



New Internet Security & Privacy Models Enabled by IPv6

Mat Ford



Agenda

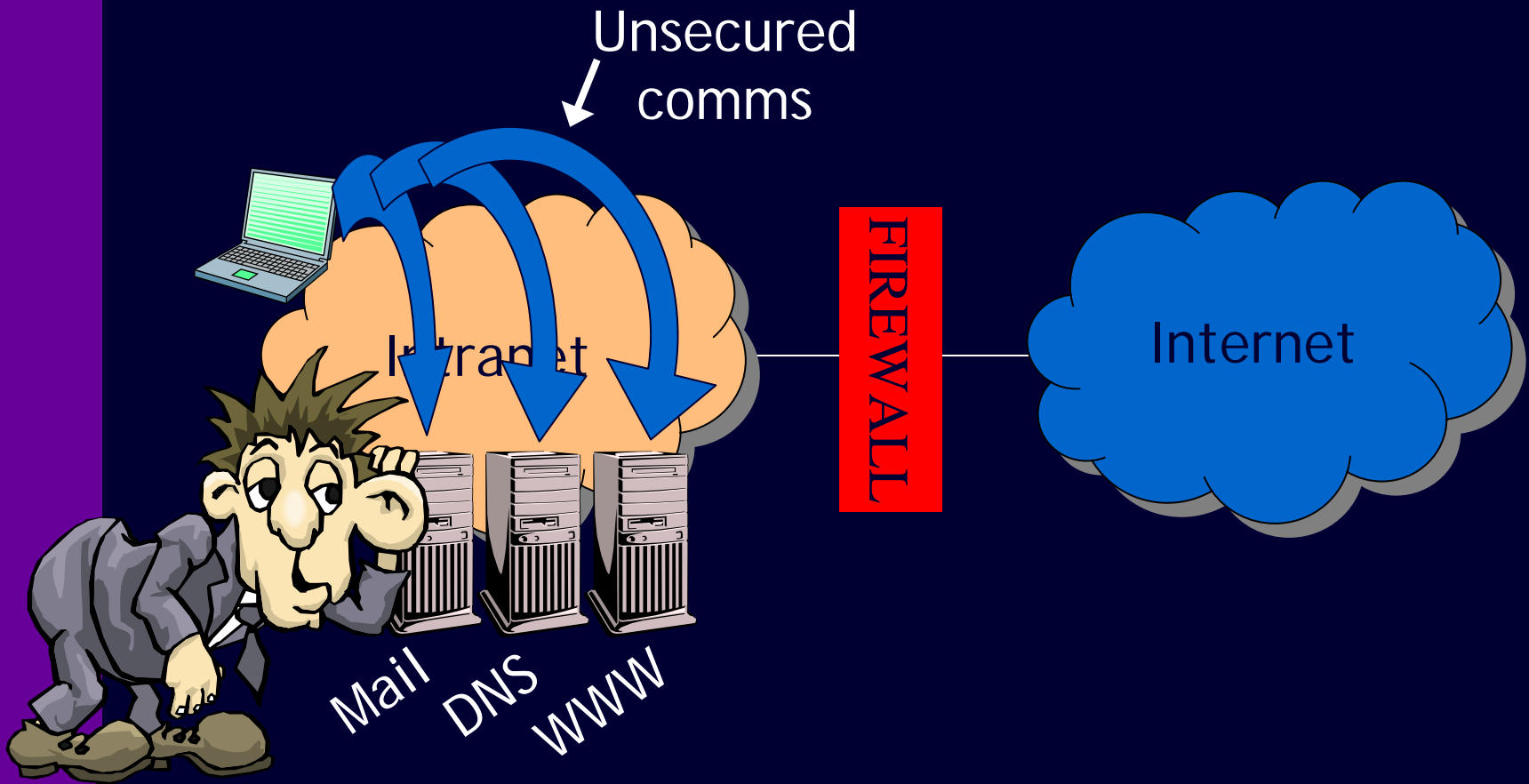
- What's different about IPv6?
- Enterprise security with IPsec
- Addressing privacy
- Secure public access networks
- Port scanning implications
- Secure mobility
- SEINIT project
- Conclusions

What's different about IPv6?

