Virus Control and Patch Management:
Balancing Protection and Resources

COMDEX Scandinavia 2004
January 20th 2004
Göteborg, Sweden

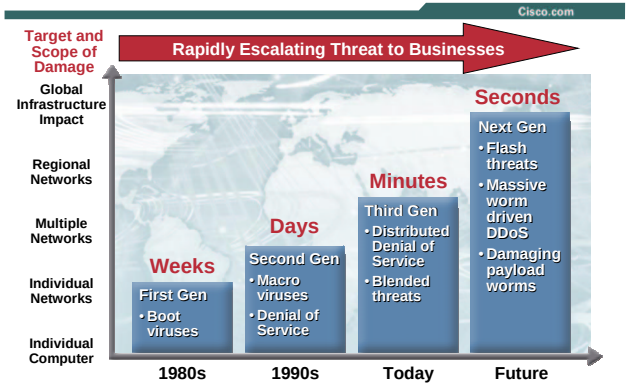
Franjo Majstor
EMEA Consulting Engineer
Cisco Systems, Inc.

Agenda

- Introduction
- Traditional Prevention Mechanisms
- Innovative approach
- Summary
- Q&A

Introduction

Threat Levels Evolution



The Sapphire Worm or "Slammer"

Problem Statement

- VU#980449 – Automatic Execution of Embedded MIME Types
  - Sep 2001 – Nimda worm
  - Nov 2001 – W32/Badtrans
  - Apr 2002 – W32/Klez
  - Jul 2002 – W32/Frethem
  - Oct 2002 – W32/Bugbear

  Patch available in April 2001
- VU#952336 – Buffer Overflow in IIS Indexing Service
  - Jul 2001 – Code Red

  Patch available in June 2001
- VU#484891 – Buffer Overflow in SQL Server Stack Buffer
  - Jan 2003 – SQLSlammer
    W32.Slammer
    Sapphire worm

  Patch available in July 2002

Why is it the problem?

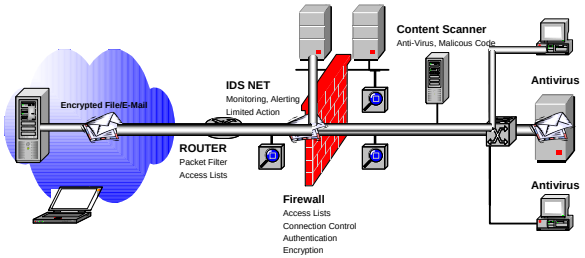
4129 vulnerabilities reported in 2002

- **To read the vulnerability description:**
  4129 x 20 min. to read *= 172 days in reading!*
- **Suppose 10% pertain to your environment:**
  413 vuls x 1 hour to install *= 51 days to install patches (per machine!)*
- **Just to read security news and patch a single system:**
  172+ 51 = 223 days (52 X 5 = 260 !!)

Even a 1% "hit rate" and 5 minutes to read new bulletins will cost almost 45 days, or about 20% of a perfectly efficient administrator.

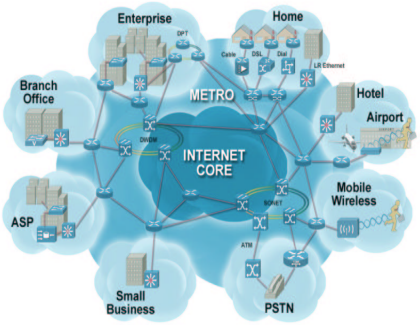
Traditional Prevention Mechanisms

Traditional Security Concepts



Networks of the today

Cisco.com



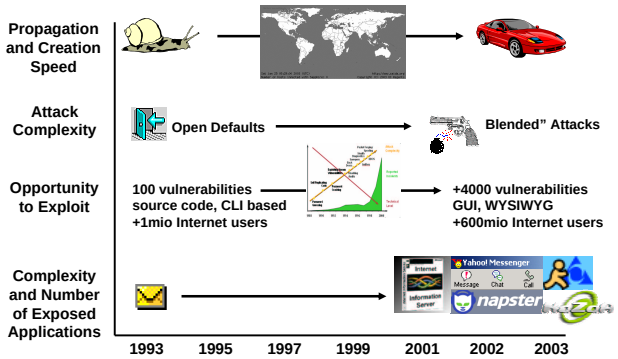
Characteristics

- Distributed Internet connections
- Need to open up data centers for more ubiquitous access
- Dramatic increase in employee mobility
- Increased use of new campus technologies like WLAN & IPT that provide more network access methods
- Growing damage due to viruses & worms

Evolution

…to fight against today's attacks?

