Design Considerations

Selected technology

For the seminar, I chose Transport Layer Security (TLS), which is the successor to SSL, and is the modern standard for encrypted communication between client and server.

Selected cards

I have chosen the following cards, (1) Politics: adversary's motivation and (2) Personal data: Human Impacts. Below I will solve the stated card tasks. I chose these cards because they highlight the need for a just and moral society in order to make the best of my chosen technology. TLS and HTTPS are of little use if authoritarian regimes refuse to use them.

Politics: Adversary's Motivation

Task:
How might the adversary use or abuse your system to affect politics? What kind of individual or group might target your system for political gain?

Solution:
This technology is very easily neutralized if governments decide to put the national internet under surveillance. Given enough time and encrypted data, some agency might figure out how to decrypt the data. Furthermore, TLS is used only if a government allows it. If they wish to do so, and many governments do, they can simply choose to enforce that communication must stay unencrypted over the internet. An adversary might easily (the ruling party for instance) steal your exposed information in order to discredit or extort you, if they deem you to be a political threat or rival.

Personal data: Human Impact

Task:
What kinds of personal data does (or could) your system collect, store, or share? How might current or future compromise, corruption, or unavailability of this data cause harm?

Solution:
As almost every instance of client server communication uses HTTPS and TLS, it would mean that all sorts of sensitive and insensitive information is encrypted, ranging from medical records to food recipes. The few instances where TLS is not used is when it is discouraged or prohibited, as is the case in some authoritarian countries. This can cause irreparable harm to individuals that do not hold the same view as the regime in charge. Freedom of speech and protection of ownership rights (in this case immaterial ownership) is vital to the progress of any country. Inhibiting the use of TLS severely jeopardizes both, and will inevitably cause harm to a nation that does so.