

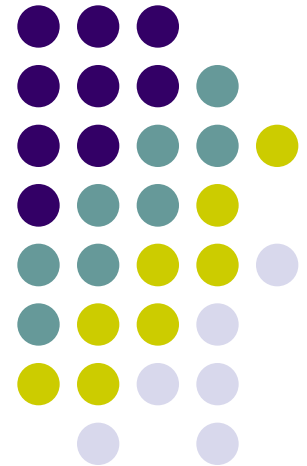
Network Security – Issues and New Challenges

Brijesh Kumar, Ph.D.

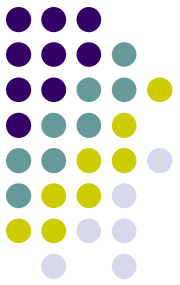
Princeton Jct, NJ 08550

Brijesh_kumar@hotmail.com

A talk delivered on 11/05/2008



Contents Overview



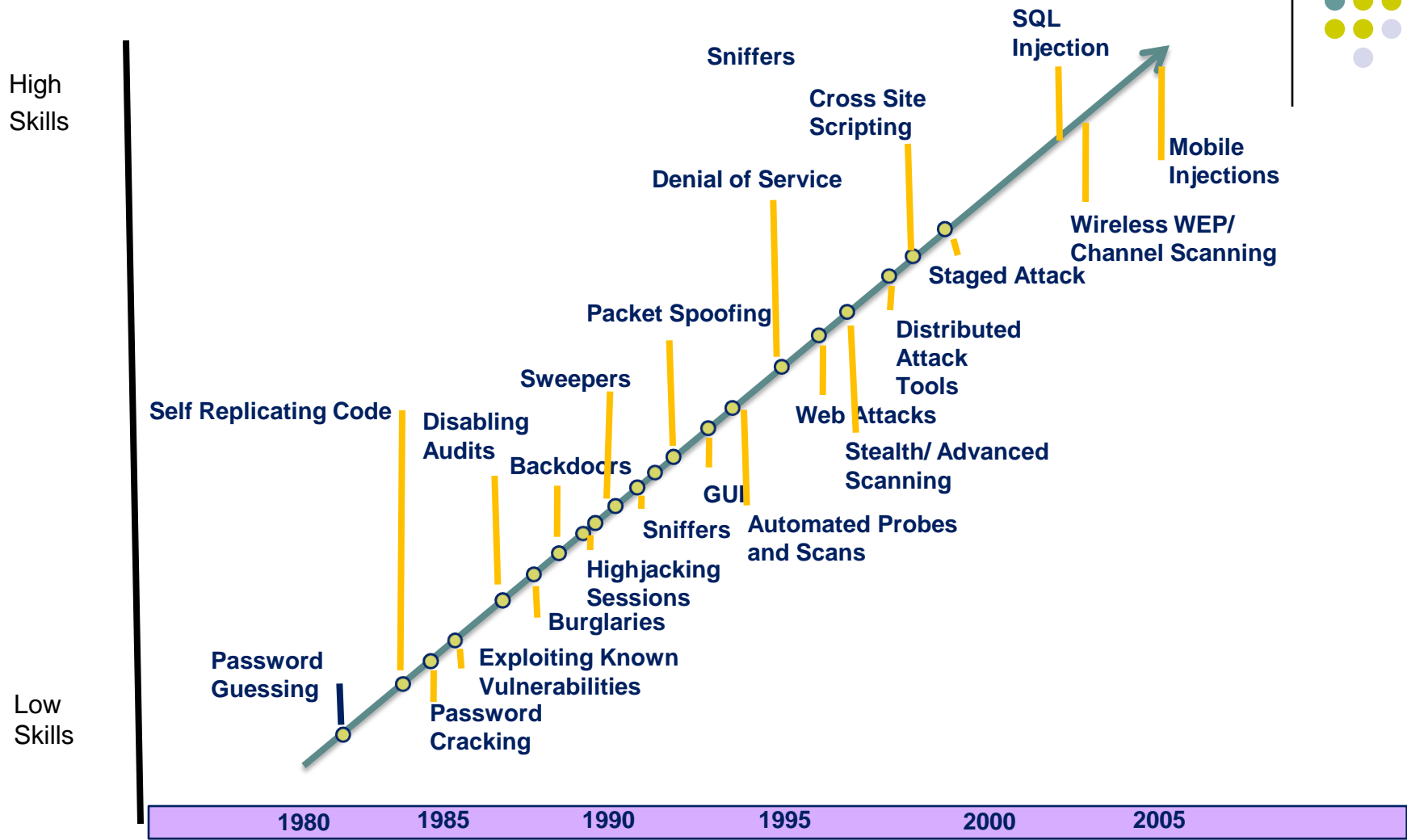
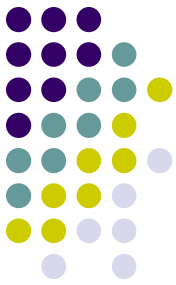
- The problem
- Historical Perspective
- Software - Vulnerability
- Networks – IP protocols, Routing, DNS and SMTP, VoIP
- Web - IIS, Apache
- Wireless - Cellular, Wi-Fi Security

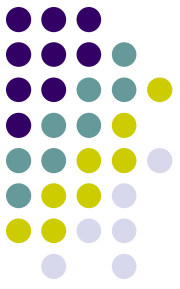


Why aren't Computer or Network Secure?

