Attacks on Virtual Storage

Data Leakage

Data Remanence

Dumpster Diving

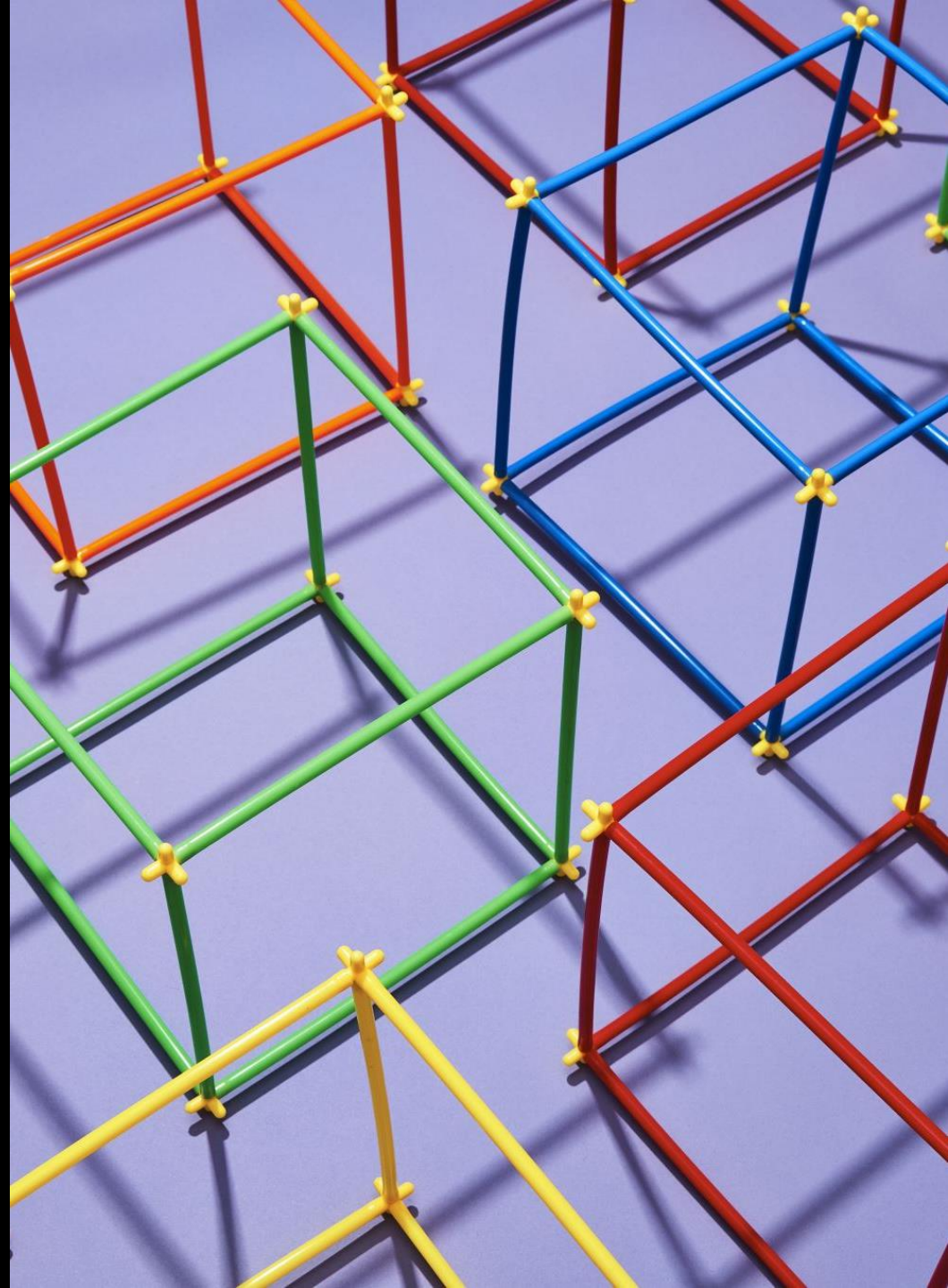
Hash Value Manipulation

Attacks on Virtual Storage

- Data Leakage:
  - Attacks such as password guessing and dumpster diving can lead to VM data leakage
  - Attacker can also use key logger and gain authentication into target VM and breach its data.

