COMP2211 - Networks and Systems
Cyber Security

Kamil Hepak

2019-20

> *"Computer security is the protection of computer systems against adversarial environments."*

We want to **allow intended** use, and **prevent unintended** use. Red vs Blue mindset - attacker vs defender.

Some terminology:

- **Asset:** Something of value to a person or organisation.
- **Vulnerability:** Weakness of a system that could be accidentally or intentionally exploited to damage assets.
- **Threat:** Potential danger of an adversary exploiting a vulnerability.
- **Risk:** Asset x Threat x Vulnerability.
- **Adversary:** An agent that circumvents the security of a system.
- **Attack:** An assault on system security.
- **Countermeasure:** Actions/processes that an owner may take to minimize risk of a vulnerability.
- **Confidentiality:** Ensuring assets are only available to those who should be allowed.
- **Integrity:** Ensuring consistency, accuracy and trustworthiness of data.
- **Availability:** Ensuring that assets are always available (e.g. in the event of an attack).
- **Accountability:** Recording actions so that users can be held accountable for their actions.
- **Reliability:** Ensuring that a system can progress despite errors.

Confidentiality, integrity and availability often have to be balanced - going too far in one sector may compromise the others.