- Both Computer and Networking Originated In the University Labs.
- University environments are collaborative places with focus on solving problems in efficient and unique ways
- Adversarial model analysis is not what researchers really did on old days
- Applies to Software to Nuclear Technologies!
- Result – quite open issues in just about every thing – Software, Protocols -- IP, TCP, SMTP, DNS
- Patchwork solutions – Discover a problem – Patch it.

Always Something New Invented

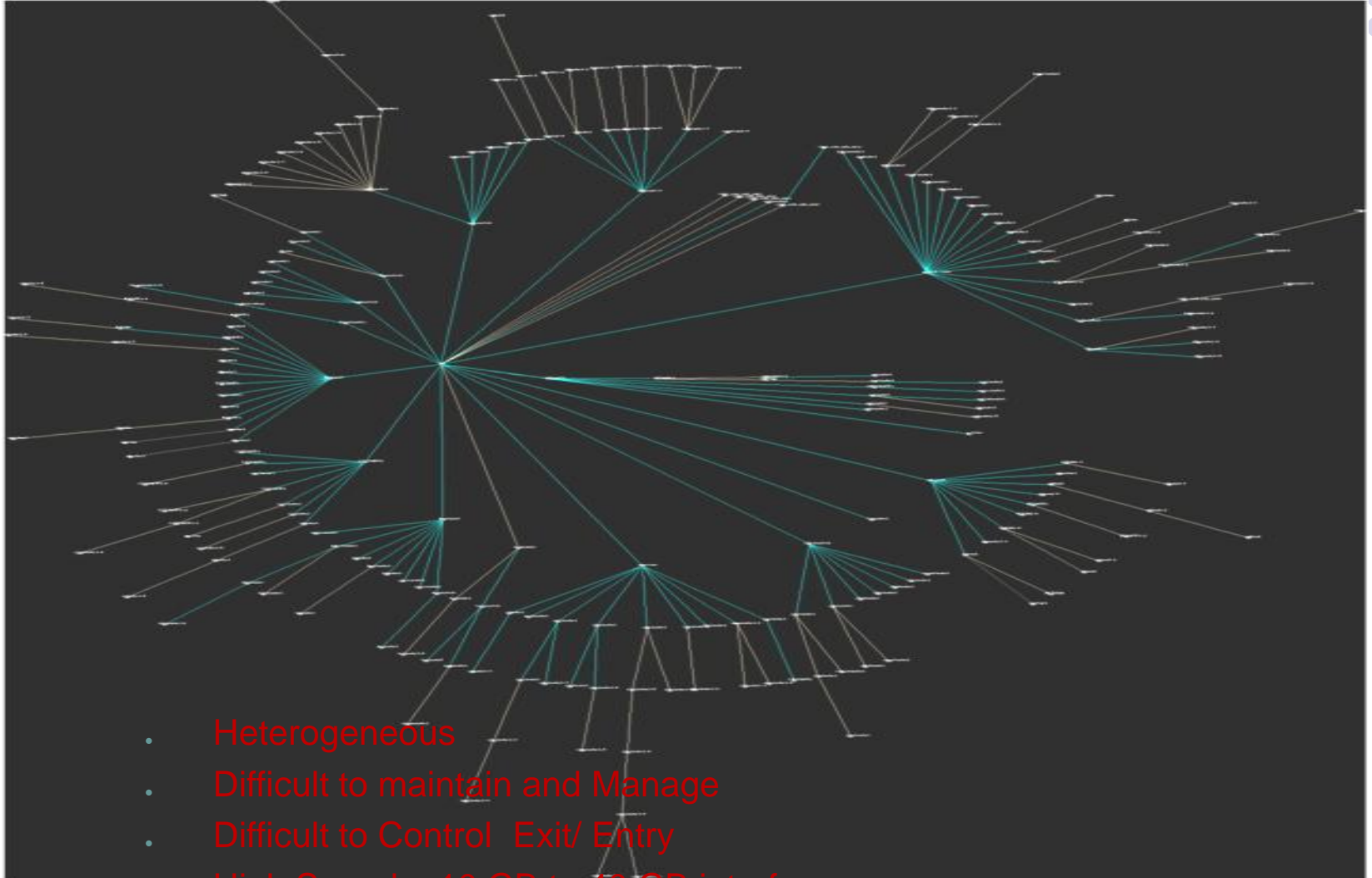
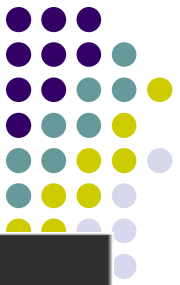




Internet is Getting Less Secure

- By every measure, Internet is becoming less secure every day:
 - More attacks, More damages and more losses
 - Severity of damages is increasing – stolen users data, credit card, Id-theft, System high-jacking
- Security is in architecture, and not in patch solutions
 - If Firewalls were so good – we would have solved all the security problems ? Is Industry fooling you?
 - If virus checker are great then why they haven't solved the security problems? Give me money every year Trap?

Modern Networks are Really Large ..



