**Use Case**

Matt owns a local manufacturing firm employing several employees. The business serves multiple large retail clients around the Midwest region like Menards and Bomgaars. Matt has a shop with warehouse space that holds all of their operational technology and significant volumes of high-value inventory. He also has a security system with cameras, an alarm, and automatic locks. He wants to take advantage of the convenience of using Home Assistant to control all of his operational technology, security system, thermostat, lighting, and POS system. As his business is growing, he recently installed and began using a computerized numerical controller (CNC) which is connected to Home Assistant through Modbus.

**Misuse Case**

Andrew is a hacker in town who’s father was recently laid off from Matt’s business. Andrew knows that Matt started using Home Assistant to control all of his devices and decides this will be a good way to cause some havoc for Matt. He uses a brute force attack in order gain access to Matt’s Home Assistant to infect some of Matt’s devices with Malware. Once he gained access to Home Assistant, he found the Modbus add-on which is connected to a very expensive and very new piece of equipment, the CNC. Andrew installed the malware on the CNC and several other connected devices. Gaining control over the CNC device, Andrew changed the rotational speed of the machine and unlocked the safety guard on the machine which put other employees in the building at serious risk of entanglement and lacerations, fractures, amputations, or even death from ejected parts.

**Prevention and Security Requirement**

This misuse case could be prevented by using layers of security measures. Primarily, password protection should prevent attackers from gaining access to Home Assistant. Secondly, Matt should enable the logger function of Home Assistant to identify anomalous and unauthorized activity should the authentication methods fail. Frequent review of the log files is necessary to identify such malicious activity. Finally, requiring additional authentication and authorization controls to be in place for access to the log files would prevent the attacker from tampering with the log files effectively “covering their tracks.”

Diagram, schematic

Description automatically generated