Trusted Grid and P2P Computing:

Security Binding, Worm Containment, DDoS Defense, and New Research Frontiers and Approaches

Professor Kai Hwang

Internet and Grid Computing Laboratory
University of Southern California,
Los Angeles, California USA

Presentations at Shanghai Jiaotong University, June 27, 2005
and Univ. of Science and Technology of China, June 29, 2005

web site: http://GridSec.usc.edu/

Contributors at USC : Min Cai, Shanshan Song, Ricky Kwok,Yu Chen, Runfang Zhou, Ying Chen, and Xiaosong Lou

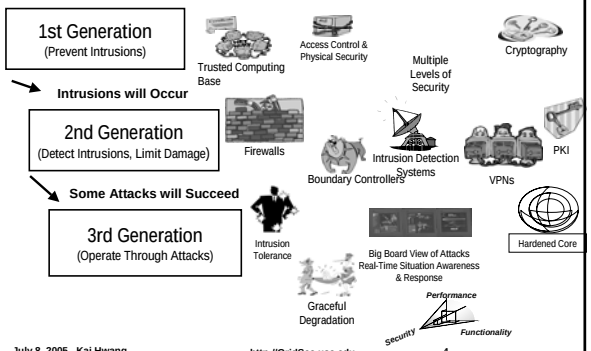
Presentation Outline:

- Internet, Grid, and P2P Computing Arena
- System and Network Security Requirements
- Collaborative Internet Worm Containment
- Cardinality Counting for DDoS Defense
- Other Hot Topics for Trusted Computing
  - Fuzzy Trust Model and Reputation Systems
  - Game-theoretic Modeling of Realistic Grids
  - Grid Performance Metrics and DETER Experiments
  - Interoperability between Wired and Wireless Grids
- Concluding Remarks and Relevant Publications

Security and Privacy Demands in Internet, Grid, and P2P Services [6]:

- Trusted E-Commerce over the Internet
- Secure communications in E-mail, FTP, etc.
- Protected download of digital contents (P2P)
- 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.

Three Generations of Defense Technology Towards Cyberspace Security Assurance



Worms and DDoS Attacks

- **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 or software vulnerability
  - Worms used to perform DDoS attacks automatically

Internet Epidemic Outbreaks in Recent Years

A pretty fast outbreak: Slammer (2003)

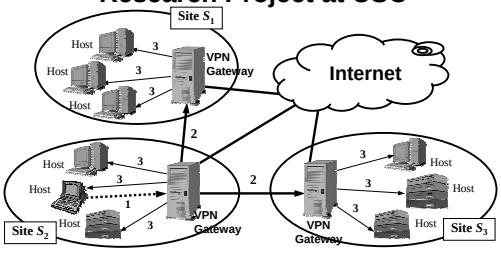
- First ~1min behaves like classic random scanning worm
  - Doubling time of ~8.5 seconds
  - CodeRed doubled every 40mins
- >1min worm starts to saturate access bandwidth
  - Some hosts issue >20,000 scans per second
  - Self-interfering (no congestion control)
- Peaks at ~3min
  - >55million IP scans/sec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

Minutes After the Initial Outbreak

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

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

The NetShield Architecture with Distributed Security Enforcement over a DHT Overlay

(IEEE *Security and Privacy Magazine*, May/June 2005 [1])

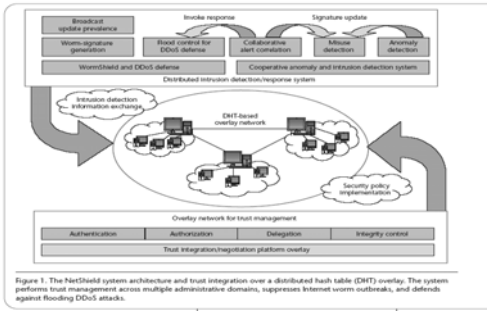


Figure 1. The NetShield system architecture and trust integration over a distributed hash table (DHT) overlay. The system performs trust management across multiple administrative domains, suppresses Internet worm outbreaks, and defends against flooding DDoS attacks.

