

# Internet Outbreaks and Worm Containment : Cyber Security Assurance

**Kai Hwang**

University of Southern California

Technical presentation at The SESASC  
Annual Meeting, Airport Hilton,  
Los Angeles, April 23, 2005



1

## Security and Privacy Demands in Internet Services and IT Applications:

- Trusted E-Commerce over the Internet
- Secure communications in E-mails
- Protected download of digital contents
- System Intrusions and Network Anomalies
- Firewalls, packet filters, VPN gateways, traffic monitors, security overlays, PKI services, etc.
- Self-defense toolkits, middleware, overlays for defense against viruses, worms, and flood attacks
- Anonymity, confidentiality, data integrity, access control, resolving policy conflicts, etc.

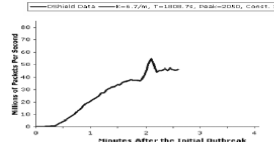
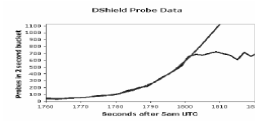


## Internet Epidemic Outbreaks in Recent Years

- *Nimda, CodeRed, Slammer, Blaster, etc.*
- CodeRed affected 360,000 web servers in 16 hours
- Slammer was the fastest worm at large in that it scanned 90% of the Internet in less than 10 minutes.

### A pretty fast outbreak: Slammer (2003)

- First ~1min behaves like classic random scanning worm
  - Doubling time of ~8.5 seconds
  - CodeRed doubled every 40mins
- >1min worm starts to saturate access bandwidth
  - Some hosts issue >20,000 scans per second
  - Self-interfering (no congestion control)
- Peaks at ~3min
  - >55million IP scans/sec
- 90% of Internet scanned in <10mins
  - Infected ~100k hosts (conservative)



See: Moore et al, IEEE Security & Privacy, 1(4), 2003 for more details

April 23, 2005, Kai Hwang

<http://GridSec.usc.edu>

3



## Internet Worm Containment :

**Reduce Vulnerability:** Preventing worms by upgrading software quality and reducing the system vulnerability.

**Scan Detection:** Filtering traffic destined at detected ports where worms appear to be scanning and spreading.

**Hygiene Enforcement:** Discovering infected hosts and keep susceptible hosts off network.

**Signature Inference:** Detecting payload content substrings to generate and disseminate signatures automatically and throttle to slow down the spread.

