Cyber Security Capabilities at The University of Texas at Dallas (UTD)

Accomplishments
June 2004 - May 2020

Cyber Security Research and Education Institute (CSI)
http://csi.utdallas.edu

Dr. Bhavani Thuraisingham
Founding Executive Director

May 31, 2020

Outline

- **Faculty**
- **History and Accomplishments**
- **Sponsors**
- **Research and Education Collaborations**
- **Research Thrusts**
- **Education Programs, Research Prototypes and Tools, I/UCRCs**
- **Affiliated I/UCRC (Sample)**
- **Cyber Operations Lab**
- **Summary and Directions**
- **Contact**

Our Faculty

Founder

- Bhavani Thuraisingham, PhD, DEng (U of Wales, U of Bristol - UK) (Prof.)

Core Faculty from the Jonsson School of Engineering and Computer Science (ECS)

- Kanad Basu, PhD (U of FL) Hardware Security (Asst. Prof)
- Feng Chen, PhD (VA Tech) Machine Learning/AI (Assoc. Prof.)
- Yvo Desmedt, PhD (U. Leuven-Belgium) Cryptography (Prof.)
- Zygmunt Haas, PhD (Stanford) Wireless Network Security (Prof.)
- Kevin Hamlen, PhD (Cornell) Language and Software Security (Prof.)
- Shuang Hao, PhD (GATech) Network Security, Measurements and DNS Attacks (Asst. Prof.)
- Kangkook Jee, PhD (Columbia) Systems Security, Malware Analysis (Asst. Prof.)
- Murat Kantarcioglu, PhD (Purdue) Data Security and Privacy (Prof.)
- Latifur Khan, PhD (U of Southern CA) Big Data Analytics for Security (Prof.)
- Chong Kim, PhD (Purdue), Cyber Physical Systems, IoT Security (Asst. Prof.)
- Yiorgos Makris, PhD (UC San Diego) Hardware Security (Prof.)
- Kamil Sarac, PhD (UC Santa Barbara) Cyber Security Education, Network Measurements (Prof.)
- Weili Wu, PhD (U of MN), Data Science, Social Media (Prof.)
- Wei Yang, PhD (UIUC), Systems Security and Software Engineering (Asst. Prof.)
- I-Ling Yen, PhD (U of Houston) IoT and Web Services Security (Prof.)

Our Faculty*

Core faculty from other schools at UT Dallas

- Alain Bensoussan, PhD (University of Paris) Risk Analysis for Security (SoM) (Prof.)
- Patrick Brandt, PhD (Ohio State U) Political Science (EPPS) (Prof.)
- Yulia Gel, PhD (St. Petersburg State University), Statistics and Machine Learning (NSM) (Prof.)
- Jennifer Holmes, PhD (U of MN) Cyber Security Policy (Dean of EPPS and Prof.)
- Daniel Krawczyk, PhD (UCLA) Psychosocial/Behavioural Aspects of Security (BBS) (Prof.)

Several affiliated faculty from ECS (Sample)

- Farokh Bastani, PhD (UC Berkeley) I/UCRC, Software Engineering (Prof.)
- Jorge Cobb, PhD (UTAustin) Cyber Security Outreach, Reliable Networks (Assoc. Prof.)
- Ebru Cankaya, PhD (Ege University) Women in Cyber Security (Assoc. Prof. of Instruction)
- Neeraj Gupta, PhD (U. of North TX) Digital Forensics (Asst. Prof. of Instruction)
- Cong Liu, PhD (UNC) Real-time Systems Security (Assoc. Prof.)
- Neeraj Mittal, PhD (UT Austin) Distributed Systems Security (Assoc. Prof.)
- Sriraam Natarajan, PhD (Oregon State U) Machine Learning (Assoc. Prof.)
- Nicholas Ruozzi, PhD (Yale U) Machine Learning (ECS) (Asst. Prof.)
- Shiyi Wei, PhD (VA Tech) Software Engineering and Security (Asst. Prof.)
- Eric Wong, PhD (Purdue), Reliable Software Engineering (Prof.)

Research Scientists/Post-Docs (Sample)

- Yan Zhou, PhD (Washington U) Machine Learning and Security
- Erick Bauman, PhD (UT Dallas) Systems Security

*** SoM: School of Management**
EPPS: Economics, Policy and Political Sciences
NSM: Natural Sciences and Mathematics
BBS: Brain and Behavioral Sciences
ECS: Engineering and Computer Science

Our Faculty

ARL South POC at UT Dallas and Research Collaborator

- Jonathan Bakdash, PhD (U of VA) Behavioural Aspects of Security

Administration

- Ms. Rhonda Walls (Project Coordinator)

Alumni/Emeritus Faculty

- Michael Baron, PhD (U of MD) Statistical Methods for Security (*Prof., American University)
- Nathan Berg, PhD (U of Kansas) Economics and Security (*Prof., U of Otago, New Zealand)
- Alvaro Cardenas, PhD (U of MD) Cyber Physical Systems Security (*Assoc Prof., UC Santa Cruz)
- Douglas Harris, PhD (SMU) Emeritus Professor and Initiator of Cyber Security at UTD
- Zhiqiang Lin, PhD (Purdue) Systems Security and Forensics (*Assoc. Prof., Ohio State)
- J.V. Rajendran, PhD (NYU) Hardware Security (* Asst. Prof., TAMU))

Alumni Lecturers/Research Scientists/Post-Docs (Sample)

