SCHOOL OF COMPUTER SCIENCE
Faculty Candidate

Raluca Ada Popa
Massachusetts Institute of Technology

Building Systems that Compute on Encrypted Data

Theft of confidential data is prevalent. In most applications, confidential data is stored at servers. Thus, existing systems naturally try to prevent adversaries from compromising these servers. However, experience has shown that adversaries still find a way to break in and steal the data.

In this talk, I will describe a new approach to protecting data confidentiality even when attackers get access to all server data: building practical systems that compute on encrypted data without access to the decryption key. In this setting, I designed and built a database system (CryptDB), a web application platform (Mylar), and two mobile systems, as well as developed new cryptographic schemes for them. I showed that these systems support a wide range of applications and incur low performance overhead. The talk will focus primarily on CryptDB and Mylar.

My work has already had impact: Google uses CryptDB's design for their new Encrypted BigQuery service, and a medical application of Boston's Newton-Wellesley hospital is secured with Mylar. Looking forward, this approach promises to solve confidentiality problems in other settings, such as big data systems, genomics processing, and machine learning over sensitive data.

Bio:
Raluca Ada Popa is a PhD candidate at MIT working in security, systems, and applied cryptography. As part of her PhD work, she built practical systems that compute over encrypted data as well as designed new encryption schemes that underlie these systems. Raluca is the recipient of a Google PhD Fellowship for secure cloud computing, Johnson award for best CS Masters of Engineering thesis from MIT, and CRA Outstanding undergraduate award from the ACM. Raluca received her undergraduate degree from MIT with two BS degrees, in computer science and in mathematics.

Thrusday, March 27
1:00 p.m. GHC 6115

Host: David Anderson

Contact: Kathy McNiff (kmm@cs.cmu.edu, x8-5099)