

Brent ByungHoon Kang

The University of North Carolina at Charlotte
Department of Software Information Systems, College of Computing and Informatics
bbkang@uncc.edu 704-687-8440 (Office)

Professional Preparation:

- Ph.D., Computer Science, University of California at Berkeley, CA. (Fall 2004)
- GAANN Fellowship, University of California at Berkeley (January 2003 – May 2004)
- M.S., Computer Science, University of Maryland at College Park, MD. (Fall 1995)
- B.S., Computer Science and Statistics, Seoul National University, Seoul. (Spring 1993)
- Graduated first among 45 computer science majors, Seoul National University

Appointments:

- Assistant Professor, University of North Carolina at Charlotte, NC. (Fall 2004 - Current)
- TIAA CREF John H. Biggs Fellowship (2007)
- Graduate Student Researcher, University of California at Berkeley, CA. (Fall 1998 - Fall 2004)
- Research Staff, Lawrence Berkeley National Laboratory, CA. (Spring 1998)
- Software Engineer, Quark, Inc, Denver, CO. (Fall 1995 - Fall 1997)
- Graduate Teaching Assistant, University of Maryland at College Park, MD. (Fall 1993 - Spring 1995)

Recent Research, Teaching and Services Activities (2005 – 7/2009):

Research:

1. **Botnet Enumeration and Defense** (Supported by NSF/KISA/Verisign, 2007 to Present): In an effort to mitigate new decentralized botnets that are resilient to traditional server take-downs, Kang has explored a series of botnet mitigation approaches that are based on effectively and comprehensively enumerating malware-infected hosts, by developing fast and timely analysis methods to gain a deeper understanding of malware behaviors, for example, through the use of HoneyActor and Reversing Memoization, exploring the fundamental limits and weaknesses of the emerging use of decentralized Command & Control (C&C) networks such as peer-to-peer, and through introspecting Top-Level-Domain (TLD) registry changes to infer a set of domain names and IP addresses most likely to be associated with current and future malware activities.
2. Kang's research efforts are directed toward analyzing botnet protocols and designing an effective enumerator based on the analysis. The resulting knowledge and information will form a basis for creating an enumeration result list that contains (i) malware-infected hosts, both within and outside LAN, (ii) the command & control servers communicating with such infected hosts, and (iii) the drop sites or email accounts utilized to collect and store stolen or compromised information. The list can be used for spam blocking, firewall configuration, DNS rewriting, and alerting sys-admins regarding local infections. Kang's research team has been freely sharing the gained botnet protocol knowledge, the enumerators, and the enumeration results with cyber defender communities through closed mailing lists, direct contacts, and publications.
3. Kang's research team's initial result, shown in ASIACCS 09 paper, reported that more than 40% of bot-infected hosts in the Storm p2p botnet were behind firewall or NAT devices, implying that traditional crawler-based enumeration would miss out a significant portion of the botnet population because crawler by design cannot contact hosts behind firewall or NAT devices. Kang's research team has experimented with using a passive p2p monitor (PPM) that is able to join the botnet as

“routing-only nodes” to snoop the p2p traffics generated from the botnet, including those behind Firewall or NAT devices. The team developed a method to distinguish if a given infected host is behind such devices and further explored the number of PPM nodes that would be needed to fully enumerate the entire population of bot-infected hosts.

4. **Waledac (a next generation P2P botnet) Research:**

Kang and his Ph.D. student were the first to **fully decode and expose Waledac’s C&C architecture, protocols and operation details**, and shared the protocol details and released decryption tools to the defender community through private mailing lists in January 2009. Anti-virus vendors have used the team’s research result (<http://www.nnl-labs.com/cblog/>) to understand the nature of Waledac. (http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/infiltrating_the_waledac_botnet_v2.pdf). Waledac is a new and persistent P2P botnet that uses PKI (Public Key Infrastructure) to encrypt its C&C traffic among peer nodes, making the network highly resilient to any mitigation efforts.

Kang’s team is currently exploring ways to **sinkhole the entire Waledac p2p botnet** in close collaboration with VeriSign and iDefense (Summer 2009). Unlike the Storm botnet, Waledac’s main control servers (TSL servers) sign their commands using a private key, thus rendering ineffective a man-in-the-middle attack between the TSL and the botnet. However, Kang’s team found a way to “completely” fill up Waledac’s peer-routing-table with sinkhole servers’ IP addresses.

