GridSec: Trusted Grid Computing with Security Binding and Self-Defense against Network Worms and DDoS Attacks

Presentation by Kai Hwang at the
***International Workshop on Grid Computing Security and Resource Management* (GSRM'05) in conjunction with the ICCS 2005, Emory University, Atlanta, May 24, 2005.**

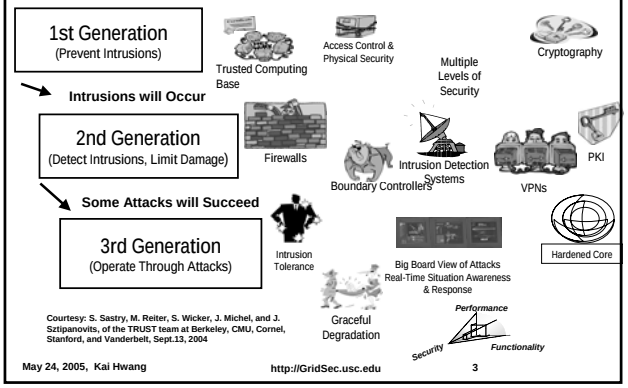
Contributors:
Min Cai, Shanshan Song, Yu-Kwong Kwok, Yu Chen, Runfang Zhou, Ying Chen, Xiaosong Lou, and Kai Hwang
University of Southern California

The research reported here was fully supported by NSF ITR Research Grant 0325409.
Project web site: http://GridSec.usc.edu/

Presentation Outline:

- Introduction to NSF GridSec Project
- NetShield Architecture Development
- Collaborative Worm Containment
- Cardinality Counting for DDoS Defense
- Hot Topics for Trusted Grid Computing

Defense Technology Towards Cyberspace Security Assurance



Courtesy: S. Sastry, M. Reiter, S. Wicker, J. Michel, and J. Sztipanovits, of the TRUST team at Berkeley, CMU, Cornel, Stanford, and Vanderbelt, Sept.13, 2004

Internet Epidemic Outbreaks in Recent Years

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)

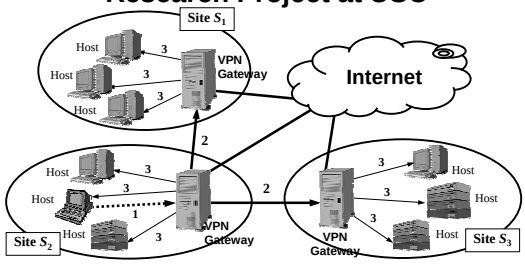
- ***Nimda, CodeRed, Slammer, Blaster, etc.***
- **CodeRed affected 360,000 web servers in 16 hours**
- **Slammer was the fastest worm at large - it scanned 90% of the Internet in less than 10 minutes.**

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

Security and Privacy Demands in Internet Services and Grid Applications:

- **Trusted E-Commerce over the Internet**
- **Secure communications in E-mail, FTP, etc.**
- **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.**

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**

Worms and DDoS Attacks Overview

- **Network Worms**
  - **Self-propagating program across a network**
  - **Exploit vulnerabilities in widely-deployed homogeneous software**
  - **Various malicious payloads, e.g. host spam-relays, launch DDoS attacks, etc.**
  - **CodeRed in 2001, Slammer in 2003**
- **Distributed Denial-of-Service (DDoS) Attacks**
  - **Overwhelm victim's resources with high-volume traffic**
  - **Exploit Internet's unrestricted communication model**
  - **Could exploit victim's protocol vulnerability, e.g. TCP SYN flood, but do not have to, e.g. UDP flood**
  - **Often use worms to prepare and perform attacks automatically - CodeRed's attack against whitehouse.gov**

The NetShield Architecture with Distributed Security Enforcement over a DHT Overlay

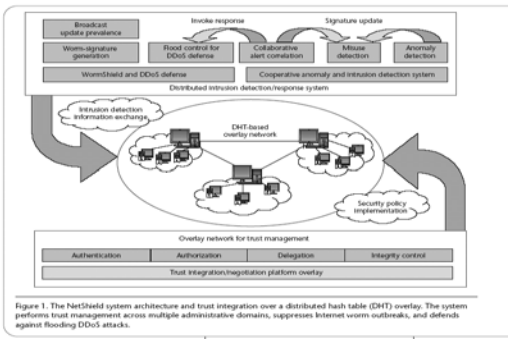


Figure 1. The NetShield system architecture and trust integration over a distributed hash table (DHT) overlay. The system performs trust management across multiple administrative domains, suppresses Internet worm outbreaks, and defends against flooding DDoS attacks.

