sogar fünf aktive Systeme hinter einem NAT-Router beobachtet. Schon nach wenigen Minuten erhielten wir fünf deutlich unterscheidbare Geraden. Nebenbei sei noch bemerkt, dass sich die Pakete auch durch ihre Time-To-Live (TTL) unterschieden, die Unix-artige Systeme standardmäßig auf 64 und Windows-Rechner auf 128 setzen. Hinter dem Router, der sie um eins herabgesetzt hatte, ergaben sich damit die Werte 63 und 127.

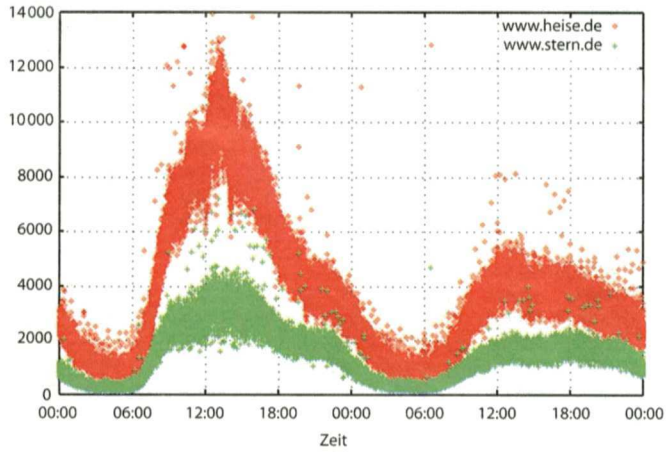
Nutzen die Rechner hinter dem NAT-Router einen gemeinsamen, lokalen Proxy (also nicht den des Providers), funktioniert diese Erkennungsmethode jedoch nicht mehr. Denn alle Verbindungen nach draußen gehen dann ja tatsächlich von einem einzigen Rechner aus.

Cluster-Forschung

Große (E-Commerce-)Sites werden häufig aus Performance-Gründen auf mehrere Systeme verteilt, die unter einer einzigen IP-Adresse erreichbar sind. Dabei tritt oft ein ähnlicher Effekt auf wie bei den Rechnern hinter dem NAT-Router: Die IP-IDs springen scheinbar wahllos. Trägt man die ermittelten IDs jedoch grafisch gegen die Zeit auf, sieht man mehrere gerade Linien. Sie rühren daher, dass jeder der Server die IP-ID sequenziell hochzählt, aber die einzelnen Anfragen bei unterschiedlichen Systemen landen.

Allerdings sind dabei mehrere Fallstricke zu beachten. So reichen die meisten Load-Balancer Ping-Anfragen gar nicht an die Server weiter, sondern beantworten sie gleich selbst – sofern sie nicht ganz gefiltert werden. Erst TCP-Pings auf den Webserver-Port 80 landen bei den Cluster-Rechnern. Und bei weiterentwickelten Load-Balancern hilft nicht einmal das: Der BigIP-Load-Balancer vor heise online beantwortet beispielsweise alle Verbindungs-Anfragen zunächst selber, sodass man immer nur dessen IP-IDs sieht. Die Cluster-Rechner bleiben unsichtbar im Hintergrund.

Die Grafik auf Seite 213 zeigt die IP-IDs von regelmäßigen Web-Anfragen auf reiseauskunft.bahn.de. Es ist deutlich zu erkennen, dass zu jedem Zeitpunkt drei verschiedene IP-ID-Folgen



Über die Differenzen der IP-IDs lassen sich heimliche Lastmessungen bewerkstelligen.

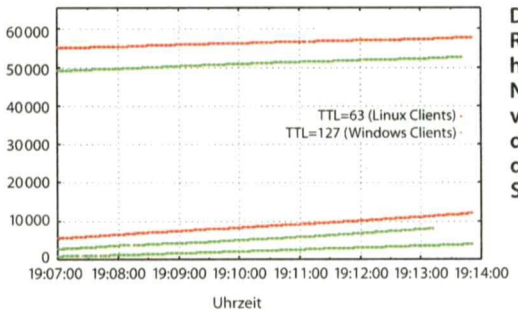
aktiv sind. Eine der Geraden verläuft flacher als die anderen beiden, was bedeutet, dass der Server weniger Pakete versendet. Vermutlich handelt es sich um ein schwächeres System.

