CYBER SECURITY RESEARCH AND EDUCATION AT THE UNIVERSITY OF TEXAS AT DALLAS (UTD)

1. INTRODUCTION

1.1 Overview of UTD's Cyber Security Research and Education Institute (CSI)

UTD's Cyber Security Research and Education Institute which now includes 11 core professors conducting research in data security and privacy, software and language security, secure networks, secure systems and forensics, hardware security, cryptography, control systems security, data mining for malware detection and security applications. The team has generated over $30M in research funding and $7M in education funding from agencies such as NSF, AFOSR, NSA, IARPA, DARPA, NGA, NASA, ONR, ARO, ARMY, and NIH as well as multiple corporations. The research projects include three NSF Career grants, two AFOSR Young Investigator Program awards, a DoD MURI award on Assured Information Sharing, a large NSF Trustworthy Computing grant on data provenance, and multiple NSF medium grants (Cyber Trust, Trustworthy Computing and NeTS programs) on policy management, in-line reference monitors and data integrity, multiple AFOSR grants on topics such as assured cloud computing and reactively adaptive malware and an NSF MRI award. The team also pioneered the first of a kind international collaboration funded by AFOSR and EOARD on cloud-based assured information sharing between UTD, Kings College – University of London, and University of Insubria – Italy between 2009 and 2014. The team also collaborates North Texas Regional Computer Forensics Laboratory for student projects, researchers from AFRL Rome, NY on assured cloud computing, and industrial research laboratories. CSI is part of UTD's Big Data Team and conducts research on analyzing and securing big data as well as social media. In addition, the team is working on transferring the technologies developed at the university to commercial development efforts. UTD CSI obtained the NSA/DHS CAE in both Cyber Security Education and Research and became the first university in Texas and the 14th university in US to obtain the highly selective NSA/DHS Center for Academic Excellence (CAE) in Cyber Operations in 2015. UTD CSI has received over $6M in SFS grants in 2010 and 2014 and will have graduated over 50 MS students under this program by 2019 and placed them in agencies such as NSA and CIA.

1.2 Our History

Background: 2004-2007: UTD established the Emergency Preparedness and Digital Forensics Institute in 2002 and subsequently obtained the CAE in June 2004. The research component of the Institute was established in October 2004 when **Dr. Bhavani Thuraisingham** was hired from the MITRE Corporation to head the Cyber Security Research Center (CSRC). Dr. Thuraisingham had worked in Cyber Security for around 19 years at that time including at Honeywell and MITRE and was an advisor to **Mr. Mike Ware** at NSA/R23 for several years. She joined UTD after a three year stint as a Program Director at NSF where she established the Data and Applications Security Initiative and was one of the co-founders of the Cyber Trust Theme. In October 2004, the Institute changed its name to Cyber Security and Emergency Preparedness Institute (CSEPI) whose executive director was **Dr. Douglas Harris**. CSRC was part of the CSEPI. Between 2004 and 2007, Dr. Thuraisingham expanded CSRC by hiring **Dr. Murat Kantarcioglu,** an expert in data security and privacy, form Purdue and **Dr. Kevin Hamlen,** an expert in software and language security**,** from Cornell, both as assistant professors. **Dr. Latifur Khan**, PhD from U. Southern CA, who was already at UTD and is a data analytics expert, also joined the center. Over the years CSRC evolved into a separate institute called the Cyber Security Research and Education Institute (CSI) focusing solely on cyber security research and education. Its total research funding since its inception in October 2004 (as CRSC) which was around $1M in Fall 2007 has grown to around $30M in Fall

2015. Furthermore, our PhD production for CSRC which was three in Fall 2007 and has now grown to over 40.

Progress during 2008 - 2009: 2008 was a breakthrough year for CSI. Dr. Kevin Hamlen had received the AFOSR YIP (Young Investigator Program award) in late 2007, and we received an AFOSR MURI grant on assured information sharing for $1M in March 2008. We also received grants from NGA and NASA to develop data analytics techniques. In addition we received a large grant from AFOSR on secure semantic service- oriented grid which evolved into secure cloud computing ($2.4M). In late 2008, Dr. Kantarcioglu received an NSF CAREER award as well as an NIH Grant in 2009. We also received an IARPA grant under the KDD program (through NSF) to develop semantic web technologies for security applications. By the end of 2009 our research funding had increased to around $8M. At the same time we started publishing in top tier data security conferences including in the Proceedings of IEEE ICDE and IEEE ICDM as well as several IEEE Transactions. During this time we graduated around five more PhD students.

It was during this time that Dr. Kantarcioglu started collaborating with the Jindal School of Management as well as the School of Economics, Policy and Political Sciences (EPPS) on topics such as risk-based data privacy and incentive-based assured information sharing. We developed novel results on applying game theory to cyber security and we published papers in several interdisciplinary venues such as GameSec. We are now known as a team to be one of the leaders in interdisciplinary research in cyber security.

We also established strong collaborations with several universities through funded projects. Our close collaborators include Purdue University, UMBC, UIUC, MIT, UTSA, U of MI, U of MN, UTEP, Vanderbilt, UIC, and UCI. We continued our collaboration with Raytheon and published several papers with the Raytheon team.

Progress during 2010-2012: **Dr. Kamil Sarac** who was conducting research in network measurements and security joined our team as the Director of Education and we were successful in obtaining a $1.8M NSF SFS Grant in Fall 2010 to educate US Citizen students to obtain their MS degrees in Cyber Security. To date we have 100% placement with many of our students joining NSA. Dr. Sarac established the annual TexSAW (Texas Security Awareness Week) which includes a symposium and student workshops to motivate and encourage students in Texas to learn cyber security.

We continued to make significant progress with respect to funding, PhD students and papers. We received multiple large grants from NSF and AFOSR as well as grants from ONR, ARO, DARPA, and DOE (via Sandia). The topics included secure sensor/social web ($1.,6M), secure data provenance (close to $1M), secure, adversarial mining, privacy-preserving record integration, and mobile systems malware detection (close to $1M)). **Dr. Zhiqiang Lin,** an expert in systems security and forensics**,** joined the team in September 2011 after his PhD from Purdue. In addition **Dr. Yiorgos Makris**, whose expertise is in hardware security, joined us from Yale as Associate Professor in Computer Engineering. Dr. Hamlen received a NSF CAREER award. Dr. Lin received a gift from VMWare to conduct research in secure virtualization. We published papers not only in the top tier data conferences such as ACM KDD, but also in top tier cyber security conferences including IEEE Security and Privacy Symposium (aka Oakland) and ACM Conference on Computers and Communications Security (CCS). We graduated around 21 PhD students during this time.

Subsequently in August 2012, world-famous cryptographer **Dr. Yvo Desmedt** joined our team from University College London. We also received prestigious external awards for our work. For example, Dr. Thuraisingham received the IEEE SMC/TS Research Leadership Award in Intelligence and Security Informatics, and the prestigious ACM SIGSAC Outstanding Contributions Award for research contributions and leadership in Data and Applications Security. She also received the Transformative Achievement Medal for her work on integrating computer sciences with social sciences from the Society for Design and Process Science. Dr. Khan received both the ACM Distinguished Scientist and IEEE SMC/TS

Technical Achievement Award and Dr. Hamlen received worldwide coverage for his research on the Frankenstein Malware.

Progress during 2013-2015: In January 2013 **Dr. Alvaro Cardenas** joined CSI as an Assistant Professor after his PhD at U of MD College Park and post doctorate research at UC Berkeley. His expertise is in control systems security and critical infrastructure protection. He began a collaboration with NIST as well as with MITRE and has a joint project with MITRE on control systems security. Due to his initiative, UTD hosted the very important NIST Cyber Security Framework Workshop (Executive Order) in September 2013.

In the meantime we continued to expand our research funding as well as publish papers in top tier venues. In August 2013 we were very fortunate to have **Dr. Zygmunt Haas** join our team. Dr. Haas is a PhD from Stanford and was a Professor at Cornell University and an expert in wireless network security. We also explored new areas by collaborating with professors from the Brain and Behavioral Sciences by investigating how hackers think. An IBM Vice President for Research visited us in February 2013 and she was very impressed with our cyber security program and nominated Dr. Bhavani Thuraisingham for an IBM Faculty Award in Cyber Security. Dr. Thuraisingham received this award in November 2013 in New York. To continue our industry collaboration, UTD's NSF IUCRC on Network Centric Systems joined our Institute. We work with this IUCRC through our collaboration with Raytheon. In January 2014 Dr. Zhiqiang Lin received his AFOSR YIP award. In June 2014 we obtained re-certifications of NSA/DHS CAE for both education and research. We were the first university in Texas to obtain these re-certifications under the new stringent requirements. We were very pleased to receive our second NSF SFS grant for $4.2M. We were also selected by NSF/NSA to participate in the collaborative INSuRE program.

2015 has been a stellar year for us with 11 NSF grants including Zhiqiang Lin's NSF CAREER award. This is a significant achievement. CSI now has three NSF CAREER and two AFOSR YIP awards. We also received a grant on cyber security policy with our School of Economics, Policy and Political; Sciences. In addition, we received our first NSA research grant. We were selected to host the Women in Cyber Security conference (out of 11 proposals submitted) in 2016. We expanded our program in hardware security by hiring **Dr. J.V. Rajendran** who completed his PhD at NYU. Above all, we became the first university in Texas and 14th in the US to receive the highly selective NSA CAE for Cyber Operations and we are starting the cyber operations education program. Over the past decade we have published papers in every top tier cyber security, data analytics, and systems conference including IEEE S&P, ACM CCS, NDSS, USENIX Security, ACM SIGMOD, ACM KDD, PVLDB, IEEE ICDM, and IEEE ICDE. We have also hosted major conferences including IEEE ICDM and will be hosting the Women in Cyber Security Conference in 2016 and ACM CCS in 2017.

Future Plans: Technical excellence is our main objective. Grants are a way to achieve this excellence. Therefore we will work hard to get grants, continue to produce quality research, collaborate with our peers and produce PhD graduates. While we now have 11 core cyber security faculty members, we have several affiliated faculty across the different schools at the university. These faculty conduct research in computer sciences related topics such as networks, fault tolerance systems, software engineering, theory and real-time systems as well as risk analysis and behavioral economics. We plan to make significant progress with our interdisciplinary research as well as research in the core cyber security areas. As a team we are ethnically diverse and our technical skills complement each other. One area we are looking to hire in the future is in usable security and privacy. We will also focus more towards increasing our industry sponsorship by continuing to work with the IUCRC. We also plan to start an Executive Master's Program in Cyber Security. We get substantial support and encouragement from the senior administration at UTD. We believe that within the next 5 years, we are poised to be one of the premier cyber security research institutes in the USA.

2. CYBER SECURITY FACULTY AND TEACHING

While CSI is an institute that spans across multiple schools and departments within a school, the CSI administration resides at the Erik Jonsson School of Engineering and Computer Science (ECS). Faculty from the ECS offer courses in the cyber security track of study, which leads to a MS or PhD degree for students interested in increasing their knowledge in information assurance, network security, data security, among others. Cyber security is also taught at UTD's Naveen Jindal School of Management (JSOM) to train students in technology managers. Faculty from the JSOM offer courses that lead to an MS in Information Technology Management degree with Information Security and Assurance track for students interested in information security risk management. These students are advised to obtain certifications such as CISA, CISSP, and CISM. In addition several faculty are affiliated with ECS, JSOM and EPPS who teach courses in related topics that contribute towards cyber security research. This section provides information about the administration, the core faculty and the affiliated faculty.

The following people have overall responsibility for Cyber Security Education and Research at UTD either as educators, managers/administrators, or project coordinators.

2.1 Cyber Security Faculty at the School of Engineering and Computer Science

Dr. Bhavani Thuraisingham: http://www.utdallas.edu/~bxt043000/
Louis A. Beecherl, Jr. Distinguished Professor of Computer Science and
Executive Director, Cyber Security Research and Education Institute

Since joining UTD in October 2004, Dr. Thuraisingham built the Cyber Security Research and Education Institute (CSI) which now has 11 core faculty and several affiliated faculty. She has overall responsibility for cyber security research and education at UTD. She has worked in cyber security for over 28 years at Honeywell, MITRE, NSF and UTD. In addition to her research in database security, assured information sharing, and secure cloud computing, Dr. Thuraisingham teaches courses in Data and Applications Security, Secure Cloud Computing, Information Systems Security, Analyzing and Securing Social Networks, Digital Forensics, Trustworthy Semantic Web, and Biometrics. Her work has not only resulted in several publications, but she has also obtained multiple patents, written several books, and received awards and fellowships from organizations such as IEEE and ACM. She has taught Cyber Security related courses at AFCEA between 1998 - 2013 as well as at several Air Force bases and federal agencies. She was also an adjunct professor first at the University of Minnesota and later at Boston University. She also has certifications in CISSP and GCFE and recently received an IBM 2013 Faculty Award for Cyber Security Education. Following are the details of the courses she teaches in Cyber Security. Course details can be found on her website at http://www.utdallas.edu/~bxt043000/.

Data and Applications Security (2005 – Present)
http://www.utdallas.edu/~bxt043000/Teaching/CS-6V81/DAS-F2013/das-F2013.html
This course is taught both at the undergraduate and graduate levels and covers the core concepts in database and applications security. Topics include secure database management, secure distributed and heterogeneous data management, secure object data management, secure web services and semantic web, secure cloud, secure social networks, secure dependable and real-time systems, and secure knowledge management.

Information Systems Security/Cyber Security Essentials (2010 – Present)
http://www.utdallas.edu/~bxt043000/Teaching/CS-6301/Cyber-Security-Essentials-SS2013/cse-ss2013.html

This course covers the ten CISSP modules including Cyber Security Governance and Risk Analysis, Security Architectures, Access Control Models, Network Security, Cryptography, Data and Applications Security, Physical Security, Business Continuity Planning, Operational Security, Legal Aspects, Privacy and Forensics. Starting in Spring 2014, she is teaching this course as part of the Executive Masters in Software Engineering at UTD.

Developing and Securing the Cloud (2012 – Present)
http://www.utdallas.edu/~bxt043000/Teaching/CS-6V81/SecureWebServices_CloudComp-S2012/sws-s2012.html
This course covers topics such as secure web services and secure semantic web, and then discusses concepts in secure cloud computing. Topics covered include identity management, secure cloud framework, secure cloud query processing, secure cloud data storage and governance. (It has evolved from the course Building Trustworthy Semantic Web.)

Analyzing and Securing Social Networks (2013 – Present)
http://www.utdallas.edu/~bxt043000/Teaching/CS-6301/Analyzing-Securing-SNs-S2013/assn-s2013.html
This course provides an overview of social networks and then addresses aspects of social network analytics. The second part of the course discusses topics such as security models for social networks and trust management and privacy for social networks.

Trustworthy Semantic Web (2006 – 2010)
http://www.utdallas.edu/~bxt043000/Teaching/CS-7301/Trustworthy-Sem-Webs-S2011/tsw-S2011.html
This course has now evolved into the secure cloud computing course starting spring 2012. The topics covered included concepts in semantic web as well as security issues including XML security, assured information sharing and policy management for semantic web.

Digital Forensics (2007 – Present)
http://www.utdallas.edu/~bxt043000/Teaching/CS-4398/F2013/dig-forensics-F2013.html
This is an undergraduate course in digital forensics that covers the topics for the GCFE certification. Topics include evidence acquisition and analysis, crime scene reconstruction, memory forensics, l file system forensics, web forensics and expert witness and report writing.

Biometrics (2005)
http://www.utdallas.edu/~bxt043000/Teaching/CS-6V81/Biometrics-F2005/biometrics-F2005.html
This course was taught once in 2005 and will be taught in the near future. Topics included concepts in biometrics, various types of biometrics systems such as finger print, iris, retina, face, gait, and keystroke. In addition, attacks on biometrics systems as well as privacy aspects were also discussed. We plan to reintroduce this course in the 2015-2016 academic year.

Dr. Kamil Sarac: http://www.utdallas.edu/~ksarac/
Associate Professor
Director of Education, CSI
Cyber Security Program Director, The Erik Jonsson School of Engineering and Computer Science

Kamil Sarac is an Associate Professor of computer science at The University of Texas at Dallas. He is also serving as the director of the information assurance education programs in the department. His research interests include computer networks and protocols, network security, network and service monitoring and Internet measurements.

CS 4396 Computer Networks Laboratory (2011 – Present)
http://www.utdallas.edu/~ksarac/cnlab/index.htm
CS 4396 Computer Networks Laboratory class aims at helping students get more insight into how the Internet works and gain hands on experience in building and configuring simple IP networks and related services. CS 6390 class covers both the classical/fundamental topics in computer networks and a number of current/recent research topics related to modern computer networks. Most of the advanced research topics are relevant to Internet related research topics and they are mostly in Layer 3 and above. Finally, CS 6349 class covers study the theoretical and practical aspects of network security including cryptography, authentication systems and security handshake pitfalls, Kerberos and PKI, TCP/IP Security, Security of TCP/IP Applications, Wireless security, and DoS defense.

CS 6349 Networks Security (Spring 2011, 2012, 2013, and Fall 2013)
http://www.utdallas.edu/~ksarac/netsec/index.htm
This course covers the theoretical and practical aspects of network security. The set of topics to be covered includes cryptography, authentication systems and security handshake pitfalls, Kerberos and PKI, TCP/IP Security, Security of TCP/IP Applications, Wireless security, DoS defense, and e-mail security among others.

CS 6390 Advanced Computer Networks (Fall 2011 – 2013)
http://www.utdallas.edu/~ksarac/acn/index.htm
This course covers both the classical/fundamental topics in computer networks and a number of current/recent research topics related to modern computer networks. Most of the advanced research topics are relevant to Internet related research topics and they are mostly in Layer 3 and above.

Dr. Murat Kantarcioglu: http://www.utdallas.edu/~muratk/cgi-bin/index.php
Associate Professor of Computer Science
Director, Data Security and Privacy, CSI

Secure Cloud Computing (Spring 2013)
http://www.utdallas.edu/~muratk/courses/cloudsec13s.htm
In this course, students are required to complete an independent project that requires them to address different data security issues in the cloud. Since the projects are chosen based on the student interests, potential projects covered topics range from embedding access control into Hadoop to encrypted query processing in the cloud.

Introduction to Data Security (Spring 2013)
http://www.utdallas.edu/~muratk/courses/dbsec12f.htm
In this undergraduate course that covers basic topics of data security, students are asked to implement a text editor that stores sensitive data in an encrypted format.
Project description: http://www.utdallas.edu/~mxk055100/NSACAE/CS4389_ProjDesc.pdf
In addition, students are asked to implement role-based access control policies using industry standard access control language XACML.
Link to homework description:
http://www.utdallas.edu/~mxk055100/NSACAE/CS-4389-Homework-Description.pdf

Introduction to Cryptography (Spring 2011 – 2012)
http://www.utdallas.edu/~muratk/courses/crypto12s.htm
In this graduate level introduction to cryptography course, students are asked to implement an extension to Google Doc to store encrypted files on Google. Please see the description of the project for more details.
http://www.utdallas.edu/~mxk055100/NSACAE/crypto-project.pdf

Dr. Kevin Hamlen:http://www.utdallas.edu/~hamlen/
Associate Professor of Computer Science
Director, Software and Systems Security, CSI

Dr. Kevin Hamlen is an Associate Professor in the Computer Science Department at The University of Texas at Dallas. His research applies and extends compiler theory, functional and logic programming, and automated program analysis technologies toward the development of scientifically rigorous software security systems. Over the past five years he has received over $8 million in federally funded research awards, including a CAREER award for malware defense from the National Science Foundation, and a Young Investigator Program (YIP) award for binary software security from the Air Force Office of Scientific Research. His most recent research on secure binary retrofitting and reactively adaptive malware received three best paper awards in 2011-2012, and has been featured in thousands of news stories worldwide, including The Economist and New Scientist. Dr. Hamlen received his PhD and MS degrees from Cornell University, and his BS from Carnegie Mellon University, where his work on proof-carrying code garnered the Allen Newell Award for Excellence in Undergraduate Research.

Language-based Security (2007 – Present)
http://www.utdallas.edu/~hamlen/cs6301fa13.html)
This course covers advanced tools and algorithms for formal software security analysis and assurance, particularly drawn from compiler theory and programming language theory. Topics covered include certifying compilers, in-lined reference monitors, software fault isolation, address space randomization, binary obfuscation, web scripting security, information flow controls, automated theorem-proving, software model-checking, binary reverse engineering, and principles of malware analysis.

Advanced Programming Languages (2007 – Present)
http://www.utdallas.edu/~hamlen/cs6371sp14.html)
This course teaches foundational principles of programming language design and semantics, as well as non-imperative programming paradigms, such as functional and logic programming. When taught by Dr. Hamlen, the course focuses heavily on the development of high-assurance software for security purposes. In particular, the formal security applications of type theory and type-safe programming languages, operational and denotational semantics, axiomatic semantics and Hoare logic, and automated software verification are discussed and studied.

Dr. Zhiqiang Lin: http://www.utdallas.edu/~zhiqiang.lin/
Assistant Professor of Computer Science
Director, Systems Security and Forensics, CSI

CS 4393: Computer and Network Security (Spring 2013 - Present)
http://www.utdallas.edu/~zhiqiang.lin/spring2014.html)
This course is a comprehensive study of the security principles and practices of computer and network systems. Topics include fundamental concepts and principles of computer security, operating system and network security, firewalls and intrusion detection systems, secret key and public key cryptographic algorithms, hash functions, authentication, SSL and Web security. The learning outcome is students are able to understand the basic principles and practices in computer and network security. In particular, understand what the foundational theory is behind computer security, what the common threats are (e.g., malware, exploit, vulnerability), and how to build the defense mechanism in a combination from OS, network and applied crypto. In support of this, the course prepares students to do basic system, network, and application-level programming/labs related to security purposes.

CS 6V81--005: Advanced Digital Forensics and Data Reverse Engineering (Fall 2011)
http://www.utdallas.edu/~zhiqiang.lin/fall2011.html
CS 6V81 is a graduate level, research-oriented, system security course. The focus is digital forensics and data reverse engineering, which tackles the problem of what information is stored in a computer system and how this information can be extracted and used. There are a wide range of applications of data reverse engineering, including digital forensics, crash analysis, game hacking, kernel rootkit defense, and malware analysis. The overall goal of this course is to introduce students to the current techniques used in both research and practice.

In particular, the course covers the underlying technical details (including the most recent techniques) of digital forensics and data reverse engineering, discusses various security applications, analyzes potential limitations of existing systems, and how to develop more secure systems. In the first a few lectures, the instructor will introduce the techniques, foundations, and applications of digital forensics and data reverse engineering. After that, in each class students will read current and seminal research papers from the reading materials.

CS 6301: Systems Security and Binary Code Analysis. (Spring 2012, Fall 2013)
http://www.utdallas.edu/~zhiqiang.lin/fall2013a.html
CS 6301 is a graduate level, research-oriented, systems and software security class. The goal of this course is to understand the low-level system details with the real system implementations from compiler, linker, loader, to OS kernel and computer architectures, examine the weakest link in each system component, explore the left bits and bytes after all these transformations, and study the state-of-the-art offenses and defenses. The learning outcome is students shall be able to understand how an attack is launched (e.g., how an exploit is created), and how to do the defense (e.g., developing OS patches, analyzing the binary code, and detecting intrusions). In particular, we cover static binary code analysis, dynamic binary code instrumentation, data flow analysis, control flow analysis, malware packing and unpacking. We also investigate the unsafe but widely used system programming language C, cover typical vulnerabilities such as buffer overflows, format strings, integer overflows, etc. We also discuss how to create robust shell code using such as ROP, HeapSpray. What's the behavior when a program is running on top of OS? Why do we use paging? How is virtual to physical address translation performed? How does MMU (e.g., TLB) helps this? How does OS manage files and disks? How can we model the program behavior when sitting at the OS layer? We will use both Linux and Windows as working kernel. We also explain how a program can be dynamically linked, and what an attacker can do to cheat the system and meanwhile what we can do to protect the system. In addition, we cover how can we defend against the common exploits, techniques including such as hypervisor level virtual machine introspection, or kernel level ASLR, and DEP, NX-bits. This class has heavy-hands on projects. The students, after taking this class, will be able to get the experience on how to build real systems with virtual machine monitors, and process instrumentations.

CS 6324: Information Security (Fall 2012*)* http://www.utdallas.edu/~zhiqiang.lin/fall2012.html)
Information Security is a comprehensive study of the principles and practices of computer system security including operating system security, network security, software security and web security. Topics include common attacking techniques such as virus, trojan, worms and memory exploits; the formalisms of information security such as the access control and information flow theory; the common security policies such as BLP and Biba model; the basic cryptography, RSA, cryptographic hash function, and password system; the real system implementations, with case study of UNIX, SELinux, and Windows; network intrusion detection; software security theory; web security; legal and ethical issues in computer security.