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]

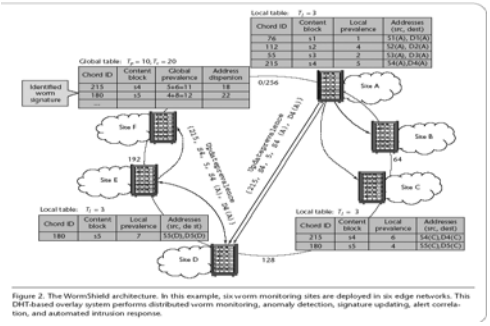
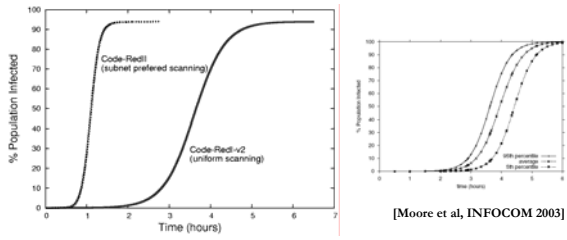


Figure 2. The WormShield architecture. In this example, six worm monitoring sites are deployed in six edge networks. This DHT-based overlay system performs distributed worm monitoring, anomaly detection, signature updating, alert correlation, and automated intrusion response.

Simulation Results

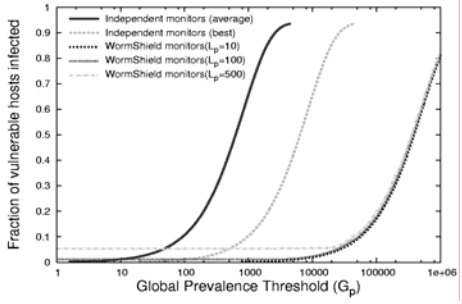
- Simulated CodeRed-like worms on an Internet configuration of 105,246 edge networks and 338,562 vulnerable hosts
- Use BGP table snapshot on July 19th, 2001 from RouteViews
- Simulated infection progress matches quite well with Moore's experimental results



[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

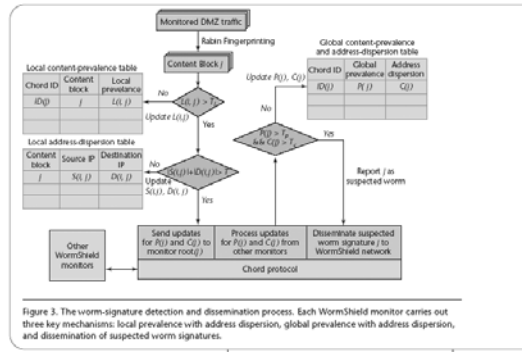
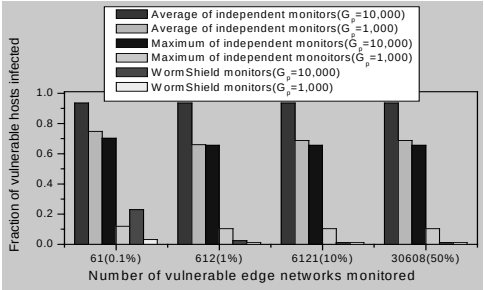


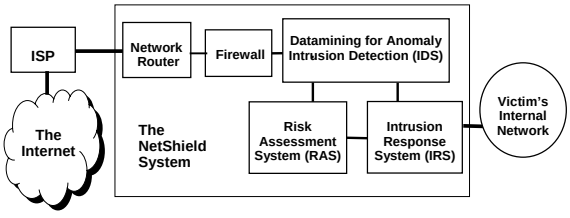
Figure 3. The worm-signature detection and dissemination process. Each WormShield monitor carries out three key mechanisms: local prevalence with address dispersion, global prevalence with address dispersion, and dissemination of suspected worm signatures.

Effects of % Edge Networks Monitored

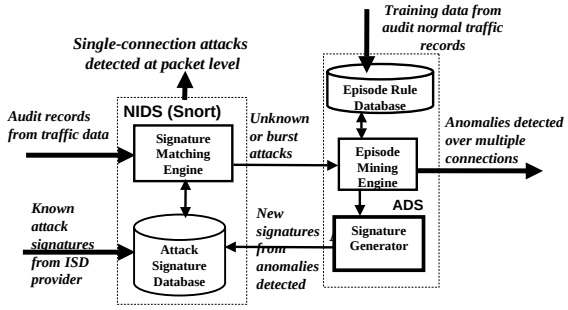
- **About 27 times reduction of infected hosts as 1% of vulnerable edge networks being monitored**



