Pick one of the following topics (one per student, first come first served).

Write a paper (minimum 2, maximum 5 pages, excluding references) on the topic that you have chosen, using the supplied template. The poster template is also provided for you.

At the end of your essay, list the resources that you have referenced. Do use accountable references such as articles, journals, books, research papers, and trusted websites such as ".gov" ".edu" ".org" etc. DO NOT use Wikipedia or such. Libraries and Google Scholar may be good starting points.

We expect to see the following important explanations in your paper:

- Problem definition & motivation
- Solutions in detail
- Comparison with other solutions if there are any.
- Evaluation (explain your findings, data that you have, or things that reader should know to understand the solutions)
- Conclusions: What did you learn from this project, which part was the hardest, which knowledge that you learned in class helped you with the project? Any feedback that you would like to provide also goes here.

Your poster needs to be legible, nice-looking, and must summarize the most important aspects of your problem and solution, in an eye-catching manner. Use the template that is provided.

TOPICS:

1. MALWARE-BUSINESS: Write a term paper that discusses the business model for adware. Use articles you can find on the web or library. Include the risks, benefits and costs for advertisers, adware designers, the people who run adware services, and victims.
2. PHISHING: For your term paper, collect enough spam e-mails for yourself and friends in order to find five phishing web sites. Compare the contents of these pages with their authentic counterparts, both in terms of HTML source and the look and feel of the pages as displayed in the browser. Add protection methods against phishing attacks based on your

analysis in your term paper. Please explain why or why not a user can perform a phishing attack if the client is using HTTPS, and possible attack techniques. Include some of the current techniques being employed against phishing.

3. CRYPTO: Discuss multiple problems associated with the implementation of cryptographic protocols. Especially focus on frequent errors where care must be taken to prevent insecurity. Use real problems related to the use of, for example, RSA, AES, El-Gamal, for encryption or signing. Use academic references.

4. SOCIAL: Write a term paper which includes all security risks that are possible in social networking websites and what the countermeasures are. Note that some networking websites provide mechanisms for users to determine the GPS coordinates of where their friends are located at any given moment. Describe some security and privacy risks that this technology presents. Do not limit your analysis and discussion to this scenario.

5. VOTING: Write a term paper that discusses key security properties that any computer voting scheme should have. Analyze some popular voting schemes in terms of their security along these lines.

6. SPAM: Write a term paper that (based on the use of an email account that regularly gets spam) classifies and categorizes the spam the account gets in a week. Categorize the spams in terms of similar goals or patterns and describe in qualitative terms the objective of the spam in each category, that is if possible, whether it is for a product, phishing attack, etc. Collect information to analyze the spam economy, and discuss the benefits to various benefactors.

7. IDS: Keep a diary that chronicles how you use your computer for an entire week. Try to include all the key elements that are included in an intrusion detection event log, including which files you read and write, which programs you run, and which web sites you visit (Your browser probably keeps a history of this last set of events itself.) Write a term paper that discusses, at high level, the types of rules and statistics that could be used to build an intrusion detection system for your computer that could tell if someone else was using it besides you. Include a discussion of how easy or difficult it is to predict normal and anomalous behavior for your computer based on your usage patterns for this week. Compare your findings with some existing IDS products.

8. BUFFER OVERFLOW: In the *StackGuard* approach to solving the buffer overflow problem, the compiler inserts a *canary* value on the memory location before the return address in the stack. The canary value is randomly generated. When there is a return from the function call, the compiler checks if the canary value has been overwritten or not. Do you think that this approach would work? Why or why not? Explain, or give a counterexample. Another approach to protecting against buffer overflows is to rely on *address space layout randomization* (ASLR). Most implementations of ASLR offset the start of each memory segment by a number that is randomly generated within a certain range at runtime. Thus,

the starting address of data objects and code segments is a random location. What kinds of attacks does this technique make more difficult, and why?

9. SPYWARE: Explain why a spyware infection that collects mouse moves and clicks, without also performing screen captures would not be very useful for a malware author to implement. Then, continue your discussion using different types of spyware, or other spying techniques that rely on hardware instead of software. Next, consider solutions to these attacks. In particular, suppose you want to use an Internet café to login to your personal online banking account, but you suspect that the computers are infected with keyloggers. Use a web browser and a text editor together, so that you may somehow type your user name and password securely. Your solution must resist a keylogger that does not perform screen captures or mouse event captures. The attacker must not be able to learn your user name or password. Keep your solution as simple as possible, as long as it is secure.

10. MALWARE-PROTECTION: Discuss how you would handle the following situations:

    a. You are a system administrator who needs to defend against self-propagating worms. What are, at least three, things you can do to make your users safer?

    b. You have suspected the existence of a polymorphic virus on your system. What are some steps that you can take to correctly identify it, during infection or propagation?

    c. You suspect you may have a rootkit installed on your system that is telling the music company whether or not you are violating copyrights with an audio CD you recently bought. How might you detect this intrusion without any outside tools?

    d. If you are a virus writer, name, up to four, techniques you would use to make your virus more difficult to detect.

11. PASSWORDS: Write a term paper about the (in)security of password-based authentication and dictionary attacks. Comparatively analyze any alternative authentication methods that you find, in terms of their security and usability. Read and very briefly summarize some research papers that make password-based authentication secure.

12. WEB ATTACKS: Design client-side systems for defending against CSRF and click-jacking attacks, as well as modifications for ActiveX to make it more secure.