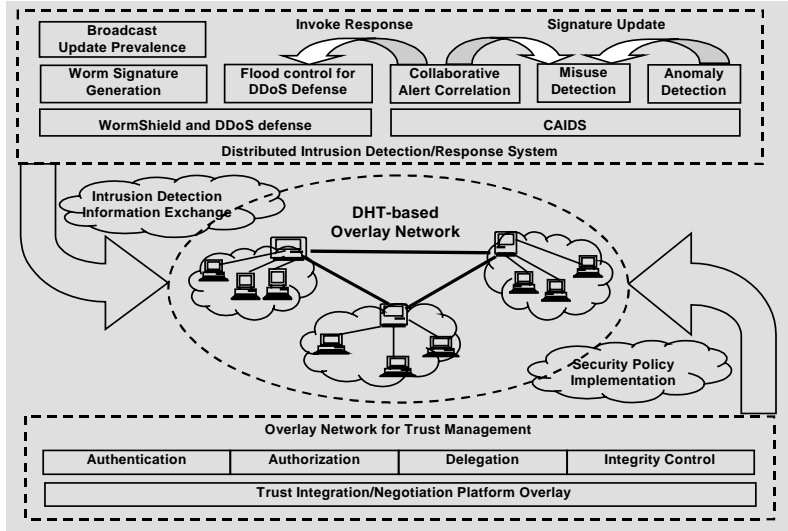
April 23, 2005, Kai Hwang

<http://GridSec.usc.edu>

4



# The NetShield Architecture with Distributed Security Enforcement over a DHT Overlay



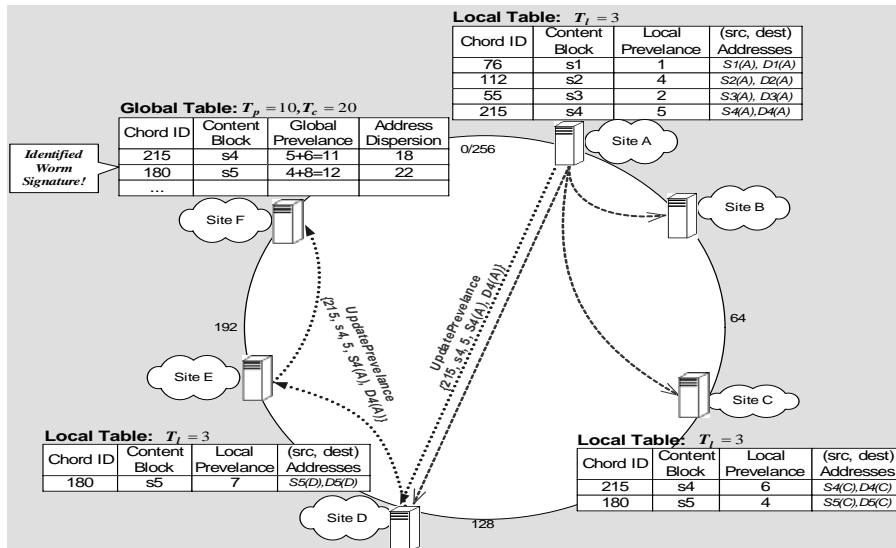
April 23, 2005, Kai Hwang

<http://GridSec.usc.edu>

5



# The WormShield Built with a DHT-based Overlay with Six Worm Monitors



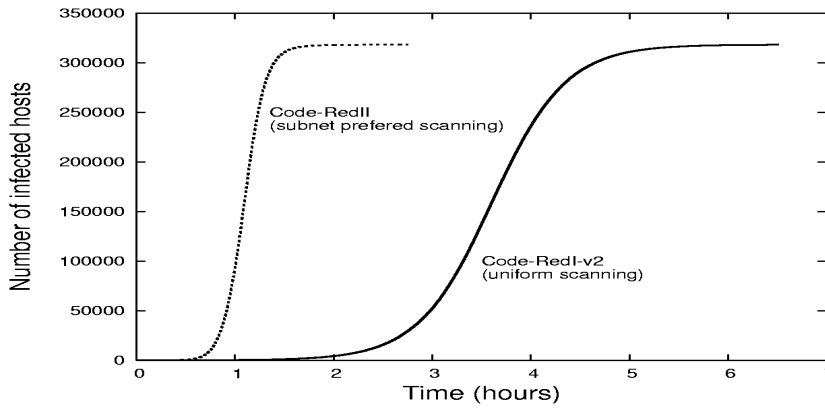
April 23, 2005, Kai Hwang

<http://GridSec.usc.edu>

6



# Signature Detection in Worm Spreading and the Growth of Infected hosts for Simulated CodeRed Worms on a Internet Configuration of 105,246 Edge networks in 11,342 Autonomous Systems Containing 338,652 Vulnerable Hosts



