IPv6 SECURITY CONSIDERATIONS

Carl Ness

IT Security Office

July 14, 2010

Oh yeah…

IT'S MY BIRTHDAY TODAY

TODAY'S AGENDA

- IPv6 Summary
- What to know
- What to watch
- What to do
- ITSO Services for IPv6
- Questions

IPV6 - BRIEFLY

- Replaces IPv4 32-bit addressing with IPv6 128-bit addressing
  - UIowa: 2620:0:e50::/48
- Dotted-quad replaced with colon-separated hex chunks
  - 128.255.1.3 → 2620:0:e50:2::1
- Intended to phase out IPv4, will co-exist for now
- DNS "A" records replaced or supplemented with quad-A (AAAA) records
- DHCP is replaced with SLAAC for dynamic addresses (for now)

So…

WHAT TO KNOW

WHAT TO KNOW

- IPv6 is widely used in the Europe and Asia (natively)
- Scanning takes literally years
  - DNS will be preferred targeting vector (BUT! Read RFC 5157)
- IPv4 verses IPv6: IPv6 is preferred
- Most modern OS have reasonable defaults
- A lot of auto-magic in IPv6
- Just because you can, doesn't mean you have to

WHAT TO KNOW

- There are some built-in security benefits of IPv6 (IPSec)
  - Not all are alive or widely used yet
- Security is just as important on IPv6 as any other protocol
- IPv6 software can be immature and vulnerable
- Security tools are weak and immature in the v6 space
- Public/Private is not well-understood
  - Not a big deal here

WHAT TO KNOW

- Malicious activity being reported by US Gov't & Google
  - IPv6-only botnets
  - Covert channels
  - Lack of NAT
  - Not all firewalls are well behaved

Next…

WHAT TO WATCH

WHAT TO WATCH

- Be aware of the dual stack
- Know thy IP address
  - What's static? What's automatic? What's both?
  - Privacy addresses preferred over global by most OS
  - http://whatismyv6.com/
- Host-based Firewalls
  - Not all are IPv6-enabled out of the box
- Tunnels – Evil
  - Especially wireless networks when laptops leave campus

WHAT TO WATCH

- No broadcast address – things happen on multicast
  - LLMNR, PNRP, SSDP, Multicast DNS
- Offering a common service? (Example: Email)
  - RBL service offering IPv6 lookups yet?
  - Feature parity between IPv4 and IPv6 stacks?

And finally…

WHAT TO DO

WHAT TO DO

- Don't panic. (yet)
- Understand IPv6
- Decide roll-out strategy
  - Disable services you don't need
  - Disable on servers, applications until everything is tested, then enable
- GPO where you can
  - Randomized Identifiers, Temporary Addresses, Router Discovery, **Tunnels**
- Monitor early and often
  - Firewall logs, application logs, server logs, etc.

WHAT TO DO

- Get into the habit of operating the dual-stack
  - Are your apps logging in v6?
  - Do your automated tools understand v6?
  - Are IP address formats hard-coded in your databases?
- Stay informed of IPv6 news
  - Especially for broadband ISP adoption
  - Applications and services adding IPv6 support every day
  - Ask your vendors!

ITSO SERVICES FOR IPv6

- Host scanning via IPv6
- Assistance with testing
- Firewall rules / Host IP filtering review
- ITSO Enterprise Service Notes:
  - At this time, IDS via IPv6 is “best effort”
  - UIAnywhere VPN – IPv4 only at this time

QUESTIONS?

IT Security Office

security@uiowa.edu

http://itsecurity.uiowa.edu

THANK YOU!