Bo Luo

Contact Information

2044 Eaton Hall or 341 Nichols Hall
The University of Kansas
Lawrence, Kansas 66045, USA
Phone: 785-864-7749
E-mail: bluo@ku.edu; bluo@ittc.ku.edu
Homepage: http://www.ittc.ku.edu/~bluo

Research Interests

My current research interests lie in the intersection of *security and privacy* and *data science*. In particular, I'm interested in:

- AI/ML security, adversarial machine learning
- Smart grid and IoT/CPS security
- Information security and privacy

Education

The Pennsylvania State University, University Park, Pennsylvania, USA

Ph.D., Information Sciences and Technology, August 2008

- Dissertation Title: "XML Access Control in Native and RDBMS-based XML Database Systems"
- Advisor: Dr. Dongwon Lee

The Chinese University of Hong Kong, Shatin, N.T., Hong Kong

M.Phil., Information Engineering, December 2003

- Thesis Title: "Video Text Detection and Extraction Using Temporal Information"
- Advisor: Dr. Xiaoou Tang

University of Sciences and Technology of China, Hefei, Anhui, P.R.China

B.E., Electronic and Information Engineering, July 2001

- Thesis Title: "Research on Digital Watermarking Techniques" (in Chinese)
- Advisor: Dr. Nenghai Yu

Academic and Professional Experiences

The University of Kansas, Lawrence, Kansas, USA

Professor, EECS **2019-present**

Director, HASS **2022-present**

Associate Professor, EECS **2014-2019**

Assistant Professor, EECS **2008-2014**

Professor in the Department of Electrical Engineering and Computer Science (EECS). Director of the High Assurance and Secure Systems (HASS) Research Center of the Institute of Information Sciences, The University of Kansas.

Japan Advanced Institute of Science and Technology, Nomi, Ishikawa, Japan
Visiting Professor **January 2020 - February 2020**

Visiting Professor at the Center for Trustworthy IoT Infrastructure (Excellent Core), School of Information Science, Japan Advanced Institute of Science and Technology (JAIST).

IBM Corporation, Silicon Valley Lab, California, USA
Summer Internship **May 2007 - August 2007**

Summer co-op with DB2 for z/OS XML Core Development & Solutions, IBM Software Group.

IBM Corporation, Silicon Valley Lab, California, USA
Summer Internship **June 2006 - August 2006**

Summer co-op with DB2 for z/OS Query Semantic and Transformation, IBM Software Group.

The Pennsylvania State University, University Park, Pennsylvania, USA
Graduate Student **September 2003 - August 2008**

Research assistant at PIKE (Penn State Information, Knowledge and wEb) group. Worked on XML and relational database security.

The Chinese University of Hong Kong, Shatin, N.T., Hong Kong
Graduate Student **August 2001 - July 2003**

Research assistant at Multimedia Lab. Worked on video text detection/extraction, and multimedia information retrieval.

University of Science and Technology of China, Hefei, Anhui, China
Undergraduate Student **September, 1996 - June 2001**

Member of the Multimedia Communications Lab (since 1999) at the Information Processing Center, USTC. Participated in several research projects under the direction of Professor Zhengkai Liu and Professor Nenghai Yu.

Honors & Awards

Best paper award, Annual Computer Security Applications Conference (ACSAC) 2021

Miller Scholar, University of Kansas, 2021

Best paper award, Annual Computer Security Applications Conference (ACSAC) 2017

Miller Scholar, University of Kansas, 2017

Miller Scholar, University of Kansas, 2016

Miller Professional Development Award for Distinguished Service, University of Kansas, 2015

CPS Week Best Poster Finalist, 2015

Refereed Publications

* Graduate student or undergraduate honors student advised (co-advised) by Bo Luo
$^+$ Graduate/undergraduate student at KU EECS

Zeyan Liu*, Fengjun Li, Zhu Li, and **Bo Luo**. LoneNeuron: a Highly-effective Feature-domain Neural Trojan using Invisible and Polymorphic Watermarks. In *ACM Conference on Computer and Communications Security (CCS)*, Los Angeles, CA, USA, 2022

Mingrui Ai, Kaiping Xue, **Bo Luo**, Lutong Chen, Nenghai Yu, Qibin Sun, and Feng Wu. Blacktooth: Breaking through the Defense of Bluetooth in Silence. In *ACM Conference on Computer and Communications Security (CCS)*, Los Angeles, CA, USA, 2022

Ishrak Hayet*, Zijun Yao, and **Bo Luo**. Invernet: An Inversion Attack Framework to Infer Fine-Tuning Datasets through Word Embeddings. In *Findings of EMNLP*, 2022.

Zeyan Liu*, Fengjun Li, Jingqiang Lin, Zhu Li, and **Bo Luo**. Hide and Seek: on the

Stealthiness of Attacks against Deep Learning Systems. In *European Symposium on Research in Computer Security (ESORICS)*, Copenhagen, Denmark, 2022. (Acceptance rate: 18.5%)

Javaria Ahmad*, Fengjun Li, and Bo Luo. IoTPrivComp: A Measurement Study of Privacy Compliance in IoT Apps. In *European Symposium on Research in Computer Security (ESORICS)*, Copenhagen, Denmark, 2022. (Acceptance rate: 18.5%)

Tao Xue, Yu Wen, **Bo Luo**, Gang Li, Yingjiu Li, Boyang Zhang, Yang Zheng, Yanfei Hu, and Dan Meng. SparkAC: Fine-Grained Access Control in Spark for Secure Data Sharing and Analytics. In *IEEE Transactions on Dependable and Secure Computing (TDSC)*. (Accepted)

Wenchi Ma*, Xuemin Tu, **Bo Luo**, and Guanghui Wang. Semantic clustering based deduction learning for image recognition and classification. *Pattern Recognition*, vol.124, 2022.

