NETWORKERS 2003

THE POWER TO TRANSFORM BUSINESS. now.

Cisco Systems

Cisco.com

BoF Security: What's next?

Session BOF- 8002

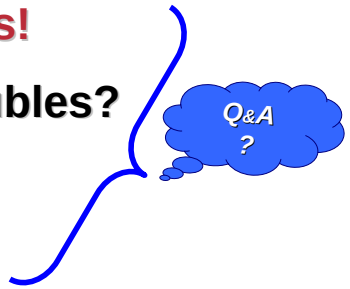
Franjo Majstor, fmajstor@cisco.com
Eric Marin, emarin@cisco.com
Thierry Van Herwijnen, therwijn@cisco.com
Marco Misitano, misi@cisco.com
Kevin Regan, kregan@cisco.com
Peter Provart, pprovart@cisco.com
Erik Lenten, elenten@cisco.com

© 2003, Cisco Systems, Inc. All rights reserved.

BoF "loose coupled" agenda

Cisco.com

- Some Security Myths!
- Future Security Troubles?
- Solutions?

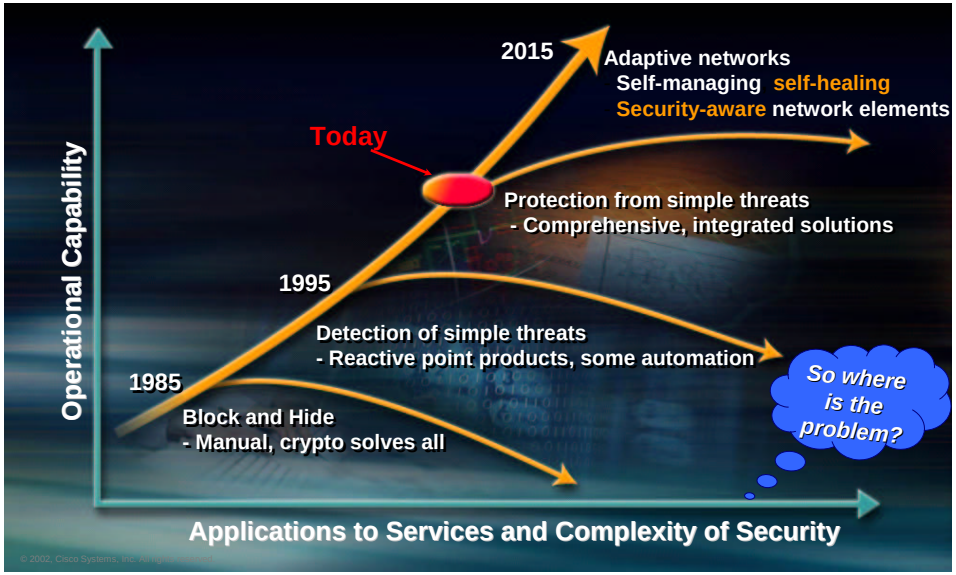


© 2003, Cisco Systems, Inc. All rights reserved.

Some Security Myths

Network Security Evolution

From Simple Detection to Simple Protection



© 2002, Cisco Systems, Inc. All rights reserved.

Solved on a another layer - eg. WLA

What about that special feature?

University of California, Berkeley

University of Maryland

Scott Fluhrer, Itsik Mantin, and Adi Shamir

Feb. 2001 — April 2001 — July 2001

Focuses on static WEP; discusses need for key management

Focuses on authentication; identifies flaws in one vendor's proprietary scheme

Focuses on inherent weaknesses in RC4; describes pragmatic attacks against RC4/WEP

* "In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks we describe…"

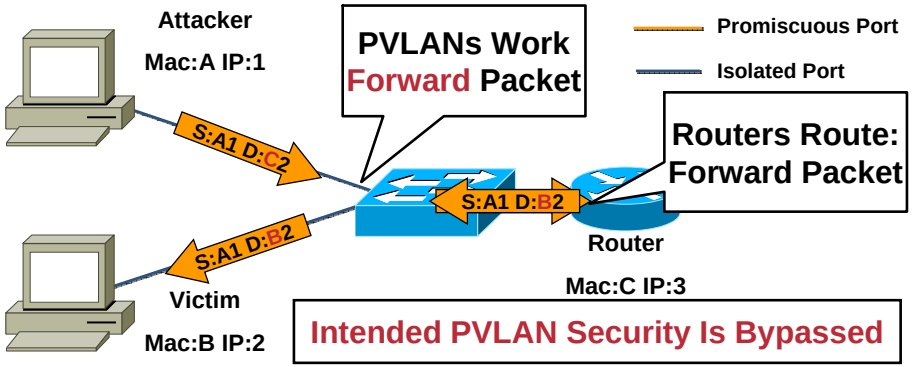
– University of California, Berkeley report on WEP security, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

© 2003, Cisco Systems, Inc. All rights reserved.