- Heterogeneous
- Difficult to maintain and Manage
- Difficult to Control Exit/ Entry
- High Speed – 10 GB to 40 GB interfaces

Network Growth



- Tremendous Network growth from 1994-2008
- Many millions of new nodes
- No national boundaries
- Makes Attacks relatively safe since there are no way to monitor or catch the culprits
- Software is still the mystery
- Not every user is a computer science graduate
- Firewalls and Virus checking don't really work.

Network Telescope at caida.org (ucsd)



Interesting stuff to study network (attack) traffic

Continuous Monitoring of Chunk of (globally) routed IP address space

- 16 million IP addresses

Little or no legitimate traffic (or easily filtered)

Unexpected traffic arriving at the network telescope can imply remote network/security events

Setup - Generally good for seeing explosions, not small events

Reaction - Depends on random component in spread

I like the data they generate – great source!

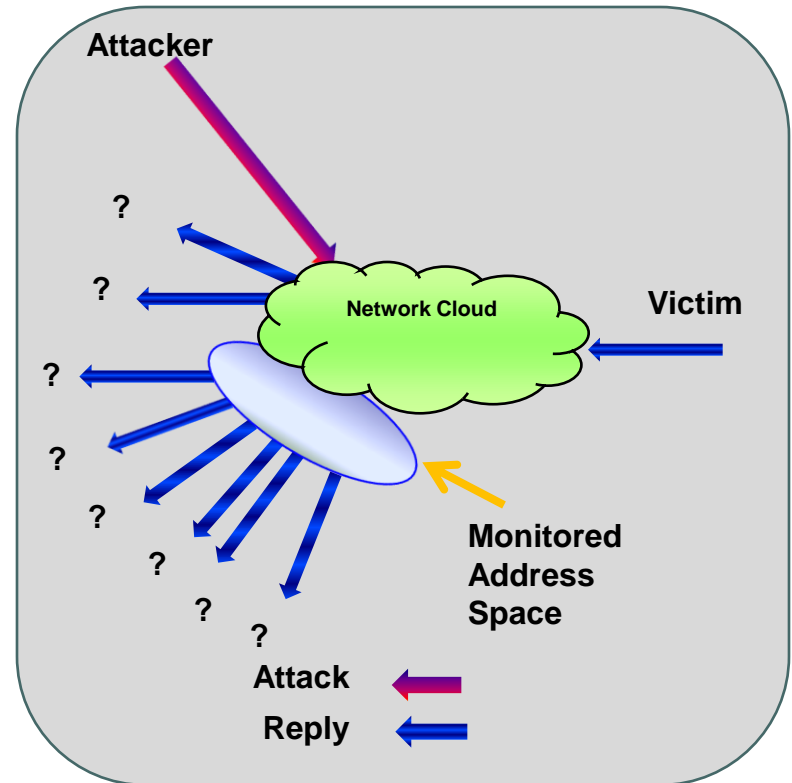
Denial-of-Service Attacks : Network Telescope Experiment



Attacker floods the victim with requests using random spoofed source IP addresses

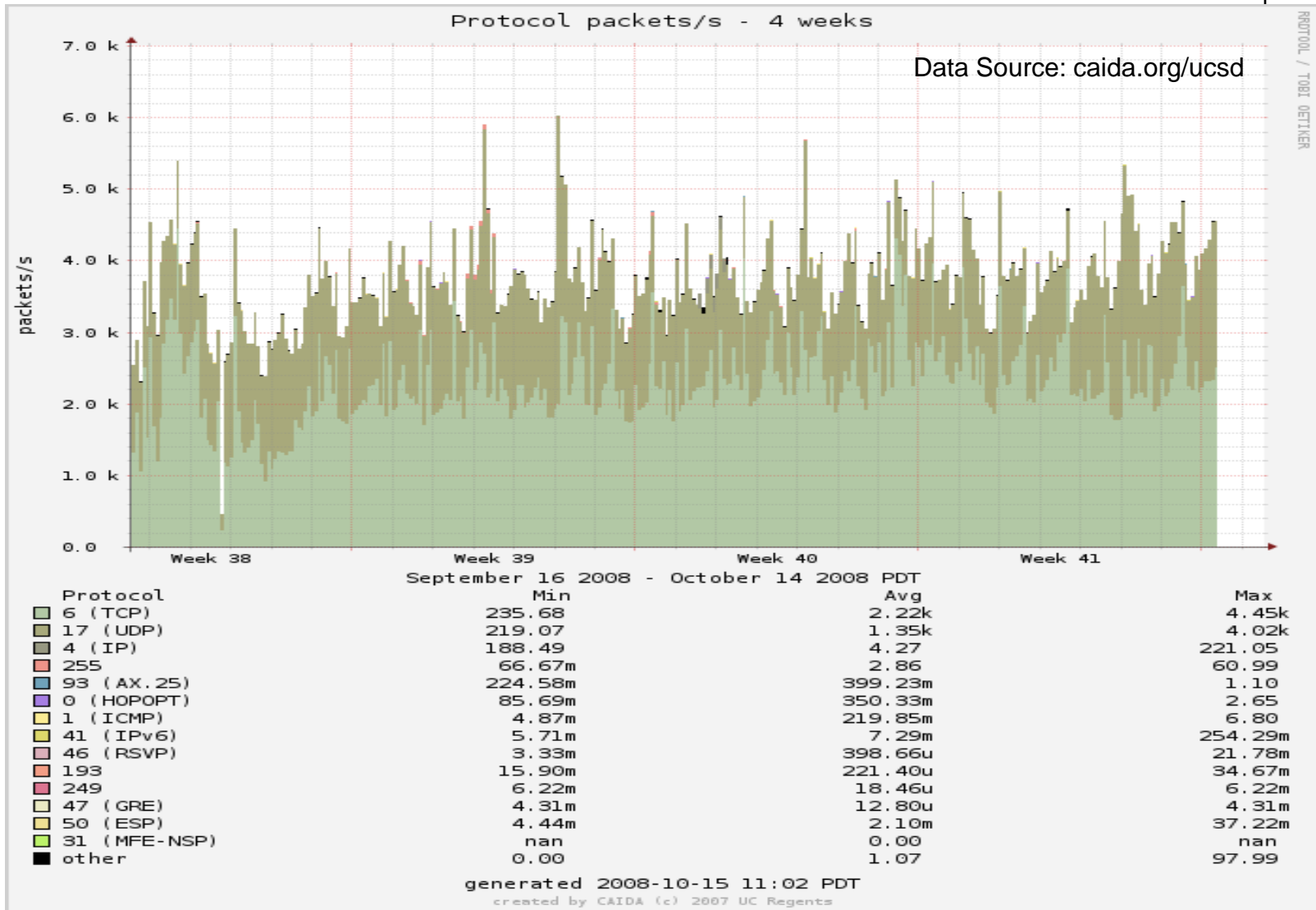
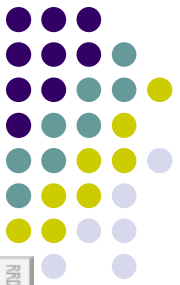
Victim believes requests are legitimate and responds to each spoofed address