Attacks on Virtual Storage

- Data Remanence:
  - Data Remanence represents residual information of the data remained after deletion.
  - Various file handling operations such as the reformatting of storage, deletion operation may result in data remanence.
  - Such operations can cause disclosure of sensitive information



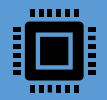
Attacks on Virtual Storage

- Dumpster Diving
  - Dumpster diving is an attempt of deriving information from data which is declared as waste.
  - The data is recovered by the attacker that is discarded by cloud users or admin to gain useful information out of it.

Attacks on Virtual Storage

- Hash Value Manipulation:
  - An attacker may manipulate the hash value of the message and can get authorized access to the file stored in the server.
  - If manipulated hash value exists in the database, server links the file to that hash value.
  - If the modified hash value does not exist, server requests a file from the user.

Attacks on Hardware (Low-Level)

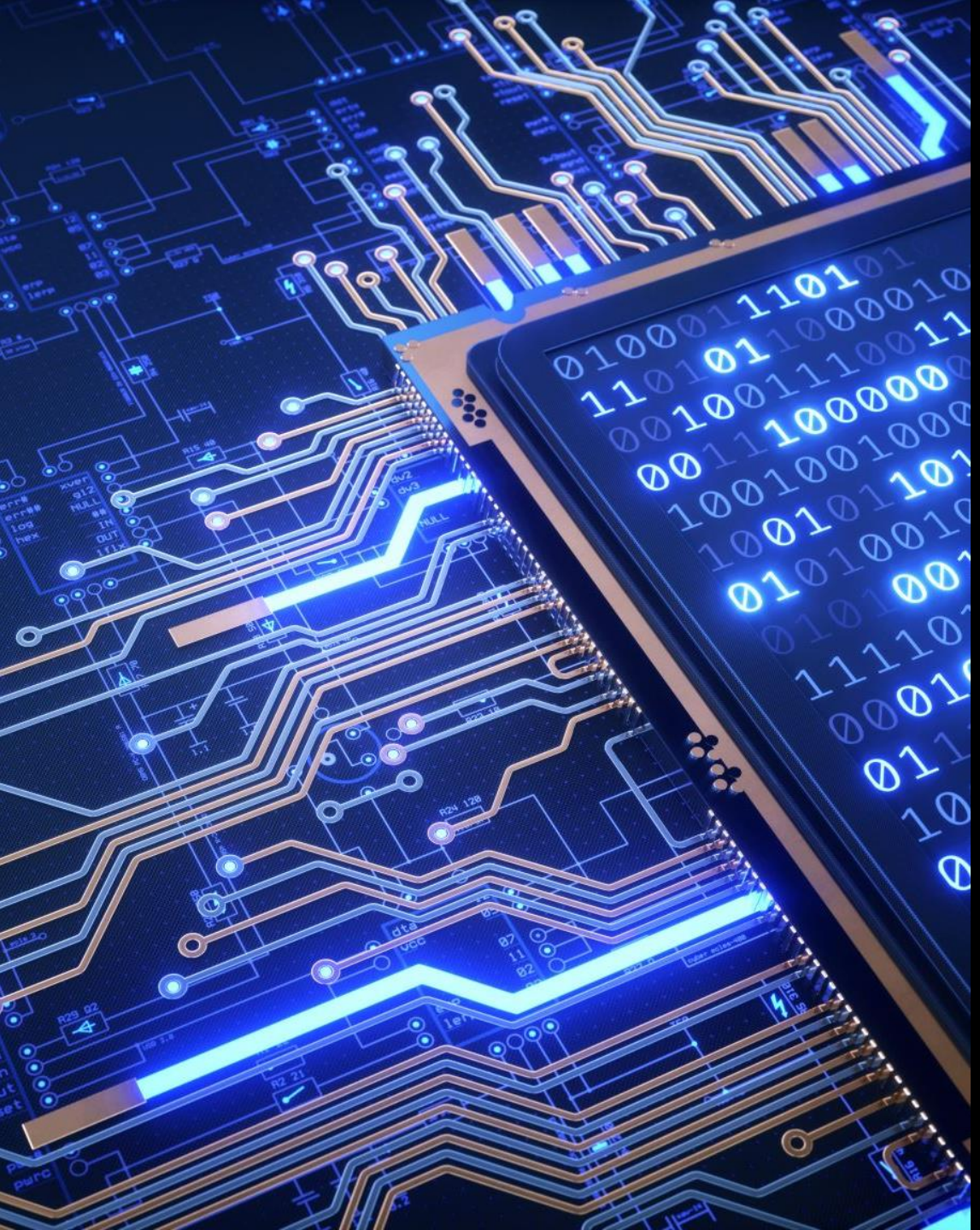


Direct Memory Access (DMA) Attack

System Management Mode (SMM)

