Possible Research Topics for CAP6135 Term Project

(There are much more interesting topics. You can choose any topic that is related to computer security)

1. In-depth tutorial on recent cybersecurity incidents (such as Sony hack, Target breach, Stuxnet…..)
2. Internet-of-Things security and privacy
    a. Existing IoT security breach
    b. Research on hardware and software security vulnerability of IoT
3. Wearable IoT/medical devices security and privacy
4. Security and privacy issues in smartphones
    a. Jail breaking in iPhone
    b. Worm propagation in smartphone: propagation theory, previous incident case study, etc.
    c. Bluetooth security issue in smartphones
    d. Vulnerability in smartphone-based payment system
    e. Vulnerabilities brought by downloaded apps; unnecessary privilege or privilege elevation in downloaded apps.
5. Social network security and privacy
    a. Social network based malware, such as previously appeared malware Boonana, Samy, RenRen, Koobface, and SpaceFlash.
    b. Spam in social network, such as in twitter network
    c. Privacy vulnerability and protection; such as Facebook privacy problem, Google circumventing Sofari privacy protection incident
6. Reputation assurance for online user reviewing system. How to make user reviews reliable against malicious attackers or bots (such as fake review to boost a product), or defend online gaming servers from automated bots
7. Botnet modeling, attack method, defense (real case study, monitoring real botnet, peer-to-peer botnet)
8. Cloud computing security and privacy
    a. Virtual machine security: such as prevent information leakage among different users on the same VM or on the same physical host.
    b. Cloud data encryption. How to encrypt data on cloud so that the cloud provider cannot read the data and: (1). it can still be searched by client, (2) it can be shared by multiple users with efficient secure key management; (3). It can still support cloud provider to efficiently save storage by merging the same data together.
    c. How to spread malware in cloud; how to defend malware in cloud environment
9. DNS security:
    a. DNS hijacking attack and defense
    b. DNS Poisoning attack and defense
    c. Case study of previous appeared DNS attack incidents
10. Email spam and phishing defense
    a. Spam detection, filtering

    b. Phishing attack defense
11. Wireless networking security
    a. Ad hoc network secure routing
    b. Reputation system for wireless networking
    c. Vehicular networking security and privacy
    d. Security and privacy protection in location service in wireless networking (such as among smart phone users)
12. Personal body area network security and privacy (for example, peacemaker security issue)
13. Wireless ad hoc network or sensor network security
    a. Secure routing protocols
    b. Detection of malicious nodes
14. Location service security and privacy (such as how to protect user's privacy when the user uses a location service such as from iPhone)
15. Web security
    a. Detection of malicious web sites (for example, by using crawling and honeypots)
    b. Detecting of phishing/fake websites
    c. Detecting malicious code injection
    d. Verifying security for all web plug-ins or extensions
    e. Browser history or cookie security issues and protection
16. CAPTCHA security
    a. Image-based CAPTCHA, video-based CAPTCHA
    b. Improving text-based CAPTCHA
    c. Defense against CAPTCHA human-solver attack
17. Software testing and security
    a. Automatic software (source code or binary code) security analysis and testing
    b. Formal model to detect bugs in source code
    c. Tainted analysis for runtime vulnerability
    d. Sandboxing
    e. New attacks and defenses against buffer overflow, heap overflow
18. RFID security and privacy
    a. Privacy protection in RFID systems
    b. Security protocols for RFID systems
    c. Real attacks against car key, gas station remote key, etc.
19. Authentications
    a. New password authentication system (such as two-factor password, hash-based password)
    b. Biometric authentication system's security problems and defense
20. Hardware or physical security
    a. Low-level device (such as network card, Bluetooth device driver) based malware
    b. Side-channel attacks (such as obtaining password/information based on sound of keyboard, computer screen light, memory chip, etc)
21. Database security

    a. SQL injection
22. Computer architecture based security
    a. Secure CPU design
    b. Secure memory design (e.g., each memory byte has a security bit support)
    c. Secure cache design to defend against side channel attack
23. Peer-to-peer system security
    a. New attack methods against existing p2p protocols such as bitTorrent
    b. Security issues in p2p video streaming
24. Network security
    a. Defense against distributed denial-of-service attack
    b. BGP router security
    c. Network traffic-based monitoring and attack detection
    d. Stepping stone identification
25. Anonymity
    a. Privacy-preserving data sharing
    b. Attacks against various anonymity protocols and systems
    c. Design of new/improved anonymity protocols
26. Black market study of hackers