Universität Osnabrück

SEMINARARBEIT

zum Seminar

IT-Sicherheit

im Sommersemester 2013

Thema:

IPv6 Privacy Extensions

Erstellt am 26.05.2013

Vorgelegt von:

Kevin Seidel
943147
Falkenstraße 43
49124 Georgsmarienhütte

Inhaltsverzeichnis

1 Einleitung

Diese Seminararbeit behandelt das Internet Protocol version 6 und dabei insbesondere die Vergabe und Erzeugung der Netzwerkadressen.

Das Internet Protocol (IP) version 6, oder kurz IPv6, ist der Nachfolger des Internet Protocol version 4 (IPv4), welches aktuell in den meisten Netzwerken verwendet wird. Die Umstellung auf ein neues Protokoll ist nötig, da durch den starken Anstieg von netzwerkfähigen Geräten, auch der Bedarf an IP-Adressen steigt. Als IPv4 in den 1980er Jahren definiert wurde, ging man davon aus, dass das Protokoll in Zukunft genügend Adressen bereitstellt, um den geforderten Bedarf zu decken. Zu der damaligen Zeit besaßen jedoch nur wenige Privatpersonen einen Computer, da diese hauptsächlich zu Forschungszwecken eingesetzt wurden. Über die letzten Jahre hat sich dieses Bild jedoch stark verändert, sodass mittlerweile viele Menschen ein oder mhrere Netzwerkgeräte besitzen. Diese sind nichtmehr nur Computer, sondern auch Smartphones, Tablets, Internet-Fernseher und andere. Durch diesen starken Anstieg waren die 4,3 Milliarden Adressen, welche IPv4 theoretisch zur Verfügung stellt, schneller aufgebraucht als bei der Erstellung des Protokolls gedacht. [NRO11] Aufgrund dieser Tatsache ist es nötig geworden ein neues Internetprotokoll zu definieren, welches diesen Engpass an Adressen lösen kann. IPv6 stellt deshalb einen deutlich größeren Adressraum zur Verfügung, welcher 2^{128} Adressen bietet und damit auch über die nächsten Jahrzehnte genügend Adressen bereitstellen sollte.

Aktuell ist die Nutzung von IPv6 noch nicht sehr verbreitet [NRO10] und der Anteil von IPv6 am gesamten Internetverkehr liegt laut Google [GOOG] bei etwa 1,5 Prozent (Stand Mai 2013). Das Problem bei der Umstellung ist vor allem ältere Hardware, welche noch keine IPv6 Unterstützung bietet. Um eine IPv6 Verbindung aufzubauen, ist es nämlich nötig, dass jedes Gerät und Netzwerk, welches bei der Verbindung genutzt wird IPv6 unterstützt. Bei dem Aufruf einer klassischen Webseite bedeutet das, dass sowohl der Server und Client, als auch alle Geräte und Netze durch die Anfragen und Antworten geschickt werden müssen, IPv6 unterstützen. Auf Grund dieser Vorraussetzung ist eine sofortige Umstellung auf IPv6 nicht möglich und das neue Protokoll muss schrittweise ausgerollt werden. Dabei ist die Inkompatibilität zwischen IPv4 und IPv6 ein Problem, was die schnellere Verbreitung verhindert. Es ist zwar möglich in IPv6 Netzwerken IPv4-Adressen und Pakete zu bearbeiten, jedoch nicht ohne größeren Aufwand. In Zukunft sollte die Nutzung von IPv6 jedoch stetig zunehmen, da mittlerweile fast alle neue Geräte, wie Router oder Modems, das neue Internet Protokoll unterstützen und damit die Nutzung ermöglichen.

Eine größere Aufmerksamkeit erfuhr IPv6 am 8.Juni 2011. An diesem Tag wurde der "World IPv6 Day" [IS11] gefeiert, welcher von der Internet Society und verschiedenen größeren Internetfirmen, beispielsweise Facebook, Google, Yahoo und andere, durchgeführt wurde. Dieser Tag hatte das Ziel IPv6 einem größeren öffentlichem Test zu unterziehen, was laut der Seitenbetreiber auch gut funktioniert hat. Aufgrund der Erfolges des "World IPv6 Day" wurde im darauf folgenden Jahr der "IPv6 Launch Day" [WIPL] durchgeführt, an welchem diverse Seiten die Unterstützung von IPv6 dauerhaft aktivierten.

Im Folgenden geht diese Arbeit genauer auf den Aufbau der neuen IPv6-Adressen, im Vergleich zu den bisher verwendeten IPv4-Adressen, ein und vergleicht dabei zum Beispiel die Unterschiede in der Notation. Darüber hinaus wird noch auf die Stateless Address Autoconfiguration eingegangen, welche es ermöglicht, dass Netzwerkgeräte ihre IP-Adressen selbstständig erstellen und somit auf manuelle Adresseingabe oder Adresszuweisungen

von einem zentralen Server verzichtet werden kann. Im Bezug auf dieses Verfahren wird zunächst die grundlegende Funktionsweise erläutert und danach wird auf die Stärken, Schwächen und mögliche Verbesserungen dieses Verfahrens eingegangen. Eine dieser Verbesserungsmöglichkeiten steht im Fokus dieser Arbeit. Die Privacy Extentions, welche eine bessere Privatsphäre und mehr Sicherheit als die klassische Stateless Address Autoconfiguration bieten. Auch hier wird zunächst deren Funktionsweise erörtert und danach die Vor- und Nachteil und mögliche Verbesserungen erläutert.

