IPv6 Sicherheit

Bedrohungen in neuem Gewand

Peter Infanger

Well-known Facts zu IPv6

- Adressen bis zum Abwinken
- modularer Header → erweiterbar
- neue Diensttypen (z.B. Anycast)
- End-zu-End Kommunikation ohne NAT für alle
- QoS kein Fremdwort mehr
- unterstützt Mobilität (Mobile IPv6)
- div. techn. Verbesserungen (Fragmentierung etc.)
- Sicherheit integriert

ähm, ist das wirklich wahr?

Good News

- Die gute Nachricht ist, dass die Security in IPv6 ziemlich ähnlich ist wie die Security in IPv4.

Bad News

- Die schlechte Nachricht ist, dass die Security in IPv6 ziemlich ähnlich ist wie die Security in IPv4.

IPv6 Security

- Security kann ein Motivationsgrund sein um nach IPv6 zu wechseln:
  - ist aber eher Marketing Hype
  - basiert auf Anforderungen für IPv6 um IPsec zu implementieren
- IPsec hat sich aber inzwischen auch gut in IPv4 etabliert
- Zwar helfen einige Features gegen Bedrohungen (z.B. Fragmentierung)
- Aber IPv6 macht nichts um Outlook oder HTTP sicherer zu machen!
- IPv6 (und IPsec) sind nicht die „Silberkugel“ für Sicherheit

Wo gibt es denn Probleme mit IPv6?

- Probleme können bereiten:
  - Auto-Konfiguration
  - Routing bzw. Routing-Steuerung
  - Übergangsszenarien bei der Einführung (z.B. Teredo oder 6to4 Szenarien)
  - ICMPv6
  - Implementierungsprobleme
  - ...

Autokonfiguration

- Kein DHCP notwendig
- Automatische Adresszuweisung (link-local und site-local bei aktivem IPv6-Router)
- Automatische Router und Nachbar-Erkennung
- Kein ARP notwendig (da MAC Teil der IPv6 Adresse)

Mängel der Autokonfiguration

- Neighbor Discovery fehlt einen Mechanismus um authorisierte Nachbarn zu bestimmen
- Bedrohungen:
  - Umleitungen,
  - Adressen stehlen, Denial of Service,
  - Advertisement und Parameter spoofing
- Jeder kann sich als Router ausgeben
  → Traffic wird über ihn umgeleitet
- Es existieren Mechanismen wie ***Stateless DHCPv6*** oder ***dynamisches DNS***, bei der sich Hosts selbst im DNS eintragen (RFC3736) können
  → was will man mehr ☺

IPv6 Transition

- Teredo
  - tunnelt IPv6 in IPv4 mittels UDP Encapsulation
  - entwickelt von Microsoft, ab XP (SP1) dabei (RFC4380)
  - ermöglicht Clients mit privaten IPv4 Adressen (also kein 6to4 machbar) trotzdem via globale IPv6 erreichbar zu sein
  - bohrt Löcher in Firewalls (daher der Name: Teredo navalis, der Schiffsbohrwurm)
  - Kontaktiert per default einen Microsoft Teredo Server (teredo.ipv6.microsoft.com)

Teredo Sicherheit

- Automatisch deaktiviert wenn lokales Netz IPv6 spricht, die Firewall abgeschalten ist oder der Client in einem AD ist (unter Vista)
- Bei XP deaktiviert wenn Client in AD ist
- Wo liegt das Problem?
  - Falls aktiviert bohrt es Löcher in die Firewall und behält diese offen
  - Teredo Server und Teredo Relay: wo stehen die und wem gehören die, bzw. wer hat Kontrolle darüber?