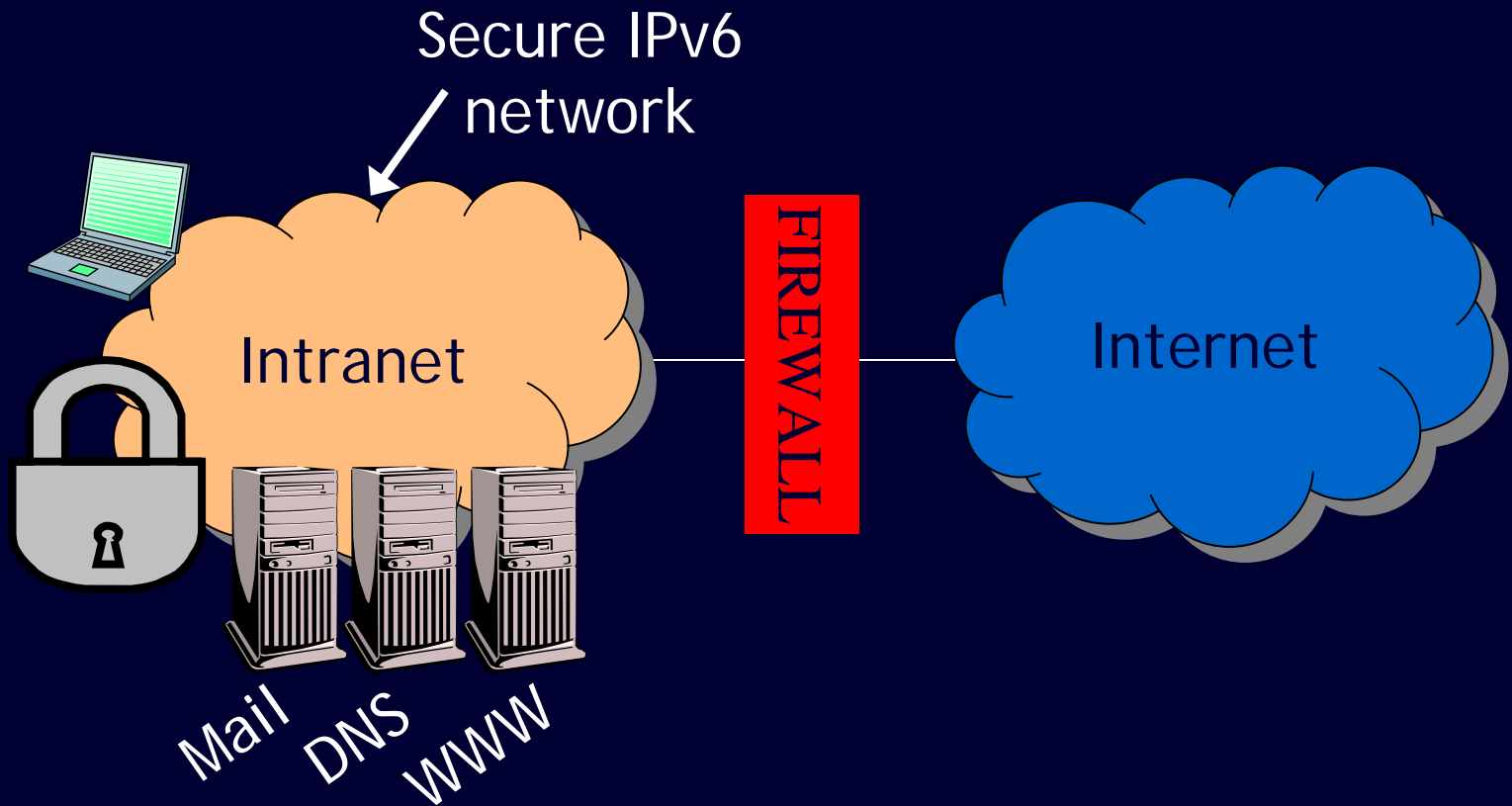
IPv6: So what's different?