Reported Observations
 $1/256^{\text{th}}$ of all *victim* responses to spoofed addresses

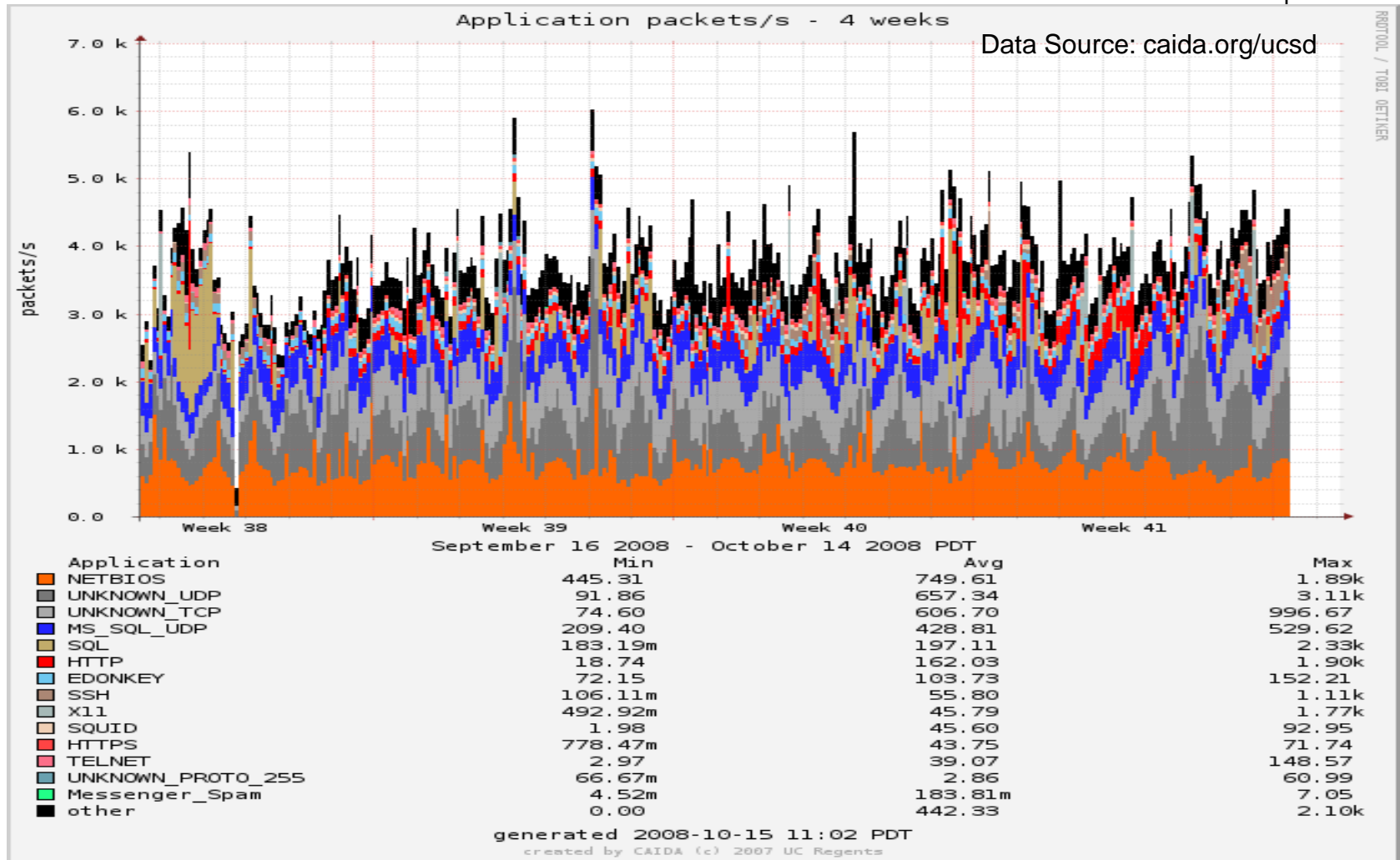
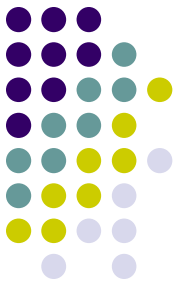


