1785

The University of Georgia

Department of Computer Science

Dr. Alan Dorsey/Dean
Franklin College of Arts and Sciences
Old College
University of Georgia
Campus

Dear Dean Dorsey,

The Computer Science Department is proposing to establish an Institute for Cybersecurity Institute and Privacy (ICSP) at the University of Georgia.
The importance of advancing research and education in cybersecurity and privacy is addressed by recent events that are reported in Section 2 of the proposal.

The increasing demand to address cybersecurity and privacy issues is reflected by the increasing funding initiatives at both the national and state levels. The White House has issued a plan that calls for large investments dedicated to advancing cyber security. Governor Deal's 2017 budget recommendation include the establishment of a Cyber Innovation and Training Center.

The Computer Science Department at UGA hosts an exceptional cyber security research program. Currently, it has four Faculty members whose research focus in entirely on cybersecurity and privacy. Their research results have been recognized at the international level. For instance, many of their publications have been featured in the most renowned and selective international conferences and peer-reviewed journals in the areas of cybersecurity and privacy (CVs are included). This ICSP will be one of the affiliated institutes with the Georgia Institutes of Informatics (GII). The establishment of this Institute will enhance the GII mission, and will go along with the University strategic plan.

One of the reasons for establishing the ICSP will be to support UGA's efforts towards applying for accreditation as a center of excellence in cyber defense research sponsored by NSA and the Department of Homeland Security. Such accreditation will allow UGA faculty to qualify for large cyber security research and scholarship grants. It is to be noted that there is only one Cyber Security Research Institute in the state of Georgia, and UGA is in an excellent position and very well qualified to be the second one.

In summary, the ICSP at UGA will serve as a platform to explore interdisciplinary cybersecurity and privacy research within UGA. In my view, this proposal is timely and of great significance to the further development of UGA's research and education as a land grant institution. I think that it will have a big impact on our Graduate programs and our research funding through UGA.

Sincerely,

Thiab Taha/Professor & Head of Computer Science Department

Proposal to Establish the

Institute for Cyber-Security and Privacy (ICSP)

at the University of Georgia

3/5/2017

1. Summary

This proposal seeks to establish an Institute for Cyber Security and Privacy at the University of Georgia. The primary objectives of the Institute will be to directly expand research in cyber security and privacy, and to indirectly enhance the cyber security and privacy curriculum currently offered at UGA.

Initially, the Institute's function will be primarily within the Department of Computer Science. The Department of Computer Science currently houses four faculty whose main areas of research are directly related to multiple aspects of cyber security and privacy. These research areas include network and system security, software security, web security, security for mobile devices and the Internet of Things (IoT), security of the Internet's core infrastructure, cyber-crime attribution, telephony security, and differential privacy.

While initially the institute will primarily involve faculty from the Department of Computer Science, one of the objectives of the institute will be to expand collaborations between cyber security researchers in the Department of Computer Science with researchers in other UGA units that conduct research related to the technical and non-technical aspect of cyber security and privacy. This may include faculty housed in the College of Engineering, the Department of Public Administration and Policy, the Department of Sociology, UGA School of Law, and the Department of Management Information Systems, among others. *The ICSP will participate as one of the institutes contributing to the Georgia Informatics Institutes for Research and Education (https://gii.uga.edu/)*.

By increasing the volume and enhancing the quality of cyber security and privacy research at UGA, the institute hopes to attract and recruit new talented faculty whose research expertise can complement current strengths in areas such as web security, security and privacy in social networks, cyber physical systems security, etc.

The Department of Computer Science currently offers several courses related to cyber security and privacy, both at the undergraduate and graduate level, and already offers a graduate certificate in cyber-security. One of the goals of the institute will be to coordinate efforts to also expand the existing cyber security and privacy curriculum.

Along with an expansion of research in cyber security and privacy, the institute will pursue the National Security Agency/Department of Homeland Security designation as a National Center of Academic Excellence in Cyber Defense Research, and will aggressively pursue new federal funding opportunities.

2. Background

Cyber security and privacy have become critical components of our digital lives. Security and privacy vulnerabilities affect every technology we use, from wearable and portable devices, such as smartwatches, smartphones, etc., to national critical infrastructure, such as the power grid and air control systems. The exploitation of such vulnerabilities has opened the doors not only to widespread cyber-crime, but also to cyber-warfare, as demonstrated by recent events related to the possible interference of foreign governments into the 2016 US presidential elections.

The need for research and expertise in the broad field of cyber security has grown tremendously in recent years. In 2015, Forbes Magazine reported that “between $9 and $21 trillion of global economic value creation could be at risk if companies and governments are unable to successfully combat cyber threats.”

- Forbes Magazine: www.forbes.com/sites/frontline/2015/07/13/why-cybersecurity-leadership-must-startat-the-top

In addition, through the Comprehensive National Security Initiative, the White House “has identified cyber security as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter.” To sustain the advancement in cyber-security defense, the Cybersecurity National Action Plan calls for an investment of over $19 billion for advancing cybersecurity.

- "FACT SHEET: Cyber security National Action Plan | whitehouse.gov." February 9, 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan. Accessed February 17, 2017.

Other federal agencies, including the Defense Advanced Research Projects Agency (DARPA), National Science Foundation (NSF), Department of Homeland Security (DHS), and the Department of Energy (DOE) have robust programs dedicated to funding cyber-security research and education, as illustrated by the following linked initiatives:

- Defense Advanced Research Projects Agency (DARPA): "DARPA Cyber Grand Challenge." http://archive.darpa.mil/CyberGrandChallenge_CompetitorSite/. Accessed February 17, 2017.

- National Science Foundation (NSF): "NSF FY 2017 Budget Request to Congress - National Science ...." https://www.nsf.gov/about/budget/fy2017/pdf/01_fy2017.pdf. Accessed February 17, 2017.

- Department of Homeland Security (DHS): "CSD Projects | Homeland Security." https://www.dhs.gov/science-and-technology/csd-projects. Accessed February 17, 2017.

- Department of Energy (DOE): "OE Announces Funding to Improve the Cybersecurity of the Nation's Power Grid." (January 20, 2016), https://energy.gov/oe/articles/oe-announces-funding-improve-cybersecurity-nation-s-power-grid. Accessed February 17, 2017.

3. Mission

The mission of the proposed Institute for Cyber Security and Privacy (ICSP) is to contribute to meeting the nation's cyber-security defense research and education needs. To this end, the ICSP will coordinate efforts related to pursuing new funding opportunities in cyber-security and privacy research and education.

