CS 460 Team 7 {WARD, Wyatt; LEHMAN, Mitchell; NYFFELER, Andrew}

Problem Statement

The modern world is an interconnected grid of powered devices. Nearly every single one of these devices are built upon the guarantee of a reliable electricity generation, regulation, and distribution system. But this system cannot be guaranteed. The systems that give electricity – the power plants, the arrays of windmills and solar cells, the dams, none of these exist solely in the abstract. Their tangible nature gives them a physical presence, and that presence gives them vulnerability.

While the first-thought way to besiege an electric system would be to plan and execute physical attacks via the usage of e.g. explosives or large rocks, this project will not focus on that aspect. The count of reports covering physical vulnerability is easily in the hundreds, and this team shalln’t ever compare to the many teams organized and composed of various international governments.

Instead, we shall cover the vulnerability of these systems to attacks taking place on the online realms, that is, cyberattacks or ‘hacks’. This vulnerability comes from many places, but among these is the strong association of tech familiarity – and thus cybersecurity – with younger generations. This is compounded by the fact that the early computer world was operated among trusted and trustable individuals, meaning that security was not a priority. The youth, then, naively aligned themselves with trust at an early age – and this alignment cemented itself until this naïveté spread like a virus to the technologically uninformed.