Source: caida.org/ucsd

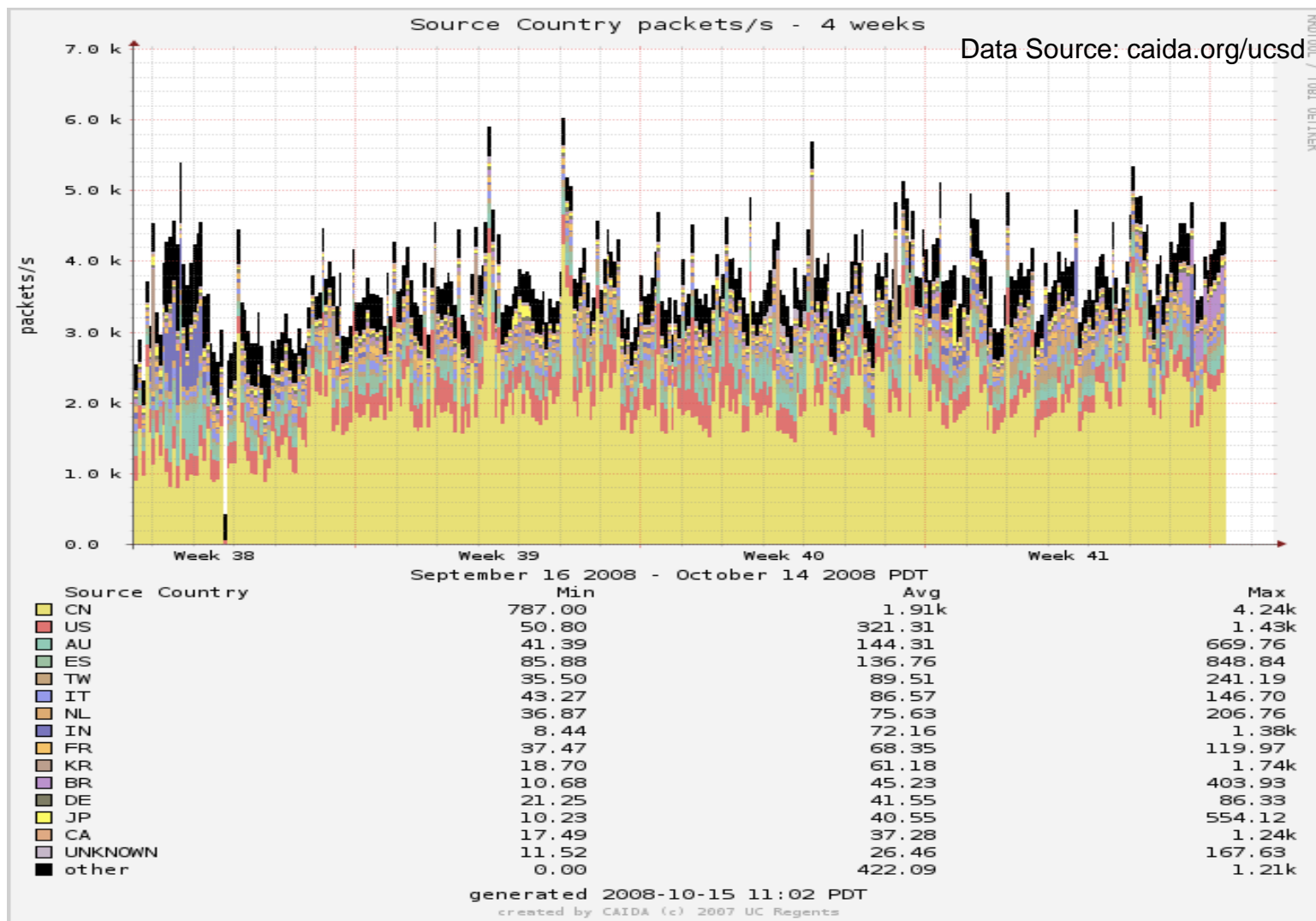
Attack packets By Protocol