The four primary goals of the institute are to:

1. Lead and advance cyber security and privacy research at the University of Georgia, in the state of Georgia, and at the national and international levels.

2. Serve as UGA's hub for interdisciplinary research in cyber security and privacy. Organize annual workshops and scientific meetings with all key stakeholders including UGA faculty, staff, and students, other universities, and industry and government representatives.

3. Meet and sustain the qualifications required to obtain designation as a NSA/DHS National Center of Academic Excellence in Cyber Defense Research.

   Key qualifications include, among others:

   - Evidence of a strong peer-reviewed publication record by faculty and students
   - Alignment of research to stated core areas of NHS/DHS including, 1) principles, 2) security mechanisms/functionality, 3) architectures, 4) assurance, 5) operations, 6) analysis, and 7) non-technical areas (including legal, policy, privacy, business, awareness, and supply chain.
   - Continuous and sustained graduate-level production with theses and dissertations related to the stated core areas; and
   - Continuous and sustained research funding, especially from DARPA, NSF, and IARPA, but also industry.

   Therefore, key criteria that should be used in the annual and periodic review of ICSP will be the success in achieving NSA/DHS designation and maintaining or building on the metrics needed to retain such designation.

4. Create the impetus and opportunity for new educational programs to be developed and offered by the Department of Computer Sciences in the areas of cyber-security and privacy education.

   For example, in 2016, due to the initiatives of the initial core faculty identified in this proposal, the Graduate Certificate in Cyber Security was developed and approved by University Council. The Graduate Certificate in Cyber Security program, offered by the Department of Computer Science, is designed to equip graduate students with both foundational and cutting-edge cybersecurity and privacy concepts, and to contribute to the formation of well-trained cyber-defense practitioners and researchers. Admission to the Certificate is open to graduate students across the university, but is specifically targeted towards graduate students in Computer Science, as well as related mathematical and engineering disciplines.

4. Value Added

In addition to the reasons relating to national security, the establishment of the ICSP brings significant and timely value to the University of Georgia due to, *i*) alignment with the stated grand challenges of UGA, *ii*) the requirement for such an established Institute to receive NSA/DHS designation, and *iii*) Governor Deal's proposed "Georgia Cyber Innovation and Training" as part of his 2017 budget. Each of these will be briefly addressed in this section to provide necessary context.

i) Alignment with the stated grand challenges of UGA

In his 2017 State of the University Address, President Morehead highlighted UGA's grand challenges, the third of which is "Promoting Cyber, Domestic, and Global Security." Thus, ICSP is very closely aligned with the stated priorities of the University of Georgia.

ii) The requirement for such an established Institute to receive NSA/DHS designation

The National Security Agency (NSA) and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in Cyber Defense (CAE-CD) program.

- Source: https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/

The goal of the program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber-defense and producing professionals with cyber-defense expertise for the Nation. The program comprises institutions receiving either designation for excellence in Education or Research or both.

A clear expectation of receiving NSA/DHS designation is the following:

"*The university has a declared, operational, and active center for Cyber Defense education or a center for Cyber Defense research. Provide a link to the center's website*."

Therefore, the establishment of ICSP at the University of Georgia not only closely aligns with the priorities of the University, it is a stated requirement for receiving NSA/DHS designation.

In the state of Georgia, seven institutions have such NSA/DHS designation.

<u>Designation as a National Center of Academic Excellence in Cyber Defense Education (CAE-CDE)</u>

Armstrong State University
Augusta University
Columbus State University
Kennesaw State University
Middle Georgia State University
University of North Georgia

<u>Designation as a National Center of Academic Excellence in Cyber Defense</u>

Research (CAE-R)

Georgia Institute of Technology

Although designation as a National Center does not carry a commitment of funding from NSA or DHS, it is clear that Georgia Tech enjoys added funding opportunities because of the designation from NSA/DHS.

In addition to Georgia Tech, seven of UGA's twelve peer institutions and four of UGA's twelve aspirational institutions have designation as a National Center for CD in Research (CD-R).

Peer Institutions having Designation as a National Center of Academic Excellence in Cyber Defense Research (CAE-R):

Ohio State University
University of Arizona
University of California – Davis
University of Florida
Iowa State University
North Carolina State University
University of Maryland

Aspirational Institutions having Designation as a National Center of Academic Excellence in Cyber Defense Research (CAE-R):

University of Illinois – Urbana-Champaign
Pennsylvania State University
University of Texas – Austin
University of Washington

iii) Governor Deal's proposed "Georgia Cyber Innovation and Training Center"

Governor Deal's 2017 budget recommendation (dated January 11, 2017) included $50 million for a new Georgia Cyber Innovation and Training Center in Augusta. The Center would be in partnership with state and federal agencies, as well as the private sector to create a secure environment for cyber-security education programs, testing and training.

The stated mission of the proposed Institute is to "promote modernization in cybersecurity technology for private and public industries through unique education, training, research, and practical applications." The vision of the Institute is to "be recognized as a world-class cyber range and training facility focused on developing the next generation cyber workforce through real-world practice, education, public-private collaboration, and interdisciplinary research in the fields of healthcare, computer science, electrical engineering, mathematics, and robotics."

The proposed Institute specifically highlights those seven institutions in the state that have designation as a National Center of Academic Excellence for either education or research.

President Morehead is quoted in Governor Deal's proposal as follows: "*The depth and breadth of the University of Georgia's expertise in cybersecurity and related fields—which ranges from training tomorrow's workforce to conducting groundbreaking research and leveraging the University's statewide infrastructure and networks—will enable this institution to play a key role* *in this critical initiative," said UGA President Jere W. Morehead. "We are committed to working with partners in government, industry and academia to enhance national security and economic vitality. Working together, we can stay one step ahead of emerging threats and create a more secure future*."

- o Georgia Cyber Innovation and Training Center. https://gov.georgia.gov/sites/gov.georgia.gov/files/related_files/press_release/Georgia%20Cyber%20Innovation%20and%20Training%20Center.pdf

5. Educational Offerings

ICSP will not initially be involved with the oversight of educational offerings at the University of Georgia. Consistent with its stated mission and goals, ICSP intends to be a leader in cutting-edge research relating to cyber-security and privacy. To this end, it is likely that ideas and concepts for new educational offerings will be developed which will be implemented and overseen by the Department of Computer Science and/or collaborating academic departments on campus.