- Larger address space
 - Not just about abolishing NAT!
 - Privacy addresses, scoped addresses
 - Cryptographically-generated addresses (CGA) & SEND
 - Port scanning implications
- IPsec implemented by default
 - My peer supports security
- Mobile IPv6

Enterprise security with IPsec



Enterprise security with IPsec



Addressing privacy (with privacy addresses)

Addressing privacy

- What do we mean by privacy?
 - Not confidentiality!
 - No association between observed IP addresses and individuals
 - No obvious correlation between communications on different networks
- Perennial tension between protecting privacy of individuals and protecting needs of society

Addressing privacy

- In IPv4, privacy is a by-product of dynamic addressing and/or NAT
- For users with static, public addresses there is NO technical privacy solution in IPv4

Addressing privacy

- No association between observed IP addresses and individuals?
- Largely a policy decision on the part of ISPs
 - Many ISPs currently use customer names to identify networks in public databases
 - Ambiguity of names can help in many cases

Addressing privacy

- No obvious correlation between communications on different networks?
- In some configurations, IPv6 nodes will construct IPv6 addresses that allow correlation of activity between networks
 - Probably unique identifier embedded in the IPv6 address
- In practice, this is not an issue – just use privacy addresses

Addressing privacy

- What are privacy addresses?
 - Huge number range available for host addressing
 - Choose random numbers and check for potential duplicates
- Provides anonymity to mobile nodes, and fixed nodes over time
- This functionality is enabled by default

Securing public access networks

Secure public access networks

- Lack of ARP security is long-standing IPv4 security weakness
- Wi-fi hotspots are hostile environments!
- Denial-of-service and MITM attacks are trivial to perform

Secure public access networks

- IPv6 addresses large enough to carry cryptographic tokens of validity
- This is a key differentiator – it is not possible to retrofit this functionality to IPv4

Secure public access networks

- SEND mitigates the threats posed by malicious hosts on a shared network
- IPv4 networks cannot be protected in this manner
- 802.1x doesn't protect you against authenticated users with malicious intent

Port scanning implications

Port scanning implications

- What do we mean by port scanning?
 - Scanning networks for hosts listening on particular ports of interest
 - Ports usually associated with a particular known vulnerability
 - Basic technique used by ‘black-hats’ to identify vulnerable hosts prior to compromise

Port scanning implications

- Typical IPv4 subnet will use 8 bits for host addressing
 - $2^8 = 256$
 - Probe one host per second = ~5 minutes
- Typical IPv6 subnet will use 64 bits for host addressing
 - $2^{64} = 18,446,744,073,709,551,616$
 - Probe one host per second = ~585 billion years!

Port scanning implications

Sounds good, but ...

- Search space can be reduced by both parties
 - Hosts numbered with 'easy' addresses (:::1)
 - Attackers can strip out 'known' fields (FFFE)
- Reduce attack time to 0-194 days
- Dual-stack apps on dual-stack hosts still vulnerable via IPv4
- Some transition mechanisms use easily guessable addresses

Port scanning implications

New attack vectors

- Harvesting addresses
 - Web server logs, email headers
- Compromised hosts make entire LAN vulnerable
 - ‘all hosts’ link-local multicast address

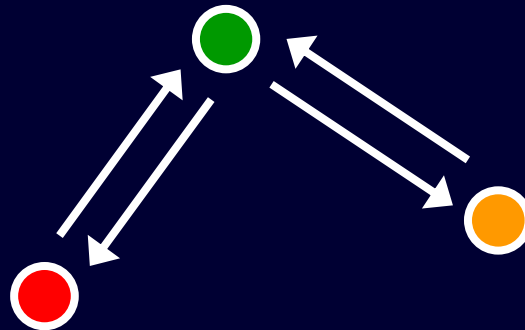
Port scanning implications

- Use Privacy Addresses by default
- Managed environments (using DHCPv6) should assign addresses from pool at random, not incrementally

Secure mobility

Secure mobility

- Mobility raises obvious security issue
 - Signalling of movement must be authenticated to prevent trivial session hijacking



