Security vulnerability and exploits

Security vulnerabilities = **any kind of software or hardware defect**

Exploit = **program written to take advantage of a known vulnerability**

Hardware vulnerabilities

- **most often the result of hardware design flaws**

- hardware vulnerabilities are specific to device models and are not generally exploited

through random compromising attempts

Software vulnerabilities

- **usually introduced by errors in the operating system or application code**

**Categorizing software vulnerabilities**

- BUFFER OVERFLOW   
 - **buffer** = **memory allocated to an application**

- **data is written beyond the limits of a buffer by doing so the application can**

**access memory allocated to other processes this can lead to a system crash or**

**data compromise, or provide escalation of privileges**

- NON-VALIDATED INPUT

- **malicious content of data inputed to program to behave in an unintended way**

- RACE CONDITIONS

- output of an event depends on ordered or timed outputs

- **condition becomes a source of vulnerability when the required order or timed**

**events do not occur in proper order or time**

- WEAKNESSES IN SECURITY PRACTICES

- **systems and sensitive data can be protected through techniques such as**

**authentication, authorization and encryption**

- ACCESS CONTROL PROBLEMS

- it is the process of controlling who can do what with stuff

- many vulnerabilities come from improper use of access controls

Software updates

Goal:  
 to stay current and avoid exploitation of vulnerabilities