Cyber Security Research and Education Institute (CSI)
The University of Texas at Dallas (UTD)

http://csi.utdallas.edu

October 15, 2015
Our History

- NSA/DHS Center for Academic Excellence in Cyber Security Education June 2004 (CAE)
- SAIAL (Security Analysis and Information Assurance Laboratory) built in July 2004
- Cyber Security Research Center (CSRC) established on October 4, 2004
- NSA/DHS Center for Academic Excellence in Cyber Security Research June 2008 (CAE-R)
- Cyber Security Research and Education Center (CySREC) established September 1, 2010 with the 1st SFS grant
- Annual TexSAW (Texas Security Awareness Week) established in October 2011 (Hon. Michael McCaul was keynote speaker at TexSAW 2012)
- Cyber Security Research and Education Institute (CSI) established on April 1, 2013
- NSA/DHS CAE and CAE-R certifications under the NSA’s new requirements in June 2014
- Celebrated 10 years in October 2014 with distinguished presentation, student posters/demos and screening of Turing Film Codebreaker
Our Faculty

Founder
• Bhavani Thuraisingham, PhD, DEng (U of Wales, U of Bristol - UK)

Faculty from the School of Engineering and Computer Science
• Alvaro Cardenas, PhD (U of MD) – Cyber Physical Systems Security
• Yvo Desmedt, PhD (U. Leuven-Belgium) - Cryptography
• Zygmunt Haas, PhD (Stanford) - Wireless Network Security
• Kevin Hamlen, PhD (Cornell) - Language and Software Security
• Murat Kantarcioglu, PhD (Purdue) - Data Security and Privacy
• Latifur Khan, PhD (U of Southern CA) - Big Data Analytics for Security
• Zhiqiang Lin, PhD (Purdue) - Systems Security and Forensics
• Yiorgos Makris, PhD (UC San Diego) - Hardware Security
• Kamil Sarac, PhD (UC Santa Barbara) - Education, Network Measurements
• J.V. Rajendran, PhD (NYU) – Hardware Security

Several affiliated faculty from multiple schools at UTD including
• Michael Baron, PhD (U of MD) - Statistical Methods for Security
• Alain Bensoussan, PhD (University of Paris) - Risk Analysis for Security
• Nathan Berg, PhD (U of Kansas) - Economics and Security (currently in New Zealand)
• Jennifer Holmes, PhD (U of MN) – Cyber Security Policy
• Patrick Brandt, PhD (Ohio State) – Political Science
• Daniel Krawczyk, PhD (UCLA) - Psychosocial Aspects of Security
Our Accomplishments

- $30M in research funding and $7M in education funding from federal agencies
- Prestigious grants and contracts including: multiple NSF Career, multiple AFOSR YIP, DoD MURI, NSF Large SatC, NSF MRI, NSA Research, ….; 11 NSF Grants in 2015 season
- Fellowships and Awards:
  - IEEE, AAAS, IACR Fellowships, IBM Faculty Award, IEEE and ACM Awards
  - e.g., IEEE CS Technical Achievement, IEEE SMC/Homeland Security Technical Achievement, ACM SIGSAC Outstanding Contributions Award
- Numerous keynote addresses, top-tier journal and conference publications (e.g., IEEE S&P, ACM CCS, ACM KDD, SIGMOD), open source tools, patents, books
- Prestigious cyber security research paper competition awards; Numerous press releases and media appearances including NY Times opinion pages column
- Professional Certifications: CISSP, GCFE, GREM (planned)
- Student placements including at IBM TJ Watson, Google Privacy, Microsoft, Amazon, E-Bay, Raytheon, L-3, TI, HP, VCE, Ericsson, Blue Cross Blue Shield, Cisco, UNCC, Clemson, UCSD Medical School, Vanderbilt Medical School, UT Southwestern Medical Center, Facebook, Intel, NSA, CIA, MITRE, MIT Lincoln Lab, Sandia, NAVAIR, Federal Reserve, ……
Our Academic Collaborators (Funded Research)
Collaborators on Funded INSuRE NSA Project

Purdue University
UMBC
UC Davis
Northeastern University
State University of New York
Stevens Institute of Technology
Carnegie Mellon University
DSU Dakota State
Research Thrust - 1

• Active Malware Defense (Hamlen et al)
  – Sponsors: AFOSR, NSF, NASA, Sandia, ONR, DARPA, Raytheon
    – Reactively Adaptive Malware and Frankenstein; Reverse Engineering for Malware Detection; Android Malware Detection; Host Health Management; Author Attribution
      – 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
Research Thrust - 2

- **Data Security and Privacy (Kantarcioglu et al)**
  - **Sponsors: AFOSR, NSF, NIH, ARO**
  - Privacy Preserving Record Linkage and Mining; Adversarial Data Mining; Secure Data Provenance; Policy and Incentive-based Assured Information Sharing; Security and Privacy for Social Networks; Inference Control; Risk-aware Data Security and Privacy

- Mohammad Saiful Islam, Mehmet Kuzu, Murat Kantarcioglu: Inference attack against encrypted range queries on outsourced databases. CODASPY 2014: 235-246
- 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
Research Thrust - 3

• Secure Cloud Computing (Lin et al)
  – Sponsors: AFOSR, 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

• 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
Research Thrust - 4

- Cryptography/Systems/Language/Networks/ Hardware Security (Cardenas, Makris, Sarac, Haas, Desmedt)
  - Sponsors: NSF, ARO, CISCO, MITRE, NIST, TI, Intel, SRC
    - Cryptography, Control and Cyber Physical Systems Security; Hardware Trojan; Wireless Network Security

- Zygmunt J. Haas: Keynote: Information Assurance in sensor networks. PerCom Workshops 2011
Research Thrust - 5

• Data/Security Analytics (Khan et al)
  – Sponsors: IARPA, NASA, NGA, AFOSR, Raytheon, Tektronix, Nokia
  – Semantic Web Data Management and Integration; Geospatial Data Management and Integration; Stream-based Novel Class Detection for Text; Social Network Data 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

  • Ahsanul Haque, Brandon Parker, Latifur Khan, Bhavani M. Thuraisingham: Evolving Big Data Stream Classification with MapReduce. IEEE CLOUD 2014: 570-577
Education Thrust (Sarac et al)

- **Sponsors: NSF, DoD, IBM, NSA**
  - NSF SFS Scholarship for Service
  - DoD IA Scholarship
  - NSF Assured Cloud Computing
  - Experimental Research Project on NSA INSuRE
  - Organizing annual cyber security exercises and competitions for students in TX and neighboring states

- **Degrees and Certificates**
- **Courses Offered**
  - Planned: Cyber Operations, Mobile System Security, Reverse Engineering for Malware
Directions

• Establishing an Industry Advisory Board, Industry Consortium and Distinguished Cyber Security Speaker Series

• Establishing close collaborations with NSA/DHS through our NSF SFS and NSA INSuRE Programs

• Continuing with outreach and TexSAW

• Planning (i) Center Scale Proposals to NSF, DoD, ….(ii) Texas-wide Cyber Security Initiative (UT System)

• Presentations at the National Privacy Research Strategy February 18-20, 2015 in Arlington VA, and help develop programs

• Continuing with obtaining Patents, developing Open source tools and carrying out Tech Transfer

• Participate in NIST FFRDC with MITRE and U of MD System

• Panel on May 8· 2015 in Austin invited by the UT System Chancellor Admiral William McCraven
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