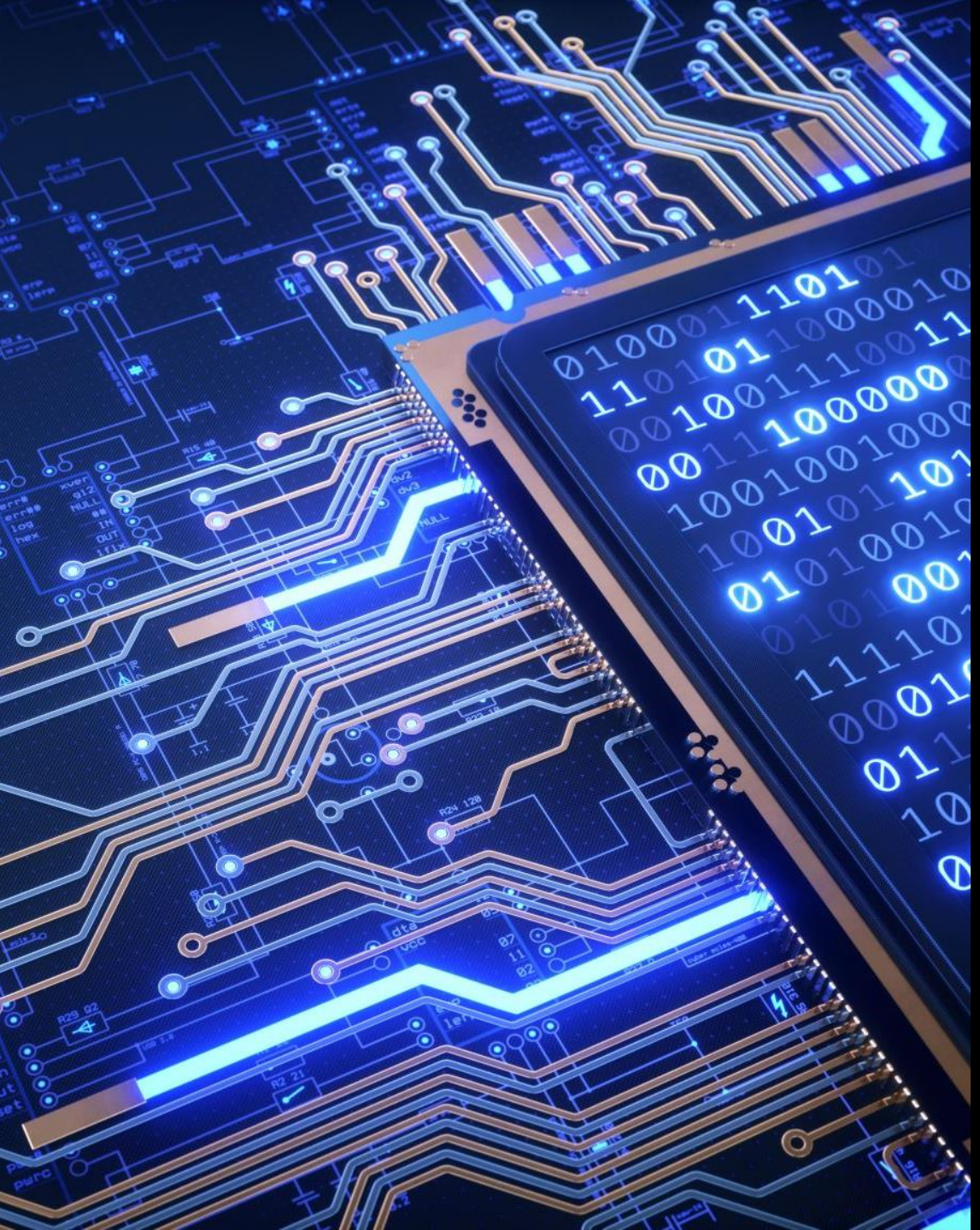
Basic input/output System (BIOS)

If physical access to the host machine is obtained, it may facilitate hardware threats on the machine