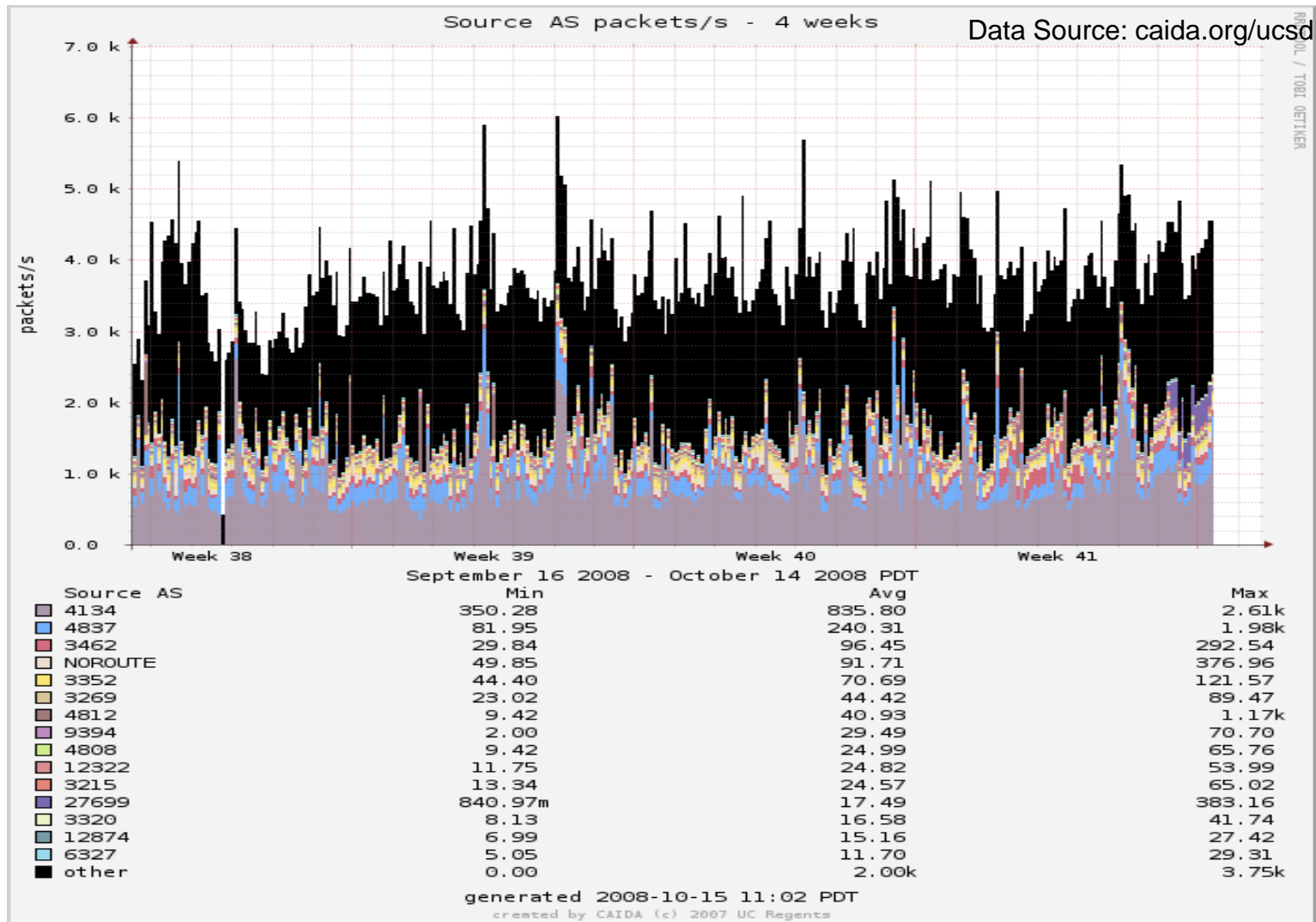
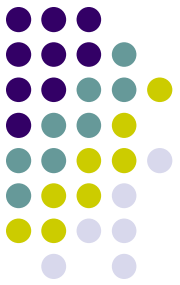
Attack packets by Application

