The Crumbling Perimeter: Mobile Computing and Internal Security Issues

Farnam Jahanian
Arbor Networks and University of Michigan

IFIP Working Group 10.4
July 1-5, 2005

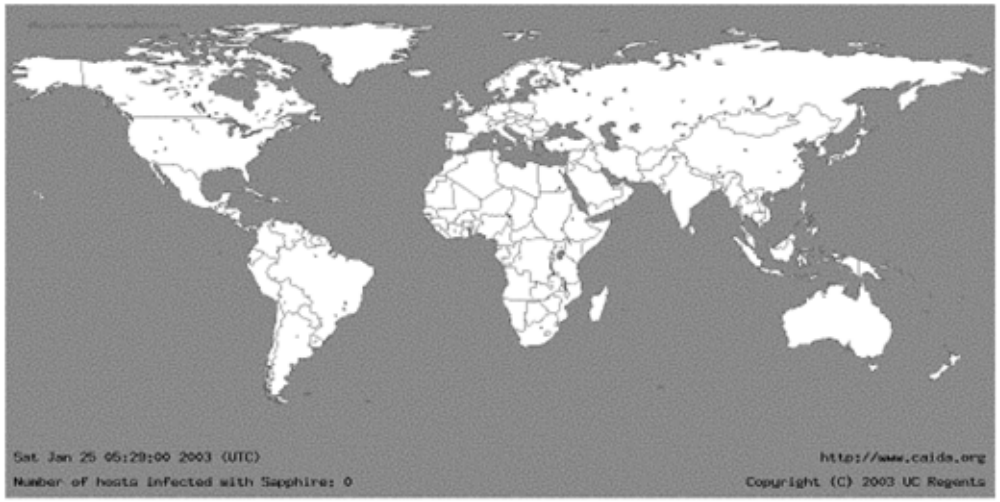
Trends in Internet Security Threats

- ***Globally scoped***, respecting no geographic or topological boundaries.
  - At peak, 5 Billion infection attempts per day during Nimda including significant numbers of sources from Korea, China, Germany, and the US. [Arbor Networks, Sep. 2001]

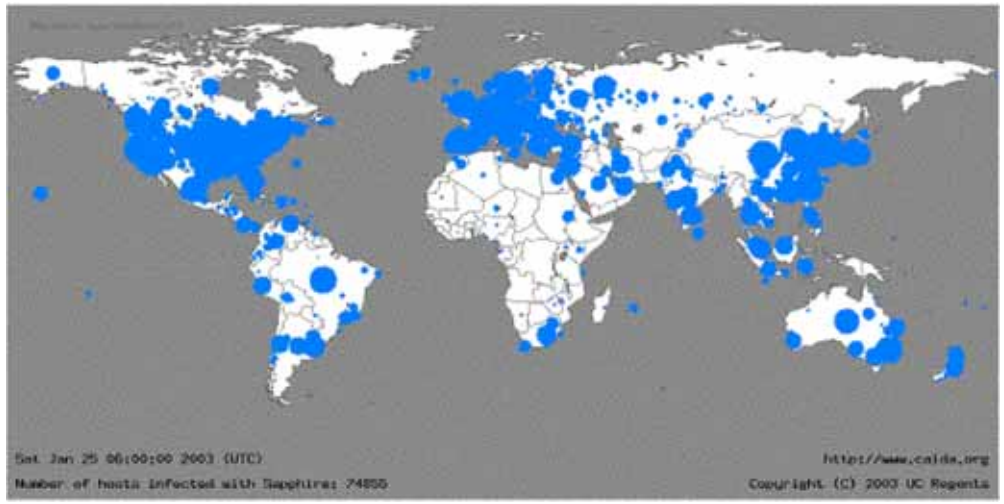
- Exceptionally ***virulent***, propagating to the entire vulnerable population in the Internet in a matter of minutes.
  - During Slammer, 75K hosts infected in 30 min. [Moore et al, NANOG February, 2003]

- ***Zero-day*** threats, exploiting vulnerabilities for which no signature or patch has been developed.
  - In Witty, "victims were compromised via their firewall software the day after a vulnerability in that software was publicized”

SQL Slammer Attack Propagation



0 hosts infected at the start



75,000 hosts infected in 30 min.

Infections doubled every 8.5 sec.

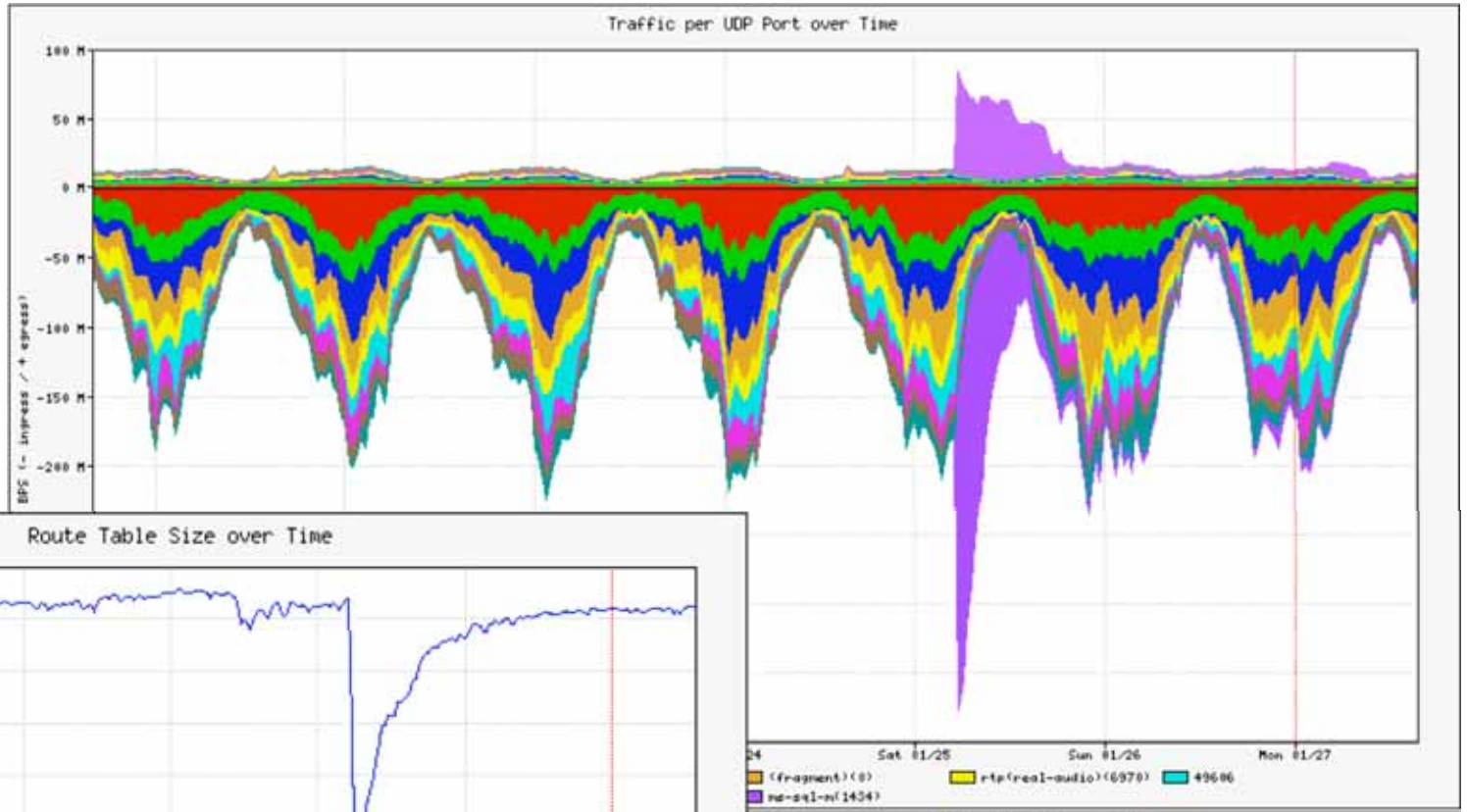
Spread 100X faster than Code Red

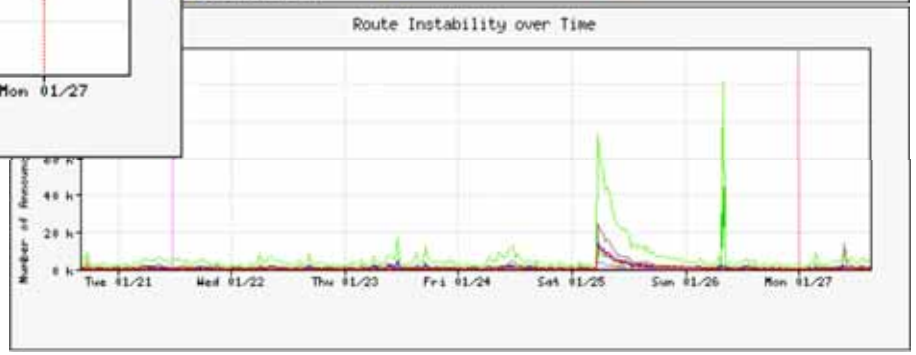
At peak, scanned 55M hosts per sec.

[Moore, Paxson, et al; NANOG February, 2003]

Impact of Slammer on the Internet

No DoS playload!



