Is Cyber Security IPv6-Ready?

HEPiX IPv6 Working Group

Bob Cowles

December, 2011

SLAC NATIONAL ACCELERATOR LABORATORY

U.S. DEPARTMENT OF ENERGY | Office of Science

Are there Security Issues?

- Architecture
- Design
- Implementation
- Configuration
- Operation
- Co-Existence with IPv4
- Tools

Architecture

- Multicast, IPsec, ICMPv6 required
- IP addresses impossible to remember
  - dead:beef
  - bebe

- Address mapping is now many to1 to many
- Fragmentation left to hosts

Design

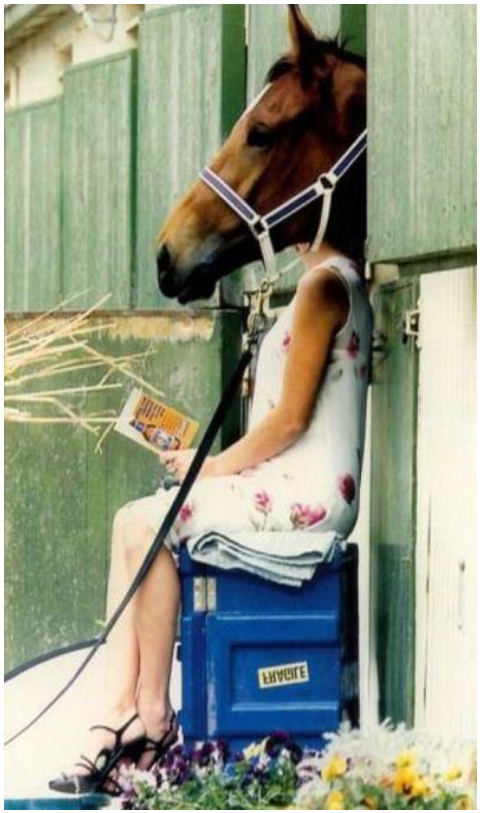
- Routing Headers bring back source routing
- Too many things are suggestions and not strictly enforced
  - TCP can adjust MSS to prevent fragmentation
  - Order of Extension Headers
- Unused fields can be covert channels
- Mobility IP

Implementation

- Implementations are still partial
  - E.g. centos firewall accepts IPv6 – does nothing
- IPv4 errors will be repeated
- Error conditions will be undetected or handled in different ways
- Inconsistencies in specs are still being discovered
- SEcure Neighbor Discovery (SEND) not widely implemented – required for adequate security
  - Protects RA/RS and ND
  - RFC3971

Configuration

- Many additional or different issues to consider
- Explosion of IP addresses / host
- Considerations in subnet and IP address assignment
  - Non-obvious vs. easy to guess?
  - Based on MAC vs. privacy
- Use routing headers? IP mobility? DHCP?



Operation

- Everything has to be tested in detail
  - Devices IPv6-Ready but associated firmware is not available (e. g. printers)
- Host option controls
  - Autoconfig vs DHCPv6
  - Mobile IP
  - IP address changing
  - Use of routing headers
  - Response to mDNS
  - Response to Neighbor Solicitations/Advertisements

Co-Existence with IPv4

- Dual stacks add complexity
- Ability to send packets over two different protocols (evade packet inspection)
- Tunnels – 6-to-4, Teredo (shipworm)
- Interactions not fully understood but will be exploited
- Windows – can turn off IPv6 but not restore via registry entry

Tools

- Some new tools, some old tools with new options
  - traceroute6 (unix), tracert -6 (windows)
  - tcpdump extended with new options and functionality (e. g. “protochain to parse extension headers)
  - wireshark, nmap is OK, snort is not ready

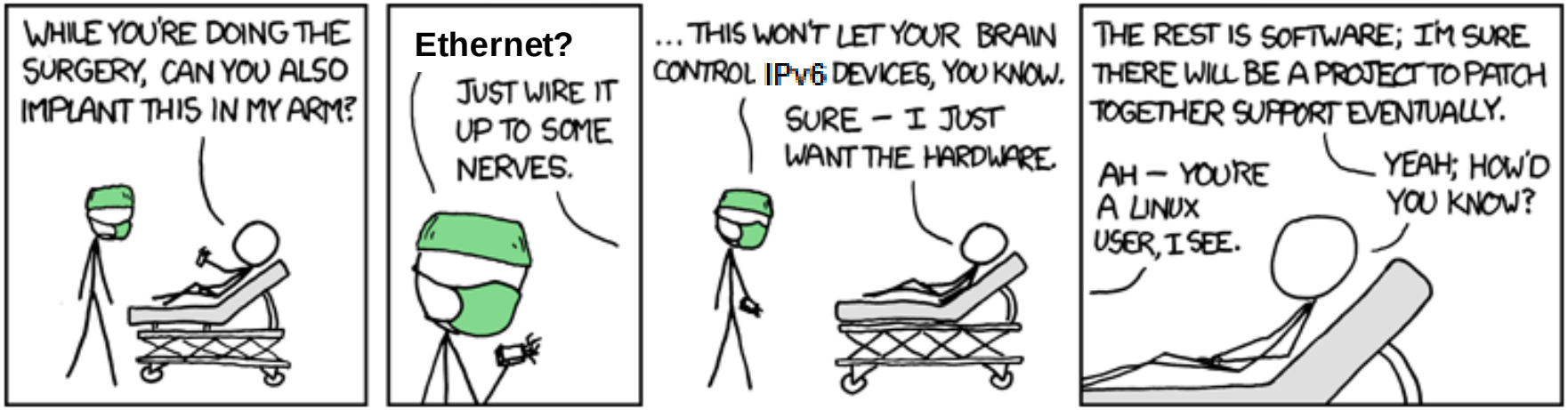
- Passive asset discovery easier than active

Security?

- Attention to configuration guidelines
  - http://www.nsa.gov/ia/_files/routers/I33-002R-06.pdf
  - http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf
- Plan transition carefully – use experiences published as guidelines
  - Join mailing lists

- Test, test
  - Everything works that is supposed to work
  - Nothing works that isn't supposed to work

Get Prepared!



Courtesy of xkdc.com

Liftoff!