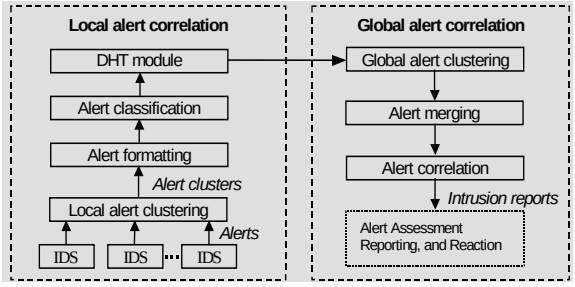
USC NetShield Intrusion Defense System for Protecting Local Networks of Grid Computing Resources



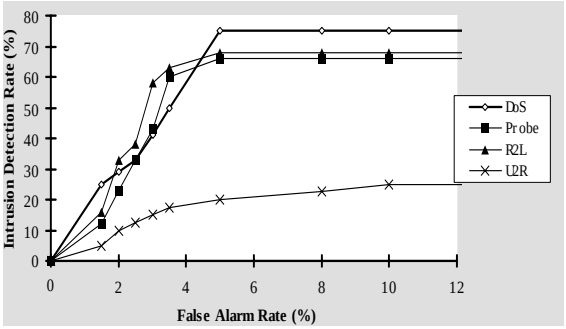
A Collaborative Anomaly and Intrusion Detection System (CAIDS), built with the Snort and a custom-designed Anomaly Detection System at USC Internet and Grid Computing Lab in 2004 [2]



Alert Operations performed in local Grid sites and correlated globally



ROC Curves for 4 Attack Classes on The Simulated CAIDS



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

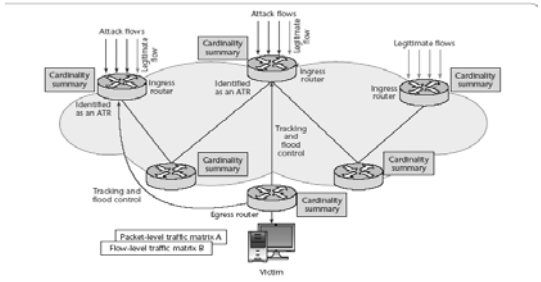
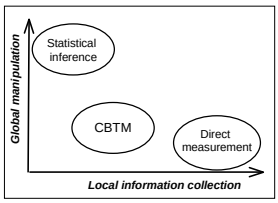


Figure 6. Traffic matrix monitoring for tracking attack-transit routers (ATRs). Collaborative routers can perform distributed tracking of ATRs by correlating the packet-level (PTM) and flow-level traffic matrix (FTM). Here, the egress router identifies two potential ATRs by correlating the PTM and FTM.

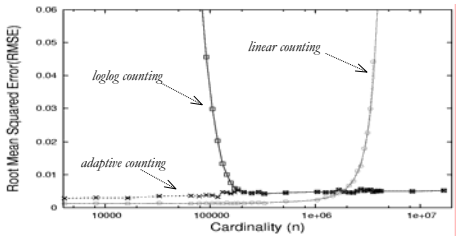
Cardinality-Based Traffic Matrix Estimation

- 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 errors
- Same memory (320 Kb) for three algorithms
- Cardinalities vary from 4K to 16M
- Scalable to cover small cardinalities and large ones



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

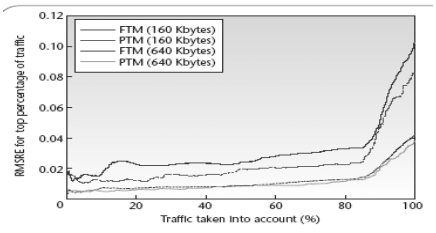


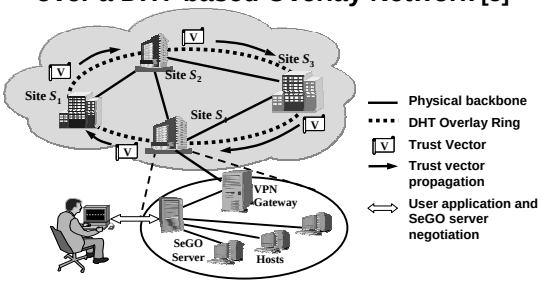
Figure 5. Root mean squared relative error (RMSRE) of packet-level (PTM) and flow-level traffic matrix (FTM) elements for various percentages of traffic. It is generally easier to accurately estimate large TM elements than small ones; accuracy improves significantly for PTM and FTM as the top percentage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