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.**

The WormShield Built with a DHT-based Overlay with Six Worm Monitors [1]

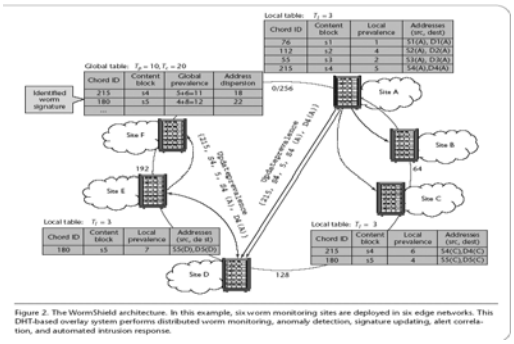
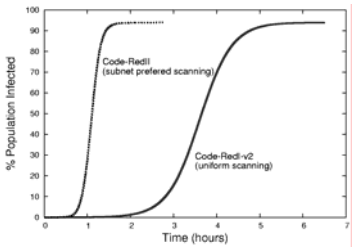
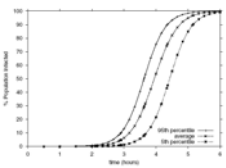


Figure 2. The WormShield architecture. In this example, six worm monitoring sites are deployed in six edge networks. This DHT-based overlay system performs distributed worm monitoring, anomaly detection, signature updating, alert correlation, and automated intrusion response.

Simulation Results

- Simulated CodeRed-like worms on an Internet configuration of 105,246 edge networks and 338,562 vulnerable hosts
- Use BGP table snapshot on July 19th, 2001 from RouteViews
- Simulated infection progress matches quite well with Moore's experimental results

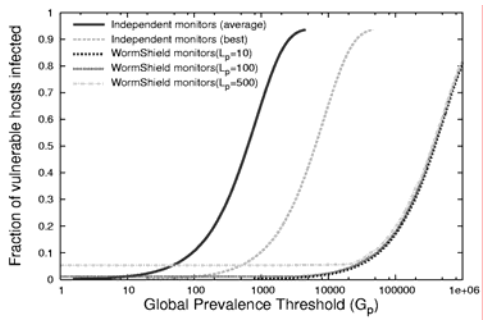




[Moore et al, INFOCOM 2003]

Effects of Global Prevalence Threshold

- Collaborative monitors detect signatures about 10 times faster than using independent monitors when *Gp*=10,000



WormShield Signature Generation Process

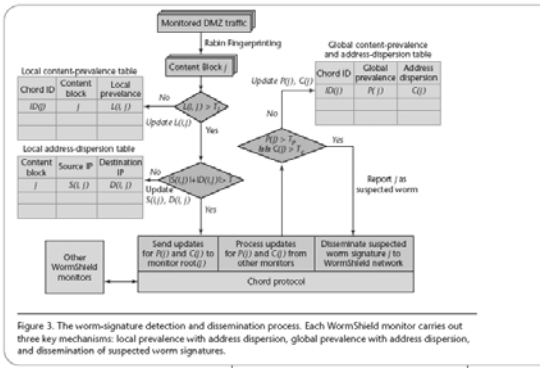
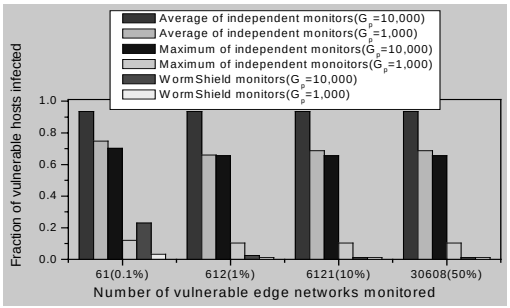


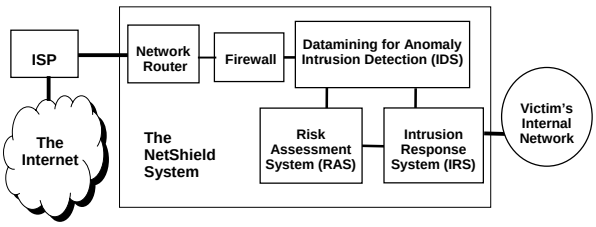
Figure 3. The worm-signature detection and dissemination process. Each WormShield monitor carries out three key mechanisms: local prevalence with address dispersion, global prevalence with address dispersion, and dissemination of suspected worm signatures.