Special Feature?

Layers on top ?

Cisco.com



Independent security research firm @stake conducted a Security Review of the virtual LAN (VLAN) technology:

Cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml

- **Note: this is not a PVLAN vulnerability as it enforced the rules!**

© 2003, Cisco Systems, Inc. All rights reserved.

Port 80: "Break on Through to the Other Side…"

Cisco.com

- **Typically opened through firewalls**
- **It can be used to attack other hosts through**
- **Tunneling through the SSL port also hides the activity from IDS**

http://www.nocrew.org/software/httptunnel.html

So far so good, but what about "THE future"?

© 2003, Cisco Systems, Inc. All rights reserved.

Future Security Troubles?

New protocols - eg. IPv6?

Any new technology ?

- **Security & IPv6:**
  - **Nothing IP4 doesn't do - IPsec runs on both**
  - **Does a lot dynamically on L3 (via ICMP), hence remove all of L2 problems, right?**
  - **Autoconfiguration**

ICMP w/o IPsec AH⇔ gives exactly same level of security as ARP for IPv4 (none)

Bootstrap security problem!

Security mechanisms built into discovery protocol ⇔ None.

Bootstrap security problem!

From RFC 2462:

« If a duplicate @ is discovered … the address *cannot* be assigned to the interface…»

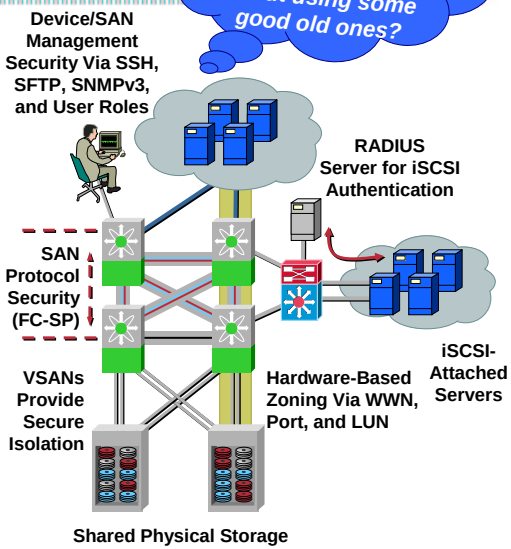
⇔ What if: Use MAC@ of the node you want to DoS and fabricate its IPv6 @

© 2003, Cisco Systems, Inc. All rights reserved.

Storage: SAN Security

New protocols, new technologies - great… ☹, how about using some good old ones?

- **Secure SAN management via roles-based access**
  - **64 customizable roles**
  - **Roles apply to CLI, SNMP, and web access**
  - **Full accounting support**
- **Secure management protocols including SSH, SFTP, and SNMPv3**
- **Secure switch control protocols**
  - **Switch to switch authentication**
  - **Switch to host authentication**
- **WWN, Port, and LUN zoning all done in hardware**
- **Full RADIUS support for switch and iSCSI host authentication**



© 2003, Cisco Systems, Inc. All rights reserved.

Web VPN's

Is this part of the problem or part of the sol…

What about new Apps?