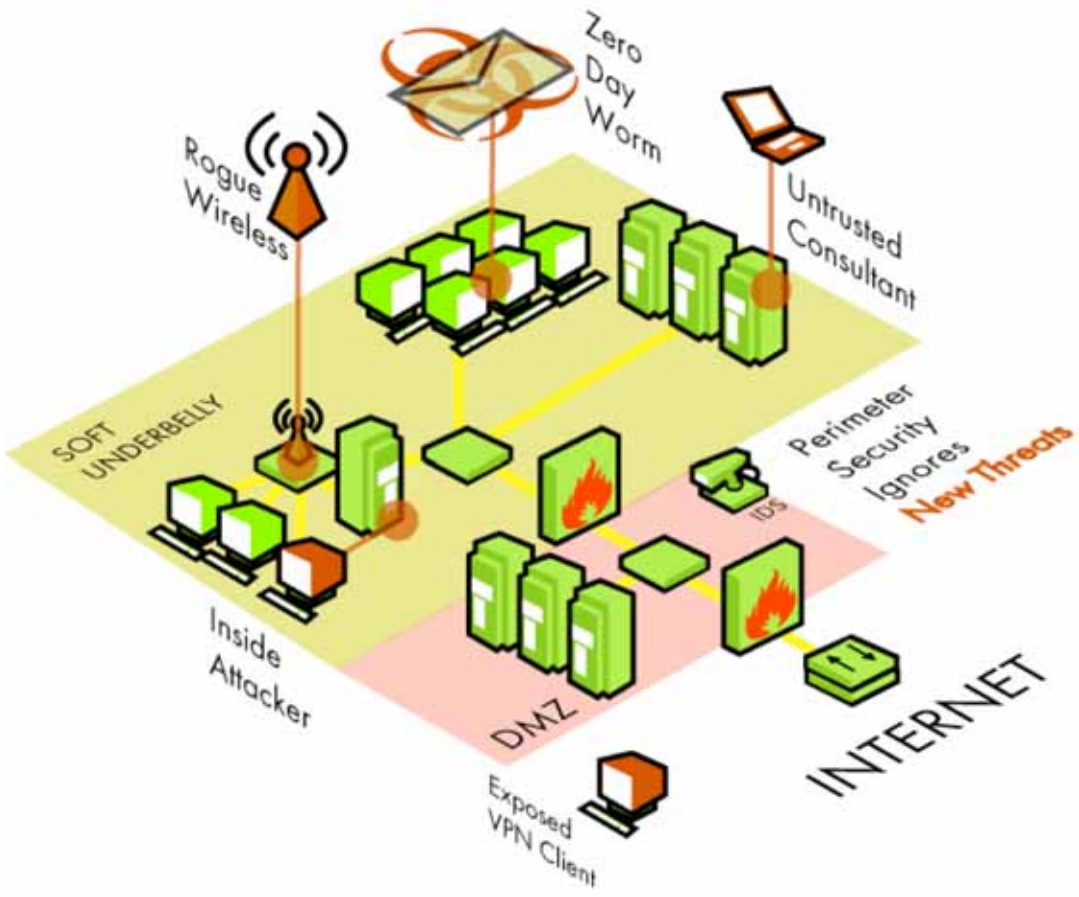


Loss of several thousand routes, mostly /24s

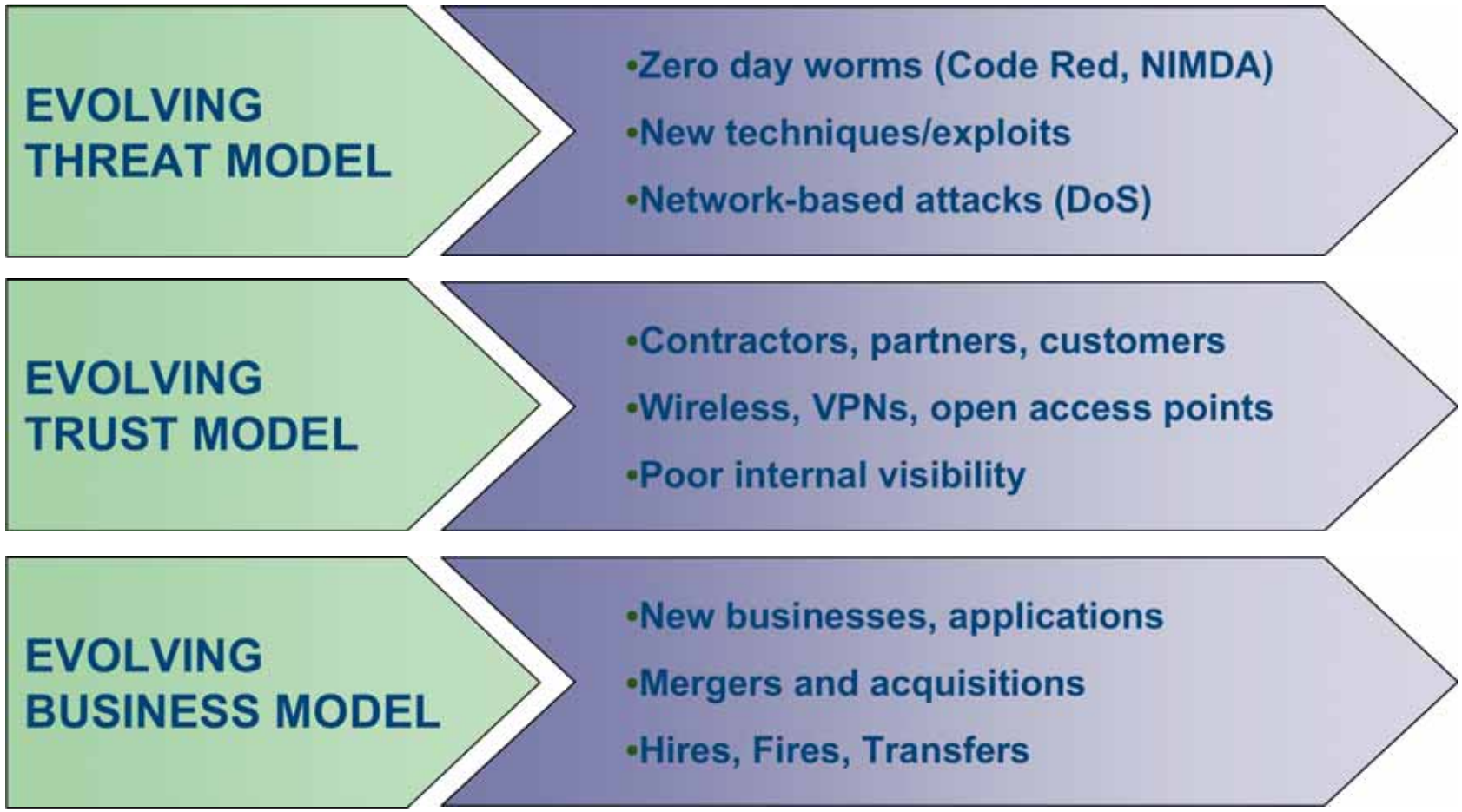
The Crumbling Perimeter

Much of perimeter security problem addressed by making perimeter vulnerability-aware (IDS, smart firewall, VA)

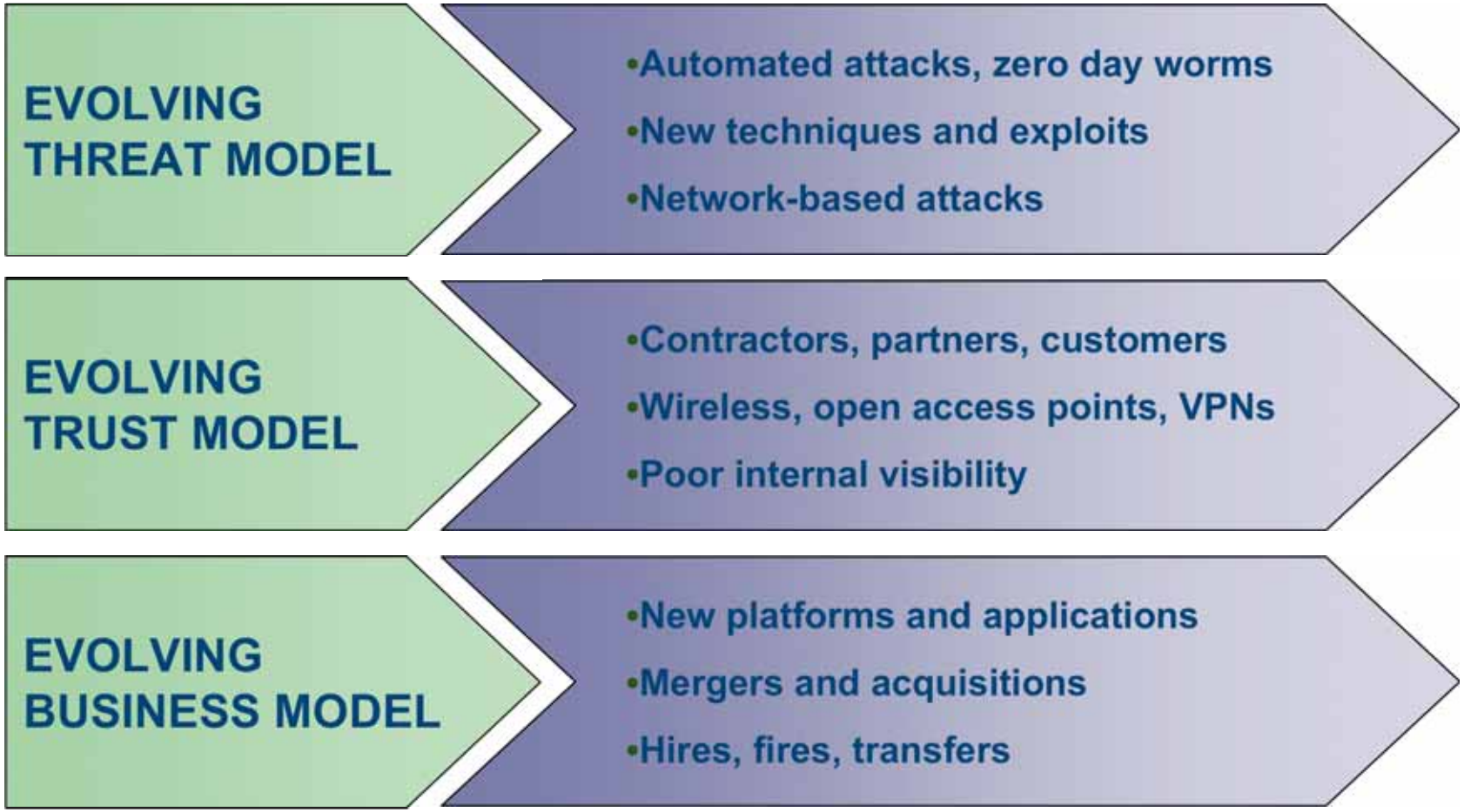
With crumbling perimeter (wireless, tunnels, etc) and near-zero visibility, internal network security has emerged as the most pressing IT security issue