2 Das Internet Protocol Version 6

2.1 Warum IPv6?

Durch den starken Anstieg von Netzwerkgeräten in den vergangen Jahren, ist es nötig geworden einen größeren Adressraum zu schaffen. IPv4 stellt, aufgrund der Adressgröße von 32 Bits, nur einen Adressraum von 2^{32} Adressen zur Verfügung, was in etwa 4,3 Milliarden Adressen entspricht. Diese Adressen sind jedoch mittlerweile knapp geworden, sodass es schon diverse implementierte Lösungsansätze für dieses Problem gibt. Eines davon ist beispielsweise die Network Address Translation (NAS) beschrieben im [RFC 3022], welche es ermöglicht nur eine öffentliche IPv4-Adresse für ein gesamtes Netzwerk aus mehreren Geräte bereitzustellen. Dies sind aber eher Notlösungen und es ist daher nötig geworden, ein neues Protokoll zu entwerfen. Dabei war eines der Ziele diese Probleme zu beseitigen und auch auf längere Sicht jedem Netzwerkgerät eine eindeutige Adresse zuordnen zu können. IP Version 6 setzt deshalb auf eine Adresslänge von 128 Bits, wodurch sich der Adressraum enorm vergrößert und etwa $3.4 * 10^{38}$ IP-Adressen bereitgestellt werden.

Eine weitere Veränderung von IPv6 gegenüber IPv4 ist die feste Größe des Headers, welcher nur die zwingend notwendigen Informationen enthält und dessen Aufbau im [RFC 2460] festgelegt ist. Dies erleichtert die Handhabung der Datenpakete im Gegensatz zu IPv4, welches eine variable Headergröße eingesetzt hat. Für zusätzliche Informationen gibt es bei IPv6 einen Extention Header, welcher jedoch nur bei Bedarf genutzt wird.

Ein weitere Vorteil von IPv6 ist, dass Internet Protocol Security (IPSec) fest im dem Standard verankert ist und daher, laut [RFC4294], von jedem IPv6-Gerät unterstützt werden muss. Dies erhöht die Sicherheit der Verbindung, da dadurch verschlüsselte Verbindungen direkt auf der Transportschicht hergestellt werden können.

2.2 Aufbau einer IPv6-Adresse

Die IPv6-Adresse unterscheiden sich deutlich von den bisher verwendeten IPv4-Adressen. IPv4-Adressen haben eine Größe von 32 Bits und werden meist in der "dotted decimal notation", das heißt in vier Blöcken von Dezimalzahlen zwischen 0 und 255, welche durch einen Punkt separiert werden, dargestellt. Dadurch lassen sich 2^{32} (ca. 4,3 Mrd.) verschiedene Adressen darstellen. Durch die Verwendung von IPv6-Adressen erhöht sich die Anzahl der Adressen drastisch, da man hier eine Adresslänge von 128 Bits verwendet, womit die Größe des Adressraumes auf 2^{128} angehoben wird. Da eine Darstellung dieser Adressen in "dotted decimal notation" aus 16 Blöcken bestehen würde und damit sehr schwer zu lesen wäre, entschloss man sich dazu die IPv6-Adressen in 8 Blöcken zu je 4 Hexadezimalziffern zusammenzufassen. Diese Blöcke werden, durch einen Doppelpunkt getrennt, notiert.

$$2001 : 0db8 : 1aAa : 0000 : CCcc : 0000 : 0000 : 0D01$$

Abbildung 1: Beispiel einer IPv6-Adresse.

Da diese Adressen im Vergleich zu IPv4-Adressen immer noch relativ lang und unübersichtlich sind, gibt es mehrere Möglichkeiten eine IPv6-Adresse zu verkürzen. So wird im [RFC 4291] vereinbart, dass man ein oder mehrere aufeinanderfolgende Blöcke, welche nur Nullen beinhalten durch "::" verkürzen kann. Dies jedoch nur einmal pro Adresse.

Ausserdem ist es möglich auf führende Nullen innerhalb eines Blockes zu verzichten.

In [RFC 5952] wird eine Empfehlung für eine etwas striktere Darstellung von IPv6-Adressen gemacht. So ist es dort vorgeschrieben innerhalb von Adressen nur Kleinbuchstaben zu verwenden. Dies dient der besseren Lesbarkeit und verhindert eine versehentliche Verwechselung von 8 und B sowie 0 und D, die bei gemischter Groß- und Kleinschreibung oder durchgängiger Großschreibung entstehen könnte.

Des Weiteren müssen führende Null innerhalb eines Blockes ausgelassen werden und Blöcke, welche nur aus Nullen bestehen, durch eine einzelne Null repräsentiert werden.