- Jan Kallberg, PhD (UT Dallas) (*Asst Prof., West Point US Military Academy)
- Mehedy Masud, PhD (UT Dallas), Malware Analysis, Data Science (*Asst. Prof., U of UAE)
- Cuneyt Gurcan Akcora, PhD (Univ. Insubria), Blockchain (*Asst. Prof., U of Manitoba)
- Mamoun Awad, PhD (UT Dallas), Data Science, Cyber Security (*Asst. Prof., U. of UAE)
- Chuanjun Li, PhD (UT Dallas), 2006-2007 (*Postdoc at Brown University)
- Greg Lee, PhD (U of Washington) (*Asst. Prof., Case Western)
- Nathan McDaniel, MS (UT Dallas) (*Research Scientist, Applied Research Center)
- Tyrone Cadenhead, PhD (UT Dallas) (*Senior Scientist, Blue Cross Blue Shield)
- Janell Straach, PhD (UT Dallas), Women in Cyber Security (*Lecturer, Rice U)

*** Position after UT Dallas**

Our History and Accomplishments

- **NSA/DHS Center of Academic Excellence in Cyber Security Education, June 2004 (CAE)**
- **SAIAL (Security Analysis and Information Assurance Laboratory), July 2004**
- **NSA/DHS Center of Academic Excellence in Cyber Security Research, June 2008 (CAE-R)**
- **First NSF SFS Grant, 2010; Follow-on grants 2014, 2019; Multiple NSF Capacity Development Grants including in Secure Cloud Computing, Big Data Security and Privacy, Blockchain**
- **Annual TexSAW (Texas Security Awareness Week) established in October 2011**
- **Hosted NIST Cyber Security Information Sharing Symposium, September 2013**
- **NSA/DHS CAE and CAE-R certifications under the NSA's new requirements in June 2014**
- **Presentations at the National Privacy Research Strategy meeting on February 18-20, 2015 in Arlington VA, and assist in developing programs**
- **Member of NIST FFRDC in Cyber Security with MITRE and U of MD System**
- **NSA/DHS Center of Academic Excellence in Cyber Operations in June 2015; first university in TX and 14th in the US**
- **Hosted/Chaired Women in Cyber Security (WiCyS) conference (April 2016) and established Center for Engaging Women in Cyber Security, Sept. 2016**
- **Hosted ACM CCS (#1 Cyber Security Research Conference) in October 2017 and top Data Science conferences IEEE ICDM (Dec. 2013), and IEEE ICDE (April 2020 – Virtual); Also hosted several prestigious smaller conferences ACM CODASPY (March 2019), SecureComm (Oct. 2015), IEEE ISI (June 2009) and SKM (Nov. 2008)**

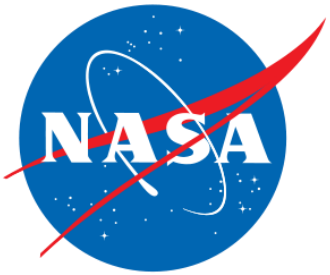
Our History and Accomplishments

- **$50M+ in competitive research funding and $15M+ in education funding in 15+ years**
- **Prestigious grants and contracts including the following:**
  - **Multiple NSF CAREER (100% success for NSF CAREER)**
  - **Multiple AFOSR YIP**
  - **DoD MURI, DURIP and several Mini-MURIs ($1-2M+ grants).**
  - **Multiple NSF MRI (Major Research Instrumentation)**
  - **NSF Large SaTC and multiple Medium SaTC**
  - **NSA Research Grant Competition held in 2015**
  - **Highly Competitive and Prestigious NSF/VMware and NSF/Amazon Partnership Grants**
  - **UT System National Security Network Grant**
  - **NSA Lablet in Science of Security (SoS) (2017)**
  - **DHS Grants in Cyber Physical Systems**
  - **NSF COVID-19 Rapid Grants (2020)**
- **Fellowships and Awards:**
  - **Multiple IEEE Fellows, ACM, AAAS, IACR, NAI Fellowships, multiple IBM Faculty Awards, NSA Science of Security Best Paper Award (2019), multiple IEEE and ACM Awards:**
    - **e.g., IEEE CS Technical Achievement Award, IEEE ComSoc Technical Recognition Awards, ACM SIGSAC Outstanding Contributions Award, multiple IEEE SMC/Homeland Security Technical Achievement Awards, ACM CODASPY Lasting Research Award, IEEE CS Services Computing Research Innovation Award, multiple ACM SACMAT 10 year Test of Time Awards**
    - **AFCEA Medal of Merit, multiple Dallas Business Journal Women in Technology Awards**

Our History and Accomplishments

- **Numerous keynote addresses, top-tier journal and conference publications (e.g., IEEE S&P, ACM CCS, ACM KDD, ACM SIGMOD, IEEE ICDM, USENIX Security, NDSS, PVLDB, IEEE ICDE, AAAI, IJCAI, open source tools, multiple patents, books).**
- **Prestigious lectures including UT Dallas Polycarp Kusch Lecture**
- **Affiliated I/UCRCs (Industry University Cooperative Research Centers in Cloud Computing, Hardware Security and Secure Software Engineering)**
- **Ten year celebration in 2014 with presentations and *CODEBREAKER* screening on life of Alan Turing**
- **Students Graduation and Placements (SFS students and PhD students):**
  - **Graduated around 80 PhD students (advised by Core ECS faculty) and numerous MS students in the Information Assurance (Cyber Security) track**
  - **Diversity: Significant percentage of female students as well as students from the African American, Hispanic American and LGBTQ groups.**
  - **Government: NSA, CIA, NAVAIR, Federal Reserve, …**
  - **FFRDC and Labs: MITRE, MIT Lincoln, Applied Physics Lab, Sandia, Los Alamos, Lawrence Livermore, …**
  - **Industry: IBM TJ Watson, Google, Microsoft, Amazon, E-Bay, Yahoo, Raytheon, L-3, TI, HP, VCE, Ericsson, AT&T, Blue Cross Blue Shield, Cisco, Facebook, Intel, Linkedin, …**
  - **US Academia: UNCC, Clemson, UCSD Medical School, Vanderbilt Medical School, UT Southwestern Medical Center, US Military Academy at West Point…**