The learning outcome is students are able to understand what are the common threats faced today, what is the foundational theory behind information security, what are the basic principles and techniques when designing a secure system, how to think adversarially, how today's attacks and defenses work in practice, how to assess threats for their significance, and how to gauge the protections and limitations provided by today's technology.

CS 7301: Recent Advances in Computing -- Operating Systems Security (Fall 2013)
http://www.utdallas.edu/~zhiqiang.lin/fall2013b.html
CS 7301 is a graduate level (PhD in particular), research-oriented, systems and security, seminar class.The goal of this course is to read, understand, and present the recent advances (which have not been systemized into a textbook yet) in operating systems security. We will select the most recent papers from both operating systems venues including SOSP, OSDI, USENIX ATC, EuroSys, ASPLOS, and security venues including IEEE S&P, ACM CCS, USENIX Security, and NDSS. In particular, we cover what's the advantage of kernel level attacks? What are the attack vectors? How are they launched? How we can defend against them? How to design the layer-below systems to secure OS kernel? What are the challenges? What is the state-of-the-art? Why do we want to design in-box monitoring? What's the advantage and disadvantage? The learning outcome is students will be able to understand the recent advances in operating systems security, the relevant security problems, and how these approaches/solutions are proposed.

Dr. Yvo Desmedt: http://www.utdallas.edu/~Yvo.Desmedt/
Jonsson Distinguished Professor
Fellow of the IACR
Director, Cryptography, CSI

CS/SE 7301.001 Information Theoretical Cryptography (Fall 2012)
The following topics, among others, will be discussed: access structure, anti-jamming techniques, authentication codes, multi-receiver authentication, one-time pad, PRMT, (black box) secret sharing, secure multiparty computation, and threshold cryptography. The focus is on schemes achieving unconditional security.

CS6377 Introduction to Cryptography (Spring 2013)
http://dox.utdallas.edu/syl32653
This course covers the basic aspects of modern cryptography, including block ciphers, pseudorandom functions, symmetric encryption, Hash functions, message authentication, number-theoretic primitives, public-key encryption, digital signatures and zero knowledge proofs.

Dr. Alvaro Cardenas: http://www.utdallas.edu/~alvaro.cardenas/
Assistant Professor of Computer Science
Director, Control Systems Security, CSI

Securing Cyber-Physical Systems and Critical Infrastructures (Fall 2013)
http://www.utdallas.edu/~alvaro.cardenas/teaching.php
Class Number: CS/SE 6301.005. The Stuxnet attack was a wake-up call to improve the security of our critical infrastructures, which include transportation networks, the power grid, and other cyber-physical systems, where computation, communications, and control are tightly integrated. This class covers the security of cyber-physical systems from a multi-disciplinary point of view, from computer science security research (network security and software security), to public-policy (e.g., the Executive Order 13636), risk-assessment, business drivers, and control-theoretic methods to reduce the cyber-risk to cyber-physical critical infrastructures.

Information Security (Spring 2014)
http://www.utdallas.edu/~alvaro.cardenas/teaching.php

Class Number: CS/CE 6324.001. Information Security is a comprehensive study of the principles and practices of computer system security including operating system security, network security, software security, and web security. Topics include common attacking techniques such as virus, trojan, worms and memory exploits; applied cryptography, and key management; intrusion detection, Security Information Event Managers (SIEM), and security analytics; trusted computing, TPM 2.0, TruztZone; access control; password protection; and legal and ethical issues in computer security.

Dr. Yiorgos Makris: http://www.utdallas.edu/~yiorgos.makris/
Associate Professor of Computer Engineering
Director, Hardware Security, CSI

CE7V80 Special Topics: Trusted and Secure Integrated Circuits and Systems (Spring 2013 - 2014)
http://www.utdallas.edu/~gxm112130/CE7V80SP14/
This course investigates the various aspects related to the design and implementation of trusted and secure integrated circuits (ICs) and systems. The vast majority of system-level security and authentication protocols have traditionally been built on the premise that the underlying hardware can be trusted. Due to globalization of the electronics supply chain, however, this assumption is no longer valid, making hardware an equally vulnerable malicious entry point as software. Accordingly, this course focuses on the technology required to support trustworthiness and secure operation of integrated circuits and the systems wherein they are deployed. Topics include physical unclonable functions (PUFs) and hardware true random number generators, along with their applications in authentication, anti-tampering, and anti-counterfeiting, hardware Trojan detection and prevention methods, trusted 3rd party hardware intellectual property (IP) acquisition frameworks, active/passive IC metering, design and implementation of cryptographic hardware, side-channel attacks, and architectural and system level support for hardware security. The course is ran as a journal club with readings assigned prior to each lecture and presentations delivered by the students on the various topics. Hands-on experience in the above areas is also obtained through semester-long projects which are carried out in parallel with the lectures.

Dr. Zygmunt Haas
Professor and Distinguished Chair in Computer Science
Director, Wireless Network Security

Advanced Computer Networks (Fall 2013)
http://www.utdallas.edu/~haas/courses/acn/
This course contains a module on Network Security, introducing basic concepts and protocols used to secure Internet traffic. For example, the course covers topics such as RSA, AES, PGP, Kerberos, SSL, IPSec, Firewalls, Intrusion Detection Systems, etc.

Wireless Networks (Spring 2014)
http://dox.utdallas.edu/syl37065
This course contains a module on Security of Wireless Networks. For example, the module introduces security in cellular systems (e.g., GSM) and in wireless local area networks (e.g., 802.11).

Dr. Latifur Khan: http://www.utdallas.edu/~lkhan/
Professor of Computer Science
Director, Big Data Analytics, CSI

Big Data Analytics and Management (Spring 2013, Fall 2013, Spring 2014)
http://dox.utdallas.edu/syl36899

This course focuses on scalable data management and mining algorithms for analyzing very large amounts of data (i.e., Big Data). Included topics are: MapReduce, NoSQL systems (e.g., key-value stores, column-oriented data stores, stream processing systems), association rule mining, large scale supervised and unsupervised learning, state-of-the-art research in data streams, and applications including recommendation systems, web and big data security. Applications to cyber security such as malware detection are also addressed.

2.2 Cyber Security Faculty at the School of Management

Faculty from ECS and JSOM conduct numerous joint interdisciplinary research projects that include Risk and Economics Analysis for Cyber Security (e.g., Incentives based assured information sharing, Data Provenance and Data Privacy). The faculty at JSOM who teach Cyber Security related courses include:

Dr. Alain Benssousan http://www.utdallas.edu/~axb046100/
Dr. Huseyin Cavusoglu http://jindal.utdallas.edu/faculty/huseyin-cavusoglu
Dr. Srinivasan Raghunathan http://www.utdallas.edu/~sraghu/
Dr. Indranil Bardhan http://www.utdallas.edu/~bardhan/

Below is a sample list of courses that are highly beneficial to our interdisciplinary research**.** These courses are listed in UTD’s JSOM course catalog https://jindal.utdallas.edu/course-description/ . Many of these courses are very important for our research in cyber security in general and data security and privacy in particular.

MIS 6330 Information Technology Security
With the advances in information technology, security of information assets has become a keenly debated issue for organizations. While much focus has been paid to technical aspects of the problem, managing information security requires more than technology. Effective information security management demands a clear understanding of technical as well as socio-organizational aspects of the problem. The purpose of this course is to prepare business decision makers to recognize the threats and vulnerabilities present in current information systems and who know how to design and develop secure systems. This course (1) uses lectures to cover the different elements of information security, (2) utilizes business cases and academic research studies to discuss information security issues faced by today's businesses, (3) keeps in touch with the security market and practices through webcasts, and (4) presents strategies and tools to develop an information security program within the organization.

MIS 4360 Network and Information Security
With the advances in information technology, security of information assets has become a keenly debated issue for organizations. While much focus has been paid to technical aspects of the problem, managing information security requires more than technology. Effective information security management demands a clear understanding of technical as well as socio-organizational aspects of the problem. The purpose of this course is to prepare business decision makers who recognize the threats and vulnerabilities present in current information systems and who know how to design and develop secure systems.

OPRE 6301 (SYSM 6303) Quantitative Introduction to Risk and Uncertainty in Business
Introduction to statistical and probabilistic methods and theory applicable to situations faced by managers. Topics include: data presentation and summarization, regression analysis, fundamental probability theory and random variables, introductory decision analysis, estimation, confidence intervals, hypothesis testing, and One Way ANOVA (Some sections of this class may require a laptop computer).

OPRE 6335 (SYSM 6304) Risk and Decision Analysis

This course provides an overview of the main concepts and methods of risk assessment, risk management, and decision analysis. The methods used in industry, such as probabilistic risk assessment, six sigma, and reliability, are discussed. Advanced methods from economics and finance (decision optimization and portfolio analysis) are presented. (Since our data security and privacy research involves risk analysis we encourage our Cyber Security students to take this course.)

OPRE 6311 Game Theory
Two person zero-sum and nonzero-sum games; Nash equilibrium; use of LP and Complementarily, N-person games; core, nucleolus, stable sets, etc. Applications to market equilibrium problems. (Since our data security and privacy research applied game theory, we encourage our Cyber Security students to take this course.)

ACCT 6334 Auditing
This course introduces the basic concepts, philosophy, standards, procedures, and practices of auditing. Topics include generally accepted auditing standards, the changing role of the independent auditor, professional conduct and ethics, auditor's reporting responsibilities, risk assessment, internal control, evidential matter, and management fraud.

HMGT 6336 (ACCT 6336) Information Technology Audit and Risk Management
Management's role in designing and controlling information technology used to process data is studied. Topics include the role of internal and external auditors in systems development, information security, business continuity, information technology, internet, change management and operations. Focus is placed on the assurance of controls over information technology risks and covers topics directly related to the Certified Information Systems Auditor (CISA) exam (Since our data privacy research focuses on medical records privacy we encourage our Cyber Security students to take this course.)

2.3 Affiliated Faculty in Cyber Security

Erik Jonsson School of Engineering and Computer Science (ECS)

Hal Sudborough, PhD (Pennsylvania State University)
http://www.utdallas.edu/~hal/
Prof. Sudborough teaches Theory of Computation and occasionally teaches Cryptography.

Ebru Celikel Cankaya, PhD (Ege University, Izmir/Turkey)
http://www.utdallas.edu/~exc067000/
Dr. Ebru Celikel is a Senior Lecturer and teaches Data and Applications Security occasionally at the undergraduate level.

Cong Liu, PhD (UNC Chapel Hill) Real-time Systems
http://www.utdallas.edu/~cxl137330/
Prof. Liu works in real-time systems and is involved in exploratory research on secure real-time systems.

Neeraj Mittal, PhD ((University of Texas at Austin)) Wireless Networks
http://www.utdallas.edu/~neerajm/
Prof. Mittal is an expert in computer networks and conducts research in wireless network security. He also introduced security units into his courses.

B. Prabhakaran, PhD (IIT Madras) Multimedia and Video Analytics
http://www.utdallas.edu/~praba/

Prof. Prabhakaran is an expert in multimedia systems and conducts research in digital watermarking. He also introduced units on digital watermarking into his courses.

Eric Wong, PhD (Purdue University) Software Engineering
http://www.utdallas.edu/~ewong/
Prof. Eric Wong does research in dependable and reliable systems as well as software engineering and testing and introduces security units in his courses.

Weili Wu, PhD (University of Minnesota) Data Management and Mining
http://www.utdallas.edu/~weiliwu/
Prof. Weili Wu conducts research in systems and theory of computation and in wireless security.

I-Ling Yen, PhD (University of Houston) Web Services and Cloud Computing
http://www.utdallas.edu/~ilyen/
Prof. Yen is an expert in service computing and has conducted substantial research in web services security.

Farokh Bastani, PhD (University of CA at Berkeley) NSF IUCRC
http://www.utdallas.edu/~bastani/
Prof. Bastani was one of the key people in initiating cyber security at UTD and worked towards hiring Prof. Thuraisingham to establish the Cyber Security Research Center. He heads an NSF IUCRC on Network Centric Systems which is affiliated with UTD's CSI.

Faculty from the Schools of (i) Management (JSOM), (ii) Economics, Policy and Political Sciences (EPPS), and (iii) Natural Sciences and Mathematics (NSM), and (iv) Brain and Behavioral Sciences (BBS)

Michael Baron, PhD (University of Maryland) Statistics Methods for Security
http://www.utdallas.edu/~mbaron/
Prof. Baron is in NSM and is an expert statistician. We are collaborating on an NSF project in applying statistical methods and will be examining cyber security as an application area.

Alain Bensoussan, PhD (University of Paris) Risk and Decision Sciences
http://www.utdallas.edu/~axb046100/
Prof. Benssousan is in JSOM and is a world famous mathematician and collaborates with us on a number of research projects. Results of this research have been incorporated into our courses. He is also listed under the Cyber Security/CS faculty.

Huseyin Cavusoglu, PhD (University of Texas at Dallas), Management Information Systems
http://jindal.utdallas.edu/faculty/huseyin-cavusoglu
Dr. Cavusoglu teaches cyber security for management students in JSOM. He also works closely with the ECS team and participates in technology exchange meetings. We are planning to introduce some joint programs between ECS and JSOM. He is also listed under the Cyber Security/CS faculty.

Daniel Krawczyk, PhD (UCLA) Psychosocial Aspects of Security
http://bbs.utdallas.edu/people/detail.php5?i=321
Prof. Krawczyk is in BBS and we are conducting joint research in applying fMRI techniques to study the minds of the hacker. The results will be incorporated into our cyber security courses.

Indranil Bardhan, PhD (University of Texas at Austin) Information Systems
http://www.utdallas.edu/~bardhan/
Prof. Bardhan is in JSOM and is involved in healthcare security. We participate in technical exchange meetings and plan to collaborate on research projects.

James Bartlett, PhD (Yale University) Cognitive Psychology
http://bbs.utdallas.edu/people/detail.php5?i=51
Prof. Bartlett is in BBS and works with Prof. Krawczyk on applying fMRI techniques to study the minds of the hacker.

Patrick Brandt , PhD (Indiana University) Political Science
http://www.utdallas.edu/~pbrandt/Patrick_Brandts_Website/Home.html
Prof. Brandt is in EPPS and is a political scientist and manages the GDELT data sets. He is working with us to using big data analytics techniques for the GDELT data sets. We have a joint NSF grant with Dr. Brandt on big data analytics.

Jennifer Holmes, PhD (University of Minnesota), Public Policy
http://www.utdallas.edu/~jholmes/
Prof. Holmes heads the Public Policy program and collaborates with Dr. Cardenas on a joint NSF grant.

Matthew Goeckner, PhD (University of Iowa) Math, Physics
http://www.utdallas.edu/~goeckner/
Prof. Goeckner is the department head of Mathematics (NSM), and works with us to bring the Math expertise to our projects as needed.

Robert Morris, PhD (Sam Houston State University) Criminology
http://www.utdallas.edu/~rgm071000/Professor_Morris_Webpage/Home.html
Prof. Morris is a criminologist in EPPS and is involved in investigating social theories. We have discussed aspects of including social theories to study hackers. We also plan to have a joint digital forensics program with EPPS.

Fang Qiu, PhD (University of South Carolina) Geographic Information Sciences
http://www.utdallas.edu/~ffqiu/
Prof. Fang Qiu is in EPPS and is an expert in geospatial systems. We have collaborated with him on geospatial system projects. This has enabled us also to explore geospatial systems security. We have introduced results from this research into our courses.

Prof. Nathan Berg, PhD (University of Kansas), Behavioral Economics
http://www.business.otago.ac.nz/econ/staff/berg.html
formerly http://www.utdallas.edu/experts/profiles/berg_nathan.html
Prof. Berg was at UTD until last Fall and collaborated with us extensively on research projects including a DoD MURI on behavioral economics of assured information sharing. He left to join University of Otago in New Zealand.

Srinivasan Raghunathan, PhD (University of Pittsburg) Economics of Security
http://www.utdallas.edu/~sraghu/,
Prof. Raghunathan's research includes economics of security. In the past we collaborated with Prof. Nathan Berg in EPPS who recently moved to New Zealand. We are investigating ways to collaborate with Prof. Raghunathan on economics related aspects of security. We plan to expand this area. He is also listed under the Cyber Security/CS faculty.

3. CORE CYBER SECURITY FACULTY RESEARCH PAST FIVE YEARS

Note: Several papers are co-authored among the faculty members. We have tried to remove duplicates as much as possible.

Dr. Bhavani Thuraisingham

(a) Journals and Conference Publications (2011-present; 5 years)

Several of Dr. Thuraisingham's papers are co-authored with Dr. Kantarcioglu and Dr. Khan. These papers are listed under Dr. Kantarcioglu and Dr. Khan's publications.

JOURNALS

- Gregory S. Lee, Bhavani M. Thuraisingham: Cyberphysical systems security applied to telesurgical robotics. Computer Standards & Interfaces 34(1): 225-229 (2012)
- Wei She, I-Ling Yen, Bhavani M. Thuraisingham, Elisa Bertino: Security-Aware Service Composition with Fine-Grained Information Flow Control. IEEE T. Services Computing 6(3): 330-343 (2013)
- W. Eric Wong, Vidroha Debroy, Richard Golden, Xiaofeng Xu, Bhavani M. Thuraisingham: Effective Software Fault Localization Using an RBF Neural Network. IEEE Transactions on Reliability 61(1): 149-169 (2012) http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6058639
- Pallabi Parveen, Nathan McDaniel, Zackary R. Weger, Jonathan Evans, Bhavani M. Thuraisingham, Kevin W. Hamlen, Latifur Khan: Evolving Insider Threat Detection Stream Mining Perspective. International Journal on Artificial Intelligence Tools 22(5) (2013)
- *The Continued War on Terrorism – How to Maintain Long-range Deterrence Against Terrorism*, To appear in Journal of Policing, Intelligence and Counter Terrorism, 2014. (co-author: Jan Kallberg).
- Jan Kallberg, Bhavani M. Thuraisingham: State Actors' Offensive Cyberoperations: The Disruptive Power of Systematic Cyberattacks. IT Professional 15(3): 32-35 (2013)
- *Cyber Operations – Bridging from Concept to Cyber Superiority.* Joint Force Quarterly. 1st quarter 2013 Kallberg, Jan, and Bhavani Thuraisingham.. (Q1 in their field – below 10 % acceptance rate).
- Reducing the Potential Perpetrator Perceived Opportunity by Injecting Fear of Failure. Kallberg, Jan, and Bhavani Thuraisingham. Terrorism and Political Violence. (Special issue - forthcoming Spring 2014).

CONFERENCE PROCEEDINGS

- Kevin W. Hamlen, Peng Liu, Murat Kantarcioglu, Bhavani M. Thuraisingham, Ting Yu: Identity management for cloud computing: developments and directions. CSIIRW 2011: 32
- *Secure Data Processing in a Hybrid Cloud*, Computing Research Repository (CoRR) abs/1105.1982, 2011 (co-authors: V. Khadilkar, M. Kantarcioglu, S. Mehrotra).
- *On Secure and Resilient Telesurgery over Unreliable Networks,* The First International Workshop on Cyber-Physical Networking Systems, p. 725 – 730, Shanghai, China, April 2011, (co-authors: M. E. Tozal, Y. Wang, E. Al-Shaer, K. Sarac, B. Chu).
- *Towards Cyber Operations - The New Role of Academic Cyber Security Research and Education*, In Proceedings of IEEE Intelligence and Security Informatics (ISI 2012), Washington DC, June 2012 (co-author: J. Kallberg).
- Pallabi Parveen, Bhavani M. Thuraisingham: Unsupervised incremental sequence learning for insider threat detection. ISI 2012: 141-143

- Pallabi Parveen, Nate McDaniel, Varun S. Hariharan, Bhavani M. Thuraisingham, Latifur Khan: Unsupervised Ensemble Based Learning for Insider Threat Detection. SocialCom/PASSAT 2012: 718-727, 2011
- Pallabi Parveen, Zackary R. Weger, Bhavani M. Thuraisingham, Kevin W. Hamlen, Latifur Khan: Supervised Learning for Insider Threat Detection Using Stream Mining. ICTAI 2011: 1032-1039
- Wei She, I-Ling Yen, Farokh B. Bastani, Bao N. Tran, Bhavani M. Thuraisingham: Role-based integrated access control and data provenance for SOA based net-centric systems. SOSE 2011: 225-234

(b) Books and Book Chapters (2009-Present, 5 years)

Books

- *Design and Implementation of Data Mining Tools,* CRC Press, June 2009 (co-authors: L. Khan, M. Awad, L. Wang).
- *Secure Semantic Service Oriented Systems,* CRC Press, 2010.
- *Data Mining Tools for Malware Detection,* CRC Press, December 2011 (co-authors: L. Khan, M. Masud).
- *Developing and Securing the Cloud*, CRC Press, November 2013.
- *Secure Data Provenance and Inference Control with Semantic Web*, CRC Press, Contract signed May 2012, Book in publication (co-authors: T. Cadenhead, M. Kantarcioglu, V. Khadilkar).

Book Chapters

C. C. Yang and B. Thuraisingham, A Generalized Approach for Social Network Integration and Analysis with Privacy Preservation, *Data Mining and Knowledge Discovery for Big Data: Methodologies, Challenges, and Opportunities*, Wesley Chu (Editor), Springer Verlag, 2014.

(c) Research Grants (2011-Present, 5 years)

"Secure Sensor Semantic Web"
Bhavani Thuraisingham, PI, Murat Kantarcioglu, co-PI, Latifur Khan, co-PI
Air Force Office of Scientific Research
05.01.2009-05.14.2014 $1,763,168

"Capacity Building for Assured Cloud Computing"
Bhavani Thuraisingham, PI, Murat Kantarcioglu, Latifur Khan, Kevin Hamlen, (co-PIs)
NSF 9/15/2011-8/31/2014, $264,580

"Semantic Approach to Behavior based IDS and Its Applications,"
Bhavani Thuraisingham (PI), Latifur Khan (co-PI), Kevin Hamlen (co-PI), Zhiqiang Lin (co-PI)
MINI MURI: Air Force Office of Scientific Research," July 2012 – June 2016, $965,758.

"A Framework for Managing the Assured Information Sharing Lifecycle"
Bhavani Thuraisinghaim PI, Murat Kantarcioglu co-PI
AFOSR 09.01.07-07.30.13, $ 1,000,000

"Secure Semantic Service Oriented Information Grid for NCES and Border Security Applications"

Bhavani Thuraisingham, PI, Murat Kantarcioglu, co-PI
AFOSR 05.01.2008-04.30.12, $2,271,640

(d) Subject matter experts for Professional Societies (2011-Present, 5 years)

Professional Memberships
IEEE Fellow (2003-Present)
AAAS Fellow (2003-Present)
BCS (British Computer Society) Fellow (2005-Present)
SDPS (Society for Design and: Process Science) Fellow (2011-Present)
SIRI (Society for Information Reuse and Integration) Fellow (2011-Present)
ACM Distinguished Scientist (2010-Present)

Awards (2011-Present, 5 years)

- 2011 AFCEA (Armed Forces Communications and Electronics Association) Medal of Merit for Service to AFCEA and Sustained Professional Excellence in Communications, Electronics, Intelligence and Information Systems
- Recipient of 2012 SDPS Transformative Achievement Gold Medal for Transdisciplinary Research in Cyber Security
- IBM Faculty Award in Cyber Security Education, 2013

Certifications:

ISC2: CISSP (Certified Information Systems Professional), July 2010, recertified October 2013

SANS Institute GCFE (Certified Forensics Expert), November 2013

Terrorism Studies, St. Andrews University, Scotland, July 2010

Editorial Boards
Very Large Database Journal, 2007 – 2011; IEEE Intelligent Systems, 2012-Present; ACM Transactions on Management Information Systems 2013-Present

Conference General/Program Chair
IEEE ICDM, Dallas TX December 2013 (General Co-Chair)
IEEE Information Reuse and Integration, Las Vegas, NV, August 2012 (Program Co-Chair)
IEEE Information Reuse and Integration, Las Vegas, NV, August 2013 Program Co-Chair)
IEEE Trustcom, July013, Melbourne, Australia, (Program Co-Chair)
IEEE Conference on Web Services, June 2014, Anchorage Alaska (Program Co-Chair)

Program Committee member for multiple conferences

Review for Journals/Conferences
IEEE Transactions on Dependable and Secure Computing

(e) Student Cyber Security Programs (2011 – Present, 5 years)

Works with the team in organizing Cyber Security courses and annual conference. Advises PhD and MS students in Cyber Security. Co-PI of the NSF SFS Grant and supports the student research efforts.

