Final Project

Due date: **Wednesday, 5/6/2020** at midnight (final report)

Preliminaries

You will choose to do a project from one of the following categories: (a) implementation, and (b) literature survey.

For the implementation project we will use one of the SEED labs, which is the Virtual Private Network (VPN) Lab, based on the TLS/SSL protocol. This lab is a good combination of what we have learnt in this course, since it covers several important concepts and tools. The detailed description and guidelines will be posted in D2L.

A literature survey project involves researching into a topic of interest of your choice (within information and network security), and write a survey paper on this topic. The survey paper needs to involve all necessary components of a typical research survey, i.e., introduction to the background and motivation, statement of the research problem(s), survey of the state-of-the-art (summarizing the idea and results of major existing works/solutions, from classical ones up to the most recent results), and analyze/compare the advantages/disadvantages of current approaches, analyze the open problems/challenges (with your own opinion) and suggest future research directions (discuss how you may solve them). Typically, to write a good survey, you are expected to read 5-10 published technical research papers in depth.

Note that, you are encouraged to choose the literature survey option if you are a graduate student (Ph.D. student or a Master student with thesis option), and you are encouraged to combine this effort with your current research.

You can work on teams of two people of your own choosing, or you may also work on your own if you wish to. Regardless of project type, you are expected to generate a final report. Selected projects will be invited to do a final in-class presentation to showcase your findings.

The project Timeline and Important Dates

- *Final Project Report*: Please start doing your project once you have determined the topic (and you should decide before April). If you have doubts about the topic (especially the survey option) please contact the instructor. Final report is due **Wednesday, 5/6/2020 at** midnight.

- *Presentations* will take place on the last week of classes. This year we will use zoom meetings due to the coronavirus situation. Approximately 6-9 projects in total will be selected for presentation due to limited time slots (about 15 minutes each). Presentations will not be graded, but may impact the assessment of your term paper.

Note that: You must work on and write your own project independently (individually, or as a team). The *maximum team size is two*.

Extra credits: there will be at most 10% bonus points for the project if you have done a beautiful job in aspect!

Implementation Guidelines

The detailed description and guidelines will be posted in D2L. If you work as a two-person team, you need to finish all the 6 tasks. If you work alone, then only finish tasks 1-5.

You will need to submit a final report, containing the description of your design, and implementation codes used for experimentation, as well as experimental results from each task (such as screenshots, figures or tables), along with your own analysis of the results. You should also describe how you test the functionalities and security of your system. In the end include a conclusion of what you have learnt in this project (experiences, findings, or even surprises). Also, in your appendix, please include a description of the organization of your code, platform, and how to compile & run your code. You should also append your code to the report.

Special NOTE: there is NO need to demonstrate your system to us (overriding the submission instructions in the lab description file), since we don't have a TA, and this semester everyone is working remotely which creates logistic challenges. Therefore, you should include as many details as possible in your lab report to prove you have successfully implemented all the tasks, for example, including step-by-step description of what you did, and screenshots in each step to demonstrate the process.

Grading: Your grade will be judged on the completeness and correctness of your implementation (30%), the completeness, correctness and quality of presented results (40%), and the overall quality (e.g., organization, and readability) of your final report (30%).

Literature survey guidelines

Paper Format: The paper should be at least 6 pages, at most 12-pt font size, and single-column single-spaced (OR at least 5 pages, 11-pt font size and double-column using IEEE journal template). Preferably written using Latex and hand in a PDF file. Word is also acceptable, but it may not deal well with mathematical formula.

Grading: Your grade will be judged on the completeness of the survey (40%), the quality of the analysis/comparison of existing solutions and your own opinion about future research/possible enhancements to the state-of-the-art (30%), and the overall quality (e.g., organization, and readability) of your paper (30%).

A non-exhaustive list of suggested literature survey topics (you may propose your own):

1. Cryptography applications on the internet today – SSL, SSH, https, WEP, WPA, SHTTP, WinPCT (compare with SSL), IPSEC, TLSP, NLSP, MSP, Netware, KryptoKnight, SNMP Security, etc. Identify the strengths and weaknesses in the existing implementations.
2. Identity-based encryption/attribute-based encryption schemes
3. Comparison of key distribution schemes for wireless sensor networks – Random vs. deterministic deployment, resource overhead, complexity, security evaluation.
4. Authentication protocols for RFIDs.
5. Anonymization of communications via Mixnets -- Explore the different types of Mixnets available (such as Tor) and the level of anonymity that they provide.