Thanks to Our Sponsors



IARPA
BE THE FUTURE

MITRE

AirForce SBIR/STIR

Sandia National Laboratories

Tektronix

vmware

Raytheon

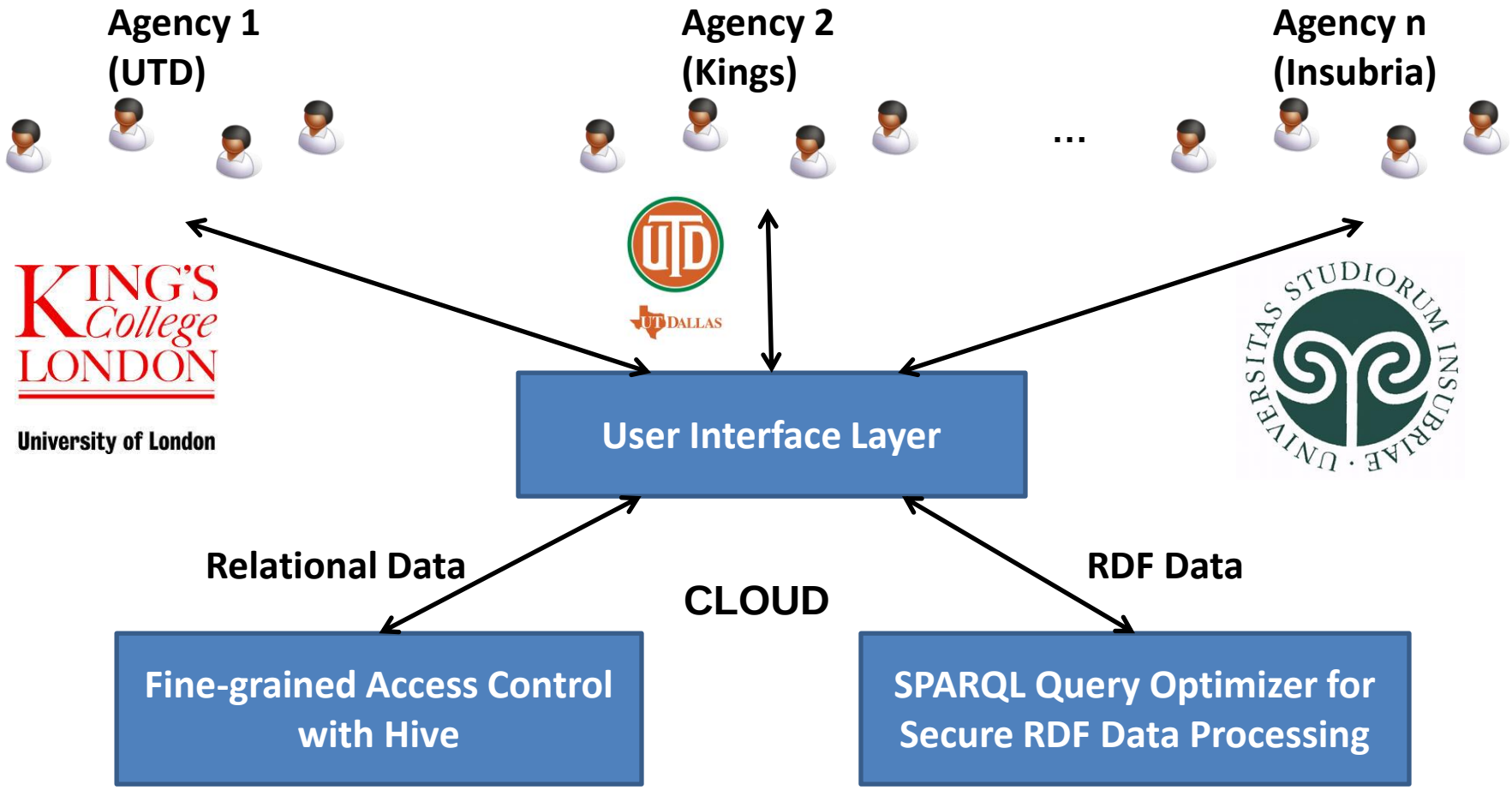
NOKIA

Our Academic Collaborators (Sample)

UTD/Kings College, London/U of Insubria, Italy Collaboration sponsored by AFOSR/EOARD

Cloud-based Assured Information Sharing

http://www.wpafb.af.mil/News/Article-Display/Article/400150/afosr-funded-initiative-creates-more-secure-environment-for-cloud-computing/



Initial List of Nine Collaborators on Funded INSuRE NSA/NSF Project

Other Collaborations (Sample)

- **ARL South: Research on Adversarial Machine Learning**
  - **UTD focus on Computer Sciences; ARL focus on Behavioral Sciences**
  - **Participated in the following ARL Planning Workshops**
    - **Cyber Fogginess (January 2016)**
    - **Research Directions for BAA (November 2017)**
    - **Organized ARL Workshop in Dallas on Adversarial Machine Learning (November 2018)**
- **AFRL: UTD faculty have participated as visiting scientist**
  - **Cloud Computing Security**
- **Collaboration with NIST**
  - **Member of the Academic Advisory Council for NIST FFRDC**
  - **Research Collaboration with NIST on Cyber Physical Systems Security**
  - **Participating in NIST Big Data Security and Privacy Working Group**
- **Discussions with NSA TX**
  - **Science of Security Lablet in Cyber Physical Systems funded in December 2017 (subcontract from Vanderbilt University)**
  - **Multiple NSA funded projects on research and curriculum development in Big Data Analytics, Security and Privacy (2017-Present)**
- **Collaborations with corporations including Raytheon, IBM, Lockheed**

