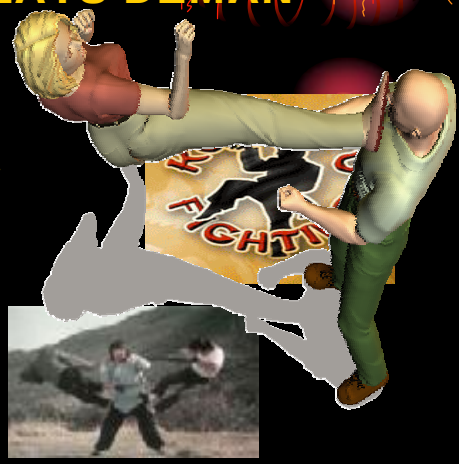
# SELF-DEFENDING NETWORK

- NETWORK THREATS DEMAN NEW SECURITY:
  - *STRATEGIES*
  - *TECHNOLOGIES*



## Self-Propagating Threats

- A combination of:
  - self–propagating threats
  - Collaborative applications
  - Interconnected environments
- Transformed security
- In to the stuff head line
- January 2003 ,The SQL slammer worm took down a sizable number of networks worldwide, and nearly felled Korea Telecom Freetel's network.
- Security has shifted from annoyance avoidance to a business-critical issue.
- Security products and services will grow 70 % between 2004 and 2007.

# Sizing Up the risk

- The number of security incident reported to the CERT Coordination Center , USA government-funded research and development center operated by Carnegie Mellon University rocketed from 9859 in 1999 to 114855 in 2003.
- Not only is the volume of threads rising so is damage potential.
- Most attack :
  - denial of service DOS
  - Trojan Horse
  - Worm
- A hacker coded sophisticated, malicious payloads into a worm, taking advantage of distributed computing power or peer-to-peer disk storage. By harnessing the true power of the network controlling tens of thousands of compromised hosts the hacker could do far more damage than the worms we 've seen.
- To defend the network need to be aware of the new nature of security threats:
  1. Shift from internal to external attacks Between 1999-2002 external attack rose 250 % according to CERT.
  2. Shorter windows to react: When attacks homed in one individual computers or networks, companies had more time to understand the threat. Now that viruses can propagate worldwide in 10 minutes. Antivirus solutions are still essential but are not enough, by the time the signature has been identified it is too late.
  3. *With self-propagation companies need network technology that can autonomously take action against threats.*

4. More difficult threat detection : They attack the application or embed the attack in the data itself which makes detection more difficult. An attack at the network layer can be detected by looking at the header information. But an attack embedded in a text file or attachment can only be detected by looking at the actual payload of the packet-something a typical firewall doesn't do.
5. A lower bar for hackers, A proliferation of easy-to-use hackers tools and scripts has made hacking available to the less technically-literate.

## Toward the self-Defendign Network

- Security threads have shifted from individual networks to the infrastructure
- The need to evolve from providing point security solution to integrated systems.
- This integrated system defend the network from several positions.
  - Firewall
  - IDS
  - Behavioral anomaly software which employs sophisticated mathematical algorithms to jude what is “normal” network activity and what is anomalous and therefore a potential threat.
- This three pronged approach to the physical security measures used at a bank.
  - *The filewall* is the guard standing outside the bank.
  - *IDS* is a 24x7 video monitoring system.
  - *Behavioral anomaly* software is someone standing outside the vault who is alert for suspicious behavior and prepared to take immediate action.
  - *Identity management* is analogous to asking customers for a photo ID or to enter a personal identification number (PIN) before receiving bank services.

With a variety of ways to detect and prevent attacks, the organization strengthens its defenses.

- A broad range of effective security technology is readily available a significant number of companies don’t take advantage of it.
- No matter how bad attack become.
- The invest in an IDS conduct vulnerability assessments hire and train people to monitor the network and take other action. What restrains them is the complexity
- If the network becomes self-defending that is it blocks attacks effectively and doesn’t require highly trained security professionals
- The equation changes and they ‘ll make the investment.

