CIS600: Cryptographic Engineering

MW 10:35-11:55 am, Link 211, Spring 2017

Course description

The course is designed for future cryptography engineers (and scientist). The course theme is to empower students with skills of correctly using cryptographic libraries and building proven secure applications. The course outcome includes:

1. deep understanding of security properties of cryptographic primitives/protocols (e.g. hashes, PKE),
2. hands-on experiences on correctly using (w.o. misuse) cryptographic libraries (e.g.**NaCL**),
3. knowledge about real usage of cryptography in security applications (e.g.**blockchain**, **Intel SGX**).

The course covers all three aspects in a systematic way (see the course schedule). Note this course does*not* cover as much the mathematical construction of pritimives (e.g. internal working of SHA256).

Instructor

Dr. Yuzhe Tang Office: CST 4-184, [http://ecs.syr.edu/faculty/yuzhe]

Textbook

Recommended *Introduction to Modern Cryptography* (2nd edition), Jonathan Katz and Yehuda Lindell
Cryptography Engineering: Design Principles and Practical Applications 1st Edition, Niels Ferguson, Bruce Schneier, Tadayoshi Kohno.

Grading

Lab/Exercises (40%), Presentation (30%), Exams (30%)

Schedule

0. Introduction to modern cryptograph

- Crash course on probability theory
- Principles of provable security and perfect secrecy

1. Private-key cryptography

- Crash course on complexity theory
- Symmetric key encryption and computational security: Block cipher, AES
- Message authentication code, hash and commitment

2. Public-key cryptography

- Crash course on number theory
- Public-key encryption: RSA, DH, Digital signatures
- The NaCL ("salt") crypto library

3. Security applications and protocols

- The case of password management
- The case of block-chain and certificate transparency
- Attestation protocols and the case of Intel SGX
- The Kerberos authentication protocol
- Tthe case of Tor project