Once sinkholed, Waledac’s worker nodes (spammer nodes) will report to the sinkhole server rather than the Waledac repeater layer (nodes with public IP address). Kang’s research team will use this unique opportunity to experiment with the effect of DHCP churning and NATing on enumeration results. By running fingerprint tools, such as p0f SYN-mode at the sinkhole server, the team can uniquely identify each infected host, since IP address alone is insufficient to uniquely identify infected hosts in certain netblocks.

In July 2009, to the team’s surprise, the Waledac botnet started to change the AES key dynamically. Understanding the dynamic key change mechanism is an urgent and challenging task that Kang’s team is working on as of this writing.

5. **Conficker Research:** Conficker is a well-known mega-scale botnet that has P2P component in its C variants. Kang has been working with the **Conficker** Cabal group, an industry-wide partnership formed to defend against the botnet (<http://www.confickerworkinggroup.org/>). One of Kang’s current research tasks is to explore whether the continuous increase in the number of infected hosts is due to consistent new infections or mainly because of DHCP churning effect: the case where the same machine takes on different IP addresses over time. The number of Conficker A/B infected hosts in contact with sinkhole servers is still increasing. (2.5 million IP addresses in February 2009; now over 4.5 million infections). The team’s daily analysis of over 4TB of sinkhole log can be found in <http://spartanlaser.gtisc.gatech.edu/reports/>
6. **Honeynet Research:** Kang has been working with a group of students in the Information Assurance Cyber Corp Scholarship Program funded by NSF in analyzing malware and understanding botnet behaviors. The team explored the peer-to-peer Storm bot’s topology and its detection techniques. The initial result has been presented as the first opening paper in *USENIX First Workshop on Hot Topics in Understanding Botnets (HotBots)* and the paper has also been featured in [PC World](#), [E Week](#), [Tech World](#) and [Symantec News](#).
7. **RepuScore and Privilege Messaging** (Supported by NSF DUE, 2005-8): Kang and his Ph.D. student have proposed and designed a number of frameworks for mitigating email spam issues. RepuScore is a collaborative reputation framework where the receiver organizations report their reputation-view about a sender to a central authority that computes a global reputation for each

sender domain. RepuScore is designed to place the onus on the sender to take responsibility for the amount of unsolicited emails they transmit. By using globally-computed quantitative scores, receivers can configure a minimum threshold reputation for emails that they will accept. RepuScore and its SpamAssassin plug-ins that the team developed have been deployed at several organizations including ESP (Email Service Provider), a local IT company and a university (other than UNCC). <http://www.repuscore.org/>

8. With the support from the **TIAA-CREF John H. Biggs Faculty Fellowship** (2006-7), Kang explored a “premise-aware access framework” that provides a “syndicated approach” in which a collective interaction of entities governing data is required to enforce data access policies. The concept of premise-aware access refers to the principle that all confidential information be accessible to authorized persons only when they are on an organization’s premises, which is particularly applicable to institutions striving to meet regulatory compliance requirements.

In an effort to address IT infrastructure design and management for SOX (Sarbanes and Oxley) compliance, Kang has developed “regColl,” a tool that efficiently collects and monitors the registry of Windows machines so that IT managers can check the health of the deployed systems against possible malware/spyware infections.

Teaching and Research Mentoring:

1. As lead-PI, Kang led a week-long faculty development workshop on **Hands-On Cyber Games and Interactive Simulations**, funded by a two year grant from NSF. 19 faculty members from across states attended the workshop conducted by UNCC in collaboration with NC A&T, a HBCU in the region. The workshop examined the use of cyber games and interactive simulations in IA education, exploring network security exploits and defense techniques. The feedback from the faculty members who took part were extremely positive; all quoted plans to incorporate the material into their IA curriculum. (<http://www.sis.uncc.edu/cybergames/download.html>)
2. Kang served as a panelist on the Information Assurance (IA) Education Panel at the **Usenix Workshop on Cyber Security Experimentation and Test (CSET 2008)**.
<http://www.usenix.org/events/cset08/tech/>
3. Kang created a series of new courses on **IT Infrastructure Design and Implementation** at UNCC. Topics include the network systems design for cyber defense, distributed systems principle, IT infrastructure design for compliance, systems recovery and secure email architecture. Kang developed the **Hands-on IT Design Exercise for Cyber Defense** based on VM as part of class components.
4. Dept. Chair also noted that the emphasis on hands-on component in Dept’s IA curriculum **has contributed to the strong enrollments**.
5. In 2009, UNCC team won **1st place in Regional CCDC Competition, March 2009**. Kang has served as a faculty advisor for UNC Charlotte since 2006. Most of the team members are/were also advised by Kang through research projects.
6. In 2006, UNCC team won **the national championship at the inaugural CCDC (Collegiate Cyber Defense Competition)**, held at San Antonio and sponsored by DHS ARPA, 2006. CCDC competition focuses on network systems administration and defense.