Secure mobility

- Mobile IPv4 requires traffic to flow via Home Agent

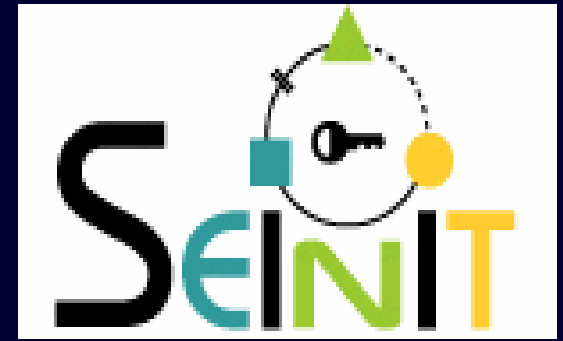


Secure mobility

- Mobile IPv6 uses 'Return-Routability' procedure to optimise routing

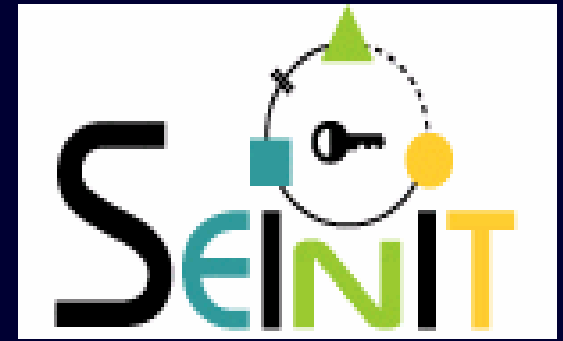


SEINIT project



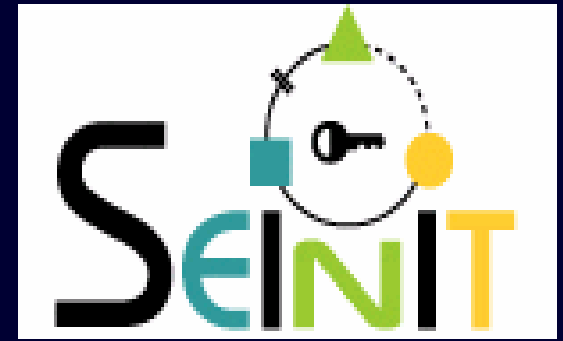
- Security Experts INITiative
- Kicked-off 01/12/03 – 2 year project
- Led by Thales Communications
- Partners include
 - 6WIND, BT, T-Systems Nova, ENST, IABG, KYOS, Telscom, Thales TRT (UK), UCL, Uni of Murcia, Waterford Institute, ISOC
- Public deliverables will be available from
 - www.seinit.org

SEINIT project



- Objectives
 - Develop a trusted and dependable security framework (end-user centric)
 - New security models, policies and components
 - Guidelines, best practice guides and training
- Input to ENISA and other European or national initiatives
- IPv6 is a core technology for the project

SEINIT project



- IPv6 Activities
 - Cryptographically Generated Addresses (CGA)
 - Integration of transition with security mechanisms
 - IPv6 routing protocol security
 - DNSsec integration
 - IPsec enhancements
 - Mobility Security (MobileIPv6)
 - Honeypot for analysing IPv6-borne attacks
 - Performance analysis
 - Operational guidelines
 - Security for IPv6-enabled applications
 - Anomaly detection systems

Conclusions

- IPv6 is not a security panacea
- Cannot protect against
 - Misconfiguration
 - Poor application design
 - Poor security design

Conclusions

- IPv6 can
 - Improve enterprise security
 - protect revenue
 - Improve wi-fi hotspot security
 - minimise outages and customer dissatisfaction
 - Increase revenue
 - Provide better communications privacy than IPv4

Conclusions

- IPv6 can
 - Improve efficiency and security of IP mobility deployments
 - reduce costs
 - Minimise exposure to port scanning
 - Protect revenue, defence in depth
- SEINIT project will be a focus for IPv6 security research going forward

www.seinit.org

Thanks for your attention!

Any Questions?

matthew.ford@bt.com

<http://www.bt.com/ipv6>