(f) Presentations (2011 – Present, 5 years)

FEATURED/KEYNOTE PRESENTATIONS

- *Data Mining for Malware Detection*, SDPS Annual Conference, Jeju Island, S. Korea, June 2011.
- *Data Mining for Malware Detection*, European Intelligence and Security Informatics, September 2011, Athens, Greece.
- *Data Mining for Malware Detection*, DFW MetroCon, October 2011, Arlington, TX.
- *Assured Cloud-based Information Sharing*, IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), December 2011, Sydney, Australia.
- *Assured Cloud Computing,* Cyber Security Conference, Cyber security conference at Arizona State University, April 2012
- *Data Mining for Malware Detection*, Special featured presentation/tutorial at SDPS Conference, Berlin, Germany, June 2012.
- *Assured Cloud-based Information Sharing*, International Symposium on Foundation of Open Source Intelligence and Security Informatics (FOSINT 2012), August 2012, Istanbul Turkey..
- *Assured Cloud-based Social Networking*, Chinese Academy of Sciences Conference on Social Computing, Beijing, China, November 2012.
- *Secure Cloud Computing*, University of North Texas/Collin College SoMiC Workshop on Cyber Security, Denton, TX, April 2013.
- *Analyzing and Securing Social Networks*, WWW Workshop on Social Network Security and Privacy, Rio De Janeiro, Brazil, May 2013.
- *Measuring Expertise and Bias in Cyber Security Using Cognitive and Neuroscience Approaches*, IEEE ISI Workshop on Social Informatics, Seattle, June 2013 (Presented by Daniel Krawczyk).
- *Cloud-based Assured Information Sharing*, Conference on Security, Privacy and Trust, Melbourne Australia, July 2013.
- *Analyzing and Securing Social Networks*, Society for Design and Process Science World Conference, Campenas, Brazil, October 2013.
- *Cloud-based Assured Information Sharing*, IEEE Cloudcom, Bristol UK, December 2013.
- *Directions for Cyber Security Research*, Featured address at the Cyber Security in Action Symposium as part of HICSS 2014, Waikoloa, HI, January 2014.

OTHER PRESENTATIONS

Synopsis: Given several presentations at Technology Exchange meetings (e.g, Air Force Office of Scientific Research), Invited seminars at universities (e.g., University of North Carolina, Greensborough, April 2012)

Dr. Kamil Sarac

(a) Publications

- Adaptive Information Coding for Secure and Reliable Wireless Telesurgery Communications, M.E. Tozal, Y. Wang, E. Al-Shaer, K. Sarac, B. Thuraisingham, B-T. Chu, Journal of Mobile Networks and Applications, Vol.18, Issue 5, October 2013, pp 697-711.
- Polynomial Time Solution to Minimum Forwarding Set Problem in Wireless Networks under Disk Coverage Model, M. Baysan, K. Sarac, and R. Chandrasekaran, *Ad Hoc Networks Journal*, *Vol.10, No. 7, pp. 1253-1266, September 2012.*
- PalmTree: An IP Alias Resolution Algorithm with Linear Probing Complexity, M.E. Tozal and K. Sarac, *Computer Communications*, *Vol. 34, No. 5, pp. 658-669, April 2011.*
- Location Matters: Eliciting Responses to Direct Probes, Ethan Blanton, Mehmet E Tozal, Kamil Sarac, and Sonia Fahmy, *IEEE IPCCC*, December 2013.
- Impact of Sampling Design in Estimation of Graph Characteristics, Emrah Cem, Mehmet E Tozal, and Kamil Sarac, *IEEE IPCCC*, Decembe 2013.
- Estimating Network Layer Subnet Characteristics via Statistical Sampling, M.E. Tozal and K. Sarac, *IFIP Networking*, Prague, Czech Republic, May 2012.
- Subnet Level Network Topology Mapping, M.E. Tozal and K. Sarac, *IEEE IPCCC*, Orlando, Florida, November 2011.
- A Security Framework for Service Overlay Networks: Operating in the Presence of Compromised Nodes, J. Kurian and K. Sarac, *Parallel and Distributed Computing and Systems*, Dallas, Texas, December 2011.
- Relay Assignment in AMT-based Multicast Content Distribution, S. Patel, K. Sarac, R. Chandrasekaran, T. Korkmaz, N. Mittal, *9th Annual Conference on Communication Networks and Services Research Conference*, Ottawa, Ontario, Canada, May 2011.

(c) Research Grants (2011-Present, 5 years)

- "DoD Information Assurance Scholarship Program", Role: PI, Department of Defense, National Security Agency, $40,000, 2013-2014.
- "DoD Information Assurance Scholarship Program", Role: PI, Department of Defense, National Security Agency, $85,894, 2012-2013.
- "Federal Cyber Service: Scholarship for Service Program in UT Dallas" (Student travel grants for TexSAW 2012 event, Role: PI, NSF, $10,000, 2012.
- "DoD Information Assurance Scholarship Program", Role: PI, Department of Defense, National Security Agency, $74,160, 2011-2012.
- "Capacity Building for Assured Cloud Computing", Role: Co-PI, NSF, $264,580, 2011-2013.
- "Federal Cyber Service: Scholarship for Service Program in UT Dallas" (Student travel grants for TexSAW 2011 event, Role: PI, NSF, $10,000, 2011.
- "Federal Cyber Service: Scholarship for Service Program in UT Dallas", Role: PI (Co-PIs: Drs. Thuraisingham, Sha, Hamlen, and Kantarcioglu), NSF, $1.8M, 2010-2014.

(d) Subject matter experts for Professional Societies (2011-Present, 5 years)

Senior member of IEEE since June 2009.
Program Committee member of several conferences

(e) Student Cyber Security Programs (2011 – Present, 5 years)

Dr. Sarac serves as the faculty mentor of UTD Computer Security Club (CSG) a campus registered student club. Dr. Sarac also serves as the director of cybersecurity education programs at the CS department since Fall 2011.

(f) Presentations (2011 – Present, 5 years)

- Panelist at NSF United States / Middle East Workshop on Trustworthiness in Emerging Distributed Systems and Networks, Koc University, Istanbul, Turkey, June 4-6, 2012
- Panelist at the Fifth Annual Workshop on Information Assurance Research & Education Information Assurance Center at Arizona State University, April 25, 2012
- Estimating Network Layer Subnet Characteristics via Statistical Sampling, M.E. Tozal and K. Sarac, IFIP Networking, Prague, Czech Republic, May 2012.

Dr. Murat Kantarcioglu

(a) Journals and Conference Publications with Links (2011-present; 5 years)

JOURNALS

- R. Heatherly, M. Kantarcioglu, B. Thuraisingham, Preventing Private Information Inference Attacks on Social Networks, IEEE Transactions on Knowledge and Data Engineering, , Vol. 25, No. 8, 2013:
- Bijit Hore, Sharad Mehrotra, Mustafa Canim, Murat Kantarcioglu, "Secure multidimensional range queries over outsourced data", The VLDB Journal, VLDB Endowment, VLDB J. 21(3): 333-358 (2012).
- Elizabeth Durham, Y. Xue, Murat Kantarcioglu, Bradley Malin, "Quantifying the Correctness, Computational Compexity, and Security of Privacy-preserving String comparators for Record Linkage". Information Fusion, 13(4): 245-259 (2012).
- Robert Nix, Murat Kantarcioglu, "Incentive Compatible Privacy-Preserving Distributed Classification", IEEE Transactions on Dependable and Secure Computing, 9(4): 451-462 (2012).
- Mustafa Canim, Murat Kantarcioglu, Bradley Malin, “Secure Management of Biomedical Data with Cryptographic Hardware”, IEEE Transactions on Information Technology in Biomedicine 16(1): 166-175 (2012).
- Ali Inan, Murat Kantarcioglu, Gabriel Ghinita, Elisa Bertino, “A Hybrid Approach to Private Record Matching”, IEEE Transactions on Dependable and Secure Computing , 9(5): 684-698 (2012)
- Khaled El Emam, Saeed Samet, Jun Hu, Liam Peyton, Craig Earle, Gayatri C. Jayaraman, Tom Wong, Murat Kantarcioglu, Fida Dankar, Aleksander Essex "A Protocol for the Secure Linking of Registries for HPV Surveillance", PLoS ONE 7(7): e39915. doi:10.1371/journal.pone.0039915
- Kevin W. Hamlen, Lalana Kagal, Murat Kantarcioglu, “Policy Enforcement Framework for Cloud Data Management”, IEEE Data Engineering Bulletin, 35(4): 39-45 (2012)
- Vaibhav Khadilkar, Kerim Yasin Oktay, Murat Kantarcioglu, Sharad Mehrotra, “Secure Data Processing over Hybrid Clouds”, IEEE Data Eng. Bulletin, 35 (4): 46-54 (2012) (http://sites.computer.org/debull/A12dec/hybrid.pdf)
- Gabriel Ghinita, Panos Kalnis, Murat Kantarcioglu, Elisa Bertino, "Approximate and Exact Hybrid Algorithms for Private Nearest-Neighbor Queries with Database Protection", Geoinformatica 15, (4): 699-726 (2011).
- Khaled El Emam,Jun Hu, Jay Mercer, Liam Peyton, Murat Kantarcioglu, Bradley Malin, David Buckeridge, Saeed Samet, Craig Earle, "A secure protocol for protecting the identity

of providers when disclosing data for disease surveillance", Journal of American Medical Informatics Association (JAMIA), 18, pp 212-217 (2011).

- Murat Kantarcioglu, Bowei Xi, Chris Clifton, "Classifier Evaluation and Attribute Selection against Active Adversaries", Springer Data Mining and Knowledge Discovery, Volume 22, Numbers 1-2, pp 291-335 (2011).
- Barbara Carminati, Elena Ferrari, Raymond Heatherly, Murat Kantarcioglu, and Bhavani Thuraisinghaim. "Semantic Web-Based Social Network Access Control", Computers and Security Journal, Volume 30, Issues 2-3, pp 108-115, (2011).
- Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, "Security Issues for Cloud Computing", International Journal on Information Security and Privacy, Vol 4, No. 2, pp 36-48 (2010)
- Sunitha Ramanujam, Vaibhav Khadilkar, Latifur Khan, Murat Kantarcioglu, Bhavani M. Thuraisingham, Steven Seida, "Update-Enabled Triplification of Relational Data into Virtual RDF Stores", Int. J. Semantic Computing 4(4): 423-451 (2010)

CONFERENCE PROCEEDINGS:

- Mohammad Saiful Islam, Mehmet Kuzu, Murat Kantarcioglu, "Access Pattern disclosure on Searchable Encryption: Ramification, Attack and Mitigation", The Network & Distributed System Security Conference, 2012
- Yan Zhou, Murat Kantarcioglu, Bhavani M. Thuraisingham, "Self-Training with Selection-by-Rejection", IEEE ICDM 2012: 795-803
- Yan Zhou, Murat Kantarcioglu, Bhavani M. Thuraisingham, "Sparse Bayesian Adversarial Learning Using Relevance Vector Machine Ensembles", IEEE ICDM 2012: 1206-1211
- Yan Zhou, Murat Kantarcioglu, Bhavani M. Thuraisingham, Bowei Xi, "Adversarial Support Vector Machine Learning", ACM KDD 2012: 1059-1067
- Mehmet Kuzu, Mohammad Saiful Islam, Murat Kantarcioglu, "Efficient Similarity Search over Encrypted Data", IEEE ICDE 2012
- Hyo-Sang Lim, Gabriel Ghinita, Elisa Bertino, Murat Kantarcioglu, "A Game-Theoretic Approach for High-Assurance of Data Trustworthiness in Sensor Networks", IEEE ICDE 2012
- 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
- Vaibhav Khadilkar, Murat Kantarcioglu, Bhavani M. Thuraisingham, "StormRider: harnessing "storm" for Social Networks", WWW 2012: 543-544
- Tyrone Cadenhead, Murat Kantarcioglu, Vaibhav Khadilkar, Bhavani M. Thuraisingham, "Design and Implementation of a Cloud-Based Assured Information Sharing System" MMM-ACNS 2012: 36-50
- Bhavani Thuraisingham, Vaibhav Khadilkar, Jyothsna Rachapalli, Tyrone Cadenhead, Murat Kantarcioglu, Kevin W. Hamlen, Latifur Khan, Mohammad Farhan Husain, "Cloud-Centric Assured Information Sharing", PAISI 2012: 1-26
- Tyrone Cadenhead, Vaibhav Khadilkar, Murat Kantarcioglu, Bhavani M. Thuraisingham, "A cloud-based RDF Policy Engine for Assured Information Sharing", SACMAT 2012: 113-116

- Mohammad Saiful Islam, Robert Nix, Murat Kantarcioglu, "A Game Theoretic Approach for Adversarial Pipeline Monitoring using Wireless Sensor Networks", IEEE IRI 2012: 37-44
- SingRu (Celine) Hoe, Murat Kantarcioglu, Alain Bensoussan, "Studying Dynamic Equilibrium of Cloud Computing Adoption with Application of Mean Field Game ", Allerton Conference 2012.
- Robert Nix, Murat Kantarcioglu, "Contractual Agreement Design for Enforcing Honesty in Cloud Outsourcing", GameSec 2012: 296-308
- SingRu (Celine) Hoe, Murat Kantarcioglu, Alain Bensoussan, "A Game Theoretical Analysis of Lemonizing Cybercriminal Black Markets", GameSec 2012: 60-77
- Robert Nix, Murat Kantarcioglu, Keesook J. Han, "Approximate Privacy-Preserving Data Mining on Vertically Partitioned Data", DBSec 2012: 129-144
- Abhijith Shastry, Murat Kantarcioglu, Yan Zhou, Bhavani Thuraisingham, "Randomizing Smartphone Malware Profiles against Statistical Mining Techniques", DBSec 2012: 239-254
- Jyothsna Rachapalli, Murat Kantarcioglu, Bhavani Thuraisingham, "Tag-based Information Flow Analysis for Document Classification in Provenance", 4th USENIX Workshop on the Theory and Practice of Provenance (TaPP '12)
- Vaibhav Khadilkar, Murat Kantarcioglu, Bhavani M. Thuraisingham, Paolo Castagna, "Jena-HBase: A Distributed, Scalable and Effcient RDF Triple Store", International Semantic Web Conference (Posters & Demos) 2012
- Mohammad Saiful Islam, Mehmet Kuzu, Murat Kantarcioglu, “Poster: inference attacks against searchable encryption protocols”. ACM Conference on Computer and Communications Security 2011: 845-448
- Murat Kantarcioglu, Alain Bensoussan, Singru Hoe, “Impact of Security Risks on Cloud Computing Adoption”, Allerton Conference 2011.
- Jyothsna Rachapalli, Vaibhav Khadilkar, Murat Kantarcioglu and Bhavani Thuraisingham, “RETRO: A Framework for Semantics Preserving SQL-to-SPARQL Translation”, EvoDyn Workshop, 2011.
- Murat Kantarcioglu, Alain Bensoussan, SingRu Celine Hoe, “Investment in Privacy-Preserving Technologies under Uncertainty” GameSec 2011: 219-238
- Mohamed Nabeel, Elisa Bertino, Murat Kantarcioglu, Bhavani M. Thuraisingham, “Towards privacy preserving access control in the cloud”, CollaborateCom 2011: 172-180
- Tyrone Cadenhead, Vaibhav Khadilkar, Murat Kantarcioglu, and Bhavani Thuraisingham, "Transforming Provenance Using Redaction", ACM SACMAT 2011: 93-102
- Mehmet Kuzu, Murat Kantarcioglu, Elizabeth Durham, Bradley Malin, "A Constraint Satisfaction Cryptanalysis of Bloom Filters in Private Record Linkage", PETS 2011: 226-245
- Raymond Heatherly, Murat Kantarcioglu,"Automatic Sanitization of Social Network Data to Prevent Inference Attacks" WWW 2011: 55-56
- Raymond Heatherly, Murat Kantarcioglu,"Extending the Classification of Nodes in Social Networks", IEEE International Conference on Intelligence and Security Informatics 2011.
- James R. Johnson, Anita Miller, Latifur Khan, Bhavani Thuraisingham, Murat Kantarcioglu, "Identification of Related Information of Interest across Free Text Documents" IEEE International Conference on Intelligence and Security Informatics 2011.

- James R. Johnson, Anita Miller, Latifur Khan, Bhavani Thuraisingham, Murat Kantarcioglu, "Extraction of Expanded Entity Phrases" IEEE International Conference on Intelligence and Security Informatics 2011.
- Tyrone Cadenhead, Murat Kantarcioglu, and Bhavani Thuraisingham, "A Framework for Policies over Provenance",3rd USENIX Workshop on the Theory and Practice of Provenance
- Tyrone Cadenhead, Vaibhav Khadilkar, Murat Kantarcioglu, and Bhavani Thuraisingham, "A Language for Provenance Access Control" ACM CODASPY 2011: 133-144
- Bowei Xi, Murat Kantarcioglu, Ali Inan, "Mixture of Gaussian Models and Bayes Error under Differential Privacy", ACM CODASPY 2011: 179-190
- Richard Wartell, Yan Zhou, Kevin W. Hamlen, Murat Kantarcioglu, Bhavani M. Thuraisingham, "Differentiating Code from Data in x86 Binaries" ECML/PKDD (3) 2011: 522-536
- Yan Zhou, W. Meador Inge, Murat Kantarcioglu, "Compression for Anti-Adversarial Learning", PAKDD (2) 2011: 198-209

(c) Research Grants (2011-Present, 5 years)

"Career: An integrated approach for efficient privacy preserving distributed data analytics"
Murat Kantarcioglu, PI
National Science Foundation
01.01.2009-12.31.2014, $400,000

"Technologies to Enable Privacy in Biobanks"
Murat Kantarcioglu, PI (subcontracted from Vanderbilt University)
NIH
07.01.2009 – 06.30.2013, $360,000 (UT Dallas Portion)

"A Systematic Defense Framework for Combating Botnets"
Murat Kantarcioglu, PI, Alain Bensoussan, co-PI
ONR, (subcontracted from Purdue University)
06.01.2009-05.30.2014, $60,000

"NeTS: Medium: Collaborative Research: A Comprehensive Approach for Data Quality Provenance in Sensor Networks"
Murat Kantarcioglu, PI
NSF
05.01.2010-04.30.2013, $150,000

"TC:Small:Collaborative:Protocols for Privacy-Preserving Scalable Record Matching and Ontology Alignment"
Murat Kantarcioglu, PI, Latifur Khan, co-PI, Bhavani Thuraisingham, co-PI
NSF
08.01.2010-07.31.2013, $259,674

"TC: Large: Collaborative Research: Privacy-Enhanced Secure Data Provenance"
Murat Kantarcioglu,PI, B. Thuraisingham co-PI, Alain Bensoussan,co-PI
08.25.2011-08.24.2016, $912,068

"A Game Theoretic Framework for Adversarial Classification"
Murat Kantarcioglu,PI, B. Thuraisingham co-PI, Nathan Berg, co-PI
Army Research Office
09/01/2012-08/31/2015, $400,000

"Ecologically Inspired Framework for Assured Information Cloud"
Murat Kantarcioglu,PI, B. Thuraisingham co-PI, Alain Bensoussan,co-PI
AFOSR,
04/01/2012-03/31/2015, $360,000

"TWC: Medium: Collaborative: Policy Compliant Integration of Linked Data"
Murat Kantarcioglu,PI, Kevin Hamlen co-PI, Latifur Khan co-PI
NSF
9/1/2012 – 8/31/2015, $399,897

"A Risk Management Framework for Identifiability in Genomics Research"
Murat Kantarcioglu PI (UT Dallas)
NIH (Subcontract from Vanderbilt Univ)
07/01/2012-06/30/2016, $300,000

(d) Subject matter experts for Professional Societies (2011-Present, 5 years)

Program Chair for GameSec Confernece 2013
Program Commitete for numerlus conferences
IEEE Senior Member, ACM Senior Member
NSF Career Award, 2009.

(e) Student Cyber Security Programs (2011 – Present, 5 years)

Dr. Kantarcioglu is an expert in data security and privacy. He supervises several PhD students and works with Cyber Security Students on course projects in his area if expertise.

(f) Presentations (2011 – Present, 5 years)

- "Adversarial Support Vector Machine Learning", August 2012, ACM KDD 2012
- "Limits of Data Mining in Detecting/Predicting Malicious Activity", June 2012, IEEE Compsac Conference
- "Randomizing Smartphone Malware Profiles against Statistical Mining Techniques", IFIP DBSEC 2012 Conference
- "Approximate Privacy-Preserving Data Mining on Vertically Partitioned Data", IFIP DBSEC 2012 Conference
- "Risk Aware Data Processing on the Cloud", IEEE Cloud 2012
- "Introduction to Hadoop and Access control in Hadoop", May 2012, Air Force Research Labs, Rome, NY
- "Mining Big Databases without Violating Privacy", March 2012, Vanderbilt University
- "Access Pattern disclosure on Searchable Encryption: Ramification, Attack and Mitigation", NDSS 2012 Conference

- “Risk Aware Query Processing in Hybrid Clouds”, NIST Cloud Assumption Buster Workshop, October, 2011
- “Transforming Provenance Using Redaction", June 2011, ACM SACMAT 2011 Conference
- “Inferring Private Information Using Social Network Data”, April 2011, University of Nevada at Reno.
- “Inferring Private Information Using Social Network Data”, November 2010, Humboldt University, Berlin.

Dr. Kevin Hamlen

(a) Publications (2011-Present, 5 years)

JOURNALS

- Safwan M. Khan and Kevin W. Hamlen. Penny: Secure, Decentralized Data Management. International Journal of Network Security (IJNS), **16**(4):289–303, July 2014, forthcoming.
- Kevin W. Hamlen and Bhavani M. Thuraisingham. Data Security Services, Solutions and Standards for Outsourcing. Computer Standards & Interfaces, **35**(1):1–5, January 2013.
- Kevin W. Hamlen, Lalana Kagal, and Murat Kantarcioglu. Policy Enforcement Framework for Cloud Data Management. IEEE Data Engineering Bulletin (DEB), Special Issue on Security and Privacy in Cloud Computing, **35**(4):39–45, December 2012.
- William Hamlen and Kevin Hamlen. An Interactive Computer Model of Two-Country Trade. International Review of Economics Education (IREE), **11**(2):91–101, November 2012.
- Kevin W. Hamlen and William Hamlen. An Economic Perspective of Message-dropping Attacks in Peer-to-peer Overlays. Intelligence and Security Informatics (ISI), **1**:6, March 2012.
- Bhavani Thuraisingham, Balakrishnan Prabhakaran, Latifur Khan, and Kevin W. Hamlen. A Database Inference Controller for 3D Motion Capture Databases. International Journal of Information Security and Privacy (IJISP), 2012, forthcoming (accepted).
- Kevin W. Hamlen and Bhavani Thuraisingham. Secure Semantic Computing. International Journal of Semantic Computing (IJSC), **5**(2):121–131, June 2011.
- Mohammad M. Masud, Tahseen M. Al-Khateeb, Kevin W. Hamlen, Jing Gao, Latifur Khan, Jiawei Han, and Bhavani Thuraisingham. Cloud-based Malware Detection for Evolving Data Streams. ACM Transactions on Management Information Systems (TMIS), **2**(3), October 2011.
- Mohammad Mehedy Masud, Clay Woolam, Jing Gao, Latifur Khan, Jiawei Han, Kevin W. Hamlen, and Nikunj C. Oza. Facing the Reality of Data Stream Classification: Coping with Scarcity of Labeled Data. Knowledge and Information Systems (KAIS), 1–32, November 2011.