Falsche Fährten

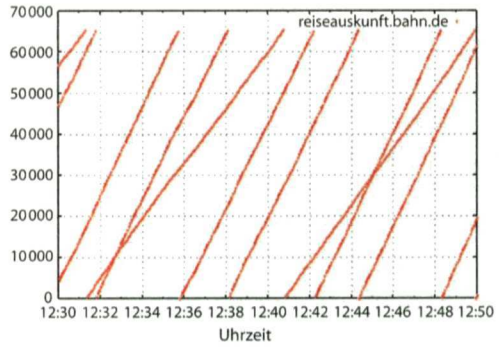
Ein Angriff auf ein System wird oft durch einen Port-Scan vorbereitet, der feststellen soll, welche Dienste auf einem Rechner erreichbar sind. Mittlerweile versuchen viele Intrusion-Detection-Systeme (IDS) und auch Personal Firewalls, solche Port-Scans zu erkennen, und schlagen dann Alarm. Oft hagelt es anschließend erboste Mails an den vermeintlichen Übeltäter beziehungsweise dessen Provider. Doch immer öfter erwischen sie dabei den Falschen. Denn mit Hilfe der so genannten Idle-Scans gelangen gewiefte Hacker an die gewünschten Informationen, ohne dass ein einziges Paket mit ihrer eigenen IP-Adresse beim Ziel ihrer Neugier ankommt und dort registriert werden könnte.

Auch dabei übernimmt die IP-ID eine Schlüsselrolle. Der Hacker sucht sich dafür zunächst ein momentan inaktives Opfer, das die IP-ID einfach hochzählt. Diesen Idle-Host deckt er mit einem kontinuierlichen Strom von Paketen ein. Dann sendet er ein Paket mit der Absenderadresse des Idle-Hosts an sein eigentliches Opfer. Abhängig davon, ob der angesprochene Port offen war oder nicht, tauscht dieser danach ein oder mehrere Pakete mit dem Idle-Host aus. Dies registriert der Angreifer durch Sprünge in der IP-ID-Sequenz. Da diese bei einem offenen Port anders ausfallen als bei einem geschlossenen, hat er damit die gewünschte Information. Details zur Funktionsweise von Idle-Scans können Sie im Artikel „Heimliche Scans und falsche Fährten" auf heise Security (www.heisec.de) nachlesen.

Ob ein Rechner über seine IP-IDs Informationen preisgibt, hängt davon ab, wie sie das Betriebssystem vergibt. Windows geht den einfachsten Weg und erhöht die IP-ID für jedes Paket um eins. Ältere Versionen wie NT 4 erhöhen sie um 256 pro Paket. Solche einfachen Sequenzen lassen sich jedoch mit ähnlichen Verfahren analysieren. Linux ab Kernel-Version 2.4.x



Die fünf Rechner hinter dem NAT-Router verraten sich durch eindeutige IP-ID-Sequenzen.



Die grafische Auswertung der IP-IDs zeigt, dass bei der Reiseauskunft der Bahn drei Rechner die Anfragen bearbeiten.

setzt die IP-ID bei TCP- und UDP-Paketen auf Null, wenn es als Server fungiert, also auf eingehende Anfragen antwortet. Um Verwechslungen bei fragmentierten Paketen zu vermeiden, setzt es dabei das Don't-Fragment-Bit. Lastmessungen auf Servern via TCP-Ping funktionieren damit nicht mehr. Bei ICMP-Paketen (Ping) und ausgehenden Verbindungen zählt der Linux-Kernel die IP-ID jedoch nach wie vor sequenziell hoch. Somit lassen sich Linux-Clients hinter einem NAT-Router nach wie vor aufspüren.