7. Kang was nominated for the **Bank of America Award for Teaching and Excellence** (2008). The memo from the Dean's office stated " ... being nominated by your peers and/or students for such a prestigious award brings a wonderful recognition to the College of Computing and Informatics ... " Also, Kang's dedication to teaching has been recognized with high ratings by students' evaluations, notably by receiving the highest score in the category: "Instructor shows enthusiasm in lecture" in all classes that he has taught.

Services:

1. Proposal Reviewer for *NSF Panel on Trusted Computing (TC) Program 2009*; Proposal Reviewer for *NSF Computing Research Infrastructure (CRI) Program 2007 and 2008*; Proposal Reviewer for *AFOSR 2009 (Anti-Spam Topic)*; Invited to be Proposal Reviewer for *The Natural Sciences and Engineering Research Council of Canada (NSERC) 2009 – sort of Canadian NSF (Botnet Security)*.
2. Program Committee Member for *Usenix Conference on Large Installation System Administration (LISA) 2008 and 2009*; Chair for the *System Administrator Education Workshop* and Coordinator of the *Posters and Work-In-Progress Sessions at LISA 2007*.
3. Program Committee Member for *CEAS (Conference on Email And Spam) 2009*, *CSET (Workshop on Cyber Security Experimentation and Test) 2009*, *NPSEC (Workshop on Secure Network Protocols) 2009*, and *SecureComm (Conference on Security and Privacy in Communication Networks) 2009*.
4. External Reviewer for *IEEE Security & Privacy Oakland Conference 2008*; Reviewer for the *Springer Journal of Intelligent Information Systems 2009*, *IEEE Transactions on Services Computing*, and *Usenix File and Storage Systems (FAST), 2005*.
5. Member of the *IT Infrastructure Committee* at UNC Charlotte, offering technical advice on IT infrastructure issues relating to the department and college (2005 to present).
6. Served on the *Undergraduate Curriculum Committee* for the SIS Dept., and coordinated the College of Computing and Informatics' Seminar in Fall 2006.
7. *Usenix* Representative for UNC Charlotte (2004 to present).
8. Faculty PI for *Planet-Lab Consortium* (Fall 2004 to present) www.planet-lab.org.
9. *Bank of America Teaching Award* Preparation Committee Member (Academic Affairs appointed group, Fall 2005).
10. *New Faculty Orientation Week* Committee Member. (Academic Affairs appointed group. Kang's suggestions regarding the web site structure have been instrumental and have received acknowledgement from staff and new faculty members.)
11. Member of the *Faculty Center for Teaching and e-Learning* Review Committee (Spring 2007; Academic Affairs appointed group).

Research Funding (Peer-Reviewed):

1. NSF CNS 0855067 Spam Processing, Archiving, and Monitoring Community Facility (SPAM Commons), PI (100%), \$120,000.00, 9/1/2009 – 8/31/2012, Awarded in FastLane 8/28/2009.
2. NSF DUE 0920179 Hands-on exercises on DETER testbed for security education, PI (100%), \$98,627.00, 9/15/2009 – 9/14/2011, Awarded in FastLane 9/8/2009.

