

## Herausforderung IPv6

**Glaubt man den Internet-Auguren, dann wird 2011 in die Geschichte eingehen als das Jahr, in dem die IPv4-Adressen zur Neige gingen. Es wird also höchste Zeit, sich intensiver mit der Protokoll-Alternative zu beschäftigen, bei der Adressknappheit kein Thema mehr ist: dem Internet Protokoll Version 6, kurz IPv6. Dieser Meinung ist offenbar auch das NIST, das am 29.12.2010 einen Leitfaden für den sicheren Einsatz von IPv6 als Special Publication 800-119 [6] herausgegeben hat.**



**Dr. Safuat Hamdy**  
Secorvo Security Consulting



**Hans-Joachim Knobloc**  
Secorvo Security Consulting

### Herausforderungen des Übergangs

Die Einführung von IPv6 ist bis in die jüngere Vergangenheit – zumindest in Europa und den USA, wo man sich rechtzeitig einen Grossteil der verfügbaren IPv4-Adressen gesichert hatte – eher gemächlich vorangegangen. Dies hat vor allem damit zu tun, dass IPv6 nicht kompatibel zu dem bisher allgemein verwendeten IPv4 ist, d. h. beim Übergang zu IPv6 können nicht einfach bestehende Strukturen und Komponenten übernommen werden. Ein Übergang ist daher nicht ohne erheblichen technischen wie organisatorischen Aufwand möglich.

Eines der Argumente für den Einsatz von IPv6 ist der im Vergleich zu IPv4 erheblich grössere Adressraum. Der Mangel an IPv4-Adressen war schon lange absehbar, wurde aber durch Konstruktionen wie Network Address Translation (NAT) weiter hinausgezögert. In Ermangelung einer breiten Nachfrage haben anfangs die Hersteller IPv6-Produkte eher zurückhaltend entwickelt und angeboten. Mittlerweile liegt der schwarze Peter eher bei den Betreibern: Seit Windows Vista ist, genau wie bei aktuellen Versionen von Linux, verschiedenen Unix-Derivaten und Mac OS, IPv6 standardmässig aktiviert.

Es ist also davon auszugehen, dass der Übergang zu IPv6 auf breiter Basis in näherer Zukunft begonnen wird. Dieser Übergang wird nicht schlagartig vonstatten gehen, sondern es wird Übergangslösungen, Übergänge zwischen den Protokollversionen und Parallelbetrieb von IPv4 und IPv6 geben. In diesem Artikel werden die Herausforderungen dieses Übergangs aus Sicherheitssicht beleuchtet.

Eine besondere Herausforderung besteht darin, dass aufgrund des bisherigen Zustandes kaum breite Erfahrung mit IPv6 besteht. In [6] heisst es dazu, dass gerade in der Anfangsphase damit zu rechnen ist, dass Angreifer potenziell über mehr Kenntnisse von IPv6 verfügen.

Ein prägnantes Beispiel, wie mit hinreichend viel Detail-Know-How der IPv6-Protokolle Angriffsszenarien konstruiert werden können, stellt der im nachfolgenden Kasten beschriebene, auf den ersten Blick relativ komplex wirkende Denial-of-Service-Angriff dar. Dieser Angriff wurde nahezu zeitgleich mit der Veröffentlichung von [6] beim 27C3 Kongress in Berlin vom Autor des IPv6 Angriffs-Toolkits THC-IPV6 präsentiert [7]. Laut eigener Aussage

## Beispiel eines Angriffs: Denial-of-Service gegen IPv6-Multicasts

Neben den vordefinierten „Link Local“ Multicast-Gruppen geht IPv6 auch vom regen Gebrauch von Multicasts über verschiedene Netzwerksegment hinweg aus. Dazu müssen die entsprechenden Netzwerkknoten bei einem zuständigen Router anmelden, dass von außen empfangene Pakete für die betreffende Multicast-Adresse an sie weiter geleitet werden sollen. Für diese Anmeldung wurde das Multicast Listener Discovery (MLD) Protokoll definiert [4].