## Cisco solution self-defending Network

- Network Admission Control (NAC). Tackles trust and identity management which is username and password.
- The cisco Trust agent which is integrated into the Cisco Security agent collect security state information from PCs and hosts such as the version of antivirus software and operating system patches.
- When the node attempts to connect to the VPN the cisco Trust Agent transmits the security state information to Cisco network access devices such as routers, switches, wireless access points and security application which enforce admission control, These device relay the security credentials to the Cisco secure access control server (ACS) which makes the decision to permit , deny , quarantine, or restrict based on customer-defined policy.
- Used IDS and behavior anomaly software with NAC becomes even more powerful.

## End-To-End Defense in Depth

- The best Defense ? A strong offense.
- The campus, the data center, full service branches and teleworkers have distinct security challenges.
- With strong defense in place many events can be detected and mitigated automatically.
- Security policies
- Security management : must incorporate tools that can digest the massive amount of data generated by multiple security devices on the network and provide uniform configurations and changes to device in a timely manner.

## Campus Network

- The Campus network is not homogeneous.
- It is divided into several security modules:
  - Some facing outward to public networks and customers
  - The rest serving internal corporate users.
- Most organizations are alert for extern threats such as worm, viruses and DDOS attack, but internal hackers can do far more damage.
- They are harder to detect.
- This occurs when the network is crunchy on the outside and soft in the middle.
- An emerging campus security threat is grabbing, listening to, and spoofing voice over IP (VoIP) traffic.

## Defense-in-depth security strategy for Campus network

- Threat defense
  - Firewall, IDS
- Trust and identity management
  - Access control server
- Secure connectivity :
  - (VPN)
- Deploy behavior-based host Intrusion Prevention System (IPS) software in addition to signature-based solutions for day-zero worm attack.
- Disallow outbound session initiation from web servers to prevent virus and worm propagation.
- Define unique hostnames and passwords for routers and switches change passwords periodically.
- Differentiate groups using filters and VLAN.
- Use an out-of-band management network and encrypt management traffic.
- Limit data flows with QoS to minimize the impact of the DDOS attacks.
- Configure Network-based Application Recognition (NBAR) to filter worms and unpermitted HTML traffic.
- User layer 2 security features such as Dynamic ARP Inspection (DIA) and DHCP snooping to prevent spoofing.
- Keep server operating system software up to date with the latest patches.
- Use 802.1X port-based authentication
- Close unused ports on all devices
- Expire user passwords after specified period
- Go beyond WEP when securing the wireless LAN.

## Defense-in-depth security strategy for The Data Center(DC)

- The Heart of the IT infrastructure is the data center.
  - Which houses the applications that keep organizations in business.
- DC has the highest density of business-critical resources including
  - Applications
  - Servers
  - Storage
  - Network
- The need to be protected
- Compartmentalize the data center into security "zones" and define polices for each one
  - Access rules
  - Rules for how zones interact
- Use of Network-based and host-based IPS that watches every servers, switch and router, for suspicious activity then configure IPS to automatically reconfigure firewalls to block packets from identified malicious soruces.
- Use IP SEC (VPN)

## Defense-in-depth security strategy for Full-Service Branch offices

- A logical extension fo the campus LAN
- But physical distances limit the ability of headquarters to protect the branch .
- Configure VPNs to prevent "back-door" hacker access to the campus network and data center.
- Where VoIP traffic traverse the WAN configure a voice- and video- enabled to VPN ($V^3PN$).
- Configure Access Control List (ACL)

## Defense-in-depth security strategy for Teleworkers

- Remote access service for home-based and mobile employees or teleworkers to increase productivity
- An issue with the traditional teleworking schemes is that teleworkers add significant uncertainly to an enterprise's security profile.
- They might connect directly to other networks such as the Internet pick up a Virus or worm and unknowingly transmit it to the enterprise network the next time they login.
- VPN solution.
- Enforce strict password rules.
- At headquarters deploy remote access gear behind the WAN edge router and firewall