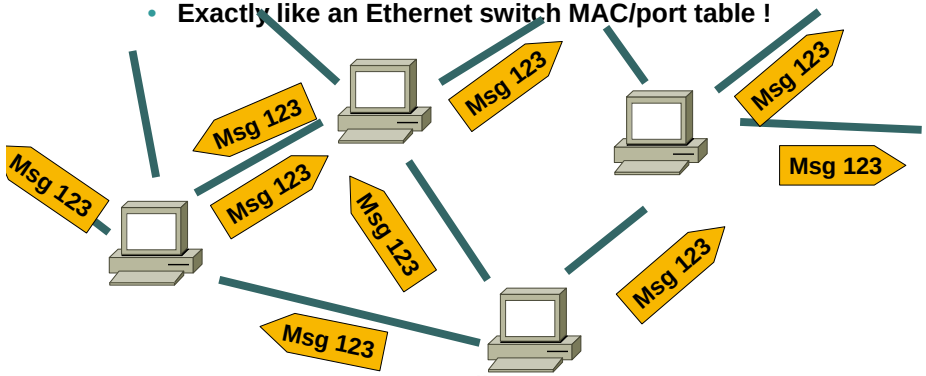
SSL VPN	IPSec VPN
Anywhere access to a limited application set using a Web browser	Robust remote access extending all applications available in the office to remote users
Easy firewall traversal	All applications, all traffic types
Enables Extranets/B2B commerce	Client software allows for application transparency
All applications accessed through browser portal or enabled by browser plug-in	Consistent user experience
Client/server support requires local application applets – Active X and/or Java dependencies	Maximum functionality for managed computers
	Requires installation and maintenance of client software if not using built-in client

© 2003, Cisco Systems, Inc. All rights reserved.

Gnutella, eDonkey, KaZaa, IM, … P

How big they really are?

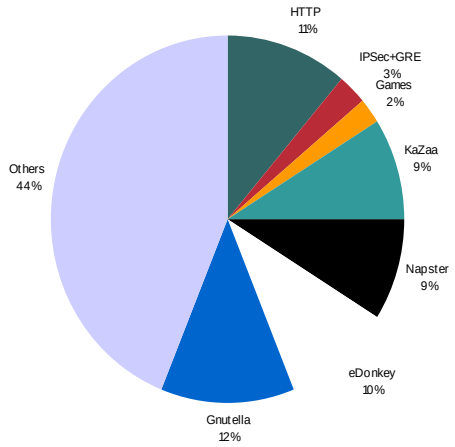
- Every message has a unique message ID
- Every servent maintains a table ID/TCP connection
- Packets with unknown message ID are flooded
- Exactly like an Ethernet switch MAC/port table !



Sending message ID 123

© 2003, Cisco Systems, Inc. All rights reserved.

Protocol Utilization on the Internet



OK, OK…are there any solutions here?

P2P = 40%

Peering traffic data collected 9th of July 2002 in a large European ISP

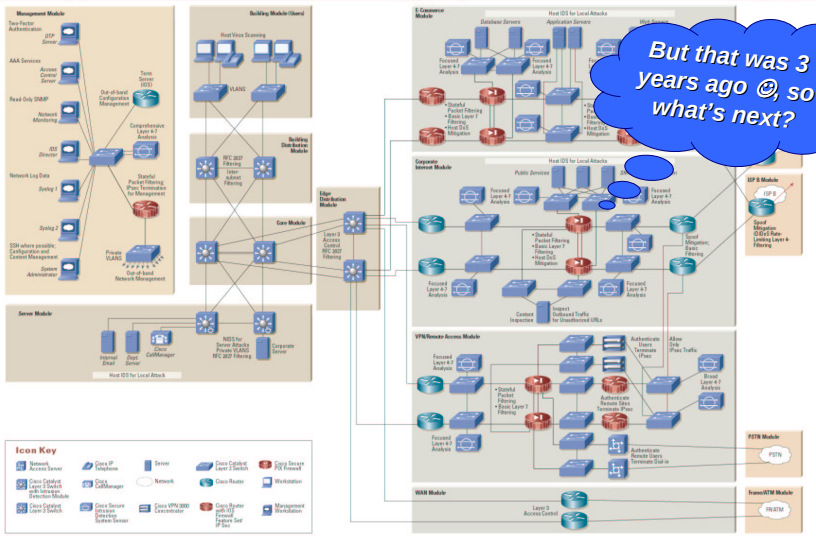
© 2003, Cisco Systems, Inc. All rights reserved.

Solutions?