6. Governance and Organization

The governance and organization of ICSP will be consistent with Academic Affairs Policy Statement No. 7 titled "UGA Policy on Center and Institutes."

a. Administrative Unit and Reporting Structure. The ICSP will be housed within the Department of Computer Science, and will administratively report to the Head of the Department of Computer Science, who in turn reports directly to the Dean of the Franklin College of Arts and Sciences. The establishment of ICSP will involve minimal additional administrative structure.

b. Founding Director of ICSP. The founding director of ICSP will be Dr. Kang Li. Dr. Li will report to the Head of the Department of Computer Science. The Director's appointment will be an administrative appointment subject to periodic review as described below.

c. ICSP Advisory Board. ICSP will have an Advisory Board that will advise the Head of the Department of Computer Science on all aspects of ICSP. The Advisory Board will meet at least annually to review annual progress of ICSP. The Advisory Board should have members within the Department, Franklin College of Arts and Sciences, and members outside the College. In addition, the Advisory Board may have members outside the University of Georgia. Advisory Board membership will be recommended by the Director and Head of the Department of Computer Sciences, and will be subject to the approval of the Dean. Advisory Board members will have three year terms that may be renewed.

d. Annual Reports. ICSP will submit an annual report summarizing progress toward achievement of the four goals detailed in this proposal.

e. Periodic Review of Director. The Director will be reviewed every five years per the accepted guidelines of the Franklin College of Arts and Sciences.

f. Periodic Review of ICSP. ICSP will be reviewed every five years. The review will address the extent to which ICSP achieved or is achieving the four stated goals. Key criteria that will be used in the annual and periodic review of ICSP will be the success in achieving NSA/DHS designation and maintaining or building on the metrics needed to retain such designation. The review report will also include a statement that continuation of the Institute is either recommended or not recommended. If continuation is not recommended, the Head of the Department of Computer Science shall decide whether to invoke the process for dissolution as described in Academic Affairs Policy Statement No. 7.

7. Institute Location and Physical Resources

ICSP will be physically located within the Department of Computer Science in Boyd GSRC within the existing laboratories and offices of the initial Core Faculty.

8. Finances

ICSP will fund itself through a combination of extramural sources including federal grants and contracts, industry contracts, and foundation grants, as well as through endowments. No new resources are required to begin the ICSP.

9. Core ICSP Faculty

The initial core faculty members of ICSP will include the following faculty members, all appointed as tenured or tenure-track faculty in the Department of Computer Science and all having primary areas of research pertaining to cyber security and privacy. NSF biosketches for all four core faculty are found in Appendix A.

Brief Bios of Four Core Faculty

Kang Li. Kang Li is a Professor of Computer Science at the University of Georgia. He is the director of the Network System and Security (NSS) Lab at UGA. He worked as a research scientist at the College of Computing of Georgia Tech before joining University of Georgia. Kang Li's research interests are in the area of computer network and operating systems, especially system issues related to data security and privacy. His recent research focuses on detecting bugs in system software such as virtualization and cloud platforms. His research topics also include DNS security and defenses against various network abuses, such as Denial-of-Service attacks, Phishing, and SPAM. His current research is supported by National Science Foundation, Intel, Cisco Systems, and Georgia Research Alliance. Current research projects in Dr. Li’s lab pertain to device and firmware security, virtualization and cloud security, and DNS security. Dr. Li is the founder of the DISEKT security team, which has competed and achieved high rankings in various global hacking competitions.

Roberto Perdisci. Dr. Perdisci is an Associate Professor in the Department of Computer Science, an Adjunct Associate Professor in the Georgia Tech School of Computer Science, and a faculty member of the UGA Institute for Artificial Intelligence. Before joining UGA he was Post-Doctoral Fellow at the College of Computing of the Georgia Institute of Technology. Dr. Perdisci also worked as Principal Scientist at Damballa, Inc., and prior to joining Damballa he was Research Scholar at the Georgia Tech Information Security Center and PhD candidate at the University of Cagliari, Italy with the Pattern Recognition and Applications Group. Dr. Perdisci’s research focuses on securing networked systems. His lab is particularly interested in web security, automating the analysis of security incidents, and defending networks from malware.

His lab often combine systems research with machine learning and large-scale data mining techniques to solve challenging computer and network security problems. He is also interested in broader aspects of networked systems, including Internet-scale measurements, analysis and optimization of systems performance, and the design of networking protocols. In 2012, Dr. Perdisci received an NSF CAREER award on a project titled "Automatic Learning of Adaptive Network-Centric Malware Detection Models."

Jaewoo Lee. Dr. Lee is an Assistant Professor in the Department of Computer Science. Before joining UGA, he was a postdoctoral research associate at Penn State University. Dr. Lee was one of the eight hires of the Presidential Informatics Hiring Initiative completed in 2016. Dr. Lee received a Ph.D. in computer science in 2014 from Purdue University where he studied privacy-preserving data analysis techniques. Dr. Lee's research interests lie at the intersections of data mining, machine learning, data privacy and security. The primary interests of his lab relate to data privacy - providing strong privacy guarantees while making accurate computations on sensitive datasets possible. His lab works on developing new methodologies for performing machine learning and data mining tasks on the privacy-enhanced data. He also works on developing efficient mining algorithms for data streams. A data stream is a sequence of data elements continuously generated at a fast rate. Due to its distinct characteristics, such as massiveness, evolving concept and high data growth rate, stream data mining poses new challenges. The research topics of interest include data privacy, machine learning, data mining on high-dimensional data, and security analytics.

Kyu Hyung Lee. Dr. Lee is an Assistant Professor in the Department of Computer Science. He earned his Ph.D. from Purdue University (2014) and MS (2008) from Hong-Ik University. His research interest lies in combining analyses at the program level and the system level to develop synergetic solutions for problems in cyber security, software reliability, and mobile security. His background broadly covers several areas: cyber security, dynamic/static program analysis, software engineering, operating systems, and distributed systems. Dr. Lee's recent publications address accurate reconstruction of android attacks via multi-layer forensic logging, enabling reconstruction of attacks on users via efficient browsing snapshots, and self destructing exploit executions via input perturbation.

Additional Core Faculty within the Department of Computer Science or outside the Department of Computer Science may apply for membership as Core Faculty subject to the majority vote by the existing Core Faculty at the time. All Core Faculty will retain their appointments in their home units. Promotion, tenure, and salary decisions will be made in the home unit according to the unit criteria in consultation with the ICSP Director.

