

## **Brent ByungHoon Kang, Ph.D.**

After receiving his Ph.D. in computer science from U.C. Berkeley, Dr. Kang joined the Dept. of Software and Information Systems that was only 2 years old but rapidly growing with tremendous potential. In line with the Dept.'s strategic goal of creating an excellent education and research program in IT system and security, Dr. Kang has focused his teaching, research and services efforts in addressing challenging problems in IT infrastructure design and administration security, particularly relating to botnets (malware), email spam, and data access compliance.

### **Teaching Activities**

Kang has created an innovative hands-on IA (Information Assurance) education program on infrastructure system security administration. Toward this effort, NSF has awarded Kang with a two-year grant stating that "the panel sees this proposal as creative and innovative ... The related work is impressive. ... The emphasis on lab design is practical and well justified ..." Kang's efforts were also recognized by the research community on cyber security experimentation and testbeds. In 2008, he was invited to be on a panel on the Information Assurance (IA) Research and Education panel at the Usenix Cyber Security Experimentation and Test (CSET 2008). In 2009, NSF awarded Kang a new grant to support the creation of hands-on materials for research training on DETER, a network security testbed. Kang has been actively serving as research advisor to students in the Information Assurance Scholarship for Service Program funded by NSF. Kang has supported and advised four Ph.D. students and eleven M.S students.

1. Kang has **created an innovative hands-on IA (Information Assurance) education program on IT security administration**. He designed a series of highly interactive exercises in which students are asked to build IT network infrastructures and services while managing and defending against realistic cyber attacks. Students design, build, and maintain IT network infrastructure systems and services, including domain name systems, web servers, email services, network file systems and directory services. At the same time, students are required to defend their infrastructure services against pseudo network attacks conducted by class instructors and volunteer security professionals.

Dept. Chair also noted that the emphasis on hands-on component in Dept's IA curriculum has **contributed to strong enrollment**.

2. From 2007 to 2009, Kang (as lead-PI) led a week-long faculty development workshop on Hands-On Cyber Games and Interactive Simulations, funded by 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.**
3. In 2008, Kang served as an invited panelist on the **Information Assurance (IA) Education Panel** at the Usenix Workshop on Cyber Security Experimentation and Test (CSET 2008).
4. In 2009, Kang received a further NSF grant, in collaboration with USC (University of Southern California), to support creating new hands-on materials for research training on **DETER, a network security research testbed**.
5. In 2009, UNCC team won **1st place in Regional CCDC Competition, March 2009**. CCDC competition focuses on network systems administration and defenses. Kang has served as a faculty advisor for UNC Charlotte. Most of the team members are/were also advised by Kang through research projects. 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.
6. 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 overall high ratings by students' evaluations, notably receiving the highest score in the category: "Instructor shows enthusiasm in lecture" in all classes that he has taught. Class evaluations by senior faculty members also reported, "Kang is confident, knowledgeable, organized, and very approachable" and "the hands-on labs are an exciting part of the course."

## Research Activities

1. **Botnet Enumeration and Defense** (Supported by NSF, ETRI, KISA, and 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 directed toward **analyzing botnet protocols** and **designing an effective enumerator** based on the analysis. The resulting enumeration would be used for spam blocking, firewall configuration, DNS rewriting, and alerting sys-admins regarding local infections.

Kang and his students are currently researching fast and timely analysis methods to gain a deeper understanding of malware behaviors, exploring the **fundamental limits and weaknesses of the emerging use of decentralized Command & Control (C&C) networks** (e.g., peer-to-peer), and **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. Kang's research team has been sharing the gained botnet protocol knowledge, the enumerators, and the enumeration results with cyber defender communities through closed mailing lists, direct contacts, and publications.

Kang's research team, in collaboration with the University of Minnesota and Georgia Tech, has also experimented with using a **passive p2p monitor (PPM)** that is able to join botnets as "routing-only nodes" to snoop the p2p traffics generated from the botnet, including those behind Firewall or NAT devices. This was because the team found that more than 40% of bot-infected hosts in p2p botnets (e.g., Storm) were behind firewall or NAT devices, implying that traditional crawler-based enumeration would miss a significant portion of the botnet population. The team developed a method to distinguish whether 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. This work was published in *ACM Symposium on Information, Computer & Communication Security (ASIACCS) 2009*.

Kang has also collaborated with Georgia Tech to understand the topology and architecture of the **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)*. The paper has been featured in [PC World](#), [E Week](#), [Tech World](#) and [Symantec News](#).