The **SAFE Blueprint** for **Secure** E-Business

SAFE protects Cisco **AVVID** (Architecture for Voice, Video and Integrated Data) networks with strategically placed security technologies that mitigate threats throughout the enterprise.

cisco.com/go/safe | cisco.com/go/security | cisco.com/go/evpn



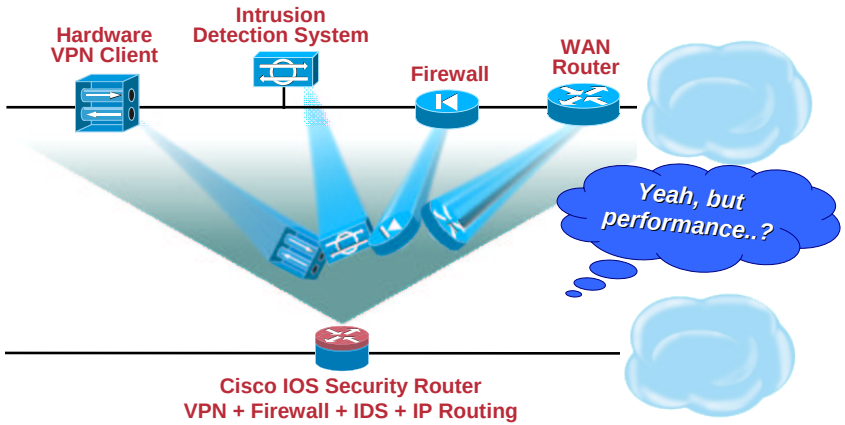
But that was 3 years ago ☺, so what's next?

© 2003, Cisco Systems, Inc. All rights reserved.

Convergence of embedded Security Functions

Cisco.com

- IPsec VPN, Inline Stateful Firewall, IDS, and IP Routing
- Eases management burden, reduces cost of ownership



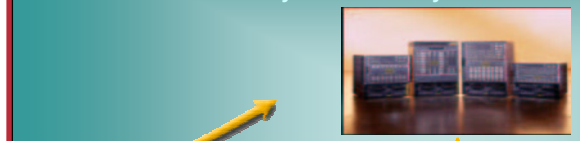
© 2003, Cisco Systems, Inc. All rights reserved.

Catalyst 6500 Switch Security

Advanced Network and Security Integration

So far so good, but what about the desktops ?!?

- Security Integration with Layer 2 Switching Services
- Multiple Security Services Integrated in a Switch
- Fastest Firewall and VPN in the Industry
- Greatest Interface Density in the Industry

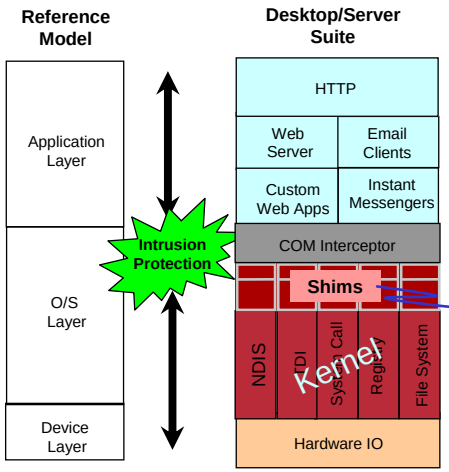


© 2003, Cisco Systems, Inc. All rights reserved.

Where to stop Worms?

Cisco Security Agent

So this is here now, ...any future things?



CSA Hybrid Approach :

- Host Intrusion Protection
- Distributed Firewall
- OS Hardening
- Malicious Code Sandbox
- Buffer Overflow Protection
- Web Server Protection
- Instant Messenger security

Architectural Features:

- Comprehensive *Kernel Shims*
- Low Computational Overhead
- *Virtual Bus* that can be extended to other applications

© 2003, Cisco Systems, Inc. All rights reserved.

Network, Hosts, and Policy are Symbiotic

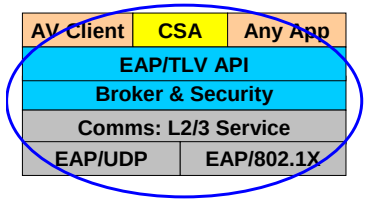
Antivirus is just the beginning... of a Network Admi

Is this a revolution?

Network Associates — YOUR NETWORK. OUR BUSINESS.

symantec.