Ausserdem ist es nun nicht mehr erlaubt einzelne Null-Felder durch "::" zu repräsentieren. Diese Schreibweise ist nur noch auf mehrere aufeinanderfolgende Null-Felder anwendbar und muss in dem Fall auch genutzt werden. Gibt es mehrere Möglichkeiten Felder durch "::" zu verkürzen, muss das mit dem größten Nutzen, das heißt mit den meisten aufeinanderfolgenden Nullen, gewählt werden. Existieren mehrere gleich große Möglichkeiten, ist die erste zu wählen.

$$2001 : db8 : 1aaa : 0 : cccc :: d01$$

Abbildung 2: Beispieladresse aus Abb. 1 unter Berücksichtigung von RFC5952

Durch die Befolgung dieser Regeln zu Darstellung von IPv6-Adressen in Textform wird die Lesbarkeit stark verbessert.

Die Netzmasken werden bei IPv6 durch Suffixe dargestellt, das heißt die Anzahl der Einsbits in der Netzmaske wird, abgetrennt durch einen Schrägstrich, hinten an die Adresse angehangen. Eine Notation der Netzmaske als Adresse, wie in IPv4 üblich, ist nun nichtmehr vorgesehen.

$$2001 : db8 : 1aaa : 0 : cccc :: d01/64$$

Abbildung 3: Beispieladresse aus Abb. 2 mit Netzmaske

Durch diese Netzmaske wird angegeben, welcher Teil der Adresse das Netzwerk identifiziert und welcher Teil das Interface repräsentiert. Der vordere Teil der Adresse, auch Präfix genannt, dient dabei zur Bestimmung des Netzes. Der hintere Teil, Interface Identifier genannt, dient zur Identifizierung eines Gerätes im Netz. Die Netzmaske gibt dabei an wie groß der Präfix ist. Beim Beispiel in Abbildung 3 ist der Präfix 64 Bit lang und wäre damit 2001:db8:1aaa:0::/64. Der Interface Identifier hat nun eine Länge von 64 Bit (128 Bit Adresslänge - 64 Bit Präfix) und lautet demnach ::cccc:0:0:d01/64.

Im Folgenden wird, wenn nicht ausdrücklich anders erwähnt, von einer Präfixlänge von 64 Bit und eine Interface Identifier-Länge von ebenfalls 64 Bit ausgegangen. Diese Längen können bei der wirklichen Verwendung variieren, haben hier, für die bessere Verständlichkeit, jedoch eine konstante Größe.

2.3 Vergabe von IPv6-Adressen

Bei IPv6 ist es im Vergleich zu IPv4 üblich, dass Geräten mehr als eine IPv6-Adresse zugeordnet wird. [RFC 4291] So besitzt jedes Netzwerkgerät in der Regel eine link-locale Adresse, welche für die grundlegende Kommunikation, zum Beispiel den Erhalt von Routernachrichten oder bei einer Direktverbindung von zwei Netzwerkgeräten verwendet wird.

Außerdem besitzen Geräte in größeren Netzwerken eine globale IP-Adresse, um beispielsweise mit dem Internet zu kommunizieren. Die Vergabe dieser IPv6-Adressen kann nach verschiedenen Vorgehensweisen erfolgen. Zum einen die manuelle Vergabe von Adressen, welche in kleinen Netzen schnell und einfach funktioniert, bei größeren Netzen jedoch einen enormen Aufwand bedeutet. Eine Alternative für größere Netze wäre die Verwendung des Dynamic Host Configuration Protocols (DHCP), welches schon für IPv4 existiert. Für IPv6 gibt es eine angepasste Version mit dem Namen DHCPv6, welches, identisch zum klassischen DHCP, dynamisch Adressen an im Netzwerk befindliche Geräte verteilt und die Adressen auf dem DHCP-Server speichert. Die nähere Vorgehensweise wird im [RFC 3315] erläutert. Durch die Speicherung der Adressen handelt es sich dabei um eine Stateful Address Configuration, im Gegensatz zur letzten Möglichkeit, der Stateless Address Autoconfiguration. Diese erzeugt IPv6-Adressen direkt auf dem Gerät, welches diese später verwenden will. Dadurch kann komplett auf einen DHCP-Server oder manuelle Konfiguration verzichtet werden. Ausserdem ist auch eine Kombination aus DHCP und Stateless Address Autoconfiguration möglich, wobei das Netzwerkgerät seine IP-Adressen selbst generiert, diese aber auch auf dem DHCP-Server gespeichert wird. Im Folgenden wird die Stateless Address Autoconfiguration genauer betrachtet.

3 Stateless Address Autoconfiguration

Die Stateless Address Autoconfiguration ist ein Verfahren zur eigenständigen Erzeugung von IP-Adressen auf Netzwerkgeräten. Dies ermöglicht eine einfache und konfigurationslose Einrichtung von Netzwerken, da zum Beispiel auf manuelle Adressvergabe oder den Einsatz von DHCP-Servern verzichtet werden kann. Selbst bei mehreren verbundenen Netzwerken ist ein DHCP-Server nicht nötig, da mittels Router Advertisements, welche die notwendigen Informationen über das Netzwerk enthalten, die einzelnen Adressen für die Netze und deren Subnetze vergeben werden können. Diese Vorgehensweise war mit IPv4 noch nicht möglich.

3.1 Funktionsweise der Stateless Address Autoconfiguration

Für die Erzeugung einer globalen IPv6-Adresse sind mehrere Schritte nötig, welche im Folgenden, basierend auf dem [RFC 4862], genauer erörtert werden.