CONFERENCE PROCEEDINGS

- Richard Wartell, Yan Zhou, Kevin W. Hamlen, and Murat Kantarcioglu. Shingled Graph Disassembly: Finding the Undecidable Path. In *Proceedings of the 18th Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD)*, May 2014, forthcoming. [acceptance rate: 16.4%]

- Safwan Mahmud Khan, Kevin W. Hamlen, and Murat Kantarcioglu. Silver Lining: Enforcing Secure Information Flow at the Cloud Edge. In *Proceedings of the 2nd IEEE Conference on Cloud Engineering (IC2E)*, March 2014, forthcoming. [acceptance rate: 20.2%]
- Yangchun Fu, Zhiqiang Lin, and Kevin W. Hamlen. Subverting System Authentication with Context-Aware, Reactive Virtual Machine Introspection. In *Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC)*, pp. 229–238, December 2013. [acceptance rate: 19.8%]
- Richard Wartell, Yan Zhou, Kevin W. Hamlen, and Murat Kantarcioglu. Shingled Graph Disassembly: Finding the Undecidable Path. In *Proceedings of the 16th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, pp. 460–462, October 2013.
- Kevin W. Hamlen. Stealthy Software: Next-generation Cyber-attacks and Defenses, Invited paper. In *Proceedings of the 11th IEEE Intelligence and Security Informatics Conference (ISI)*, pp. 109–112, June 2013.
- Safwan M. Khan and Kevin W. Hamlen. Computation Certification as a Service in the Cloud. In *Proceedings of the 13th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid)*, pp. 434–441, May 2013. [acceptance rate: 22.18%]
- Richard Wartell, Vishwath Mohan, Kevin W. Hamlen, and Zhiqiang Lin. Securing Untrusted Code via Compiler-Agnostic Binary Rewriting. In *Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC)*, pp. 299–308, December 2012. [acceptance rate: 19%] [Best Student Paper]
- Richard Wartell, Vishwath Mohan, Kevin W. Hamlen, and Zhiqiang Lin. Binary Stirring: Self-randomizing Instruction Addresses of Legacy x86 Binary Code. In *Proceedings of the 19th ACM Conference on Computer and Communications Security (CCS)*, pp. 157–168, October 2012. [acceptance rate: 19%] [NYU-Poly AT&T Best Applied Security Paper of the Year, 2nd place, 2012]
- Vishwath Mohan and Kevin W. Hamlen. Frankenstein: Stitching Malware from Benign Binaries. In *Proceedings of the 6th USENIX Workshop on Offensive Technologies (WOOT)*, pp. 77–84, August 2012. [acceptance rate: 40%]
- Safwan M. Khan and Kevin W. Hamlen. AnonymousCloud: A Data Ownership Privacy Provider Framework in Cloud Computing. In *Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 170–176, June 2012. [acceptance rate: <30%]
- Safwan M. Khan and Kevin W. Hamlen. Hatman: Intra-cloud Trust Management for Hadoop. In *Proceedings of the 5th IEEE International Conference on Cloud Computing (CLOUD)*, pp. 494–501, June 2012. [acceptance rate: 19%]
- Kevin W. Hamlen, Micah M. Jones, and Meera Sridhar. Aspect-oriented Runtime Monitor Certification. In *Proceedings of the 18th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, pp. 126–140, March–April 2012. [acceptance rate: 24%]
- Pallabi Parveen, Zackary R. Weger, Bhavani Thuraisingham, Kevin W. Hamlen, and Latifur Khan. Supervised Learning for Insider Threat Detection Using Stream Mining. In *Proceedings of the 23rd IEEE International Conference on Tools with Artificial Intelligence (ICTAI)*, pp. 1032–1039, November 2011. [acceptance rate: 30%] [Best Paper, Special Session on Stream Data Mining]

- Pallabi Parveen, Jonathan Evans, Bhavani Thuraisingham, Kevin W. Hamlen, and Latifur Khan. Insider Threat Detection using Stream Mining and Graph Mining. In *Proceedings of the 3rd IEEE Conference on Privacy, Security, Risk and Trust (PASSAT)*, pp. 1102–1110, October 2011. [acceptance rate: 8%]
- Micah Jones and Kevin W. Hamlen. A Service-oriented Approach to Mobile Code Security. In *Proceedings of the 8th International Conference on Mobile Web Information Systems (MobiWIS)*, pp. 531–538, September 2011. [acceptance rate: 36%]
- Meera Sridhar and Kevin W. Hamlen. Flexible In-lined Reference Monitor Certification: Challenges and Future Directions. In *Proceedings of the 5th ACM SIGPLAN Workshop on Programming Languages meets Program Verification (PLPV)*, pp. 55–60, January 2011. [acceptance rate: 60%]

(b) Book and book chapters (2009-Present, 5 years)

Will be co-editing a book on Next Generation Malware based on the ACSAC conference workshops he chaired in December 2013.

(c) Research Grants (2011-Present, 5 years)

Binary Retrofitting of Untrusted Software Components for Secure Software Complexity Reduction
PI: Kevin Hamlen
Office of Naval Research (ONR)
11/1/13–10/31/16, $593K

Metamorphic Extensions to Frankenstein Malware for Defensive Testing
PI: Kevin Hamlen; Co-PIs: Latifur Khan, Zhiqiang Lin
Raytheon Company (IUCRC Project)
8/12/13–8/11/14, $35K

TWC: Medium: Collaborative Research: Policy Compliant Integration of Linked Data
PI: Murat Kantarcioglu; Co-PIs: Kevin Hamlen, Latifur Khan
National Science Foundation (NSF)
9/1/12–8/31/15, $1.2M total ($400K for UTD)

MRI: Development of an Instrument for Assured Cloud Computing
PI: Latifur Khan; Co-PIs: Kevin Hamlen, Murat Kantarcioglu
National Science Foundation (NSF)
10/1/12–9/30/15, $300K

Semantic Approach to Behavior-based IDS and its Applications
PI: Bhavani Thuraisingham; Co-PIs: Latifur Khan, Zhiqiang Lin, Kevin Hamlen
U.S. Air Force Office of Scientific Research (AFOSR)
4/1/12–3/31/16, $2.2M total ($966K for UTD)

DUE: Capacity Building for Assured Cloud Computing

PI: Bhavani Thuraisingham; Co-PIs: Latifur Khan, Kamil Sarac, Murat Kantarcioglu, Kevin Hamlen
National Science Foundation (NSF)
9/15/11–8/31/14, $265K

TC: Medium: Collaborative Research: Securing Web Advertisements: Fixing the Short-term Crisis and Addressing Long-term Challenges
PI: Kevin Hamlen
National Science Foundation (NSF)
9/1/11–8/31/14, $1.2M total ($527K for UTD)

CAREER: Language-based Security for Polymorphic Malware Protection
PI: Kevin Hamlen
National Science Foundation (NSF)
8/1/11–7/31/16, $504K

Adaptive Malware Detection over Evolving Malwares: Attacks and Defenses
PI: Latifur Khan; Co-PIs: Kevin Hamlen, Bhavani Thuraisingham
U.S. Army
9/1/11–9/30/12, $350K

(d) Subject matter experts for Professional Societies (2011-Present, 5 years)

PROFESSIONAL MEMBERSHIPS
Institute of Electrical and Electronics Engineers (IEEE), 2010-present
Association of Computing Machinery (ACM), 2008-present

Awards
NSF Career Award 2011
AFOSR YIP (Young Investigator Award) 2007

(e) Student Cyber Security Programs (2011 – Present, 5 years)

Dr. Hameln is an expert in programming language and software security. He supervises several PhD students and works with Cyber Security Students on course projects in his area if expertise.

(f) Presentations (2011-Present, 5 years)

Invited speaker, Intel Annual Security Conference, 2013.
Invited speaker, North Texas Contingency Planning Association, 2013.
Invited talk, U. Illinois at Chicago, Computer Science Department, 2013.
Colloquium Speaker, U. Texas at Arlington, Computer Science Department, 2013.
Colloquium Speaker, Southern Methodist University, Computer Science Department, 2013.
Poster Presentation, 16th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2013.
Invited talk, 11th IEEE Intelligence and Security Informatics Conference (ISI), 2013.
Speaker, 18th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), 2012.

Dr. Zhiqiang Lin

(a) Publications (2011-present, 5 years)

JOURNALS

- "Data-Centric OS Kernel Malware Characterization". Junghwan Rhee, Ryan Riley, Zhiqiang Lin, Xuxian Jiang, Dongyan Xu. *IEEE Transactions on Information Forensics and Security*, Volume 9, Issue 1, January 2014.
- "Towards Guest OS writable Virtual Machine Introspection". Zhiqiang Lin. VMware Technical Journal. Volume 2, Issue 2, December 2013.
- "Bridging the Semantic Gap in Virtual Machine Introspection via Online Kernel Data Redirection". Yangchun Fu, and Zhiqiang Lin. In ACM Transactions on Information and System Security (TISSEC), Volume 16 Issue 2, September 2013.

CONFERENCE PROCEEDINGS

- "Hybrid-Bridge: Efficiently Bridging the Semantic-Gap in Virtual Machine Introspection via Decoupled Execution and Training Memoization". Alireza Saberi, Yangchun Fu, and Zhiqiang Lin. To appear in *Proceedings of the 21st ISOC Network and Distributed System Security Symposium*, San Diego, CA, February 2014
- "SMV-Hunter: Large Scale, Automated Detection of SSL/TLS Man-in-the-Middle Vulnerabilities in Android Apps". David Sounthiraraj, Justin Sahs, Zhiqiang Lin, Latifur Khan, and Garrett Greenwood. To appear in *Proceedings of the 21st ISOC Network and Distributed System Security Symposium*, San Diego, CA, February 2014
- "Subverting System Authentication with Context-Aware, Reactive Virtual Machine Introspection". Yangchun Fu, Zhiqiang Lin, and Kevin Hamlen. In *Proceedings of the 29th Annual Computer Security Applications Conference*, New Orleans, Louisiana, December 2013.
- "Obfuscation-resilient Binary Code Reuse through Trace-oriented Programming". Junyuan Zeng, Yangchun Fu, Kenneth Miller, Zhiqiang Lin, Xiangyu Zhang, and Dongyan Xu. In *Proceedings of the 20th ACM Conference on Computer and Communications Security*, Berlin, Germany, November 2013.
- "CPU Transparent Protection of OS Kernel and Hypervisor Integrity with Programmable DRAM". Ziyi Liu, Jonghyuk Lee, Junyuan Zeng, Yuanfeng Wen, Zhiqiang Lin, and Weidong Shi. In*Proceedings of the 40th International Symposium on Computer Architecture*, Tel-Aviv, Israel. June 2013.
- "AUTOVAC: Towards Automatically Extracting System Resource Constraints and Generating Vaccines for Malware Immunization". Zhaoyan Xu, Jialong Zhang, Guofei Gu, and Zhiqiang Lin. In*Proceedings of the 33rd International Conference on Distributed Computing Systems*, Philadelphia, USA. July 2013.
- "Manipulating Semantic Values in Kernel Data Structures: Attack Assessments and Implications". Aravind Prakash, Eknath Venkataramani, Heng Yin, and Zhiqiang Lin. In*Proceedings of the 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN-PDS)*, Budapest, Hungary, June 2013
- "Exterior: Using a Dual-VM Based External Shell for Guest-OS Introspection, Configuration, and Recovery". Yangchun Fu, and Zhiqiang Lin. In *Proceedings of the 9th ACM SIG-*

PLAN/SIGOPS International Conference on Virtual Execution Environments, Houston, TX, March 2013

- "Securing Untrusted Code via Compiler-Agnostic Binary Rewriting". Richard Wartel, Vishwath Mohan, Kevin Hamlen, and Zhiqiang Lin. In *Proceedings of the 28th Annual Computer Security Applications Conference*, Orlando, FL, December 2012.
- "OS-Sommelier: Memory-Only Operating System Fingerprinting in the Cloud". Yufei Gu, Yangchun Fu, Aravind Prakash, Zhiqiang Lin, and Heng Yin. In *Proceedings of the 3rd ACM Symposium on Cloud Computing*, San Jose, CA, October 2012.
- "Binary Stirring: Self-randomizing Instruction Addresses of Legacy x86 Binary Code". Richard Wartel, Vishwath Mohan, Kevin Hamlen, and Zhiqiang Lin. In *Proceedings of the 19th ACM Conference on Computer and Communications Security*, Raleigh, NC, October 2012.
- "Bin-Carver: Automatic Recovery of Binary Executable Files". Scott Hand, Zhiqiang Lin, Guofei Gu, and Bhavani Thuraisingham. In *Proceedings of the 12th Annual Digital Forensics Research Conference*, Washington DC, August 2012
- "Space Traveling across VM: Automatically Bridging the Semantic Gap in Virtual Machine Introspection via Online Kernel Data Redirection". Yangchun Fu, and Zhiqiang Lin. In *Proceedings of the 33rd IEEE Symposium on Security and Privacy*, San Fransisco, CA, May 2012
- "DIMSUM: Discovering Semantic Data of Interest from Un-mappable Memory with Confidence". Zhiqiang Lin, Junghwan Rhee, Chao Wu, Xiangyu Zhang, and Dongyan Xu. In *Proceedings of the 19th ISOC Network and Distributed System Security Symposium*, San Diego, CA, February 2012

(c) Research Grants (2011-Present, 5 years)

- **"**Safe, and Reuse-oriented Reverse Engineering of Functional Components from x86 Binaries". (PI Zhiqiang Lin). $475,000, DARPA (subcontracted from Purdue University). 12/01/2011-11/30/2014

- Semantic Approach to Behavior-Based IDS and Its Applications. $965,757. (PI Bhavani Thuraisingham, Co-PI Kevin Hamlen, Latifur Lkhan, and Zhiqiang Lin) Binghamton University (Original Source: AFOSR) 04/012012-03/31/2015

- "Vulcan: Automatically Generating Tools for Virtual Machine Inspection from Legacy Binary Code". (PI Zhiqiang Lin). $68K. 10/1/2012-9/30/2013

(d) Subject matter experts for Professional Societies (2011-Present, 5 years)

Awards
AFOSR YIP (Young Investigator Award) 2014

Program co-Chair

IEEE International Performance Computing and Communications Conference 2013

The Next Generation Malware Attacks and Defense Workshop (NGMAD), 2013

Publication Chair

IEEE International Performance Computing and Communications Conference 2012

Program Committee Member

IEEE International Conference on Distributed Computing Systems 2014
IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing 2014
ACM Symposium on Information, Computer and Communications Security 2013
IEEE International Conference on Big Data 2013
The third International Symposium on Secure Virtual Infrastructures 2013
The 9th China International Conference on Information Security and Cryptology 2013
IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing 2013
International Conference on Privacy, Security and Trust 2013
International Workshop on Security in Embedded Systems and Smartphones 2013
Annual Digital Forensics Research Conference 2013
IEEE Services Workshop on Security and Privacy Engineering 2013
Workshop on Hardware and Architectural Support for Security and Privacy 2013
International Conference on Availability, Reliability and Security 2012
IEEE Services Workshop on Security and Privacy Engineering 2012
Workshop on Hardware and Architectural Support for Security and Privacy 2012
IEEE International Performance Computing and Communications Conference 2012

(e) Student Cyber Security Programs (2011 – Present, 5 years)

Teaches courses in malware analysis and is extremely active with the Cyber Security students in conducting lab exercises.

Dr. Yvo Desmedt

(a) Publications (2011-Present, 5 years)

- Shah Mahmood, Yvo Desmedt: Two new economic models for privacy. SIGMETRICS Performance Evaluation Review 40(4): 84-89 (2013)
- Manal Adham, Amir Azodi, Yvo Desmedt, Ioannis Karaolis: How to Attack Two-Factor Authentication Internet Banking. Financial Cryptography 2013: 322-328
- 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)
- Yvo Desmedt: A Brief Survey of Research Jointly with Jean-Jacques Quisquater. Cryptography and Security 2012: 8-12
- Yvo Desmedt, Pyrros Chaidos: Applying Divertibility to Blind Ballot Copying in the Helios Internet Voting System. ESORICS 2012: 433-450
- Shah Mahmood, Yvo Desmedt: Your Facebook deactivated friend or a cloaked spy. PerCom Workshops 2012: 367-373
- Shah Mahmood, Yvo Desmedt: Online Social Networks, a Criminals Multipurpose Toolbox (Poster Abstract). RAID 2012: 374-375
- Yvo Desmedt, Josef Pieprzyk, Ron Steinfeld: Active Security in Multiparty Computation over Black-Box Groups. SCN 2012: 503-521

- Stelios Erotokritou, Yvo Desmedt: Human Perfectly Secure Message Transmission Protocols and Their Applications. SCN 2012: 540-558
- Shah Mahmood, Yvo Desmedt: Usable Privacy by Visual and Interactive Control of Information Flow. Security Protocols Workshop 2012: 181-188
- Shah Mahmood, Yvo Desmedt: Your Facebook Deactivated Friend or a Cloaked Spy (Extended Abstract). CoRR abs/1203.4043 (2012)
- Yongge Wang, Yvo Desmedt: Edge-Colored Graphs with Applications To Homogeneous Faults. CoRR abs/1207.5439 (2012)
- Yongge Wang, Yvo Desmedt: Edge-colored graphs with applications to homogeneous faults. Inf. Process. Lett. 111(13): 634-641 (2011)
- Qiushi Yang, Yvo Desmedt: Secure Communication in Multicast Graphs. ASIACRYPT 2011: 538-555
- Shah Mahmood, Yvo Desmedt: Poster: preliminary analysis of Google+'s privacy. ACM Conference on Computer and Communications Security 2011: 809-812
- Yongge Wang, Yvo Desmedt: Homogeneous Faults, Colored Edge Graphs, and Cover Free Families. ICITS 2011: 58-72
- Yvo Desmedt: Access Structure. Encyclopedia of Cryptography and Security (2nd Ed.) 2011: 20
- Yvo Desmedt, Goce Jakimoski: Broadcast Authentication from an Information Theoretic Perspective. Encyclopedia of Cryptography and Security (2nd Ed.) 2011: 170-171
- Yvo Desmedt: Covert Channels. Encyclopedia of Cryptography and Security (2nd Ed.) 2011: 265-266
- Yvo Desmedt: Deniable Encryption. Encyclopedia of Cryptography and Security (2nd Ed.) 2011: 322-323
- Yvo Desmedt: ElGamal Public Key Encryption. Encyclopedia of Cryptography and Security (2nd Ed.) 2011: 396
- Yvo Desmedt: Fiat-Shamir Identification Protocol and the Feige-Fiat-Shamir Signature Scheme. Encyclopedia of Cryptography and Security (2nd Ed.) 2011: 457-458
- Yvo Desmedt: Knapsack Cryptographic Schemes. Encyclopedia of Cryptography and Security (2nd Ed.) 2011: 695-704
- Yvo Desmedt: Man-in-the-Middle Attack. Encyclopedia of Cryptography and Security (2nd Ed.) 2011: 759
- Yvo Desmedt, Qiushi Yang: Perfectly Secure Message Transmission. Encyclopedia of Cryptography and Security (2nd Ed.) 2011: 922-924
- Yvo Desmedt: Relay Attack. Encyclopedia of Cryptography and Security (2nd Ed.) 2011: 1042
- Yvo Desmedt: Station-to-Station Protocol. Encyclopedia of Cryptography and Security (2nd Ed.) 2011: 1256
- Yvo Desmedt, Goce Jakimoski: Stream and Multicast Authentication. Encyclopedia of Cryptography and Security (2nd Ed.) 2011: 1260-1263
- Yvo Desmedt: Threshold Cryptography. Encyclopedia of Cryptography and Security (2nd Ed.) 2011: 1288-1293
- Yvo Desmedt: Trojan Horses, Computer Viruses, and Worms. Encyclopedia of Cryptography and Security (2nd Ed.) 2011: 1319-1320
- Shah Mahmood, Yvo Desmedt: Preliminary Analysis of Google+'s Privacy. CoRR abs/1111.3530 (2011)
- Qiushi Yang, Yvo Desmedt: Efficient 2-Round General Perfectly Secure Message Transmission: A Minor Correction to Yang and Desmedt's Protocol. IACR Cryptology ePrint Archive 2011: 265 (2011)

(b) Book and book chapters (2009-Present, 5 years)

Y. Desmedt, editor. Information Theoretic Security, Second International Conference, ICITS 2007, (Lecture Notes in Computer Science 4883) , New York, 2009. Springer-Verlag.

(c) Research Grants (2011-Present, 5 years)

$500,000 STAR grant, State of Texas

(d) Subject matter experts for Professional Societies (2011-Present, 5 years)

Fellow of the prestigious International Association for Crypto logic Research (IACR)
Program Chair of the Information Security Conference (ISC)
Editor in Chief IET Information Security Journal
Editor of the Journal of Computer Security
Chair of the Steering Committee of:

- International Conference on Cryptology and Network Security
- International Conference on Information Theoretic Security

Member of the Steering Committee of the International Workshop on Practice and Theory in Public Key Cryptography (PKC)

(e) Student Cyber Security Programs (2011 – Present, 5 years)

Prof. Desmedt joined UTD in August 2012. He teaches courses in cryptography and is involved in student Cyber Security programs.

(f) Presentations (2011-Present, 5 years)

- Workshop "Secret Sharing and Cloud Computing," Institute of Mathematics for Industry, Kyushu University, Japan: Secure Multiparty Computation to Protect Cloud Computing (June 2011)
- The 8th IEEE/FTRA International Conference on Secure and Trust Computing, Data Management, and Applications," Loutraki, Greece, 30 Years Computer
- Hacking: Can we achieve Secure and Trusted Computing (June 2011)
- International Workshop on Network Topologies," Brussels, Belgium:
- A Survey of Generalized Connectivity and its Applications in Security (July 2011)
- Seventh International ICST Conference on Security and Privacy in Communication Networks (SecureComm 2011)," London, UK: Why Security Engineering Fails (Sept. 2011)
- Public-Key Cryptography, Dagstuhl, Germany: Active Security in General Secure Multi-Party Computation via Black-Box Groups (Sept. 2011)
- Symposium on Mathematical Theory in Cryptologic Research," Chinese Association for Cryptologic Research, Beijing, China: A Survey of Generalized Connectivity and its Applications in Security (Dec. 2011)

Invited performance: October 5, 2012, workshop on Cryptographic Technologies suitable for Cloud Computing," Kyushu University, Fukuoka, Japan, Secure Multiparty Computation almost without Verifiable Secret Sharing

Invited performance: October 26-27, 2012, Workshop - Online Security and Civil Rights: A Fine Ethical Balance On the Key Role Intelligence Agencies can play to Restore our Democratic Institutions

Invited performance: December 6-7, 2012, Beijing, China, Keynote lecture at the workshop on the International View of Cryptography and Security and Their Use in Practice: Focus on Mobile and Embedded Computing, Deployment issues related to cryptography in cloud computing and social networks"

At seminar series (e.g., Universities):

- Invited colloquia presentation: April 27, 2012, CISE, University of Florida, Gainesville, Protecting against Insider Threats
- Invited colloquia presentations: May 10, 2012, Department of Computer Science, University of Calgary: Active Security in General Secure Multi-Party Computation via Black-Box Groups Why Security Engineering Fails
- Invited colloquia presentation: September 21, 2012, University of North-Carolina Charlotte, Secure Multiparty Computation for Cloud Security
- Invited colloquia presentation: October 12, 2012, Nippon Telegraph and Telephone Corp., Musashino Research and Development Center, Japan, Secure Multiparty Computation: an alternative approach
- Invited colloquia presentations: October 15, 2012, National Institute of Information and Communications Technology, Koganei (Tokyo): Secure Multiparty Computation for Cloud Security, New Models for Privacy and Privacy in Social Networks, Two Problems with the Internet Helios System
- Invited colloquia presentation: December 18, 2012, Department of Electrical Engineering, Universite Catholique de Louvain, Belgium, New Models for Privacy and Privacy in Social Networks
- Invited performance: April 4, 2013, panel member of the panel \Panel Member: Security of Online Banking" at Financial Cryptography, Okinawa, Japan.
- Invited performance: May 22, 2013, invited participant at the Mathematics of Information- Theoretic Cryptography Workshop, May 21-25, 2013, Leiden, the Netherlands, with lecture: Functional Secret Sharing.
- Invited performance: May 31, 2013, invited speaker at the International State of the Art Cryptography Workshop, May 30-31, 2013, Athens, Greece, The bumpy road to deployment: mislabeling practical and theoretical research.
- Invited performance: June 18, 2013, invited speaker at Defence IT, June 18-19, 2013, Brussels, Belgium, Private and Secure Communication with an Adversarial Insider.
- Invited performance: September 3, 2013, invited speaker at the workshop Variety of Algebraic,Nonlinear and Dynamical Equations With Applications in Learning, Life Sciences and Esecurity
- September 3-4, 2013, Leuven, Belgium, From Public Key Infrastructures to Secure Multiparty Computation
- Invited performance: September 5, 2013, keynote speaker at Secure Digital Ecosystems conference, September 5-6, 2013, Leuven, Belgium, An academic vision on cyber security in the future: Self evolving defenses against self evolving malware.