MLD verwendet vier eigens definierte ICMPv6 Nachrichtentypen: Mit MLD Generic Queries fragt ein Router ob es im betreffenden Segment Knoten gibt, die Multicasts für irgendeine Adresse empfangen wollen, mit MLD Specific Queries kann er nach Knoten fragen, die sich für eine bestimmte Multicast-Adresse registrieren wollen. Ein Gerät kann sich darauf hin per MLD Report melden und die Multicast-Adresse angeben, für die es sich registrieren will. Will ein registriertes Gerät nicht mehr länger mit Multicast-Nachrichten versorgt werden, sendet es ein MLD Done. Um Mehrfachregistrierungen zu vermeiden, wird dynamisch jeweils nur ein Router im Segment zum sogenannten MLD Query Router bestimmt, der die MLD Queries schickt.

Das Ziel des nachfolgend beschriebenen von vanHauser vorgestellten Angriffs [7] ist es, diesen Mechanismus im lokalen Segment zu stören und alle lokalen Geräte von entfernten Multicasts abzuschneiden. Dazu führt der Angreifer die folgenden drei Schritte durch:

1. Er sendet eine MLD Generic Query mit gefälschter Quelladresse fe80:: (der niedrigstmöglichen Adresse im lokalen Segment). Da stets der Router mit der niedrigsten Adresse zum MLD Query Router bestimmt wird, übernimmt er damit diese Funktion.
2. Er sendet für jedes Gerät, das er vom Multicast abschneiden will, ein entsprechendes MLD Done mit gefälschter Quelladresse. Auf diese Abmeldung müsste der MLD Query Router mit einer MLD Specific Query reagieren, um zu ermitteln, ob ein anderes Gerät diesen Multicast übernehmen möchte. Daraufhin würde das echte Gerät sich wieder mit einer MLD Response anmelden. Da der Angreifer sich zuvor selbst zum MLD Query Router erhoben hat, unterbleibt jedoch diese MLD Specific Query.
3. Bleiben MLD Queries (auf die hin sich die vom Angreifer abgehängten Geräte erneut registrieren würden) zu lange aus, geht der vorige MLD Query Router davon aus, dass er diese Rolle wieder übernehmen muss, und beginnt erneut mit der Aussendung der Queries. Der Angreifer muss also regelmäßig MLD Queries aussenden, die zwar von den anderen Routern, nicht jedoch von den abgehängten Geräten empfangen werden. Um dies zu erreichen, sendet er seine MLD Generic Queries an die oben erwähnte MAC-Adresse 33:33:00:00:00:02, die mit der Multicast-Adresse ff02::2 der lokalen Router korrespondiert .

kostete ihn die Entwicklung von der Idee über das Detailstudium der einschlägigen RFCs bis zum Kodieren eines Proof-of-Concept Angriffstools ganze zwei Stunden.

### Kinderkrankheiten

IPv6 ist noch bei weitem nicht so intensiv untersucht und erprobt wie IPv4. Es ist daher zu erwarten, dass IPv6 noch für eine gewisse Zeit unter konzept- und implementierungsbedingten Schwachstellen zu leiden hat, was die beiden nachfolgenden Beispiele belegen:

Die aktuelle Fassung von IPv6 wurde 1998 in RFC 2460 [5] definiert. Darin ist zwar die Fragmentierung von zu langen Paketinhalten durch Aufteilen in mehrere Pakete und Einfügen des Fragment-Erweiterungsheaders spezifiziert – eine mögliche Überlappung von Fragmenten wird jedoch nicht betrachtet. Dabei sind böswillig erzeugte Frag-

mente, die im Regelbetrieb so nicht auftreten könnten, eine seit langem bekannte Quelle von Denial-of-Service-An-

griffen. Und bereits im Jahre 1995 wurde in RFC 1858 [9] dargelegt, wie überlappende Fragmente dazu genutzt werden können, um beispielsweise TCP-Portnummern, die eine Firewall im anfänglichen Fragment eines IP-Pakets bereits geprüft und freigegeben hat, durch nachfolgende Nachrichten doch noch abzuändern. Diese Lücke wurde für IPv6 erst 2009, elf Jahre nach RFC 2460, gestopft und in RFC 5722 [8] endgültig festgelegt, dass IPv6-Pakete, deren Frag-

mente sich überlappen, unbedingt verworfen werden müssen.