10. Affiliated Faculty and Staff Membership

Although ICSP will be physically located and organized within the Department of Computer Science, any interested faculty or staff including postdoctoral fellows associated with the University of Georgia will be eligible to apply for membership as Affiliated Faculty or Affiliated Staff. Applicants should submit a resume or curriculum vitae with a cover letter stating their interest and the extent to which the applicant may contribute to the mission and goals of ICSP. Affiliate membership will be subject to the majority vote of the existing Core Faculty. All Affiliated Faculty will retain their appointments in their home units.

11. Student Membership

Any current undergraduate or graduate UGA student may apply for Student membership. Applicants should submit a resume or curriculum vitae with a cover letter stating their interest and the extent to which the applicant may contribute to the mission and goals of ICSP. Student membership will be subject to the majority vote of existing Core Faculty.

12. Letters of Support

1. Alan Dorsey, Dean, Franklin College of Arts and Sciences
2. David Lee, Vice President, Office of Vice President for Research

13. Appendix A. NSF biosketches of initial four core faculty

Dr. Kang Li, Professor, Department of Computer Science
Dr. Roberto Perdisci, Associate Professor, Department of Computer Science
Dr. Jaewoo Lee, Assistant Professor, Department of Computer Science
Dr. Kyu Hyung Lee, Assistant Professor, Department of Computer Science

UNIVERSITY OF
GEORGIA

Old College
Athens, Georgia 30602
TEL 706-542-3400
www.franklin.uga.edu

Franklin College of Arts and Sciences
Office of the Dean

March 1, 2017

Dear Members of the Curriculum Committee,

I write in support of the proposal to establish an **Institute of Cyber Security and Privacy** (ICSP) at UGA. This proposal is submitted by the Department of Computer Science.

The importance of cyber security and privacy research and education are evident in every corner of our lives, from elections to online commerce to personal communications. The great demand to address cyber security and privacy issues is reflected by the increasing funding initiatives at both the national and state levels. The White House has issued a plan that calls for investment for advancing cyber security, and Governor Nathan Deal recently proposed a Cyber Innovation and Training Center in Georgia.

UGA is well positioned to offer an excellent cyber security research program. The Department of Computer Science has multiple faculty whose research focus is on cyber security and privacy, and we anticipate interest and participation by other Franklin College and UGA faculty with related interests.

One of the first priorities for ICSP is to secure designation as a National Center of Academic Excellence in cyber defense research sponsored by the National Security Agency and the Department of Homeland Security. One benefit of such an institute is that it would allow UGA to qualify for large cyber security research and scholarship grants. ICSP will also serve as a platform to explore interdisciplinary research at UGA.

I view this proposal as timely and of great significance that will advance UGA's research and education missions. I enthusiastically support the formation of the Institute of Cyber Security and Privacy.

Sincerely,

Alan T. Dorsey
Dean

UNIVERSITY OF
GEORGIA

OFFICE OF RESEARCH
147 Paul D. Coverdell Center for Biomedical and Health Sciences
Athens, GA 30602
TEL 706-542-5969 | FAX 706-542-5978
www.uga.edu

March 6, 2017

Dear University Curriculum Committee,

This letter is in support of the proposal, submitted by the Department of Computer Science, to establish an Institute for Cyber Security and Privacy (ICSP) at UGA.

The importance of advancing research and education in cybersecurity and privacy is highlighted by recent events, such as the use of cyber-attacks by a foreign country to potentially influence the results of US elections, numerous breaches into corporate databases and personal communications, and denial-of-service attacks against popular web services and critical cyber-infrastructure. Within our own UGA community, employees and students were directly impacted by the hacking of Anthem two years ago. We should not, therefore, be surprised to see the increasing demands for better cyber security defense and privacy protections.

This new and increasing demand to address cybersecurity and privacy issues is reflected by increasing funding initiatives at both the national and state levels. The White House has issued a plan that calls for large investments dedicated to advancing cybersecurity. Governor Deal's recommended 2017 budget includes the establishment of a Cyber Innovation and Training Center in the State of Georgia.

UGA has an impactful cyber security research program, primarily housed within the Department of Computer Science, which currently has four faculty whose research is entirely focused on cybersecurity and privacy. Their research has been recognized at the international level. For instance, many of their publications have been featured in top-tier international conferences and peer-reviewed journals in the areas of cybersecurity and privacy.

ICSP will be the catalyst for UGA's application for accreditation as a center of excellence in cyber defense research sponsored by NSA and the Department of Homeland Security. Such accreditation will allow UGA faculty to qualify for large cybersecurity research and scholarship grants. The cybersecurity center at UGA will also serve as a platform for interdisciplinary cybersecurity and privacy research here on campus.

In conclusion, I view this proposal as timely and of great significance to our impact as a land grant institution. I support the formation of the Institute of Cyber Security and Privacy with considerable enthusiasm.

Sincerely,

David Lee

David Lee, Ph.D.
Vice President for Research

BIOGRAPHICAL SKETCH

Kang Li

Education

Ph.D., Computer Science and Engineering November 2002
Oregon Health & Science University, Portland, Oregon, USA.

B.S., Computer Science and Engineering July 1995
Tsinghua University, Beijing, China.

Professional Experience

Department of Computer Science Aug 2003 ~ present
University of Georgia
Professor (assistant 2003-, associate 2009-)

The Intel Science and Technology Center for Secure Computing May 2013 ~ present
UC Berkeley, California, USA
Faculty member

Center for Experimental Research in Computer Systems Dec 2002 ~ Aug 2003
College of Computing
Georgia Institute of Technology
Research Scientist II

Department of Computer Science and Engineering Sep 1997 ~ Nov 2002
Oregon Health & Science University, Oregon, USA
Graduate Research Assistant

Selected Honors And Awards

Distinguished Paper Award of Network and Distributed System Security Symposium (2016)
DARPA Cyber Grand Challenge Finalist Award (2015-2016)
Intel Research Award (2014)
Teaching Excellence Award in Computer Science, University of Georgia (2013)
Best Paper Award of the Tenth Annual Conference on Detection of Intrusions and Malware & Vulnerability Assessment (2013)
Best Paper of ACM Computer Communication Review (2012)
Cisco Research Award (2009)
Singapore A-Star Research Panel Member (2008)

Research Grants

1. Kang Li (co-PI), “Passive and Active DNS Monitoring Tools for Detecting and Tracking the Evolution of Malicious Domain Names”, funded by National Science Foundation (NSF), with Roberto Perdisci (PI), $299,068, September 1, 2011 – February 28, 2017.