Research Thrust - 1

- **Software Security and Active Malware Defense (Hamlen et al)**
  - **Sponsors: NSF, AFOSR, NSA, NASA, ONR, DARPA,Sandia, Raytheon, Lockheed**
    - **Reactively Adaptive Malware and Frankenstein; Reverse Engineering for Malware Detection; Android Malware Detection; Host Health Management; Author Attribution**

- Frederico Araujo**, Kevin W. Hamlen**, Sebastian Biedermann, Stefan Katzenbeisser: From Patches to Honey-Patches: Lightweight Attacker Misdirection, Deception, and Disinformation. ACM Conference on Computer and Communications Security 2014: 942-53
- Richard Wartell, Vishwath Mohan, **Kevin W. Hamlen**, **Zhiqiang Lin**: Binary stirring: self-randomizing instruction addresses of legacy x86 binary code. ACM Conference on Computer and Communications Security 2012: 157-168
- David Sounthiraraj, Justin Sahs, Garret Greenwood, **Zhiqiang Lin**, **Latifur Kha**n: SMV-Hunter: Large Scale, Automated Detection of SSL/TLS Man-in-the-Middle Vulnerabilities in Android Apps. NDSS 2014
- Yangchun Fu, **Zhiqiang Lin**, **Kevin W. Hamlen**: Subverting system authentication with context-aware, reactive virtual machine introspection. ACSAC 2013: 229-238
- Vishwath Mohan, **Kevin W. Hamlen**: Frankenstein: Stitching Malware from Benign Binaries. WOOT 2012: 77-84
- Ehab Al-Shaer, Jinpeng Wei, **Kevin W. Hamlen**, Cliff Wang: Autonomous Cyber Deception - Reasoning, Adaptive Planning, and Evaluation of HoneyThings. Springer 2019.

Research Thrust - 2

- **Data Security and Privacy (Kantarcioglu, Thuraisingham et al)**
  - **Sponsors: NSF, ARO, NIH, AFOSR, ONR, NSA**
    - **Privacy Preserving Record Linkage and Mining; Adversarial Machine Learning; Secure Data Provenance; Policy and Incentive-based Assured Information Sharing; Security and Privacy for Social Networks; Inference Control; Risk-aware Data Security, Data Science for COVID-19 and Security/Privacy.**

- Yan Zhou, **Murat Kantarcioglu**, **Bhavani M. Thuraisingham**, Bowei Xi: Adversarial support vector machine learning. KDD 2012: 1059-1067
- Mohammad Saiful Islam, Mehmet Kuzu, **Murat Kantarcioglu**: Inference attack against encrypted range queries on outsourced databases. CODASPY 2014: 235-246
- Mehmet Kuzu, **Murat Kantarcioglu**, Elizabeth Ashley Durham, Csaba Tóth, Bradley Malin: A practical approach to achieve private medical record linkage in light of public resources. JAMIA 20(2): 285-292 (2013)
- Raymond Heatherly, **Murat Kantarcioglu**, **Bhavani M. Thuraisingham**: Preventing Private Information Inference Attacks on Social Networks. IEEE Trans. Knowl. Data Eng. 25(8): 1849-1862 (2013)
- Hyo-Sang Lim, Gabriel Ghinita, Elisa Bertino, **Murat Kantarcioglu**: A Game-Theoretic Approach for High-Assurance of Data Trustworthiness in Sensor Networks. ICDE 2012: 1192-1203
- **Bhavani M. Thuraisingham**, Tyrone Cadenhead, **Murat Kantarcioglu**, Vaibhav Khadilkar: Secure Data Provenance and Inference Control with Semantic Web. CRC Press 2014, ISBN 978-1-4665-6943-0

Research Thrust - 3

- **Secure Cloud Computing and Social Media (Thuraisingham et al)**
  - **Sponsors: AFOSR, NSF, VMware**
    - **Virtual Machine Introspection and VM Space Traveler; Secure Virtualization; Hybrid Cloud Security; Secure Cloud Data Storage; Secure Cloud Query Processing; Assured Information Sharing in the Cloud**

- Yangchun Fu, **Zhiqiang Lin**: Space Traveling across VM: Automatically Bridging the Semantic Gap in Virtual Machine Introspection via Online Kernel Data Redirection. IEEE Symposium on Security and Privacy 2012: 586-600
- Alireza Saberi, Yangchun Fu, **Zhiqiang Lin**: Hybrid-Bridge: Efficiently Bridging the Semantic-Gap in VMI via Decoupled Execution and Training Memoization. NDSS 2014
- Erman Pattuk, **Murat Kantarcioglu**, **Zhiqiang Lin**, Huseyin Ulusoy: Preventing Cryptographic Key Leakage in Cloud Virtual Machines. USENIX Security 2014: 703-718
- Safwan Mahmud Khan, **Kevin W. Hamlen**: Hatman: Intra-cloud Trust Management for Hadoop. IEEE CLOUD 2012: 494-501
- Kerim Yasin Oktay, Vaibhav Khadilkar, Bijit Hore, **Murat Kantarcioglu**, Sharad Mehrotra, Bhavani M. Thuraisingham: Risk-Aware Workload Distribution in Hybrid Clouds. IEEE CLOUD 2012: 229-236
- **B. Thuraisingham**, et al, Analyzing an Securing Social Networks, CRC Press, 2016.