Sohaib Kiani*, Sana Awan$^+$, Chao Lan, Fengjun Li, and Bo Luo. Two Souls in an Adversarial Image: Towards Universal Adversarial Example Detection using Multi-view Inconsistency. In *Annual Computer Security Applications Conference (ACSAC)*, 2021. (Acceptance rate: 24.5%) (ACSAC Distinguished Paper Award)

Sana Awan$^+$, **Bo Luo**, and Fengjun Li. CONTRA: Defending against Poisoning Attacks in Federated Learning. In *European Symposium on Research in Computer Security (ESORICS)*, 2021.

Prashanthi Mallojula*, Javaria Ahmad*, Fengjun Li, and **Bo Luo**. You Are (not) Who Your Peers Are: Identification of Potentially Excessive Permission Requests in Android Apps. In *IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2021.

Congwu Li, Le Guan, Jingqiang Lin, **Bo Luo**, Quanwei Cai, Jiwu Jing, Jing Wang. Mimosa: Protecting Private Keys against Memory Disclosure Attacks using Hardware Transactional Memory. In *IEEE Transactions on Dependable and Secure Computing (TDSC)*, vol. 18, iss. 3, 2021.

Lingjing Yu, **Bo Luo**, Jun Ma, Zhaoyu Zhou, and Qingyun Liu. You Are What You Broadcast: Identification of Mobile and IoT Devices from (Public) WiFi. In *USENIX Security Symposium*, 2020. (Acceptance rate: 16.1%)

Abdulmalik Humayed*, Fengjun Li, Jingqiang Lin, and **Bo Luo**. CANSentry: Securing CAN-Based Cyber-Physical Systems against Denial and Spoofing Attacks. In *European Symposium on Research in Computer Security (ESORICS)*, 2020. (Acceptance rate: 19.6%) [pdf]

Tao Xue, Yu Wen, **Bo Luo**, Boyang Zhang, Yang Zheng, Yanfei Hu, Yingjiu Li, Gang Li, and Dan Meng. GuardSpark++: Fine-Grained Purpose-Aware Access Control for Secure Data Sharing and Analysis in Spark. In *Annual Computer Security Applications Conference (ACSAC)*, 2020. (Acceptance rate: 23.2%)

Sohaib Kiani*, Sana Awan$^+$, Jun Huan, Fengjun Li, and **Bo Luo**. WOLF: Automated Machine Learning Workflow Management Framework for Malware Detection and Other Applications. In *Annual Hot Topics in the Science of Security Symposium (HoTSoS)*, 2020.

Fangjie Jiang, Quanwei Cai, Jingqiang Lin, **Bo Luo**, Le Guan, and Ziqiang Ma. TF-BIV: Transparent and Fine-grained Binary Integrity Verification in the Cloud. In *Annual Computer Security Applications Conference (ACSAC)*, 2019. (Acceptance rate: 22.6%).

Qiaozhi Wang*, Hao Xue$^+$, Fengjun Li, Dongwon Lee, and **Bo Luo**. #DontTweetThis: Scoring Private Information in Social Networks. In *19th Privacy Enhancing Technologies Symposium (PETS)*, 2019 (Acceptance rate: 16/91, Vol 4. 2019).

Zhaoyu Zhou, Lingjing Yu, Qingyun Liu, Yang Liu, and **Bo Luo**. Tear Off Your Disguise: Phishing Website Detection using Visual and Network Identities. In *International Conference on Information and Communications Security (ICICS)*, 2019.

Ziqiang Ma, Quanwei Cai, Jingqiang Lin, **Bo Luo**, and Jiwu Jing. Towards the Optimal Performance of Integrating WARM and DELAY against Remote Cache Timing Side Channels on Block Ciphers. In **Journal of Computer Security**, vol 27, iss. 5, 2019.

Adaku Uchendu, Jeffrey Cao, Qiaozhi Wang*, **Bo Luo**, and Dongwon Lee. Characterizing Man-made vs. Machine-made Chatbot Dialogs. In *Truth and Trust Online (TTO)*, 2019.

Linzhi Jiang, Liqun Chen, **Bo Luo**, Athanasios Giannetsos, Kaitai Liang, and Jinguang Han. Towards Practical Privacy-Preserving Processing over Encrypted Data in IoT: An Assistive Healthcare Use Case. In *IEEE Internet of Things Journal*, vol. 6, iss. 6, 2019.

Anirudh Narasimman*, Qiaozhi Wang*, Fengjun Li, Dongwon Lee, and **Bo Luo**. Arcana: Enabling Private Posts on Public Microblog Platforms. In *34th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC)*, Lisbon, Portugal, June 2019.

Le Guan, Chen Cao, Sencun Zhu, Jingqiang Lin, Peng Liu, Yubin Xia, and **Bo Luo**. Protecting Mobile Devices from Physical Memory Attacks with Targeted Encryption. In *12th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2019.

Hao Xue$^+$, Qiaozhi Wang*, **Bo Luo**, Hyunjin Seo, and Fengjun Li. Content-Aware Trust Propagation Towards Online Review Spam Detection. In *ACM Journal of Data and Information Quality (JDIQ)*, vol. 11, iss. 3, 2019.

Lei Yang$^+$, Chris Seasholtz*, **Bo Luo** and Fengjun Li. Hide Your Hackable Smart Home From Remote Attacks: The Multipath Onion IoT Gateways. In *European Symposium on Research in Computer Security (ESORICS)*, Barcelona, Spain, September 2018. (Acceptance rate: 19.7%)

Le Guan, Jingqiang Lin, Ziqiang Ma, **Bo Luo**, Luning Xia, and Jiwu Jing. Copker: A Cryptographic Engine against Cold-Boot Attacks. In *IEEE Transactions on Dependable and Secure Computing (TDSC)*, vol. 15, iss. 5, Sept-Oct 2018.