2. Kang Li (PI), gift from Intel Corp, “Collaboration in Intel Science and Technology Center for Secure Computing”, with Robert Perdisci (Co-PI), $40,000, September 1, 2014 – August 31, 2018.

3. Kang Li (PI), *CNS-1319115*, “CSR: Small: Detecting Flaws in Virtual Devices by Conformance Checking”, funded by National Science Foundation (NSF), $469,829, October 1, 2013 – September 30, 2016.

4. Kang Li (PI), *SaTC-1318881*, “SaTC: EDU: Enhancing and Broadening Computer Security Education with Stepwise and Reusable Problem-solving Challenges”, funded by National Science Foundation (NSF), with Roberto Perdisci (co-PI), $298,854, October 1, 2013 – September 30, 2015.

5. Kang Li (PI), gift from Intel Corp, “Detecting Malicious Web Exploitations by Mining Multi-Source Provenance Data”, with Robert Perdisci (Co-PI), $40,000, September 1, 2013 – August 31, 2014.

6. Kang Li (co-PI), *SDCI-1127395*, “Sec: Passive and Active DNS Monitoring Tools for Detecting and Tracking the Evolution of Malicious Domain Names”, funded by National Science Foundation (NSF), with Roberto Perdisci (PI), $379,988, September 1, 2011 – August 31, 2014.

7. Kang Li (PI), “Research with Undergraduate Students for CT-T”, funded by National Science Foundation (NSF), $15,000, August 1, 2010 – July 31, 2011.

8. Kang Li (PI), “Enabling Statistical-based Traffic Classification”, funded by Cisco Systems, $30,000, Dec 1, 2009 – Nov 30, 2012.

9. Kang Li (PI), *CNS-0716357*, “CT-T: Collaborative Research Adaptive Attacks and Defenses in Denial of Information”, funded by National Science Foundation (NSF), with Lakshmish Ramaswamy (Co-PI), $231,854, August 1, 2007 – July 31, 2010.

10. Kang Li (PI), “Enhancing Online Security with Communication Dampened Devices”, funded by ISC, $99,082 (including matching fund from Georgia Research Alliance), July 1, 2007 – June 30, 2008.

11. Kang Li (PI), *GRA.TC06.G*, “High Speed Statistical-based Anti-spam System”, funded by Georgia Research Alliance, $10,000, February, 2006 – December 31, 2006.

12. Kang Li (co-PI), “System-Level Techniques for Energy-Aware Computing”, funded by State of Georgia, Yamacraw Research Program, with David K. Lowenthal (PI), Scott Watterson, Suchi Bhandarkar and Amit Sheth, $27,150, July 1, 2003 – June 30, 2004.

13. Kang Li (PI), “Resisting SPAM with Network Puzzles”, UGA Junior Faculty Research Grant, $9,572, February 2, 2004 – December 31, 2004.

Selected Publications

1. Jianjun Chen, Jian Jiang, Xiaofeng Zheng, Haixin Duan, Jinjin Liang, Kang Li, Tao Wan, and Vern Paxson. “Forwarding-Loop Attacks in Content Delivery Networks”, in the proceedings of

the *23th Annual Network and Distributed System Security Symposium (NDSS 2016)*, February 2016, won the 2016 best paper award.

2. Christopher J. Neasbitt, Bo Li, Roberto Perdisci, Long Lu, Kapil Singh, and Kang Li, "WebCapsule: Towards a Lightweight Forensic Engine for Web Browsers", in the proceedings of ACM Conference on Computer and Communication Security (*ACM CCS 2015*), November 2015.
3. Guodong Zhu, Kang Li, and Yibin Liao, "Towards Automatically Deducing Key Device States for the Live Migration of Virtual Machines", in the proceedings of IEEE Cloud 2015, July 2015.
4. Ikseon Choi, Sejin Kim, Younseok Lee, and Kang Li. A Preliminary Study on Undergraduate Students' Learning Experiences While Solving Basic Cybersecurity Challenges, in the 2015 Work-in-Progress Workshop of ACM ICER, Omaha, Nebraska, August 2015
5. Christopher J. Neasbitt, Roberto Perdisci, Kang Li, and Terry Nelms, "ClickMiner: Towards Forensic Reconstruction of User-Browser Interactions from Network Traces", in the proceedings of ACM Conference on Computer and Communication Security (*ACM CCS 2014*), November 2014.
6. Jinjing Liang, Jian Jiang, Haixin Duan, Kang Li, Tao Wan, and Jianping Wu, "When HTTPS Meets CDN: A Case of Authentication in Delegated Service", in proceedings of 35th IEEE Symposium on Security and Privacy (*IEEE S&P 2014*), May, 2014.
7. Babak Rahbarinia, Roberto Perdisci, Andrea Lanzi, and Kang Li, "PeerRush: Mining for Unwanted P2P Traffic", in *Journal of Information Security and Applications*, April 24, 2014.
8. Lakshmish Ramaswamy, Raga Sowmya Tummalapenta, Deepika Sethi, Kang Li, and Calton Pu, "Harnessing Context for Vandalism Detection in Wikipedia", in *Journal of Collaborative Computing*, Volume 1, Number 1, May 2014.
9. Lakshmish Ramaswamy, Raga Sowmya Tummalapenta, Kang Li, and Calton Pu, "A Content-Context Centric Approach for Detecting Vandalism in Wikipedia", in the proceedings of 9th IEEE International Conference on Collaborative Computing (*CollaborateCom 2013*), October, 2013.
10. Phani Vadrevu, Babak Rahbarinia, Roberto Perdisci, Kang Li, and Manos Antonakakis, "Measuring and Detecting Malware Downloads in Live Network Traffic", in the proceedings of the 18th European Symposium on Research in Computer Security (*ESORICS 2013*), September 2013.
11. Babak Rahbarinia, Roberto Perdisci, Andrea Lanzi, and Kang Li, "PeerRush: Mining for Unwanted P2P Traffic", in the proceedings of the 10th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (*DIMVA 2013*), July 2013, won the 2013 best paper award.
12. Jinjing Liang, Jian Jiang, Haixin Duan, Kang Li, and Jianping Wu, "Measuring Query Latency of Top Level DNS Servers", in the proceedings of the 14th Passive and Active Measurement Conference (*PAM 2013*), March 2013.
13. Kevin Warrick, Roberto Perdisci, and Kang Li, "Measuring the lifecycle of Malicious Domains", in the poster session of the *IEEE Symposium on Security and Privacy* (*IEEE S&P 2012*), May 2012.
14. Haixin Duan, Nicholas Weaver, Zongxu Zhao, Meng Hu, Jian Jiang, Jinjin Liang, Kang Li and Vern Paxson, "Hold-On: Protecting against DNS Packet Injection", in the proceeding of the workshop of Securing and Trusting Internet Names (*SATIN* 2012), March, 2012.
15. Jian Jiang, Jinjing Liang, Kang Li, Jun Li, Haixin Duan, and Jianping Wu, "Ghost Domain Names: Revoked Yet Still Resolvable", in the proceeding of the *19th Annual Network and Distributed System Security Symposium (NDSS 2012)*, February 2012.
16. Kang Li, and other Anonymous Authors. "The Collateral Damage of Internet Censorship by DNS Injection", in *ACM Computer Communication Review* (CCR) Volume 42, Number 3, page 21-27, July 2012. Awarded as a best paper of 2012 ACM CCR.