Der Autokonfigurationsprozess wird automatisch mit der Aktivierung des Netzwerkgerätes gestartet. Dazu wird zuerst eine link-local Adresse erstellt. Diese erlaubt grundlegende Kommunikation im eigenen Netzwerk. Sie setzt sich aus einem festgelegtem Präfix für link-locale Adressen (fe80::/64) und dem gerätespezifischen Interface Identifier zusammen. Dieser Adresspräfix, sowie andere Präfix für site-local Adressen oder die Multicast-Adressen sind im [RFC 3513] festgelegt. Die Interface Identifier wird standardmäßig aus der Media Access Control(MAC)-Adresse des Netzwerkgerätes gebildet. Die MAC-Adresse besteht dabei aus der Organizationally Unique Identifier (OUI), welche vom Hersteller abhängig ist und einer Network Interface Card-Nummer (NIC), welche das Gerät bestimmt. Diese Kombination von OUI und NIC sollte weltweit eindeutig sein. Um diese 48 Bits lange MAC-Adresse auf die für den Interface Identifier vorgesehene Länge von 64 Bits zu bringen, wird die MAC-Adresse in der Mitte geteilt und dort wird der Wert "FF:FE" eingesetzt. Ausserdem wird das siebte Bit von links invertiert, welche angibt, ob die MAC-Adresse global oder lokal administriert wird.

Bevor diese vorläufige Adresse, egal ob manuell, durch DHCP oder Stateless Address Autoconfiguration zugewiesen, an ein Gerät gebunden wird, muss deren Eindeutigkeit im Netzwerk überprüft werden, da sonst Datenpakete zu den falschen Geräten transportiert werden könnten. Dies geschieht mittels Duplicate Address Detection. Einzige Ausnahmen einer Duplicate Address Detection sind Anycast Adressen oder eine explizite Deaktivierung des Vorgangs. Zur Überprüfung der Eindeutigkeit von Adresse werden sogenannte Neighbor Solicitations und Neighbor Advertisements verwendet. Neighbor Solicitations haben als Empfänger die vom Gerät generierte vorläufige Adresse und als Sender die nicht spezifizierte Adresse (::). Um eine Antwort auf diese Nachricht zu erhalten, ist es zunächst nötig, dass das Interface dem all-nodes Multicast, welcher dem Broadcast in IPv4 entspricht und an alle angebundenen Adressen verschickt, und dem solicited-node Multicast, welcher speziell für die Duplicate Address Detection zuständig ist, beizutreten. Falls nun schon ein Interface diese vorläufige Adresse besitzt, erhält es die Neighbor Solicitation und antwortet mit einem Neighbor Advertisement. Unser Interface empfängt dieses Neighbor Advertisement, wodurch es weiß, dass die vorläufige Adresse nicht eindeutig ist und damit nicht an das Gerät gebunden werden kann.

Falls das Interface während der Duplicate Address Detection eine Neighbor Solicitation mit der selben Adresse von einem anderen Gerät erhält, versuchen zwei Geräte gleichzeitig die gleiche Adresse zu verwenden. In diesem Fall sollte keines der Geräte seine vorläufige

Adresse benutzen. Es kann jedoch auch vorkommen, dass die Neighbor Solicitation von unserem Gerät kommt, falls der Multicast die Packete auch an den Sender zurückschickt. Dies muss vom Gerät erkannt werden und es sollte die Nachricht in diesem Fall verwerfen.

Wenn die Duplicate Address Detection fehlschlägt und unser Interface Indentifier aus der Hardware-Adresse gebildet wurde, sollten alle IP-Operationen eingestellt werden. Falls kein Neighbor Advertisement zurück kommt, kann die Adresse an das Gerät gebunden werden undfür die zukünftige Kommunikation verwendet werden.

Nachdem die link-local Adresse gebildet wurde, ist es nun möglich eine globale Adresse zu generieren. Dies ist jedoch nur möglich, falls sich ein Router im Netzwerk befindet, da hierfür sogenannte Router Advertisements nötig sind. Die Router Advertisements enthalten Informationen über das Netzwerk, wie zum Beispiel den zu verwendenden Präfix. Sie werden vom Router automatisch in periodischen Abständen geschickt, können jedoch auch durch Router Solification angefragt werden.

Ein Gerät sendet also zuerst eine Router Solification und wartet auf ein Router Advertisement als Antwort. Nach einem vorgegebenen Zeitraum ohne Antwort wird dies noch einmal ausgeführt. Dies geschieht so lange bis ein Router antwortet oder die vorgegebene Maximalanzahl von Anfragen erreicht ist. Antwortet der Router, wird aus dem in dem Router Advertisement enthaltenen Präfix und dem vom Gerät vorher gebildeteten Interface Identifier eine globale Adresse gebildet. Auch für diese Adresse wird vor der Benutzung eine Duplicate Address Detection durchgeführt. Bei bestehen der Duplicate Address Detection, wird die Adresse nun für den gesamten Netzwerkverkehr genutzt, wobei die link-locale Adress immer noch ihre Gültigkeit besitzt.

Erhält man kein Router Advertisement, geht das Gerät davon aus, dass kein Router im Netzwerk existiert.