Chen Cao, Le Guan, Ning Zhang, Neng Gao, Jingqiang Lin, **Bo Luo**, Peng Liu, Ji Xiang, Wenjing Lou. CryptMe: Data Leakage Prevention for Unmodified Programs on ARM Devices. In *International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2018)*, 2018. (Acceptance rate: 22.8%)

Lingjing Yu, Sri Mounica Motipalli*, Dongwon Lee, Peng Liu, Heng Xu, Qingyun Liu, Jianlong Tan and **Bo Luo**. My Friend Leaks My Privacy: Modeling and Analyzing Privacy in Social Networks. In *ACM Symposium on Access Control Models and Technologies*

(SACMAT), Indianapolis, IN, June 2018.

Jianan Li, Chao Liu, Min Yu, **Bo Luo**, Song Li, Kai Chen, Weiqing Huang, and Bin Lv. FGFDect: A Fine-Grained Features Classification Model for Android Malware Detection. In *EAI International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2018. (Short Paper)

Le Guan, Shijie Jia, Bo Chen, Fengwei Zhang, **Bo Luo**, Jingqiang Lin, Peng Liu, Xinyu Xing, and Luning Xia. Supporting Transparent Snapshot for Bare-metal Malware Analysis on Mobile Devices. In *Annual Computer Security Applications Conference (ACSAC)*, 2017. **ACSAC Best Paper Award.**

Abdulmalik Humayed*, Jingqiang Lin, Fengjun Li, and **Bo Luo**. Cyber-Physical Systems Security – A Survey. In *IEEE Internet of Things Journal*. Volume: 4 Issue: 6, 2017.

Linzhi Jiang, Chunxiang Xu, Xiaofang Wang, **Bo Luo**, and Huaqun Wang. Secure outsourcing SIFT: Efficient and Privacy-preserving Image Feature Extraction in the Encrypted Domain. In *IEEE Transactions on Dependable and Secure Computing (TDSC)*, vol. 17, iss. 1, 2017.

Quanwei Cai, Jonathan Lutes*, Jingqiang Lin, and **Bo Luo**. A-Tor: Accountable Anonymity in Tor. In *International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2017. (Short Paper)

Chao Lan$^+$, Yuhao Yang*, Xiaoli Li$^+$, **Bo Luo**, and Jun Huan. Learning Social Circles in Ego-Networks based on Multi-View Network Structure. In *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, vol. 29, iss. 8, Aug 2017.

Qiaozhi Wang*, Jaisneet Bhandal*, Shu Huang and **Bo Luo**. Classification of Private Tweets. In *International Journal of Semantic Computing (IJSC), Special Issue on ICSC2017 Best Papers*, Vol. 11, No. 04, pp. 541-562, 2017. (6/26 papers were selected from ICSC 2017)

Abdulmalik Humayed*, and **Bo Luo**. Using ID-Hopping to Defend Against Targeted DoS on CAN. In *International Workshop on Safe Control of Connected and Autonomous Vehicles (SCAV), in conjunction with CPS Week 2017*, Pittsburgh, PA, 2017.

Qiaozhi Wang*, Jaisneet Bhandal*, Shu Huang and **Bo Luo**. Classification of Private Tweets using Tweet Content. In *IEEE International Conference on Semantic Computing (ICSC)*, San Diego, CA, 2017.

Yang Tian*, Ranjith Sompalli*, Guanghui Wang, and **Bo Luo**. Textual Ontology and Visual Features Based Search for a Paleontology Digital Library. In *IEEE International Conference on Tools with Artificial Intelligence (ICTAI)*, San Jose, 2016.

Jingqiang Lin, **Bo Luo**, Le Guan, and Jiwu Jing. Secure Computing using Registers and Caches: the Problem, Challenges and Solutions. In *IEEE Security & Privacy Magazine*, vol. 14, no. 6, 2016.

Fengjun Li, Xin Fu, and **Bo Luo**. POSTER: A Hardware Fingerprint Using GPU Core Frequency Variations. In *ACM Conference on Computer and Communications Security (CCS)*, Denver, CO, 2015 (Poster).

Le Guan, Jingqiang Lin, **Bo Luo**, Jiwu Jing, and Jing Wang. Protecting Private Keys against Memory Disclosure Attacks using Hardware Transactional Memory. In *IEEE Symposium on Security & Privacy (Oakland)*, 2015.

Manogna Thimma*, Fang Liu, Jingqiang Lin, and **Bo Luo**. HyXAC: Hybrid XML Access Control Integrating View-based and Query-rewriting Approaches. In *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, vol 27, issue 8, 2015.

Jamuna Gopal*, Shu Huang, and **Bo Luo**. FamilyID: A Hybrid Approach to Identify Family Information from Microblogs. In *29th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSec)*, Fairfax, VA, 2015.

Hariprasad Sampathkumar*, Xue-Wen Chen, and **Bo Luo**. Ontology-based Visualization of Healthcare Data Mined from Online Healthcare Forums. In *IEEE International Conference on Healthcare Informatics (ICHI)*, Dallas, TX, 2015.

Abdulmalik Humayed*, and **Bo Luo**. Poster Abstract: Cyber-Physical Security for Smart Cars – Taxonomy of Vulnerabilities, Threats, and Attacks. In *6th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*, Seattle, WA, 2015 (CPS Week Best Poster Finalist).

Abdulmalik Humayed*, and **Bo Luo**. Cyber-Physical Security for Smart Cars – Issues, Survey and Challenges. In *2nd International IFIP Workshop on Emerging Ideas and Trends in Engineering of Cyber-Physical Systems (EITEC)*, Seattle, WA, 2015.