13. COOKIES: Write a term paper that describes the privacy and legitimacy concerns of cookies. Use a web browser (or add-on) that allows you to examine the cookies your browser stores. Begin by deleting all current cookies, and then visit popular news, shopping, social networking, or other favorite sites of yours. Determine what information the cookies set by each site holds, and write about security and privacy implications.

14. PHYSICAL SECURITY: You want to plant a bug in Company X's office to acquire business intelligence because they are a competitor. The package needs to get into their server room and get hooked up to sensitive hardware. You know the complex hires several guards from a private security company that regularly patrol and check for authentication by using well-known badges. You know that they regularly outsource several functions including janitorial staff, pest control, and purchasing IT equipment. These jobs have a high turnover rate, but require authentication in order to get access to the premises in the form of a work order for IT supplies and pest control. The janitorial staff is a recurring service, but with a lower turnover rate. They are also periodically inspected by officials, but are usually provided with advanced notice of their arrival. What is your high-level plan of action? A guard challenges you when you enter how do you continue your mission? What is your story? Why is this a good plan? What are your options for acquiring access to sensitive areas? If you realize you are a target of this attack, how will you defend against it?

15. PASSPORT: Passports are printed on special paper and have various anti-counterfeiting physical features. Develop a print-your-own passport pilot program where a passport is a digitally signed document that can be printed by the passport holder on standard paper. You can assume that border control checkpoints have the following hardware and software: two-dimensional barcode scanner, color monitor, cryptographic software, and the public keys of the passport-issuing authorities of all the countries participating in the pilot program. Describe the technology and analyze its security and usability. Is your system more secure than traditional passports? Compare your solution with currently existing passport technologies.

16. RFID: Write a term paper that discusses the different kinds of RFIDs including both self-powered and not. Address privacy concerns raised by wide-spread RFID use, such as in electronic passports, electronic ID cards, and inventory management. Use research articles as your main sources, and list any solutions and open problems that you find.

17. OPEN SOURCE: Choose a piece of open source software with published vulnerabilities. After downloading the source code, identify the vulnerable code and develop a security advisory describing the bug, its security, and any information necessary for implementing a solution.

18. DRM: Write a term paper that compares and contrasts the needs of digital content providers to protect their rights to a fair compensation for the user of their work with the various restrictions possible using the DRM technology. Include discussions of the conflicts of fair use and possible rights revocation. Your discussion should cover multiple aspects, such as music, movie, game, and news industry.

19. EMAIL: What are the comparative benefits of blacklisting and greylisting of emails? Also discuss the use of secure email that is signed and encrypted. In this discussion, pay special attention to S/MIME and explain whether or not the following properties are provided, and why. If it is not provided by S/MIME, explain how to provide it via other methods.

a. Confidentiality: Only the recipient can read the message.

b. Integrity: The recipient can detect changes to the message.

c. Sender identification: The recipient is assured of the identity of the sender.

20. ANONYMIZATION: Do an experiment involving the use of additive noise for protecting a database from inference attacks. Your database should begin by generating a specific list of values that have a mean of 25. Then, anonymize these values by adding a random noise value, which is designed to have an expected value of 0. For example, you can use uniformly distributed noise in the range [-1,1] or use a Normal (Gaussian) noise with mean 0. Test this anonymization method for a database of 1000, 10000, 100000 values with different noise. Document your observations. Then, read about “k-anonymity” and also “differential privacy”. Compare these two approaches with each other, and with your approach. Explain the benefits of each, and possible privacy and usability (functionality) implications.

21. SOCIAL NETWORKING: Learn about security and privacy properties of both centralized social networks (e.g., Facebook, Google Plus, Twitter, LinkedIn) and decentralized ones (e.g., Diaspora). Pay special attention as to where they employ cryptographic techniques versus non-cryptographic ones. What type of trust is needed to be assumed for the privacy of the user to be satisfied? Write a comparative study regarding different security and privacy measures taken by several such social networks.

22. FORENSICS: Attempt to trace the evolution of computer crime over time. Extrapolate and predict the new exploits that are to be expected in the next 20 years. Detail your prediction methodology and your past dataset.

23. DEFENCES: Choose one or more secure networking technologies (Firewall, VPN, IDS etc), explain which attacks it/they mitigate and how the risk of a successful attack is diminished. Also explain the security issues that remain open, in spite of the available security measures.

24. CRYPTOCURRENCIES: Choose at least 5 well-known cryptocurrencies, compare and contrast them in terms of usage differences, security infrastructure, and vulnerability to common threats, such as double spending, account and coin theft, etc. Do not simply focus on economics, focus on security instead.

25. WALLETS: Consider at least 3 common wallet programs and at least 3 common companies for the cryptocurrency trade market. Compare and contrast their security against each other in terms of the common threats, such as double spending, account and coin theft, etc. Also, compare and contrast using a wallet program and company for security, usage, etc. Consider recent infamous attacks.

26. CONSENSUS ALGORITHMS: Compare and contrast Proof of Work, Proof of Stake and Byzantine Fault Tolerance consensus algorithms by taking into account their use in

blockchain in terms of their security against common attacks, decentralization, usage, and efficiency.

27. MACHINE LEARNING: Survey and identify the issues in the current machine learning and artificial intelligence technologies related to security and privacy. Also, discuss current trends for defences against the possible threats. Make sure that your focus is the application of machine learning for security.

28. GAME THEORY: Survey and identify at least 3 applications of game theory related to computer and network security. For each of them, show how game theory and mechanism design improves efficiency in contrast to cryptographical guaranteed approaches.