6. Cryptography applications in smart cards, ATM machines, etc.
7. Cellular network security, for example, security in GSM, or 4G/LTE/5G networks.
8. User authentication and password replacements
9. Mobile device/smart-phone security, e.g., user authentication or continuous authentication (beyond password)
10. DDoS attacks/ botnets on the Internet, and defense techniques
11. Electronic voting
12. Blockchains, or cryptocurrencies, including bitcoin and others
13. Security in emerging wireless networks/technologies, such as vehicular ad hoc networks, mobile social networks, near-field communications, etc.
14. Establishment of keys, security associations/device pairing protocols in wireless networks
15. Wireless physical layer security
16. Jamming/anti-jamming techniques in wireless networks
17. Location privacy in wireless networks
18. Security and privacy in machine learning

Final Report

Each team should provide a self-contained, readable final report. The following format is suggested but you do not have to follow it exactly.

1. Title and abstract
2. Introduction -- Include background material and motivation
3. Statement of the research problem(s): outline what is the common goals to achieve, such as system model, security requirements, threat models (types of adversaries existing work assume and what are the usual goals of the adversary), and major technical challenges in this domain.
4. Main Body – survey of the state-of-the-art (summarizing the ideas and results of major existing works/solutions, from classical ones up to the most recent results), and critically analyze/compare the advantages/disadvantages of current approaches (e.g., in terms of security, performance and/or usability).
5. Conclusions – what you have learnt from this survey so far.
6. Future work and open problems: analyze the open problems/challenges (with your own opinion) and suggest future research directions (discuss how you may solve them).
7. References.

List of Major Security/Networking Conferences and Journals

- IEEE Symposium on Security & Privacy (S&P, a.k.a. Oakland)
- ACM Computer and Communications Security (CCS)
- ISOC Network and Distributed System Security Symposium (NDSS)
- The USENIX Security Symposium
- International Cryptology Conference (CRYPTO)
- IEEE Conference on Communications and Network Security (CNS)
- ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec)
- European Symposium on Research in Computer Security (ESORICS)
- Annual conference of the ACM Special Interest Group on Data Communication (SIGCOMM)
- ACM MOBICOM, ACM MOBIHOC
- IEEE INFOCOM, IEEE ICNP, IEEE ICDCS

- ACM Transactions on Privacy and Security (TOPS), formerly called: ACM Transactions on Information and System Security (TISSEC)

- IEEE Trans. on Dependable and Secure Computing (TDSC)
- IEEE Trans. on Information Forensics and Security (TIFS)
- IEEE Journal on Selected Areas in Communications (JSAC)
- IEEE Trans. on Networking (ToN)
- IEEE Trans. on Parallel and Distributed Systems (TPDS)
- IEEE Trans. on Mobile Computing (TMC)
- ACM Trans. on Sensor Networks (TOSN)
- IEEE Trans. on Wireless Communications (TWC)

Google Scholar is a good way to search for papers (http://scholar.google.com). To download IEEE papers, go to www.ieeexplore.ieee.org and search for the conference/journal proceedings. To download ACM papers, go to http://portal.acm.org and search for the conference proceedings/transactions (you will need to connect to our university's VPN in order to download the PDF of most papers!). To view the paper list of a particular conference, first Google the conference name with the year and go to its website. For example, NDSS's website: www.isoc.org/isoc/conferences/ndss. The conference proceedings are usually available in the sponsoring association's repository, such as IEEExplore or ACM Digital Library (You may not be able to access these websites outside of the campus unless you use VPN).

To aid you, a sample survey paper can be found on D2L/the homepage of the instructor: http://wiser.arizona.edu/papers/WCM2009.pdf

Presentation guidelines

If selected, presentations should last around 15 minutes (including question and answer). They must be self-contained, and should be clear and precise. Briefly introduce the topic including any background information, describe the research problems and challenges, several major existing solutions that you have surveyed, and provide your analysis and comparison of those solutions, and identify the future work and open questions, briefly discuss how they can be solved. The following format is suggested:

1. Title -- Name the project and all the team members
2. Outline -- Summarize the full presentation
3. Introduction -- Introduce the purpose and goals of the project. Provide any background material necessary to understand the presentation. And provide the overview of the problems studied.
4. If doing a survey ---- survey of state-of-the-art solutions: use one slide to describe each of the major existing solutions that you have surveyed.
5. If doing implementation ---- provide the main approach or high level architecture/workflow for your implementation.
6. Findings - provide your analysis and comparison of those solutions, and what you have learnt from them
7. Conclusion and future work - identify the future work and open questions, briefly discuss how they can be solved.