Yuhao Yang*, Chao Lan$^+$, Xiaoli Li$^+$, **Bo Luo**, and Jun Huan. Automatic Social Circle Detection Using Multi-View Clustering. In *ACM Conf. on Information and Knowledge Management (CIKM)*, 2014 (Acceptance rate: 20.9%).

Wenrong Zeng*, Yuhao Yang*, and **Bo Luo**. Using Data Content to Assist Access Control for Large-Scale Content-Centric Databases. In *IEEE International Conference on Big Data (IEEE BigData)*, 2014 (Acceptance rate: 18.5%).

Hariprasad Sampathkumar*, Xue-wen Chen, and **Bo Luo**. Mining Adverse Drug Reactions from Online Healthcare Forums using Hidden Markov Model. *BMC Medical Informatics and Decision Making*, 14:91, 2014.

Le Guan, Jingqiang Lin, **Bo Luo**, and Jiwu Jing. Copker: Computing with Private Keys without RAM. In *Network and Distributed System Security Symposium (NDSS)*, 2014 (acceptance rate: 18%).

Meeyoung Park*, Hariprasad Sampathkumar*, **Bo Luo**, and Xue-wen Chen. Content-based Assessment of the Credibility of Online Healthcare Information. In *IEEE Workshop on Big Data in Bioinformatics and Health Informatics (IEEE BHI)*, Santa Clara, CA, 2013.

Wenrong Zeng*, Yuhao Yang*, and **Bo Luo**. Poster: Access Control for Big Data using Data Content. In *IEEE International Conference on Big Data*, Santa Clara, CA, 2013 (Poster).

Manogna Thimma*, Tsam Kai Tsui*, and **Bo Luo**. HyXAC: a hybrid approach for XML access control. In *ACM Symposium on Access Control Models and Technologies (SACMAT)*, Amsterdam, The Netherlands, June 2013.

Fengjun Li, **Bo Luo**, Peng Liu, Dongwon Lee, and Chao-Hsien Chu. Enforcing Secure and

Privacy-Preserving Information Brokering in Distributed Information Sharing. In *IEEE Transactions on Information Forensics & Security*, Vol. 8, Iss. 6, pp. 888-900, June 2013.

Yuxin Chen*, Hariprasad Sampathkumar*, **Bo Luo**, and Xue-wen Chen. iLike: Bridging the semantic gap in vertical image search by integrating text and visual features. In *IEEE Transactions on Knowledge and Data Engineering*, Vol. 25, Iss. 10, 2013.

Haibin Liu, **Bo Luo**, and Dongwon Lee. Location Type Classification Using Tweet Content. In *11th International Conference on Machine Learning and Applications (ICMLA)*, Boca Raton, FL, December, 2012.

Shu Huang, Min Chen, **Bo Luo**, and Dongwon Lee. Aggregate Social Activity Prediction by Using Continuous-time Stochastic Process. In *21st ACM Conf. on Information and Knowledge Management (CIKM)*, Maui HI, USA, October 2012. Acceptance Rate: 13.4%

Jingqiang Lin, **Bo Luo**, Jiwu Jing and Xiaokun Zhang. GRADE: Graceful Degradation in Byzantine Quorum Systems. In *31st International Symposium on Reliable Distributed Systems (SRDS)*, Irvine, CA, October 2012.

Fengjun Li, and **Bo Luo**. Preserving Data Integrity for Smart Grid Data Aggregation. In *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Tainan, November 2012.

Hariprasad Sampathkumar*, **Bo Luo**, and Xue-wen Chen. Mining Adverse Drug Side-effects from Online Medical Forums. In *IEEE Conference on Healthcare Informatics, Imaging, and Systems Biology (HISB)*, La Jolla, CA, September 2012 (poster).

Yuanliang Meng$^+$, Junyan Li$^+$, Patrick Denton$^+$, Yuxin Chen*, **Bo Luo**, Paul Selden and Xue-Wen Chen. IPKB: A Digital Library for Invertebrate Paleontology. In *ACM/IEEE Joint Conference on Digital Libraries (JCDL)*, Washington, DC, June 2012.

Yuxin Chen*, and **Bo Luo**. S2A: Secure Smart Household Appliances. In *ACM Conference on Data and Application Security and Privacy (CODASPY)*, San Antonio, TX, February 2012. Acceptance rate: 18.6%

Yuhao Yang*, Jonathan Lutes*, Fengjun Li, **Bo Luo** and Peng Liu. Stalking Online: on User Privacy in Social Networks. In *ACM Conference on Data and Application Security and Privacy (CODASPY)*, San Antonio, TX, February 2012. Acceptance rate: 18.6%

Hongliang Fei$^+$, Ruoyi Jiang$^+$, Yunhao Yang*, **Bo Luo**, and Jun Huan. Content based Social Behavior Prediction: A Multi-task Learning Approach. In *Proceedings of the 20th ACM International Conference on Information and Knowledge Management (CIKM)*, Glasgow, UK, October 2011. (short paper).

Avindra Fernando$^+$, Jun Huan, Justin Blumenstiel, Jin Li, Xue-wen Chen, and **Bo Luo**. Identification of Transposable Elements of the Giant Panda (Ailuropoda Melanoleura) Genome. *Workshop on Next-generation Sequencing Analysis, in conjunction with IEEE International Conference on Bioinformatics and Biomedicine*, Atlanta, GA, November 2011.

Bo Luo, Dongwon Lee, Wang-Chien Lee, and Peng Liu. QFilter: Rewriting Insecure XML Queries to Secure Ones using Non-Deterministic Finite Automata. In *The VLDB Journal*, Vol. 20, No. 3, pp.397-415, 2011.

