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

http://csi.utdallas.edu

Dr. Bhavani Thuraisingham
Founding Executive Director

September 2017
Outline

• Faculty
• History and Accomplishments
• Sponsors
• Collaborations
• Research Thrusts
• Education Programs, Research Prototypes and Tools, and Cyber Operations
• Affiliated I/UCRC
• Summary and Directions
• Contact
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
- Jorge Cobb, PhD (UTAustin) Cyber Security Outreach, Reliable Networks
- Yvo Desmedt, PhD (U. Leuven-Belgium) Cryptography
- Zygmunt Haas, PhD (Stanford) Wireless Network Security
- Kevin Hamlen, PhD (Cornell) Language and Software Security
- Shuang Hao, PhD (GATech) Network Security, Measurements and DNS Attacks
- 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
- J.V. Rajendran, PhD (NYU) Hardware Security (now at Texas A&M)
- Kamil Sarac, PhD (UC Santa Barbara) Cyber Security Education, Network Measurements

Several affiliated faculty from multiple schools at UTD (Sample)
- Michael Baron, PhD (U of MD) Statistical Methods for Security (currently at American University)
- Farokh Bastani, PhD (UC Berkeley), I/UCRC, Secure Software Engineering
- 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
- Cong Liu, PhD (UNC Chapel Hill) Real-time Systems and Security
Our History and Accomplishments

• NSA/DHS Center for Academic Excellence in Cyber Security Education, June 2004 (CAE)
• SAIAL (Security Analysis and Information Assurance Laboratory) July 2004
• NSA/DHS Center for Academic Excellence in Cyber Security Research, June 2008 (CAE-R)
• First NSF SFS Grant, 2010; Follow-on Grant 2014.
• 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 for Excellence in Cyber Operations in June 2015; first university in TX and 14th in the US
• Hosting ACM CCS (#1 Cyber Security Research Conference) in October 2017.
Our History and Accomplishments

• Over $36M in research funding and $8M in education funding in 12 years from federal agencies

• Prestigious grants and contracts including the following:
  • Multiple NSF CAREER (100% success for NSF CAREER 5/5)
  • Multiple AFOSR YIP
  • DoD MURI and several Mini-MURIs ($1-2M+ grants).
  • NSF Large SatC and multiple Medium SatC
  • NSF MRI (Major Research Instrumentation)
  • NSA Research Grant Competition held in 2015
  • Highly Competitive and Prestigious NSF/VMware Partnership Research Grant (Small center scale award).
  • UT System National Security Network Grant.

• Fellowships and Awards:
  • IEEE, AAAS, IACR Fellowships, IBM Faculty Award, IEEE and ACM Awards
  • e.g., IEEE CS Technical Achievement, ACM SIGSAC Outstanding Contributions Award, IEEE SMC/Homeland Security Technical Achievement, ACM CODASPY Research Award, IEEE CS Services Computing Research Innovation Award, AFCEA Medal of Merit
Our History and Accomplishments

• Numerous keynote addresses, top-tier journal and conference publications (e.g., IEEE S&P, ACM CCS, ACM KDD, ACM SIGMOD, Usenix Security, NDSS), open source tools, multiple patents, books.

• Affiliated I/UCRC (Industry University Cooperative Research Center)

• Student Placements (SFS students and PhD students):
  • Government: NSA, CIA, NAVAIR, Federal Reserve, …
  • FFRDC and Labs: MITRE, MIT Lincoln, Applied Physics Lab, Sandia, Los Alamos, …
  • 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, …
  • Academia: UNCC, Clemson, UCSD Medical School, Vanderbilt Medical School, UT Southwestern Medical Center, US Military Academy at West Point…
Our Academic Collaborators (Funded Research)
UTD/Kings College, London/U of Insubria, Italy
Collaboration sponsored by AFOSR/EOARD
Cloud-based Assured Information Sharing


Agency 1 (UTD)
Agency 2 (Kings)
Agency n (Insubria)

User Interface Layer

Relational Data
Fine-grained Access Control with Hive

CLOUD

SPARQL Query Optimizer for Secure RDF Data Processing

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

- Purdue University
- UMBC
- University of California Davis
- Northeastern University
- University of Maryland
- Iowa State University
- Stevens Institute of Technology
- Carnegie Mellon University
- Dakota State University
Other Collaborations (Sample)