Spoofing in IPv4 mit 6to4

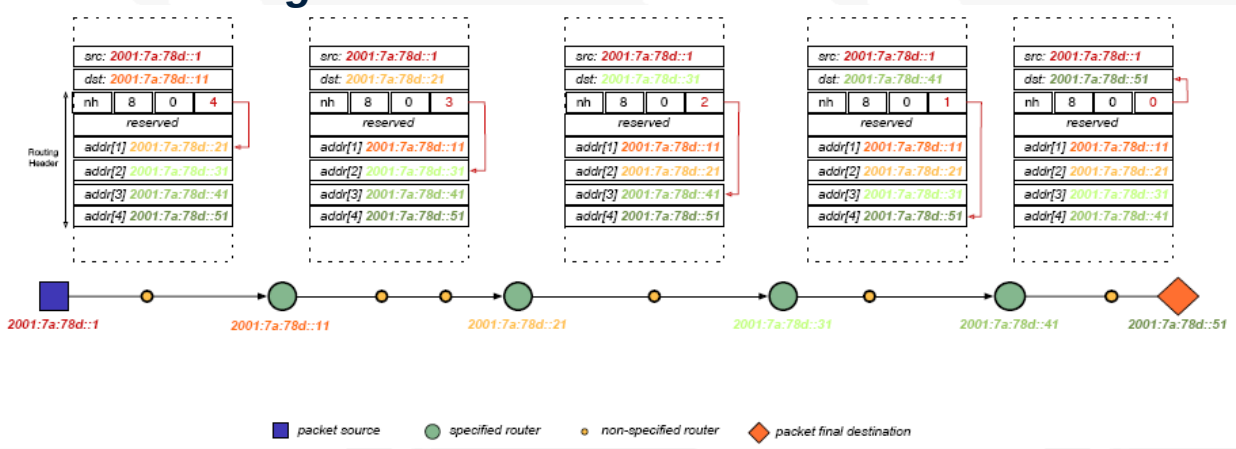
- Mittels Spoofing des 6to4 Tunneling kann Traffic von IPv4 in eine IPv6 Netzwerk eingeschleust werden:
  - IPv4 Quelle: spoofed IPv4 Adresse
  - IPv4 Ziel: 6to4 Relay (192.88.99.1, gemäss RFC3068 ein weltweit verteilter Cluster von Relays)
  - IPv6 Quelle: 2002::Spoofed-Source
  - IPv6 Ziel: gültige Zieladresse

Gemischte IPv4/IPv6 Umgebungen

- Verhindern von automatischen „Übersetzungsmöglichkeiten“ zwischen IPv4 und IPv6, man sollte die „Dual Stack“ Variante benutzen
- Nur authorisierte Systeme dürfen als Tunnel-Endpunkte verwendet werden
- „automatische Tunnels“ mit IPsec sichern

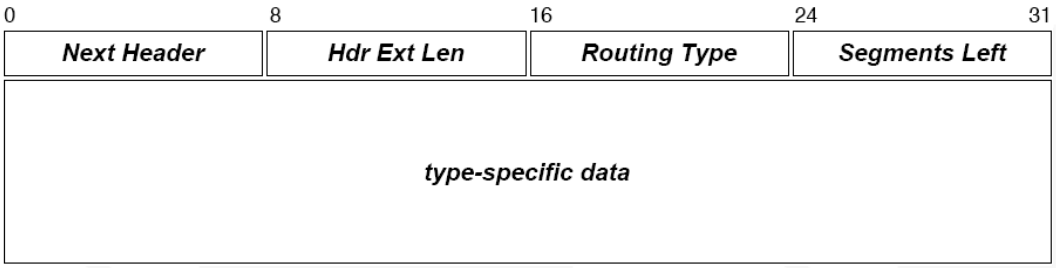
Eingriff ins Routing: Routing Header

- RFC2460 definiert Routing Header als Quelle einer Liste mit zu besuchenden Nodes auf dem Weg zum Ziel
- Typ 0 (RH0): bietet also eine gegenüber IPv4 erweiterte ***source-routing*** Funktion an.