Jonathan Lutes*, Meeyoung Park*, **Bo Luo**, and Xue-wen Chen. Healthcare Information Networks: Discovery and Evaluation. In *IEEE Conference on Healthcare Informatics, Imaging, and Systems Biology (HISB)*, San Jose, CA, July 2011.

Yuxin Chen*, Brian Potetz, **Bo Luo**, Xue-wen Chen, and Yunfeng Lin. Cephalometric Landmark Tracing Using Deformable Templates. In *IEEE Conference on Healthcare Informatics, Imaging, and Systems Biology (HISB)*, San Jose, CA, July 2011.

Fengjun Li, Yuxin Chen*, **Bo Luo**, Dongwon Lee and Peng Liu. Privacy-Preserving Group Linkage. In *23rd Scientific and Statistical Database Management Conference (SSDBM)*, Portland, OR, July 2011.

Fengjun Li, **Bo Luo**, and Peng Liu. Secure and Privacy-Preserving Information Aggregation for Smart Grids. In *International Journal of Security and Networks, Special Issue on Security and Privacy in Smart Grid*, Vol. 6, No.1 pp. 28 - 39, 2011.

Michael Steve Stanley Laine^{+}, Gunes Ercal, and **Bo Luo**. User Groups in Social Networks: An Experimental Study on YouTube. In *The 44th Hawaii International Conference on System Sciences (HICSS)*, Kauai, HI, Jan 2011.

Yuxin Chen*, Nenghai Yu, **Bo Luo**, and Xue-wen Chen. iLike: Integrating Visual and Textual Features for Vertical Search. In *ACM Multimedia*, Firenze, Italy, October 2010. Acceptance rate: 17%

Fengjun Li, **Bo Luo**, and Peng Liu. Secure Information Aggregation for Smart Grids Using Homomorphic Encryption. In *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Gaithersburg MD, October 2010.

Fengjun Li, **Bo Luo**, Peng Liu, and Chao-Hsien Chu. A Node-failure Resilient Anonymous Communication Protocol through Commutative Path Hopping. In *IEEE Conference on Computer Communications (INFOCOM)*, San Diego, CA, March 2010. Acceptance rate: 17.5%

Bo Luo, and Dongwon Lee. On Protecting Private Information in Social Networks: A Proposal. *In Workshop on Modeling, Managing, and Mining of Evolving Social Networks (M3SN) - in conjunction with IEEE ICDE*, Shanghai, China, 2009.

Fengjun Li, **Bo Luo**, Peng Liu, Dongwon Lee, and Chao-Hsien Chu. Automaton Segmentation: A New Approach to Preserve Privacy in XML Information Brokering. In *14th ACM Conf. on Computer and Communication Security (CCS)*, Alexandria, VA, USA, October 2007. Acceptance rate: 18%.

Bo Luo, Dongwon Lee, and Peng Liu. Pragmatic XML Access Control Enforcement using Off-the-shelf RDBMS. In *12th European Symposium On Research In Computer Security (ESORICS)*, Dresden, Germany, September 2007. Acceptance rate: 23%

Yan Xiao, **Bo Luo**, Dongwon Lee. Security-Conscious XML Indexing. In *12th International Conference on Database Systems for Advanced Applications (DASFAA)*, Bangkok, Thailand, April 2007.

Fengjun Li, **Bo Luo**, Peng Liu, Dongwon Lee, Prasenjit Mitra, Wang-Chien Lee, and Chao-Hsien Chu. In-broker Access Control: Towards Efficient End-to-End Performance of Information Brokerage Systems. *International Journal on Intelligent Control and Systems,* *Special Issue on Information Assurance*, 12(4): 283-292, Dec 2007.

Fengjun Li, **Bo Luo**, Peng Liu, Dongwon Lee, Prasenjit Mitra, Wang-Chien Lee, and Chao-Hsien Chu. In-broker Access Control: Towards Efficient End-to-End Performance of Information Brokerage Systems. In *Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC)*, IEEE Computer Society, Taiwan, June 2006. Acceptance rate: 25%

Bo Luo, Dongwon Lee, Wang-Chien Lee, and Peng Liu. Deep Set Operators for XQuery. In *Second International Workshop on XQuery Implementation, Experience and Perspectives (XIME-P)*, Baltimore, USA, Jun. 2005.

Bo Luo, Dongwon Lee, Wang-Chien Lee, and Peng Liu. QFilter: Fine-Grained Run-Time XML Access Control via NFA-based Query Rewriting. In *Proceedings of ACM Thirteenth Conference on Information and Knowledge Management (CIKM)*, pp 543-552, Washington D.C., USA, Nov. 2004. Acceptance rate: 19%

Bo Luo, Dongwon Lee, Wang-Chien Lee, and Peng Liu. A Flexible Framework for Architecting XML Access Control Enforcement Mechanisms. In *VLDB Workshop on Secure Data Management in a Connected World (Springer Lecture Notes in Computer Science, vol 3178)*, pp. 133-147, August 2004.

Kennis Tam, Lam Ching Yu, Dacheng Tao, Hao Liu, **Bo Luo**, and Xiaoou Tang. Content-Based SMIL Retrieval. In *Proceedings of Third International Conference on Image and Graphics (ICIG)*, pp 146-149, IEEE Computer Society Press, 2004.

Bo Luo, Xiaoou Tang, Jianzhuang Liu and Hongjiang Zhang. Video Caption Detection and Extraction Using Temporal Information. In *Proceedings of the IEEE International Conference on Image Processing (ICIP)*, vol. 1, pp. 297-300, Barcelona, Spain, September 2003.

