Rajat Sethi – CPSC 8580

**Paper Summary – Zero Trust Architecture**

The idea of Zero Trust centers around the Principle of Least Privilege, where subjects and users have as little access as necessary to the files on the system. Zero Trust takes this a step further and makes access control a heavily fine-tuned process. Even physical proximity to the server is not enough to earn implicit trust in these types of Zero Trust systems. Permissions must be given on a dynamic, case-by-case basis. When a subject needs access, they must be vetted first at a policy decision/enforcement point before they are granted those permissions. Once they have completed their task, they are stripped of their permissions until they need it again. It is a cycle of asking, vetting, and rescinding.

This applies to more than just permissions as well, as it can also work for allocating resources. The system determines how much data or processing speed a subject can use, then temporarily gives it to them. This type of Zero Trust helps prevents denial of service attacks.

One of the main problems with this type of architecture is the amount of effort necessary to maintain this level of access control. An enterprise needs developers to secure these systems, then system administrators to maintain the logs, maybe a few network engineers to control traffic. For a massive company, this might be feasible, albeit a bit slow. But for smaller companies, this system is quite unrealistic.

That being said, even if a company does not have that large of a software development team, there are some basic principles that they can follow. They can have automated systems that grant/revoke permissions. They should not give permission to individuals even if they’re physically in the company building. And they can give slices of resources instead of the whole system.