Project

ECE750: Computer Security

Prepared by Kami Vaniea*

June 23, 2025

Masters students only. Undergraduates can safely ignore the project.

1 Overview

For this project you will be looking into a technology of your choice where security or privacy is a selling point of the technology. Meaning that the technology advertises itself as having security or privacy features. For example Firefox's private tabs and Chrome's Incognito which both offer a form of privacy protections when browsing the Internet. Or WhatsApp and Signal which both offer secure messaging. You will be looking into what the technology claims to do, and evaluating if it fulfills those promises.

Some context: One reason that people do not purchase or use more secure technology is that they lack the ability to assess the security of products. This situation is known as a *lemon market* where the product seller knows significantly more about the quality of the product than the consumer, allowing them to keep the knowledge secret, lie about it, or use confusing language. Consumers are also unwilling to pay more for security and privacy because they cannot assess the security of the products themselves.

There are several ways to solve a lemon market situation, the best one is to limit the information asymmetry so that consumers have reliable information about the products. For example, the US State of California was one of the first to implement mandatory data breach reporting. Any consumer can check the public list of data breaches impacting Californians and see if a company has a history of losing customer data. Similarly the Federal Trade Commission (FTC) in the US forbids "deceptive trade practices" or in other words, lying. In 2014, for example, the FTC fined Snapchat which claimed that messages sent would "disapear". But, among other issues, it "stored video snaps unencrypted on the recipient's device in a location outside the app's "sandbox," meaning that the videos remained accessible to recipients who simply connected their device to a computer and accessed the video messages through the device's file directory." In other words, Snapchat claimed that messages were protected and would disappear, but did not take the technical measures to ensure that was the case. So their marketing materials were deceptive.

Closer to home, University of Waterloo had M&M snack machines that contained video cameras to track demographics of who was using the machines. The Information Privacy Commissioner for Ontario Decision found that the machines' use did not comply with law (FIPPA).

Project aim: There are many future situations where you will need to be able to judge if software meets the security and privacy needs of yourself or your employer. At the very least, you will need to be able to evaluate and choose between API and library options. This project aims to help you learn about evaluating such technologies by having you apply course concepts at a greater depth in regards to a software of your choice.

2 Groups

The project can be completed individually or in groups of one or two students taking the class.

*Modified from earlier version that Mohammadtaghi Badakhshan helped design.

3 Selecting the technologies

The selected technology needs to have a clear security or privacy aspect to it. It is fine if its primary purpose is not security, for example, WhatsApp's primary purpose is communication, but it has a clear security component in that secure messaging is a key part of their marketing.

The technology you select must:

- Be software or an IoT device that connects to a network - purely hardware or other technology like security-themed card games are out of scope for this project. It needs to have software that can be assesssed or generate network traffic that can be assessed.
- Have some form of public marketing. The marketing can be something as simple as a GitHub page. But the content needs to explain the software's purpose at a high level, not just technical documentation.
- Some form of technical documentation, open source code, or evaluations by a third party need to exist. Blog posts by the companies about how the technology works are fine. There needs to be some way to get more detail about how the technology is implementing their promises.

3.1 Finding technologies

There is no strict limitation on what software you can pick, other than what is described above. Below are some ideas where you can find lists of security software, but you are welcome to look beyond these.

- Wikipedia Comparison of disk encrypted software - which has a long list of encryption tools.
- Wikipedia Comparison of cross-platform instant messaging clients - Not all of these are security technologies, but the are interesting because they interoperate with other messaging platforms which can add or reduce security.
- EFF has a list of Tools from EFF's Tech Team - listing tools that they have created. Many of these have competitors made by other organizations.
- https://www.privacytools.io has an extensive list of security and privacy technologies.

4 Investigate the technology

After you select a technology you will need to evaluate its security. To do so, you should consider the way the technologies market themselves, any technical details you can find, and also what you yourself are able to test or deduce.

4.1 Marketing materials

Start with the way the technology describes itself to consumers in terms of security or privacy. What are they claiming they do? If a consumer were to only look at the home page, and the download page, what kinds of protections might they think the software will provide? You can also consider information found in advertisements. Anything where the technology creator/owner is trying to explain to consumers why they should use the product and why it will protect their privacy or security without getting into software-engineer level detail.

4.2 Technical information

Marketing materials tend to use overly broad terms like "messages are secure" or "posts are anonymous". Identify these promises in the prior step and then as much as possible figure out what these terms actually mean technically. Technical descriptions by the technology creator/owner are a great place to start. Groups that care about privacy and security tend to be open about how they are implementing them. Popular technologies have also often been evaluated by a third party researcher or group which can be enlightening.

Many technologies are built on reasonable approaches, so for many choices you will not find serious problems. But you may find situations where the technology choices do not directly align with what you or another consumer might expect. For example, Windows Recall claimed that the collected data was encrypted (true). But when researchers looked into it, they realized Microsoft meant that the whole disk was encrypted by default, so the Recall data was also encrypted because it was stored on the disk. But any users with a valid account can decrypt the disk, so the data is not protected from other account owners. No Recall-specific encryption was being used. Similarly, Telegram claims to have encrypted chats (it does) but upon careful examination of their detailed descriptions we learn that only some chats are encrypted, most are not.