17. Danesh Irani, Steve Webb, Kang Li, and Calton Pu. “Modeling Unintended Personal Information Leakage from Multiple Online Social Networks”, in *IEEE Internet Computing* special issue on Security and Privacy in Social Networks. Volume 15, Issue 3, Pages 13-19, May, 2011.
18. Yong Wei, Suchendra Bhandarkar, Kang Li, and Lakshmish Ramaswamy, “Video Personalization in Heterogeneous and Resource-constrained Environments”, in *Springer Multimedia System Journal*, Volume 17, Number 6, Pages 523-543, April, 2011.
19. Zhenyu Zhong and Kang Li, “Speed up Statistical Spam Filters by Approximation”, *IEEE Transactions on Computers*, Vol. 60, No. 1, pp. 120-134, January 2011.
20. Douglas Brewer, Kang Li, Laksmish Ramaswamy, and Calton Pu, “A Link Obfuscation Service to Detect Webbots”, 2010 *IEEE International Conference on Services Computing*, pp. 433-440, July 2010.
21. Danesh Irani, Steve Webb, Calton Pu, and Kang Li, “Study of Trend-Stuffing on Twitter through Text Classification”, in *Proceedings of the Conference on Email and Anti-Spam (CEAS 2010)*, Seattle, WA, July 2010.
22. Kang Li, Zhenyu Zhong, and Lakshmish Ramaswamy, “Privacy-Aware Collaborative Spam Filtering”, in *IEEE Transactions on Parallel and Distributed Systems (IEEE TPDS)*, in vol. 20, No. 5, May 2009.
23. Yong Wei, Suchendra Bhandarkar, and Kang Li, “Client-centered Multimedia Content Adaptation”, in *ACM Transactions on Multimedia Computing, Communications and Applications (ACM TOMCCAP)*, Vol.5, Issue 3, No.22. August 2009.
24. Danesh Irani, Steve Webb, Kang Li and Calton Pu, " Large Online Social Footprints - An Emerging Threat " in the proceeding of *IEEE Symposium on Secure Computing (Securecom09)*, September 2009.
25. Krishna Vangapandu, Douglas Brewer and Kang Li, "A Study of URL Redirection Indicating Spam", in proceedings of *the Conference on Email and Anti-Spam (CEAS 2009)*, Mountain View, July 2009.
26. Zhenyu Zhong, Lakshmish Ramaswamy, and Kang Li, “ALPACAS: A Large-scale Privacy-Aware Collaborative Anti-Spam System”, in proceedings of *IEEE Infocom 2008*, April 15-18, Phoenix, Arizona, 2008.
27. Siddhartha Chattopadhyay, Suchendra Bhandarkar, and Kang Li, “Model-based Power Aware Compression Algorithms for MPEG-4 in Mobile Environments”, in *IEEE Transactions on Multimedia*, Vol 9, Issue 1, pp. 1 – 8, 2007.
28. Siddhartha Chattopadhyay, Suchendra Bhandarkar and Kang Li, “Human Motion Capture Data Compression by Model-Based Indexing”, in *IEEE Transactions on Visualization and Computer Graphics*, Vol 13, No. 1, pp. 5 – 14, 2007.
29. Kang Li and Zhenyu Zhong, “Fast Statistical Spam Filter by Approximate Classifications”, in *ACM Performance Evaluation Review*, Vol. 34, No. 1, pp. 347 – 358, June 2006. (also published in ACM SIGMETRICS 2006)
30. Haijin Yan, David Lowenthal, Kang Li, Rupa Krishnan, and Larry Peterson, “Client-Centered, Energy-Efficient Wireless Communication on IEEE 802.11b Network”, in *IEEE Transaction on Mobile Computing*, Volume 5, pp. 1575 – 1590, 2006.

Dr. Roberto Perdisci

Dept. of Computer Science, University of Georgia - Athens, GA 30602
e-mail: perdisci@cs.uga.edu – phone: +1 (706) 542 3482
http://roberto.perdisci.com

(a) Professional Preparation

University of Cagliari, Italy - Research Doctorate in Computer Engineering (Mar. 2007)
University of Cagliari, Italy - Laurea Degree in Electronic Engineering (Dec. 2003)

(b) Appointments

2015–curr.: **Associate Professor**, Dept. of Computer Science, University of Georgia - Athens, GA
2015–curr.: **Adjunct Associate Professor**, College of Computing, Georgia Institute of Technology - Atlanta, GA
2010–2015: **Assistant Professor**, Dept. of Computer Science, University of Georgia - Athens, GA
2012–2015: **Adjunct Assistant Professor**, College of Computing, Georgia Institute of Technology - Atlanta, GA
2013–2014: **Faculty Researcher**, Intel/Berkeley Science and Technology Center for Secure Computing, Secure Computing Research for Users' Benefit (SCRUB)
2009–2010: **Post-Doctoral Fellow**, College of Computing, Georgia Institute of Technology - Atlanta, GA
2007–2009: **Principal Scientist**, Damballa Inc., Atlanta, GA
2005–2007: **Research Scholar**, College of Computing, Georgia Institute of Technology - Atlanta, GA

(c) Awards and Honors

2016 Outstanding Reviewer Award - 19th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2016)
2015 Fred C. Davison Early Career Scholar Award - University of Georgia Research Foundation ("awarded to an early career scholar in the sciences" - "the most promising up and coming researcher/scholar, whose trajectory projects remarkable success")
2014 M. G. Michael Award for Excellence in Research - University of Georgia, Franklin College of Arts and Sciences.
2013 Outstanding Faculty Research Award - University of Georgia, Department of Computer Science.
2013 Best Paper Award at the 10th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2013).
2012 NSF Faculty Early Career Development (CAREER) Award.