• ARL South: Research on Adversarial Machine Learning
  – UTD focus on Computer Sciences; ARL focus on Behavioral Sciences
  – UTD support from ARO
  – Participated in ARL Planning Workshop on Cyber Fogginess (January 2016)

• 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 wish NIST on Cyber Physical Systems Security
  – Participating in NIST Big Data Security and Privacy Working Group

• Collaboration with NSA TX Planned
  – NSA TX visiting us on August 23, 24 2017 to discuss collaborations
  – Preparing two Science of Security Proposals to be submitted on August 21
    (one team with Purdue, other with Vanderbilt)
Research Thrust - 1

• Active Malware Defense (Hamlen et al)
  – Sponsors: AFOSR, NSF, NSA, 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 Machine Learning; 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:** NSF, 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

- Safwan Mahmud Khan, **Kevin W. Hamlen**: Hatman: Intra-cloud Trust Management for Hadoop. IEEE CLOUD 2012: 494-501

Research Thrust - 4

  – Sponsors: NSF, MITRE, NIST, Intel, AFOSR
  • 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
Research Thrust - 5

- Hardware Security (Makris, Rajendran et al)
  - **Sponsors:** NSF, ARO, Intel, TI, SRC
  - Yu Liu, Ke Huang, **Yiorgos Makris:** Hardware Trojan Detection through Golden Chip-Free Statistical Side-Channel Fingerprinting. DAC 2014: 1-6
Research Thrust - 6

• Data/Security Analytics (Khan et al)
  – Sponsors: IARPA, NASA, NGA, AFOSR, Raytheon, Tektronix, Nokia
  – Security integrated with Semantic Web Data Management, Geospatial Data Management; Stream-based Novel Class Detection; 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
Research Thrust - 7

- **Network Security/Cryptography (Haas, Sarac, Desmedt, Cobb, Mittal, et al)**
  - **Sponsors: NSF, CISCO**

- **Zygmunt J. Haas**: Keynote: Information Assurance in sensor networks. PerCom Workshops 2011
- **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)
Cyber Security Education (Sarac et al)

- **Sponsors: NSF, DoD, IBM, NSA**
  - NSF SFS Scholarship for Service
    - Started in Fall 2010 and would have graduated 50+ US Citizen students by 2020 and placed them with Federal Government.
  - 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 System (smart phones), Planning for Big Data Security and Privacy.
    - Developing labs and practical programs for students
  - Experimental Research Project INSuRE
    - Participating in INSuRE program for five straight semesters since January 2015.
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 to make the students and public aware of Cyber Security
Cyber Security Education (Sarac et al)

- **Sponsors:** NSF, DoD, IBM, NSA

- **Degrees and Certificates**
  - Masters degrees in Cyber Security (special track), Certificates for Undergraduate students, Around 40+ PhD students working on their Theses in Cyber Security at any one time.

- **Courses Offered**

  - Planned: Cyber Operations, Mobile System Security, Reverse Engineering for Malware.
Sample Systems, Prototypes and Tools Developed from Research, Education and Experimentation

• Data Analytics 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 (Thuraisingham)
  – Two patents and exploring commercialization
• Reverse Engineering and Binary Code Analysis Tools (Lin)
  – Multiple systems including smart phone malware analysis
• Other Tools and Systems
  – Hardware Trojan Detection (Makris)
  – Tools for IoT Security (Cardenas)
  – Network Measurements (Sarac)
Cyber Operations Lab: Initial Stage

- SAIL 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.
Affiliated I/UCRC: 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

<table>
<thead>
<tr>
<th>U.S. Army</th>
<th>Texas Instruments</th>
<th>Sprint</th>
<th>Samsung</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raytheon</td>
<td>POUNdra</td>
<td>NTT DATA</td>
<td>LOCKHEED MARTIN</td>
</tr>
<tr>
<td>LG</td>
<td>Intel</td>
<td>FireHost</td>
<td></td>
</tr>
<tr>
<td>COMPUMATRICE</td>
<td>Boeing</td>
<td>AMD</td>
<td>AFRL</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

UNT UNIVERSITY OF NORTH TEXAS
UT DALLAS
SMU
ASU ARIZONA STATE UNIVERSITY
MISSOURI S&T University of Science & Technology
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 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 Research Partnership.

• Directions
  – Establish an Industry Consortium
  – Fully Functional Cyber Operations Lab
  – Large Center Grant ($10M+)
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