CS 6500: Network Security
Term Project Requirements

Jan. – May 2022 Semester
Description revised on March 9, 2022
Due Dates:
Proposal: March. 16, 2022, 11PM (Online)
Completed Project: Apr. 30, 2022, 11PM (Online)

The objective of the term project is read and **implement** any one security protocol / mechanism. This can be done individually or a team of up to 2 members. The total number of hours devoted to the term project by **EACH** student is approximately **30 hours**. The workload and expected outcome of a 2-member team project will be roughly twice that of an individual project **60 hours**. Hence, the project outcome is expected to be commensurate with this amount of time.

1 Project Proposal

A three/four-page project proposal should be submitted online by **March 16, 11pm.** Format: 11-point Times Roman (or similar) font, 1 inch margin, A4 pagesize. If the project is to be done as a team, the team members (max. of 2) details should be included in the report. There should be no plagiarized material from the original paper or any other published work.

The project proposal, written in your own words, should present: (a) the protocol/mechanism/approach to be implemented in sufficient detail; (b) the programming language and the development environment; (c) the expected learning from the project; (d) testing and performance study plan (high-level).

2 Final Project Code and Report

The final project report will be detailed technical report containing

- Abstract: One paragraph
- Introduction and Motivation
- Relevant Background Material
- Detailed Problem Definition
- Details of Implementation
- Details of Testing and Performance Study, as appropriate
- Conclusions

The project code, test scripts, sample outputs and the final project report (PDF) should be submitted as a single tar.gz file online by April 30, 2022. The project code may also be submitted on a private github repository and shared with the instructor and TAs.

Notes

- The same grade will be assigned to both members of the team.

  In case a team member finds that the other team member is not contributing anything to the project, the concerned team member should bring it to the instructor's attention immediately.

- Change of team composition will not be permitted after March 31, 2022. In case there is a change in team composition, the revised proposal should be submitted on or before March 31, 2022 for instructor approval.

- If one of the team members drops out of the course or the project in the middle of the semester, the other team member is expected to take the project to completion individually. New members will not be permitted to added in such cases.

- Teams should not discuss with each other about their selected projects. It is expected that each individual and team will have a different project to work upon.

- Suggestions for project ideas: Please start brainstorming and ask questions in class!

3 Suggestions

These are only starting points. This is not meant to be an exhaustive list.

The objective of the term project assignment is to encourge you to think creatively beyond what is in the textbook, conceptualize new ideas, concretize them into complete mechanisms and implement the same. It is alright to carve out a larger scheme in the early stages and narrow down the scope given the time limitations.

After the semester is over, selected team members will be invited, based on the contribution's strengths, to author a technical article to a conference/journal. This submission is not mandatory and will have no influence on the project or course grade. The instructor need not be a co-author of such submissions and will participate in the article writing only if the students invite.

Note: For ambitious projects where 75-80% of the work is completed by April 30, 2022 and additional time is required to finish the project satisfactorily, an additional 2-3 week extension will be given without penalty. This is not to be viewed as an automatic extension. Projects where no significant progress is reported as of April 30 will not be given any penalty-free extension.

- Implement modifications of existing protocols (such as KerberosV5 modified using public-key cryptography, IPSec, ISAKMP, IKE, WiFi WPA2/WPA3, etc.) with all basic functionalities.

- Concepts not covered in class can also be considered: e.g. Group Key Establishment, Group Key in Multicast Nodes, Group Authentication, Blockchain systems such as Ethereum (not just applications), etc. These must use the security mechanisms (and extensions) discussed in class.

- Implement a major portion of key mechanisms/protocols in published research papers such as in top-tier conferences such as ACM CCS, USENIX NSDI, IEEE CNS, Securecomm, etc. and related journals in the field, e.g. IEEE Transactions on Information Forensics and Security and IEEE Transactions on Dependable and Secure Computing.

  ACM CCS 2021: `https://www.sigsac.org/ccs/CCS2021/accepted-papers.html`

  - DroneKey: A Drone-Aided Group-Key Generation Scheme for Large-Scale IoT Networks, Han et al., `https://dl.acm.org/doi/pdf/10.1145/3460120.3484789`
  - Efficient Online-friendly Two-Party ECDSA Signature, Xue et al., `https://dl.acm.org/doi/10.1145/3460120.3484803`

  See: `https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8858`
  `https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206` for sample journal papers.