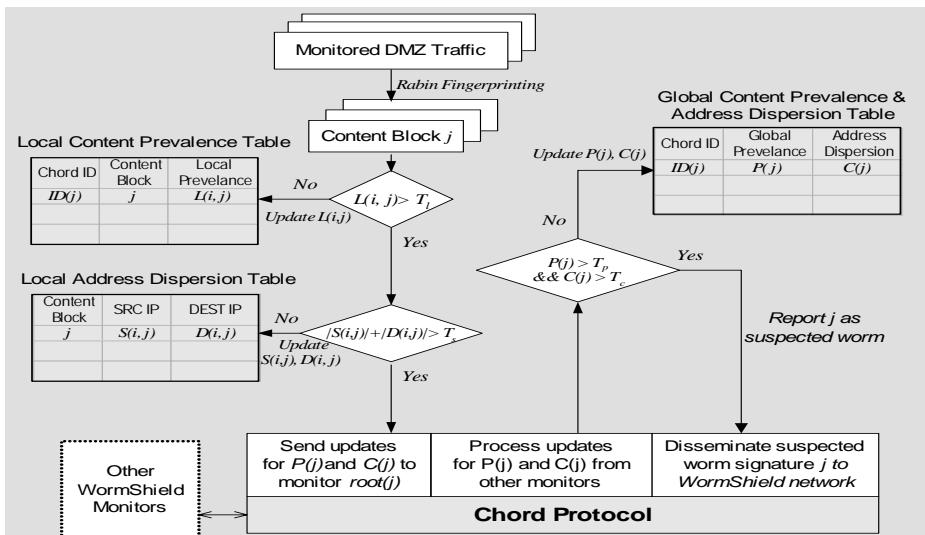
April 23, 2005, Kai Hwang

<http://GridSec.usc.edu>

7



## The WormShield Signature Generation Process



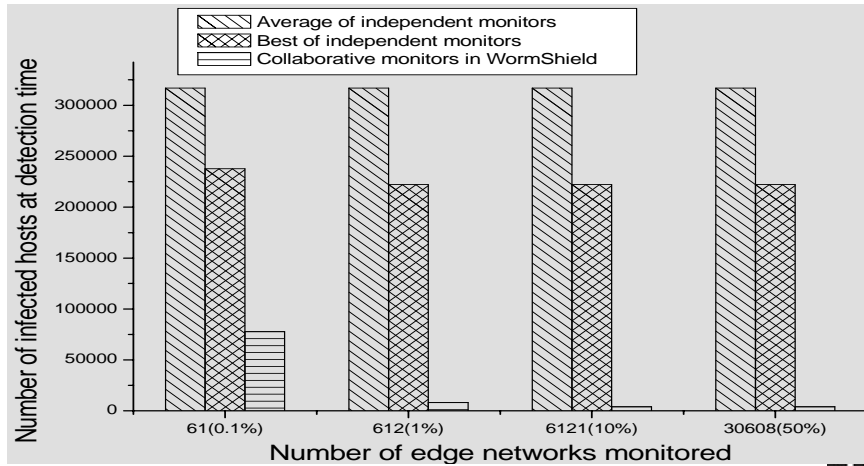
April 23, 2005, Kai Hwang

<http://GridSec.usc.edu>

8



# Reduction of Infected Hosts by Independent vs. Collaborative Monitoring over the Edge Networks



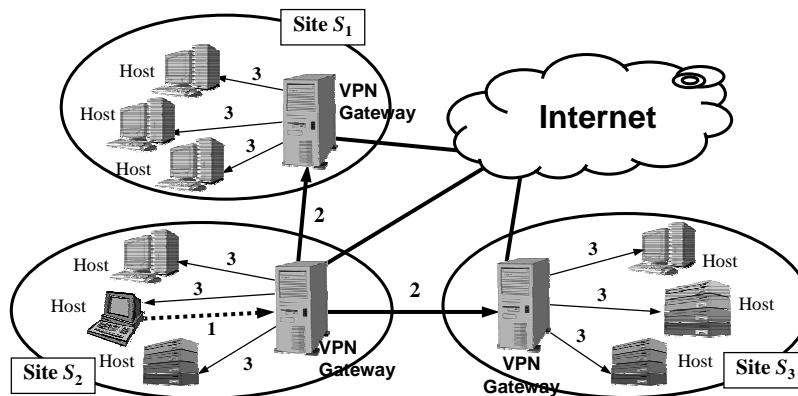
April 23, 2005, Kai Hwang

<http://GridSec.usc.edu>

9



## GridSec: A Network Security Research Project at USC



Steps for automated self-defense at resource site :

- ..... Step 1: Intrusion detected by host-based firewall /IDS
- Step 2: All VPN gateways are alerted with the intrusions
- Step 3: Gateways broadcast response commands to all hosts