Auch eine weitere Schwachstelle der ursprünglichen IPv6-Definition wurde erst etliche Jahre später behoben: Mit RFC 5095 [1] wurden 2007 die Routing Header des Typs 0 (RH0) wieder abgeschafft, als man erkannte, dass sie missbraucht werden können, um ein einzelnes IPv6-Paket zigfach zwischen zwei angegriffenen Systemen hin- und her wandern zu lassen und auf diese Weise mit wenig Aufwand eine Netzwerk-Strecke zu überlasten.

Es ist zu erwarten, dass in den kommenden Jahren der ernsthaften und breiten Nutzung von IPv6 noch weitere derartige Probleme auftauchen werden, die durch die Umstände einer allgemeinen Umstellung noch verschärft werden könnten. Von grosser Bedeutung ist daher die Fähigkeit der Hersteller, auf neue Probleme zu reagieren und entsprechende Updates für Netzwerkkomponenten und -geräte kurzfristig bereitzustellen. Der Sorgfalt des Betreibers dagegen bleibt bis auf weiteres überlassen, sich davon zu vergewissern, dass seine als „IPv6-fähig“ angepriesenen Komponenten nicht nur einen Mindestumfang des Protokolls nach älteren Spezifikationen umsetzen, sondern der Hersteller auch die aktuellen sicherheitsrelevanten Standards berücksichtigt hat.

### **Sicherheit im Design(?)**

Beim Entwurf von IPv6 wurden von Beginn an auch Aspekte der Sicherheit berücksichtigt, allerdings auf teilweise eher einseitige Weise. Dies zeigt sich im Wesentlichen in der Entwicklung von IPsec, dessen Unter-

stützung in IPv6 zwingend vorgeschrieben ist. Einige Hersteller nehmen es jedoch, besonders bei mobilen Geräten mit knapp bemessener Leistung, mit dieser Vorschrift nicht so genau, implementieren IPv6 also ohne IPsec. Auch viele Anwender scheuen den nötigen Aufwand, IPsec in der Praxis stabil und sicher zu betreiben.

Daneben muss festgestellt werden, dass im Gegensatz zur Unterstützung die tatsächliche Verwendung von IPsec nur ausnahmsweise vorgeschrieben ist, etwa für verschiedene Steuernachrichten für Mobile IPv6 (MIPv6). Tatsächlich ist IPsec in vielen Fällen überhaupt nicht praktikabel anwendbar, etwa wenn ein Router zwischen zwei Endpunkten eine Fehlermeldung an den Absender eines Pakets zurückschickt. Im Zusammenhang mit Multicast ist IPsec nur beschränkt einsetzbar, so funktioniert der Anti-Replay-Mechanismus von IPsec bei Multicast nicht.

Selbst wenn man darüber hinweg sieht, bleibt immer noch die Herausforderung, ein flexibles aber einfach anzuwendendes Schlüsselmanagement zu betreiben.

Es scheint jedoch so, dass sich der Beitrag zur Sicherheit in IPv6 durch IPsec erschöpft hätte, frei nach der Devise: Sicherheit ist kein Problem, wir haben doch IP-sec. Angesichts der vorstehend beschriebenen Kinderkrankheiten von IPv6 (die rückblickend betrachtet leicht vermeidbar gewesen wären) ist damit zu rechnen, dass noch weitere, bisher verborgene Sicherheitsprobleme zutage treten werden, die durch den Einsatz von IPsec

nicht oder nicht pauschal gelöst werden können.