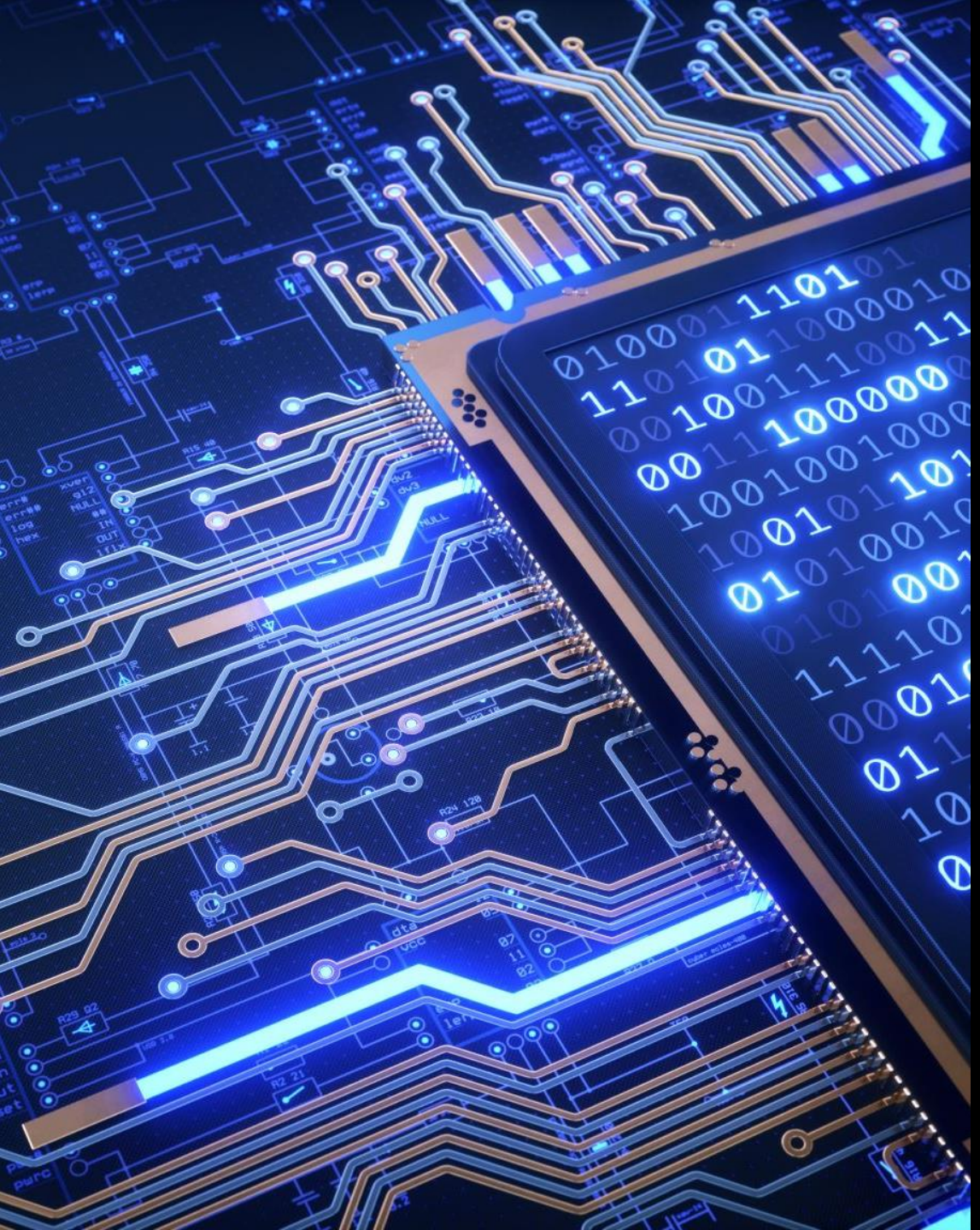
Attacks on Hardware (Low-Level)

- Direct Memory Access (DMA) Attack:
  - DMA code can be subjected to malware infections to launch stealthy attacks against host-kernel by executing on dedicated hardware.
  - An attacker can access cryptographic keys for the hard disk and user's sensitive information located in a cache



Attacks on Hardware (Low-Level)

- System Management Mode (SMM)
  - SMM is the highly privileged mode of CPU which deals with system security and power management functions
  - On insertion of the SMM pin, the CPU saves its entire state in separate address location called as SMRAM.
  - SMM is vulnerable to cache poisoning attack which allows an attacker to insert malicious code temporarily in SMRAM.



Attacks on Hardware (Low-Level)

- Basic input/output System (BIOS)
  - BIOS is responsible for implementation of SMM
  - Any vulnerability in BIOS can be used to tamper the SMM functioning and allows an attacker to take illegitimate access to system security functions