Research Thrust - 4

- **Cyber Physical Systems and IoT Security (Gee, Kim, Liu, et al)**
  - **Sponsors: NSF, NSA, MITRE, NIST, Intel, AFOSR, DHS**
    - **Control Systems Security, Integrating Secure Systems with Real-time Systems, Policy-related Security**

- Carlos Barreto, Jairo Alonso Giraldo, **Alvaro A. Cárdenas**, Eduardo Mojica-Nava, Nicanor Quijano: Control Systems for the Power Grid and Their Resiliency to Attacks. IEEE Security & Privacy 12(6): 15-23 (2014)
- Junia Valente, **Alvaro A. Cárdenas**: Using Visual Challenges to Verify the Integrity of Security Cameras. ACSAC 2015: 141-150
- **Cong Liu**, Jian-Jia Chen: Bursty-Interference Analysis Techniques for Analyzing Complex Real-Time Task Models.RTSS 2014: 173-183
- Jian-Jia Chen, Wen-Hung Huang, **Cong Liu**: k2U: A General Framework from k-Point Effective Schedulability Analysis to Utilization-Based Tests. RTSS 2015: 107-118
- Suphannee Sivakorn, **Kangkook Jee**, Yixin Sun, Lauri Kort-Parn, Zhichun Li, Cristian Lumezanu, Zhenyu Wu, Lu-An Tang, Ding Li: Countering Malicious Processes with Process-DNS Association. NDSS 2019
- Taegyu Kim, **Chung Hwan Kim**, Junghwan Rhee, Fan Fei, Zhan Tu, Gregory Walkup, Xiangyu Zhang, Xinyan Deng, Dongyan Xu: RVFuzzer: Finding Input Validation Bugs in Robotic Vehicles through Control-Guided Testing. USENIX Security Symposium 2019: 425-442

Research Thrust - 5

- **Hardware Security (Makris, Basu et al)**
  - **Sponsors: NSF, ARO, Intel, TI, SRC**
    - **Hardware Trojans, Counterfeiting, IP Piracy, Reverse Eng., Security Verification and Validation, EDA Tools for Security**

- Yu Liu, Ke Huang, **Yiorgos Makris**: Hardware Trojan Detection through Golden Chip-Free Statistical Side-Channel Fingerprinting. DAC 2014: 1-6
- Ke Huang, Yu Liu, Nenad Korolija, John M. Carulli, **Yiorgos Makris**: Recycled IC Detection Based on Statistical Methods. IEEE Trans. on CAD of Integrated Circuits and Systems 34(6): 947-960 (2015)
- Ujjwal Guin, Ke Huang, Daniel DiMase, John M. Carulli, Mohammad Tehranipoor, **Yiorgos Makris**: Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain. Proceedings of the IEEE 102(8): 1207-1228 (2014)
- **Kanad Basu**, Samah Mohamed Saeed, Christian Pilato, Mohammed Ashraf, Mohammed Thari Nabeel, Krishnendu Chakrabarty, Ramesh Karri: CAD-Base: An Attack Vector into the Electronics Supply Chain. ACM Trans. Design Autom. Electr. Syst. 24(4): 38:1-38:30 (2019)
- **Jeyavijayan Rajendran**, Ozgur Sinanoglu, Ramesh Karri: Regaining Trust in VLSI Design: Design-for-Trust Techniques. Proceedings of the IEEE 102(8): 1266-1282 (2014)

Research Thrust - 6

- **Security Analytics and Machine Learning (Khan, Chen, Ruozzi, et al)**
  - **Sponsors: NSA, IARPA, NASA, NGA, AFOSR, Raytheon, Tektronix, Nokia, IBM**
    - **Data Science/Machine Learning for Cyber Security and Public Health; Geospatial/Semantic Web Data Management; Stream and Social Media Analytics; Big Data Management and Analytics**

- Mohammad M. Masud, Qing Chen**, Latifur Khan**, Charu C. Aggarwal, Jing Gao, Jiawei Han, Ashok N. Srivastava, Nikunj C. Oza: Classification and Adaptive Novel Class Detection of Feature-Evolving Data Streams. IEEE Trans. Knowl. Data Eng. 25(7), 2013.
- Ahsanul Haque, Swarup Chandra, **Latifur Khan**, Charu Aggarwal: Distributed Adaptive Importance Sampling on graphical models using MapReduce. IEEE BigData Conference 2014: 597-602
- Jose Cadena, **Feng Chen**, Anil Vullikanti: Graph Anomaly Detection Based on Steiner Connectivity and Density. Proceedings of the IEEE 106(5): 829-845 (2018)
- Nannan Wu, Wenjun Wang, **Feng Chen**, Jianxin Li, Bo Li, Jinpeng Huai: Uncovering Specific-Shape Graph Anomalies in Attributed Graphs. AAAI 2019
- Yuanzhen Guo, Hao Xiong, **Nicholas Ruozzi**: Marginal Inference in Continuous Markov Random Fields Using Mixtures. AAAI 2019: 7834-7841
- Yi-Fan Li, Yang Gao, Gbadebo Ayoade, Hemeng Tao, **Latifur Khan**, Bhavani M. Thuraisingham: Multistream Classification for Cyber Threat Data with Heterogeneous Feature Space. WWW 2019: 2992-2998

Research Thrust - 7

- **Network Security (Haas, Sarac, Hao, Cobb, et al)**
  - **Sponsors: NSF, ONR, CISCO**
    - **Wireless Network Security, Network Measurements, Software Defined Networks**

