Cloud Computing Concepts

CS3132

Dr. Anand Kumar Mishra

NIIT University

Vulnerabilities, Threats, and Risks

A vulnerability is a flaw or weakness in an asset’s design, implementation, or operation and management that could be exploited by a threat.

A threat is a potential for a threat agent to exploit a vulnerability.

A risk is the potential for loss when the threat happens

More vulnerabilities you have, the greater potential for threats and the higher your risk

Asset

- Asset includes people, property, and information
    - People includes employees and other stakeholders of an organization,
    - Property means both tangible and intangible items carrying some value
    - Information means any kind of useful data such as accounts, records, etc.
- These assets are exposed to a threat, risk, and vulnerability

An intangible asset is a non-monetary asset that cannot be seen or touched. Ex. trademark, Patents, Software

Tangible assets are physical assets that can be seen, touched and felt.

exposes your organization to threats

Vulnerability

- A vulnerability is a weakness, flaw or other shortcoming in a system (infrastructure, database or software), but it can also exist in a process, a set of controls, or simply just the way that something has been implemented or deployed
- Identifying vulnerabilities is akin to answering the question,
  - “How could harm occur?”
- Sometimes, a vulnerability can exist simply from an asset’s implementation or deployment
- Example:
  - A vulnerability is leaving your car unlocked in a public parking lot. Leaving the doors unlocked does not necessarily mean harm will occur, but it is an opening for someone to go through your car
  - A vulnerability is leaving your door unlocked overnight. It alone isn’t a problem, but if a certain person comes along and enters that door, some bad, bad things might happen.

a malicious or negative event that takes advantage of a vulnerability

Threat

- Anything that could exploit a vulnerability, which could affect the confidentiality, integrity or availability of your systems, data, people and more.
- Identifying threats is akin to answering the question,
  - “Who or what could cause harm?”
- A threat is anything that could exploit a vulnerability and hinder the confidentiality, integrity, and availability of anything valuable
- Threats can either be natural or human-made and accidental or deliberate
- Example:
  - the owner of the car did not lock their door, so a carjacker could exploit the opportunity. This means the threat is human-made and deliberate.

Threat

When an adversary or attacker has the opportunity, capability and intent to bring a negative impact upon your operations, assets, workforce and/or customers

- Examples of this can include malware, ransomware, phishing attacks and more

An attacker may have the intent and capability to do harm, but no opportunity

- Example: Your organization may have no vulnerabilities to exploit due to a solid patch management program or strong network segmentation policies that prevent access to critical systems. Chances are likely, however, that you do have vulnerabilities, so let’s consider the risk factor.

the potential for loss and damage when the threat does occur

Risk

- Once we know an asset’s vulnerabilities and threats, we can determine
  - how much risk is posed to the asset owner
- This measure is the combination of the likelihood that a threat exploits a vulnerability and the scale of harmful consequences
- Example:
  - If you drive a fancy car and keep valuables in it, then your cost is high
  - Also, if you park the unlocked car in a crime-laden area, then the probability that a threat occurs is also high
  - Combining these two factors shows your car is at elevated risk in this situation.

Risk

- Risk is the probability of a negative (harmful) event occurring as well as the potential of scale of that harm
- Cybersecurity teams begin to measure the risk:
  1. Estimate how often an adversary or attacker is likely to attempt to exploit a vulnerability to cause the desired harm.
  2. Gauge how well your existing systems, controls and processes can standup to those attempts.
  3. Determine the value of the impact or harm the adversary may cause if the adversary is indeed successful.
- Risk = threat x vulnerability

Cloud security

- Cloud security is the set of cybersecurity measures used to protect cloud-based applications, data, and infrastructure
    - This includes –
        - applying security policies, practices, controls, and other technologies like
            - identity and access management and
            - data loss prevention tools
        - to help secure cloud environments against unauthorized access, online attacks, and insider threats

Cloud security

Cloud security refers to the cybersecurity policies, best practices, controls, and technologies used to secure applications, data, and infrastructure in cloud environments

Cloud security works to provide **storage and network protection** against internal and external threats, access management, data governance and compliance, and disaster recovery

Cloud Security – how does it work?