Internal Security Challenge: The Soft Underbelly



Internal Security Challenge: The Soft Underbelly



Yesterday … Availability Attacks

A Dramatic Transformation and Escalation

Rise of the Botnets (Zombie Armies)

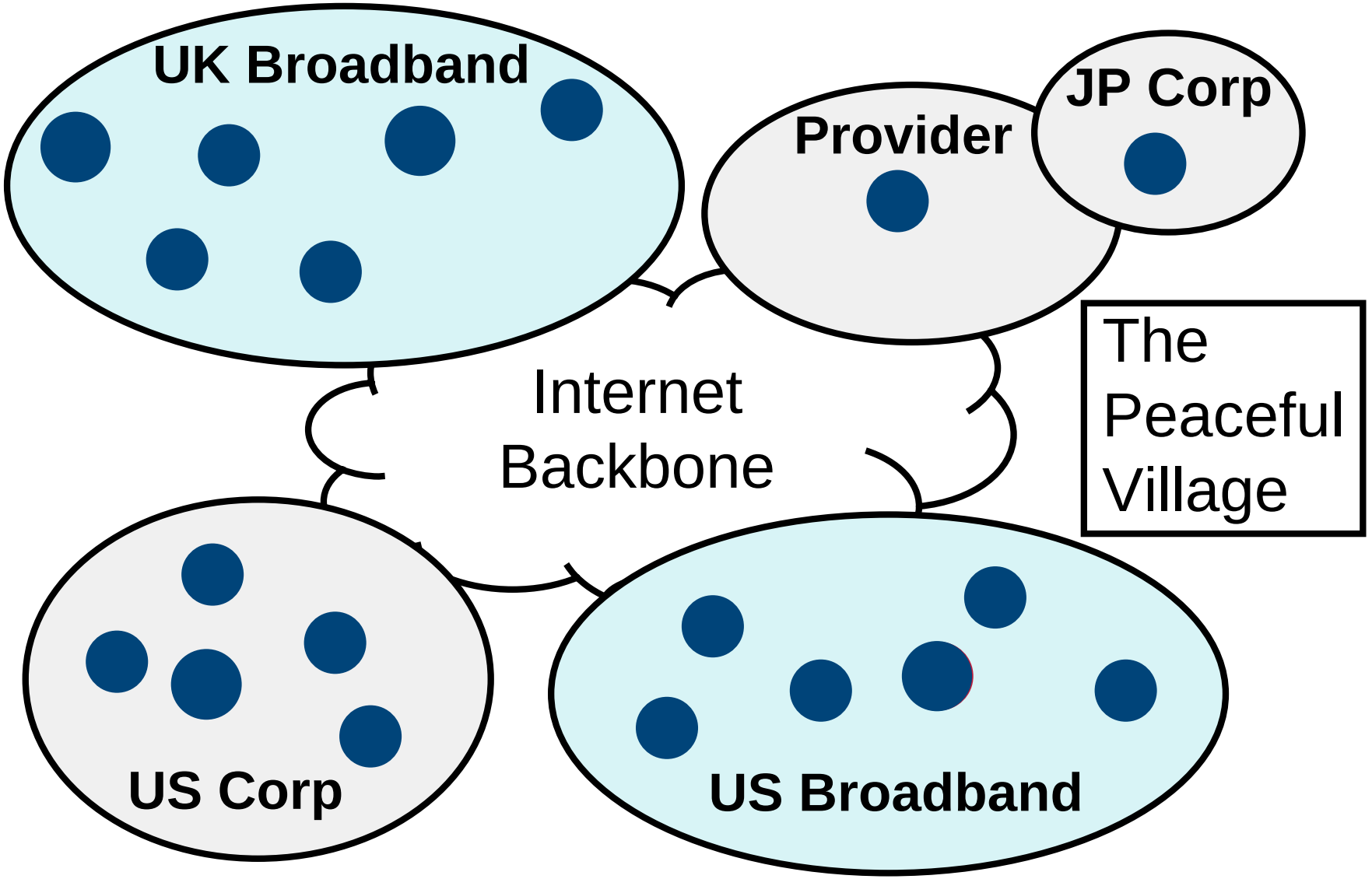
- 1000's of new bots each day [Symantec 2005]
- Over 900,000 infected bots as phishing attacks are growing at 28% per month [Anti-Phishing Working Group 2005]
- A single botnet comprised of more than 140,000 hosts was observed "in the wild" [CERT Advisory CA-2003-08, March 2003]

Attackers have learned a compromised system is more useful alive than dead!

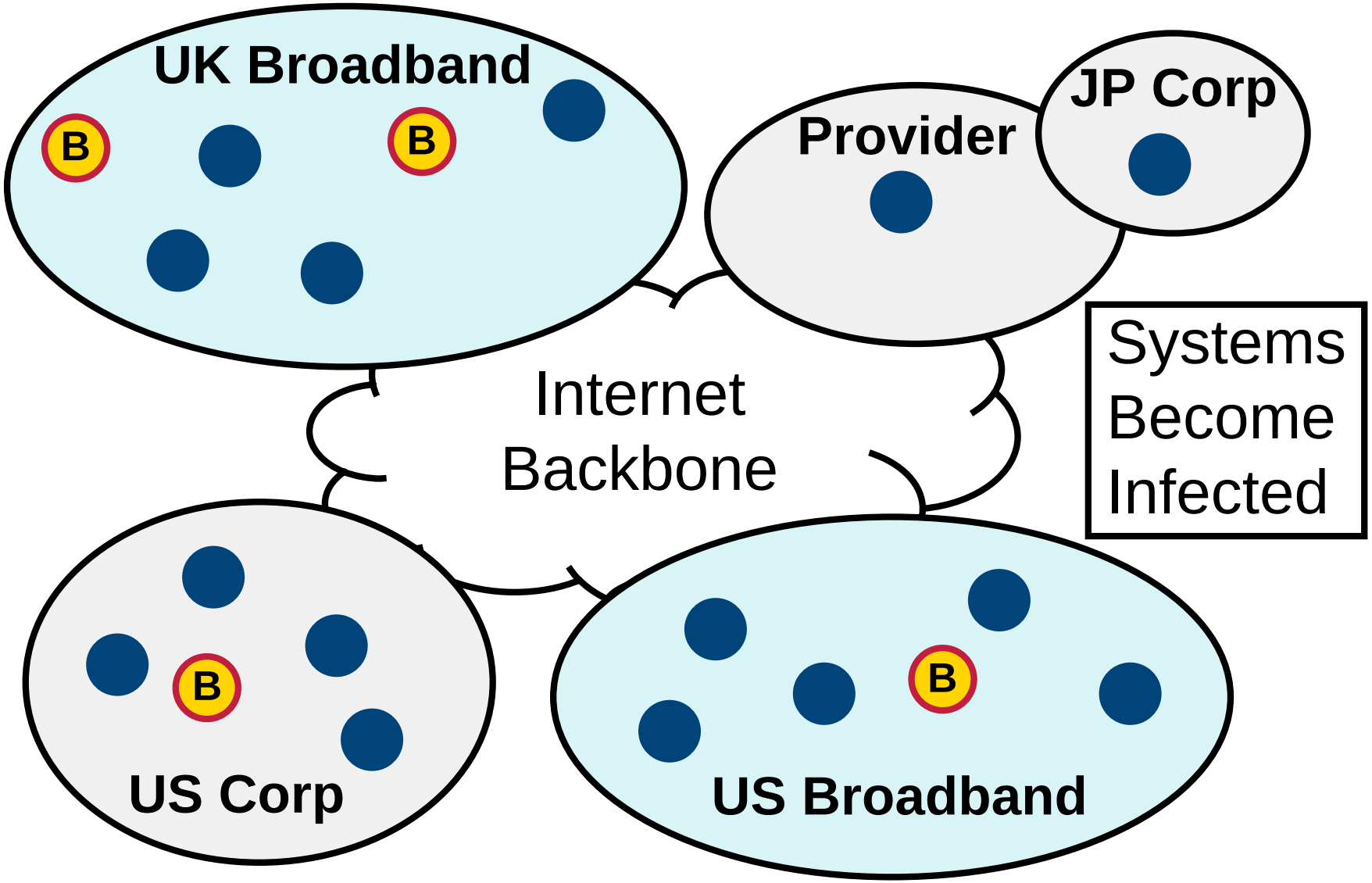
(*evasion/economics?*)