- **Zygmunt J. Haas**: Keynote: Information Assurance in sensor networks. PerCom Workshops 2011
- S. M. Nazrul Alam, **Zygmunt J. Haas**: Coverage and connectivity in three-dimensional networks with random node deployment. Ad Hoc Networks 34: 157-169 (2015)
- Milen Nikolov, **Zygmunt J. Haas**: Towards Optimal Broadcast in Wireless Networks. IEEE Trans. Mob. Comput. 14(7): 1530-1544 (2015)
- Ramon Novales, **Neeraj Mittal**, **Kamil Saraç**: SKAIT: A parameterized key assignment scheme for confidential communication in resource constrained ad hoc wireless networks. Ad Hoc Networks 20: 163-181 (2014)
- Matthew Joslin, Neng Li, **Shuang Hao**, Minhui Xue, Haojin Zhu: Measuring and Analyzing Search Engine Poisoning of Linguistic Collisions**.** IEEE Symposium on Security and Privacy 2019: 1311-1325
- Kevin Borgolte, Tobias Fiebig, **Shuang Hao**, Christopher Kruegel, Giovanni Vigna: Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates. NDSS 2018
- Rezwana Reaz, Hrishikesh B. Acharya, Ehab S. Elmallah, **Jorge Arturo Cobb**, Mohamed G. Gouda: Policy Expressions and the Bottom-Up Design of Computing Policies**.** NETYS 2017: 151-165

Research Thrust - 8

- **Cryptography (Desmedt, Kantarcioglu, et al)**
  - **Sponsors: NSF**
    - **Secure Multi-Party Computation, Crypto Protocols, Privacy, Blockchain/Bitcoin**

- Erman Pattuk, **Murat Kantarcioglu**, Huseyin Ulusoy, Bradley A. Malin: CheapSMC: A Framework to Minimize Secure Multiparty Computation Cost in the Cloud. DBSec 2016: 285-294
- Erman Pattuk, **Murat Kan**tarcioglu, Zhiqiang Lin, Huseyin Ulusoy: Preventing Cryptographic Key Leakage in Cloud Virtual Machines. USENIX Security Symposium 2014: 703-718
- **Yvo Desmedt**, Fred Piper: Perfect Anonymity. IEEE Trans. Information Theory 65(6): 3990-3997 (2019)
- **Yvo Desmedt**, Josef Pieprzyk, Ron Steinfeld, Xiaoming Sun, Christophe Tartary, Huaxiong Wang, Andrew Chi-Chih Yao: Graph Coloring Applied to Secure Computation in Non-Abelian Groups. J. Cryptology 25(4): 557-600 (2012)
- Harsh Bimal Desai, **Murat Kantarcioglu**, Lalana Kagal: A Hybrid Blockchain Architecture for Privacy-Enabled and Accountable Auctions. Blockchain 2019: 34-43
- Nazmiye Ceren Abay, Cuneyt Gurcan Akcora, Yulia R. Gel, **Murat Kantarcioglu**, Umar D. Islambekov, Yahui Tian, Bhavani M. Thuraisingham: ChainNet: Learning on Blockchain Graphs with Topological Features. ICDM 2019: 946-951

Research Thrust - 9

- **Secure Software Engineering (Wei, Yang, Yen et al)**
  - **Sponsors: NSF**
    - **Security Testing, Secure Design, Secure Services**
      - George Klees, Andrew Ruef, Benji Cooper, **Shiyi Wei**, Michael Hicks: Evaluating Fuzz Testing. ACM Conference on Computer and Communications Security 2018: 2123-2138
      - Qi Wang, Pubali Datta, **Wei Yang**, Si Liu, Adam Bates, Carl A. Gunter: Charting the Attack Surface of Trigger-Action IoT Platforms. ACM Conference on Computer and Communications Security 2019: 1439-1453
      - Karan Ganju, Qi Wang, **Wei Yang**, Carl A. Gunter, Nikita Borisov: Property Inference Attacks on Fully Connected Neural Networks using Permutation Invariant Representations. ACM Conference on Computer and Communications Security 2018: 619-633
      - Sultan Alsarra, **I-Ling Yen**, Yongtao Huang, Farokh B. Bastani, Bhavani M. Thuraisingham: An OpenRBAC Semantic Model for Access Control in Vehicular Networks. SACMAT 2019: 93-102
      - Wei She, **I-Ling Yen**, Bhavani M. Thuraisingham, Elisa Bertino: Policy-Driven Service Composition with Information Flow Control. ICWS 2010: 50-57
      - Austin Mordahl, Jeho Oh, Ugur Koc, **Shiyi Wei**, Paul Gazzillo: An empirical study of real-world variability bugs detected by variability-oblivious tools. ESEC/SIGSOFT FSE 2019: 50-61

Some High-Priority Research Focus Areas

- **Integrating Cyber Security with Artificial Intelligence/Machine Learning/Data Science (AI/ML/DS)**
  - **AI/ML/DS Applications for Cyber Security including Software and Hardware Security, Insider Threat Detection, Malware Analysis**
  - **Handling attacks to ML models; Adversarial Machine Learning**
  - **Privacy Aware AI/ML/DS**
  - **AI for Good; Fairness and Bias in AI**
- **Cyber Physical Systems and IoT Security**
  - **E.g., Autonomous Vehicles, Critical Infrastructures, Internet of Transportation**
- **Autonomous/Adaptive Cyber Deception**
- **Binary Code Analysis and Malware Detection**
- **Blockchain and Cyber Security**
- **Applications: Geospatial Sciences, Social Sciences, Political Sciences, Healthcare/Public Health, Counter-Terrorism.**

Cyber Security Education (Sarac et al)