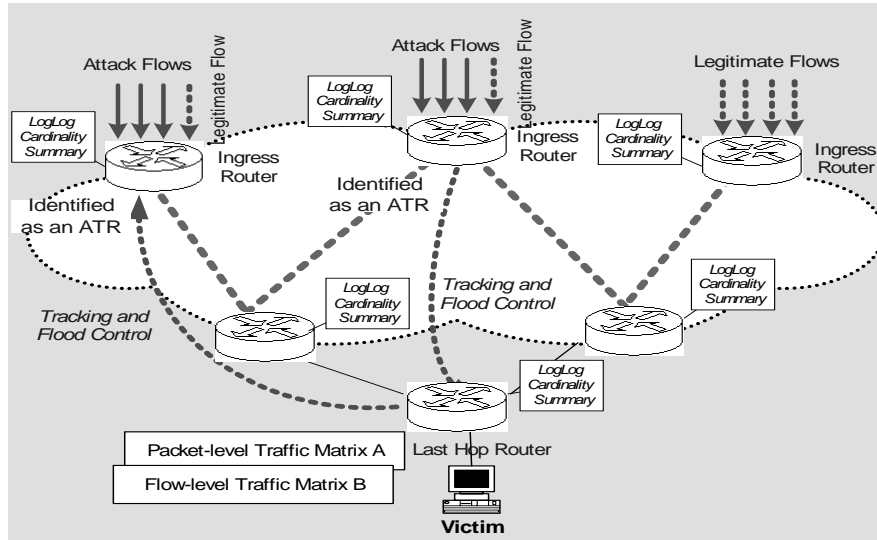
April 23, 2005, Kai Hwang

<http://GridSec.usc.edu>

10



## Packet/Flow Counting for Tracking Attack-Transit Routers (ATRs)



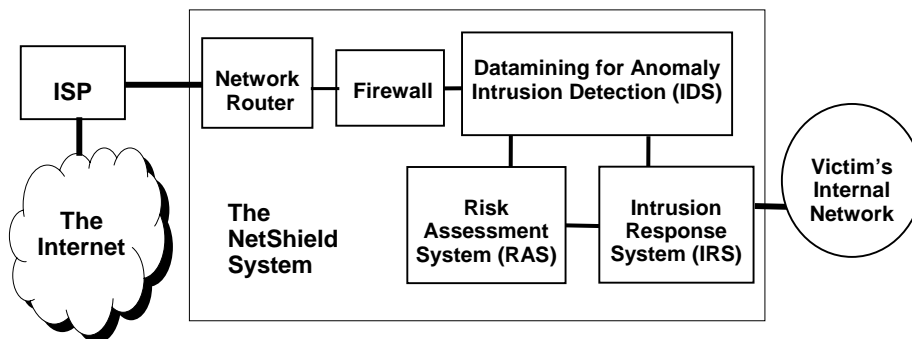
April 23, 2005, Kai Hwang

<http://GridSec.usc.edu>

11



## USC NetShield Intrusion Defense System for Protecting Local Network of Grid Computing Resources



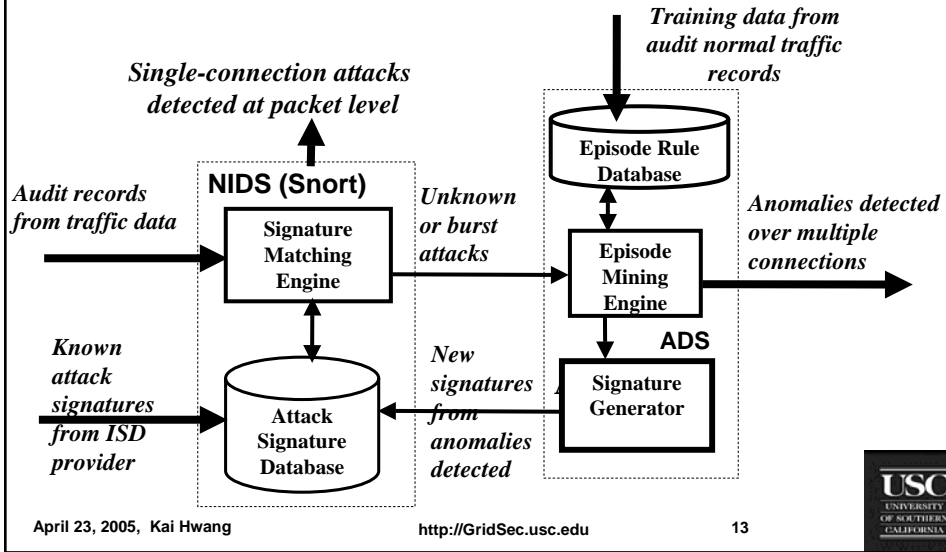
April 23, 2005, Kai Hwang

<http://GridSec.usc.edu>

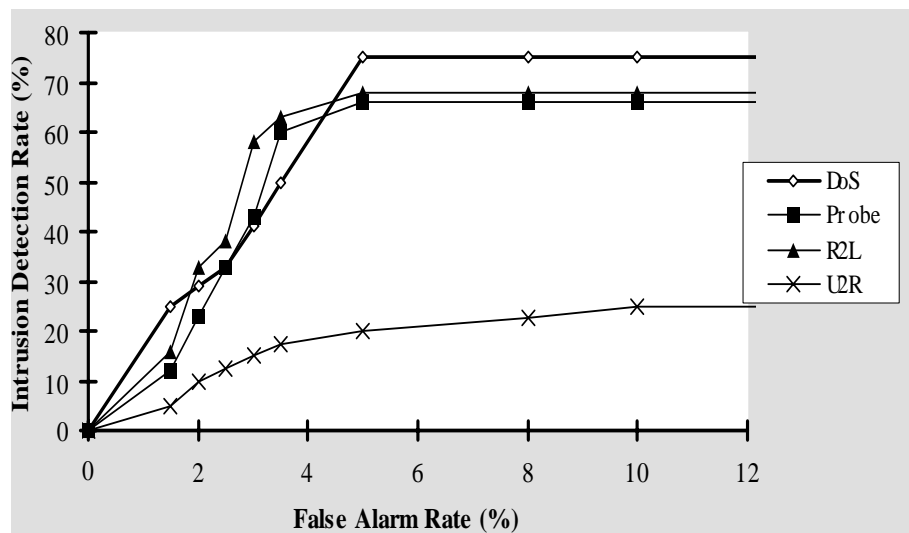
12



## A Collaborative Anomaly and Intrusion Detection System (CAIDS), built with the Snort and an Anomaly Detection System at USC Internet and Grid Computing Laboratory in 2004



## ROC Curves for 4 Attack Classes on The Simulated CAIDS



## Hot Security Research Areas:

- Efficient and enforceable trust models are very much in demand for networked and distributed systems: PKI services, VPN tunneling, trust negotiation, security overlays, reputation systems, etc.
- Large-scale security benchmark experiments in open Internet environments are infeasible. The NSF/HSD DETER testbed is designed to perform security experiments towards sustainable cybertrust over all edge networks.
- Internet datamining for security control and for guarantee of Quality-of-Service in real-life network applications – Interoperability between wired and wireless networks is a wide-open area for further research.

April 23, 2005, Kai Hwang

<http://GridSec.usc.edu>

15



## To Probe Further :

1. M. Cai, K. Hwang, Y. K. Kwok, Y. Chen, and S. S. Song, "Fast Containment of Internet Worms and Tracking of DDoS Attacks with Distributed-Hashing Overlays", *IEEE Security and Privacy*, to appear Nov/Dec. 2005.
2. K. Hwang "Defending Distributed Computing Systems from Malicious Intrusions and Network Anomalies", Keynote address at *IEEE Workshop on Security in Systems and Networks (SSN'05)*, in conjunction with *IEEE IPDPS 2005*, Denver, April 8, 2005.

Download from web site: <http://GridSec.usc.edu>

April 23, 2005, Kai Hwang

<http://GridSec.usc.edu>

16