3.2 Probleme der Stateless Address Autoconfiguration

Probleme mit der Stateless Address Autoconfiguration werden im [RFC 4941] erläutert, welcher mit den Privacy Extentions auch einen Lösungsansatz bietet. Ein Problem bei der Stateles Address Autoconfiguration entsteht dabei durch die Verwendung eines konstanten Interface Identifiers für die IP-Adresse. Da der Interface Identifier in den meisten Fällen aus der MAC-Adresse generiert wird, bleibt dieser über die gesamte Lebensdauer des Netzwerkgerätes konstant und ändert sich selbst bei einem Wechsel des Netzwerkes nicht. Das heißt, selbst wenn der Präfix der IPv6-Adresse wechselt, lässt sich das Gerät und damit meist auch der Nutzer, über den Interface Identifier mit sehr großer Trefferwahrscheinlichkeit zurückverfolgen. So lässt sich beispielsweise mittels eines Netzwerksniffers bestimmen, wann ein Gerät kommuniziert hat, mit wem es kommuniziert hat und, durch den Präfix der IPv6-Adresse, in welchem Netz es sich befand. Besonders problematisch ist dies bei mobilen Geräten, wie zum Beispiel Smartphones oder Laptops, welche oft ihren Standort ändern. So können deren Bewegungen sehr leicht verfolgt werden, da sich zwar der Präfix der Adresse bei einem Netzwechsel ändert, der Interface Identifier jedoch konstant bleibt. Es kann also bestimmt werden, wann sich eine Gerät in einem bestimmten Netzwerk aufgehalten hat, wie viel Zeit er dort verbracht hat und zu wem er sich verbunden hat.

Dies ermöglicht nicht nur gezieltere Angriffe, sondern auch die Platzierung von Werbung, welche auf den jeweiligen Benutzer abgestimmt ist, ohne das dieser es weiß.

Ein weiteres Problem, welches bei der Nutzung von MAC-Adressen für der Erzeugung des Interface Identifier entsteht, ist die Möglichkeit, dadurch die Hardware des Gerätes zu bestimmen. Da die MAC-Adressen eindeutige Herstellerkennungen enthalten, lässt sich die darunterliegende Hardware leichter bestimmen und dadurch gezielt angreifen. So kann man beispielsweise anhand der MAC-Adresse Apple Geräte erkennen und in Folge dessen gezielte Angriffe auf das verwendete Betriebssystem durchführen.

Ein Ansatz zur Lösung des Problems geben die Privacy Extentions für IPv6.

4 IPv6 Privacy Extensions

Durch den Einsatz der IPv6 Privacy Extensions ([RFC 4941]) sollen die vorher beschriebenen Probleme der Stateless Address Autoconfiguration gelöst werden. Dies geschieht dadurch, dass der Interface Identifier nicht mehr nur aus der bearbeiteten MAC-Adresse besteht und damit über die gesamte Lebensdauer des Gerätes gleich bleibt, sonder dynamisch erzeugt wird. Dadurch wird eine Zuordnung von einer IPv6-Adresse zu einem bestimmten Gerät nahezu unmöglich und die vorher beschriebenen Probleme mit der Privatsphäre werden gelöst.

Da durch die Privacy Extentions jedoch nur der Interface Identifier geändert wird, ist die Gefahr einer konstanten Zuordnung einer Adresse zu einem Gerät nicht komplett gelöst. Jedes Netzwerk bekommt seinen eigenen Präfix, welcher ebenfalls konstant sein kann. So lässt sich bei kleinen Netzwerken, bestehend aus wenigen oder sogar nur einem Gerät, über den Präfix eine relativ genaue Zuordnung der Adresse zu einem Gerät machen und das, obwohl der Interface Identifier ständig wechselt. Bei Adressen, welche bei einem Domain Name System(DNS) - Server registriert sind, bringt eine Verwendung der Privacy Extentions ebenfalls wenig, da bei wechselnder IP der DNS-Name meist gleich bleibt. Da über den DNS-Namen eine eindeutige Zuordnung möglich ist, hat der wechselnde Interface Identifier keinerlei Vorteile. Es gibt jedoch auch Geräte, welche sowohl als Client, als

auch als Server agieren. Hier ist es möglich dem Gerät zwei IPv6-Adressen zuzuweisen. So kann die Serveradresse im DNS eingetragen sein und ist dadurch öffentlich erreichbar. Der Client hingegen bekommt eine private IPv6-Adresse, auf welche die Privacy Extentions angewandt werden. Dabei muss jedoch gegeben sein, dass man keinerlei Zusammenhang zwischen den beiden Adressen herstellen kann. Es ist daher nötig bei der Generierung eine Zufallsvariable mit einzubeziehen, um dies zu verhindern.

4.1 Einsatz der Privacy Extentions

Das Ziel der Privacy Extensions ist es, bei erhöhter Sicherheit und Privatsphäre, die gleiche einfache Handhabung und automatische Adressgenerierung wie bei der Stateless Address Autoconfiguration sicherzustellen. Es soll somit ermöglicht werden, aus dem zufällig erstellten Interface Identifier verschiedene Adressen, mit unterschiedlichen Präfixen, zu erstellen. Eine andere Möglichkeit ist die Generierung eines spezifischen Interface Identifiers für jeden Präfix, um damit keinen Zusammenhang zwischen den einzelnen Adressen herzustellen. Dies führt jedoch möglicherweise zu einer Performancereduzierung. Aus diesem zufälligen Interface Identifier sollen sich zudem keine zukünftigen oder vergangenen Interface Identifier ableiten oder berechnen lassen. Die Generierung des Interface Identifiers erfolgt in einem vorher festgelegten Zeitintervall, welches standardmäßig bei 24 Stunden liegt. Die Zeit kann jedoch durch den Nutzer geändert werden.