3. NSF CNS 0845937 CAREER: Understanding Malware and Its Infected Hosts Enumeration and Mitigation, PI (100%), \$638,259.00, 2009 – 2014, Pending in FastLane as of 8/31/2009. (The proposal was submitted in July 2008.)
4. NSF DUE0723808 Focused Faculty Development Workshop on Cyber Games and Interactive Simulations, B. Kang (Lead-PI), B. Chu, G. Ahn*, with NC A&T A. Yu, K. Williams, X. Xu, D. Yuan. Awarded, 9/2007 – 9/2009, Total \$466,993 (UNCC \$240,000, NC A&T SU \$226,993),
 “The panel sees this proposal as creative and innovative. It has quite a few merits. ... The related work is impressive. ... The emphasis on lab design is practical and well justified. The format of collaboration is just right.”
5. NSF DUE0830624 Carolina Cyber Defense Scholarship, B. Chu (PI), B. Kang (Co-PI), X. Wu, G. Ahn*, and T. Holt*, 9/2008 - 9/2012, Awarded, \$1,194,140.
 As co-PI, Kang led and advised the research projects for the students with cyber defense scholarships. (Co-PIs marked with * no longer work on the projects.)
6. NSRI/ETRI (Electronics and Telecommunications Research Institute) - Case Studies on Botnet-Infection Assessment, PI (100%), 8/2009 – 6/2010, Awarded, \$53,435.
7. KISA (Korea Information Security Agency) - A000488301, Detecting, Monitoring and Attacking Peer to Peer Botnets, PI (100%), 8/2008 – 2/2009, Awarded, \$15,000.
 KISA is a government agency that aims to establish a safe and reliable information society through the development and support of information security related technology. (Call For Proposal was issued on www.kisa.or.kr, peer-reviewed and evaluated.)
8. TIAA-CREF John H. Biggs Fellowship, \$7,000 + (\$3,080 UNCC overhead matching), PI (100%), Awarded, 2007. Peer-reviewed.
9. UNCC Faculty Research Grant, UNC Charlotte, (\$6,000), PI (100%), 2005. Awarded, Peer-reviewed.

Other Grants and Supports:

10. Verisign (iDefense) grant, 2008- current, \$20,000 + 1 Ph.D Support. B. Kang.
11. iDefense supported PI’s research by providing 1Ph.D student support and \$20,000.
12. Bank of America IT Security, Plausible Scenarios of Catastrophic Cyber Events Project, Project-lead. (Participants: J. Dominick, W. Wang, Y. Wang, and B. Chu) 8/2008 – 12/2008, \$40,000
 Kang led this project team from beginning to the end, and served as main technical contact person on behalf of the team. Kang wrote 8 scenarios out of 12 scenarios in the final reports, put together and edited what other members in the team have submitted, advised team of students in this project, and created the project report in dynamic web content in addition to final report.
13. HoneyNet (Malware) Research Project, Bank of America, (\$35,000), Co-PI, 2005-2007
14. IntePoint Junior Faculty Fellowship, IntePoint Inc., (\$12,500), PI (100%), 2005-2006
15. Support-Intelligence, Co-lo server access, 2008, B. Kang.
16. IBM, Co-lo server access, 2009, B. Kang.

Research Impact:

Malware research results and impact on real world:

1. Kang has explored a series of botnet mitigation approaches directed toward **analyzing botnet protocols** and **designing an effective enumerator** based on the analysis. The resulting enumerations are used for spam blocking, firewall configuration, DNS rewriting, and alerting sys-admins regarding local infections through email and direct contacts.
(The team also notified ITS at UNCC when infections were found at the UNC Charlotte Network and other UNC universities.)
2. When you **search for “Waledac Protocol” on search engines such as google, our research blog on Waledac appears at the top.**
<http://www.google.com/search?q=Waledac+Protocol>
3. Anti-virus vendors (such as TrendMicro report) have used the team’s research result to understand the nature of Waledac protocol.
4. The work on **Storm peer-to-peer botnet**, and the initial results were presented as the first opening paper in *USENIX First Workshop on Hot Topics in Understanding Botnets (HotBots)*.
5. When you **search for “peer to peer botnet” on search engine such as google, our HOTBOT 07 paper appears at the top.**
<http://www.google.com/search?q=peer%20to%20peer%20botnet>.
6. The paper has been featured in *PC World*, *E Week*, *Tech World* and *Symantec News*.
7. **Google Scholar shows 81 citations**
<http://scholar.google.com/scholar?cites=2048079897991465875&hl=en>
ACM portal shows citations by ACM publications.
<http://portal.acm.org/citation.cfm?id=1323129&dl=GUIDE&coll=GUIDE&CFID=49600286&CFTOKEN=93914426>
8. The HOTBOT07 paper was also cited in the CRS Report for Congress “Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress”
<http://openers.com/document/RL32114/2008-01-29/>
9. The Conficker research result is being used by defender community for tracking and assessing the Conficker malware infections.
<http://spartanlaser.gtisc.gatech.edu/reports/>
10. Recently, the cyber defense organizations in the countries such as Korea and Spain have asked Kang to assess the botnet infections in their countries.