  - Significant more firepower: *Broadband (1Mbps Up) x 100s == OC3!!!*
- An entire economy is evolving around bot ownership
  - Sell and trade of bots ($0.10 for "generic bot", $40 or more for an "interesting bot; e.g., a .mil bot)
  - Bots are a commodity - no significant resource constraints

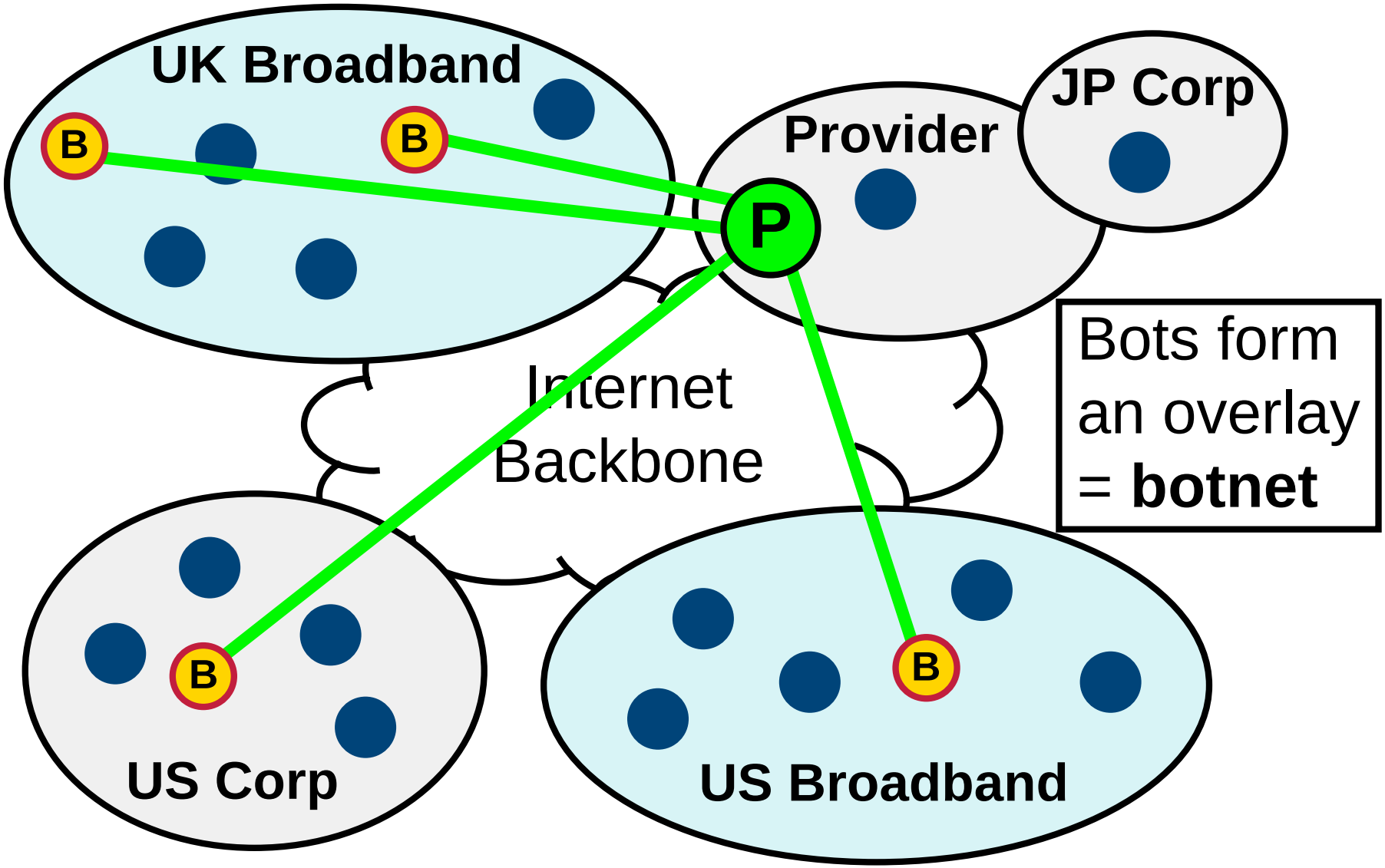
The Botnet


UK Broadband
Provider
JP Corp
Internet
Backbone
The
Peaceful
Village
US Corp
US Broadband

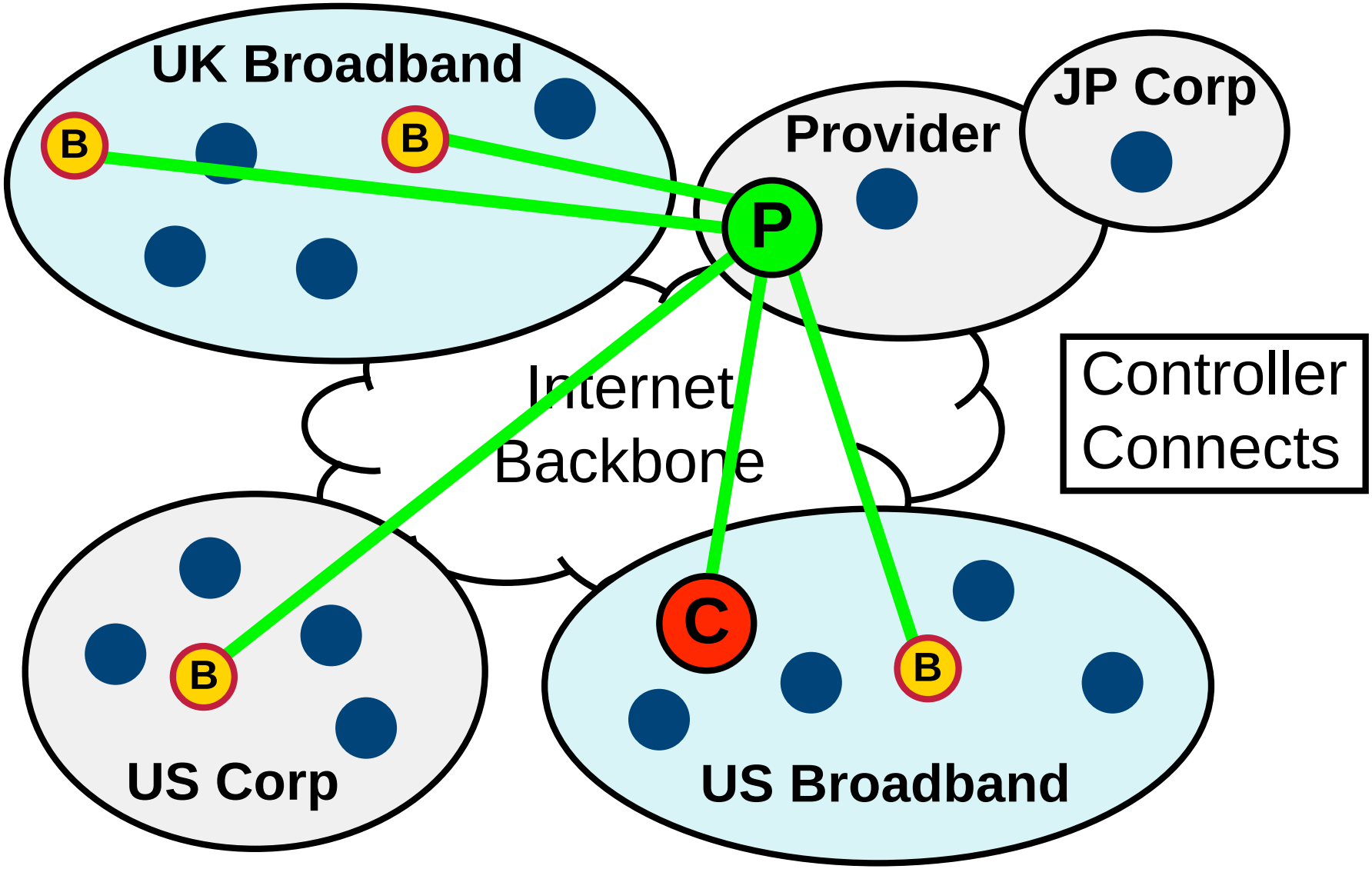
The Botnet


UK Broadband
B
B
Provider
JP Corp
Internet
Backbone
Systems
Become
Infected
B
US Corp
B
US Broadband

