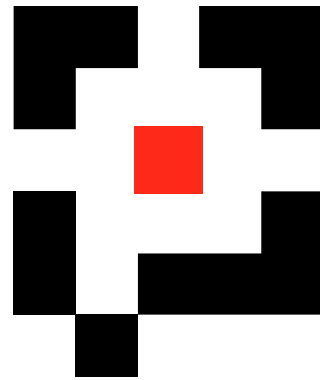


I
N
D
I
A
N
A

U
N
I
V
E
R
S
I
T
Y

Presentation by ANML
June 2004



pervasive **technology** labs

AT INDIANA UNIVERSITY

IPv6 and Security

A Bold Statement

“...our soldiers need better information in order to make better decisions—who to help and who to kill. The lack of security and flexibility in the current IPv4 protocol is a drag on our wing. This isn't about do you trust the Internet for your kid's homework, it's do you trust your kid's life. If we fail, people die.”

- Defense Department Will Require IPv6 Compliance, Says DoD's John Osterholz. From *Market Wire*, June 26, 2003.



pervasivet^{technology}labs

AT INDIANA UNIVERSITY

What is This Added Security?

...(not much)...



Overview

- That was another bold statement (and we had better back it up!)
- We will focus first on the *differences* in security between IPv4 and IPv6, then on the *similarities*
- This will include some social arguments



IPsec Support

- The major difference is that an IPv6 device *must* support IPsec
 - IPsec is available for both IPv4 and IPv6 but is not a *requirement* for IPv4
 - Configuration and use is functionally identical between IPv4 and IPv6
- This still leaves the question of when to actually use IPsec



IPsec Support

- IPsec is difficult to install and configure on most platforms
 - This is especially true with the retirement of the FreeS/WAN project
- Biggest problem is key distribution
 - Requires infrastructure support (e.g., special DNS RRs) and dedicated professional staff
 - If you get this part wrong, you gain complexity without any additional security



IPsec Adoption

- IPsec has been around since 1995, but still sees limited use outside of L2TP-based VPNs
- Why?
 - Much more ubiquitous support for SSL
 - IPsec and NAT don't mix well at all



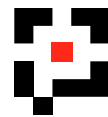
SSL vs. IPsec

- IPsec is better than SSL because it provides much better protection for packet headers
 - Provides *confidentiality, accountability, and authentication*
 - No more spoofed headers, etc.
- SSL is better than IPsec because you have it right now and it works pretty well for just about everything you want to do



Won't NATs Go Away?

- Part of the *purpose* of IPv6 is to restore the end-to-end model by providing more addresses
 - But address depletion is not the only motivating force behind NATs
 - Security practices are at least as much to blame
- NATs probably provide the best cost-to-benefit ratio of any simple security measure
 - A NAT box is dirt-cheap and easy to configure
 - It also completely breaks the end-to-end model
- There will still be NATs in IPv6



Address Sparsity

- Many IPv4 worms and cracking tools do scans of IPv4 address space to find hosts
- IPv6 increases the size of the address space by over 79,000,000,000,000,000,000,000,000,000,000 times
 - Properties of the address structure can pare down the search space somewhat
 - Nevertheless, brute force search of IPv6 address space will be completely intractable



Does This Gain Us Security?

- It does eliminate a primary technique of a great deal of malware (and some legitimate research efforts)
- Lists of hosts to attack will be harvested from system configuration files, e-mail addresses, Web sites, server logs, etc.
 - This is exactly how the Morris worm worked back in the late 1980s



Does This Gain Us Security?

- How well-known will a host need to be before its address leaks into this lists?
 - How much spam do you get?
- There is a bright side to this:
 - A long list of addresses takes up a lot of space and provides forensic evidence
 - You won't have packet-of-death attacks like SQL Slammer any more
 - Worms are more likely to report back to their source



Exposure of MAC Addresses

- Standard IPv6 addresses contain the MAC address in the lower 64 bits of the addresses
 - This is information that was usually confined to a single broadcast domain before
 - The manufacturer of your NIC is now public knowledge and may associate you with a known vulnerability



Things That Stay the Same

- IPv6 doesn't change TCP or UDP at all
- IPv6 doesn't patch vulnerabilities in individual applications or OSes
- IPv6 doesn't force network administrators to do egress filtering
- IPv6 doesn't mandate *use* of any security features



Things That Stay the Same

- A recent survey of CERT's top 100 vulnerabilities shows only *one* of them to be specific to IPv4
 - You'll still have e-mail trojans, buffer overruns, macro viruses, and so forth
 - You'll also still have SYN floods, RST attacks, OS fingerprinting, hijacked connections, and the like



Code Maturity

- Most of the IPv6 code in the world is new and untested in comparison to IPv4
- This code is certain to contain more flaws and vulnerabilities than its IPv4 equivalents
 - It's larger and much more complex
 - It has not yet stood the test of time—or attacks
- This situation will slowly improve over time
 - IPv6 isn't low-hanging fruit yet, so there's little motivation to attack it



Code Maturity

- Flaws will be opened in existing applications as they are ported from IPv4 to IPv6
 - IPv6 involves many more programming changes than just bigger addresses
 - Net increase in lines of line
- New code will be written to deal with (or reinvent) third-party libraries that do not handle IPv6 and cannot be modified



Protocol Maturity

- Not only is IPv6 code comparatively immature, but so are its standards
- Example: *A6* vs. *AAAA* DNS records
 - *A6* was clever, but raised concerns about DoS attacks using infinitely recursive delegated lookups
 - Now relegated to experimental status
- Similar concerns have been expressed about protocols for tunneling IPv6 in IPv4 networks



Protocol Maturity

- Many features are not fully specified yet
 - What do you do with the Priority field?
 - What's the exact structure of the Flow Label?
 - What's the format of Aggregatable Global Unicast Addresses *this year*?
 - When and how often do I do MTU discovery?
 - How do anycast addresses actually work?



Router Maturity

- Issues with code and protocol maturity come together in the routers
 - A vulnerable host may result in the loss of a single system
 - A vulnerable router may result in the loss of a substantial piece of the network
- Catch-22: Router vendors can't spend too much on testing IPv6 stacks until IPv6 gets more popular, and IPv6 has a hard time getting more popular until router vendors spend more time testing their IPv6 stacks



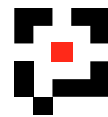
Competing and Complex Standards

- In some ways, IPv6 suffers from “design by committee” spread across multiple committees
- The IPv6 Address Oracle has to draw from over a dozen different RFCs
- Examples of multiple standards
 - DNS: AAAA vs. A6
 - Tunnels: At least four different approaches
 - Resolver: *getipnodebyaddr()* vs. *getaddrinfo()*



Best Practices

- Be prepared to devote considerable resources to development and maintenance of key infrastructure if you plan to use IPsec
- Adopt new features of IPv6 sparingly until their standards processes are finalized
- Allow for the existence of more undiscovered flaws in IPv6 code when assessing risks
- Subject ported applications to the same level of review and testing as new ones



Best Practices

- Have clear definitions of “IPv6 ready” and “IPv6 aware” when you compare vendors’ products
- Pay close attention to new RFCs as they come out—and changes in the status of old ones
- Design new protocols in such a way that they will continue to operate through a NAT
- Don’t write IPv6-only applications; make them dual-stack instead



Conclusion

- IPv6 does not make for a completely different world of security
- Expect a low level of incidents initially (*obscurity*), followed by a much higher level (*exploitation*), followed by a slow decline to the level we see now with IPv4 (*stasis*)