(d) Funding

- DARPA BAA 16-34 – "Rhamnousia: Attributing Cyber Actors Through Tensor Decomposition and Novel Data Acquisition" [Sub] (Recommended for Award – $498,531 to be awarded to UGA – Anticipated Start Date: 11/21/2016 – Duration: 4.5 years)
- NSF CNS - "TWC: Medium: Collaborative: Exposing and Mitigating Cross-Channel Attacks that Exploit the Convergence of Telephony and the Internet" [UGA's PI; Collaborative Grant with GaTech] ($299,068 awarded to UGA – Start Date: 08/15/2015 – Duration: 4 years)
- DHS TTP – "AMICO: Accurate Behavior-Based Detection of Malware Downloads" [PI] ($350,000 – Start Date: 08/15/2014 – Duration: 3 years)

- NSF DUE - “EDU: Enhancing and Broadening Computer Security Education with Stepwise and Reusable Problem-solving Challenges” [Co-PI] ($298,854 – Start Date: 09/15/13 – Duration: 2 years)
- Intel Corporation – “Automatic Discovery, Categorization, and Trace-Back of New Web Based Attacks via Scalable Multi-Source Data Mining” [Co-PI] ($80,000 gift grant, September 2013)
- DHS BAA 11-02 – “Comprehensive Understanding of Malicious Overlay Networks” [Sub] ($300,000 awarded to UGA – Start Date: 10/1/2012 – Duration: 3 years)
- NSF CNS – “CAREER: Automatic Learning of Adaptive Network-Centric Malware Detection Models” [PI] ($402,601 – Start Date: 06/01/12 – Duration: 5 years)
- NSF ACI – “SDCI Sec: Passive and Active DNS Monitoring Tools for Detecting and Tracking the Evolution of Malicious Domain Names” [PI] ($379,988 – Start Date: 09/01/11 – Duration: 3 years)
- UGA OVPR Junior Faculty Research Grant – “Countering Click Malware” [PI] ($11,403 – July 2011 to July 2012)

(e) Recent Selected Publications

1. Phani Vadrevu, Jienan Liu, Bo Li, Babak Rahbarinia, Kyu Hyung Li, and **Roberto Perdisci**. Enabling reconstruction of attacks on users via efficient browsing snapshots. In **NDSS**’*17: Proceedings of the Network and Distributed System Security Symposium*, page (15 pages), 2017. (acceptance rate 16.1% = 68/423).
2. Terry Nelms, **Roberto Perdisci**, Manos Antonakakis, and Mustaque Ahamad. Towards measuring and mitigating social engineering software download attacks. In *Proceedings of the 25th* **USENIX Security Symposium**, 2016. (acceptance rate 15.6% = 72/463).
3. Christopher Neasbitt, Bo Li, **Roberto Perdisci**, Long Lu, Kapil Singh, and Kang Li. WebCapsule: Towards a lightweight forensic engine for web browsers. In **ACM CCS**’*15: Proceedings of the 22th ACM conference on Computer and communications security*, 2015. (acceptance rate 19.8% = 128/646).
4. Terry Nelms, **Roberto Perdisci**, Manos Antonakakis, and Mustaque Ahamad. WebWitness: Investigating, categorizing, and mitigating malware download paths. In *Proceedings of the 24th* **USENIX Security Symposium**, 2015. (acceptance rate 15.7% = 67/426).
5. Maria Konte, **Roberto Perdisci**, and Nick Feamster. ASwatch: An AS reputation system to expose bulletproof hosting ASes. In **ACM SIGCOMM**’*15: 2015 ACM Conference on Special Interest Group on Data Communication*, pages 625–638, 2015. (acceptance rate 15.6% = 40/256).
6. Christopher Neasbitt, **Roberto Perdisci**, Kang Li, and Terry Nelms. ClickMiner: Towards forensic reconstruction of user-browser interactions from network traces. In **ACM CCS**’*14: Proceedings of the 21th ACM conference on Computer and communications security*, 2014. (acceptance rate 19.5% = 114/585).

(f) Service

- **Recent Conference Technical Program Committees**: 2017 USENIX Security Symposium; 2016-2017 International World Wide Web Conference (WWW), Security & Privacy Track; 2015-2016 ACM Conference on Computer and Communications Security (CCS); 2016 International Symposium on Research in Attacks, Intrusions and Defenses (RAID); 2016 European Symposium on Research in Computer Security (ESORICS); 2016 IEEE/IFIP International Conference on Dependable Systems and Networks (DSN); 2015 Network and Distributed Systems Security Symposiu (NDSS).
- **University Service**: 2014 Franklin IT Taskforce; 2015-2016 James L. Carmon Scholarship Committee; 2013-2014 Dept. of Computer Science Awards Committee Chair.

Biographical Sketch: Kyu Hyung Lee

Dr. Kyu Hyung Lee
Department of Computer Science, University of Georgia
Athens, GA 30602-7404

kyuhlee@cs.uga.edu
http://www.cs.uga.edu/~kyuhlee/

Professional Preparation

Hong-Ik University, Seoul, South Korea	Computer Engineering	B.Sc.	2005
Hong-Ik University, Seoul, South Korea	Computer Engineering	M.S.	2008
Purdue University, West Lafayette, IN	Computer Science	Ph.D.	2014

Appointments

2014-present	Assistant Professor of Computer Science, University of Georgia, Athens, GA
2008-2014	Research Assistant, Purdue University, West Lafayette, IN

Five Related Publications

1. Xingzi Yuan, Omid Setayeshfar, Hongfei Yan, Pranav Panage, Xuetao Wei, Kyu Hyung Lee. "DroidForensics: Accurate Reconstruction of Android Attacks via Multi-layer Forensic Logging," *In 12th ACM Asia Conference on Computer and Communications Security (AsiaCCS'17),* Abu Dhabi, UAE, 2017.

2. Phani Vadrevu, Jienan Liu, Bo Li, Babak Rahbarinia, Kyu Hyung Lee, Roberto Perdisci. "Enabling Reconstruction of Attacks on Users via Efficient Browsing Snapshots," *In Proceedings of the 24th Annual Network and Distributed System Security Symposium (NDSS'17),* San Deigo, CA, 2017.

3. Yonghwi Kwon, Brendan Saltaformaggio, I Luk Kim, Kyu Hyung Lee, Xiangyu Zhang, Dongyan Xu. "A2C: Self Destructing Exploit Executions via Input Perturbation," *In Proceedings of the 24th Annual Network and Distributed System Security Symposium (NDSS'17),* San Deigo, CA, 2017.