Spiele mit dem Routing Header

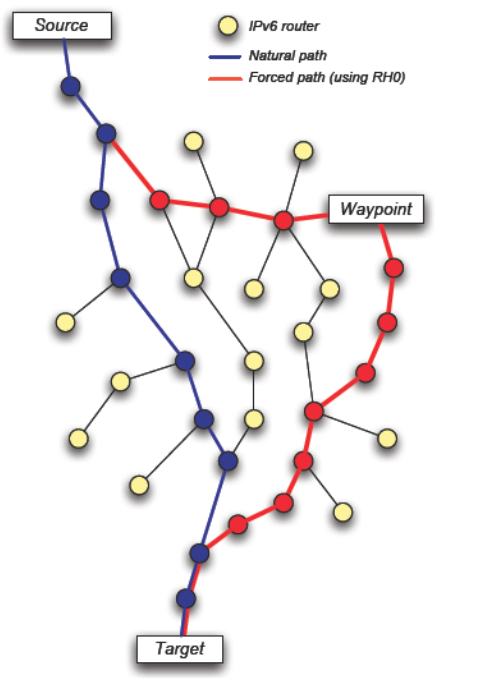
- Datenverkehr Umleiten
- „Storage in the Network“
- Bandwidth Amplification



IPv6 Routing Header

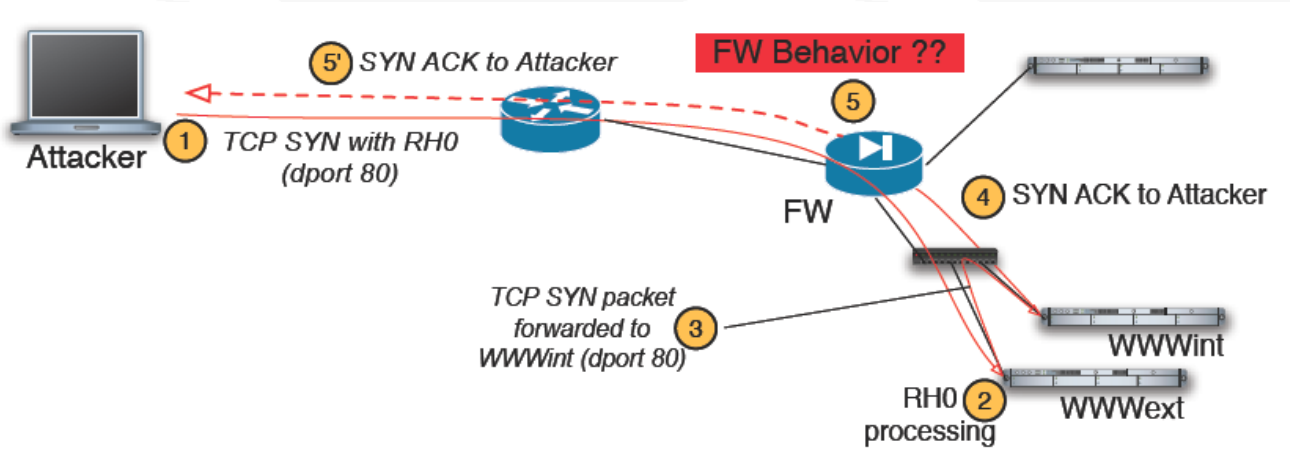
Datenverkehr Umleiten

- Gut geeignet um rauszufinden, ob ein ISP Ingress Filter aktiviert hat: ein Boomerang Paket (mit gespoofter Absenderadresse) an einen Router der RH0 unterstützt senden. Falls Paket retour kommt sind keine Filter etabliert.