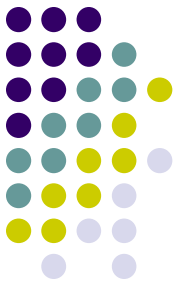


Attack Packets by Originating Country

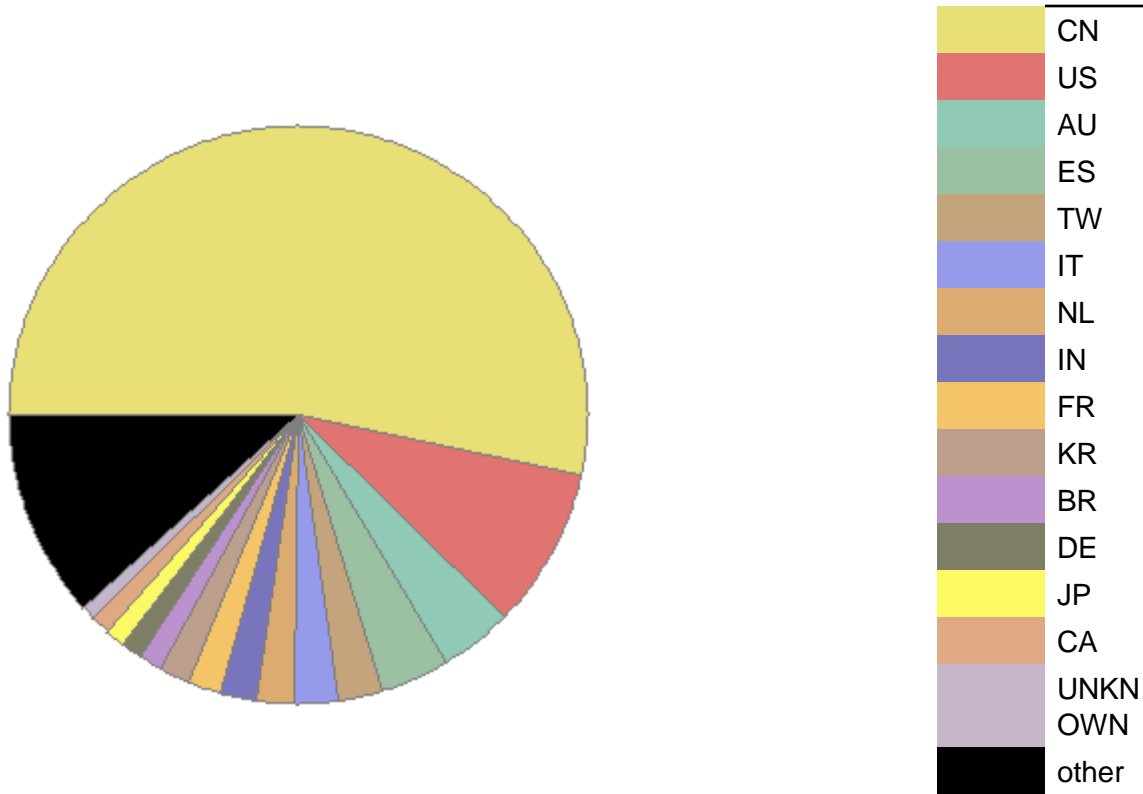


Attack Packets By AS Number

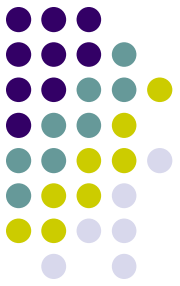




Attack packets by Source Country



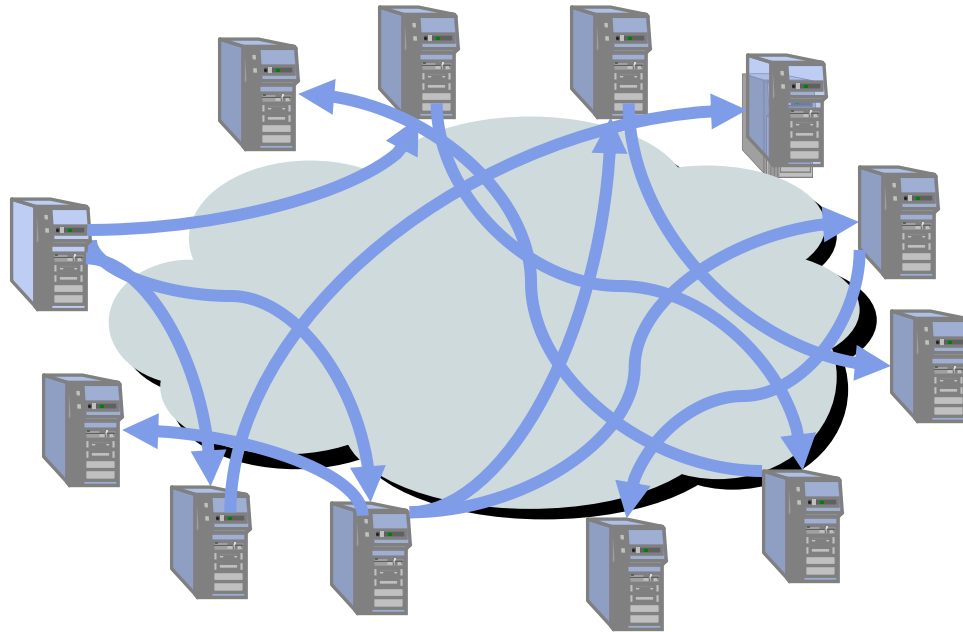
Data Source: caida.org/ucsd



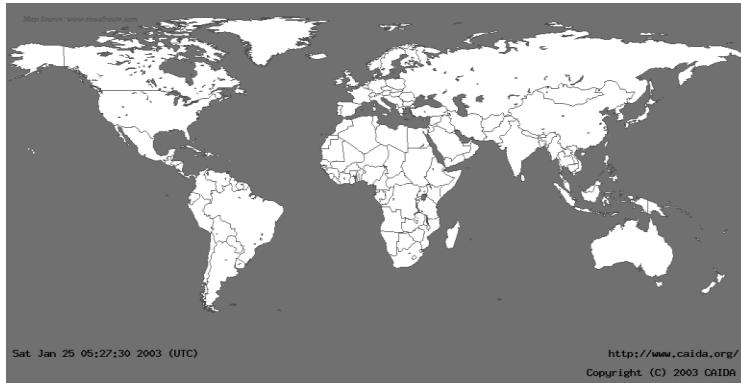
Network Worm Spread

Self-propagating self-replicating network program

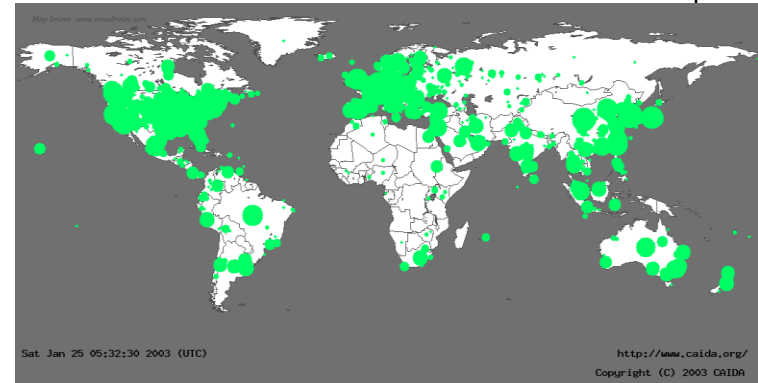
- Exploits some vulnerability to infect remote machines
 - No human intervention necessary
- Viral Nature - Infected machines continue propagating infection



