

Solving the right problems

Brian Carpenter

IBM

May 2004

Spam and pop-ups are a passing phase

- I once told Tim Berners-Lee that the Web is the froth on top of the Internet. He didn't quite agree, but...
- Spam & pop-ups are the froth on top of the froth
 - A little bit annoying
 - Easy to filter most of it
 - Will recede as a problem
 - Not interesting



Viruses are due to bad software engineering

- Techniques to build secure operating system kernels have been known since the 1960s.
- How to design efficient programming languages safe against buffer overflow has been known since the 1970s.
- There is no excuse for the poor engineering that has laid many operating systems open to virus vandals.
 - Virus filters and checkers are just a palliative
 - We really need secure programming languages and secure O/S kernels

Denial of service and spoofing attacks are here to stay

- DoS and spoofing attacks seem to be intrinsic to connectionless datagram networks, since per-packet authentication at every node is basically uneconomic.
- Source validation, intrusion defence, and intrusion detection are here to stay.
 - Firewalls and IDS are part of the architecture

Any use to you?

- My 802.11b address: 00-40-96-33-3C-F6
- My 802.3 address: 00-10-A4-8F-C4-2E



Privacy and anonymity are not the same thing

- Despite some attempts, nobody has yet invented an effective form of anonymous payment on the Internet.
- Until that happens, no transaction can be truly anonymous – there will always be a trail back to the subscriber or credit card holder.
 - Privacy concerns associated with hardware addresses are pretty bogus
 - Real privacy concerns should be about handling of non-anonymous data by service providers

The really hard problem

- Half the crimes on the Internet are inside jobs
 - Treating all inside systems and users alike is a big error
 - Security policy needs to be per-system, per-user, and applied end to end at network and applications level
 - For example, IPv6 to enable e2e network security and Web Services to enable e2e applications security
 - This is the real challenge for the next ten years