Cisco.com



Emerging Speed of Network Attacks

Cisco.com

1980s-1990s
Usually had weeks or months to put defense in place.

2000-2002
Attacks progressed over hours, time to assess danger and impact. Time to implement defense.

2003-Future
Attacks progress on the timeline of seconds.

SQL Slammer Worm:
Doubled every 8.5 seconds
After 3 min : 55M scans/sec
1Gb Link is saturated after one minute

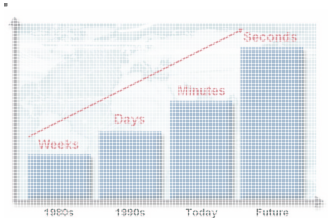
In 1/2 the time it took to read this slide, your network And all of your applications would have become unreachable!

SQL Slammer was a warning. Newer "Flash" worms are exponentially faster.

Threat Levels Escalating

Cisco.com

- Magnitude of infrastructure threats increasing
- Rapid worldwide propagation of attacks
- Current point product solutions can't keep up

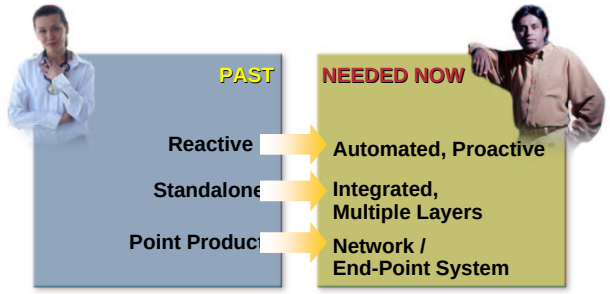


Cisco.com

Innovative Approach

Approach to Security Must Change

Cisco.com



A Collaborative Systems Approach

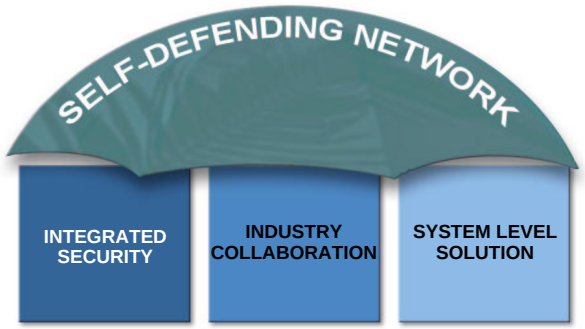
The Network as the Human Body

Cisco.com

- IT infrastructure (and network) needs to operate same as human body…
- Viruses… ever-present fact of life
  - We carry them with us
  - We pick them up from all sorts of contact
- Human body functions at high level even though we carry viruses and disease
- Self-Defending Network modeled around Autoimmune concept

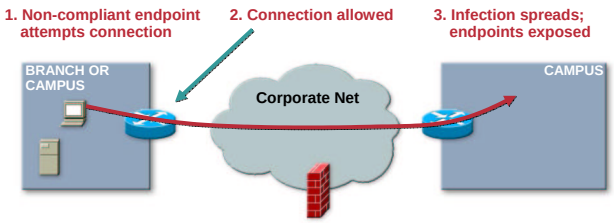
Self-Defending Network

Cisco.com

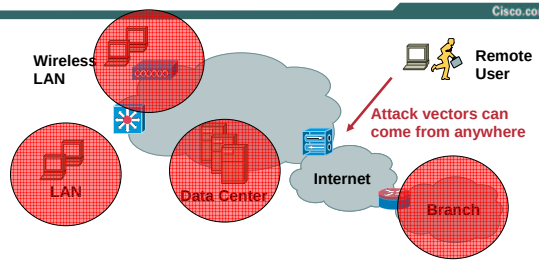


Network Admission Control

Cisco.com

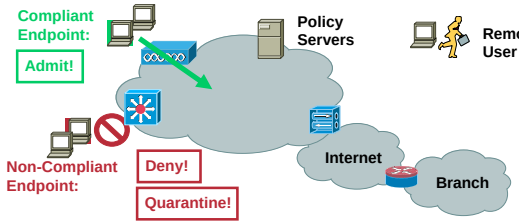


Internet Worm Infection



- Self propagating worms continue to disrupt business, causing downtime and continual patching
- Locating and isolating infected systems is time and resource intensive
- Multiple types of users, access methods, and endpoints compound the problem