Other Hot Topics on Security Research

for Realistic Grid Platforms and P2P Networks:

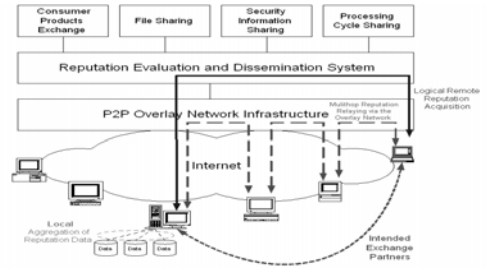
- Fuzzy trust Model for security binding in Grids [3] and reputation system for P2P services over the Internet [4]
- Game-theoretic Model for modeling selfish and non-cooperative Grids in real-life world [5].
- NSF/HSD DETER testbed – An isolated Internet simulator built at USC/ISI and UC Berkeley for Large-scale security benchmark experiments
- Interoperability between wired Grids and wireless Grids - a new challenge for pervasive Grid/P2P computing.

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



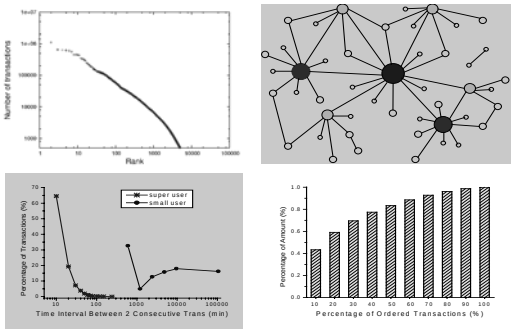
Cooperating gateways working together to establish VPN tunnels for trust integration

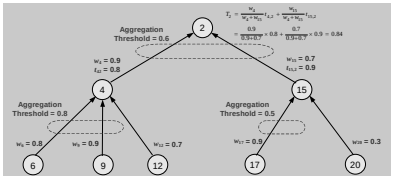
Trusted P2P Transactions with Fuzzy Reputation Aggregation [4]



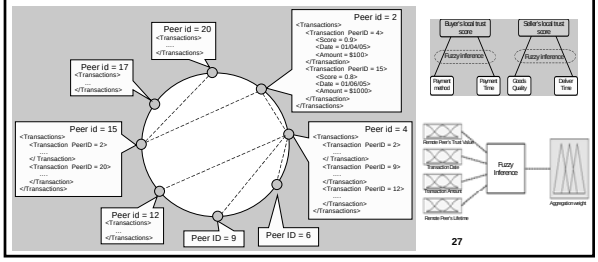
e-Trust: A peer reputation system built with a P2P overlay network for trusted commodity exchanges over the Internet, like eBay transactions

eBay transaction trace by ranks, hot spots, request interval, and transaction amounts.

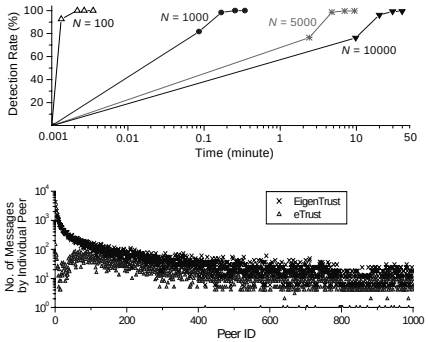




Trust Aggregation using Fuzzy Inferences

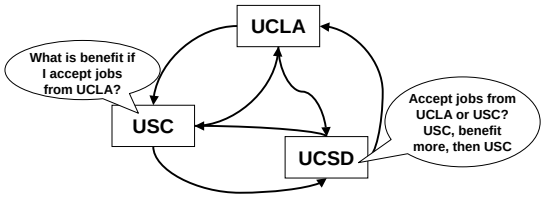


Simulated Performance of the eTrust system compared with the EigenTrust system in processing eBay traces