4.2 Generierung des zufälligen Interface Identifiers

Bei der Generierung des randomisierten Interface Identifiers gibt es zwei verschiedene Vorgehensweisen. Die erste Vorgehensweise setzt einen persistenten Speicher für die Erzeugung des Interface Identifiers voraus. Diese Variante verzichtet auf die Generierung eine Zufallszahl bei der Erzeugung eines neuen Interface Identifiers. Hier muss nur bei erster Inbetriebnahme eine Zufallszahl zu generiert werden.

Die zweite Methode wird bei nicht vorhandenem Speicher eingesetzt. Dort ist es nötig bei jeder neuen Erzeugung eines Interface Identifiers, auch eine neue Zufallszahl generieren.

Bei einem Gerät, welches nach der ersten Methode vorgeht und somit über persistenten Speicher verfügt, wird bei der ersten Inbetriebnahme eine 64 Bit Zufallszahl generiert. Diese sollte von hoher Qualität und damit schwer zu erraten sein. Bei dieser Methodik muss immer ein 64 Bit langes "history value" vorhanden sein. Dieses wird entweder, wie oben beschrieben, bei Erst-Start generiert oder wurde aus der vorherigen Erzeugung eines Interface Identifiers gespeichert.

Der eigentliche Vorgang der Erzeugung des Interface Identifiers beginnt damit, dass man das "history value" an den, durch die Stateless Address Autoconfiguration erzeugten, Interface Identifier anhängt. Hiervon wird nun der Message-Digest Algorithm 5 (MD5)-Hash erzeugt, welcher 128 Bit lang ist. Es ist jedoch auch möglich andere Hashingverfahren zu verwenden. Für den Interface Identifier werden die linken 64 Bit verwendet und das siebte Bit wird auf 0 gesetzt, um die Adresse als lokal zu setzen. Wie bei der Stateless Address Autoconfiguration werden auch hier die Adressen auf ihre Einzigartigkeit hin getestet. Falls der Interface Identifier in einem reservierten Bereich liegt oder schon verwendet wird, ist es nötig ihn erneut zu generieren. Dies geschieht unter Verwendung der rechten 64 Bit des zuvor errechneten MD5-Hashes als "history value", welche an den Interface Identifier angehängt wird. Mit diesem neuen "history value" wird das Verfahren von oben

erneut angewand. Dies geschieht solange, bis man eine gültige Adresse erhält. Falls kein Konflikt vorherrscht und eine gültige Adresse bestimmt wurde, werden die rechten 64 Bit des Hashes als history value auf den persistenten Speicher geschrieben.

Der statische Interface Identifier wird deshalb in das Verfahren mit einbezogen, damit es durch gleiche Zufallszahl-Generatoren nicht zu ständigen Konflikten kommt, falls zwei Geräte immer wieder die selben Zufallszahlen generieren.

Die zweite Methode, welche bei der Absenz von Speicher zur Anwendung kommt, geht ähnlich vor. Statt jedoch auf das "history value" zurückzugreifen, ist es nötig bei jeder neuen Erstellung eines Interface Identifiers auch eine neue Zufallszahl zu generieren. Danach kann das Verfahren aus der ersten Methode angewandt werden.

5 Mögliche Verbesserungen der Privacy Extentions

Die Privacy Extentions sind zwar eine enorme Verbesserung gegenüber dem Standardverfahren der Stateless Address Autoconfiguration, jedoch nicht ohne weiteres Verbesserungspotenzial. Da der Grad der Sicherheit beziehungsweise der Privatsphäre dort stark von dem Zeitintervall der Generierung eines neuen Interface Identifier abhängt. Ausserdem bleibt auch hier der Interface Identifier bei einem Wechsel in ein anderes Netzwerk und damit bei einem Wechsel des Adresspräfix, konstant. So lässt sich die Adresse immer noch ohne Probleme einem Client zuordnen. Dadurch wird ist es für mögliche Angreifer immer noch möglich ihn zu verfolgen und zuzuordnen.

Ein möglicher Verbesserungsvorschlag wird in [BWO11] gemacht. Dort wird eine Einbeziehung des Präfixes in die Erzeugung von Interface Identifiern vorgeschlagen. Dadurch unterscheidet sich der Interface Identifiers eines Gerätes in verschiedenen Netzwerken, auch wenn sich die Ausgangszahl für die Generierung nicht verändert hat.

