Topics for Midterm, Spring 2020

Security Basics
  Problems with Provable Security
  Social Engineering
  Risk Mitigation
  Kerckhoff’s Principle
  Vulnerability Disclosure
  Security vs. Privacy
  Passwords
  Classes of Attacks and Countermeasures

Cryptographic Protocols
  Authentication Protocols
  Man-in-the-Middle Attacks
  Reflection Attacks
  Chosen Protocol Attacks
  Key Management Strategies
  Kerberos
  BAN Logic
  Pseudo-Random Number Generation
  One-way Functions
  Symmetric Key Cryptography
  Modes of AES
  Weaknesses in the use of AES
  Public Key Cryptography
  RSA in Practice
  Diffie-Hellman Key Exchange
  Elliptic Curves in Practice
  Digital Signatures
  PKI

Software Security
  Password Cracking
  System-level Authentication Mechanisms
  Filesystem Security