Exam 2 review

Bo Luo
bluo@ku.edu

Exam 2

- Time: Tuesday April 30
- Closed book, closed notes
- No electronic devices!
- Two-page cheat sheet allowed. Letter size, double sided.
- 35% of the final grade

Exam 2

- Format
  - Multiple choice
  - Short answers: security analysis, etc.
  - Security analysis: find security issues in a design, and suggest solutions
- Coverage
  - Software and OS security (about 25%)
  - Network security (about 40%)
  - IDS (about 10%)
  - Privacy (about 20%)
  - Cloud computing security (about 5%)

一大题+判断或多选

重点

一大题+判断或多选

Software Security

- Basic concepts
  - What is a secure program? Means different things to different people
  - Terminology: error, fault, failure 3 个概念
- Software flaws (non-malicious) 怀有恶意的
  - Validation errors 4 个
  - Domain errors
  - Buffer overflow
  - TOCTTOU

Software Security

- Malicious software 怀有恶意的
  - Trojan Horses
  - Viruses, virus detection
  - Worms, worm distribution
  - Rootkits
- Malware controls 恶意软件
  - Developmental controls
  - OS controls

OS Security

- OS: still software
  - All software security vulnerabilities still apply
  - tradeoff between: Sharing and Protection
- OS must protect users from each other
  - memory protection
  - file protection
  - general control and access to objects
  - user authentication

OS Security

- OS protection – separation.
- Levels (types) of protection
- Memory protection
  - Protecting OS kernel
  - Process isolation
  - Access control (general objects)

Network Security

- Threats
  - Threat precursors 前兆
  - Wiretapping 搭线窃听
  - Packet Sniffing: why? How?
  - Spoofing 滑稽模仿
  - DDoS
  - UDP echo-chargen
  - smurf
  - Syn-flood
  - etc.
  -

Network Security

- Controls
  - Design: separation, single point of failure, redundancy, recovery
  - Encryption: link vs. end to end
  - Protocols:
    - SSL/TLS: SSL sequence: negotiation, key exchange, authentication, session
    - SSH: Similar to SSL, No certificates!
    - ~~IPSec~~
  - **Firewall: why? How? What can/cannot be protected**
  - IDS and Honeypots: know the concept

Case 1 won't be able to block the infected computer from sending information to the server. Case 1 won't be able to block the trojan horse from spreading in the local network.

Case 2 depends on the port that is used by the trojan horse. If it uses a popular port (e.g., port 80 for HTTP), it won't be blocked by the firewall. Otherwise, the firewall may be able to block the trojan horse from sending information to the server. The firewall won't be able to block the trojan horse from spreading in the local network.

Network Security

- Applications
  - Web Security
    - Phishing 网络诱骗
    - SQL Injection
    - Cookies and cross-site scripting
  - Email security
    - ~~S/MIME~~

IDS

- Intrusion & intruder behavior
- IDS
  - Sensors, Analyzers, UI
- Detection quality
  - Base rate fallacy
- IDS approaches
  - Anomaly detection, Signature detection
- IDS vs. firewalls
- ~~Big data analytics and security intelligence~~
  - You only need to understand the first 33 slides of IDS

Privacy

- What is privacy?
  - Definitions
  - Common practices
- Data privacy
  - Why? How?
  - *k*-anonymity (how to achieve?)
  - *l*-diversity (know the concept)
  - ~~Differential Privacy~~

Privacy

- Anonymous network
  - Chaum's MIX
  - Random routing
    - Onion routing
    - ~~Crowds~~
  - Dining cryptographers
  - Yau's millionaire problem (know the concpet)
    - ~~FairPlay~~
  - ~~Record linkage and PPRL~~