At seminar series (e.g., Universities):

- Invited colloquia presentation: April 8, 2013, Nippon Telegraph and Telephone Corp., Musashino Research and Development Center, Japan, Divertible Proofs and Weaknesses of Internet Voting
- Invited colloquia presentation: April 19, 2013 Lecture for IEEE Dallas, What is the Future of Cryptography?
- Invited colloquia presentation: June 21 Department of Electrical Engineering, Universite Catholique de Louvain, Belgium, Functional Secret Sharing.
- Invited colloquia presentation: June 10, 2013, Kyushu University, Fukuoka, Japan, Functional Secret Sharing.
- Invited colloquia presentation: June 21, 2013, Department of Electrical Engineering, Universite Catholique de Louvain, Belgium, Functional Secret Sharing.
- Invited colloquia presentation: August 7, 2013 Department of Computer Science, University of Calgary, Canada, Functional Secret Sharing

- Invited colloquia presentation: August 9, 2013 Department of Computer Science, University of Calgary, Canada, Human Perfectly Secure Message Transmission Protocols and their Applications
- Invited colloquia presentation: August 13, 2013 Department of Computer Science, Stanford University, Functional Secret Sharing
- Invited colloquia presentation: September 13, Microsoft Research, Cambridge, UK, Is The Rise of Cloud Storage, Cloud Computing and Social Networks a Consequence of a Failed OS (Operating System) Design?
- Invited colloquia presentation: November 27, 2013, Nanyang Technological University, School of Physical & Mathematical Sciences, Singapore, Perfectly Secure Message Transmission using Covering Designs

Dr. Yiorgos Makris

(a) Publications (2011-Present, 5 years)

Journal Papers

- N. Karimi, M. Maniatakos, C. Tirumurti, **Y. Makris**, "On the Impact of Performance Faults in Modern Microprocessors," *Journal of Electronic Testing: Theory & Applications (JETTA), Springer,* vol. 29, no. 3, pp. 351-366, 2013 (pdf)
- M. Maniatakos, P. Kudva, B. Fleischer, **Y. Makris**, "Low-cost Concurrent Error Detection for Floating Point Unit (FPU) Controllers," *IEEE Transactions on Computers (TCOMP),* vol. 62, no. 7, pp. 1376-1388, 2013 (pdf)
- M. Maniatakos, C. Tirumurti, **Y. Makris**, "Global Signal Vulnerability (GSV) Analysis for Selective State Element Hardening on Modern Microprocessors," *IEEE Transactions on Computers (TCOMP),* vol. 61, no. 9, pp. 1361-1370, 2012 (pdf)
- N. Kupp, **Y. Makris**, "Applying the Model-View-Controller Paradigm to Adaptive Test," *Special Issue on Yield Learning of the IEEE Design and Test of Computers (D&T),* vol. 29, no. 1, pp. 28-35, 2012 (pdf)
- E. Love, Y. Jin, **Y. Makris**, "Proof-Carrying Hardware Intellectual Property: A Pathway to Trusted Module Acquisition," *Special Issue on Integrated Circuits and System Security of the IEEE Transactions on Information Forensics and Security (TIFS),* vol. 7, no. 1, pp. 25-40, 2012 (pdf)
- N. Kupp, H. Huang, P. Drineas, **Y. Makris**, "Improving Analog and RF Device Yield through Performance Calibration," *IEEE Design and Test of Computers (D&T),* vol. 28, no.3, pp. 64-75, 2011 (pdf)
- N. Karimi, M. Maniatakos, C. Tirumurti, A. Jas, **Y. Makris**, "A Workload-Cognizant Concurrent Error Detection Method for a Modern Microprocessor Controller," *Special issue of IEEE Transactions on Computers (TCOMP) on Concurrent On-Line Testing and Error/Fault Resilience of Digital Systems,* vol. 60, no. 9, pp. 1174-1187, 2011 (pdf)
- M. Maniatakos, N. Karimi, C. Tirumurti, A. Jas, **Y. Makris**, "Instruction-Level Impact Analysis of Low-Level Errors in a Modern Microprocessor Controller," *Special issue of IEEE Transactions on Computers (TCOMP) on Concurrent On-Line Testing and Error/Fault Resilience of Digital Systems,* vol. 60, no. 9, pp. 1160-1173, 2011 (pdf)

Conference Papers

- Y. Liu, Y. Jin, **Y. Makris**, "Hardware Trojans in Wireless Cryptographic ICs: Silicon Demonstration & Detection Method Evaluation," *Proceedings of the ACM/IEEE Design Automation Conference (ICCAD)*, 2013 (to appear) (pdf)

- K. Huang, N. Kupp, J. Carulli, **Y. Makris**, "Process Monitoring through Wafer-level Spatial Variation Decomposition," *Proceedings of the IEEE International Test Conference (ITC)*, S5.3.1-S5.3.10, 2013 (pdf)
- K. Huang, J. Carulli, **Y. Makris**, "Counterfeit Electronics: A Rising Threat in the Semiconductor Manufacturing Industry," *Proceedings of the IEEE International Test Conference (ITC)*, L3.4.1-L3.4.4, 2013 (pdf)
- Y. Jin, D. Maliuk, **Y. Makris**, "A Post-Deployment IC Trust Evaluation Architecture," *Proceedings of the IEEE On-Line Test Symposium (IOLTS)*, pp. 224-225, 2013 (pdf)
- M. Maniatakos, M. Michael, **Y. Makris**, "Challenges and Benefits of Multiple Bit Upset (MBU) Vulnerability Analysis in Modern Microprocessors," *Proceedings of the IEEE On-Line Test Symposium (IOLTS)*, pp. 49-54, 2013 (pdf)
- Y. Jin, B. Yang, **Y. Makris**, "Cycle Accurate Information Assurance by Proof Carrying-Based Signal Sensitivity Tracing," *Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 99-106, 2013 (pdf)
- O. Sinanoglu, N. Karimi, J. Rajendran, R. Karri, Y. Jin, K. Huang, **Y. Makris**, "Reconciling the IC Test and Security Dichotomy," *Proceedings of the IEEE European Test Symposium (ETS)*, pp. 176-181, 2013 (pdf)
- K. Huang, N. Kupp, J. Carulli, **Y. Makris**, "On Combining Alternate Test with Spatial Correlation Modeling in Analog/RF ICs," *Proceedings of the IEEE European Test Symposium (ETS)*, pp. 64-69, 2013 (pdf)
- K. Huang, N. Kupp, J. Carulli, **Y. Makris**, "Handling Discontinuous Effects in Modeling Spatial Correlation of Wafer-level Analog/RF Tests," *Proceedings of the IEEE Design Automation and Test in Europe Conference (DATE)*, pp. 553-558, 2013 **(Best Paper Award)** (pdf)
- M. Maniatakos, M. Michael, **Y. Makris**, "AVF-driven Parity Optimization for MBU Protection of In-core Memory Arrays," *Proceedings of the IEEE Design Automation and Test in Europe Conference (DATE)*, pp. 1480-1485, 2013 (pdf)
- N. Kupp, **Y. Makris**, "Integrated Optimization of Semiconductor Manufacturing: A Machine Learning Approach," *Proceedings of the IEEE International Test Conference (ITC)*, pp. PTF.1.1-PTF.1.10, 2012 (pdf)
- N. Kupp, K. Huang, J. Carulli, **Y. Makris**, "Spatial Estimation of Wafer Measurement Parameters Using Gaussian Process Models," *Proceedings of the IEEE International Test Conference (ITC)*, pp. 5.1.1-5.1.8, 2012 (pdf)
- M. Maniatakos, M. Michael, **Y. Makris**, "Vulnerability-Based Interleaving for Multi-Bit Upset (MBU) Protection in Modern Microprocessors," *Proceedings of the IEEE International Test Conference (ITC)*, pp. 19.2.1-19.2.8, 2012 (pdf)
- N. Kupp, K. Huang, J. Carulli, **Y. Makris**, "Spatial Correlation Modeling For Probe Test Cost Reduction in RF Devices," *Proceedings of the IEEE International Conference on Computer-Aided Design (ICCAD)*, pp. 23-29, 2012 (pdf)
- K. Huang, J. Carulli, **Y. Makris**, "Parametric Counterfeit IC Detection via Support Vector Machines," *Proceedings of the IEEE Defect and Fault Tolerance Symposium (DFTS)*, pp. 7-12, 2012 (pdf)
- Y. Jin, M. Maniatakos, **Y. Makris**, "Exposing Vulnerabilities of Untrusted Computing Platforms," *Proceedings of the IEEE International Conference on Computer Design (ICCD)*, pp. 131-134, 2012 (pdf)
- D. Maliuk, **Y. Makris**, "A Reconfigurable Dual-Mode Weight Storage Analog Neural Network Experimentation Platform," *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 2889-2892, 2012 (pdf)
- Y. Jin, **Y. Makris**, "Proof Carrying-Based Information Flow Tracking for Data Secrecy Protection and Hardware Trust," *Proceedings of the IEEE VLSI Test Symposium (VTS)*, pp. 252-257, 2012 (pdf)

- D. Maliuk, N. Kupp, **Y. Makris**, "Towards a Fully Stand-Alone Analog/RF BIST: A Cost-Effective Implementation of a Neural Classifier," Proceedings of the IEEE VLSI Test Symposium (VTS), pp. 62-67, 2012 (pdf)
- Y. Jin, D. Maliuk, **Y. Makris**, "Post-Deployment Trust Evaluation in Wireless Cryptographic ICs," *Proceedings of the IEEE Design Automation and Test in Europe Conference (DATE)*, pp. 965-970, 2012 (pdf)
- Y. Jin, **Y. Makris**, "PSCML: Pseudo-Static Current Mode Logic," *Proceedings of the IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, pp. 41-44, 2011 (pdf)

- N. Kupp, H.-G. Stratigopoulos, P. Drineas, **Y. Makris**, "On Proving the Performance of Alternative RF Tests," *Proceedings of the IEEE International Conference on Computer-Aided Design (ICCAD)*, pp.762-767, 2011 (pdf)
- Y. Jin, **Y. Makris**, "Is Single-Scheme Trojan Prevention Sufficient?," *Proceedings of the IEEE International Conference on Computer Design (ICCD)*, pp. 305-308, 2011 (pdf)
- N. Kupp, H. Stratigopoulos, P. Drineas, **Y. Makris**, "Feature Selection Methods For Analog and RF Test: A Case Study" *Proceedings of the SRC Technology and Talent for the 21st Century Conference (TECHCON)*, 2011 **(Best-in-Session Award)** (pdf)
- E. Love, Y. Jin, **Y. Makris**, "Enhancing Security via Provably Trustworthy Hardware Intellectual Property," *Proceedings of the IEEE Symposium on Hardware-Oriented Security and Trust (HOST)*, pp. 12-17, 2011 (pdf)
- M. Maniatakos, C. Tirumurti, A. Jas, **Y. Makris**, "AVF Analysis Acceleration via Hierarchical SFI," *Proceedings of the IEEE European Test Symposium (ETS)*, pp. 87-92, 2011 (pdf)
- N. Kupp, H. Stratigopoulos, P. Drineas, **Y. Makris**, "PPM-Accuracy Error Estimates for Low-Cost Analog Test: A Case Study," *Proceedings of the IEEE International Mixed Signals, Sensors, and Systems Workshop (IMS3TW)*, 2011 **(Best Student Paper Award)** (pdf)
- M. Maniatakos, P. Kudva, B. Fleischer, **Y. Makris**, "Exponent Monitoring for Low-Cost Concurrent Error Detection in FPU Control Logic," *Proceedings of the IEEE VLSI Test Symposium (VTS)*, pp. 235-240, 2011 (pdf)
- N. Kupp, M. Slamani, **Y. Makris**, "Correlating Inline Data with Final Test Outcomes in Analog/RF Devices," *Proceedings of the IEEE Design Automation and Test in Europe Conference (DATE)*, pp. 812-817, 2011 (pdf)

(b) Book and book chapters (2009-Present, 5 years)

- (Editor), "Advanced Circuits for Emerging Technologies," John Wiley & Sons, 2012 (H. Stratigopoulos,**Y. Makris**, "Checkers for On-line Self-Testing of Analog Circuits," (invited)) (link)
- M. Tehranipoor, C. Wang (Editors), *Introduction to Hardware Security and Trust*, Springer, 2011 (Y. Jin, E. Love, **Y. Makris** , "Design for Hardware Trust," (invited)) (link)
- L. T. Wang, C. E. Stroud, and N. A. Touba (Editors), *System on-Chip Test Architectures*, Morgan-Kaufman Publishers, 2007 (**Y. Makris**, section 8.4,"Circuit-Level Approaches to Soft Error Mitigation," (invited)) (link)

(c) Research Grants (2011-Present, 5 years)

Source	Title	Period	PI(s)	Amount
Intel Corp.	Gift to Support Research in Information-Rich Sample Selection	11/01/13-10/31/14	Y. Makris	$30K

NSF 1311860 NSF 1319105	TWC: Small: Collaborative: Toward Trusted 3rd-Party Microprocessor Cores: A Proof Carrying Code Approach	10/01/13-09/30/16	Y. Jin Y. Makris	$460K
SRC / TxACE 1836.131	Process Variation Anatomy: A Statistical Nexus between Design, Manufacturing, and Yield	08/01/13-07/31/16	Y. Makris	$330K
NSF 1255754 SRC 2413.001	Cross-Layer Intelligent System-Based Adaptive Power Conditioning for Robust and Reliable Mixed-Signal Multi-Core SoCs	04/01/13-03/31/16	Y. Makris D. Ma	$320K
ARO CS 60709	Trusted Module Acquisition Through Proof-Carrying Hardware IP	02/01/12-01/31/15	Y. Makris	$330K
NSF 1017719 NSF 1149465	THWART: Trojan Hardware in Wireless ICs: Analysis and Remedies for Trust	09/01/10-08/31/14	Y. Makris	$500K

(d) Subject matter experts for Professional Societies (2011-Present, 5 years)

Program Chair:

IEEE VLSI Test Symposium (VTS'13 - '14)

Technical Program Committee Member:

IEEE International Test Conference (ITC'11 - '13)
IEEE/ACM Design Automation Conference (DAC'12 - '13)
TxACE Symposium (TxACE '12)
ACM/IEEE Interaction Conference on Computer-Aided Design (ICCAD '09 -'11)
IEEE VLSI Test Symposium (VTS'08 -'13)
IEEE Design Automation and Test in Europe (DATE'07 -'11, '13 - '14)
IEEE Symposium on Defect and Fault Tolerance in VLSI Systems (DFTS'08 -'10, '12 - '13)
IEEE On-Line Testing Symposium (IOLTS'05 -'13)
IEEE European Test Symposium (ETS'04 -'14)
IEEE International Symposium on Hardware Oriented Security and Trust (HOST'08 - '13)
IEEE International Workshop on Test/Validation of High-Speed Analog Circuits (TVHSAC'13)
Workshop on Cryptographic Hardware and Embedded Systems (CHES'12)
IEEE International Mixed-Signals, Sensors, and Systems Test Workshop (IMS3TW'11 - '13)
IEEE Microprocessor Test and Verification Workshop (MTV'10 - '12)
IEEE International Workshop on Reliability Aware System Design and Test (RASDAT'10 - 12)

(e) Student Cyber Security Programs (2011 – Present, 5 years)

Prof. Makris teaches courses in hardware security and is involved in student Cyber Security programs.

(f) Presentations (2011-Present, 5 years)

Too High Frequency to Test - What is the Quality Impact?
Panelist, IEEE Test and Validation of High-Speed Analog Circuits Workshop, Anaheim, CA, Sep '13 (Host: S. Sunter)
Parametric Counterfeit IC Detection via Support Vector Machines
NYU-Abu Dhabi "Do you Trust Your Chip?" Workshop, New York, NY, Apr '13 (Host: M. Maniatakos)
Spatial Wafer-Level Correlation Modeling for Test Cost Reduction in Analog/RF Circuits
Freescale Semiconductor, Austin, TX, April '13 (Host: R. Raina)
Intel Corp, Santa Clara, CA, March '13 (Host: S. Natarajan)
Invited Talk, IEEE Workshop on Defect and Adaptive Test Analysis, Anaheim, CA, Nov '12 (Host: A. Sinha)
TxACE Weekly Meeting, University of Texas at Dallas, Richardson, TX, Nov '12 (Host: K. O)
Hardware Security and Trust
Tutorial, IEEE Design Automation and Test in Europe (DATE) Conference, Grenoble, France, Mar '13 (Host: F. Fummi)
Texas Security Awareness Week (TexSAW), Richardson, TX, Oct '12 (Host: J. Shapiro)
Tutorial, IEEE International Conference on Computer Design (ICCD), Montreal, Canada, Sep '12 (Host: S. Tahar)
A Model-View-Controller (MVC) Framework for Adaptive Test
TxACE E-Seminar, University of Texas at Dallas, Richardson, TX, Nov '11 (Host: K. O)
On-Chip Neural Classifiers for Post-Deployment Trust Monitoring in Wireless Cryptographic ICs
Elevator Talks at the International Test Conference, Anaheim, CA, Sep '11 (Host: S. Mitra)
Post-Production Performance Calibration in Analog/RF ICs
TxACE Weekly Meeting, University of Texas at Dallas, Richardson, TX, Sep '11 (Host: K. O)
Post-Deployment Trust Monitoring in Wireless Cryptographic ICs
NYU-Abu Dhabi "Do you Trust Your Chip?" Workshop, New York, NY, Apr '11 (Host: O. Sinanoglu)
Proof-Carrying Hardware Intellectual Property: A Pathway to Trusted Module Acquisition
ARO Workshop on Trusted Hardware, Arlington, VA, Apr '11 (Hosts: C. Wang & M. Tehranipoor)
Trusted Integrated Circuits: Challenges & Opportunities Ahead
University of Belgrade, Belgrade, Serbia, Mar '13 (Host: I. Tartalja)
Technical University of Crete, Chania, Greece, Mar '13 (Host: A. Dollas)
National Technical University of Athens, Athens, Greece, Mar '13 (Host: Y. Papananos)
University of Athens, Athens, Greece, Mar '13 (Host: D. Gizopoulos)
University of Texas, Dallas, TX, Mar '11 (Host: N. Al-Dhahir)
A Machine Learning Approach to Robust Analog/RF Integrated Circuits
Brown University, Providence, RI, Mar '11 (Host: I. Bahar)
University of New Mexico, Albuquerque, NM, Mar '11 (Host: P. Zarkesh-Ha)

Dr. Alvaro Cardenas

(a) Publications (2011-Present, 5 years)

https://www.perform.csl.illinois.edu/Papers/USAN_papers/13BER01.pdf
R Berthier, JG Jetcheva, D Mashima, JH Huh, D Grochocki, RB Bobba, AA ...
Smart Grid Communications (SmartGridComm), 2013 IEEE International Conference

http://www.utdallas.edu/~alvaro.cardenas/papers/CIP2013.pdf
R Chow, A Cardenas, E De Cristofaro
Critical Infrastructure Protection VII, 21-32

Big Data Analytics for Security
AA Cardenas, PK Manadhata, SP Rajan
IEEE Security & Privacy 11 (6), 0074-76

Controllability of Dynamical Systems: Threat Models and Reactive Security
C Barreto, AA Cárdenas, N Quijano
Decision and Game Theory for Security, 45-64

Resilience of Process Control Systems to Cyber-Physical Attacks
M Krotofil, AA Cárdenas
Secure IT Systems, 166-182

A game theory model for electricity theft detection and privacy-aware control in AMI systems
AA Cárdenas, S Amin, G Schwartz, R Dong, S Sastry
Communication, Control, and Computing (Allerton), 2012 50th Annual Allerton Conference

Depth-First Forwarding (DFF) in Unreliable Networks
U Herberg, A Cardenas, M Dow, T Iwao, S Cespedes
IETF RFC 6971

(c) Research Grants (2011-Present, 5 years)

"Enabling Secure Control Architectures for Cyber Physical Systems (SCAPS)". Award by MITRE corporation. 2013. $40,000.

(d) Subject matter experts for Professional Societies (2011-Present, 5 years)

Panels

- Birds of a Feather on Security for the ACM 2014 Richard Tapia Conference on Broadening Participation in Computer Science.
- Cyber-Physical Systems Security: Tutorial at the 2013 ACSAC Security Conference.
- Invited talk to NIST Roadmapping Workshop: Measurement of Security Technology Performance Impacts for Industrial Control Systems. December 4-5, 2013.
- Panelist. Implications of Cloud Computing on the Security of Grid Systmes TCIPG Industry Workshop.
- Panelist. Security Analytics for Critical Infrastructure: Challenges and Research Directions SafeConfig 2013.
- Resilience of Process Control Systems to Cyber-Physical Attacks Plant Automation and Decision Support track of the 2013 American Fuel and Petrochemical Manufacturers (AFPM) Technology Forum. October 7-9, Dallas, TX.
- Big Data Analytics and Security Intelligence. NIST Cloud Security Working Group. April 10, 2013.

- Big Data Analytics in Smart Grid Applications. (pdf) Panel: Smart Grid and the Cloud. Fourth IEEE PES Innovative Smart Grid Technologies Conference (ISGT). February 26, 2013.
- Short and Long-Term Research Challenges for Protecting Critical Infrastructure Systems. (pdf) Symantec Research Seminar. December 18, 2012.
- Short and Long-Term Research Challenges for Protecting Critical Infrastructure Systems. (pdf) Plenary talk Schedule SchlossDagstuhl Seminar 12502. Securing Critical Infrastructures from Targeted Attacks. Marc Dacier, Frank Kargl, Alfonso Valdes (organizers). December 9-12, 2012.

Conference Committees

- IEEE Symposium on Security and Privacy 2014 IEEE S&P 2014. http://www.ieee-security.org/TC/SP-Index.html
- 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2014)
- 12th International Conference on Privacy, Security and Trust PST 2014 http://pst2014.ryerson.ca
- Financial Cryptography FC 2014. http://fc14.ifca.ai
- Third Conference on High Confidence Networked Systems HiCoNS 2014. http://www.hi-cons.org
- 4th Conference on Decision and Game Theory for Security GameSec 2013 http://www.gamesec-conf.org
- 6th Workshop on Artificial Intelligence and Security AISec 2013 https://sites.google.com/site/ccsaisec2013/
- 20th ACM Computer and Communications Security CCS 2013 http://www.sigsac.org/ccs/CCS2013/index.html
- 11th International Conference on Applied Cryptography and Network Security ACNS 2013. http://acns2013.cpsc.ucalgary.ca
- 23rd International Joint Conference on Artificial Intelligence IJCAI 2013. http://ijcai13.org
- 11th International Conference on Privacy, Security and Trust PST 2013 http://unescoprivacychair.urv.cat/pst2013/index.php?m=security
- Second Conference on High Confidence Networked Systems HiCoNS 2013. http://www.hi-cons.org/

(e) Student Cyber Security Programs (2011 – Present, 5 years)

Prof. Cardenas joined UTD in January 2013. He teaches courses in critical infrastructure protection and and is involved in student Cyber Security programs.

(f) Presentations

Prof. Cardenas has been at UTD since January 2013. As listed above, he has participated in numerous panel presentations

Dr. Zygmunt Haas

Dr. Haas joined UTD from Cornell University in August 2013. While at Cornell he carried out extensive research in wireless network security. We have listed mainly his contributions made while at UTD.

(a) Book Chapter

- Zygmunt J. Haas, Lin Yang, Meng-Ling Liu, Qiao Li, and Fangxin Li, “Current Challenges and Approaches in Securing Communications for Sensors and Actuators,” Chapter 17 in the “Art of Wireless Sensor Networks,” H.M. Ammari, ed., Springer-Verlag Berlin Heidelberg, 2014, DOI: 10.1007/978-3-642-40009-7_17

(f) Presentations (2011-Present, 5 years)

- Z.J. Haas, “Big Data and Its Security Implications” presented at: (1) National Taiwan University (NTU), Taipei, Taiwan, December 16, 2013; (2) National Sun Yat-sen University, Kaohsiung, Taiwan, December 18, 2013; (3) National Tsing Hua University, Hsinchu, Taiwan, December 19, 2013
- Z.J. Haas, “Big Data and Security Implications" Keynote Speech, *EUSPN’13, 4th International Conference on Emerging Ubiquitous Systems and Pervasive Networks*, Niagara Falls, Ontario, Canada, October 21-24, 2013
- Z.J. Haas, “Security of Big Data" at the Cornell Engineering Alumni Association conference, Washington, DC, May 13, 2013
- Z.J. Haas, “Stochastic Routing,” DIMACS Workshop on Connectivity and Resilience for Large-Scale Networks, Rutgers University, Piscataway, NJ, April 12-13, 2012
- Z.J. Haas, “*Information Assurance for Sensor Networks,*” Winter 2012 CIS Distinguished Lecture Series, Computer and Information Science Department, College of Engineering and Computer Science. University of Michigan-Dearborn, March 16, 2012
- Z.J. Haas, “*Information Assurance for Sensor Networks,*” Invited Talk, Department of Electrical Engineering and Computer Science, UC Berkeley, Berkeley, CA, September 7, 2011
- Z.J. Haas, “*Information Assurance for Vehicular Sensor-based Networks,*” Closing Keynote, 4th *IEEE International Symposium on Wireless Vehicular Communications (WiVeC’11)*, San Francisco, CA, September 6, 2011
- Z.J. Haas, “*Information Assurance for Sensor Networks,*” Invited Talk, Department of Electrical Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan, August 15, 2011
- Z.J. Haas, “*New Directions and Challenges in Information Assurance with Applications for Sensor Networks,*” Invited Talk, Department of Electrical Engineering, NCTU, Hsinchu, Taiwan, August 12, 2011
- Z.J. Haas, “*New Directions and Challenges in Information Assurance with Application to Sensor Networks,*” Invited Talk, Department of Electrical Engineering, Boston University, July 14, 2011
- Z.J. Haas, “*Information Assurance and Sensor Network Security,*” Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL, April 14, 2011
- Z.J. Haas, “*Information Assurance and Sensor Network Security,*” Computer and Information Sciences department, Temple University, Philadelphia, PA, March 31, 2011
- Z.J. Haas, “*Information Assurance for Sensor Networks,*” Keynote Speech, *IEEE PerCom 2011 (Information Quality and Quality of Service (IQ2S) Workshop*), Seattle, WA, March 21, 2011

Dr. Latifur Khan

(a) Publications

JOURNALS

- Jeffrey Partyka, Pallabi Parveen, Latifur Khan, Bhavani M. Thuraisingham, Shashi Shekhar: Enhanced geographically typed semantic schema matching. J. Web Sem. 9(1): 52-70 (2011)

- Mohammad M. Masud, Tahseen Al-Khateeb, Kevin W. Hamlen, Jing Gao, Latifur Khan, Jiawei Han, Bhavani M. Thuraisingham: Cloud-based malware detection for evolving data streams. ACM Trans. Management Inf. Syst. 2(3): 16 (2011)
- 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): 1484-1497 (2013)

- Mohammad M. Masud, Clay Woolam, Jing Gao, Latifur Khan, Jiawei Han, Kevin W. Hamlen, Nikunj C. Oza: Facing the reality of data stream classification: coping with scarcity of labeled data. Knowl. Inf. Syst. 33(1): 213-244 (2011)

- Mohammad M. Masud, Jing Gao, Latifur Khan, Jiawei Han, Bhavani M. Thuraisingham: Classification and Novel Class Detection in Concept-Drifting Data Streams under Time Constraints. IEEE Trans. Knowl. Data Eng. 23(6): 859-874 (2011)

- Mohammad Farhan Husain, James P. McGlothlin, Mohammad M. Masud, Latifur R. Khan, Bhavani M. Thuraisingham: Heuristics-Based Query Processing for Large RDF Graphs Using Cloud Computing. IEEE Trans. Knowl. Data Eng. 23(9): 1312-1327 (2011)

CONFERENCES

- Mohammad Farhan Husain, James P. McGlothlin, Latifur Khan, Bhavani M. Thuraisingham: Scalable Complex Query Processing over Large Semantic Web Data Using Cloud. IEEE CLOUD 2011: 187-194
- Tahseen Al-Khateeb, Mohammad M. Masud, Latifur Khan, Bhavani M. Thuraisingham: Cloud Guided Stream Classification Using Class-Based Ensemble. IEEE CLOUD 2012: 694-701

- Tahseen Al-Khateeb, Mohammad M. Masud, Latifur Khan, Charu C. Aggarwal, Jiawei Han, Bhavani M. Thuraisingham: Stream Classification with Recurring and Novel Class Detection Using Class-Based Ensemble. ICDM 2012: 31-40, 2011

- Justin Sahs, Latifur Khan: A Machine Learning Approach to Android Malware Detection. EISIC 2012: 141-147
- David Sounthiraraj, Justin Sahs, Zhiqiang Lin, Latifur Khan, and Garrett Greenwood. "SMV-Hunter: Large Scale, Automated Detection of SSL/TLS Man-in-the-Middle Vulnerabilities in Android Apps". To appear in *Proceedings of the 21st ISOC Network and Distributed System Security Symposium*, San Diego, CA, February 2014

(b) Books and Book Chapters (2009-Present, 5 years)

- Listed under Dr. Bhavani Thuraisingham's books

(c) Research Grants (2011-Present, 5 years)

"MRI: Development of an Instrument for Assured Cloud Computing"
Latifur Khan (PI) Murat Kantarcioglu (Co-PI) Kevin Hamlen (Co-PI)
NSF
10/01/2012-09/30/2015, $300,000

"Situational Awareness of Topic Drift and Birth-Death in Cyber,"
Latifur Khan
Department of Energy, 170K,
09/01/2012—08/30/2015

"ATD: Efficient online detection based on multiple sensors, with applications to cybersecurity and discovery of biological threats,"
Michael Baron (PI) Latifur Khan (Co-PI)
NSF
10/01/2013—09/30/2016 $392,502

(d) Subject matter experts for Professional Societies (2011-Present, 5 years)

Professional Memberships
ACM Distinguished Scientist (2012-Present)
IEEE Senior Member (2000-Present)

Awards

- IEEE Technical Achievement Award, IEEE Systems Man and Cybernetics Society and the IEEE Transportation Systems Society, 2012.