In dem Paper wird der Interface Identifier anhand des Präfixes und einer Zufallszahl gebildet, statt die MAC-Adresse mit einzubeziehen. Dadurch wird die Sicherheit enorm erhöht. Der Generator für die Zufallszahlen sollte zudem kryptographisch sicher sein, damit die vorhergegangenen und nachfolgenden Wert nicht erraten werden können. Die Erzeugung des Interface Identifier erfolgt, wie bei den Privacy Extentions, über die Erstellung eines Hashes. Dieser wird hierbei jedoch aus der Zufallszahl addiert mit n, angehängt an den Präfix erstellt. Das n ist hierbei ein Offset, welcher bei Systemstart oder Wechsel der Zufallszahl auf 0 gesetzt wird und um eins inkrementiert wird, falls eine Adresskollision vorliegt. Dies verhindert die erneute Generierung einer Zufallszahl, indem diese einfach um den Offset inkrementiert wird. Als Hashverfahren wird hier mindestens SHA-2 empfohlen, um die Berechnung der Zufallszahl bei Kenntnis der Adresse und des Präfixes zu vermeiden, da es deutlich schwerer zu knacken ist als MD5, welches bei den Privacy Extentions verwendet wird.

Für die Festlegung des Intervalles, in welchem die Zufallszahl erzeugt wird, werden dort mehrere Möglichkeiten genannt. Zum einen ist eine zeitabhängige Änderung wie bei den Privacy Extentions möglich. Hierbei ist jedoch die Wahl des Wertes entscheidend. So muss das Intervall so groß gewählt werden, dass die bestehenden Verbindungen nicht zu stark beeinträchtigt werden, da bei Wechsel des Interface Identifiers und dem damit verbundenen Wechsels der IP-Adresse, die bestehende Verbindung beendet wird. Das Intervall sollte jedoch auch klein genug sein, um eine mögliche Zuordnung einer IP-Adresse zu einem Gerät zu machen.

Eine andere Möglichkeit, welche dieses Problem umgeht, ist die Generierung der Zufallszahl, wenn sich das Gerät mit einem Netzwerk verbindet. Dies geschieht entweder beim Start des Gerätes oder bei einem Wechsel des Netzwerks. Da bei einem Wechsel des Netzwerkes ohnehin alle bestehenden Verbindungen beendet werden, gibt es keine Probleme durch zu schnell wechselnde Adressen. Ausserdem ist der Zeitraum, in dem eine neue Zufallszahl generiert wird, klein genug, um einen ausreichenden Grad an Sicherheit zu gewährleisten.

Eine ähnliche Lösung ist die Generierung der Zufallszahl bei jedem Systemneustart. Dadurch werden ebenfalls ungewollte Verbindungsabbrüche verhindert, die Sicherheit dieser Lösung ist jedoch stark von der Häufigkeit der Neustarts abhängig.

Eine Möglichkeit, welche vor allem bei Firmennetzwerken interessant ist, ist die Generierung der Zufallszahl bei der Installation des Betriebssystems. Dadurch bleibt der Interface Identifier in einem Netzwerk bei jeder Anmeldung gleich, wechselt man jedoch

in eine anders Netzwerk, wird durch die Einbeziehung des Präfixes, ein anderer Interface Identifier verwendet. Ein Tracking des Gerätes durch mehrere Netzwerke wird so zwar verhindert, eine IP-Adresse lässt sich dennoch dem dazugehörigen Client im passenden Netzwerk zuordnen.

Die letzte Möglichkeit ist die Generierung der Zufallszahl vom Nutzer anstoßen zu lassen. Dies umgeht ebenfalls das Risiko ungewollter Verbindungsabbrüche, kann jedoch auch zu Sichheitsrisiken führen, falls der Nutzer sich nicht darüber im klaren ist, dass dies manuell geschehen muss oder der Nutzer es einfach vergisst.

Daher empfehlen die Autoren, die Zufallszahl bei jeder neuen Verbindnung zu einem Netzwerk zu erzeugen, da dies den besten Kompromiss zwischen Nutzbarkeit und Sicherheit darstellt.

6 Fazit

Bei der näheren Betrachtung zeigt sich, dass IPv6 nicht nur Vorteile mit sich bringt, sondern auch einige Nachteile. Der große Adressraum erlaubt beispielsweise eine sehr viel größere Anzahl an Geräten im Internet. So kann sich nun jedes Gerät mit einer eigenen globalen IP-Adresse mit dem Internet verbinden. Außerdem ist es nicht mehr nötig NAT zu benutzen, was Vorteile bringt, da beispielsweise keine manuelle Portweiterleitung benötigt wird. Doch dadurch die große Anzahl an Adressen ergibt sich natürlich auch die Gefahr, dass jedes Netzwerkgerät eine feste IP-Adresse zugeteilt bekommt. Es gäbe dabei zwar den Vorteil, dass beispielsweise Updates vom Hersteller direkt zu allen verkauften Netzwerkgeräten geschickt und damit automatisch aufgespielt werden, womit Sicherheitslücken schnell geschlossen werden können. Aber es erlaubt auch, dass dadurch ein System gezielt angegriffen werden kann. Diese feste Zuordnung kann auch zu einer mangelnden Privatsphäre und auch zum Verlust der Anonymität im Internet führen. Beispielsweise wird so Webseiten ermöglicht wiederkehrende Benutzer zu erkennen und Angreifer haben es einfacher die IP-Adresse einem spezifischen Gerät oder sogar einem Nutzer zuzuordnen.

Diese festen Adressen sind auch ein Schwachpunkt der mittels Stateless Address Autoconfiguration erzeugten Adressen. Diese Schwachstelle wird durch die Privacy Extentions teilweise geschlossen, aber auch diese sind noch nicht perfekt. Man sieht an den vorgestellten Verbesserungen, dass in Zukunft noch einige Verbesserungen in IPv6 einfließen werden. Dies ist jedoch nur möglich, wenn das Protokoll zunehmend genutzt wird, da erst durch die großflächige Nutzung neue Schwachstellen gefunden und, die daraus entstehenden Probleme, gelöst werden können.

