Ipv6 Threats to Communication

Steven M. Bellovin
smb@cs.columbia.edu
http://www.cs.columbia.edu/~smb

What is Security?

- Confidentiality
- Integrity
- Availability
- More generally, packets go to the desired destination reliably, and only to that destination.

Threats

- Attackers can eavesdrop on packets
- Attackers can damage, or forge packets
- Attackers can delay or drop packets
- You hand the packets to your enemy for delivery

The Internet Model

- The Internet makes no guarantees about security
- Packets may be dropped, damaged, duplicated, or reordered by the network
- Security must be *end-to-end*

Is IPv6 Better?

- Does IPv6 protect packets better?
- Does it help with delivery?
- In short, is security a reason to prefer IPv6?

- Sort of...

Areas of Improvement

- IPsec
- No NATs
- Address privacy
- Availability
- Secure Neighbor Discovery
- Worm defense?
- But what about tunnels?

IPsec

- Protects all upper-layer protocols.
- Requires no modifications to applications.
  - But smart applications can take advantage of it.
- Useful for host-to-host, host to gateway, and gateway-to-gateway.
  - Latter two used to build VPNs.

Doesn't IPsec work with IPv4?

- Yes
- It isn't standard with v4, but by now virtually all hosts support it
- Few implementations support host-to-host mode.
  - Even fewer applications can take advantage of it.
- IPv6 implementations are likely to behave the same way

IPsec is not a Distinguisher

- IPsec is too common in today's Internet
- The protocol was carefully designed to work with both versions of IP
- It was once a distinguishing factor for security. That's no longer the case.
- Might the implementations be more powerful?

No NATs for IPv6

- NATs break IPsec, especially in host-to-host mode.
- With no NATs needed, fewer obstacles to use of IPsec.
- Note carefully: NATs provide no more security than a stateful packet filter firewall.

NATs versus Firewalls

- There is a common belief that NATs are a stronger security device than firewalls
- NATs pass inbound packets if an outbound packet has created a state table entry
- Dynamic packet filter firewalls behave in exactly the same way
- Most firewalls also provide application-level protection – which NATs don't do

Let Me Repeat That

- NATs are not security devices. IPv6 without NATs is *not* less secure.

Address Switching

- Hosts can pick new addresses frequently.
  - Prevents tracking of usage.
- Improves privacy
  - Not precisely a security mechanism
- But can cause problems for security log files
- Using separate IP address per process group can simplify firewalls.

Availability

- Multiple addresses per host help with multihoming.
- Auto-renumbering permits switching providers without downtime.
- Autoconfiguration helps prevent mistakes.

Secure Neighbor Discovery

- A new feature in IPv6 protects neighbor discovery messages
- ND-spoofing – or ARP-spoofing in IPv4 – is a major security threat
- No equivalent protection mechanism in IPv4
- But – must have out-of-band knowledge of the local router's public key

SEND Authorization

- Authentication is not *authorization*
- SEND can secure the binding between an IPv6 address and a MAC address – but how do you know the IP address you're asking for is the right one?
- This is a difficult human factors problem, especially for hotspots

Worm Defense

- Some worms spread by probes of the address space
- A 128-bit space is too big for random probes
- Will that stop worms?

Probably Not...

- Hybrid techniques
- Site-local all-routers multicast to find nets
- All-nodes multicast to hosts on a LAN
- BGP tables, mail headers, web logs, etc. to find other addresses
- Besides, many worms operate at a higher level – email, word processing packages, etc.

Tunnels

- IPv6 transition mechanisms rely heavily on tunnels
- It's hard to block tunnels at firewalls
- For that matter, few firewalls understand IPv6

The Risks of Tunnels

- The tunnel problem is a major obstacle to IPv6 deployment
- People don't want to make their security weaker during the transition
- The problem is solvable with tunnel-aware firewalls
- Availability of such firewalls may be a major gating factor in v6 deployment

Firewalls

- Firewalls, though obsolescent, are still an important network security device
- The primary purpose of a firewall is to keep the bad guys away from buggy code
- That won't change with IPv6
- We'll still need firewall-like functionality, whether in outboard boxes or integrated with hosts

Flow Labels

- Can flow labels prevent DoS attacks?
- Probably not – too many mechanisms are still undefined
- Most applications are unlikely to use flow labels, because setting up a circuit is expensive

Matching Against the Definition of Security

- Confidentiality and integrity mechanisms are the same as in Ipv4
  - Some improvement in both because of SEND; it protects sessions that don't warrant strong crypto
- Availability is significantly better
  - SEND helps with that, too
- Tunnels remain a challenge

Conclusions

- IPv6 gives a noticeable – though not dramatic – improvement in security.
- The biggest difference is SEND.
  - Implementation matters a lot
- We may get some short-term defense against some worms.
- The very large address space may provide for other, innovative security mechanisms.