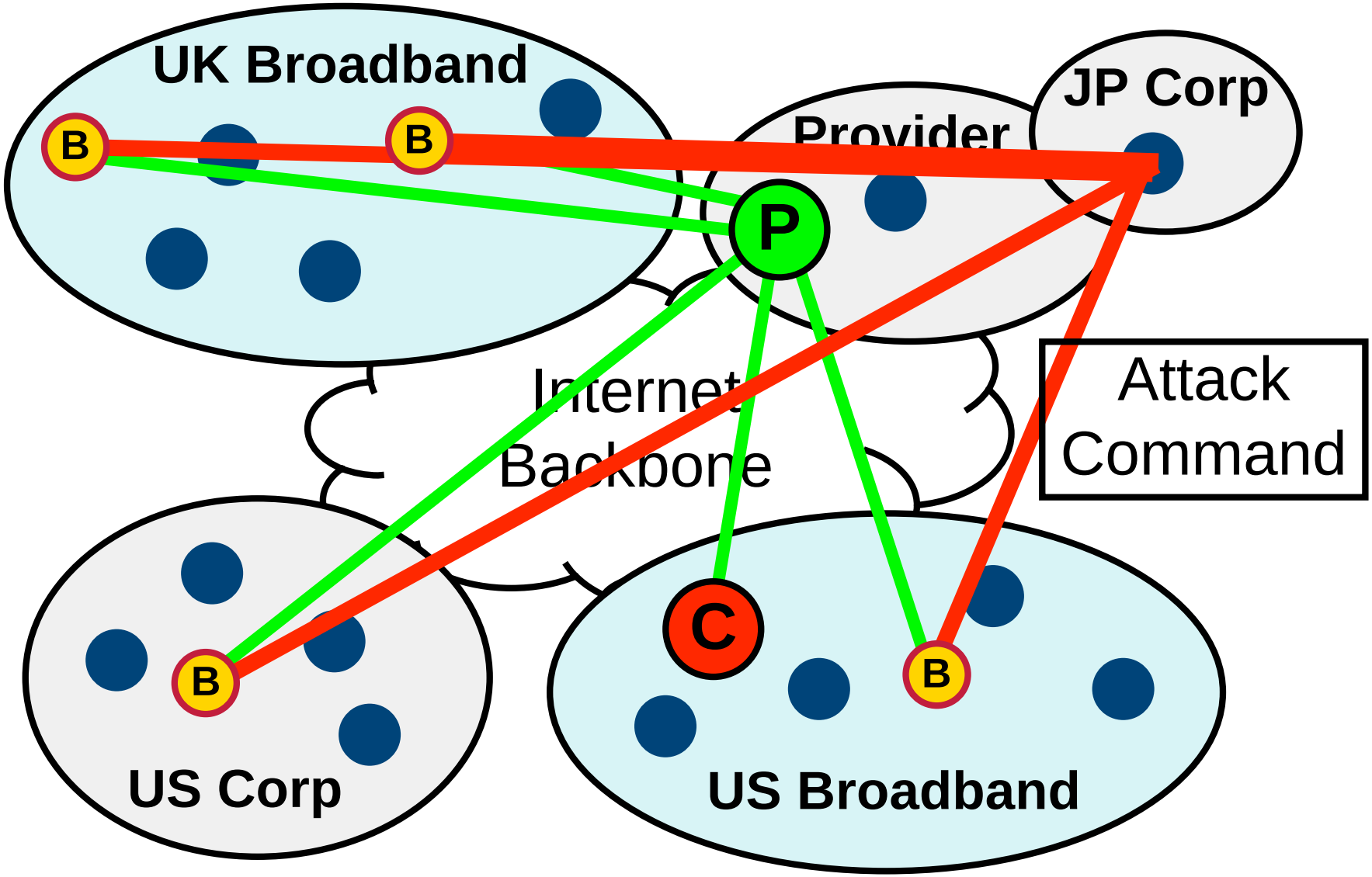
The Botnet


UK Broadband
B
B
Provider
P
JP Corp
Internet
Backbone
Bots form
an overlay
= botnet
B
US Corp
B
US Broadband

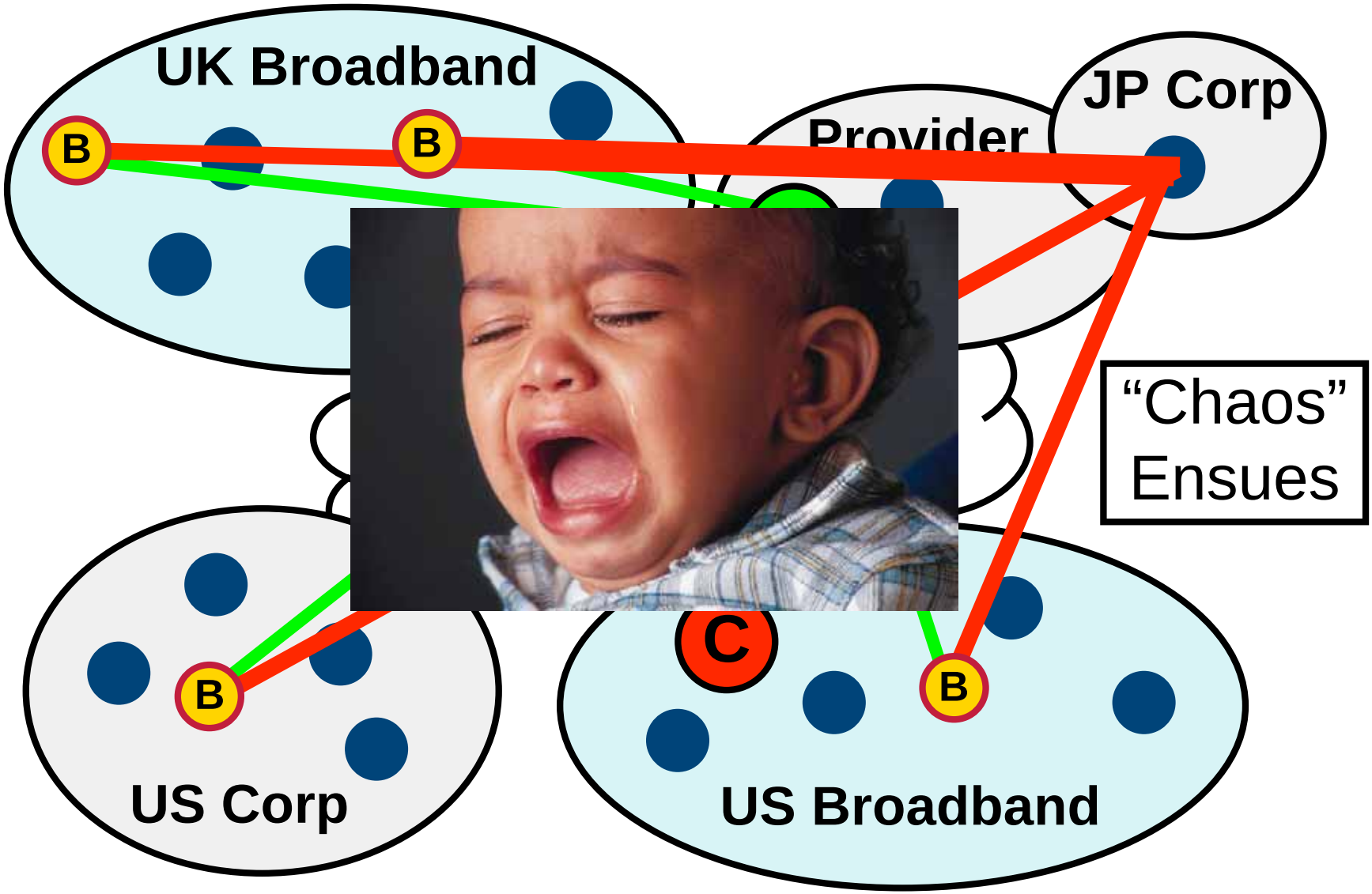
The Botnet


UK Broadband
B
B
Provider
P
JP Corp
Internet
Backbone
Controller
Connects
B
C
B
US Corp
US Broadband

The Botnet


UK Broadband
B
B
JP Corp
Provider
P
Internet
Backbone
Attack
Command
C
B
B
US Corp
US Broadband

The Botnet


UK Broadband
JP Corp
Provider
B
B
"Chaos"
Ensues
C
B
B
US Corp
US Broadband

Mobile Computing

Distinguishing Characteristics:

- Relatively resource-poor mobile elements
- Potential variability in network connectivity
- Constraints on power consumption and energy source
- Inherent vulnerability of mobile devices
- Increased tension between autonomy & interdependence: application-aware vs. application-transparent [Satyanarayanan et. al.]
- Not so subtle: wireless medium and node mobility

Impact on Security Design

- Stringent resource constraints (cpu, power) may lead to weaker protection
- Low-end devices can hardly perform computation-intensive tasks such as asymmetric cryptographic alg.
- Shared medium (wireless channel) is accessible to both legitimate users and malicious attackers
- Preservation of location discovery and privacy for mobile users

Note on perimeter defense and best practices!

