Security Concerns With Tunneling

draft-ietf-v6ops-tunnel-security-concerns-00

Dave Thaler
Suresh Krishnan
Jim Hoagland
Status

• Formerly draft-ietf-v6ops-teredo-security-concerns-02.txt
• Most points were not really unique to Teredo (many apply to tunnel brokers, MIP, TURN, VPNs, 6to4, etc)
• Don’t want to write a draft per protocol that says the same thing
  – Although some of the points are made in security considerations sections of existing protocols
• So changed the draft to be generic
• Added Dave Thaler as co-author
Security Devices/Software

• Security devices/software often do packet inspection
• **This draft takes no position on whether that is good or bad**
• The fact is, it exists
  – and people use them and expect certain security properties
• If tunnels bypass them in some way, the tunnels are seen by such admins as a security/policy violation
Dealing With Security Devices

• Don’t automatically tunnel to the Internet from a “managed” network
  – But may be hard to tell if network is “managed”
  – Implementations should require explicit user consent to enable tunneling, at least for the first time
    • Is this too strong?
• Hosts should prefer native connectivity over tunnels
  – If tunnel address space is well-known, add to Prefix Policy Table [RFC3484]
• One incentive for a managed network to provide native IPv6 is to reduce demand for IPv6 transition tunnels
• If tunneling isn’t an acceptable risk, admins may block tunneling
Identifying tunneled data packets

• How can a tunneled data packet be identified?
  – By protocol number (MIP, 6to4, ISATAP, etc.)
  – By port number (L2TP, some Teredo, etc.)
  – By tunnel server address
  – Pretend you’re the destination for parsing purposes and see if it parses according to that protocol
    • But this may incorrectly identify other packets too
Tunnels May Bypass In/Egress Filtering

- Ingress/egress filters in routers being tunneled over won’t see the inside IP addresses
- Could update routers to recognize tunnels (ugly)
- Tunnel servers can do filtering
- Can do checks in tunnel clients
  - If v4 addr embedded in v6 addr and supports peer-to-peer tunneling (e.g., 6to4, ISATAP, 6over4, etc), check if addrs correspond
  - If supports server-client tunneling, check if packet came from known server
    - Implies some secure server discovery mechanism (manual config, secure DNS resolution, whatever)
Increased Attack Surface Area

• If tunnel allows inbound access from public Internet, this may bypass a network “firewall”
  – Host-based “firewall” may still drop eventually
• If tunnel allows inbound access from a private network (e.g., a VPN), this still increases the amount of attackable code, but not as much
• Additional Recommendations:
  – Activate tunnels only when needed
Exposure of a NAT Hole

• NAT mappings kept stable means more discoverable
• External address/port may be easy to learn from client’s inner address
  – Client’s inner address may be discoverable in DNS, p2p systems, etc
• Tunnel packets are seen by more parties than native packets (e.g., due to longer paths)
• Learning the external address/port provides access to the entire inner address
  – Not just the application port that’s communicating with the outside
Public Tunnels Widen Holes in Stateful Address Filters

• Some devices only allow inbound packets from destinations that have been sent packets
• Public tunnels bypass this and may eliminate need for attacker to spoof
  – Host-based “firewall” may still drop

• Recommendations:
  – Activate tunnels only when needed
  – Consider whether tunnel server should do stateful filtering (TURN allows this for instance)
Guessing Addresses

• Some tunneling protocols make guessing addresses easier than an address scan especially for IPv6 (for IPv4 not so much)
  – Well-known or popular address prefix?
  – Embed popular server address?
  – Some address bits are constant?
Profiling Targets

• If a tunnel protocol is available on only a subset of host platforms, this helps attacker know what/how to attack
• Similarly if a specific tunnel server is used primarily by a subset of platforms
• Similarly for the client port (range)
• Information about the NAT type (e.g., cone NAT) can be used to target attacks
• If looking at an address reveals any of this information, this profiling can be done passively
  – Aside: This applies to MAC-based address generation too, not just tunnels
Other areas

• Attacks on tunnel server configuration
• Source routing [RFC5095]