- **Sponsors: NSF, DoD, IBM, NSA**
  - **NSF SFS Scholarship for Service**
    - **Started in Fall 2010 and would have graduated around 80+ US Citizen students by 2024 and placed them with Federal Government.**
  - **Interdisciplinary Masters in Cyber Security offered from School of Economics, Policy and Political Sciences (EPPS) Fall 2020 (Holmes et al)**
  - **DoD IA Scholarship**
    - **Participated in the DoD IASP program for Capacity Building and Student Education in the mid to late 2000s.**
  - **NSA GenCyber 2016**
    - **Summer camp for Junior and Senior High School students in practical cyber security education and experimentation.**
  - **NSF Capacity Development**
    - **Assured Cloud Computing, Secure Mobile Systems, Big Data Security and Privacy, Software Defined Networks, Blockchain**
    - **Developing labs and practical programs for students**
  - **Experimental Research Project INSuRE (Information Security Research and Education)**
    - **Participating in INSuRE program for 12 straight semesters since January 2015 – December 2020.**

Cyber Security Education (Sarac et al)

- **Sponsors: NSF, DoD, IBM, NSA**
  - **TexSAW: Annual cyber security exercises and competitions**
    - **Modeled after NYU's CSAW.**
    - **Held since 2011; Around 40-80 students participate from TX and neighboring states in practical cyber security exercises and workshops.**
  - **Professional Education**
    - **Offering courses on Cyber Security Essentials that cover the CISSP modules as well as additional topics in Cyber Security for the Local Industry and Students (especially non Computer Science students).**
    - **Have also taught for AF bases via AFCEA as well as to the DoD and the Intelligence Community.**
  - **Cyber Security Outreach**
    - **Talks at High Schools, DFW Public Libraries, General Public to make the students and public aware of Cyber Security**
  - **Extensive participation/organization: WiCyS, WiDS, Cyber-W, WiSC, WICE**
    - **Women in Cyber Security, Women in Data Science, Women in Cyber Security Research, Women in Services Computing, Women in Communications Engineering, - - -**

Cyber Security Education (Sarac et al)

- **Sponsors: NSF, DoD, IBM, NSA**
  - **Degrees and Certificates**
    - **Masters degrees in Cyber Security (special track in Computer Science), Certificates for Undergraduate students, Around 40+ PhD students working on their Theses in Cyber Security at any one time.**
    - **Interdisciplinary Masters offered from the School of Economics, Policy and Political Sciences (EPPS); includes topics in behavioral sciences, management sciences, social sciences and computer sciences as they relate to cyber security**
  - **Courses Offered**
    - **Computer and Information Security, Network Security, Data and Applications Security and Privacy, Digital Forensics, Cryptography, Secure Web Services, Secure Cloud Computing (with support from IBM and NSF), Hardware Security, CISSP Modules as part of Cyber Security Essentials, Secure Social Networks, Machine Learning for Security, Big Data Analytics, Critical Infrastructure Protection, Biometrics, Security Engineering, Software Reverse Engineering, Control Systems Security, Cyber Physical Systems Security, Binary Code Analysis.**
    - **Planned New Thrusts: Trustworthy Machine Learning, Advanced Network Security, Cyber Security Policy and Risk.**

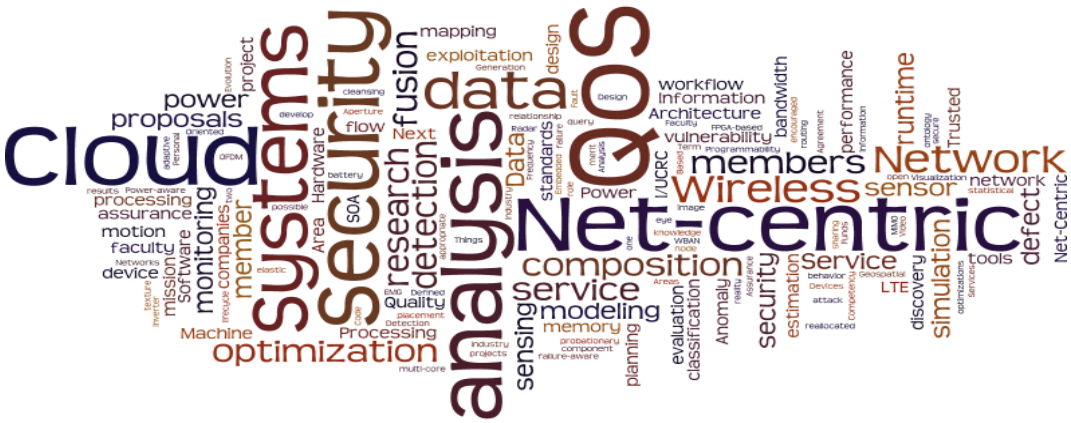
Systems, Prototypes and Tools Developed from Research, Education and Experimentation, IUCRCs

- **Data Science Tools for Malware Detection (Khan)**
  - **Botnet detection, Email worm detection, Buffer overflow detection**
- **Cyber Deception Tools and Experimentation with Malware (Hamlen)**
  - **Honeypatching, Frankenstein**
- **Secure Cloud Data Storage System (Kantarcioglu)**
  - **Currently being commercialized with NSF SBIR**
- **Social Media Analytics System (Khan/Thuraisingham)**
  - **Multiple patents and NAI Fellowship**
- **Reverse Engineering and Binary Code Analysis Tools (Lin)**
  - **Multiple systems including smart phone malware analysis**
- **Other Tools and Systems (Sample)**
  - **Hardware Trojan (Makris); IoT Security (Cardenas); Network Measurement (Sarac)**
- **Affiliated IUCRCs**
  - **Net-Centric and Cloud Software Systems (NCSS) – Bastani**
  - **Security and Software Engineering Research Center (S2ERC) - Wong**
  - **Center for Hardware and Embedded Systems Security and Trust (CHEST) – Makris**

Affiliated NSF I/UCRC (Sample): Net-Centric and Cloud Software Systems (NCSS):