4. Shiqing Ma, Kyu Hyung Lee, Chung Hwan Kim, Junghwan Rhee, Xiangyu Zhang and Dongyan Xu, "Accurate, Low Cost and Instrumentation-Free Security Audit Logging for Windows," *In Proceedings of the Annual Computer Security Applications Conference (ACSAC'15),* Los Angeles, CA, 2015

5. Kyu Hyung Lee, Xiangyu Zhang and Dongyan Xu. "High accuracy attack provenance via binary-based execution partition," *In Proceedings of the 20th Annual Network and Distributed System Security Symposium (NDSS'13),* San Deigo, CA, 2013.

Five Other Publications

1. Chung Hwan Kim, Junghwan Rhee, Kyu Hyung Lee, Xiangyu Zhang and Dongyan Xu. "PerfGuard: Binary-Centric Application Performance Monitoring in Production Environments," *In Proceeding of the 24th ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE'16),* Seattle, WA, 2016

2. Kyu Hyung Lee, Xiangyu Zhang and Dongyan Xu. “LogGC: Garbage Collecting Audit Log,” *In 20th ACM Conference on Computer and Communications Security (CCS13),* Berlin, Germany, 2013.

3. Kyu Hyung Lee, Nick Sumner, Xiangyu Zhang and Patrick Eugster. “Unified Debugging of Distributed Systems with Recon,” *In Proceedings of the 41st IEEE/IFIP International Conference on Dependable Systems and Networks (DSN-DCCS’11),* Hong Kong, China, 2011.

4. Kyu Hyung Lee, Yunhui Zheng, Nick Sumner and Xiangyu Zhang. “Toward Generating Reducible Replay Log,” *In Proceedings of the 32nd ACM SIGPLAN conference on Programming Language Design and Implementation (PLDI’11),* San Jose, CA, 2011.

5. Soyeon Park, Weiwei Xiong, Zuoning Yin, Rini Kaushik, Kyu H. Lee, Shan Lu and Yuanyuan Zhou, “PRES: Probabilistic Replay with Execution Sketching on Multiprocessors,” *In Proceedings of the 22nd ACM Symposium on Operating Systems Principles (SOSP’09),* Big Sky, MT

Five Synergistic Activities

1. PC member for the 24th ACM Conference on Computer and Communications Security (ACM CCS 2017)

2. PC member for IEEE International Workshop on Security, Trust, and Privacy for Software Applications, 2016

3. Reviewer of the IEEE Transaction on Computers, the Journal of Computer Science and Technology 2015

4. Guest Editor of the Journal of Computer Science and Technology, 2015

5. Reviewer for funding agencies, National Science Foundation (NSF) panelist 2015

Biographical Sketch

Jaewoo Lee
Assistant Professor
University of Georgia
Athens, GA 30602
(706) 542-8241
jaewoo.lee@uga.edu
http://www.cs.uga.edu/~jwlee

Professional Preparation

Yonsei University	Seoul, South Korea	Computer Science	B.S. 2006
Yonsei University	Seoul, South Korea	Computer Science	M.S. 2008
Purdue University	West Lafayette, IN	Computer Science	Ph.D. 2014
Penn State University	State College, PA	Computer Science	Postdoc.

Appointments

Since 2016	Assistant Professor, University of Georgia
2014 - 2016	Postdoctoral Research Associate, Penn State University

Publications

- Jaewoo Lee and Daniel Kifer. Postprocessing for Iterative Differentially Private Algorithms. In ICML 2016 Workshop on Theory and Practice of Differential Privacy, ICML, 2016 (poster)
- Yue Wang, Jaewoo Lee, and Daniel Kifer. Differentially Private Hypothesis Testing, Revisited. ArXiv e-prints, November 2015 (under review)
- Jaewoo Lee, Yue Wang, and Daniel Kifer. Maximum Likelihood Postprocessing for Differential Privacy under Consistency Constraints. In Proceedings of the 21st ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD, 2015
- Jaewoo Lee and Chris Clifton. Top-k Frequent Itemsets via Differentially Private FP-trees. In Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD, 2014
- Rajesh Kalyanam, Lan Zhao, Carol X. Song, Yuet Ling Wong, Jaewoo Lee, and Nelson B. Villoria. iData: A Community Geospatial Data Sharing Environment to Support Data-driven Science. In Proceedings of the Conference on Extreme Science and Engineering Discovery Environment: Gateway to Discovery, XSEDE, 2013
- Jaewoo Lee and Chris Clifton. Differential identifiability. In Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining, KDD, 2012
- Jaewoo Lee and Chris Clifton. How much is enough? Choosing ϵ for Differential Privacy. In Information Security, volume 7001 of LNCS, pages 325–340. Springer Berlin / Heidelberg, 2011
- Hazem Elmeleegy, Ahmed Elmagarmid, and Jaewoo Lee. Leveraging Query Logs for Schema Mapping Generation in U-MAP. In Proceedings of the 2011 ACM SIGMOD International Conference on Management of Data, SIGMOD, 2011
- Hazem Elmeleegy, Jaewoo Lee, El Kindi Rezig, Mourad Ouzzani, and Ahmed Elmagarmid. U-MAP: A System for Usage-based Schema Matching and Mapping. In Proceedings of the 2011 ACM SIGMOD International Conference on Management of Data, SIGMOD, 2011 (demo)
- Jae Woo Lee, Nam Hun Park, and Won Suk Lee. Efficiently Tracing Clusters over High-dimensional On-line Data Streams. Data Knowledge & Engineering, 68(3):362–379, March 2009

- Jae Woo Lee and Won Suk Lee. A Coarse-grain Grid-based Subspace Clustering Method for Online Multi-dimensional Data Streams. In Proceedings of the 17th ACM Conference on Information and Knowledge Management, CIKM, 2008

Grants

- Differentially Private Learning of Deep Sum-product Networks, Jaewoo Lee, UGA internal faculty research grant (submitted)
- Statistical Estimation from Privacy-Enhanced Data, Jaewoo Lee, Computer and Information Science and Engineering Research Initiation Initiative, NSF (in progress)

Ph.D. Thesis Advisor: Chris Clifton (Purdue University)

Collaborators: Daniel Kifer (PennState University), Adam Smith (PennState University), Zhiyun Qian (UC Riverside), Zhichun Li (NEC Labs), Zhenyu Wu (NEC Labs), Junghwan Rhee (NEC Labs), Mustaque Ahamad (Gatech)