Anti-spam research impact on real world:

11. RepuScore and its SpamAssassin plug-ins have been **deployed at several organizations including an ESP (Email Service Provider), a local IT company, and a college in Oregon** (<http://www.repuscore.org/>).

12. Kang's work on Privilege Messaging was **presented as the opening paper at USENIX Conference on Large Installation System Administration (LISA) in 2007.**

Previous work on decentralized data concurrency and security:

<http://scholar.google.com/scholar?q=brent+byunghoon+kang>

13. This dissertation work has been published in the Proceedings of 23rd International Conference on Distributed Computing Systems, "Hash History Approach for Reconciling Mutual Inconsistency,"
14. This paper has been cited by 34 other publications, according to Google Scholar, as of Aug 31st 2009. <http://scholar.google.com/scholar?q=brent+byunghoon+kang>

Publications (Refereed):

1. "The Waledac Protocol: The How and Why," G. Sinclair, C. Nunnery, B. Kang, Proceeding of 4th IEEE International Conference on Malicious and Unwanted Software (Malware 2009).
2. "Towards Complete Node Enumeration in a Peer-to-Peer Botnet," **B. Kang**, E. Chan-Tin, C. Lee, J. Tyra, H. Kang, C. Nunnery, Z. Wadler, G. Sinclair, N. Hopper, D. Dagon, and Y. Kim, ACM Symposium on Information, Computer & Communication Security (ASIACCS), 2009 <http://portal.acm.org/citation.cfm?id=1533064>
3. "Tracking Email Reputation for Authenticated Sender Identities," G. Singaraju, J. Moss and **B. Kang**, Fifth Conference on Email and Spam (CEAS), 2008 <http://www.ceas.cc/2008/papers/ceas2008-paper-33.pdf>
4. "Interactive simulation tools for information assurance education", H. Yu, K. Williams, J. Xu, X. Yuan, B. Chu, **B. Kang**, T. Kombol, Proceedings of ACEIS 2009: The Second Annual Conference on Education in Information Security
5. "Concord: A Secure Mobile Data Authorization Framework for Regulatory Compliance," G. Singaraju and **B. Kang**, USENIX 22nd Large Installation System Administration Conference (LISA), 2008 http://www.usenix.org/event/lisa08/tech/full_papers/singaraju/singaraju.pdf
6. "RepuScore: Collaborative Reputation Management Framework for Email Infrastructure," G. Singaraju and **B. Kang**, Accepted to USENIX 21st Large Installation System Administration Conference (LISA), 2007 http://www.usenix.org/events/lisa07/tech/full_papers/singaraju/singaraju.pdf
7. "Peer-to-Peer Botnets: Overview and Case Study," J. Grizzard, V. Sharma, C. Nunnery, **B. Kang**, and D. Dagon, USENIX First Workshop on Hot Topics in Understanding Botnets (HotBots), 2007 http://www.usenix.org/events/hotbots07/tech/full_papers/grizzard/grizzard_html/. This paper was also featured in [PC World](#), [E Week](#), [Tech World](#) and [Symantec News](#).
8. "Privilege Messaging: An Authorization Framework over Email Infrastructure," **B. Kang**, G. Singaraju, and S. Jain, USENIX 20th LISA, 2006 http://www.usenix.org/events/lisa06/tech/full_papers/kang/kang.pdf
9. "RegColl: Centralized Registry Framework for Infrastructure System Management," **B. Kang**, V. Sharma, and P. Thanki, USENIX 19th LISA, 2005 http://www.usenix.org/events/lisa05/tech/full_papers/kang/kang.pdf

10. "Hash History Approach for Reconciling Mutual Inconsistency," **B. Kang**, R. Wilensky, J. Kubiatiowicz, Proceedings of 23rd International Conference on Distributed Computing Systems, 2003
https://oceanstore.cs.berkeley.edu/publications/papers/abstracts/hh_icdcs03_kang.html
11. "Network Support for Mobile Multimedia using a Self-adaptive Distributed Proxy," Z. Mao, H. So, **B. Kang**, and R. Katz, Proceedings of 11th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV), 2001
<http://portal.acm.org/citation.cfm?id=378360&coll=portal&dl=ACM>
12. "Toward a Model of Self-administering Data," **B. Kang** and R. Wilensky, Proceedings of the first ACM/IEEE-CS Joint Conference on Digital Libraries (JCDL), 2001
<http://portal.acm.org/citation.cfm?doid=379437.379703>