Rethinking the Classic Client-Server Model

- Small set of trusted servers augmented by end-to end authentication and encrypted transmission
- Mobility may temporarily blur the distinction between client and server to achieve performance or availability
  - Sensitive data cached on client
  - Client emulating server functions when limited/no connectivity
  - Shipping client functions to resource-rich server

Mobile Ad Hoc Networks

Distinguishing Characteristics:

- Self-configuration and self-maintenance
- Open peer-to-peer architecture
- Lack of dedicated network (routing) infrastructure
- Routing and packet forwarding done by mobile nodes
- Lack of a centralized monitoring or management point
- Absence of a certification authority

Impact on Security Design

- No clear line of defense: boundary between inside and outside blurred
- No well-defined place for deploying security monitoring (IDS) or access control mechanisms (firewall)
- Internal security issue if a mobile node is compromised
- Potential disruption of routing substrate
- Highly dynamic topology with frequent joins and departures

Classification of Attacks

- Attacks on the wireless infrastructure
- Using wireless network to gain foothold into the wired network
  - Internal security attacks
  - Jumping-off point for launch attacks
- Attacks on mobile devices

Infrastructure Attacks

- Packet sniffing and “war driving”
  - Identifying SSID in Wi-Fi networks
  - Traffic analysis
  - Useful when combined with other data
- Rogue access points
- Jamming (causing interference to an 802.11 network)
- Attacks on routing and packet forward infrastructure

Attacks on Mobile Ad hoc Networks

- Link layer attacks:
  - Vulnerability of 802.11 WEP to several types of cryptographic attacks
    - WEPCrack and AirSnort
  - DoS attacks on channel contention and reservation schemes
  - Exploiting binary exponential backoff to deny access to the wireless channel from its local neighbors
  - Backoffs at link layer incurring chain reaction in upper layer protocols such as TCP

- Network layer attacks in mobile ad hoc networks:
  - Routing attacks: advertising routing updates that do not follow specification … disrupt protocol operation and poison routing state at other nodes
  - JellyFish attacks: target closed-loop flows responsive to delay or loss – i.e. target end-to-end congestion control of TCP
    - Packet reordering
    - Periodic dropping
    - Delay-variance attacks
    - Duplicating packets
  - Blackhole attacks: target open-loop flows by dropping all packets after correctly receiving them at MAC layer

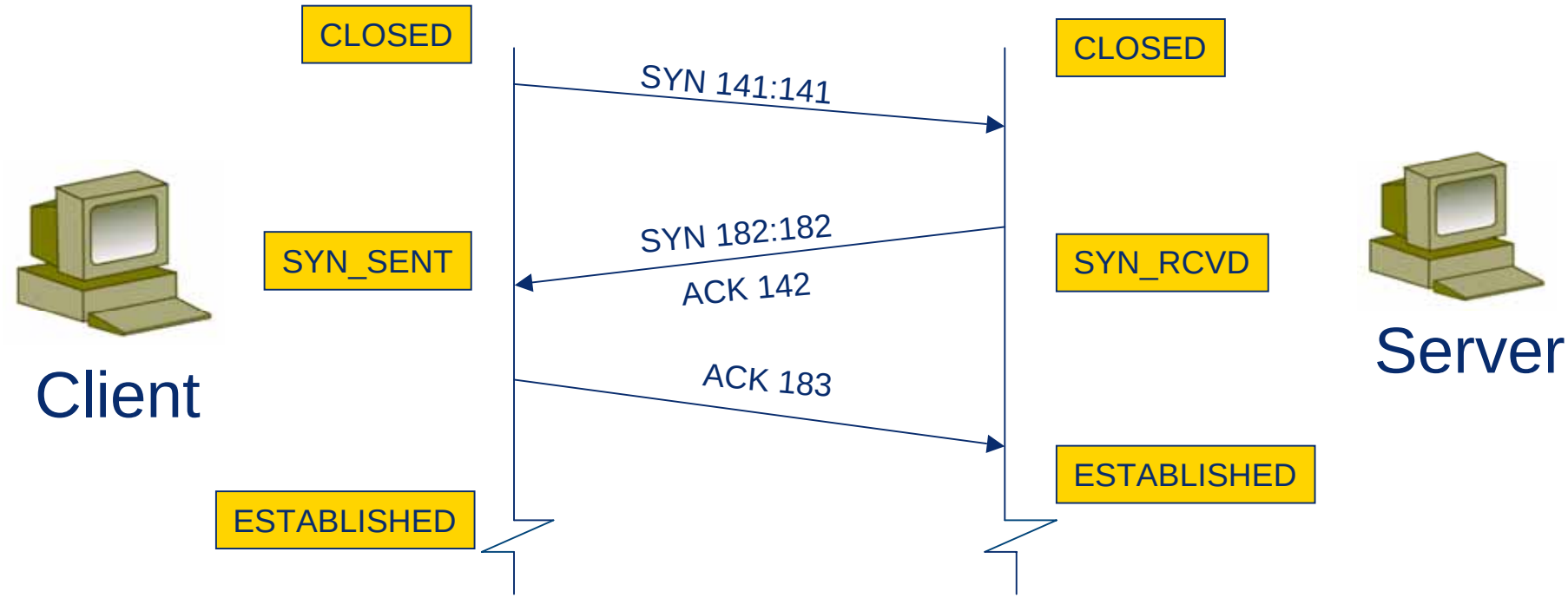
Classification of Attacks

- Snooping
  - Identifying SSID in Wi-Fi networks
  - Traffic analysis
  - Useful when combined with other data
- Man-in-the-middle attack
  - Replaying captured messages
- Bogus access points
- Attacks based on signal leakage

- Jumping-off point from which attacks are launched
- Attacks on keys in wireless networks:
  - Brute-force attacks
  - Dictionary attacks
  - Algorithmic attacks

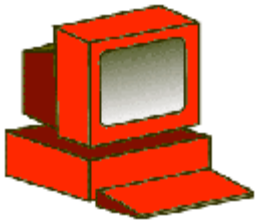
Denial-of-Service Attacks

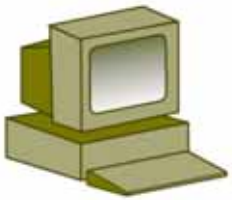
Example: TCP SYN Flood



Normal sequence for TCP connection establishment (3-way handshake)

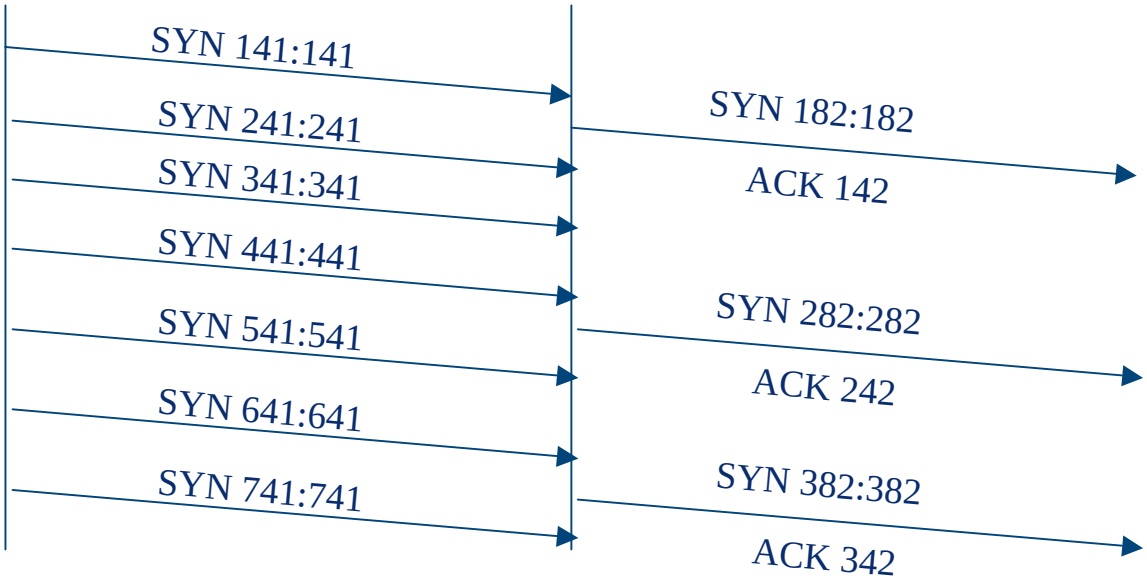
Example: TCP SYN Flood (cont.)