2. **Waledac (a next generation P2P botnet) Research:** Waledac is a new and persistent P2P botnet that uses PKI (Public Key Infrastructure) to encrypt its C&C(Command & Control) traffic among peer nodes, making the network highly resilient to defenders' mitigation efforts. Kang and his Ph.D. student were **the first to fully decode and expose Waledac's C&C architecture, protocols and operation details**, and released the protocol details and decryption tools to the defender community through private mailing lists in January 2009. Anti-virus vendors have used the team's research result to understand the nature of Waledac. This ongoing work was recently accepted to appear in the *4th International Conference on Malicious and Unwanted Software (Malware 2009)*, with the following comments from the reviewers: "...**Well written, and fascinating reading...**", "...**it's a very good paper (the best one I reviewed)...**", "The paper is written very well. It covers all details about the communication protocol the Waledac worm uses, starting with it's C&C structure, the hierarchy as well as protocol messages...". Kang's team, in collaboration with VeriSign, is currently exploring ways to sinkhole the entire Waledac p2p botnet.
3. **Conficker Research:** Kang has been working with the Conficker Cabal group, an industry-wide partnership formed to defend against the Conficker 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 team's daily analysis of over 9TB (TeraBytes) of sinkhole log can be found in <http://spartanlaser.gtisc.gatech.edu/reports/>

4. **Media Coverage:** Kang's botnet and malware research efforts were featured in the *International Bank Fraud Newsletter Article*, "Botnets: An Avenue to Cyber Crime and Fraud", as well as in UNCC Magazine's Fall 2007 issue. Kang's work was also aired on WSOC TV's Channel 9 Evening News on March 31, 2009. (<http://www.wsoc.tv/news/19060258/detail.html#->).
5. **RepuScore and Privilege Messaging** (Supported by NSF DUE, 2005-8): Dr. Kang has explored and designed a number of frameworks geared towards mitigating email spam issues. One such framework is RepuScore, a collaborative reputation framework that Kang and his Ph.D. student developed, where receiver organizations report their reputation-view about a sender to a central authority that computes a global reputation ("RepuScore") for each sender domain. By using the globally-computed quantitative scores, receiver organizations are able to configure a minimum threshold reputation for the sender domains from which they are willing to accept emails. Kang's **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/>). This work was published in LISA and CEAS conferences and **the previous work on privilege messaging was presented as the opening paper at USENIX Conference on Large Installation System Administration (LISA) in 2007.**
6. With the support from the **TIAA-CREF John H. Biggs Faculty Fellowship** (2007), 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. Premise-aware access is particularly applicable to institutions striving to meet regulatory compliance requirements such as SOX (Sarbanes and Oxley). This work was published as "Concord: A Secure Mobile Data Authorization Framework for Regulatory Compliance." in LISA 2008.

### Services Activities:

As Kang's research and teaching efforts began to gain recognition by the research and academic communities, he has been invited to serve on a number of proposal review panels, including NSF, AFOSR, and NSERC. He has also served on the program committee for publication venues in the areas of anti-spam, malware, and systems administration, as well as serving on many University committees.

- **Proposal Reviewer:** NSF Panel on Trusted Computing (TC) Program 2009, NSF Computing Research Infrastructure (CRI) Program 2007 and 2008; **Proposal Reviewer:** AFOSR (Air Force Office of Scientific Research) 2009 (Anti-Spam Topic); **Proposal Reviewer:** The Natural Sciences and Engineering Research Council of Canada (NSERC) 2009 (Botnet Security).
- **Program Committee Member:** Usenix Conference on Large Installation System Administration (LISA) 2008 and 2009; **Chair of the System Administrator Education Workshop** and Coordinator of the Posters and Work-In-Progress Sessions at LISA 2007. **Program Committee Member:** CEAS (Conference on Email And Spam) 2009, CSET (Workshop on Cyber Security Experimentation and Test) 2009, NPSEC (Workshop on Secure Network Protocols) 2009, SecureComm (Conference on Security and Privacy in Communication Networks) 2009, and Malware (International Conference on Malicious and Unwanted Software) 2010. **Reviewer:** IEEE Security & Privacy Oakland Conference 2008, Springer Journal of Intelligent Information Systems 2009, IEEE Transactions on Services Computing.
- **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). Served on the **Undergraduate Curriculum Committee** for the SIS Dept., and coordinated the College of Computing and Informatics' Seminar in Fall 2006. **Usenix Representative** for UNC Charlotte (2004 to present); **Faculty PI for Planet-Lab Consortium**, a large-scale testbeds for network applications. (2004 to present).
- **Academic Affairs Appointed Committees:** Bank of America Teaching Award Preparation Committee (2005), New Faculty Orientation Week Committee (Kang's suggestions on new faculty handbook website have been instrumental and received acknowledgement from staff and new faculty members), Faculty Center for Teaching and e-Learning Review Committee (2007).