Cloud security mainly focuses on

- how to implement **policies**, **processes**, and **technologies** together
  - so they ensure:
    - data protection, support regulatory compliance, and provide control over privacy, access, and authentication for users and devices

Cloud service providers (CSPs) typically follow **a shared responsibility model**,

- which means implementing cloud computing security is both the responsibility of the cloud provider and the customer
- Think of it as a responsibility framework that defines which security tasks belong to the cloud provider and which are the duty of the customer

Cloud Security – how does it work?

CSP is always responsible for the cloud and its core infrastructure,

Customer is expected to secure anything that runs “in” the cloud, such as

network controls, identity and access management, data, and applications

Shared responsibility models vary depending on the service provider and the cloud computing service model you use—**the more the provider manages, the more they can protect**

Cloud computing service model	Your responsibility	CSP responsibility
Infrastructure as a service (IaaS)	You secure your data, applications, virtual network controls, operating system, and user access.	The cloud provider secures compute, storage, and physical network, including all patching and configuration.
Platform as a service (PaaS)	You secure your data, user access, and applications.	The cloud provider secures compute, storage, physical network, virtual network controls, and operating system.
Software as a service (SaaS)	You are responsible for securing your data and user access.	The cloud provider secures compute, storage, physical network, virtual network controls, operating system, applications, and middleware.

Cloud security solutions

- Cloud security is constantly evolving and adapting as new security threats emerge
- As a result, many different types of cloud security solutions are available on the market today, and the list below is by no means exhaustive
  - Identity and access management (IAM):
  - Data loss prevention (DLP):
  - Security information and event management (SIEM):
  - Public key infrastructure (PKI):

Identity and access management (IAM)

- IAM services and tools allow administrators to centrally manage and control who has access to specific cloud-based and on-premises resources
- IAM can enable you to actively monitor and restrict how users interact with services, allowing you to enforce your policies across your entire organization.

Data loss prevention (DLP)

- DLP can help you gain visibility into the data you store and process by providing capabilities to automatically discover, classify, and deidentify regulated cloud data

Security information and event management (SIEM)

- SIEM solutions combine security information and security event management to offer automated monitoring, detection, and incident response to threats in your cloud environments
- Using AI and ML technologies, SIEM tools allow you to examine and analyze log data generated across your applications and network devices—and act quickly if a potential threat is detected

Public key infrastructure (PKI)

- PKI is the framework used to manage secure, encrypted information exchange using digital certificates
- PKI solutions typically provide authentication services for applications and verify that data remains uncompromised and confidential through transport
- Cloud-based PKI services allow organizations to manage and deploy digital certificates used for user, device, and service authentication.

Benefits of Cloud Security

Greater visibility

Only an integrated cloud-based security stack is capable of providing the centralized visibility of cloud resources and data that is vital for defending against breaches and other potential threats

Cloud security can provide the tools, technologies, and processes to log, monitor, and analyze events for understanding exactly what's happening in your cloud environments

Centralized security

Cloud security allows you to consolidate protection of cloud-based networks for streamlined, continuous monitoring and analysis of numerous devices, endpoints, and systems

It also enables you to centrally manage software updates and policies from one place and even implement and action disaster recovery plans.

Benefits of Cloud Security

Reduced costs

With cloud security, you don’t have to pay for dedicated hardware to upgrade your security or use valuable resources to handle security updates and configurations

CSPs provide advanced security features that allow for automated protection capabilities with little to no human intervention

Data protection

The best cloud computing providers will provide data security by design, offering strong access controls, encryption for data at rest and in transit, and data loss prevention (DLP) to secure your cloud data wherever it’s located or managed.