Bo Luo, Xiaogang Wang, and Xiaoou Tang. A World Wide Web Based Image Search Engine Using Text and Image Content Features. In *Proceedings of IS&T/SPIE Electronic Imaging 2003, Internet Imaging IV*, pp. 123-130, Santa Clara, USA, Jan. 2003

Xiaoou Tang, **Bo Luo**, Xinbo Gao, Edwige Pissaloux, and Hongjiang Zhang. Video Text Extraction Using Temporal Feature Vectors. In *Proceedings of IEEE International Conference on Multimedia and Expo (ICME)*, vol. 1, pp. 85-88, Lausanne, Switzerland, Aug. 2002

Bin Xie, **Bo Luo**, and Fengjun Li. *Website Construction Under Linux*, Mechanical Industry Publishing House of China, ISBN 7-111-08156-0, May 2000. (in Chinese)

Invited Publications

Fengjun Li, **Bo Luo**, Peng Liu, Anna C. Squicciarini, Dongwon Lee, and Chao-Hsien Chu. Defending against Attribute-Correlation Attacks in Privacy-Aware Information Brokering. In *4th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*, Orlando, FL, USA, 2008.

Funding

NSF OIA-1028098: "CDI-Type II: Computational Methods to Enable an Invertebrate Paleontology Knowledgebase"; Role: Co-PI (with Xue-wen Chen); Amount: $1,532,523; Duration: 09/15/2010-09/15/2014.

- ○ Xue-wen Chen left KU in summer 2012. KU receive a sub-grant of $377,832. Bo Luo is the PI on the sub-grant.

NSF CNS-1321908: "KanSec: the Greater Kansas Area Security Workshop"; Role: PI; Amount: $16,000

NSF CNS-1422206: "SBE TWC: Small: Collaborative: Privacy Protection in Social Networks: Bridging the Gap Between User Perception and Privacy Enforcement"; Role: PI; Amount: $220,162; Duration: 10/01/2014-09/30/2017.

NSF IIS-1513324: "RAPID: III: Data Collection and Risk Evaluation Learning in Identifying High Risk Ebola Subpopulations for the Intervention and Prevention of Large-scale Ebola Virus"; Role: Co-PI; Amount: $188,730; Duration: 12/01/2015-11/30/2016.

NSF DGE-1565570: "CyberCorps: New Scholarships for Service (SFS) Program at the University of Kansas - Jayhawk SFS"; Role: PI; Amount: $4,697,514; Duration: 01/01/2016-12/31/2021.

NSA H98230-17-1-0281: "The University of Kansas GenCyber Summer Camp"; Role: PI; Amount: $99,875; Duration: 04/15/2017-04/16/2018.

NSA "Science of Security for Cyber-physical Systems"; Role: Co-PI, Lablet Leadership Team member; Amount: $14,752,121; Duration: 10/01/2017 - 09/30/2022.

NSF DGE-1922649: "NRT-HDR: Internet of Catalysis-Harnessing Data Science for Catalyst Design"; Role: Co-PI; Amount: $2,999,998; Duration: 09/01/2019-08/31/2024.

NSF IIS-2014552: "SCH: INT: Collaborative Research: Privacy-Preserving Federated Transfer Learning for Early Acute Kidney Injury Risk Prediction"; Role: Co-PI; Amount: $579,941; Duration: 10/01/2020-09/30/2024.

Teaching

* New Prep

Fall 2008
- *EECS700 Advanced Database Systems**. Enrollment: 19, Evaluation: 4.76/5.0

Spring 2009
- *EECS767 Information Retrieval**. Enrollment: 36, Evaluation: 4.80/5.0

Fall 2009
- *EECS647 Intro. to Database Systems**. Enrollment: 23, Evaluation: 4.29/5.0
- *EECS700 Advanced Database Systems*. Enrollment: 24, Evaluation: 4.65/5.0

Spring 2010
- *EECS767 Information Retrieval*. Enrollment: 34, Evaluation: 4.88/5.0

Fall 2010
- *EECS647 Intro. to Database Systems*. Enrollment: 26, Evaluation: 4.65/5.0
- *EECS761 Programming paradigm**. Enrollment: 24, Evaluation: 4.95/5.0

Spring 2011
- *EECS767 Information Retrieval*. Enrollment: 21, Evaluation: 5.0/5.0

Fall 2011
- *EECS168/169 Programming I**. Enrollment: 36, Evaluation: 4.48/5.0
- *EECS710 Information Security & Assurance**. Enrollment: 24, Evaluation: 4.86/5.0

Spring 2012
- *EECS767 Information Retrieval*. Enrollment: 16, Evaluation: 4.93/5.0

Fall 2012

- *EECS168/169 Programming I*. Enrollment: 90, Evaluation: 4.71/5.0
- *EECS647 Intro. to Database Systems*. Enrollment: 35, Evaluation: 4.92/5.0

Spring 2013

- *EECS690 Intro to Computer and Information Security**. Enrollment: 41, Evaluation: 4.97/5.0

Fall 2013

- *EECS746 Database Systems*. Enrollment: 28, Evaluation: 4.84/5.0

Spring 2014

- *EECS690 Intro to Computer and Information Security*. Enrollment: 25, Evaluation: 5.0/5.0
- *EECS767 Information Retrieval*. Enrollment: 34, Evaluation: 4.96/5.0

Fall 2014

- *EECS647 Intro. to Database Systems*. Enrollment: 47, Evaluation: 4.58/5.0

Spring 2015

- *EECS565 Intro to Computer and Information Security*. Enrollment: 58, Evaluation: 4.89/5.0
- *EECS746 Database Systems*. Enrollment: 38, Evaluation: 4.91/5.0

Fall 2015

- *EECS765 Intro to Cryptography and Computer Security**. Enrollment: 23, Evaluation: 4.84/5.0