In Submission:

1. "Technologies for Node Enumeration in a Second Generation Peer-to-Peer Botnet," C. Nunnery, G. Sinclair, C. Lee, **B. Kang**, in submission, Aug 2009
2. "RepuScore: An Open Source Email Reputation Framework," G. Singaraju and **B. Kang**, in review 2009, ACM Transaction on Internet Technology (TOIT)
3. "Enumeration of Decentralized Botnets," C. Nunnery, G. Sinclair and B. Kang, in preparation for submission 2009, ACM Transaction on Internet Technology (TOIT)

Book Chapter: (Refereed)

"Decentralized Peer-to-Peer Botnet Architectures," B. Kang and C. Nunnery, Book Chapter: "Advances in Information & Intelligent Systems", 2009 Springer Studies in Computational Intelligence, SCI 251, pp. 251–264. Springer-Verlag Berlin Heidelberg 2009

Dissertation:

B. Kang, Ph.D. Dissertation, "[S2D2: A Framework for Scalable and Secure Optimistic Replication](http://www.eecs.berkeley.edu/Pubs/TechRpts/2004/5917.html)." UC Berkeley TechReport, UCB/CSD-04-1351, <http://www.eecs.berkeley.edu/Pubs/TechRpts/2004/5917.html>

Committee: Robert Wilensky (Chair), John Kubiatiowicz, Eric Brewer, and John Chuang

Kang worked on **Summary Hash History ("SHH")** as part of his dissertation research at the University of California at Berkeley. SHH is a secure decentralized update tracking mechanism that was designed by him to figure out the exact sets of updates to be exchanged during pair-wise data synchronization in a tamper-proof manner. Kang's dissertation research in large-scale distributed data synchronization and replication has been expanded into designing a secure synchronization protocol for WinFS, a next generation Windows File Systems. In collaboration with Microsoft Research, this work will potentially impact the data replication mechanism in Active Directory and the shared folder replication in Windows servers in the next release of Windows File Systems.

This dissertation work has been published in Proceedings of 23rd International Conference on Distributed Computing Systems, "Hash History Approach for Reconciling Mutual Inconsistency". According to google scholar, as of Aug 31st 2009, this paper has been "cited by 35 other publications" <http://scholar.google.com/scholar?q=brent+byunghoon+kang>.

Refereed Poster/Demo and Work-In-Progress:

- G. Sinclair, B. Kang, Work-in-Progress Session, “Challenges in Sinkholing a Resilient P2P Botnet (Is It Possible or Not?)”, Usenix Security 2009, <http://www.usenix.org/events/sec09/wips.html>
- C. Nunnery, B. Kang, V. Sharma, and J. Grizzard, Poster Session, “Locating Zombie Nodes and Botmasters in Decentralized Peer-to-Peer Botnets” Usenix Security 2007, <http://www.usenix.org/events/sec07/poster.html>
- B. Kang, V. Sharma, P. Thanki, and G. Singaraju, Demo/Poster Session, Vsync: “A Version-based Unidirectional Synchronization Tool”, Second Workshop on Real, Large Distributed Systems (WORLDS '05)
- B. Kang, Poster/Work-in-Progress Session, “Can Replicas Converge across Partitioned Networks”, 3rd USENIX File and Storage Systems 2004, San Francisco <http://www.usenix.org/events/fast04/wips/>
- B. Kang, Poster Session, “A Scalable and Secure Approach for Decentralized Ordering”, 19th Symposium on Operating Systems Principles (SOSP-2003), October 19-22, 2003, Bolton Landing, NY, USA
- B. Kang, Work-in-Progress Session, “A Hash-History Based Approach to Management of Weakly Consistent Replicas”, 18th Symposium on Operating Systems Principles (SOSP-2001), October 21-24, 2001, Banff, Canada

Invited Talks:

