IA/CD/CYBER SECURITY COURSES

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 (EECS). Faculty from the ECS offer courses in the IA 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. IA/CD 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, CISM and Comp TIA Security. 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 IA Education and Research at UTD either as educators, managers/administrators, or project coordinators.

Cyber Security Educators:

1. **Dr. Bhavani Thuraisingham**: [http://www.utdallas.edu/~bxt043000/](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 ten core faculty and several affiliated faculty. She has overall responsibility for IA/CD Research and Education at UTD. She has worked in IA/CD 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 IA/CD 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 IA/CD. Course details can be found on her website at [http://www.utdallas.edu/~bxt043000/](http://www.utdallas.edu/~bxt043000/).

   **Data and Applications Security** (2005 – Present)
   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.

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)**
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)**
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.

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)**
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, file system forensics, web forensics and expert witness and report writing.

**Biometrics (2005)**
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 2014-2015 academic year.

2. **Dr. Kamil Sarac:** [http://www.utdallas.edu/~ksarac/](http://www.utdallas.edu/~ksarac/)
   Associate Professor
   Director of Education, CSI
   IA 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, DoS defense, and e-mail security.

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.

Cyber Security Senior Management/Administrators

The department head of Computer Science and the Dean of Engineering Computer Science have management oversight for cyber security. Their names and links to their CVs are listed below.

3. Dr. Gopal Gupta – Department Head of Computer Science, UTD
http://www.utdallas.edu/~gupta/
Dr. Gupta’s expertise is in Logic Programming. He has also conducted research in buffer overflow detection and was the Director of Cyber Security Education prior to assuming his role as the Department Head in 2009.

4. Dr. Mark Spong – Dean of Erik Jonsson School of Engineering and Computer Science at UTD
http://www.utdallas.edu/~mspong/
Dr. Spong’s expertise is in Control Theory and Robotocis. Prior to joining UTD in 2008 he was a chaired professor at the University of Illinois at Urbana Champaign (UIUC). While at UIUC he was one of those instrumental in establishing the TRUST Institute.

Cyber Security Project Coordinators

Ms. Rhonda Walls and Mr. Bao Tran are project coordinators. Ms Walls is responsible for the day-to-day management of the Cyber Security Institute (CSI). She will be the focal point for the operation of CSI. Mr. Bao Tran used to work extensively on collecting the material for our prior NSA CAE applications. He will continue to review our work and work with Ms Walls. Their names with links to their bio/resume are provided below.
IA/CD CYBER SECURITY FACULTY AND COURSES

At the UTD’s CSI, in addition to the IA/CD faculty Bhavani Thuraisingham and Kamil Sarac listed under 7a, the core IA faculty members in ECS include Murat Kantarcioglu (data security and privacy), Kevin Hamlen (software and language security), Zhiqiang Lin (systems security and forensics), Alvaro Cardenas (control systems security), Yvo Desmedt (cryptography), Yiorgos Makris (hardware security), Zygmunt Haas (wireless network security), and Latifur Khan (data analytics and security). Core IA faculty members from JSOM include Alain Bensoussan, Huseyin Cavusoglu, Srinivasan Raghunathan and Indranil Bardhan.

IA/CD FACULTY AT ECS

1. Dr. Murat Kantarcioglu: [http://www.utdallas.edu/~muratk/cgi-bin/index.php](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](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](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.
   In addition, students are asked to implement role-based access control policies using industry standard access control language XACML.
   Link to homework description:

   **Introduction to Cryptography** (Spring 2011 – 2012)
   [http://www.utdallas.edu/~muratk/courses/crypto12s.htm](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](http://www.utdallas.edu/~mxk055100/NSACAE/crypto-project.pdf)

2. Dr. Kevin Hamlen: [http://www.utdallas.edu/~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 Ph.D. and M.S. degrees from Cornell University, and his B.S. 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)
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.

3. **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)
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)
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 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.


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, SE-Linux, 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 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.

   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](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.

5. Dr. Alvaro Cardenas: [http://www.utdallas.edu/~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)
   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)
   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.

   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/CE7V80S14/](http://www.utdallas.edu/~gxm112130/CE7V80S14/)
   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 run 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.

7. **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/](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](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).

8. **Dr. Latifur Khan**: [http://www.utdallas.edu/~lkhan/](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](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.

IA/CD FACULTY AT JSOM

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 IA/CD related courses include:

Dr. Alain Benssousan [http://www.utdallas.edu/~AXB046100/](http://www.utdallas.edu/~AXB046100/)
Dr. Huseyin Cavusoglu [http://jindal.utdallas.edu/faculty/huseyin-cavusoglu](http://jindal.utdallas.edu/faculty/huseyin-cavusoglu)
Dr. Srinivasan Raghunathan [http://www.utdallas.edu/~sraghu/](http://www.utdallas.edu/~sraghu/)
Dr. Indranil Bardhan [http://www.utdallas.edu/~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/](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 IA 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 IA 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 IA students to take this course.)

IA/CD AFFILIATED FACULTY

Erik Jonsson School of Engineering and Computer Science (ECS)

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

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

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

4. Neeraj Mittal, PhD (University of Texas at Austin) Wireless Networks  
   [http://www.utdallas.edu/~neerajm/](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.

5. B. Prabhakaran, PhD (IIT Madras) Multimedia and Video Analytics  
   [http://www.utdallas.edu/~praba/](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.
6. Edwin Sha, PhD (Princeton) Embedded Systems
   [http://www.utdallas.edu/~edsha/](http://www.utdallas.edu/~edsha/)
   Prof. Edwin Sha does research in embedded systems and has taught cyber security introductory courses both at the undergraduate and graduate level for several years between 2004 and 2011.

7. Eric Wong, PhD (Purdue University) Software Engineering
   [http://www.utdallas.edu/~ewong/](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.

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

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

10. Farokh Bastani, PhD (University of CA at Berkeley) NSF IUCRC
    [http://www.utdallas.edu/~bastani/](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)

11. Michael Baron, PhD (University of Maryland) Statistics Methods for Security
    [http://www.utdallas.edu/~mbaron/](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.

12. Alain Bensoussan, PhD (University of Paris) Risk and Decision Sciences
    [http://www.utdallas.edu/~axb046100/](http://www.utdallas.edu/~axb046100/)
    Prof. Bensoussan 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 IA/CS faculty.

13. Huseyin Cavusoglu, PhD (University of Texas at Dallas), Management Information Systems
    [http://jindal.utdallas.edu/faculty/huseyin-cavusoglu](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 IA/CS faculty.

14. Daniel Krawczyk, PhD (UCLA) Psychosocial Aspects of Security
   [Link](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.

15. Indranil Bardhan, PhD (University of Texas at Austin) Information Systems
   [Link](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.

16. James Bartlett, PhD (Yale University) Cognitive Psychology
   [Link](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.

17. Patrick Brandt, PhD (Indiana University) Political Science
   [Link](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 also plan to investigate security and privacy for GDELT.

18. Matthew Goeckner, PhD (University of Iowa) Math, Physics
   [Link](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.

19. Robert Morris, PhD (Sam Houston State University) Criminology
   [Link](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.

20. Fang Qiu, PhD (University of South Carolina) Geographic Information Sciences
    [Link](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.

21. Prof. Nathan Berg, PhD (University of Kansas), Behavioral Economics
    [Link](http://www.business.otago.ac.nz/econ/staff/berg.html)
    formerly [Link](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.

22. 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 IA/CS faculty.