### **Abschottung und Filterung**

Als Betreiber eines Netzwerks steht man vor der grundsätzlichen Frage, wann der Umstieg auf IPv6 erfolgen soll. Ist dies nicht unmittelbar der Fall, dann sollte die IPv6-Funktionalität in dem Netzwerk unterbunden werden, denn ansonsten besteht die Gefahr, dass Angreifer IPv6-Funktionalität verwenden, um Sicherheitsmechanismen zu umgehen. So wurde beispielsweise von Malware berichtet, die versucht, per IPv6 mit ihrem Controlserver zu kommunizieren, um nicht von IPv4-basierten Intrusion Detection Mechanismen entdeckt zu werden. Zugleich sollte an den Netzwerkübergängen IPv6 in beide Richtungen gefiltert werden, um unerwünschte Rückwirkungen und Datenabflüsse in das bzw. aus dem Netz über IPv6 zu unterdrücken.

Steht eine Umstellung oder ein Parallelbetrieb bevor, so sollte die IPv6-Funktionalität der Netzwerkkomponenten, wie Router und Firewalls, genau studiert werden. Besondere Aufmerksamkeit erfordert die Filterung unerwünschten Verkehrs. So lässt sich beispielsweise ICMPv4 pauschal blockieren, denn auf die dadurch verlorengegangene Funktionalität konnte man ggf. verzichten. ICMPv6 jedoch darf nicht pauschal gefiltert werden, da sonst unter Umständen überhaupt keine Kommunikation über IPv6 zustande kommt. Die korrekte, selektive Filterung von ICMPv6 ist von solcher Bedeutung, dass dem Thema ein eigener RFC gewidmet wurde (RFC 4890 [3]).

Bei der Filterung ist auch darauf

zu achten, dass Adressen aus verschiedenen Gültigkeitsbereichen (Scopes) unterschiedliche Sichtbarkeit haben. So dürfen beispielsweise Link-Local-Adressen (vergleichbar den privaten IPv4-Adressen) niemals geroutet werden. Dies ist insbesondere deswegen von Bedeutung, weil eine Anzahl von ICMPv6-Nachrichten nur für den Link-Local-Gebrauch vorgesehen ist. Andere ICMPv6-Nachrichten betreffen spezielle Anwendungen wie etwa MIPv6. Solange der Einsatz von MIPv6 nicht vorgesehen ist, sollten alle diesbezüglichen ICMPv6-Pakete ausgefiltert werden.

Darüber hinaus sollte bei der Filterung auch IPv6 Extension Header berücksichtigt werden. Dies entspricht der Behandlung von IPv4 Header-Optionen; der entscheidende Unterschied ist aber, dass ein IPv6-Paket beliebig viele Erweiterungen haben darf, für deren Reihenfolge mit einer Ausnahme keine Vorschriften gemacht werden. Auch hier gilt, zunächst zurückhaltender zu sein und Pakete mit fragwürdigen Erweiterungen im Zweifelsfalle zu verwerfen.

### Adressen und Adressräume

Ein weiteres Gebiet mit Potenzial für unerwünschte Nebenwirkungen haben die IPv6-Adressen und die definierten Adressräume. Eine IPv6-Adresse ist viermal so lang wie eine IPv4-Adresse. Trotz aller Versuche, eine kompakte Notation für IPv6-Adressen zu finden bleiben IPv6-Adressen im Allgemeinen unhandlich und eine manuelle Verarbeitung fehlerträchtig. Schon allein die Vielzahl erlaubter, äquivalenter Schreibweisen für eine bestimmte IPv6-Adresse könnte zu Sicherheitsproblemen führen:

Vor einem lexikalischen Vergleich, beispielsweise für die Blacklist-Prüfung einer URL, muss sie auf jeden Fall in eine kanonische Darstellung gebracht werden.

