Security Education in U of Minnesota

Yongdae Kim
U of M Security Program Overview

Faculty Members

- Nick Hopper: privacy, crypto, information hiding
- Yongdae Kim: distributed system security, applied crypto
- Andrew Odlyzko: crypto, security economics

Classes

- F08 – CSci 5271: Intro. to computer security
- S09 – CSci 5471: Modern Cryptography
- F09 – CSci 8271: Security and Privacy in Computing
Privacy and Information Hiding

Anonymity hides who connects to whom.

In what sense is a TOR connection anonymous?

Can we build something provably better?

Watermarks “protect” digital goods

Many people think secure digital watermarking is impossible

Can we prove it?
System Security

Distributed System
- P2P, MANET, SensorNet, Internet, and BotNet!
- Skype, DNS, BitTorrent, eDonkey
- Example
  - How much resource is required to shutdown 1M nodes eDonkey network?
  - How to detect zombies in Botnet?
  - How can we design robust routing protocol?
    - 10% faulty nodes for 5,000 nodes network ⇒ Only 30% message delivery

Storage System
- Why do we still have endless security breaches?
- Usability/Manageability
- How can we provide confidentiality and integrity efficiently with ever growing storage?
  - Key management
- How long must the data be secured? Often 30 years!
CSci 5271: Intro

* Introduction to Computer Security
* An introductory graduate course
* Cover a broad variety of elementary topics in security
  - Focusing on the scientific principles involved in various security technologies
  - Rather than the specifics of any particular technology.

* Goals
  - "think like an adversary"

* Prerequisite: Completed an undergrad CS major
  - Undergrad OS
  - Write and debug with C/Java
CSci 5271: Textbook

* Textbooks

- Ross Anderson's "Security Engineering"
- David Wheeler's "Secure Programming for Linux and Unix."
- Schneier and Ferguson's "Practical Cryptography,"
- Manzezes, Van Oorschot, and Vanstone's "Handbook of Applied Cryptography"
CSci 5271: Topics

* Computer Security
  - Control flow vulnerabilities, Defensive programming, Access control, Trustworthy OS, DB Security

* Network Security
  - Crypto, Web/Internet security, IDS, Malware, DoS, Privacy, DRM, Voting
CSci 5471: Intro

- Modern Cryptography
- Introductory grad course on cryptography
- theoretical foundations and practical applications

Prerequisite
- Discrete math
- Have evaluation test on the first day

Topics
- Introduction, Math, Symmetric Ciphers, Hash Functions, Public Key Encryption, Digital Signatures, Identification, Key Establishment
CSci 5471: Other Info

🌟 Textbook

- Menezes, Van Oorschot, and Vanstone's "Handbook of Applied Cryptography"
- Mao's “Modern Cryptography”
- Schneier's “Applied Cryptography”
- Katz and Lindell’s “Introduction to Modern Cryptography”
- Stinson’s “Cryptography: Theory and Practice”

🌟 Course format

- Biweekly quiz/homework, Final exam, Project
CSci 8271

- Security and Privacy in computing
- Graduate course on security
- Understanding state of art in security research
- Reading 40 ~ 60 papers
- 2/3 of lectures is presented by students.

Topics
- P2P/Storage/Routing/VOIP security, Privacy, Cool attacks
QUESTION?
kyd@cs.umn.edu