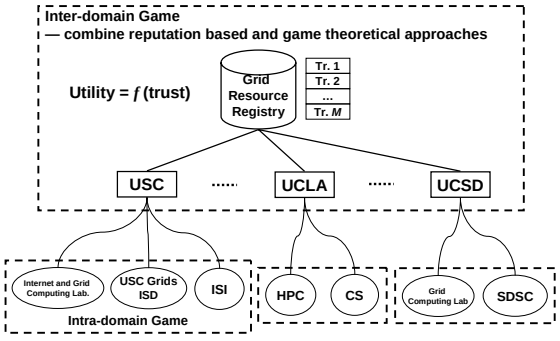


Game-Theoretic Approach to Solving the Selfish Grid Computing Problem

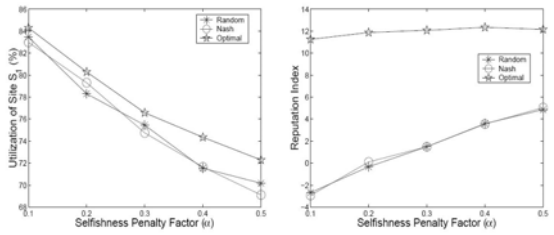
Game theory is intended to provide a theory of strategic behavior when all parties in the game interact directly, rather than through the third party, and with the goal to maximize all the individual benefits.



Hierarchical Grids

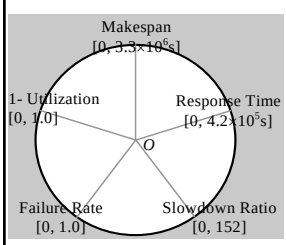


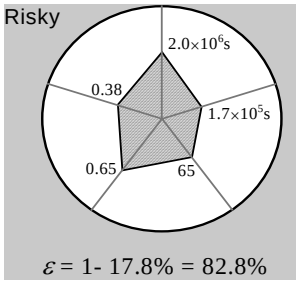
Grid Performance Enhancement
under Different Gaming Strategies



(e) Utilization (f) RI versus α

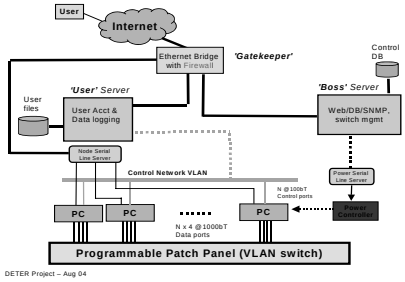
Performance Metrics for Trusted Grid Computing [6]





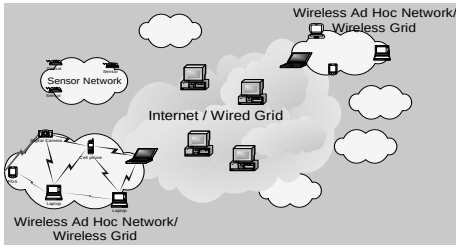
ε = 1- 17.8% = 82.8%

DETER Testbed Benchmark Experiments



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

Wired Grids vs. Wireless Grids
– The Interoperability Issues



- **Air interfaces, admission control, disconnection handling, wireless PKI, security binding, and QoS all demand extensive research and development**
- **Interoperability demands to support wired and wireless communications in distributed clusters, grids , and pervasive computing applications**

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 monitory, detection, and suppression.**
- **Extensive benchmark experiments on the DETER testbed will prove the effectiveness, still a long way to achieve assurance.**
- **Fuzzy trust model is effective to support distributed security enforcement in both computational Grids and P2P systems.**
- **Game-theoretic approach provides a viable solution to the selfish and non-cooperative problems in realistic network platforms**
- **Wireless Grids needed for pervasive applications must be built to be interoperable with existing wired backbone networks**

Related Publications:

(Download from 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. **S. Song, K. Hwang, R Zhou, and Y.K. Kwok, " Trusted P2P Transactions with Fuzzy Reputation Aggregation", *IEEE Internet Computing Magazine Special Issue on Security for P2P and Ad Hoc Networks*, submitted March 2005.**
5. **Y. K. Kwok, S. Song, and K. Hwang, "Selfish Grid Computing: Game Theoretic Modeling and NAS Performance Results", *ACM/IEEE Int'l Conf. on Cluster Computing and The Grids (CCGrid 2005),* Cardiff, U.K., May 9-12, 2005**
6. **K. Hwang, Y. Kwok, S. Song, M. Cai, R. Zhou, Yu. Chen, Ying. Chen, and X. Lou, "GridSec: Trusted Grid Computing with Security Binding and Self-Defense against Network Worms and DDoS Attacks", *Int'l Workshop on Grid Computing Security and Resource Management* (GSRM'05), in conjunction with the *ICCS 2005*, Emory University, Atlanta, May 22-25, 2005.**