Exam Review

CS 558: Advanced Computer Security

Dong (Kevin) Jin

Final Exam

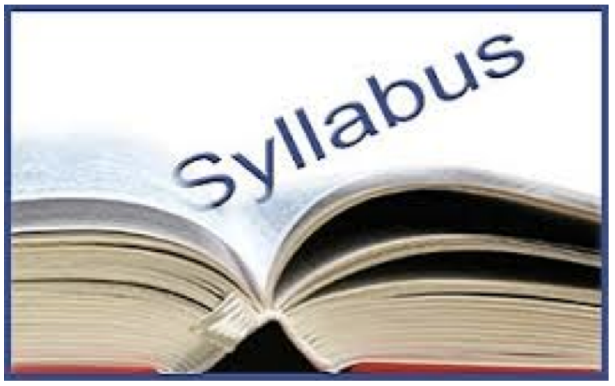
- Time: 5/1, normal class period
- Location: same as the lecture room

- Exam ground rules:
  - Two sheets of notes will be allowed.
  - You can write on both sides of the note page.
  - Otherwise the exam is closed book.
  - No calculators will be allowed.

- Covering all topics in the lectures. You will need to review the lecture materials, such as lecture slides, papers, piazza discussions, etc.

Course Syllabus

- DoS
- SDN
- Critical Infrastructure Protection
- Machine Learning and Applications in Malware Detection
- Spam
- Malware (virus, worm, botnet)

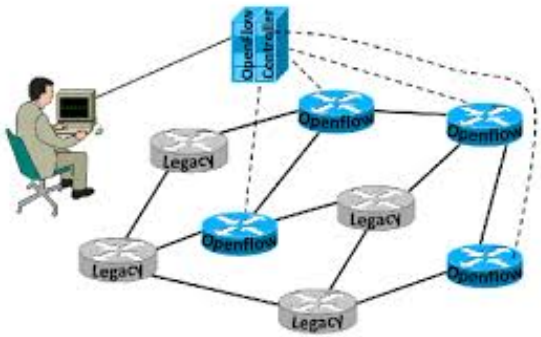


DoS

- What is DoS?
- Why are DoS attacks hard to defend against?
- DDoS Attack Taxonomy
  - Degree of Automation, Scanning Strategy, Propagation, Exploited Weakness, Source Address Validity …
- Defense
  - Filtering-Based and Proof-Based (e.g., SYN cookie, ASV …)
- Paper
  - ASV, Backscatter analysis

SDN

- Why do traditional networks fall short?
- What is SDN?
- OpenFlow and SDN applications
- What benefits and challenges does SDN bring?
- Paper
  - VeriFlow (three steps)
  - Topology tampering attacks



Critical Infrastructure Protection

- Critical infrastructure + advanced computer and network technology
  - More Efficient or More Vulnerable?
  - Interdependency of Systems
- 2003 Blackout
  - Root cause
  - Cyber-Security Dimension
- Stuxnet
  - How Stuxnet Worked
  - Tech Overview
- Advanced Metering Infrastructure
- Paper
  - Stuxnet
  - Cyber attack on the Ukrainian power grid

Machine Learning and Applications in Malware Detection

- Hidden Markov Models
  - The three problems
- Signature detection not work for metamorphic malware
- Signature-based vs anomaly detection
- Malware Detection/Classification
  - HMM
  - K-Means
- Papers
  - HMM
  - Microsoft malware classification challenge

Spam

- Both Unsolicited and Bulk
- Why spam is a problem?
- How do spammers conceal their identity?
- Countermeasures
  - Spam filter, blacklisting/graylisting, DomainKeys, SPF, SpamTracker
- Paper
  - Email spam (Spamalytics)

Malware

- Set of instructions that cause a system's security policy to be violated
  - Virus
  - Worm
  - Botnet
    - motives and analysis techniques
    - architectures and strategies
- Malware Detection
  - Signature detection
  - Change detection
  - Anomaly detection
- Distributed Hash Tables (DHT)
- Paper
  - Centralized Botnet (Torpig takeover and analysis)
  - P2P Botnet