Spring 2016

- *EECS565 Intro to Computer and Information Security*. Enrollment: 52, Evaluation: 4.84/5.0
- *EECS767 Information Retrieval*. Enrollment: 40, Evaluation: 4.88/5.0

Fall 2016

- *EECS565 Intro to Computer and Information Security*. Enrollment: 22, Evaluation: 4.62/5.0
- *EECS765 Intro to Cryptography and Computer Security*. Enrollment: 18, Evaluation: 4.93/5.0

Fall 2017

- *EECS700 Digital Forensics**. Enrollment: 20, Evaluation: 4.73/5.0

Spring 2018

- *EECS565 Intro to Computer and Information Security*. Enrollment: 57, Evaluation: 4.46/5.0
- *EECS767 Information Retrieval*. Enrollment: 35, Evaluation: 4.71/5.0

Fall 2018

- *EECS700 Digital Forensics*. Enrollment: 19, Evaluation: 4.67/5.0

Spring 2019

- *EECS565 Intro to Computer and Information Security*. Enrollment: 51, Evaluation: 4.74/5.0
- *EECS647 Intro to Database Systems*. Enrollment: 39, Evaluation: 4.80/5.0

Fall 2019

- *EECS690 Digital Forensics*. Enrollment: 20, Evaluation: 4.71/5.0

Spring 2020

- *EECS565 Intro to Computer and Information Security*. Enrollment: 39
- *EECS647 Intro to Database Systems*. Enrollment: 77

Fall 2020

- *EECS569 Digital Forensics.* Enrollment: 26

ADVISING

Committee Chair: Doctoral

Zeyan Liu
- Dissertation topic (tentative): "Adversarial Machine Learning"

Javaria Ahmad
- Dissertation topic (tentative): "TBD (IoT and Privacy)"

Prashanthi Mallojula
- Dissertation topic (tentative): "TBD (Privacy)"

Sohaib Kiani
- Dissertation topic (tentative): "IoT Security and Privacy"
- Expected Graduation: Spring 2021;

Chris Seasholtz
- Dissertation topic (tentative): "IoT Security and Privacy"
- Expected Graduation: Spring 2021;

Wenchi Ma (Co-advised with Guanghui Wang)
- Dissertation: "Object Detection and Classification based on Hierarchical Semantic Features and Deep Neural Networks"
- Graduation: Summer 2021

Qiaozhi Wang
- Dissertation: "Towards the Understanding of Private Content – Content-based Privacy Assessment and Protection in Social Networks"
- Graduation: Spring 2020
- Current Employment: Machine Learning Engineer, Apple

Abdulmalik Humayed
- Dissertation: "Securing CAN-Based Cyber-Physical Systems"
- Graduation: Fall 2018
- Current employment: Assistant Professor, Jazan University

Hariprasad Sampathkumar
- Dissertation: "A Framework for Information Retrieval and Knowledge Discovery from Online Healthcare Social Networks"
- Graduation: Fall 2015 (Part-time student); Ph.D. Proposal passed: Spring 2013

Wenrong Zeng
- Dissertation: "Content-Based Access Control for Relational Database Management Systems"
- Graduation: Spring 2015; Ph.D. Proposal passed: Spring 2013
- Senior Data Scientist, LinkedIn

Yuhao Yang
- Dissertation: "Protecting Attributes and Contents in Online Social Networks"
- Graduation: Spring 2014; Ph.D. Proposal passed: Spring 2013
- Employment: Software Engineer, Microsoft

Meeyoung Park (co-advised with Xue-wen Chen)
- Dissertation: "HealthTrust: Assessing the Trustworthiness of Healthcare Information on the Internet"

- Graduation: Fall 2013; Ph.D. Proposal passed: Fall 2012
- First Employment: Postdoctoral Fellow, University of Michigan

Jong Cheol Jeong (co-advised with Xue-wen Chen)

- Dissertation: "New methodology measuring semantic functional similarity based on bidirectional integration"
- Graduation: Spring 2013
- Current Employment: Assistant Professor, University of Kentucky

Committee Chair: Master's

Lei Wang

- I Know What You Type on Your Phone: Keystroke Inference on Android Device Using Deep Learning
- Spring 2019

Shahammadullah Shaik

- Semi-Supervised Entity Recognition in Noisy Text
- Spring 2018

Sri M Motipalli

- Analysis of Privacy Protection Mechanisms in Social Networks using the Social Circle Model
- Spring 2018

Xi Chen

- A Two-layer Text Classifier for Private Tweets
- Summer 2017

Jaisneet Bhandal

- Classification of Private Tweets using Tweets Content
- Spring 2017

Yang Tian

- Integrating Textual Ontology and Visual Features for Content Based Search in an Invertebrate Paleontology Knowledgebase
- Summer 2016

Anil Pediredla

- Information Revelation and Privacy in Online Social Networks
- Summer 2016

Chris Seasholtz

- Security and Privacy Vulnerabilities in Unmanned Aerial Vehicles
- Spring 2016

Ranjith Sompalli

- Computational Methods to Enable an Invertebrate Paleontology Knowledge Base
- Spring 2016

Anirudh Narasimman

- Arcana: Private Tweets on a Public Microblog Platform
- Spring 2016

Caitlin McCollister

- Predicting Author Traits Through Topic Modeling of Multilingual Social Media Text

- Spring 2016;

Sambhav Sethia
- Sentiment Analysis on Wikipedia People Pages Using Enhanced Naive Bayes Model
- Spring 2015;

Jonathan Lutes
- SafeExit: Exit Node Protection for TOR
- Spring 2015;

Jamuna Gopal
- I Know Your Family: A Hybrid Information Retrieval Approach to Extract Family Information from Microblogs
- Summer 2014;

