## Discussion Thread: Cybersecurity Domain Separation-Simplicity of Design-Minimization

Simplicity of Design

Simplicity of Design in the realm of cybersecurity is about how engineers can prevent hackers from attacking systems by providing less avenues for them to choose from. A good example would be to think of a game of hide and seek If your goal was to find them, you wouldn’t want a mansion, because it would take forever to find the person. The same can be said with software and networks. The more variables, scripts, processes, nodes, and routers, the less our chance is at preventing infiltration.

The way we design programs around networks has a lot of impact on the cybersecurity side of things. If we were to write a program that create a large amount of traffic data, the security team would have to potentially scour through hundreds or thousands of packets to see where an injection attack occurred. This is more prevalent to us today because every day we transmit a lot of information, think about how your apple watch tracks your heartrate, or how YouTube always recommends specific videos based on what you have watched. Robust projects need robust engineers who can create projects and defending potential attacks on said projects.

The idea of having more simplistic designs also have repercussions in all of design If we make systems that are complicated, they are more difficult to deconstruct and more difficult to improve. What this means is that a potential issue would take more time and more resources to resolve it however in a simpler design, it will be very easy to find and resolve any issues. Take for example Microsoft Windows’ operating system, it has a large number of working parts and if there was an error in it, it would take a long time to find it. But in Linux for example, the more simple organization and easy to navigate design allows for quick acknowledgement of bugs or attacks.