Effects of % Edge Networks Monitored

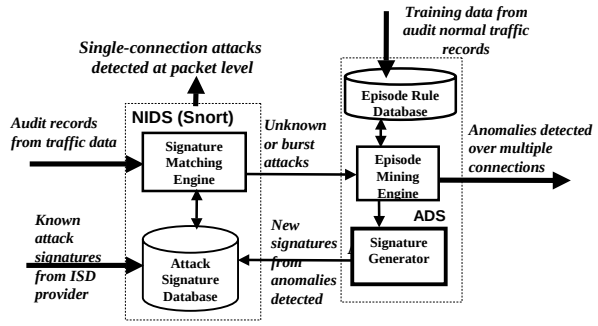
- **About 27 times reduction of infected hosts as 1% of vulnerable edge networks being monitored**



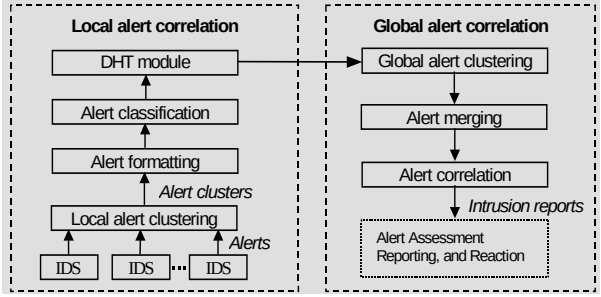
USC NetShield Intrusion Defense System for Protecting Local Network of Grid Computing Resources



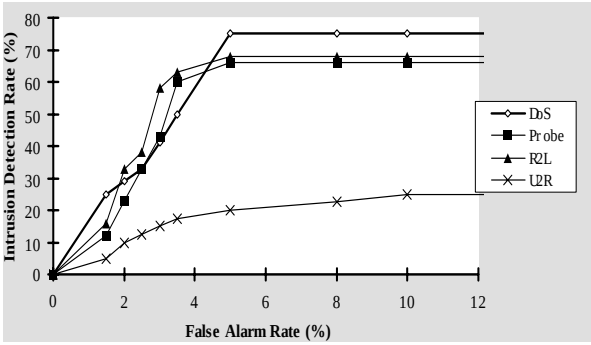
A Collaborative Anomaly and Intrusion Detection System (CAIDS), built with the Snort and an Anomaly Detection System at USC Internet and Grid Computing Lab in 2004 [2]



Alert Operations performed in local Grid sites and correlated globally

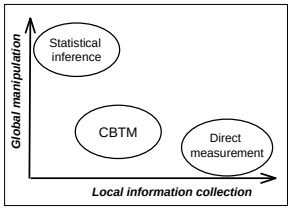


ROC Curves for 4 Attack Classes on The Simulated CAIDS



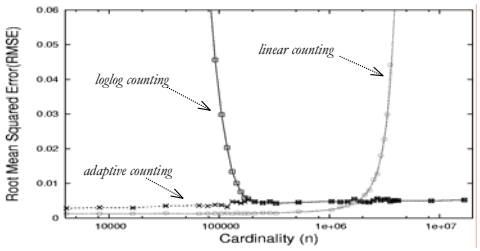
Cardinality-Based Traffic Matrix Estimation

- Traffic Matrix (TM) for diagnosing deliberate network anomalies
- Need to obtain TM in a fast and accurate manner
- Both packet-level TM (PTM) and flow-level TM (FTM)
  - Unusual increase in small flows, e.g. flooding attacks and scanning worms
- Limitations of existing TM estimation approaches
  - Not accurate enough (10% avg. error)
  - Not fast enough (hourly)
  - PTM only
- Two steps: local information collection by global manipulation
  - Statistical inference
  - Direct measurement
- Cardinality-Based TM Estimation (CBTM) – A balanced method



Scalability of Adaptive Counting

- *Root Mean Squared Error* (RMSE), reflects both bias and standard error
- Same memory (320Kbit) for three algorithms
- Cardinalities vary from 4K to 16M
- Scalable to both small cardinalities and large ones



Packet-Level and Flow-Level Internet Traffic Monitory for Worm and DDoS Flooding Control

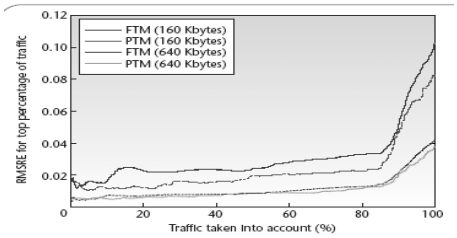


Figure 5. Root mean squared relative error (RMSRE) of packet-level (PTM) and flow-level traffic matrix (FTM) elements for various percentages of traffic. It is generally easier to accurately estimate large TM elements than small ones; accuracy improves significantly for PTM and FTM as the top percentage of traffic taken into account decreases.