Dr. Farokh Bastani et al

- Independent Center affiliated with the Cyber Security Institute
- Net-Centric and Cloud Software & Systems
  - Develop net-centric applications
    - Integrate communication systems, networked sensor systems, command and control systems, etc.
  - Service-based and component-based technologies
    - Compose services into applications dynamically; Verification, validation, and reliability assessment of the composed system in real-time
    - Incorporate security services to assure overall system security
  - Leverage cloud computing for deployment of composite systems
    - Resource management, SLA compliance, workload modeling



Some NCSS I/UCRC Members

UNT
UNIVERSITY OF NORTH TEXAS

UT DALLAS

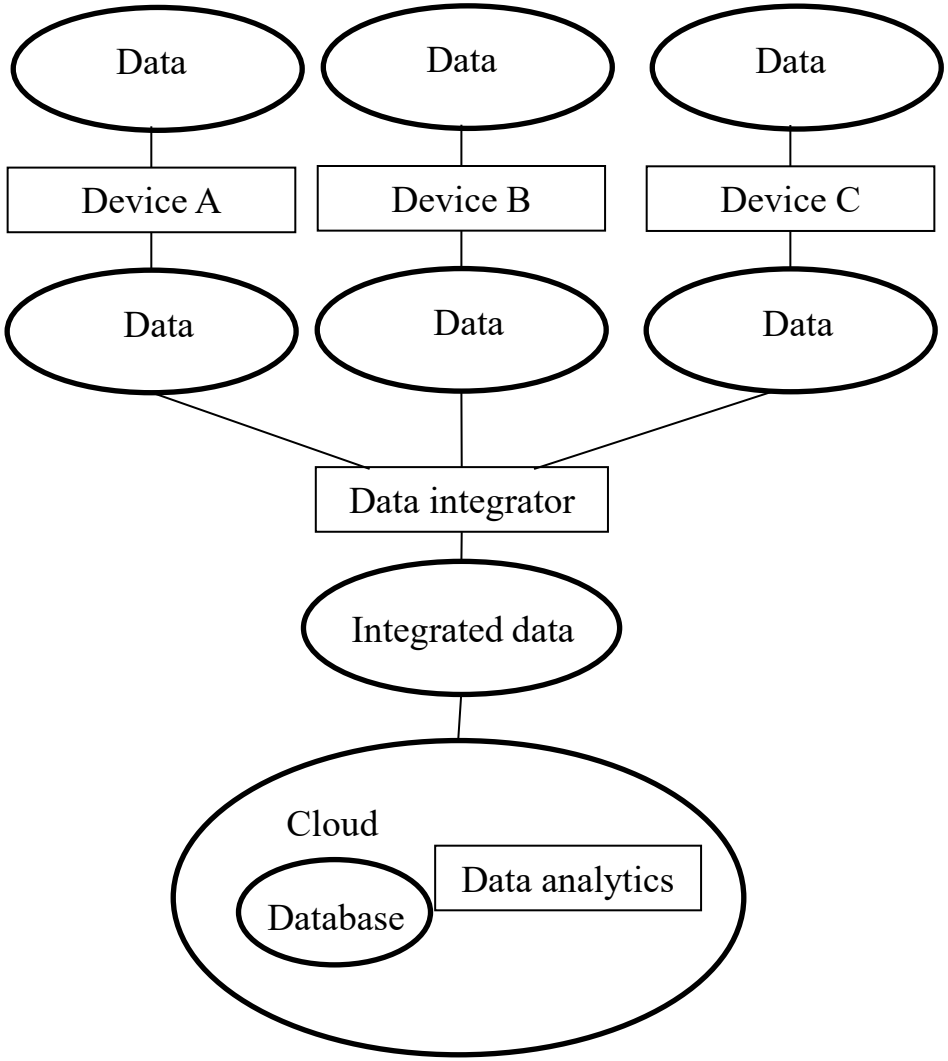
SMU

ASU ARIZONA STATE UNIVERSITY

MISSOURI S&T
University of Science & Technology

Cyber Operations Lab in Progress Funding including from ARO

- **SAIAL (Security Analysis and Information Assurance Lab) being converted into a Secure IoT Systems Lab**
  - **Layered Architecture (Hardware, Network, System, Database, Applications such as smart phones)**
  - **Student projects (BS, MS, PhD) to carry out attacks at different levels (ethical hacking) and develop security solutions.**
  - **Will be made available to our partners in government, industry and academia.**



Summary and Directions

- **Summary**
  - **NSA/DHS Certifications in CAE, CAE-R, and Cyber Operations**
  - **Award Winning Faculty with Research in all aspects of Cyber Security/Data Science with Publications in Top Tier Journals and Conferences.**
  - **Strong Cyber Security Education Program with multiple NSF SFS grants.**
  - **Collaborations with Academia, Industry and Government Labs**
  - **Multiple Patents and Commercialization Activities**
  - **Prestigious Grants including NSF CAREERs, AFOSR YIPs, MURI, NSA/VMWare and NSF/Amazon Research Partnership Grants, NSA SoS Lablet, Multiple NSF Large, Medium and Small SatC grants, Multiple MRI and DURIP grants, - - -**
- **Directions**
  - **Security and Privacy for the COVID Pandemic**
  - **Fully Functional Cyber Operations Lab**
  - **Focus on new thrusts as technology evolves**
  - **Large Center Grant ($10M+)**
  - **Establish an Industry Consortium**

Contact

- **Ms. Rhonda Walls, Project Coordinator**
  rhonda.walls@utdallas.edu, (972) 883-2731
- **Dr. Bhavani Thuraisingham, Founding Executive Director**
  bhavani.thuraisingham@utdallas.edu, (972) 883-4738
- **Follow us @CyberUTD**
- **YouTube Channel:**
  https://www.youtube.com/channel/UCdkdO2DUNqpqGLmeJjiXujA?