Lecture 2

Spectre Vulnerability

- useful if your process is part of a bigger process and can reach memory outside of its sandbox
- Error: only restoring the registers not the cache

```
unsigned char array1[16] /* base array */
int array1_size = 16; /* size of the base array */
int x; /* the out of bounds index */
unsigned char array2[256 * 256]; /* instrument for timing channel attack */
// ...
if (x < array1_size) {
    y = array2[array1[x] * 256];
}
```

```
Algorithm:
1. create a small array array1
2. choose an index x such that array1[x] is out of bounds
3. trick the CPU into speculative execution (make it to read array1_size from slow
memory and to guess wrongly)
4. create another uncached memory array called array2 and read
array2[array1[x]] to load this cell into the cache
5. read the entire array2 and observe the timing; it will reveal what the value of
array1[x] was
```

Dependability Concepts and Terminology

- **System**: an entity that interacts with other entities, i.e., other systems, including hardware, software, humans, and the physical world with its natural phenomena
- **Environment**: The other systems are the environment of the given system
- **System Boundary**: the common frontier between the system and its environment
- **Component**: The structure of a system is composed out of a set of components, where each component is another system. The recursion stops when a component is considered atomic.
- **Total State**: of a given system is the set of the following states: computation, communication, stored information, interconnection, and physical condition.
- **Function**: what the system is intended to do and is described by the functional specification
- **Behavior**: what the system does to implement its function and is described by a sequence of states
- **Service**: delivered by a system is its behavior as it is perceived by a its user(s); a user is another system that receives service from the service provider
- **Correct Service**: is delivered when the service implements the system function
- **Service Failure (Failure)**: is an event that occurs when the delivered service deviates from correct service

- **Error**: part of the total state of the system that may lead to its subsequent service failure
- **Fault**: is the adjudged or hypothesized cause of an error. A fault is active when it produces an error, otherwise it is dormant
- **Dependability (original)**: is the ability of a system to deliver service than can justifiably be trusted
- **Dependability (revised)**: of a system is the ability to avoid service failures that are more frequent and more severe than is acceptable
- **Dependability Attributes**:
    - Availability: readiness to deliver correct service
    - Reliability: Continuity of correct service
    - Safety: absence of catastrophic consequences
    - Integrity: absence of catastrophic consequences on the user(s) and environment
    - Maintainability: ability to undergo modifications and repairs
    - Confidentiality: absence of unauthorized disclosure of information
- **Security**: a composite of the attributes of confidentiality, integrity, and availability
- **Fault Prevention**: aims at preventing the occurrence or introduction of faults
- **Fault Tolerance**: aims at avoiding service failures in the presence of faults
- **Fault Removal**: aims at reducing the number and severity of faults
- **Fault Forecasting**: aims at estimating the present number, the future incidence, and the likely consequences of faults

Dependability Metrics

Reliability

R(t) of a system S is defined as the probability that S is delivering correct service in the time interval [0, t]

- reliability R(t) for non repairable systems is the Mean Time To Failure (MTTF), normally expressed in hours
- reliability R(t) for repairable systems is the Mean Time Between Failures (MTBF), normally expressed in hours
- The mean time it takes to repair a repairable system is called the Mean Time To Repair (MTTR), normally expressed in hours.
- These metrics are valid in the steady-state, i.e., when the system does not change or evolve.

Availability

A(t) of a system S is defined as the probability that S is delivering correct service at time t.

- metric for the average, steady-state availability of a repairable system is A = MTBF/(MTBF + MTTR), normally expressed in percent
- A certain percentage-value may be more or less serious depending on the “failure distribution” (the “burstiness” of the failures)

Safety

S(t) of a system S is defined as the probabilty that S is delivering correct service or has failed in a manner that does cause no harm in [0, t]

- S(t) is the Mean Time To Catastrophic Failure (MTTC), defined similarly to MTTF and normally expressed in hours