Yuanliang Meng
- Building an Intelligent Knowledgebase of Brachiopod Paleontology
- Summer 2013;

Manogna Thimma
- Hybrid XML Access Control
- Summer 2012;

Yuxin Chen
- Integrating Visual and Textual Features for Image Search
- Summer 2011;

Sandeep Kakarla
- Thesis/Report: Incorporating Boolean Querying into Keyconcept
- Fall 2010;

Professional Service

Program Committee Member, 18th International Conference on Applied Cryptography and Network Security (ACNS) 2020

Program Committee Member, The 21st International Conference on Information and Communications Security (ICICS) 2019

PC Area Chair, IEEE International Conference on Multimedia and Expo (ICME), 2019

Program Committee Member,IEEE International Conference on Machine Learning and Applications (ICMLA) 2019

Program Committee Member, 5th ACM Cyber-Physical System Security Workshop (CPSS) 2019

Panelist, NSF, February 2018.

Track Chair, IEEE International Conference on Mobile Ad hoc and Sensor Systems (MASS), 2018.

Program Committee Member, 4th ACM Cyber-Physical System Security Workshop (CPSS) 2018

Conference Chair, IEEE International Conference on Machine Learning and Applications (ICMLA), December 2017.

Panelist, NSF, February, March, April, September 2017.

Panelist, NSF, April 2016.

Program Committee Member, IEEE International Conference on Machine Learning and Applications (ICMLA), December 2016.

Program Committee Member, AAAI Fall Symposium on Privacy and Language Technologies (PLT), 2016.

Panelist, NIH, 2015.

Program Committee Member, IEEE International Conference on Machine Learning and Applications (ICMLA), December 2015.

Program Committee Member, IEEE International Conference on Cyber Security and Cloud Computing (CSCloud), 2015.

Registration Chair, IEEE International Conference on Bioinformatics and Biomedicine (BIBM), 2015.

Program committee member: 6th International Symposium on Cyberspace Safety and Security, Paris, France, August, 2014.

Program committee member, workshop chair: IEEE International Conference on Machine Learning and Applications (ICMLA), Detroit, MI, December 2014.

Program committee member: The 16th International Asia-Pacific Web Conference (AP-Web), Changsha, China, September 2014

Program committee member: IEEE International Conference on Machine Learning and Applications (ICMLA), Miami, FL, December 2013.

Program committee member: The 15th International Asia-Pacific Web Conference (AP-Web), Sydney, Australia, April, 2013

Organizing committee chair: KanSec: The 3rd Greater Kansas Area Security Workshop, The University of Kansas, March 2013.

Senior program committee member (meta-reviewer): IEEE International Conference on Machine Learning and Applications (ICMLA), December 2012.

Organizing committee member: KanSec: The 2nd Greater Kansas Area Security Workshop, Fort Hays State University, October 2012.

Special Session Co-Chair: IEEE International Conference on Machine Learning and Applications, Special Session on Learning on the Web, Boca Raton, FL, 2012

Treasurer: ACM Conference on Information and Knowledge Management (CIKM), Maui, HI, USA, 2012.

Financial Chair: Second IEEE Conference on Healthcare Informatics, Imaging, and Systems Biology (HISB), La Jolla, California, USA, 2012.

Co-founder and Organizing committee member: The 1st Greater Kansas Area Security Workshop, Kansas State University, March 2012.

Publicity Co-Chair: IEEE International Conference on Machine Learning and Applications (ICMLA), Honolulu, USA, December 2011.

Program committee member: International Conference on Image and Graphics, Hefei, China, August 2011

Financial Chair: First IEEE Conference on Healthcare Informatics, Imaging, and Systems Biology (HISB), 2011

Program committee member: The Third International Conference on Emerging Databases (EDB), 2011

Program committee member: The FTRA Third International Workshop on Privacy Enhanced Technology and Security Engineering (PETSE), 2011

Special Session Co-Chair: The Ninth International Conference on Machine Learning and Applications (ICMLA 2010), Special Session on Learning for Web-based Knowledge Discovery

Area Chair: IEEE Workshop on Mining and Management of Biological and Health Data, in conjunction with IEEE International Conference on Bioinformatics & Biomedicine, 2010

Program committee member: The 2nd International Conference on Internet (ICONI), 2010

Program committee member: International Workshop on Wireless Computing and System (WCS), in conjunction with The IEEE Sixteenth International Conference on Parallel and Distributed Systems (ICPADS), 2010

Program committee Member: The 18th ACM Conference on Information and Knowledge Management (CIKM), 2009

Program committee Member: The 11th ACM International Workshop on Web Information and Data Management (WIDM), 2009

Program committee Member: The 12th International Asia-Pacific Web Conference (AP-Web), 2009

Journal reviewer: *IEEE Transactions on Information Forensics and Security*

Journal reviewer: *IEEE Transactions on Dependable and Secure Computing*

Journal reviewer: *IEEE Internet of Things Journal*

Journal reviewer: *IEEE Transactions on Smart Grid*

Journal reviewer: *IEEE Transactions on Knowledge and Data Engineering*

Journal reviewer: *IEEE Transactions on Systems, Man, and Cybernetics: Part B*

Journal reviewer: *Elsevier Information Systems*

Journal reviewer: *Elsevier Information Sciences*

Journal reviewer: *Elsevier Computers & Security*

Journal reviewer: *Elsevier Neurocomputing*

Journal reviewer: *Elsevier Computer Vision and Image Understanding*

Journal reviewer: *Journal of Computer Science and Technology*

Journal reviewer: *Pattern Recognition Letters*

Journal reviewer: *Journal of Database Management*

Journal reviewer: *Data & Knowledge Engineering*, 2006