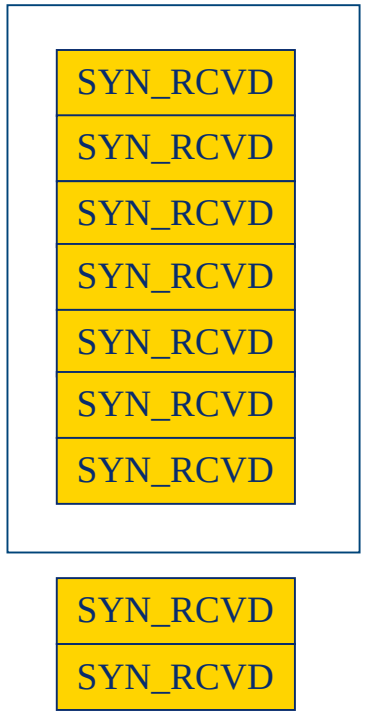


Attacker

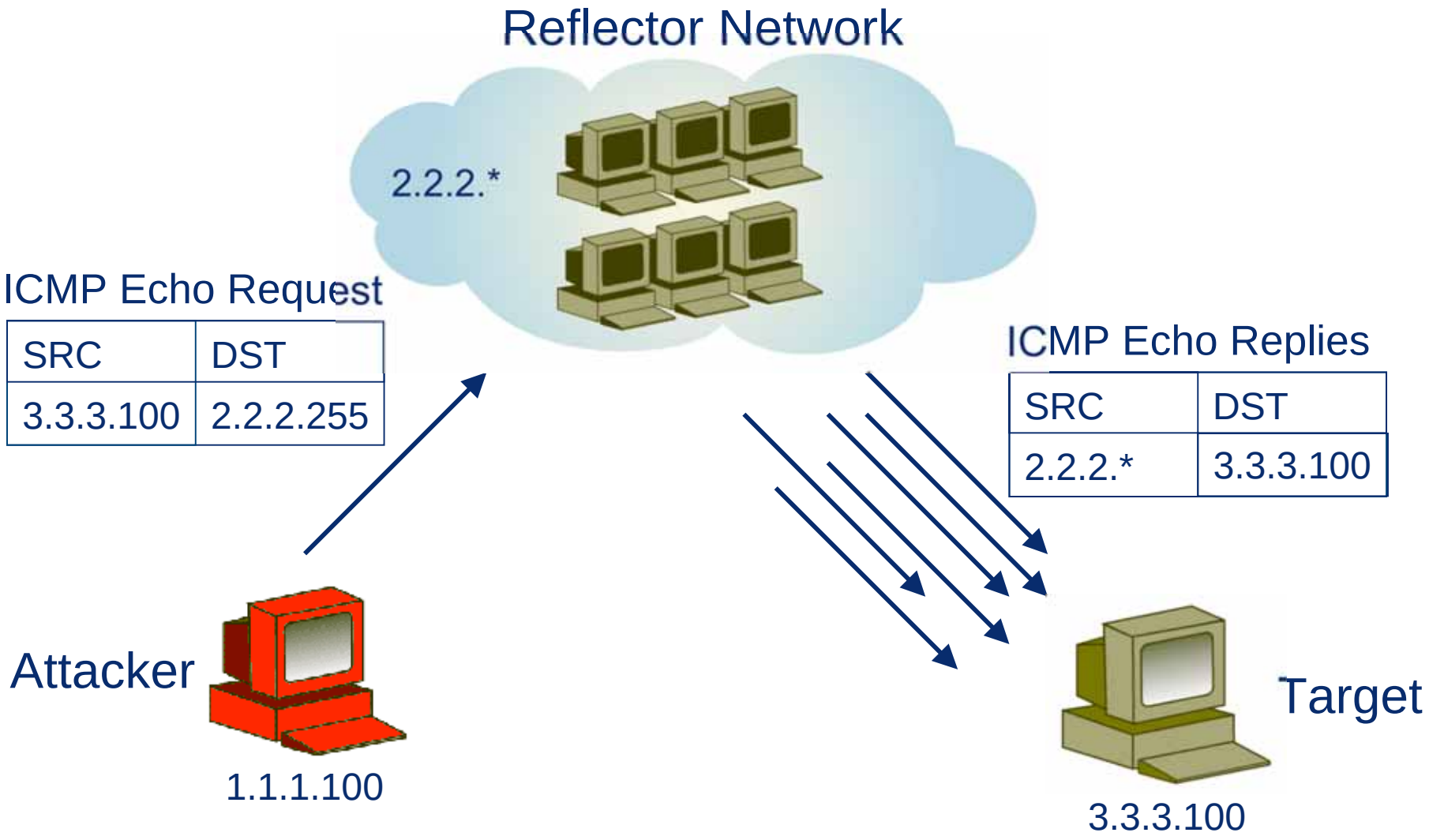
Server



Listen Queue



Example: Smurf Attack



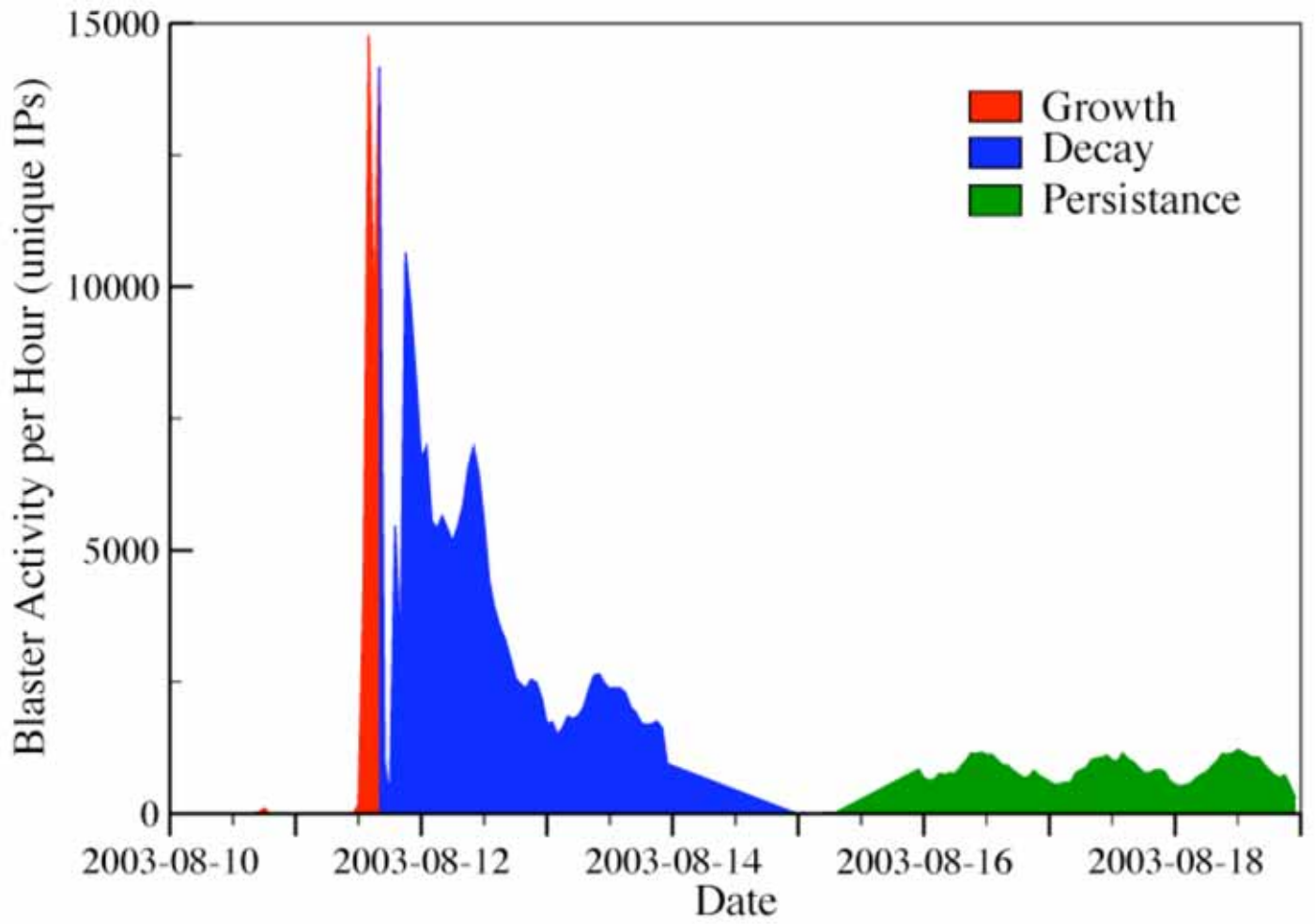
Denial-of-Service Attacks

- DoS attacks by gaining a foothold in the wired network
- DoS attacks using rouge wireless devices
- DoS attacks on wireless access points
- DoS attacks on services offered to mobile users
- DoS attacks by jamming frequency channels
- DoS attacks via network-layer packet blasting

Traffic analysis techniques employed by existing DDoS detection and mitigation solutions is not readily applicable to wireless networks with mobile nodes.

- What about malicious code, worms and viruses?
  - Implications for wireless networks and mobile devices