Die Vergabe von IPv6-Adressen sollte daher automatisiert erfolgen. Eine Möglichkeit dafür besteht in der neu geschaffenen zustandslosen Selbstkonfiguration von Netzwerkkarten. Alternativ kann eine IPv6-Adresse analog zu IPv4 auch über DHCPv6 vergeben werden.

Der Adressraum von IPv6 ist im Vergleich zu IPv4 enorm gross, und in der Literatur finden sich zahlreiche blumige Vergleiche zur Darstellung der Adressfülle. Genau wie bei IPv4 steht aber die theoretische Maximalzahl von IPv6-Adressen gar nicht zur freien Vergabe zur Verfügung. Es gibt verschiedene reservierte Adressbereiche, die verschiedene Funktionen erfüllen, etwa für Multicast, Local-Link-Unicast usw. Natürlich bleibt immer noch eine nahezu unvorstellbare Fülle an Adressen übrig. Davon hat IANA jedoch zunächst nur den Bereich 2000::/3 für Global Unicast vergeben; der Bereich 4000::/2 bis fc00::/9 ist für eine weitere Vergabe vorgesehen, aber noch reserviert.

Leider enthält der Bereich 2000::/3 Teilbereiche, die für spezielle Verwendungszwecke vorgesehen sind oder waren, wie z. B. 2001:0000::/32 für IPv6-Tunneling per Teredo oder 2002::/16 für 6to4. Noch ärgerlicher ist der Bereich 2001:db8::/32, der in den meisten Dokumentationsbeispielen verwendet wird und daher als nicht routbar deklariert ist, oder 3ffe::/16, dessen Verwendung für 6bone als obsolet gilt. Was soll mit Paketen

passieren, deren Quell- oder Zieladresse aus solchen Bereichen stammt? Für die Administratoren eines Netzwerkes bedeutet dies, die Filterregeln an den Firewalls um entsprechende Filter-Einträge zu ergänzen und derartige Pakete pauschal zu verwerfen.

### IPv6 und Netzwerksicherheitskomponenten

Doch noch darf man nicht davon ausgehen, dass Netzwerksicherheitskomponenten wie Firewall und IDS IPv6 stets in ausreichendem Masse unterstützen. Eine „IPv6-kompatible“ Firewall wird zwar in jedem Fall IPv6-Datenverkehr empfangen und weiterleiten können. Sie sollte auch in der Lage sein, die üblichen Filterfunktionen auf TCP6- und UDP6- Datenverkehr anzuwenden.

Doch IPv6 ist ein hochgradig erweiterbares Protokoll mit diversen verkettbaren Erweiterungsheadern, verschiedenen Untertypen von Routing-Headern und Optionen, über Routern und Zielsystemen verschiedenste Anweisungen zur Behandlung eines Pakets übermittelt werden können. Und dieser Erweiterungsmechanismus wird stetig für die Standardisierung neuer Funktionsmerkmale benutzt. So können, zumindest in der Theorie, mittels spezieller Header-Optionen mehrere Gigabyte grosse Jumbo-Pakete verschickt werden.

Das bedeutet, um bestimmte, im Einzelfall erwünschte Funktionsmerkmale wie z. B. MIPv6 nicht von vornherein unmöglich zu machen, dürfen all diese Optionen und Erweiterungen nicht in Bausch und Bogen verboten und blockiert werden. Stattdessen müssen Sie wie oben für

## PLATTFORM FÜR INFORMATIONSSICHERHEIT

ICMPv6 geschildert selektiv behandelt werden. Doch an derartigen Einstellmöglichkeiten mangelt es momentan noch vielen Produkten.

### Zusammenfassung

Zusammenfassend lässt sich sagen, dass die Herausforderungen durch IPv6 jeden betreffen, selbst Netz- und Systembetreiber, die (noch) gar kein IPv6 einsetzen. Sie müssen darauf achten, IPv6 an Netzwerkübergängen und auf Systemen zuverlässig zu deaktivieren, damit Angreifer das Protokoll nicht zum Umgehen von IPv4-basierten Sicherheitsmechanismen nutzen können.