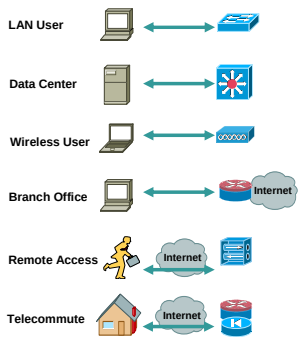
Ideal Solution: An Integrated System



- Multiple components are required for a complete solution
  - Endpoint Security solutions knows security condition: type/compliance/etc
  - Policy Servers know compliance/access rules
  - Network access devices (routers, switches) enforce admission policy
- Virus/worm prevention and containment requires industry collaboration

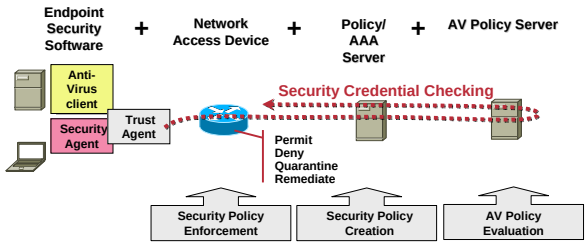
Network Access Devices

Ubiquitous, Quarantine services, Transparency



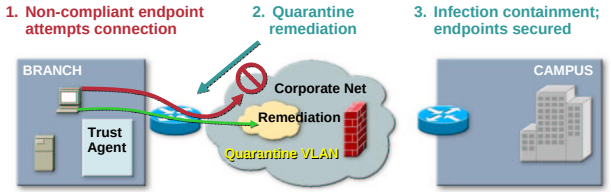
- Ensure hosts comply to corporate policy (such as AV policy) before they can pass traffic to the network
  - Prevent attacks that start as soon as the device connects
  - Enforce on the network access device - no reliance on the host
  - Similar to 802.1x/AAA services
  - Isolate/quarantine hosts prior to access (L3/4 ACLs & L2 VLANS)
- Ensure all ways into and out of the network are covered
  - Cover wired, wireless, L3 gateways, dial-in, and IPsec remote access
  - Provide a consistent approach for all methods

Network Admission Control Elements



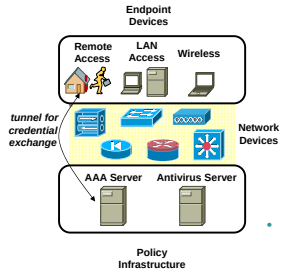
Based on endpoint security posture, appropriate admission policy will be enforced in the network

Network Admission Control at work



Policy Validation Layers

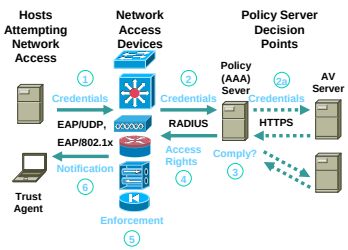
Flexible credentials, Multi-vendor, Trust model, Scalability



- Endpoint device credentials evaluated by policy infrastructure
  - Network provides transport and enforcement service
  - Extensible model, seamless to network devices
  - Ensure security through authentication of credential requestor and encrypting the information
  - Allow policy servers to evaluate their client application credentials for compliance (e.g. AV policy server evaluates AV credentials
- Provide scalable environment
  - Centralize the AAA function
  - Provide 'exception' handling for non-responsive hosts (printers, old machines)

Network Admission Control Solution

NAC Solution: Leverage the network to intelligently enforce access privileges based on endpoint security posture



NAC Characteristics:

Ubiquitous solution for *all* connection methods
Validates *all* hosts
Leverages investments in network and AV solutions
Quarantine & remediation services
Scalability Deployment

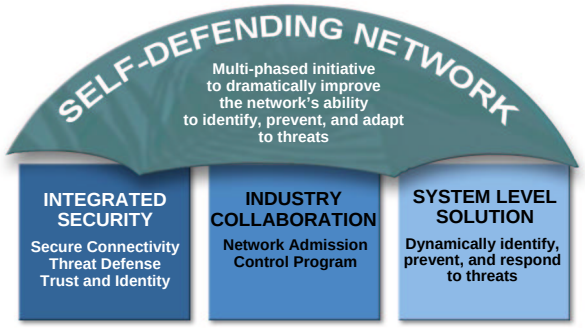
Network Admission Control Benefits

One Integrated System:

- Endpoint Security Solutions know security condition
- Policy Servers know compliance / access rules
- Network Access Devices enforce admission policy

Summary

Security Solution



Q and A

Cisco Systems

Virus Control and Patch Management:
Balancing Protection and Resources

Franjo Majstor
EMEA Consulting Engineer
Cisco Systems, Inc.

