Semester Project
MSCS 630

Pablo Rivas

Posted: Jan/20/20; Points: 100

1 Overview and Timeline

The goal of the semester project is to help you work on a larger project related to security algorithms and protocols, more specifically, to cryptography. You will gain experience in the development, implementation, analysis, and/or application of the things we discuss in class. It will help prepare you for further work in cybersecurity, or help you use cryptography for another project, e.g., your thesis.

The timeline for this project is the following:

- **Proposals**: due through Piazza by midnight on Sunday, March 8.
- **Milestone**: due on GitHub by midnight on Sunday, April 12.
- **5-minute YouTube presentation**: link due on Piazza by midnight on Sunday, May 10.
- **Final writeup**: due via GitHub by midnight on Sunday, May 10.

2 Project Topics

You first need to pick a project topic for your **Desktop App, Android App, or iOS App**. You can talk to professor Rivas during his virtual (or physical) office hours about choosing a topic, and to brainstorm with each other. There are typically three kinds of projects:

1. Data encryption app. This is the most common type of project: pick an application that interests you, and explore the best way to apply data encryption to solve the problem. This has to implement AES at 128 bits or better.
2. Data authentication app. Pick a problem or family of problems, and develop an app that digitally signs and authenticates data of some kind such as images, messages, documents, etc. This has to implement at least SHA-1 at 128 bits or better.
3. Full encryption and authentication app. Make a non-trivial app that requires encryption and authentication of data using AES and SHA-1 at 64 bits or better. This is typically difficult to do withing the timeline.
4. Novel encryption or authentication algorithm and app. Researh a novel algorithm, implement it, improve it, and make an app that uses it. It needs to be as robust as AES or the SHA family. This is typically quite difficult given the timeline.

Great projects can come from students combining their interest in an application with things they're learning from this class. So it's good to choose something you're excited about. This is a good chance to start work on a research project.

Getting started and choosing a topic can be a bit difficult, so it's good to look around for other ideas as inspiration. Good places are talking with your classmates or your professor, and looking at published work

in cryptography conferences such as those from the IACR[1]. A good project writeup will follow the style of these papers, and be of publishable quality.[2]
Please note the following: projects will be evaluated based on:

1. The technical quality of the work. (That is, do the technical choices make sense? Is the approach reasonable? Are the proposed algorithms or applications clever and interesting? Do the authors convey novel insight about the problem and/or algorithms?)

2. Significance. (Did the authors choose an interesting or a "real" problem to work on, or only a small "toy" problem? Is this work likely to be useful and/or have impact?)

3. The novelty of the work, and the clarity of the writeup.

Note that the amount of code that you write and the time that you spend on the project are less important than your ability to do interesting or significant work and communicate it clearly. So pick an interesting project where you can actually make some progress.

3 Project Submission Details

Here are more details on submitting the different parts of the project. Please see the important dates at the beginning of this document for when each part is due. For all project submissions you will use Piazza or the **same** repository you have been using submiting your work in a folder named "`prj`".

3.1 Project Proposal

10 points
Your project proposal should be a simple writeup giving the proposed title of the project, and a 50-100 word description of what you plan to do. Please submit your proposal through Piazza, NOT as a normal email nor as an attachment to one. Make your post in the designated space for it.

3.2 Milestone

20 points
This report should describe what you've accomplished so far, and very briefly state what else you plan to do. The milestone will help you keep on track. You should view it as an early draft of the writeup you will turn in at the end of the semester. Specifically, you can write it as if you're writing the first few pages of your final report, so you can use most of the milestone text in your final report. Please write the milestone (and final report) keeping in mind that the intended audience is Dr. Rivas or others familiar with cryptography. Thus, for example, you should not spend two pages explaining what encryption is.

Your milestone report should be at most 3 pages long. Please submit the milestone through GitHub, NOT as an email attachment. Please submit your milestone in .pdf format, using Word or LaTeX to prepare the document. Submit your work in a folder named "`milestone`" inside the folder "`prj`". The name of the .pdf should be formatted as "`lastname-ProjectTitle.pdf`", where lastname is your last name and ProjectTitle is the abbreviated title of your project.

As you write the milestone and final report, please pay attention to follow a similar format of other cryptography research papers (see IACR conference papers above). In particular, many experimental papers have the following structure:

- **Abstract**. A brief overview of the paper.
- **Introduction**. Describes the motivation of this work and outlines the rest of the paper.
- **Background and/or Related Work**. Describes what other researchers in the same area have done, and how they perhaps could be improved.

[1] `https://www.iacr.org/publications/`
[2] Here is a paper a former student and I published: `https://csce.ucmss.com/cr/books/2018/LFS/CSREA2018/IPC4114.pdf`

- **Methodology**. Describes what is the approach taken in this paper.
- **Experiments**. Describes the experiments performed, including details on the data used.
- **Discussion and/or Analysis**. Examines the results of the experiments and draws some conclusions about their significance.
- **Conclusion**. Summarizes the paper and its findings.
- **References / Bibliography**. Gives properly formatted references to other scholarly work that this work is built on. Note that the references should be scholarly, which means things like refereed conference and journal articles. Importantly, that rules out things like most websites, basic textbooks, and press articles.

3.3 YouTube Video Presentation

30 points

You will give a presentation in a YouTube video about your work during. Each person is expected to prepare a 5-minute video presentation with powerpoint-style slides that describe your work. Five minutes is not much time, so keep it brief: at most 5 slides total. We will adhere to the 5 minute schedule so that everyone has a chance to watch each other's video, and so that there is time for feedback and comments on Piazza. Submit your YouTube video Link on Piazza in the designated space for all of us to watch and comment.

3.4 Final Writeup

40 points

Final project writeups can be at most 8 pages long. Please submit your final writeup on GitHub in a folder named "`doc`" inside a folder named "`prj/writeup`", where lastname is your last name. The name of the .pdf should be formatted as "`lastname-ProjectTitle.pdf`", where lastname is your last name, and where ProjectTitle is the abbreviated title of your project. You will also submit any data that you used/produced for testing in a folder named "`data`" and any code produced inside a folder named `code`, especially code that will reproduce the results you claim to have achieved in your writeup.

The following is a tree-like directory structure of the desired organization for the semester project, where the root folder / is your GitHub repository root folder:

```
/
└── prj/
    ├── proposal/ … This directory will have proposal
    │              .doc/.tex and .pdf files (optional).
    ├── milestone/ … This directory will have milestone
    │               .doc/.tex and .pdf files.
    ├── presentation/ … This directory will have presentation
    │                   .tex/.ppt/.odp/.key/.pdf or video
    │                   files (optional).
    ├── writeup/ … This directory will have final
    │   │          writeup .doc/.tex and .pdf files (in
    │   │          doc/) and two folders where you will
    │   │          have any test data (in data/) and
    │   │          code produced (in code/).
    │   ├── doc/
    │   ├── data/
    │   └── code/
```

4 Expectations

The semester project, the App, is a very challenging project that can be done individually if time is managed correctly. My recommendation is that you work individually. However, I will allow team projects of up to two people. If you decide to work in a team, please make sure that all names are in every submission and that it is clear that it is a team project. Once a team is formed, you may not dissolve the team afther the first submission of work is done, unless, of course, there is a justified reason, e.g., drop out, plagiarism, health, etc.

Graduate students are expected to have superior programming and research skills and are expected to show that in their work. Do your best and you will do just fine.