Editorial Boards

- **Associate Editor** of *IEEE Transactions on Knowledge & Data Engineering (TKDE),* IEEE Computer Society since June 2011.
- **Associate Editor** of *International Journal of Data Mining, Modeling and Management (IJDMMM),* Inderscience Publishers, Switzerland, since 2008.

Conference General/Program Chair/Local Chair
IEEE ICDM, Dallas TX December 2013 (Local Chair)
IEEE ISI, Seattle, Washington, June 2013 (Program Co-Chair)
SIAM SDM Austin, TX, May 2013 (Local Chair)

Program Committee member for multiple conferences

Review for Journals/Conferences
IEEE Transactions on Dependable and Secure Computing

(e) Student Cyber Security Programs (2011 – Present, 5 years)

Works with the team in organizing Cyber Security courses and annual conference. Advises PhD and MS students in Cyber Security. Co-PI of the NSF SFS Grant and supports the student research efforts.

(f) Presentations (2011 – Present, 5 years)

<u>FEATURED/KEYNOTE PRESENTATIONS</u>

- *Assured Cloud-based Information Sharing*, PAISI (Pacific Asia Intelligence and Security Informatics) May 2012, Kuala Lumpur, Malaysia.

- *Assured Cloud-based Information Sharing*, AFOSR-EOARD Conference (Intl. Conference on Mathematical Models, Models and Architectures for Computer Network Security), October 2012, St. Petersburg, Russia.

4. STUDENT RESEARCH IN CYBER SECURITY

For a sample faculty working in Cyber Security, we list the Cyber Security theses and papers for some of their students.

Dr. Bhavani Thuraisingham

Student Thesis with links

- Tyrone Cadenhead, 2011 Secure Data Provenance Using Semantic Web Technologies, August 2011 Tyrone Cadenhead Dissertation.pdf
- Wei-She, 2011 Secure Service Composition with Information Flow Control, December 2011 dissertation-She.pdf
- Parveen Pallabi 2013, Insider Threat Detection with Stream Mining and Big Data, December 2013 http://www.utdallas.edu/~lkhan/papers/ThesisParveen.pdf
- Vaibhav Khadilkar 2013, Assured Information Sharing (AIS) Using the Cloud Assured Information Sharing (AIS) using the Cloud.pdf
- Liangliang Xiao, 2012 Secure query communication and processing protocols for critical cloud applications. Dissertation-Xiao.pdf

Student Papers (student names are in bold)

Pallabi Parveen, **Nathan McDaniel**, **Zackary R. Weger**, **Jonathan Evans**, Bhavani M. Thuraisingham, Kevin W. Hamlen, Latifur Khan: Evolving Insider Threat Detection Stream Mining Perspective. International Journal on Artificial Intelligence Tools 22(5) (2013)

Wei She, I-Ling Yen, Bhavani M. Thuraisingham, Elisa Bertino: Security-Aware Service Composition with Fine-Grained Information Flow Control. IEEE T. Services Computing 6(3): 330-343 (2013)

Lidan Fan, **Zaixin Lu**, Weili Wu, Bhavani M. Thuraisingham, **Huan Ma**, **Yuanjun Bi**: Least Cost Rumor Blocking in Social Networks. ICDCS 2013: 540-549

Sheikh M. Qumruzzaman, Latifur Khan, Bhavani M. Thuraisingham: Behavioral sequence prediction for evolving data stream. IRI 2013: 482-488

Jyothsna Rachapalli, **Vaibhav Khadilkar**, Murat Kantarcioglu, Bhavani M. Thuraisingham: REDACT: a framework for sanitizing RDF data. WWW (Companion Volume) 2013: 157-158

W. Eric Wong, Vidroha Debroy, **Richard Golden**, **Xiaofeng Xu**, Bhavani M. Thuraisingham: Effective Software Fault Localization Using an RBF Neural Network. IEEE Transactions on Reliability 61(1): 149-169 (2012)

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

Abhijith Shastry, Murat Kantarcioglu, Yan Zhou, Bhavani M. Thuraisingham: Randomizing Smartphone Malware Profiles against Statistical Mining Techniques. DBSec 2012: 239-254

Pranav Parikh, Murat Kantarcioglu, **Vaibhav Khadilkar,** Bhavani M. Thuraisingham, Latifur Khan: Secure information integration with a semantic web-based framework. IRI 2012: 659-663

Pallabi Parveen, Bhavani M. Thuraisingham: Unsupervised incremental sequence learning for insider threat detection. ISI 2012: 141-143

Satyen Abrol, Latifur Khan, **Vaibhav Khadilkar,** Bhavani M. Thuraisingham, Tyrone Cadenhead: Design and implementation of SNODSOC: Novel class detection for social network analysis. ISI 2012: 215-220

Tyrone Cadenhead, Murat Kantarcioglu, **Vaibhav Khadilkar**, Bhavani M. Thuraisingham: Design and Implementation of a Cloud-Based Assured Information Sharing System. MMM-ACNS 2012: 36-50

Bhavani M. Thuraisingham, **Vaibhav Khadilkar, Jyothsna Rachapalli**, Tyrone Cadenhead, Murat Kantarcioglu, Kevin W. Hamlen, Latifur Khan, Mohammad Farhan Husain: Cloud-Centric Assured Information Sharing. PAISI 2012: 1-26

Tyrone Cadenhead, **Vaibhav Khadilkar**, Murat Kantarcioglu, Bhavani M. Thuraisingham: A cloud-based RDF policy engine for assured information sharing. SACMAT 2012: 113-116

Pallabi Parveen, Nate McDaniel, Varun S. Hariharan, Bhavani M. Thuraisingham, Latifur Khan: Unsupervised Ensemble Based Learning for Insider Threat Detection. SocialCom/PASSAT 2012: 718-727

Ashraful Alam, Latifur Khan, Bhavani M. Thuraisingham: Geospatial Resource Description Framework (GRDF) and security constructs. Computer Standards & Interfaces 33(1): 35-41 (2011)

Tyrone Cadenhead, Vaibhav Khadilkar, Murat Kantarcioglu, Bhavani M. Thuraisingham: A language for provenance access control. CODASPY 2011: 133-144

Pallabi Parveen, Zackary R. Weger, Bhavani M. Thuraisingham, Kevin W. Hamlen, Latifur Khan: Supervised Learning for Insider Threat Detection Using Stream Mining. ICTAI 2011: 1032-1039

Wei She, I-Ling Yen, Bhavani M. Thuraisingham, **San-Yih Huang**: Rule-Based Run-Time Information Flow Control in Service Cloud. ICWS 2011: 524-531

Richard Wartell, Yan Zhou, Kevin W. Hamlen, Murat Kantarcioglu, Bhavani M. Thuraisingham: Differentiating Code from Data in x86 Binaries. ECML/PKDD (3) 2011: 522-536

Tyrone Cadenhead, Vaibhav Khadilkar, Murat Kantarcioglu, Bhavani M. Thuraisingham: Transforming provenance using redaction. SACMAT 2011: 93-102

Wei She, I-Ling Yen, Farokh B. Bastani, Bao N. Tran, Bhavani M. Thuraisingham: Role-based integrated access control and data provenance for SOA based net-centric systems. SOSE 2011: 225-234

Vaibhav Khadilkar, Murat Kantarcioglu, Bhavani M. Thuraisingham, Sharad Mehrotra: Secure Data Processing in a Hybrid Cloud. CoRR abs/1105.1982 (2011)

Dr. Kamil Sarac

Adaptive Information Coding for Secure and Reliable Wireless Telesurgery Communications, **M.E. Tozal**, Y. Wang, E. Al-Shaer, K. Sarac, B. Thuraisingham, B-T. Chu, Journal of Mobile Networks and Applications, Vol.18, Issue 5, October 2013, pp 697-711.

Polynomial Time Solution to Minimum Forwarding Set Problem in Wireless Networks under Disk Coverage Model, **M. Baysan**, K. Sarac, and R. Chandrasekaran, *Ad Hoc Networks Journal*, *Vol.10, No. 7, pp. 1253-1266, September 2012.*

PalmTree: An IP Alias Resolution Algorithm with Linear Probing Complexity, **M.E. Tozal** and K. Sarac, *Computer Communications*, *Vol. 34, No. 5, pp. 658-669, April 2011.*

Location Matters: Eliciting Responses to Direct Probes, Ethan Blanton, **Mehmet E Tozal**, Kamil Sarac, and Sonia Fahmy, *IEEE IPCCC*, December 2013.

Impact of Sampling Design in Estimation of Graph Characteristics, **Emrah Cem, Mehmet E Tozal**, and Kamil Sarac, *IEEE IPCCC*, Decembe 2013.

Estimating Network Layer Subnet Characteristics via Statistical Sampling, **M.E. Tozal** and K. Sarac, *IFIP Networking*, Prague, Czech Republic, May 2012.
Subnet Level Network Topology Mapping, **M.E. Tozal** and K. Sarac, *IEEE IPCCC*, Orlando, Florida, November 2011.

A Security Framework for Service Overlay Networks: Operating in the Presence of Compromised Nodes, **J. Kurian** and K. Sarac, *Parallel and Distributed Computing and Systems*, Dallas, Texas, December 2011.

Relay Assignment in AMT-based Multicast Content Distribution, **S. Patel**, K. Sarac, R. Chandrasekaran, T. Korkmaz, N. Mittal, *9th Annual Conference on Communication Networks and Services Research Conference*, Ottawa, Ontario, Canada, May 2011.

Dr. Murat Kantarcioglu

Dr. Kantarcioglu is an Associated Professor and the recipient of an NSF CAREER Award. He has graduated several PhD Students and has several more in the pipeline. Below is a sample of the PhD theses as well as papers published with students.

Thesis

- Mehmet Kuzu (2013) Practical Privacy Preserving Record Integration and Search http://www.utdallas.edu/~mxk055100/NSACAE/dissertation-mehmet-kuzu.pdf
- Robert Nix (2012) Efficient incentive compatible secure data sharing http://www.utdallas.edu/~mxk055100/NSACAE/dissertation-robert-nix.pdf
- Raymond Heatherly (2011) Privacy-preserving social network analysis http://www.utdallas.edu/~mxk055100/NSACAE/dissertation-raymond-heatherly.pdf
- Mustafa Canim (2011) Exploiting modern hardware for secure data management http://www.utdallas.edu/~muratk/NSACAE/dissertation-mustafa-canim.pdf

Sample Papers

Bijit Hore, Sharad Mehrotra, **Mustafa Canim**, Murat Kantarcioglu, "Secure multidimensional range queries over outsourced data", The VLDB Journal, VLDB Endowment, VLDB J. 21(3): 333-358 (2012).

Robert Nix, Murat Kantarcioglu, "Incentive Compatible Privacy-Preserving Distributed Classification", IEEE Transactions on Dependable and Secure Computing, 9(4): 451-462 (2012).

Vaibhav Khadilkar, Kerim Yasin Oktay, Murat Kantarcioglu, Sharad Mehrotra, "Secure Data Processing over Hybrid Clouds", IEEE Data Eng. Bulletin, 35 (4): 46-54 (2012) (http://sites.computer.org/debull/A12dec/hybrid.pdf)

Murat Kantarcioglu, Bowei Xi, Chris Clifton, "Classifier Evaluation and Attribute Selection against Active Adversaries", Springer Data Mining and Knowledge Discovery, Volume 22, Numbers 1-2, pp 291-335 (2011).

Barbara Carminati, Elena Ferrari, **Raymond Heatherly**, Murat Kantarcioglu, and Bhavani Thuraisinghaim. "Semantic Web-Based Social Network Access Control", Computers and Security Journal, Volume 30, Issues 2-3, pp 108-115, (2011).

Mehmet Kuzu, **Mohammad Saiful Islam**, Murat Kantarcioglu, "Efficient Similarity Search over Encrypted Data", IEEE ICDE 2012

Mehmet Kuzu, Murat Kantarcioglu, Ali Inan, Elisa Bertino, Elizabeth Durham, Bradley Malin: Efficient privacy-aware record integration. EDBT 2013: 167-178 http://www.edbt.org/Proceedings/2013-Genova/papers/edbt/a17-kuzu.pdf

Dr. Kevin Hamlen

Dr. Hamlen is an Associate Professor and is the receipient of an NSF CAREER Award and an AFOSR Young Investigator Program (YIP Award). He has graduated five PhD students and has several more in the pipeline. Below is a sample of PhD theses as well as papers he has published with students.

PhD/MS Thesis

- Safwan Khan (PhD): Decentralizing Trust: New Security Paradigms for Cloud Computing.
- http://www.utdallas.edu/~hamlen/khan13thesis.pdf
- Richard Wartell (PhD): Rewriting x86 Binaries Without Code Producer Cooperation
- http://www.utdallas.edu/~hamlen/wartell12thesis.pdf
- Micah Jones (PhD). Declarative Aspect-oriented Security Policies for In-lined Reference Monitors. Ph.D. Thesis (Advisor: Kevin Hamlen), The University of Texas at Dallas, Richardson, Texas, December 2011. [BibTeX]
- Aditi A. Patwardhan (MS). Security-aware Program Visualization for Analyzing In-lined Reference Monitors. Master's Thesis (Advisors: Kevin Hamlen and Kendra Cooper), The University of Texas at Dallas, Richardson, Texas, June 2010. [BibTeX]
- Dhiraj V. Karamchandani (MS). Surveying the Landscape of ActionScript Security Trends and Threats. Masters Thesis (Advisor: Kevin Hamlen), The University of Texas at Dallas, Richardson, Texas, December 2013. [BibTeX]

Papers

Richard Wartell, Yan Zhou, Kevin W. Hamlen, and Murat Kantarcioglu. Shingled Graph Disassembly: Finding the Undecidable Path. In *Proceedings of the 18th Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD)*, May 2014, forthcoming. [acceptance rate: 16.4%]

Safwan Mahmud Khan, Kevin W. Hamlen, and Murat Kantarcioglu. Silver Lining: Enforcing Secure Information Flow at the Cloud Edge. In *Proceedings of the 2nd IEEE Conference on Cloud Engineering (IC2E)*, March 2014, forthcoming. [acceptance rate: 20.2%]

Yangchun Fu, Zhiqiang Lin, and Kevin W. Hamlen. Subverting System Authentication with Context-Aware, Reactive Virtual Machine Introspection. In *Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC)*, pp. 229–238, December 2013. [acceptance rate: 19.8%]

Richard Wartell, Yan Zhou, Kevin W. Hamlen, and Murat Kantarcioglu. Shingled Graph Disassembly: Finding the Undecidable Path. In *Proceedings of the 16th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, pp. 460–462, October 2013.

Safwan M. Khan and Kevin W. Hamlen. Computation Certification as a Service in the Cloud. In *Proceedings of the 13th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid)*, pp. 434–441, May 2013. [acceptance rate: 22.18%]

Richard Wartell, **Vishwath Mohan**, Kevin W. Hamlen, and Zhiqiang Lin. Securing Untrusted Code via Compiler-Agnostic Binary Rewriting. In *Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC)*, pp. 299–308, December 2012. [acceptance rate: 19%] [Best Student Paper]

Richard Wartell, **Vishwath Mohan**, Kevin W. Hamlen, and Zhiqiang Lin. Binary Stirring: Self-randomizing Instruction Addresses of Legacy x86 Binary Code. In *Proceedings of the 19th ACM Conference on Computer and Communications Security (CCS)*, pp. 157–168, October 2012. [acceptance rate: 19%] [NYU-Poly AT&T Best Applied Security Paper of the Year, 2nd place, 2012]

Vishwath Mohan and Kevin W. Hamlen. Frankenstein: Stitching Malware from Benign Binaries. In *Proceedings of the 6th USENIX Workshop on Offensive Technologies (WOOT)*, pp. 77–84, August 2012. [acceptance rate: 40%]

Safwan M. Khan and Kevin W. Hamlen. AnonymousCloud: A Data Ownership Privacy Provider Framework in Cloud Computing. In *Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 170–176, June 2012. [acceptance rate: <30%]

Safwan M. Khan and Kevin W. Hamlen. Hatman: Intra-cloud Trust Management for Hadoop. In *Proceedings of the 5th IEEE International Conference on Cloud Computing (CLOUD)*, pp. 494–501, June 2012. [acceptance rate: 19%]

Bhavani Thuraisingham, **Vaibhav Khadilkar**, **Jyothsna Rachapalli**, **Tyrone Cadenhead**, Murat Kantarcioglu, Kevin Hamlen, Latifur Khan, and Farhan Husain. Cloud-Centric Assured Information Sharing, Invited paper. In *Proceedings of the 7th Pacific Asia Workshop on Intelligence and Security Informatics (PAISI)*, pp. 1–26, May 2012.

Kevin W. Hamlen, **Micah M. Jones**, and **Meera Sridhar**. Aspect-oriented Runtime Monitor Certification. In *Proceedings of the 18th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, pp. 126–140, March–April 2012. [acceptance rate: 24%]

Pallabi Parveen, **Zackary R. Weger**, Bhavani Thuraisingham, Kevin W. Hamlen, and Latifur Khan. Supervised Learning for Insider Threat Detection Using Stream Mining. In *Proceedings of the 23rd IEEE*

International Conference on Tools with Artificial Intelligence (ICTAI), pp. 1032–1039, November 2011. [acceptance rate: 30%] [Best Paper, Special Session on Stream Data Mining]

Pallabi Parveen, **Jonathan Evans**, Bhavani Thuraisingham, Kevin W. Hamlen, and Latifur Khan. Insider Threat Detection using Stream Mining and Graph Mining. In *Proceedings of the 3rd IEEE Conference on Privacy, Security, Risk and Trust (PASSAT)*, pp. 1102–1110, October 2011. [acceptance rate: 8%]

Richard Wartell, Yan Zhou, Kevin W. Hamlen, Murat Kantarcioglu, and Bhavani Thuraisingham. Differentiating Code from Data in x86 Binaries. In *Proceedings of the European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML PKDD)*, 3:522–536, September 2011. [acceptance rate: 20%]

Micah Jones and Kevin W. Hamlen. A Service-oriented Approach to Mobile Code Security. In *Proceedings of the 8th International Conference on Mobile Web Information Systems (MobiWIS)*, pp. 531–538, September 2011. [acceptance rate: 36%]

Meera Sridhar and Kevin W. Hamlen. Flexible In-lined Reference Monitor Certification: Challenges and Future Directions. In *Proceedings of the 5th ACM SIGPLAN Workshop on Programming Languages meets Program Verification (PLPV)*, pp. 55–60, January 2011. [acceptance rate: 60%]

Dr. Zhiqiang Lin

Dr. Zhiqiang Lin joined UTD in September 2011 as Assistant Professor and is the recipient of an AFOSR Young Investigator Program (YIP) Award. He is supervising 6 PhD students, and has supervised 4 MS students. Below is a list of papers published with his students.

JOURNALS

"Bridging the Semantic Gap in Virtual Machine Introspection via Online Kernel Data Redirection". **Yangchun Fu,** and Zhiqiang Lin. In ACM Transactions on Information and System Security (TISSEC), Volume 16 Issue 2, September 2013.

CONFERENCE PROCEEDINGS

"Hybrid-Bridge: Efficiently Bridging the Semantic-Gap in Virtual Machine Introspection via Decoupled Execution and Training Memoization". Alireza Saberi, **Yangchun Fu**, and Zhiqiang Lin. To appear in *Proceedings of the 21st ISOC Network and Distributed System Security Symposium*, San Diego, CA, February 2014

"SMV-Hunter: Large Scale, Automated Detection of SSL/TLS Man-in-the-Middle Vulnerabilities in Android Apps". **David Sounthiraraj**, **Justin Sahs**, Zhiqiang Lin, Latifur Khan, and Garrett Greenwood. To appear in *Proceedings of the 21st ISOC Network and Distributed System Security Symposium*, San Diego, CA, February 2014

"Subverting System Authentication with Context-Aware, Reactive Virtual Machine Introspection". **Yangchun Fu**, Zhiqiang Lin, and Kevin Hamlen. In *Proceedings of the 29th Annual Computer Security Applications Conference*, New Orleans, Louisiana, December 2013.

"Obfuscation-resilient Binary Code Reuse through Trace-oriented Programming". **Junyuan Zeng**, **Yangchun Fu**, b, Zhiqiang Lin, Xiangyu Zhang, and Dongyan Xu. In *Proceedings of the 20th ACM Conference on Computer and Communications Security*, Berlin, Germany, November 2013.

"CPU Transparent Protection of OS Kernel and Hypervisor Integrity with Programmable DRAM". Ziyi Liu, Jonghyuk Lee, **Junyuan Zeng**, **Yuanfeng Wen**, Zhiqiang Lin, and Weidong Shi. In *Proceedings of the 40th International Symposium on Computer Architecture*, Tel-Aviv, Israel. June 2013.

"Exterior: Using a Dual-VM Based External Shell for Guest-OS Introspection, Configuration, and Recovery". **Yangchun Fu**, and Zhiqiang Lin. In *Proceedings of the 9th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments*, Houston, TX, March 2013

"OS-Sommelier: Memory-Only Operating System Fingerprinting in the Cloud". **Yufei Gu**, **Yangchun Fu**, Aravind Prakash, Zhiqiang Lin, and Heng Yin. In *Proceedings of the 3rd ACM Symposium on Cloud Computing*, San Jose, CA, October 2012.

