Encrypted communications and threat models

Adrianna Holden-Gouveia
Website: `https://aholdengouveia.name`
in: aholdengouveia
: aholdengouveia
: aholdengouveia

Objectives:

1. Learn how to create a threat model including a risk assessment
2. Describe how to come up with an encrypted communications plan

Complete the following problems

Be sure that you are able to assess risks and then prioritize them as part of your threat model. Make sure that you include both written communications such as email as well as the phone and text communication options you should say if you are using a VPN why or why not and some things that you would need to look for if you are going to use one.

You should focus on the technology not the risks that involve dangers of people doing potentially dangerous things. For example if you are talking about a protest, there are risks of being in person and being pepper sprayed, but remember we're looking at the technology used for organizing the protest so the risks are about the technology used to organize it not dangers of showing up. For those that are struggling with how to do this. There are a lot of resources for how to threat model for companies or applications, the research and steps used will be the same here, you're putting yourself in the shoes of one someone in the following scenarios and imagining what you need to do to stay safe.

Think about the following questions:

- What's reasonable? what's over the top?
- What avenues have more risks? less?
- Is there anything you're missing?

Research the scenario of your choice thoroughly to get an idea of what it's like for that group of people and what they might be worried about. How might their worries and threats be different then yours(You don't need to share this, it's just food for thought)?

Some references that may be helpful:

- `https://en.wikipedia.org/wiki/Threat_model`
- `https://blog.securityinnovation.com/creating-your-own-personal-threat-model`

Don't forget about cell phones almost everyone in one of these scenarios is going to have a cell phone and that needs to be protected as well and you need to talk about how you are going to protect the cell phone.

Please pick ONE of the following scenarios to do your threat modeling on.

1. You are organizing a protest in a country that doesn't have peaceful protest protection such as Hong Kong or Egypt. You need to organize a protest and protect yourself and other protesters, what do you do? Read more about the protests and concerns here:
   - `https://www.bbc.com/news/world-middle-east-49800213`
   - `https://www.bbc.com/news/world-asia-china-53942295`
2. You vising a country with restrictions on the internet, you want to be able to communicate with your friends and family back home safely, use a Google search and be on social media. What do you do? (Don't just say VPN, there is more to this then that and even a VPN needs more then Google "good vpn" and pick the top result, what questions to you need to know about a VPN? provider? how do they work and what protections do you get?)

- https://hackernoon.com/the-spread-of-internet-censorship-around-the-world-7i1mn3zwb
- https://cyber.harvard.edu/pubrelease/internet-control/

3. You are a minority in a country that is persecuting you, such as a member of the LGBTA+ community in Russia, or a Uygher muslim in China. You want to talk to your family and organize others to help protect you and others. What do you do? Read more and

    - https://www.cbsnews.com/news/china-puts-uighurs-uyghyrs-muslim-children-in-prison-re-education-internment-camps-vice-news/
    - https://www.reuters.com/article/us-russia-activist-court/russian-lgbt-activist-fined-for-gay-propaganda-family-drawings-idUSKBN24B2IY

4. You are part of a conspiracy to try to smuggle persecuted people out of an area they are in danger (such as what happened during the underground railroad or helping people escape Nazi Germany) and you need to find a way to communicate with the next places that the people you are helping are going to go and what their next steps are. Examples in the modern day might include:

    - https://www.cfr.org/global-conflict-tracker/conflict/israeli-palestinian-conflict
    - https://www.amnesty.org/en/countries/middle-east-and-north-africa/israel-and-occupied-palestinian-territories/report-israel-and-occupied-palestinian-territories/
    - https://time.com/5318718/central-american-refugees-crisis/

5. You work for the company that is doing research but your research has proved that the company's product is dangerous and you need to communicate this to your government how do you do this while keeping your safety and your family safety in mind. Or alternatively you work for the government and you have information that they do not want to exposed but it is dangerous information that people should know (I.e. Snowden) how do you go about protecting yourself and your family.

- https://www.bbc.com/news/technology-54013527
- https://www.washingtonpost.com/news/federal-eye/wp/2014/07/31/5-famous-whistleblowers-from-the-federal-government/

If none of these appeal to you you may come up with another scenario. However you must check with the teacher before using your scenario to make sure that it works.

Reference information for CRAP/CRAAP

Turn in your report including your sources, you need at least 5, and a CRAP reliability checklist/paragraph for EACH source. CRAP or CRAAP is used to define the quality of your sources.

- You need at least 5 sources, and a CRAP reliability checklist/paragraph for EACH source.
- You may use either APA or MLA for your citations. If you want to use something else please just check with me first.
- Do not copy/paste from anywhere without citing your reference. Quoting or paraphrasing from a web site should include a citation.
- If you copy and paste into your paper, it is a quotation. It needs quotes and a link to the information (the link may be cut and paste from the address bar).
- If you use material that is only changed in minor ways (words or phrases omitted, shortened or slightly rearranged) it is a citation. It does not need quotes but does need a link to show from whence it came.
- If you take information from one source and substantially rephrase the material (paraphrase) it should be cited (show a link).
- Material drawn from multiple sources put in your own words does not need a direct citation but the sources would show up in any included bibliography.

- You can find instructions and more explanations for CRAP/CRAAP checklists at the following places
  - CRAP test explanation 1 `https://cccs.libguides.com/CRAPTest` or
  - CRAP test explanation 2 `https://libguides.butler.edu/c.php?g=117303&p=1940068`
  - Wikipedia explanation `https://en.wikipedia.org/wiki/CRAAP_test`

Deliverables

- Your threat model
- Your threat model must include at least 10 risks (number them!)
- Prioritize your threats from severe to mild risk and organized in a table from highest risk to lowest risk including notes on why you ordered them the way you did.
- A paragraph or two that includes your plan for how to mitigate each of those risks including an explanation of how your plan matches to the risks and how your plan is taking care as much as possible of the threats that the scenario faces.
- You must have at least five resources
- Your CRAP/CRAAP checklist for EACH of your 5 sources, but they should all be in the same document which can be different then the paper, or at the end of the paper