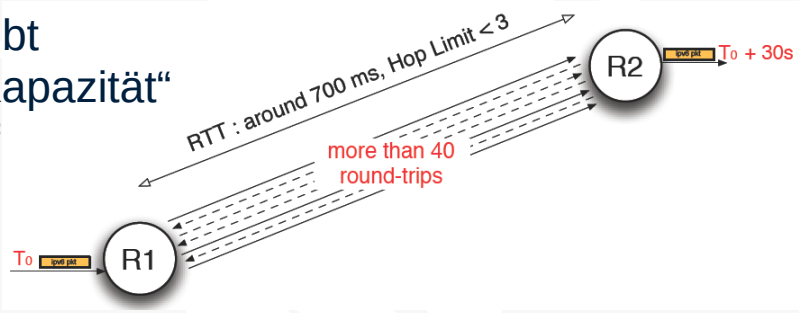
Spielereien mit der DMZ

- Facts:
  - BSD Hosts verarbeiten RH0 standard-mässig
  - Wie gehen Firewalls mit IPv6 States bzw. mit RH0 Filterung um?



Speicher im Netzwerk/Bandwidth Amplification

- Ziel: ein Paket so lange wie möglich im Netzwerk behalten
- Lösung: RH0 abwechslungsweise mit R1 bzw. R2 Adresse versehen
- Ergebnis: bei 4MB/s upload, 0.7s RTT und 43 RH0 = ca. 30s Laufzeit zwischen R1 und R2 ergibt ca. 16MByte „Speicher-Kapazität“ sowie Bandbreitenbedarf von ca. 172MB/s



Mitigierung von IPv6 Amplification

- RFC2827 (Source Address Spoofing) Ingress Filterung etablieren
- Ingress Filter von Paketen mit einer Multicast Source Adresse implementieren
- Versichern, dass Host RFC2463 befolgt (ICMPv6 Spezifikation)

Routing Header wirklich notwendig?

- Frage: gibt es irgend einen vernünftigen Grund, dass der Absender den Pfad des Paketes durchs Netzwerk bestimmen kann?
- Bei IPv4 ignoriert man diese Option schon lange, weshalb sollte man sie nun bei IPv6 benötigen?
- Umfasst ca. 17% der IPv6 Spezifikation, war der Aufwand gerechtfertigt?

→ Empfehlung: Routing Header nicht zulassen bzw. nicht beachten!

no ipv6 source-route

ICMPv6

- Keine Broadcast Adressen in IPv6
  - „smurf“-Attacken durch ICMP Pakete an Broadcast Adressen gehen also nicht mehr
- Wie seht es aber mit den Multicast Adressen aus?
  - IPv6 Spezifikation verbietet die Erzeugung von ICMPv6 als Antwort auf Pakete an globale Multicast Adressen (abgesehen von der „paket to big“ Message.
- Aaaaaber: leider unbestimmt Gefahr durch ICMPv6 Pakete mit einer globalen Multicast Source Adresse!!!

Altbekannte Probleme

- Implementierungen weisen Fehler auf:
  IPv6 Routing Header vulnerability
  (http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml)
  → blöder aber extrem lästiger und effektiver DoS Angriff (Router crashed)

Was hat sich nicht verändert?

- Virus und Würmer
- Sniffing: ohne IPsec genau gleich anfällig wie bisher
- Application Layer Angriffe: auch mit IPsec vorhanden, die Mehrheit der Angriffe laufen über diese Schicht.
- Man-in-the-Middle Angriffe: ohne IPsec genau gleich anfällig wie bisher
- Flooding: keine Veränderung (Verbesserung ☹) gegenüber IPv4

Zusammenfassung

- Die IETF arbeitet fortwährend an der IPv6 Sicherheit, sei es bei ICMPv6, IPv6 Firewall, Mobilität, Uebergangsphase etc.
- Hacker beginnen nach einem Einbruch, versteckte IPv6 Netzwerk zu etablieren
- Steigender Einsatz von IPsec abhängig von PKIs und anderen Benutzer Authentisierungsmechansimen
- Es gibt noch wenig „Standard-Tricks“ für IPv6 Firewalls
- Sicherheitsanalysen müssen Teil jeder ISP- bzw. Enterprise-weiten IPv6 Umsetzung sein
- Das Internet so wie es von der IETF definiert wurde stimmt nicht immer mit dem implementierten und eingesetzten Internet überein

Fragen