ISTeC

The Information Science and Technology Center

Colorado State University

Distinguished Lectures

Fall 2017

Colorado State University's Information Science and Technology Center (ISTeC) ***presents two lectures by***

Dr. Moti Yung

Security and Privacy Scientist, Snap Inc., and
Adjunct Research Faculty
CS Department, Columbia University

ISTeC Distinguished Lecture

In conjunction with the Department of Computer Science, and the Department of Electrical and Computer Engineering Seminar Series

"My Business is None of Your Business: Employing Secure Computation for Core Business"

Monday, Sept. 25, 2017
Reception with refreshments: 10:30 a.m.
Lecture: 11:00 a.m.-12:00 noon
Morgan Library Event Hall

Department of Computer Science, and the Department of Electrical and Computer Engineering Seminar Series Sponsored by ISTeC

"Gestalt vs. Constructivism: Designing Blind Cloud Storage in the Real"

Tuesday, Sept. 26, 2017
Lecture: 9:30-10:30 a.m.
Stadium 1204

Abstracts

My Business is None of Your Business: Employing Secure Computation for Core Business

Innovations in security and privacy are critical to advancing modern computing in our time. I will present an effort involving deployment of commercial applications designed and built as a 'secure multi-party computation protocol for specific tasks' to be used repetitively to achieve a number of concrete ubiquitous business goals. In these applications, the outputs are calculated in the presence of privacy constraints which prevent parties from sharing their individual inputs directly and openly. I will also discuss what I think are the reasons for the inherent difficulty of developing such routines in general (for achieving business goals). In particular, I will survey what I believe to be the reasons that for almost 40 years since secure computation protocols was invented as a basic theoretical notion (the third component of modern cryptography), capturing specific and then general computational tasks, and in spite of its theoretical and even more recent commendable experimentation success, the notion has not yet been widely and seriously used in achieving routine relevant business goals by main stream industry (in contrast with symmetric key and public key cryptosystems and protocols, which were the first and second invention of modern cryptography, and were also proposed 40-45 years ago, and are used extensively, primarily to implement secure authenticated channels). I will cover some of the basic methodology taken to deploy the technology.

Gestalt vs. Constructivism: Designing Blind Cloud Storage in the Real

Design of a basic primitives involves specification, and then designing and implementing it. The foundations of systems approach, typically implies that the specification and design have to capture the primitive in its entirety (analogous to the abstract concept of Gestalt applied in art and science). Therefore the designer needs to capture all functions (correctness properties) and safe operation (security and privacy properties) based on the complete picture. In actuality, often one needs to retrofit a primitive into a live and existing system; this aspect captures the fact that systems are to be kept alive, the process of securing systems is ongoing, and engineering constraints exist in the real world while new functions need to be supported. As a result, in reality one has to design security primitives and understand them based on relations among existing and new components (analogous to the concept of Constructivism). In the classical body of knowledge of security the Gestalt approach and designing from the start dominate, and is strongly advocated, but in the reality of system building the opposite is true.

The speaker will demonstrate the specification and the design of Snapchat's cloud memory which was introduced into the system with the main privacy goal of hiding the content from the server itself. This is an example of design in practice vs. design foundations. The existing component, the approach, and the novelty will be covered, and explained.

Speaker Biography

Dr. Moti Yung is a computer scientist whose main interests are in cryptography, security, and privacy. He is currently with Snap Inc. Yung earned his Ph.D. from Columbia University in 1988. He worked at IBM Research, was a vice president and chief scientist at CertCo, and was director of Advanced Authentication Research at RSA Laboratories, and a research scientist with Google. He holds an adjunct faculty appointment at Columbia University where he co-advised several Ph.D. students over the years. He has served as consultant to leading companies and to open projects with various governments as well. Yung's major interests are building strong useful foundations for the field based on practical needs and reality of systems, and, on the other hand, transforming theoretical ideas into practice. He has contributed extensively to numerous new cryptographic ideas, foundations, techniques, protocols, and systems, and to new central notions like encryption, signature, and protocols (one example is innovating the notion of public key cryptosystems secure against chosen-ciphertext attack -- currently a major requirement from public-key encryption operating on the Internet). He has also contributed to innovative security and privacy industrial constructions embedded in actual large scale systems and networks. Examples of the latter are IBM's SNA network authentication, the Greek National Lottery system, the security and privacy aspects of Google's global systems such as the Ad Exchange (ADX), Google private Ads attribution based on off line user activities, and Snapchat's cloud storage security). He also predicted innovations that were later adopted by business (like "social based authentication for account recovery"). Further, his interest in the subtlety of the notion of "trusted systems" has led to predicting what is known as ransomware, and predicting the crypto subversion attack vector: a deniable algorithm substitution attacks on cryptosystems (which was allegedly mounted within the deployed American Federal Information Processing Standard detailing the Dual_EC_DRBG). He is a fellow of the ACM, IEEE, IACR, and the European Assoc. for Theoretical Computer Science (EATCS), and a recipient of ACM's SIGSAC Outstanding Innovation Award.

To arrange a meeting with the speaker, please contact Prof. Indrajit Ray (Indrajit.Ray@colostate.edu).

Upcoming Distinguished Lectures

Oct. 16

"Tracing the Arc of Smartphone Application Security"

11:00 a.m.-12:00 noon

Morgan Library Event Hall

Dr. Patrick McDaniel

Oct. 30

"Large-Scale Machine Learning and AI: A Cross-Industry Perspective"

11:00 a.m.-12:00 noon

Morgan Library Event Hall

Dr. Ashok Srivastava

ISTeC (Information Science and Technology Center) is a university-wide organization for promoting, facilitating, and enhancing CSU's research, education, and outreach activities pertaining to the design and innovative application of computer, communication, and information systems. For more information please see ISTeC.ColoState.edu.