Witty March 16 – 2004

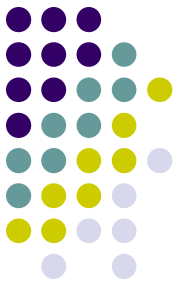


● Before 9:30PM (PST)



● After 9:45PM (PST)

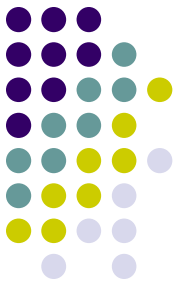
- ~12,000 hosts infected in **30 minutes**
- Averaged more than 11 million probes per second world-wide
- Unstoppable (UDP Scan of Hosts at Line rates)
- Irreparably destroyed a significant number of infected computers



What we learnt from this

- Patch model of networked device security doesn't work
- End-user behavior alone cannot solve current software security problems
- End-user behavior cannot effectively mitigate current software security problems
- Study Concluded:
 - Actively address prevention of software vulnerabilities
 - Turn our attention to developing large-scale, robust, reliable infrastructure that can mitigate current security problems without end-user intervention

Emergence of Botnets



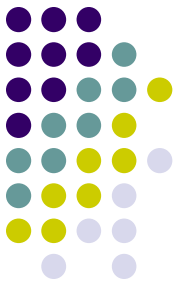
Significant transition in motivation for widespread, non-specific malicious activity

- From notoriety -> want to be noticed
- To money -> want stealth to protect revenue stream
- No one does it just for fun – (Too risky)

So how do you make money?

- Sending spam – 90% mails are spam
- DoS extortion – Blackmail, Threats
- Active (phishing) and passive identity theft

New Challenges



- Malicious software development is Group activity with a purpose.
- Need expertise to build scalable, manageable distributed (negatively) purposeful software systems. Time and resource needed.
- Coordinated activity makes current antivirus activities increasingly irrelevant
- Signature-based security don't work in this environment
- Increasing system complexity + naïve / untrained IT/ Software Developers = Security Disaster

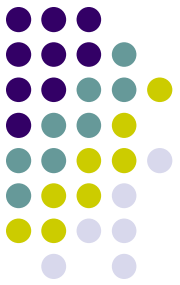
Malicious Code



- Tracking Software – Evil Biz
- Advertising Display Software - Internet is built on adverts.
- Remote Control Software – Session Hijacking, Data Transporting
- Redirection Software - Absolute Evil
- System Modifying Software – Rootkits, Spyware of All kinds, Very Nasty, Hard to Remove.
- Security Analysis Software
- Automatic Download Software –Click yes or no – it will still download.
- Passive Tracking Technologies
 - Spyware / Snoopware
 - Keylogger (Unauthorized)
 - Screen Scraper (Unauthorized)



Typical intrusion scenario



All intrusion attempts go through a simple three steps:

- **Footprinting:** To identify and find out more information about the target
- **Scanning:** To look for open back doors
- **Exploiting:** To attempt to gain access through the back doors
- **Conquered:** Establishing the compromised system for the next intrusion.

Security Measures



Security measures Can be defined as Three

- Prevention
 - – UAC, Cryptography, Firewalls
- Detection
 - - IDS – Audit Trail, Logs and Forensic (e.g., Snort)
- Response.
 - Depends On the Nature of Compromise (Technical/
Legal, Combined)

Software Security



- **Secure Operating Systems** -
 - Example - Secure Linux Project
 - Access Control and Privileges controlled
 - Inter-process barriers
 - Access control barriers for inter task communications
 - Sandboxed Tasks

- **Defensive programming**

Majority of software subversion vulnerabilities result from a few known kinds of coding defects. Common software defects include:

- buffer overflows,
- format string vulnerabilities,
- integer overflow, and
- code/command injection.

Network Security



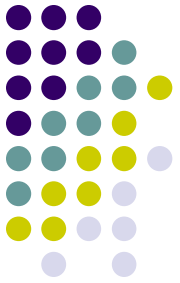
- Security Domain plans
- Traffic flow separation
- Perimeter protection
- Defense in depth
- Secure protocols (IPSEC, SSH)
- Security systems (Firewalls, VPNs etc.)

- **Wireless:**
 - Wireless Wi-Fi Security – So much has already been written and said.
 - Cellular Wireless – So far Isolated from these threats. But Emerging.

Some new research Areas in Security



- NSF's Next gen Network – Redesign protocols with clean slate.
- Security and Privacy in Low power Sensor Networks
- Security and Privacy in Ad-hoc Wireless Networks
- Secure Operating Systems
- Proactive Web Security
- Multi-point Distributed Intrusion Detection Systems
- Systems Approaches for Constructing Distributed Trust
- Reputation systems for improved collaborative anomaly and intrusion detection for internetworking protocols
- Cellular Systems Vulnerabilities and protections
- Proactive Spam control
- Botnet detection and counter/ reverse attacks



Thank You –