**Introduction to Cyber Security**

Asset = Something of value to its owner, that is being protected (tangible or intangible)

Threat = Intention to cause damage. A hostile act aimed by an attacker at an asset.

Threat Actor = The attacker that poses a threat.

Vulnerability = Defect in the target system. Could be a bug in code, flaw in design of the system or a consequence of improper configuration or user action.

Exploit = Way to take advantage of a known vulnerability. Usual objective is to take over the asset.

**Stride and Dread**

There are multiple ways of classifying threats. Two examples are STRIDE and DREAD, which provide good structures for determining the type of a given threat.

SRIDE threat model = Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege.

* Spoofing: when someone illegally accesses a system using another user’s authentication info.
* Tampering: covers unauthorized changes made to persistent data, inside a machine or in transport
* Repudiation: system should be able to trace user operations to provide evidence of what happened in case of a breach
* Information Disclosure: covers the exposure of info to unauthorized individuals
* Denial of Service: server or service is made temporarily unavailable.
* Elevation of Privilege: an unprivileged user finds a way to gain sufficient privileges to compromise the system.

DREAD threat model = Damage, Reproducibility, Exploitability, Affected Users, Discoverability. A mnemonic checklist for prioritizing threats based on severity.