Auch IPv4 war anfangs nicht ohne größere Fehler und auch IPv6 wird sich im Laufe der kommenden Jahre immer weiter entwickeln und sich dadurch stetig verbessern.

Bis sich IPv6 schlussendlich durchsetzen wird beziehungsweise der Großteil des Netzwerkverkehrs über dieses Protokoll abgewickelt wird, dauert es noch einige Jahre. Das lieg vor allem daran, das noch immer viele ältere Netzwerkgeräte verwendet werden, welche nicht IPv6-kompatibel sind. Daher ist eine sofortige Umstellung nicht möglich und muss schrittweise erfolgen. Aktionen wie der "World IPv6 Day" helfen dabei, da sie sowohl die Nutzer als auch die Anbieter von Webdiensten und die Internetdienstanbieter auf die Vorteile von IPv6 hinweist.

Auch in Deutschland haben Internetdienstanbieter, wie zum Beispiel die Deutsche Telekom [GO12] oder Kabel Deutschland [HE12], bereits damit begonnen IPv6-Adressen an Endkunden zu verteilen. Dadurch ist die Verbreitung von IPv6 hierzulande auch höher als der Durchschnitt und liegt, laut einer Statistik von Google, bei etwa 2,7 Prozent.

Durch Verbesserungen und einer größeren Beachtung, sowohl von Nutzer als auch von den Internetdienstanbieter, des neuen Internetprotokolls IPv6 kann die Geschwindigkeit der Verbreitung weiter beschleunigt werden.

Bis der gesamte Netzwerkverkehr auf IPv6 setzt, wird es voraussichtlich noch sehr lange dauern, da mit der Umstellung auch hohe Kosten verbunden sind.

7 Quellen

[GOOG] Google, *IPv6 Statistics*, http://www.google.com/ipv6/statistics.html.

[RFC 2460] S. Deering and R. Hinden, *Internet Protocol, Version 6 (IPv6) Specification*, RFC 2460 (Draft Standard), December 1998, Updated by RFCs 5095, 5722, 5871, 6437, 6564, 6935.

[RFC 3022] P. Srisuresh and K. Egevang, *Traditional IP Network Address Translator (Traditional NAT)*, RFC 3022 (Informational), January 2001.

[RFC 3315] R. Droms and J. Bound and B. Volz and T. Lemon and C. Perkins and M. Carney, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*, RFC 3315 (Proposed Standard), July 2003, Updated by RFCs 4361, 5494, 6221, 6422, 6644.

[RFC 3513] R. Hinden and S. Deering, *Internet Protocol Version 6 (IPv6) Addressing Architecture*, RFC 3513 (Proposed Standard), April 2003, Obsoleted by RFC 4291.

[RFC 4291] ———, *IP Version 6 Addressing Architecture*, RFC 4291 (Draft Standard), February 2006, Updated by RFCs 5952, 6052.

[RFC4294] J. Loughney, *IPv6 Node Requirements*, RFC 4294 (Informational), April 2006, Obsoleted by RFC 6434, updated by RFC 5095.

[RFC 4862] S. Thomson and T. Narten and T. Jinmei, *IPv6 Stateless Address Autoconfiguration*, RFC 4862 (Draft Standard), September 2007.

[RFC 4941] T. Narten and R. Draves and S. Krishnan, *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*, RFC 4941 (Draft Standard), September 2007.

[RFC 5952] S. Kawamura and M. Kawashima, *A Recommendation for IPv6 Address Text Representation*, RFC 5952 (Proposed Standard), August 2010.

[IS11] Webseite der Internet Society, *2011 World IPV6 Day*, http://www.internetsociety.org/ipv6/archive-2011-world-ipv6-day, 2011.

[BWO11] D. Barrera, G. Wurster, P.C. van Oorschot, *Back to the Future: Revisiting IPv6 Privacy Extensions*, LOGIN: The USENIX Magazine, vol. 36, no. 1, pp. 16 - 26, Juni 2013.

[NRO11] Number Resource Organization, *Free Pool of IPv4 Address Space Depleted*, http://www.nro.net/news/ipv4-free-pool-depleted, Juni 2013.

[HE12] heise Netze, *IPv6-Feldtests bei Kabel Deutschland*, http://www.heise.de/netze/meldung/IPv6-Feldtests-bei-Kabel-Deutschland-1559624.html, Juni 2013.

[NRO10] Number Resource Organization, *NRO and OECD Highlight that IPv6 Deployment is Too Slow* , http://www.nro.net/news/nro-and-oecd-highlight-that-ipv6-deployment-is-too-slow, Juni 2013.

[GO12] Jens Ihlenfeld (golem.de), *Telekom verteilt IPv6-Adressen an Kunden*, http://www.golem.de/news/ipv6-telekom-verteilt-ipv6-adressen-an-kunden-1211-96035.html, Juni 2013.

[WIPL] Webseite des World IPv6 Launch, *World IPV6 Launch*, http://www.worldipv6launch.org/, Juni 2013.