CS-Specific Research Projects

Students in CSC 580 will work in teams of 3-4 students to complete a semester-long project. As an option for the Spring 2018 semester, we are doing a trial of ***collaborative projects*** between CSC 580 (Cryptography and Security in Computing) and ISM 324 (Secure Networked Systems), with a topic related to cloud storage security. Background on cloud storage and information about collaborative projects are provided in a separate handout. Students in CSC 580 who do not opt for a collaborative project can complete a pure ***technical project*** in teams of 3-4 CSC 580 students. These teams are also strongly encouraged to focus their project on a topic in security of cloud storage, but can pick another topic of similar depth with the permission of the instructor. Project depth should be appropriate for the student level (advanced undergraduate or master's student): while projects must follow the style and structure of real computer science research, there is no expectation that research "make a contribution to the field" as a real research project would.

Technical project reports are expected to follow the standards of computer science and computer security research, both in terms of focus and structure, and must be formatted to computer science publication standards (standard IEEE conference paper formatting templates will be provided for both Word and LaTeX, providing regular two column single-spaced papers). The length should be 12-15 pages in this format. One CSC 580 class day will be devoted to discussing computer science research practices and standards, and students will explore aspects of this in a homework assignment early in the semester.

1 Technical Project Topic Suggestions

The following are project topic suggestions for technical projects.

Technical Project Idea 1: Robust efficiency evaluation
For a project of this type, the team should design a test suite and efficiency evaluation mechanism to thoroughly evaluate Nextcloud and at least one other cloud storage service. Test cases should include variations on the number of files (up to approximately 10,000 files) and file size, and comparisons of unencrypted and encrypted storage (as allowed by the systems under evaluation). Efficiency should include measures of CPU and network usage. Ideally, this project should result in a model that can predict the processor and network bandwidth requirements based on environment parameters.

Technical Project Idea 2: Comparison of Nextcloud with composed end-to-end solutions

For this project, Nextcloud security and efficiency will be compared to solutions that use both an unencrypted cloud storage solution (e.g., Dropbox, Box, or Google Drive) and an encrypted filesystem to gain similar security benefits. For example, in Linux a user might stack an encrypted filesystems such as EncFS or eCryptfs on top of a cloud sync'ed directory. In addition to security and efficiency evaluations, you should also address issues of portability and use across different desktop OSes and mobile devices.

Technical Project Idea 3: Proposing and testing extensions to Nextcloud e2e encryption
The early release of Nextcloud end-to-end encryption has some two significant issues. First, nested directories (directories inside directories) are not possible in the Android client, and it's not clear how they are handled in the Linux desktop client. Second, copying or moving a file from an unencrypted folder to an encrypted folder within a single Nextcloud repository does not encrypt the file in the supposedly-encrypted folder (technically this is because the client only issues WebDAV copy/move commands to the server, which makes an identical copy). A project team can propose, implement, and evaluate a trial solution to either of these problems.

Technical Project Idea 4: Providing assurance to the end user
A big benefit of end-to-end encryption is that the end user does not need to trust the cloud storage provider. However, the end-user must trust the client software provider, including any update mechanism provided with the software. How does the user know that there is not just an illusion of security, while the client software actually provides a backdoor for dishonest parties to gain access to the data? A backdoor can be inserted either in the original software installation or surreptitiously installed through a software update. Unlike the other topic ideas, it is not clear how this problem can be solved, but a project team can come up with one or two ideas and do a careful evaluation of how they would work. A couple of ideas to consider are third-party software certification (and signing), or some type of self-certifying or proof-carrying code (most likely for a small part of the overall code). This is a highly-speculative topic, and will require more ingenuity and creativity to solve than the other topics.

2 Timeline and Deliverables

Tuesday, January 16: Joint meeting of CSC 580 and ISM 324 to discuss collaborative project possibilities (location to be announced).

Tuesday, February 6: Project Proposal
Students submit a document describing the project that their team will undertake. Students must provide a brief outline of the approach they plan to take, at a sufficient level to specify which aspects take an experimental approach and which are more analysis/design focused.

Tuesday, February 20: Project Plan
The project plan fills in details that were outlined in the project proposal, providing specifics

on approaches that will be taken. Students must identify at least three relevant references from the published research literature, and for each one provide a full citation along with a brief description of the paper's results and how the paper relates to the project. The project plan should also include a schedule of self-identified project milestones, where each milestone is a specific and clear deliverable.

Tuesday, April 3: Progress Report
The progress report should be a brief summary of progress, and an early draft of the project report. The project should be far enough along by this point where the report should include the full introduction and prior work sections (some statements in the introduction that describe final results can be incomplete or placeholder statements, to be finished after all results have been obtained). The results section(s) should be included, but can be outlines with placeholder notes (e.g., "table of timing experiment results will go here").

Tuesday, April 17: Final Project Report
As described above, students will complete and submit a full research-style paper, using a standard research paper template. All components of a standard research paper should be present (introduction, prior work summary, results, discussion, and conclusion/open problems), and the paper should be 12-15 pages. The paper should include a 1-2 paragraph abstract, as described in the template.

Sample Grading Rubric

Research Design (40%): Interesting and substantial research questions were formulated, and an appropriate research approach designed to address the research questions. The research procedure is documented so that it is clear, reproducible, and gives results that can be trusted as answers to the research questions.

Results presentation and discussion (30%): Results presented in a clear and understandable form, using tables, charts, and graphs as appropriate. Prior work section and results discussion clearly represent the results, how they support research findings, and how they fit into the existing body of knowledge. Conclusion and open problems are stated that clearly describe what results are closed and suggests directions for future directions and extensions of the work.

Paper Organization and Clarity/ Presentation (15%): The paper includes all standard research paper components (introduction, prior work summary, results, discussion, and conclusion with open problems), with an abstract that summarizes the most important parts and results of the paper. The paper uses headings and the information flows well from one section to the next. The writing is clear and correct.

Milestones Completed On-time (15%): All of the milestones were completed by the specified dates and were thorough.