Für Sicherheitsexperten bietet sich ein weites Feld, die Sicherheitseigenschaften von IPv6 und seiner vielen im Laufe der Zeit ergänzten Funktionsmerkmale zu analysieren und Schwachstellen zu erkennen. Hersteller sind gefordert, mögliche Implementierungsfehler, wie sie bei IPv4-Implementierungen im Laufe der Jahre entdeckt und beseitigt wurden, bei IPv6 ebenfalls auszuräumen oder, besser noch, von vornherein zu vermeiden. Neue, sicherheitsrelevante Spezifikationen müssen zügig umgesetzt werden. Speziell Hersteller von Netzwerksicherheitsprodukten müssen sich auf die neuen Funktionen und IPv6-Optionen einstellen und diese in ihre Prüfung mit einbeziehen. Netzbetreiber und -administratoren schliesslich, die IPv6 nutzen wollen, sollten Zeit für eine sorgfältige Planung von Parallelbetrieb IPv6/IPv4, Tunneling- und Übergangs- und Migrations-szenarien verwenden, um sich durch die zusätzliche Komplexität keine ungewollte Blöße zu geben. Allen gemeinsam

kann nur geraten werden, sich intensiv in die neue Protokollversion und ihre Sicherheitseigenschaften einzuarbeiten und ein Auge auf die immer noch laufende Standardisierung neuer IPv6-Funktionsmerkmale zu haben. Ein guter Ausgangspunkt dazu ist die eingangs genannte NIST Special Publication 800-119 [6].

### Literatur

- [1] J. Abley, P. Savola, G. Neville-Neil, Deprecation of Type 0 Routing Headers in IPv6, RFC 5095, [www.rfc-editor.org/rfc/rfc5095.txt](http://www.rfc-editor.org/rfc/rfc5095.txt)
- [2] M. Crawford, Transmission of IPv6 Packets over Ethernet Networks, RFC 2464, [www.rfc-editor.org/rfc/rfc2464.txt](http://www.rfc-editor.org/rfc/rfc2464.txt)
- [3] E. Davies, J. Mohacsi, Recommendations for Filtering ICMPv6 Messages in Firewalls, RFC 4890, <http://www.rfc-editor.org/rfc/rfc4890.txt>
- [4] S. Deering, W. Fenner, B. Haberman, Multicast Listener Discovery (MLD) for IPv6, RFC 2710, [www.rfc-editor.org/rfc/rfc2710.txt](http://www.rfc-editor.org/rfc/rfc2710.txt)
- [5] S. Deering, R. Hinden, Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, [www.rfc-editor.org/rfc/rfc2460.txt](http://www.rfc-editor.org/rfc/rfc2460.txt)
- [6] S. Frankel, R. Graveman, J. Pearce, M. Rooks, Guidelines for the Secure Deployment of IPv6, National Institute of Standards and Technology Special Publication 800-119, Dezember 2010, [csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf](http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf)
- [7] M. „vanHauser“ Heuse, Recent advances in IPv6 insecurities, 27th Chaos Communication Congress, Berlin 2010, [events.ccc.de/congress/2010/Fahrplan/events/3957.en.html](http://events.ccc.de/congress/2010/Fahrplan/events/3957.en.html)
- [8] S. Krishnan, Handling of Overlapping IPv6 Fragments, RFC 5722, [www.rfc-editor.org/rfc/rfc5722.txt](http://www.rfc-editor.org/rfc/rfc5722.txt)
- [9] G. Ziemba, D. Reed, P. Traina, Security Considerations for IP Fragment Filtering, RFC 1858, [www.rfc-editor.org/rfc/rfc1858.txt](http://www.rfc-editor.org/rfc/rfc1858.txt)