The key to this step is to try and find the details about how security is being implemented. And then lookup the terms being used. Try and find answers to questions like: "what type of encryption is being used?" Or "how is data being modified so that it cannot be traced back to the user?" You are welcome to review open source code if that helps. But you are not required to do so. At this stage it is fine to trust that the technology creator/owner is telling the truth, though they may be being intentionally unclear or not mentioning important information. So if they say they are using AES-128 bit encryption, it is ok to assume that is true, but your next question should be what they are using it for and in what situations are they possibly not using it.

Information sources: Make sure to keep track of the information sources you are using so you can cite them in the report. Also think about the relative quality of the sources you use. The official documentation has high quality. But other sites you need to use your own judgment. Even places like StackOverflow are known to have variable quality of information, especially as the question get less popular. A good StackOverflow answer will link to other more official documentation. Similarly with sites like Wikipedia, which are excellent places to start looking, but you should be following their references.

4.3 Testing the technology

From your research above, select one testable question that you have. The question should be specific enough to be testable. Questions like "is it secure" are far too broad. Aim for something more specific where you can clearly measure the answer. The question needs to be something you feel capable of testing using the skills and technology available to you. Unless you have taken an encryption course, I recommend avoiding questions requiring you to assess the quality of encryption. The test you do should meaningfully impact your assessment of the technology. Ideally it will help you better understand the technical information you found, answer a follow-on question, or possibly confirm something you read from a less-reliable source.

For example, you may want to know if a "secure and private" website is using any form of advertising trackers. So you could look at the Javascript code that it loads. You could also monitor the website's network traffic in-browser to see what websites are being contacted and what information is being sent to them. Then investigate those websites to see what they are and who owns them.

As another example, you could investigate where the technology is storing files and what kinds of protections are being applied to those files. You can test what access control protections are being used. Also if it is being encrypted by the program or just relying on full-disk encryption. Once you know how it is being stored, you can lookup online how secure that storage approach is and if there are any known problems with it. Programs store files in a range of places so you would also need to find the OS-appropriate places where files hidden from users are often stored.

4.4 Research papers

A masters means engagement with research. It is expected that the resulting report for the project include engagement with at least 2 research publications that relate to either the the claims made by the technology. Or that relate to testing the technology.

The technical information and testing steps above should also include looking at research papers. There are loads of research papers about the security of consumer technologies. Everything from the expectations users have around products, to the theoretical security guarantees, to the actual security of implementations. At least three research publications from peer-reviewed publication venues must be cited. The publications can be about the specific technology, a technology it relies on, or that type of technology. We expect to see

the papers cited in sections 3 and 4 of the report. It is ok if one of the three citations is in section 2, but the others need to be sections 3 and 4.

5 Report

Write a report containing the sections and information enumerated below. The report can be a maximum of 5 pages: 3 pages of text, 1 page of figures, and 1 page for a bibliography. So the main report should fit in three pages with the other two pages being used for images (if needed) and bibliography. The text should be no smaller than 10 point, and the font should be a common readable font. Pages need to have at least a 1-inch margin, which the default settings for Word and LaTeX automatically provide.

1. **Introduction**
   - List all students involved in the project.
   - The technology's name and a link to its home page.
   - 1-2 sentences describing the technology and security or privacy aspect of it. The description needs to be clear at a high level but it need not be complex. For example: "Signal is a messaging app that uses end-to-end encryption when sending messages."
2. **Claims:** Describe the security and/or privacy claims of the technology in terms of the security definition given in the first lecture. If there are many claims, focus on the ones you consider to be important for the primary functionality or that you plan on testing further. Describe how the technology is defining "secure" or "private". For example, a baby monitor might claim to be "secure" in that information sent is confidential and only authorized parties can use the monitor as a speaker (Authorization). We expect that most reports will need about one paragraph to explain claims.
3. **Related Work:** Connect the claims to related work. The related work need only cite and discuss 2 papers, it does not have to be comprehensive. But it should either add depth to the claims of the technology OR provide context for the technology investigation.
4. **Technology Investigation:** Focus in on a couple of the key claims and explain how they are technically implemented. For example, if encryption is being used to protect data in motion, what algorithm is being used? We expect to see citations being used to backup the technical investigation.
5. **Test:** Describe the test you ran. The description should include the following information:
   - Claim or technical point being tested.
   - Question you are testing, what are you trying to find out or prove. Be specific here as the question needs to be possible to test.
   - How you went about finding out or proving the answer to the question. What steps you took and what technologies you used. Some justification should also be provided about why this particular testing approach is appropriate. For example, in-browser network analysis is a good choice because it helpfully isolates network traffic associated with a specific webpage.
   - What did you find? What is the answer to your question?
6. **Conclusion:** Imagine your employer is considering using this technology for employees. Would you recommend they use it? Why or why not?
7. **References:** Cited using a major style like APA or MLA. These may take up to one page.