COT 5428 Formal Foundations for Cybersecurity

Catalog Description
Formal models and methods for achieving rigorous security guarantees. Cryptographic indistinguishability properties, reduction proofs. Formal analyses of security APIs. Secure information flow. (3 credits)

Prerequisites
CIS 5370 Principles of Cybersecurity

Type
Required for MS in Cybersecurity

Course Objectives
This course focuses on formal models and methods for security analysis, with the goal of discovering precisely what is (and is not) guaranteed by various security technologies. For instance, we will study reduction proofs showing that certain cryptosystems built from AES satisfy IND-CPA ("indistinguishable under chosen plaintext attack") security; remarkably, such cryptosystems cannot be deterministic. Students will get hands-on experience with the automated ZooCrypt tool for analyzing cryptosystems. The formal approach to cybersecurity will be explored in a variety of other settings, including security APIs, secure information flow and quantitative information flow.

Topics
- Cryptography
- ZooCrypt
- Security APIs
- Secure Information Flow
- Quantitative Information Flow

Textbooks
Mihir Bellare and Phillip Rogaway, *Introduction to Modern Cryptography*
http://cseweb.ucsd.edu/~mihir/cse207/classnotes.html

Gilles Barthe, Juan Manuel Crespo, Benjamin Grégoire, César Kunz, Yassine Lakhnech, Benedikt Schmidt, and Santiago Zanella-Béguelin, *ZooCrypt: Fully Automated Analysis of Padding-Based Encryption in the Computational Model*
http://easycrypt.gforge.inria.fr/zoocrypt/

Riccardo Focardi, Flaminia Luccio, Graham Steel, *An Introduction to Security API Analysis* http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/FLS-fosad11.pdf

Geoffrey Smith, *On the Foundations of Quantitative Information Flow*
http://users.cis.fiu.edu/~smithg/papers/fossacs09.pdf

Last Update
Geoffrey Smith, 1/22/2014.