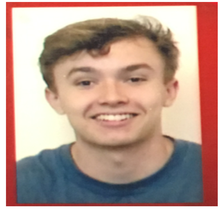
Covert Channels of Communication

Students: Ian Armstrong, John Schlagbaum, Noah Orr
Advisor: Professor John Franco



Problem:

Covert Channels can be built virtually anywhere without detection and cause damage to unaware systems. Education on the matter is lacking.

Solution:

A readable library of covert channels in different domains.

Challenges:

- *Domain knowledge*
- *Time*
- *Creativity*
- *Low-level programming*

Overview:

A covert channel of communication is a method of transmitting data using elements that were not intended of communication, so that the transmission of data is hidden from regular purview.

Future Work:

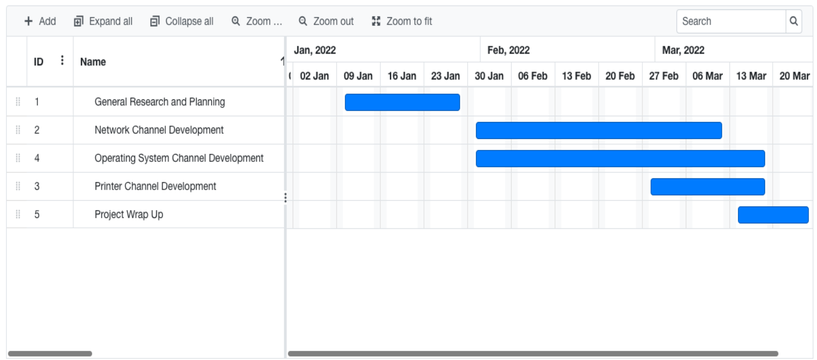
Domain Knowledge

- As we gain professional experience, with new technologies, ideas for new covert channels will arise.

Detection & Metrics

- Improvement on making these channels less detectable by learning and measuring the metrics necessary.

Gannt Chart:



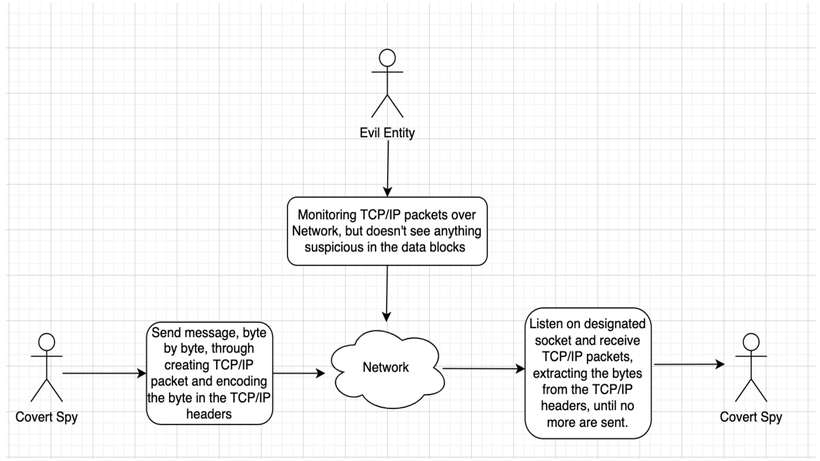
Results

Overall, our team was successful in our venture. We created our covert channels to prove concepts, not for performance or flexibility. With more time spent learning and programming, we could definitely improve our channels. Our library can be found on GitHub using this link: https://github.com/Ianarm11/senior-design . Our team learned a lot through completing this project.

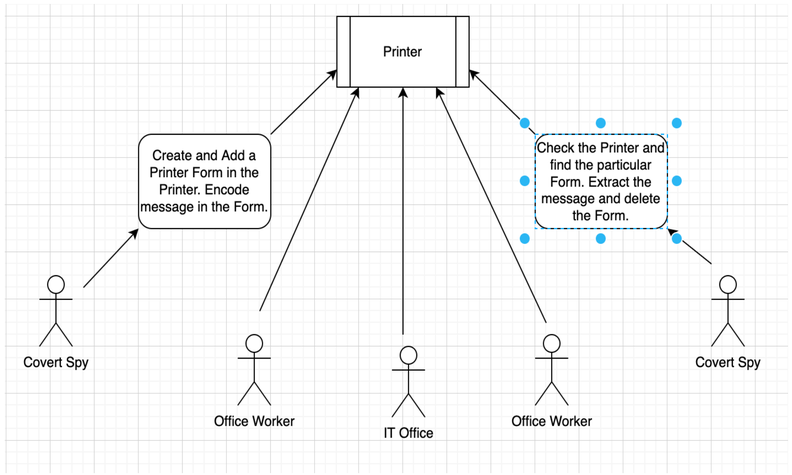
References:

[1] Tian, J, Xiong, G, Li, Z, Gou, G, 2020, A Survey of Key Technologies for Constructing Network Covert Channels.
[2] Okhravi, H, Bak, S, King, S, Design, Implementation and Evaluation of Covert Channel Attacks.
Lipp, M, Schwarz, M, Gruss, D, Prescher, T, Haas, W, Fogh, A, Horn, J, Mangard, S, Kocher, P, Genkin, D, Yarom, Y, Hamburg, M, Meltdown: Reading Kernel Memory from User Space.
[3] Kocher, P, Horn, J, Fogh, A, Genkin, D, Gruss, D, Haas W, Hamburg, M, Lipp, M, Mangard, S, Prescher, T, Schwarz, M, Yarom, Y, Spectre Attacks: Exploiting Speculative Execution.
[4] Bharti, V, Snigdh, I, Benalia, H, Mahmood, R, 2007, Practical Development and Deployment of Covert Communication in IPv4.
[5] Du, Wenliang, seedsecuritylabs.org, Syracuse University.

Network Channel Flow Chart:



Printer Channel Flowchart:



Operating System Channel Flowchart: