Flipped Classroom Session 9: Threat Modelling

CS-C3130 Information Security, 10.10.2023

Consider the Abloy Cliq electronic key system, described here:

- https://www.abloy.com/au/en/documents/catalogues/protec2-cliq-technical-brochure/ABLOY%20PROTEC2%20CLIQ%20Technical%20Brochure.pdf

You might have seen a wall unit like this one in the CS building:

- https://www.abloy.com/gb/en/products/digital-key-systems/protec2-cliq/programming-devices/cliq-wall-pd

Each morning when I arrive at work, I have to insert my key into this unit, which connects to a server, which communicates with the key. Only after doing this can I use my key to open my office.

This unusual requirement allows the locks to be installed without connecting them to power or the network. You can even buy padlocks that work with the system:

- https://www.abloy.com/global/en/our-products/products/padlocks/electronic-padlocks/protec-cliq-padlocks

The server determines which locks I can access, and is managed by facilities personnel. They configure the server based on instructions from Human Resources.

It is also important to maintain access logs. This is complicated by the fact that the locks aren't connected to the network. This is solved by storing access logs on both the lock *and* the key. Each time a key is inserted into a wall unit, its logs are uploaded to the server. A special *programming key* can be used to configure locks, as well as to download the logs from a lock without waiting for all the keys that used it to be inserted into a wall unit.

Draw a diagram of the system, along with all of its dataflows, and analyse the security threats against it and its users.