- ASIACCS Conference Talk, March 2009, “Toward Complete Enumeration of a P2P Botnet”
- KISA Seminar, January 2009, “Detecting, Monitoring and Mitigating Peer to Peer Botnets”
- SNU (Seoul National University) Seminar, January 2009, “Accurate Enumeration of P2P Botnet”
- North Carolina Systems Administrators Organization (NC*SA) Invited Talk, <http://www.ncsysadmin.org/>, June 2006, “Privilege Messaging & Reputation Services”
- LISA Conference Talk, Dec 2006, “Privilege Messaging: An Authorization Framework over Email Infrastructure”
- UNCC COIT Seminar, 2005, “Research on IT Infrastructure Systems and Services”
- Lawrence Berkeley National Laboratory, Invited Talk, 2004, “S2D2 Framework for Scalable and Secure Optimistic Replication”
- Microsoft Invited Talk, 2004, “S2D2 Framework for Scalable and Secure Optimistic Replication”
- P2P Seminar, 2003, “Summary Hash History for Scaling Secure Optimistic Replication”
- ICDCS Conference talk, 2003, “Hash History Approach for Reconciling Mutual Inconsistency”
- Berkeley Tahoe Retreat, 2002, “Scalable Hash History Approach for Optimistic Replication”
- JCDL Conference talk, 2001, “Toward a Model of Self-administering Data”
- RIDT Conference talk, 1998, “Unified Table Approach for Typographic Rendering”

Patents:

Utility Patents:

- “System for Adjusting Spacing between Adjacent Characters and Method”- Quark, Inc., Denver, CO, on April 21, 1997; Sole Inventor.

Provisional Patents:

- Mobile Advertisement Provision and Verification Framework, USPTO Appl No. 60/749,166, 1/23/2006. Notably, this idea won the top-10 finalist position at Five Venture Competition at Charlotte, April, 2006. Utility patent in progress by UNC Charlotte.
- Concord: A Framework for Securing File Access for a Partially Trusted Server and Revocable Client, 11/14/2005.

Media Coverage:

- WSOC TV Channel 9 news, March 2009: Kang's botnet and malware research efforts were aired on WSOC news and also appeared on WSOC's news web site: <http://www.wsoc.tv/news/19060258/detail.html#->
- UNCC Magazine, Fall 2007: Highlighted Kang's research on cyber security.
- International Bank Fraud Newsletter Article, "Botnets: An Avenue to Cyber Crime and Fraud": Featured Kang's research work on botnet malware.

Thesis and Qualification Exam Committee:

- Gautam Singaraju, Ph.D. Dissertation (Chair), 2009.
- Chris Nunnery, Ph.D. Qualification Exam, 2009.
- Greg Sinclair, Ph.D. Qualification Exam, 2009.
- Aritra Dasgupta, Ph.D. Qualification Exam, 2008.
- Vikram Sharma, M.S. Thesis, 2007.
- Graduate Faculty Representative for the Doctoral Committee of J.W. Jeong, Dept. of Applied Mathematics, Advisor, Prof. H.S. Oh, 2007

Students Advised and Graduated:

- Gautam Singaraju, Ph.D, Graduated Summer 2009. Dept-TA/NSF support.
- Chris Nunnery, Ph.D, Started 2008, GAANN Fellowship.
- Greg Sinclair, Ph.D. Started 2008, iDefense (Verisign) support.
- Jonathan Blanton, M.S./(Ph.D) Started 2008 - . NSF support.
- Zachariah Wadler, M.S. Graduated 2009. (Employed by DoE)
- Jonathan Peterson, M.S. Graduated 2009. (Employed by DoD)
- Jonathan Lavender, M.S. Graduated 2008. (Employed by NSA)
- Dennis Underwood, M.S. Graduated 2008. (Employed by NSA)
- Joshua Soles, M.S. Graduated 2009. (Employed by US Army CERDEC (Communications-Electronics Research, Development, and Engineering Center))
- Adam Wenner, M.S. Graduated 2009. (Employed by Federal Reserve Bank)
- Vikram Sharma, M.S. Thesis Graduated 2007. (A Start-up Venture)
- Pratik Thanki, M.S. Graduated 2006, (Bank of America Systems Group)
- Srivathsan Varadarajan, M.S. Graduated 2006, (TIAA-CREF I.T. Systems Group)
- Carson Black, M.S. Graduated 2006, (Vanguard Network Applications Group)
- Sumeet Jain M.S. Graduated 2006, (Software Solutions Lab.)