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

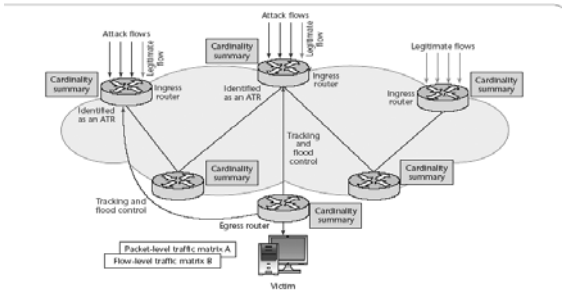
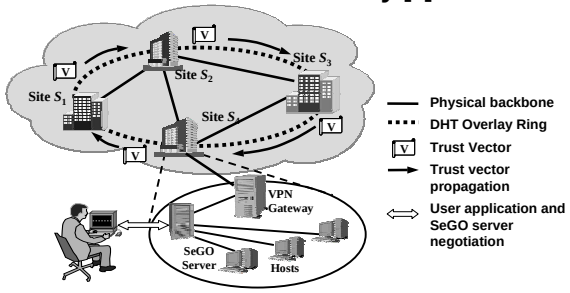


Figure 6. Traffic matrix monitoring for tracking attack-transit routers (ATRs). Collaborative routers can perform distributed tracking of ATRs by correlating the packet-level (PTM) and flow-level traffic matrix (FTM). Here, the egress router identifies two potential ATRs by correlating the PTM and FTM.

Hot Topics for Grid Security Research:

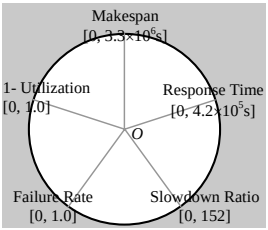
- The Fuzzy Trust Model for security binding and trust integration [3] and the Game-theoretic Model for modeling selfish and non-cooperative Grids [4].
- Large-scale security benchmark experiments on the NSF/HSD DETER testbed towards sustainable cybertrust in real-life Internet and Grid applications.
- Internet datamining for security control and for guarantee of Quality-of-Service in real-life applications – Interoperability between wired Grids and wireless Grids is a wide-open area.

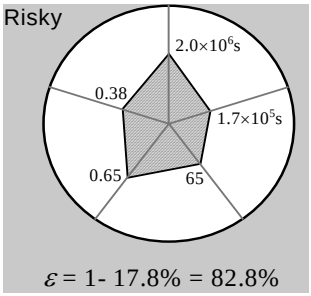
Fuzzy Aggregation for Trust Integration over a DHT Overlay [3]



Cooperating gateways working together to establish VPN tunnels for trust integration

Performance Metrics for Trusted Grid Computing

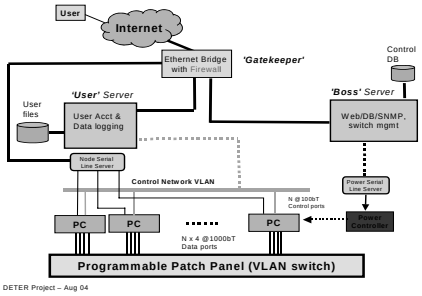




Effects of Fuzzy Trust Integration

ε = 1- 17.8% = 82.8%

DETER Testbed Benchmark Experiments



DETER Testbed funded by the National Science Foundation (NSF) and the Department of Homeland Security (DHS)

Final Remarks

- **The NetShield built with DHT-based security overlay networks support distributed intrusion and anomaly detection, alert correlation, collaborative worm containment, and flooding attack suppression.**
- **The CAIDS can cope with both known and unknown network attacks, secure many cluster/Grid/P2P operations in using common Internet services: telnet, http, ftp, Email, SMTP, authentication, etc.**
- **Automated virus or worm signature generation plays a vital role to monitor network epidemic outbreaks and to give early warning of large-scale system intrusions, network anomalies, and DDoS flood attacks. Extensive benchmark experiments on the DETER test bed will prove the effectiveness.**

Related Publications: (Download http://GridSec.usc.edu)

1. **M. Cai, K. Hwang, Y. K. Kwok, Y. Chen, and S. S. Song, "Fast Internet Worm Containment", *IEEE Security and Privacy*, May/June, 2005.**
2. **K. Hwang, Y. Chen, and H. Liu, " 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.**
3. **S. Song, K. Hwang, and Y.K. Kwok, " Trusted Grid Computing with Security Binding and Trust Integration", *Journal of Grid Computing, August, 2005***
4. **Y. K. Kwok, S. Song, and K. Hwang, "Selfish Grid Computing: Game Theoretic Modeling and NAS Performance Results", *ACM/IEEE CCGrid – 2005,* Cardiff, U.K., May 11, 2005**