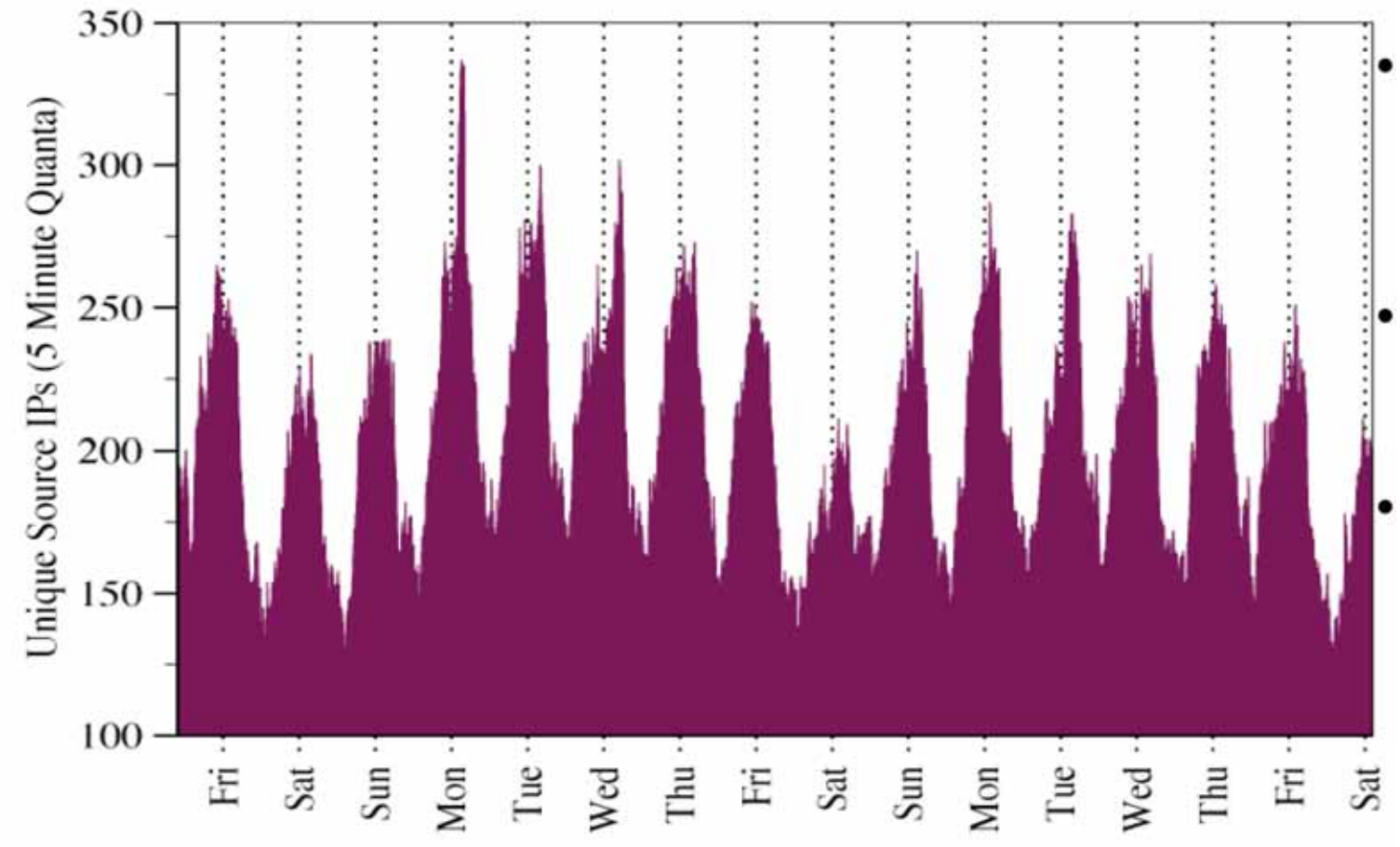
Internet Worms



- Blaster Worm released August 11, 2003
- IMS Observed 286,000 IPs
- Doubling every 2.3 hours
- 40,000 hosts/hour
- Half-life = 10.4 hours

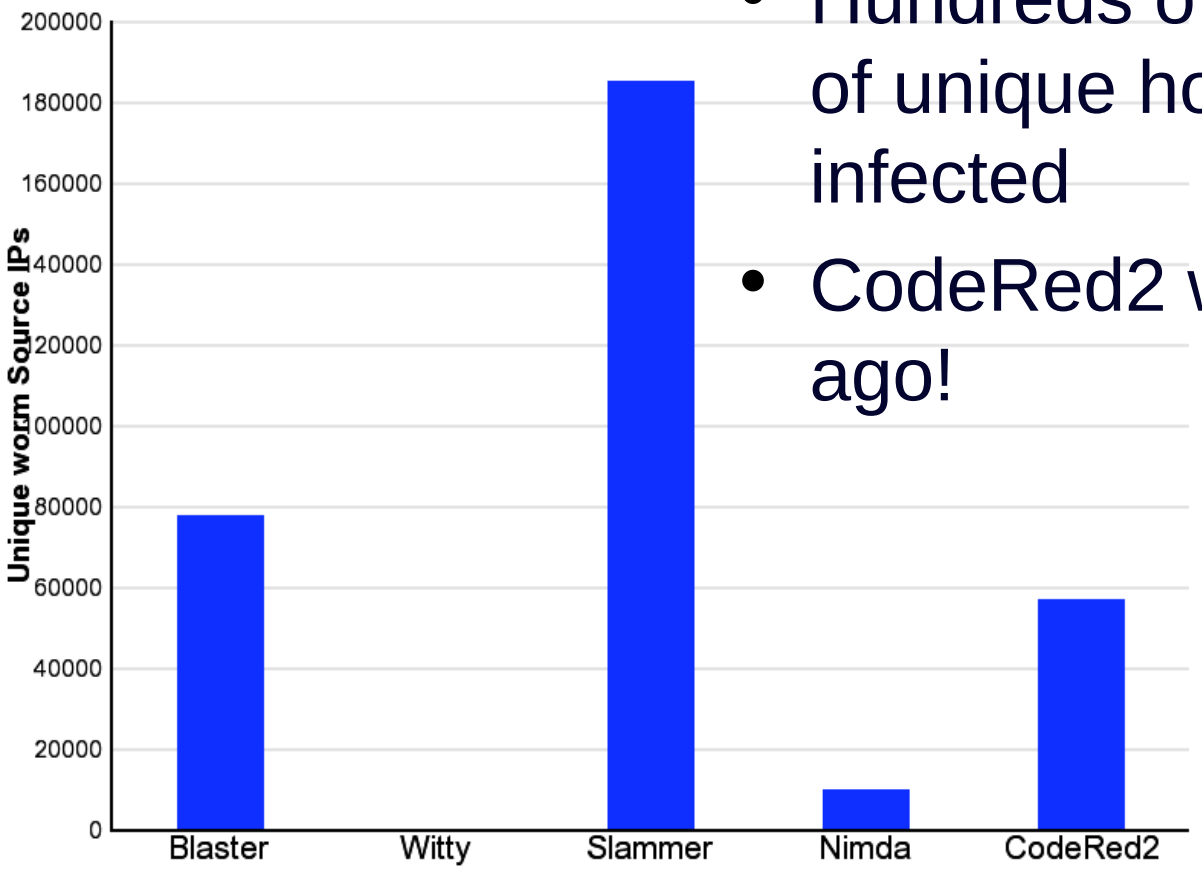
Outbreak of Blaster worm showing 3-phase life cycle

Blaster Circadian Pattern



- Cycles correspond with work week
- Saturday sees lowest activity
- Are infected hosts being rebooted?

Persistence of Internet Worms



- Hundreds of thousands of unique hosts still infected
- CodeRed2 was *years* ago!

Airborne Viruses

- As handheld devices become increasingly pervasive and interconnected, smart phones and PDAs will become increasingly susceptible to worms, viruses and Trojan horses.

- Broad range of applications: email, sms, web surfing, multi-player games, camera, e-transactions

- "The race to own a new platform!"

- Unlike desktop counterparts, security measures for these devices are relatively immature. Combined with unsecured wireless networks, the potential for fast propagating viral spread multiplies.

- Several methods of infection:
  - Synchronizing handheld with its desktop
  - Passing malicious code by infrared beam
  - Passing via unsecured wireless access

Airborne Viruses (cont.)

Palm OS Phage Virus:

- The first to successfully attack the Palm OS handheld platform in 2000. When executed, infects all third-party application program.
- When a carrier palm is synchronized with a clean palm, the clean palm could receive the virus in any infected file.
- This virus in turn copy itself to all other applications.

- Palm Security Update: Posted August 20, 2003

  “This SecurityPatch.prc software will address a password security issue that was discovered on Palm Zire 71 and Tungsten T2 handhelds. The issue relates to a condition that may compromise the password lock out of the device.”

Airborne Viruses (cont.)

- Windows CE PDAs have most of the ingredients for viral spread: fast processor, writeable memory, Pocket MS Word, Pocket outlook mail client.

- Potential is even greater if you combine a Microsoft mobile device OS with .NET distributed programming platform … small footprint, interconnected and running on a broad range of intelligent devices including cameras, Internet appliances, smart phones.

Airborne Viruses (cont.)

- Internet-based smart phones are increasingly vulnerable.

- Example:
  - SMS-based attack on Tokyo's emergency response system
  - Denial-of-service attack using SMS messages
  - The message hit 100,000 users inviting them to visit a web page
  - Activated a script to call 110, the emergency response number in Tokyo

Airborne Viruses (cont.)

Bluetooth Vulnerability: The Register June 2005

- Tel Aviv University in Israel - have come up with an exploit which allows hackers to pair with devices without alerting their owner.

- gets around limitations of a security attack first described by Ollie Whitehouse of security firm @Stake last year … needed to eavesdrop the initial connection process between two devices.

- a way to force this pairing process by masquerading as a device, already paired with a target, that has supposedly forgotten a link key used to secure communications.

Internal -v- Perimeter Environment

	PERIMETER	INTERNAL
NETWORK	**TENS** of targets **MEGABITS** of traffic	**THOUSANDS** of targets **GIGABITS** of traffic
APPLICATIONS	**TENS** of applications **WEB, MAIL, DNS**	**HUNDREDS** of applications **CUSTOM** protocols, **PEER-TO-PEER, COMMERCE**
POLICY	**INSIDE** and **OUTSIDE** groups **DEFAULT DENY**	**HUNDREDS** of groups **DEFAULT ALLOW**

Internal -v- Perimeter Protection

	PERIMETER	INTERNAL
THREATS	KNOWN EXPLOITS SCANNING	INSIDER MISUSE ZERO-DAY ATTACKS
IMPACT	INTERNET OUTAGE	DISRUPTION TO CONSUMER and BUSINESS ACCESS
DEPLOYMENT	ACCESS POINTS	DISFUSED THROUGHOUT NETWORK

Questions?

- What if we expand the pool of bots and botnets to include 2+Billion smart phone and PDAs?
- How do secure a broad rage of new mobile platforms and applications?
- What is the deployment model for security devices such as firewall, IDS, IPS? Where is the perimeter?
- How would convergence of networking and security devices in the wired world affect mobile computing?
- …