TREND MICRO



Cisco Trust Agent

- **Initial focus on AV**
  - Extensible model for host to network validation
  - Ensuring host OS patch and AV policy compliance
  - Built with Antivirus co-sponsors NAI, Symantec, TrendMicro
  - Support Microsoft Windows NT, XP, 2000
  - Use Cisco Trust Agent for comms, brokerage, and security
  - To be distributed by Cisco and partners, potentially bundled with AV solutions
- **Expand to include other apps & policies**
  - Security software: Personal firewall, HIPS
  - Application software: MS Office
  - Policies: no Kazaa

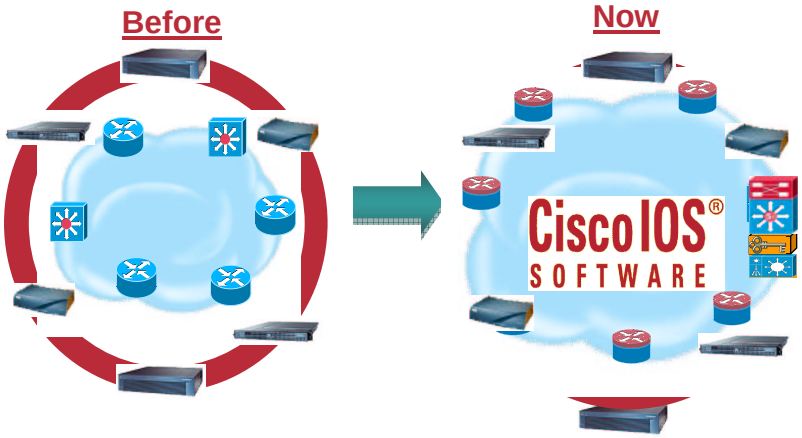
© 2003, Cisco Systems, Inc. All rights reserved.

Evolution of Network Security

Layers…? Vision?

Cisco.com

Additional Layers of Defense within the Network



Increasing role of Security-Integrated Network devices

© 2003, Cisco Systems, Inc. All rights reserved.

Cisco's Security Vision

Is that it?

Cisco.com

Cisco's Security Vision

What happened to good old layered approach?

Cisco.com

SELF-DEFENDING NETWORK

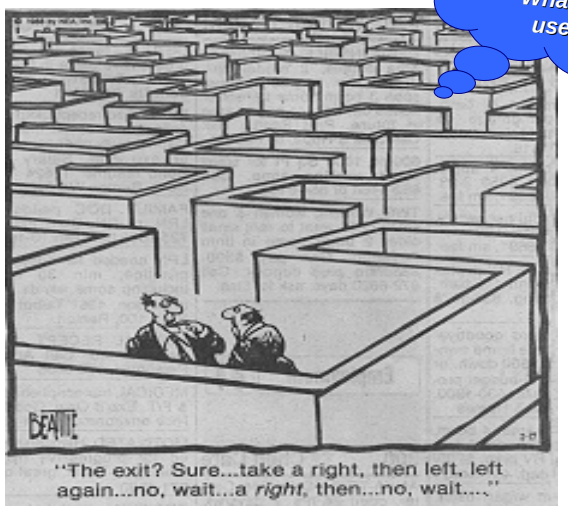
Multi-phased initiative to dramatically improve the network's ability to identify, prevent, and adapt to threats

INTEGRATED SECURITY	INDUSTRY COLLABORATION	SYSTEM LEVEL SOLUTION
Secure Connectivity Threat Defense Trust and Identity	Network Admission Control Program	Dynamically identify, prevent, and respond to threats End-to-End

© 2003, Cisco Systems, Inc. All rights reserved.

Good Security is a Layered A

Did we forget something…?
***
What about users?!?



© 2003, Cisco Systems, Inc. All rights reserved.

Well, we are all just …hu

Hope you had fun... That was the goal isn't it ☺?

"Only two things are infinite, the universe and a human stupidity, and I'm not sure about the former."

Albert Einstein

"If you think technology can solve your security problems, than you don't understand the problems and you don't understand the technology."

Bruce Schneier, Secrets & Lies - Digital Security in a Networked World

"…the human factor is truly security's weakest link."

Kevin D. Mitnick, The Art of Deception

Thank you!

Cisco.com

No more questions? ☹

BoF Security: What's next?

Franjo Majstor, fmajstor@cisco.com
Eric Marin, emarin@cisco.com
Thierry Van Herwijnen, therwijn@cisco.com
Marco Misitano, misi@cisco.com
Kevin Regan, kregan@cisco.com
Peter Provart, pprovart@cisco.com
Erik Lenten, elenten@cisco.com

Ah, Yes ☺ evaluations?

NETWORKERS 2003
THE POWER TO TRANSFORM BUSINESS. now.

Please Complete Your Evaluation Form

Session BOF- 8002

BoF: Security: What's next?

Cisco Systems

© 2003, Cisco Systems, Inc. All rights reserved.

Cisco Systems