"Bin-Carver: Automatic Recovery of Binary Executable Files". **Scott Hand**, Zhiqiang Lin, **Guofei Gu**, and Bhavani Thuraisingham. In *Proceedings of the 12th Annual Digital Forensics Research Conference*, Washington DC, August 2012

"Space Traveling across VM: Automatically Bridging the Semantic Gap in Virtual Machine Introspection via Online Kernel Data Redirection". **Yangchun Fu**, and Zhiqiang Lin. In *Proceedings of the 33rd IEEE Symposium on Security and Privacy*, San Fransisco, CA, May 2012

Dr. Alvaro Cardenas

Dr. Cardena joined UTD as an Assistant Professor in January 2013. His research is in control systems security and critical infrastructure protection. He is supervising four PhD students. He is also advising an undergraduate researcher who obtained an award from CRA-W for security analytics and visualization. http://bigdatautd.wordpress.com/ Below is a paper published with his student.

Carlos Barreto, Alvaro A. Cárdenas, Nicanor Quijano: Controllability of Dynamical Systems: Threat Models and Reactive Security. GameSec 2013: 45-64,
http://www.utdallas.edu/~axc127431/papers/GameSec2013.pdf

Dr. Yiorgos Makris

Dr. Makris joined UTD as an Associated Professor in Computer Engineering in September 2011 and is advising several PhD students. Below is a sample of papers published with his students.

Y. Liu, Y. Jin, Y. Makris, "Hardware Trojans in Wireless Cryptographic ICs: Silicon Demonstration & Detection Method Evaluation," Proceedings of the ACM/IEEE Design Automation Conference (ICCAD), pp. 399-404, 2013
Link: http://www.utdallas.edu/~gxm112130/papers/iccad13.pdf

K. Huang, J. Carulli, Y. Makris, "Counterfeit Electronics: A Rising Threat in the Semiconductor Manufacturing Industry," Proceedings of the IEEE International Test Conference (ITC), L3.4.1-L3.4.4, 2013
Link: http://www.utdallas.edu/~gxm112130/papers/itc13a.pdf

K. Huang, J. Carulli, Y. Makris, "Parametric Counterfeit IC Detection via Support Vector Machines," Proceedings of the IEEE Defect and Fault Tolerance Symposium (DFTS), pp. 7-12, 2012
Link: http://www.utdallas.edu/~gxm112130/papers/dfts12.pdf

Dr. Latifur Khan

Mohammad M. Masud, Tahseen Al-Khateeb, Kevin W. Hamlen, Jing Gao, Latifur Khan, Jiawei Han, Bhavani M. Thuraisingham: Cloud-based malware detection for evolving data streams. ACM Trans. Management Inf. Syst. 2(3): 16 (2011)

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): 1484-1497 (2013)

Mohammad M. Masud, Clay Woolam, Jing Gao, Latifur Khan, Jiawei Han, Kevin W. Hamlen, Nikunj C. Oza: Facing the reality of data stream classification: coping with scarcity of labeled data. Knowl. Inf. Syst. 33(1): 213-244 (2011)

Mohammad M. Masud, Jing Gao, Latifur Khan, Jiawei Han, Bhavani M. Thuraisingham: Classification and Novel Class Detection in Concept-Drifting Data Streams under Time Constraints. IEEE Trans. Knowl. Data Eng. 23(6): 859-874 (2011)

Justin Sahs, Latifur Khan: A Machine Learning Approach to Android Malware Detection. EISIC 2012: 141-147

David Sounthiraraj, Justin Sahs, Zhiqiang Lin, Latifur Khan, and **Garrett Greenwood**. "SMV-Hunter: Large Scale, Automated Detection of SSL/TLS Man-in-the-Middle Vulnerabilities in Android Apps". To appear in *Proceedings of the 21st ISOC Network and Distributed System Security Symposium*, San Diego, CA, February 2014

Tahseen Al-Khateeb, Mohammad M. Masud, Latifur Khan, Bhavani M. Thuraisingham: Cloud Guided Stream Classification Using Class-Based Ensemble. IEEE CLOUD 2012: 694-701

Other Cyber Security Faculty:

Dr.Yvo Desmedt joined UTD in August 2012 a Chaired Professor and Dr. Zygmunt Haas joined UTD in August 2013 as Chaired Professor. They have not yet graduated PhD students at UTD. However, Dr. Desmedt and Dr. Haas have graduated several PhD students in their prior positions (University College London, Cornell University). We have not listed their students' thesis and student publications at their prior institutions.

Part 6b.
List Cyber Security courses that require research paper(s) or virtual/physical lab project(s). Provide Cyber Security course titles that require these papers/lab projects within 5 years of application. Provide link to course syllabus.
Point Value: 1 point per course/3 points required/20 points maximum

Dr. Bhavani Thuraisingham

Each of the following courses have a lab project as well as two papers. Students may choose a topic discussed in class and develop a system/tool. Students submit electronically the source code and a design document for the project. Student use the resources of the CSI Lab facilities to carry out the projects.

Data and Applications Security (Fall 2011, 2012, 2013)
http://www.utdallas.edu/~bxt043000/Teaching/CS-6V81/DAS-F2013/das-F2013.html

As part of the programming/lab project, each student designs and develops a system/tool. The systems developed include the following: Secure E-Commerce System, Query Rewriting System for Access Control, XACML-based access control system for healthcare applications.

Information Systems Security (Summer 2011, 2012, 2013)
http://www.utdallas.edu/~bxt043000/Teaching/CS-6301/Cyber-Security-Essentials-SS2013/cse-ss2013.html
As part of the programming/lab project, each student designs and develops a system/tool. The systems developed include the following: Cryptographic system, Intrusion detection system, and Face recognition system.

Developing and Securing the Cloud (Spring 2012, Spring 2014)
http://www.utdallas.edu/~bxt043000/Teaching/CS-6V81/SecureWebServices_CloudComp-S2012/sws-s2012.html
As part of the programming/lab project, each student designs and develops a secure cloud computing system. Students utilize the Hadoop/MapReduce framework to implement the system. The systems developed incude a secure cloud query processing system, XACML-based access control system for the cloud, Identity management system for the cloud.

Analyzing and Securing Social Networks (Spring 2013)
http://www.utdallas.edu/~bxt043000/Teaching/CS-6301/Analyzing-Securing-SNs-S2013/assn-s2013.html
As part of the programming/lab project, each student designs and develops a secure social computing system. The systems developed incude access control system for a social network and a privacy preserving social network system.

Digital Forensics (Fall 2011, 2012, 2013)
http://www.utdallas.edu/~bxt043000/Teaching/CS-4398/F2013/dig-forensics-F2013.html
Each student carries out two projects. One is a digital forensics project that utilizes the ENCASE tool. The students use the forensic tool and carry out forensics analysis and write a report. The second is a programming project where a student developed a forensics tool. These tools include keyword search tools and crime scene reconstruction tools.

Dr. Kamil Sarac

CS 4396 Computer Networks Lab (Spring 2011, 2012, 2013, 2014)
http://www.utdallas.edu/~kxs028100/cnlab/Syllabus.pdf
This course enables students to gain hands-on experience with real networks by building networks in a virtual laboratory environment. Projects may include establishing an intra-domain routing infrastructure in the laboratory; establishing inter-domain network topologies with BGP used to connect the different autonomous systems; running network services/applications on top of this network, including DHCP, DNS, HTTP, and configuring firewalls.

CS 6349 Network Security (Spring 2011, 2012, 2013, 2014, Fall 2013)
http://www.utdallas.edu/~kxs028100/netsec/Syllabus.pdf
The hands on laboratory project activities in this class include a password cracking exercise; an in-class cyber wars exercise where students attack and defend computing systems in an isolated virtual laboratory environment; and a capture the flag competition where students work on solving a number of cybersecurity challenges.

Dr. Murat Kantarcioglu

Secure Cloud Computing (Spring 2013)
http://www.utdallas.edu/~muratk/courses/cloudsec13s.htm
In this course, students are required to an independent project that requires them to address different data security issues in the cloud. Since the projects are chosen based on the student interests, potential projects covered topics ranging from embedding access control into Hadoop to encrypted query processing in the cloud.

Introduction to Data Security (Spring 2013)
http://www.utdallas.edu/~muratk/courses/dbsec12f.htm
In this undergraduate course that covers basic topics of data security, students are asked to implement a text editor that stores sensitive data in an encrypted format.
Link to project description:
http://www.utdallas.edu/~mxk055100/NSACAE/CS4389_ProjDesc.pdf
In addition, students are asked to implement role based access control policies using industry standard access control language XACML.
Link to homework description:
http://www.utdallas.edu/~mxk055100/NSACAE/CS-4389-Homework-Description.pdf

Introduction to Cryptography (Spring 2012, Spring 2011)
Link to Course Syllabus: http://www.utdallas.edu/~muratk/courses/crypto12s.htm
In this graduate level introduction to cryptography course students are asked to implement an extension to Google Doc to store encrypted files on Google. Please see the description of the project for more details
http://www.utdallas.edu/~mxk055100/NSACAE/crypto-project.pdf

Dr. Kevin Hamlen

Language-based Security (Spring 2011, Fall 2012, Fall 2013)
http://www.utdallas.edu/~hamlen/cs6301fa13.html
Students complete final projects in teams of 3-4. Projects are team-specific, and involve implementing one of the research-level language-based security analyses covered in the course, or using an existing security framework in a novel way to enforce new security policies on untrusted software. Past projects have included the development of a software model-checker for secure bytecode verification, formal certification of an algorithm implementation using the Coq program-proof co-development framework, and extension of an existing software fault isolation system to support non-Linux applications.

Dr. Zhiqiang Lin
CS 4393: Computer and Network Security (Spring 2013, Spring 2014)
http://www.utdallas.edu/~zxl111930/spring2014.html
This course is a comprehensive study of the security principles and practices of computer and network systems. Topics include fundamental concepts and principles of computer security, operating system and network security, firewalls and intrusion detection systems, secret key and public key cryptographic algorithms, hash functions, authentication, SSL and Web security. The learning outcome is students are able to understand the basic principles and practices in computer and network security. In particular, understand what the foundational theory is behind computer security, what the common threats are (e.g., malware, exploit, vulnerability), and how to build the defense mechanism in a combination from OS, network and applied crypto. In support of this, the course prepares students to do basic system, network, and application-level programming/labs related to security purposes.

Dr. Yiorgos Makris
CE7V80 Special Topics: Trusted and Secure Integrated Circuits and Systems (Spring 2013 - 2014)

This course investigates the various aspects related to the design and implementation of trusted and secure integrated circuits (ICs) and systems. Hands-on experience is also obtained through semester-long projects which are carried out in parallel with the lectures. Below are some example titles of student project reports.

Andrew Folloder, "Experiences with Proof-Carrying Code and Information Flow Tracking in Trusted 3rd Party Hardware IP Acquisition"
Kiruba Subramani & Yichuan Lu, "Side-Channel Attack Resistant Wireless Cryptographic ICs through Random Knob Tuning"
Yu Liu, "Hardware Trojans in Wireless Cryptographic ICs"
Liwei Zhou, "Hardware Suport for Workload Execution Forensics Analysis"

5. INTERDISCIPLINARY PROGRAMS IN CYBER SECURITY

5.1 Interdisciplinary Courses

Cyber Security units and modules are included in several of the Non Cyber Security tracks at UTD. In addition there are special tracks in Non-Cyber Security areas that provide complementary skills required to carry out Cyber Security Research. We provide a sample. http://catalog.utdallas.edu/2013/graduate/programs/ecs/computer-science#computer-science-mscs

CS 6360 **Database Design**: Methods, principles, and concepts that are relevant to the practice of database software design. Database system architecture; conceptual database models; relational and object-oriented databases; database system implementation; query processing and optimization; transaction processing concepts, concurrency, and recovery; security. This course introduces students to the fundamental concept in relational databases. Students are introduced to: 1) Conceptual, logical and physical organization of data, 2) Use of both formal and commercial (e.g. SQL/PL-SQL) query languages, 3) Query optimization and 4) XML, XPath, and Xquereis. These concepts are exercised further by a number of assignments (homeworks) and two exams that involve design and implementation of services provided by a relational file system and semi-structured data models. Data security is also introduced as part of this course.

CS 6390 Advanced Computer Networks
In this class, we spend two lecture hours covering an overview of fundamental network security topics including symmetric and asymmetric key crypto and secure hash functions and their use in building secure remote authentication protocols as well as secure communication services for confidentiality, integrity and source authentication. We also cover KDCs and PKIs and SSL and its use for secure online commerce applications. The class also includes a hands-on homework exercise where students analyze network traffic captured from an operational network and infer application layer activities involved in the generation of the traffic. Finally, we use another hands-on homework exercise where students use various network debugging and diagnostic tools to query and learn configuration information about an operational network.

CS 6362 **Advanced Software Architecture and Design Concepts**
This course describes the methodologies for the development, evolution, and reuse of software architecture and design, with an emphasis on object-orientation. Identification, analysis, and synthesis of system data, process, communication, and control components. Decomposition, assignment, and composition of functionality to design elements and connectors. Use of non-functional requirements for analyzing trade-offs and selecting among design alternatives. Transition from requirements to software architecture, design, and to implementation. State of the practice and art. Aspects of security architecture are also introduced in this course.

CS 6367 **Software Testing, Validation and Verification**
Fundamental concepts of software testing. Functional testing. GUI based testing tools. Control flow based test adequacy criteria. Data flow based test adequacy criteria. White box based testing tools. Mutation testing and testing tools. Relationship between test adequacy criteria. Finite state machine based testing. Static and dynamic program slicing for testing and debugging. Software reliability. Formal verification of program correctness. Aspects of security testing are also introduced in this course.

CS 6375 **Machine Learning**
Algorithms for training perceptions and multi-layer neural nets: back propagation, Boltzmann machines, and self-organizing nets. The ID3 and the Nearest Neighbor algorithms. Formal models for analyzing learnability: exact identification in the limit and probably approximately correct (PAC) identification. Computational limitations of learning machines. This course is extremely beneficial for our Cyber Security research in malware detection.

CS 6371 **Advanced Programming Languages**
Functional programming, Lambda calculus, logic programming, abstract syntax, denotational semantics of imperative languages, fixpoints semantics, verification of programs, partial evaluation, interpretation and automatic compilation, axiomatic semantics, applications of semantics to software engineering. This course also introduced students to secure programming languages.

CS 6378 **Advanced Operating Systems**
Concurrent processing, inter-process communication, process synchronization, deadlocks, introduction to queuing theory and operational analysis, topics in distributed systems and algorithms, checkpointing, recovery, multiprocessor operating systems. Security issues such as access control are also introduced in thus course.

CS5333 Discrete Structures
This course is about the Mathematical foundations of computer science. Topics include logic, sets, relations, graphs and algebraic structures. In addition, combinatorics and metrics for performance evaluation of algorithms will be covered. This course provides the foundations for understanding the foundations of cyber security needed for many of our Cyber Security courses.

EE/CE/CS 6304: Computer Architecture (Spring 2012, Fall 2012 - 2013)
Trends in processor, memory, I/O and system design. Techniques for quantitative analysis and evaluation of computer systems to understand and compare alternative design choices in system design. Components in high performance processors and computers: pipelining, instruction level parallelism, memory hierarchies, and input/output. Students will undertake a major computing system analysis and design project. This course prepares students to take the hardware security course **Trusted and Secure Integrated Circuits and Systems** (discussed in Item 7).

5.2 Interdisciplinary Tracks that enhance Cyber Security Research

We have several programs, degrees and tracks both within the School of Engineering and Computer Science (ECS) as well as in other schools that enhance UTD's Cyber Security Research. Due to these programs we have several interdisciplinary projects from NSF, AFOSR and ARO and have substantial number of publications. Below we list a sample of our programs. We also like a sample of our publications resulting from this interdisciplinary research. The names of professors at UTD outside of ECS are in bold.

5.2.1 Tracks in ECS (Engineering and Computer Science)

Data Science

Massive amounts of structured and unstructured data is being generated continuously from sensor network and online user activities on e-commerce and social-media websites. **Big Data**, as this massive amount of data is called, leads to many challenges such as (a) How do companies manage and process this massive amount of data? (b) How do companies automatically learn hidden trends and patterns in this data? (c) How do companies gather actionable intelligence to improve their bottom line? This track covers **tools and techniques** that directly address these challenges. Students take a variety of courses including Big Data Analytics, Database Systems, Machine Learning and Statistical Methods. The track is relevant to Cyber Security as many of the data analytics tools are utilized in our research for malware detection.

Executive Masters in Software Engineering

UTD has initiated The Executive Master of Science in Computer Science - Software Engineering. The first batch of students is expected to graduate in Spring 2014. The program offers a number of courses including in software architectures, database systems and cyber security. It provides practical professional education to Dallas-area software professionals, preparing them for positions of increasing responsibility throughout their careers. The Cyber Security course which is being taught during Spring 2014 covers the CISSP (Certified Information Systems Security Professional) Modules as well as topics in Critical Infrastructure Protection among others. http://cs.utdallas.edu/executiveMSSE/

Systems Engineering

Systems Engineering is a department in the School of Engineering and Computer Science. It offers a Certificate in Cyber Security Systems (CCSS). This is a graduate level interdisciplinary certificate program in cyber security. The program is a joint program between the Engineering School (Computer Science department and Systems Engineering department) and School of Management (JSOM) at UTD. The program provides a common core for all students in the program and provides specialization in the computer science aspects or systems engineering aspects or management (risk and security audit) aspects of cyber security. The program was approved by the University senate in November 2013 and is now accepting applications for the Fall 2014 semester.

The Six Tracks in Computer Science at UTD

The CS department offers six concentration tracks at the graduate level including: (1) traditional CS, (2) networks and telecommunications, (3) intelligent systems, (4) systems, (5) software engineering, and (6) information assurance/cyber security. Most of these tracks include classes that provide students with the necessary skills to conduct research in Cyber Security. In addition, they include various classes where relevant Cyber Security topics are included in their syllabi (such as Advanced Computer Networks class in network and telecommunications track covers fundamentals of network security topics and software testing, validation and verification class covers security testing, etc). http://catalog.utdallas.edu/now/graduate/programs/ecs/computer-science

5.2.2 Tracks in Other Schools at UTD

The **Naveen Jindal School of Management** (JSOM) offers a variety of Master of Science degrees as well as Certificates which includes concentration in Information Assurance.

(a) The **Master of Science in Information Technology and Management** (MS ITM) degree program requires a minimum of 36 semester credit hours consisting of basic business courses, IT foundation courses, IT elective courses and other electives. The business courses give students a better understanding of issues that occur at the interface between IT and business. The IT foundation courses cover the essentials of IT. The IT elective courses provide in-depth knowledge of technology and technology-management issues. In addition, students may select approved electives that maximize their goals. The program also offers opportunities for students with special interests to concentrate in a specific track within the IT area, such as business intelligence and analytics, enterprise systems**, information security and assurance,** IT consulting and management services, or healthcare systems.

(b) Obtaining certifications in specific areas of IT can enhance career prospects. Certifications relevant to Cyber Security are in **Business Intelligence and Data Mining**. This is because we conduct extensive research on applying analytics for cyber security applications. The certificate program, which requires courses in business perspective, statistics, data preparation, and data mining, demonstrates the working partnership between UT Dallas and SAS Institute, a leading provider of data mining and business intelligence software and services.

(c) The graduate certificate in **Healthcare Information Technology (IT)** emphasizes practical concepts in healthcare IT and hands-on experience gained using electronic medical records (EMR) software such as Epic. The learning outcomes for the program include the following: Identify and understand the key information requirements for managing and working with healthcare information systems; Understand analytics related to healthcare information to develop sound healthcare decisions; and Understand the core functionalities of a leading EMR software platform, including how it supports clinical information workflows in a paperless environment, and its interconnectivity with other clinical and business systems. We conduct extensive research in data privacy with funding from NIH. Therefore, exposure to healthcare IT-related issues will benefit our students a great deal.

(d) We carry out extensive research with JSOM's **International Center for Decision and Risk Analysis** (ICDRiA) on several of our research projects in Cyber Security funded by NSF, AFOSR, ARO and others. Risk Management is a growing and highly-relevant field of study. While probability and statistics are the primary quantitative techniques of Risk Management, there are many other techniques (such as optimization, decision theory, control theory, and game theory) which play an essential role in managing risk. The goal is to build both the knowledge and application of these techniques with specific attention to the interdisciplinary aspects. Our approach is to develop relevant models—validated by practitioners—to derive concepts and results which help to understand the impact of uncertainties. We provide useful, tested tools for mitigating risks and decision-making. We focus on the situation of several players, with various possibilities of rules of game. The Center also offers a number of courses in risk management. http://jindal.utdallas.edu/centers-of-excellence/international-center-for-decision-and-risk-analysis/

The School of Economic, Political and Policy Sciences (EPPS) offers two graduate certificates relevant to Cyber Security. They are in Geospatial Intelligence (GEOINT) and Homeland Security. http://www.utdallas.edu/dept/graddean/CAT2012/EPPS/PRE/certificates_epps.htm In addition, EPPS also has one of the top criminology programs in the USA as well and a strong programs in Economics and Public Policy. Knowledge of these topics is important for our research in (a) geospatial data security, (b) cyber operations, (c) digital forensics, (d) economics of cyber security and (e) policy-related aspects of security and privacy.

a. The **GEOINT** certificate program produces graduates that have met the requirements for such professionals set forth by the United States Geospatial Intelligence Foundation (USGIF). The GEOINT is a rapidly evolving field that demands certain technical skill sets, the ability for individual rapid critical thinking and a global awareness of supporting information for national security and other intelligence activities.

b. Strengthening the preparedness of the U.S requires a body of trained professionals in homeland security. The relative novelty of homeland security as a field of practice and study further strengthens the need for expanding the training and educational needs of both current homeland security professionals and other professionals with an interest in moving in to a career in homeland security. The graduate certificate in **Homeland Security** is directed to homeland security professionals and those aspiring to such employment in both government and business. (http://www.utdallas.edu/epps/public-affairs/dl/Homeland_Security_Certificate_Flyer.pdf

c. **The Center for Crime and Justice Studies'** mission is to advance our understanding of crime and criminal justice through collaboration between criminal justice scholars and criminal justice professionals, to inform criminal justice policy makers and the public on "what works" in criminal justice through transparent scientific and objective research, and to help refine the criminal justice process to reduce the costs of justice while maintaining public safety and public demands for punishment. The Center provides a venue for faculty, graduate students, policy makers, and Criminal Justice practitioners to conduct scientific research pertaining to all things crime and justice. This surrounds human development, criminality, victimization, policing, courts, and reentry back into society. The Center will also offer professional training and certification programs for criminal justice professionals as well as publish newsletters for criminal justice scholars and practitioners on pressing justice related issues. http://www.utdallas.edu/epps/ccjs/

d. EPPS offers a variety of programs in Economics including a Master of Science in **Applied Economics.** This degree provides an excellent graduate-level education in economics, with emphasis on the development of theoretical understanding of economic phenomena, quantitative skills that can be applied to economic problems and critical thinking to understand how to best apply economic theory and quantitative skills to real-world problems. The knowledge students gain in Game Theory is especially important for our research in adversarial modeling and mining. http://www.utdallas.edu/epps/economics/degrees.html

e. EPPS offers a Masters degree in **Public Policy** (MPP). What makes a professional career in public policy unique is the emphasis on tackling "wicked problems" — the challenging issues that define the public agenda and require talented individuals to devote their energy to finding solutions. The MPP degree offers students an education to succeed in this dynamic, global workforce. Our interdisciplinary degree will teach students economic and statistical analyses as well as communication skills that will help them succeed. We conduct extensive research in data privacy and believe that students will benefit from exposure to policy related aspects.

The School of Brain and Behavioral Sciences (BBS) at UTD has graduate programs in cognitive neuroscience and psychology, among others. We conduct joint research with BBS to understand the minds of the hackers and therefore these programs are relevant to our research in Cyber Security. http://bbs.utdallas.edu/graduate/

(a) The Master of Science degree in **Applied Cognition and Neuroscience** (ACN) program incorporates methodologies from such diverse fields as psychology, neuroscience and computer science. Students in the ACN program may choose to specialize in one or more of the following areas: Cognition and Neuroscience, Computational Modeling/Intelligent Systems, Human Computer Interaction, and Neurological Diagnosis and Monitoring. http://bbs.utdallas.edu/acn/

(b) The Master of Science in **Psychological Sciences** program provides advanced psychology training to prepare serious student scholars for nationally prominent doctoral programs in clinical and experimental psychology. Students will obtain research experience, advanced course-work and applied experience in psychology. This research-focused program requires students to work with a research mentor and to be actively involved in at least one research laboratory throughout the two-year training. Students also have the opportunity to gain additional applied experiences through the thriving internship program in the School of Behavioral and Brain Sciences. http://bbs.utdallas.edu/psyscims/

UTD's **School of Arts, Technology and Emerging Communications** provides one of the top and fastest growing programs in the world in **Arts and Technology.** This program is carried out jointly with the School of Engineering and Computer Science (ECS). The undergraduate Arts and Technology program will offer a focused, rigorous, interdisciplinary education emphasizing the creation, application and implications of interactive digital content. The program will emphasize the fusion of creative with critical thinking and theory with practice. Students will gain both practical skills and conceptual understanding. In addition to the basic understanding of the interaction of technology with the creative arts, students may choose from elective possibilities to focus on either Digital Arts and Design, which will emphasize the role and potential of computer-generated visual images, or Games and Interactive Narrative, which will emphasize the nature and potential of interactive games. Arts and Technology majors at UT Dallas will be prepared to make use of their academic training in a wide range of occupations in industries such as advertising, communications, education and entertainment. UTD's Cyber Security Institute Faculty is having discussions with the Arts and Technology Program director on how to incorporate security and privacy aspects into their program. http://www.utdallas.edu/atec/

5.3 Sample Interdisciplinary Research

Dr. Murat Kantarcioglu

Dr. Murat Kantarcioglu has carried out extensive interdisciplinary research in cyber security. Specifically he has applied game theory, risk analysis and economics in his research. Below are his sample papers.