Ein komplizierteres Verfahren hat Sun für Solaris implementiert: Aktuelle Solaris-Systeme verwenden für jedes Zielsystem, mit dem sie Pakete austauschen, einen separaten, unabhängigen Zähler, der aber ebenfalls inkrementell arbeitet. Bei Solaris lassen sich deshalb keine heimlichen Lastmessungen und auch keine Idle-Scans durchführen. Hinter einem Router kann ein aktives Solaris-System durch die verschiedenen Host-Sequenzen sogar mehrere aktive Rechner vorspiegeln. Aktuelle OpenBSD-Systeme verwenden zufällige IP-IDs, sodass sich daraus keine Rückschlüsse mehr ziehen lassen.

Die Folgen

Die Tatsache, dass beliebige Personen die Last auf einem Internet-Server beobachten können, sollte man nicht auf die leichte Schulter nehmen. Zuverlässige Aussagen über die tatsächlich transferierten Datenmengen oder auch nur die Anzahl der Verbindungen kann man über die IP-ID zwar nicht gewinnen. Aber es sind durchaus Szenarien vorstellbar, in denen beispielsweise die Tatsache, dass auf einem Server der Verkehr plötzlich ansteigt, Konkurrenten interessante Informationen liefert. Es könnte zum Beispiel den geheim gehaltenen Start eines Testprogramms verraten. Ein stetiger Abfall der Last über einen längeren Zeitraum könnte Beobachter zu der Vermutung verleiten, dass sich das Online-Angebot und damit die Umsatzentwicklung einer Firma auf dem absteigenden Ast befindet – eine Information, deren Veröffentlichung das Management sicher gerne selbst gesteuert hätte.

Da sich diese Lastmessungen mit ganz gewöhnlichen HTTP-Anfragen durchführen lassen, kann man sie auch nicht durch eine Firewall blockieren. Um sich zuverlässig gegen diese einfache Form der Spionage zu schützen, muss man Systeme einsetzen, die keine einfach vorhersagbaren IP-ID-Sequenzen verwenden.

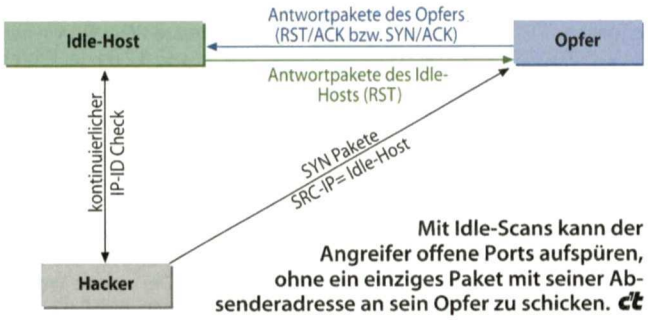
T-Online-Kunden, die in ihrer WG eine DSL-Flatrate gemeinsam nutzen, haben nach unseren Erfahrungen keinen Grund zur Panik. Bisher ist uns kein Fall bekannt, in dem der Provider dieses Verfahren eingesetzt hätte, um einen Vertragsverstoß nachzuweisen. Im schlimmsten Fall droht ihnen die Kündigung und sie müssen sich einen neuen Provider suchen.

Ein ernst zu nehmendes Problem sind die indirekten Port-Scans via IP-ID. Netzwerk-Administratoren und auch die Beschwerdestellen bei den Providern können nicht mehr davon ausgehen, dass Log-Dateien über Port-Scans Hinweise auf den wirklichen Verursacher liefern. Erst wenn es zu einem tatsächlichen Verbindungsaufbau kommt, kann man davon ausgehen, dass die verdächtige Verbindung auch tatsächlich von der Gegenstelle initiiert wurde. Bei modernen Port-Scan-Verfahren kommt ein solcher Verbindungsaufbau jedoch genauso wenig zustande wie bei den Idle-Scans. Beschwerden, dass von einer bestimmten IP-Adresse aus Port-Scans durchgeführt würden, sollte man sich zukünftig also besser schenken. (ju)

Literatur

[1] Steven M. Bellovin, A Technique for Counting NATted Hosts, www.research.att.com/~smb/papers/fnat.pdf

Soft-Link 0323212



Mit Idle-Scans kann der Angreifer offene Ports aufspüren, ohne ein einziges Paket mit seiner Absenderadresse an sein Opfer zu schicken. c't