- Murat Kantarcioglu, Alain Bensoussan, SingRu Celine Hoe: Investment in Privacy-Preserving Technologies under Uncertainty. GameSec 2011:219-238 (with JSOM)
- Daniel C. Krawczyk, James Bartlett, Murat Kantarcioglu, Kevin W. Hamlen, Bhavani M. Thuraisingham: Measuring expertise and bias in cyber security using cognitive and neuroscience approaches. ISI 2013:364-367 (with BBS)
- Nathan Berg, Chunyu Chen, Murat Kantarcioglu: Experiments in Information Sharing CoRR abs/1305.5176 (2013) (with EPPS)

Prof. Latifur Khan

While Prof. Khan is a member of the Core Cyber Security Faculty due to his extensive research in Data Mining for Malware Detection, he is a renowned expert in data analytics. Below are his student's thesis and papers that include aspects of Cyber Security. For example, his student Dr, Farhan's thesis was on Cloud Query Processing. One chapter of this thesis is on access control for the cloud where query rewriting techniques are developed in accordance with the security policies (Chapter 7 of Thesis). Similarly Dr. Neda's thesis also has a chapter on privacy preserving federated query processing (Chapter 7). Furthermore, Dr. Sunitha's thesis descrives extensive applications of formal methods for data model interoperability (Apendix), and Dr. Abrol's thesis work has been expanded into a system for homeland security applications with a patent. Following is a sample of interdisciplinary theses and student papers.

Thesis

- M. Farhan Husain (PhD, 2011) Data Intensice Query Processing for Semantic Web Data Using Hadoop and Mapreduice. May 2011 http://www.utdallas.edu/~lkhan/papers/ThesisHussain.pdf

- Neda Alipanah (PhD, 2012) Federated Query Processing Using Ontology Structure and Ranking in a Service Oriented Environment, May 2012 http://www.utdallas.edu/~bxt043000/Students/Alipanah-NedaDissertation.pdf
- Jeffrey Partyka (PhD, 2012), Learning-Based Geospatial Schema Matching Guided by External Knowledge, December 2011 http://www.utdallas.edu/~lkhan/papers/JeffDissertation.pdf
- Satyen Abrol (PhD, 2013) Location Mining in Online Social Networks, May 2013 http://www.utdallas.edu/~lkhan/papers/Thesis-SatyenAbrol-April.pdf
- Sunitha Ramanujam (PhD. 2011), Towards an Integrated Semantic Web: Interoperability Between Data Models Ph.D. Thesis (Advisors: Latifur Khan and Kevin Hamlen), The University of Texas at Dallas, Richardson, Texas, December 2011. [BibTeX].

Student Papers

- Mohammad Farhan Husain**,** James P. McGlothlin, Latifur Khan, Bhavani M. Thuraisingham: Scalable Complex Query Processing over Large Semantic Web Data Using Cloud. IEEE CLOUD 2011: 187-194
- Tahseen Al-Khateeb, Mohammad M. Masud, Latifur Khan, Bhavani M. Thuraisingham: Cloud Guided Stream Classification Using Class-Based Ensemble. IEEE CLOUD 2012: 694-701
- **Jeffrey Partyka, Pallabi Parveen**, Latifur Khan, Bhavani M. Thuraisingham, Shashi Shekhar: Enhanced geographically typed semantic schema matching. J. Web Sem. 9(1): 52-70 (2011)
- Satyen Abrol, Latifur Khan, Bhavani M. Thuraisingham: Tweecalization: Efficient and intelligent location mining in twitter using semi-supervised learning. CollaborateCom 2012: 514-523
- **Mohammad Farhan Husain, James P. McGlothlin, Mohammad M. Masud,** Latifur R. Khan, Bhavani M. Thuraisingham: Heuristics-Based Query Processing for Large RDF Graphs Using Cloud Computing. IEEE Trans. Knowl. Data Eng. 23(9): 1312-1327 (2011)
- **Tahseen Al-Khateeb, Mohammad M. Masud,** Latifur Khan, Charu C. Aggarwal, Jiawei Han, Bhavani M. Thuraisingham: Stream Classification with Recurring and Novel Class Detection Using Class-Based Ensemble. ICDM 2012: 31-40, 2011
- Neda Alipanah, Latifur Khan, Bhavani M. Thuraisingham: Optmized ontology-driven query expansion using map-reduce framework to facilitate federated queries. Comput. Syst. Sci. Eng. 27(2) (2012)
- James P. McGlothlin, Latifur Khan, Bhavani M. Thuraisingham: RDFKB: A Semantic Web Knowledge Base. IJCAI 2011: 2830-2831

Dr. Bhavani Thuraisingham

While Cyber Security is Dr. Thuraisingham's main focus, she is also involved in data analytics for counter-terrorism applications (she has a certificate in Terrorism Studies in St. Andrews University Scotland.). Below is a sample of her papers that are mainly involved with data analytics.

- Neda Alipanah**,** Pallabi Parveen, Latifur Khan, Bhavani M. Thuraisingham: Ontology-Driven Query Expansion Using Map/Reduce Framework to Facilitate Federated Queries. ICWS 2011: 712-713
- Zhong Wang**,** Wei Wang**,** Joonmo Kim, Bhavani M. Thuraisingham, Weili Wu: PTAS for the minimum weighted dominating set in growth bounded graphs. J. Global Optimization 54(3): 641-648 (2012)
- Vaibhav Khadilkar, Murat Kantarcioglu, Bhavani M. Thuraisingham, Paolo Castagna: Jena-HBase: A Distributed, Scalable and Effcient RDF Triple Store. International Semantic Web Conference (Posters & Demos) 2012
- Vaibhav Khadilkar**,** Murat Kantarcioglu, Bhavani M. Thuraisingham: StormRider: harnessing "storm" for social networks. WWW (Companion Volume) 2012: 543-544

Prof. I-Ling Yen

Prof. Yen conducts research in dependable systems that has included secure dependable systems research. Sample of her papers with her students are listed below.

- Manghui Tu, Hui Ma, Liangliang Xiao, I-Ling Yen, Farokh B. Bastani, Dianxiang Xu: Data Placement in P2P Data Grids Considering the Availability, Security, Access Performance and Load Balancing. J. Grid Comput. 11(1): 103-127 (2013)
- Hui Ma, Favyen Bastani, I-Ling Yen, Hong Mei: QoS-Driven Service Composition with Reconfigurable Services. IEEE T. Services Computing 6(1): 20-34 (2013)
- Liangliang Xiao, I-Ling Yen: Security analysis for order preserving encryption schemes. CISS 2012: 1-6
- Wenke Zhang, Favyen Bastani, I-Ling Yen, Kevin Hulin, Farokh B. Bastani, Latifur Khan: Real-Time Anomaly Detection in Streams of Execution Traces. HASE 2012: 32-39
- Yunqi Ye, Liangliang Xiao, I-Ling Yen, Farokh B. Bastani: Leveraging Service Clouds for Power and QoS Management for Mobile Devices. IEEE CLOUD 2011: 235-242
- Angie Shia, Farokh B. Bastani, I-Ling Yen: A Highly Resilient Framework for Autonomous Robotic Swarm Systems Operating in Unknown, Hostile Environments. ISADS 2011: 147-153
- Panfeng Xue, I-Ling Yen, Kendra M. L. Cooper: QoS-driven dynamic adaptation in media intensive systems. SOCA 2011: 1-8

Prof. Neeraj Mittal

Prof. Mittal conducts research in distributed systems that has included secure distributed systems research. Sample of his papers with his students are listed below.

- Miguel Correia, Neeraj Mittal: Dependability issues in cloud computing: extended papers from the 1st international workshop on dependability issues in cloud computing - DISCCO. Operating Systems Review 47(2): 20-22 (2013)
- Ramon Novales, Neeraj Mittal: Parameterized key assignment for confidential communication in wireless networks. Ad Hoc Networks 9(7): 1186-1201 (2011)

6. CYBER SECURITY OUTREACH

6.1 Shared Courses

Dr. Eric Wong of the Computer Science (CS) department runs an NSF-funded Course, Curriculum, and Laboratory Improvement (CCLI) project on software testing and software security. In the context of this project, Dr. Wong has deve loped several course modules on software testing and software security for sharing with other institutions. Currently, the project has four external collaborators adapting and using this curriculum. These include Dr. Natarajan Meghanathan of Jackson State University (a minority serving institution), Dr. Junhua Ding of East Carolina University, Dr. Sudipto Ghosh of Colorado State University, and Dr. William Slater of Collin College. In addition, the project has several other internal faculty members involved in the educational activities within the scope of the project. As an example, Dr. Wong teaches courses on this topic at Collin College as guest lecturer and Dr. Veerasamy conducted a 2-day workshop on the topic at Jackson State University during February 7-8, 2013. For more information about this project, please refer to the project web site at http://paris.utdallas.edu/ccli/.

In addition, Drs. Sarac and Wong of the CS department at UT Dallas are currently working on organizing a Research Experience for Teachers (RET) program that aims at training and educating high school computer science and technology teachers on mobile security and social network security domains. The program will include a 10 week RET summer program where teachers will work with Drs. Sarac and Wong as well as several PhD students on hands-on research topics in the area. The expected outcome is to equip teachers with the necessary domain knowledge to transfer it to their classes in their schools. We will also provide technical and curricular support to high school teachers in transfering the knowledge to their students during the academic year. The department submitted a grant proposal to NSF's RET program to fund this activity starting in summer 2014.

Regarding curriculum sharing with K-12 schools, Dr. Veerasamy developed and shared a curriculum on Alice programming with Harmony School of Innovation at Carrollton, Springridge Elementary School in Richardson, and JL Long Middle School in Dallas. In addition, Dr. Veerasamy and several graduate students in our department are conducting after school programming clubs in Harmony School of Business and Harmony Science Academy Garland where they introduce programming concepts using hands-on approach and popular tools like Scratch, Logo, Alice and JavaScript tools. Dr. Sarac of CS is also working with the administrators of Harmony Public Schools (HPS) Dallas Cluster in introducing cyber security-related courses into a new pathway program that HPS systems is planning for two of their high schools in their Dallas cluster. http://www.utdallas.edu/k12/clubs/

6.2 Collaboration with Community Colleges

The School of Engineering and Computer Science has a process where transfer students from other institutions including minority institutions and two-year community college students can transfer their credits to our degree programs. Undergraduate advisors are involved in transcript evaluation and course transfers for academic classes taken in such schools. In addition, the School has articulation agreements with Collin College and Richland College, the two main community colleges in the area, for directly transferring course work for the students from those colleges to UT Dallas Engineering School.
Please see:
http://www.utdallas.edu/~kxs028100/CAE/CollinCollegeArticulation.pdf
http://www.utdallas.edu/~kxs028100/CAE/RichlandCollegeArticulation.pdf

6.3 Sponsorship/organization of workshops and exercises by UT Dallas

The Computer Science Department at UT Dallas organizes an annual Texas Security Awareness Week (TexSAW) event that includes student-oriented cyber security workshops and competitions. Starting in October 2011, each year, we invite students from higher education institutions across the state of Texas to participate in this activity. During the first day of the event, students are offered three 2-hour hands-on workshops on (1) web security, (2) exploit development, and (3) penetration testing. During the second day of the event, students participate in a half-day capture-the-flag competition where they put their newly learned skills into practice. During the 3rd TexSAW event in October 2013, we had about 50 students participating in the event from a dozen higher education institutions across the state of the Texas. http://csi.utdallas.edu/events_chronology/event1_2013.html. In 2014, we hosted 40 students from six Texas schools. http://ecs.utdallas.edu/research/centers/csi/events/TexSAW-2014/TexSAW_2014.html

Participation in cyber defense exercises by UT Dallas UT Dallas' Computer Security Group (CSG) is a student club founded and run by the students pursuing cyber security related degrees in the Computer Science Department. CSG is mostly run by students who are currently supported by federally funded scholarship programs in cyber security including NSF Cybercorp© SFS program where Dr. Sarac serves as PI. Dr. Sarac also serves as the faculty mentor of CSG. Among several different educational and training activities, students in CSG group actively participate in various cyber security competitions. According to ctftime.org, the team currently ranks 96th out of over 3000 CTF teams globally and ranks as the 13th US team in the list. Below is a sample list of the competitions that the group participated during the past three years:

1. Seven UT Dallas students placed 45th out of 178 team in Codegate Pre-quals in Spring 2011, a global cyber competition held by South Korea.
2. In 2011, ten UT Dallas students competed as a team in Hack.lu, a German CTF held as part of the annual Hack.lu conference. They placed 42nd out of 108 teams.
3. In 2011, around a dozen UT Dallas students competed as a team in pCTF, a cyber competition held by Carnegie Mellon University. They placed 43rd out of 589 teams.
4. In 2011, three teams of four-students from UT Dallas participated in CSAW, NYU-Poly CTF. UT Dallas students placed 24th in prequals globally and placed 8th out of US based undergraduate teams. One of the teams participated in the finals in New York and placed 7th out of 12 US based teams.
5. In 2011, around 20 UT Dallas students led by Dr. Lin participated in UCSB iCTF event.
6. In 2012, the team ranked 15th out of 235 teams in ForbiddenBITS CTF event.
7. In 2012, two CSG teams participated in the finals at NYU-Poly CSAW finals and ranked 8th and 12th out of 15 finalist teams.
8. In 2013, CSG team ranked 22nd out of 321 teams in HackIM event.
9. In 2013, CSG team ranked 25th out of 124 teams in Ghost in the Shellcode competition event.
10. In 2013, CSG team ranked 17th out of 1387 teams in NYU-Poly CSAW qualifications.

For a full list of the cyber security competitions participated by CSG, please see https://ctftime.org/team/333.

Sponsorship/organization of workshops for K-12 schools by UT Dallas The CS department also organizes several programming clubs all the way from 3rd graders to adults. These clubs include Scratch Club (from 3rd graders to adults); Logo Club (from 3rd graders to adults); Alice Club (from 6th graders to adults); JavaScript Club, Java and Advanced Java Clubs (from 6th graders to adults). For Spring 2014 schedule and for more details about the content of these clubs, please refer to the program web page at http://www.utdallas.edu/k12/clubs/.

Sponsorship/organization of workshops for college students at UT Dallas Dr. Wong of CS conducts an NSF sponsored summer Research Experience for Undergraduates (REU) program on software safety and software security. This is a 10-week program where 10 students are recruited nationally to participate in this program to conduct research in the software security and software safety topics. The program provides a very good research experience for the participants and often involves industry involvement from defense contractor companies such as Raytheon, Lockheed Martin Aeronautics Company, and EDS/HP. For more information about this program and related research projects and teaching materials, please refer to the project web site at http://paris.utdallas.edu/reu/index.html.

As mentioned above, within the context of our annual TexSAW event, we organize three 2-hour workshops on hands-on cybersecurity topics including (1) web security, (2) exploit development, and (3) penetration testing. During the 2013 TexSAW event, we had 50 students participating in this event from over a dozen Texas colleges and universities including minority serving colleges/universities (such as UT San Antonio and UT El Paso) and two-year community colleges (such as Richland College and Collin College).

6.4 Shared events

The TexSAW event mentioned above included an afternoon session where the PIs of the CAE institutions in DFW metroplex area including UT Dallas, University of North Texas, University of Dallas, and Southern Methodist University shared their ideas and experiences in developing successful cyber security education programs for other higher education institutions interested in starting such programs. This event provided a platform for those who are interested in starting similar cyber security education programs to make connections with CAE institution PIs and establish relations. The audience consisted of educators from area high schools and North Texas colleges and universities in addition to people from industry.
See http://csi.utdallas.edu/events_chronology/event1_2013_conference_schedule.html.

The CCLI project of Dr. Wong mentioned in part 1.a above involves shared courses with four other universities/colleges participating in this project. http://paris.utdallas.edu/ccli/

6.5 Sample External Research Collaborations

UTD conducted extensive collaboration on joint research project funded by NSF, AFOSR, ONR, ARO, NIH and others. Here are example projects and links to some of the papers. The universities as well as names of professors and students from other universities are in bold.

AFOSR MURI: A Framework for Managing the Assured Information Sharing Lifecycle 2009-2013; With **University of Maryland Baltimore County, Purdue University, University of Illinois Urbana Champaign, University of Michigan and University of Texas San Antonio.**
Tim Finin, Anupam Joshi, Hillol Kargupta, Yelena Yesha, Joel Sachs, Elisa Bertino, Ninghui Li, Chris Clifton, Gene Spafford, Bhavani M. Thuraisingham, Murat Kantarcioglu, Alain Bensoussan, Nathan Berg, Latifur Khan, Jiawei Han, ChengXiang Zhai, Ravi S. Sandhu, Shouhuai Xu, Jim Massaro, Lada A. Adamic: Assured Information Sharing Life Cycle. ISI 2009: 307-309
Link: http://csi.utdallas.edu/Paper_Links/05137331.pdf
(This is the project overview. Several papers have resulted from this project and are listed under Part 8)

NSF TC: Large: Collaborative Research: Privacy-Enhanced Secure Data Provenance 2011-2016: With **University of Texas San Antonio, Purdue University**
Chenyun Dai, Dan Lin, Elisa Bertino, Murat Kantarcioglu: An Approach to Evaluate Data Trustworthiness Based on Data Provenance. Secure Data Management 2008: 82-98
Link: sdm08.pdf
(this paper was instrumental in write the proposal and winning the NSF grant)

NSF TWC: Medium: Collaborative: Policy Compliant Integration of Linked Data" 2012-2015: **University of Maryland Baltimore County, Massachusetts Institute of Technology**
Kevin W. Hamlen, Lalana Kagal, Murat Kantarcioglu: Policy Enforcement Framework for Cloud Data Management. IEEE Data Eng. Bull. 35(4): 39-45 (2012)
Link: http://www.utdallas.edu/~hamlen/hamlen12deb.pdf

NSF TC:Small:Collaborative: Protocols for Privacy-Preserving Scalable Record Matching and Ontology Alignment 2010-2013 With **Purdue University**
Ali Inan, Murat Kantarcioglu, Gabriel Ghinita, Elisa Bertino: A Hybrid Approach to Private Record Matching. http://csi.utdallas.edu/Paper_Links/06200290.pdf

ARO A Game Theoretic Framework for Adversarial Classification 2012-2015 With **Purdue University**
Yan Zhou, Murat Kantarcioglu, Bhavani M. Thuraisingham, Bowei Xi**:** Adversarial support vector machine learning. KDD 2012: 1059-1067
Link: http://www.utdallas.edu/~mxk055100/publications/kdd2012.pdf

NIH "**Technologies to Enable Privacy in Biobanks**" 2009-2013 With **Vanderbilt University**, Mehmet Kuzu, Murat Kantarcioglu, Elizabeth Ashley Durham, Csaba Toth, Bradley Malin: A practical approach to achieve private medical record linkage in light of public resources. JAMIA 20(2): 285-292 (2013)
Link: J Am Med Inform Assoc-2013-Kuzu-285-92.pdf (there is now a follow-on grant from NIH between Vanderbilt University and UTD.)

6.6 Community Outreach

The CS department at UT Dallas organizes various outreach programs for local schools. In Fall 2013 semester, Dr. Sarac of CS together with the volunteer graduate students in CSG club (https://csg.utdallas.edu/) started a cyber security training program for high school students to prepare them for Air Force Association's Cyber Patriot competitions. During the Fall 2013 semester, we trained three cyber patriot competition teams from the Dallas metropolitan area. We plan to continue this program for future years as an outreach program in cyber security education to high school students in the area. In addition, Dr. Page of CS runs a competitive programming training program where he works with computer science teachers of several area high schools to identify promising students and runs computer programming training courses for high school students. Several high school teachers also participate in these courses along with their students.

As mentioned earlier,, Drs. Sarac and Wong of CS department organizing a Research Experience for Teachers (RET) program that aims at training and educating high school computer science and technology teachers on mobile security and social network security domains. The expected outcome is to equip teachers with necessary domain knowledge to transfer it to their classes in their schools. We also plan to provide technical and curricular support to high school teachers in transferring the knowledge to their students during the academic year. In this context, during Fall 2013 semester, Drs. Sarac and Wong visited three area high schools including Liberty High School of Frisco Texas, Hillcrest High School of Dallas Texas, and Allen High School of Allen Texas, and delivered guest lectures on social networks and their security and privacy implications to high school students.

The CS department also organizes several programming clubs all the way from 3rd graders to adults. These clubs include Scratch Club (from 3rd graders to adults); Logo Club (from 3rd graders to adults); Alice Club (from 6th graders to adults); JavaScript Club, Java and Advanced Java Clubs (from 6th graders to adults). For Spring 2014 schedule and for more details about the content of these clubs, please refer to the program web page at http://www.utdallas.edu/k12/clubs/.

In addition, the Computer Science facebook page is another way in which we advertise the activities that are scheduled. https://www.facebook.com/UTDCSDept.

7. PhD Students Graduated from CSI and Positions

1. Mamoun Awad, 2005, University of UAE
2. Lei Wang, 2006, Microsoft
3. Manghui Tu, 2006, Purdue University, Calimet
4. Li Liu, 2008, Ebay
5. Ryan Layfield, 2008, Cisco
6. Mehmet Gunes, 2008, U of NV, Reno
7. Mehedy Masud, 2009, University of UAE
8. Hai Vu, 2009, Cisco

9. Zhong Wang, 2010 Financial Services, Shanghai
10. Mustafa Canim, 2010, IBM Watson Research Center
11. Ali Inan, 2011, Isik University, Turkey
12. Wei-She, 2011, Intel
13. Tyrone Cadenhead, 2011, Blue Cross Blue Shield
14. Micah Jones, 2011, L3 Communications
15. Jeffrey Partyka, 2011, Raytheon
16. Farhan Husain, 2011, Amazon
17. Ashad Ul Abedin, 2011, BloomReach Inc., CA
18. Sunitha Ramanujan, 2011, Startup company, TX
19. Raymond Heatherly, 2011, Vanderbilt University
20. James McGlothlin, 2011, Fusion Consulting TX
21. Robert Nix, 2012, Lipscomb University
22. Richard Wartell, 2012, Startup in San Fransicso
23. Tahseen Al-khateeb, 2012, Marketo Inc, CA
24. Neda Alipanah, 2012, UC San Diego Medical School
25. Saleem Ahmed, 2012, BloomReach Inc., CA
26. Mehmet Tozal, 2012, U . of LA (Lafayette)
27. Liangliang Zhao, 2012, Frostberg State University
28. Satyen Abrol, 2013, VMWare
29. Parveen Pallabi, 2013, VCE Corporation, TX
30. Vaibhav Khadilkar, 2013, Startup company, TX
31. Safwan Khan, 2013, Yahoo
32. Lidan Fan, 2014, UT Tyler
33. Meera Sridhar, 2014, UNC Charlotte
34. Erman Pattuk, 2014, LinkedIn
35. Vishwath Mohan, 2014, Google
36. Brandon Parker, 2014, L3 Communications
37. Saiful Islam, 2014, Microsoft
38. Yangchun Fu, 2015, VMware
39. Jyothsna Rachapalli, 2015, Nutraspace

Current PhD Students of the Core Faculty

Data Security and Privacy

- Fahad Shaon
- Huseyin Ulusoy
- Harichandan Roy

Programming Language and Software Security

- Frederico Araujo
- Gilmore Lundquist
- Wenhao Wang

Systems Security and Malware Analysis

Yufei Gu
Junyuan Zeng
Yafeng Lu

Husheng Zhou
Huibo Wang
Erick Bauman

Control Systems Security and Critical Infrastructure Protection

- Junia Valente
- Mustafa Faisal
- Carlos Barreto
- David Urbina

Cryptography

- Vipin Singh Sehrawat

Big Data Analytics for Security

- Khaled Al-Naami
- Ahmad M Mustafa
- Ahsanul Haque
- Justin Sahs
- Ridwanur Rahman
- M. Solaimani
- Swarup Chandra
- M. Anduleeb Ifthekar

Hardware Security

- Yu Liu
- Mohammad Mahdi Bidmeshki
- Mr. Liwei Zhou

Wireless Networks, Cloud, and Security

- Ashkan Yousefpour
- Hailong Yang
- Panfeng Xue
- Juliette Ugirumurera
- Ke Xu: Wireless QoS
- Shuyang Gu

Network Measurements and Security

- Emrah Cem
- Ahmed Uddin Nazim
- Richard Antiabong