Benefits of Cloud Security

Cloud compliance

Cloud providers go to great lengths to comply with both international and industry compliance standards, often undergoing rigorous independent verifications of their security, privacy, and compliance controls

Advanced threat detection

Reputable CSPs also invest in cutting-edge technologies and highly skilled experts to provide real–time global threat intelligence that can detect both known and unknown threats in the wild and in your networks for faster remediation

Cloud security risks and challenges

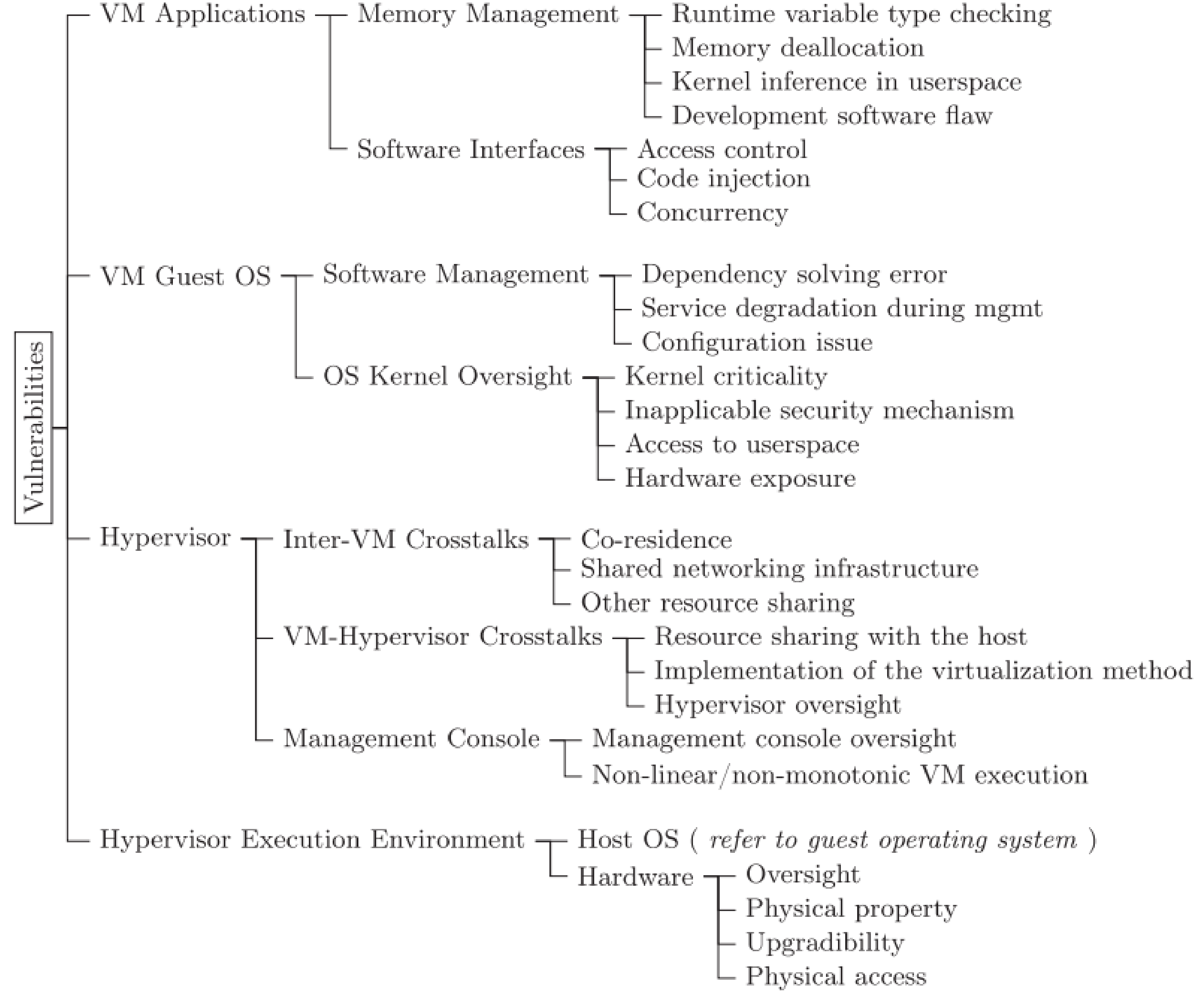
- Cloud suffers from similar security risks that you might encounter in traditional environments, such as insider threats, data breaches and data loss, phishing, malware, DDoS attacks, and vulnerable APIs
- Lack of visibility
    - Cloud-based resources run on infrastructure that is located outside your corporate network and owned by a third party
    - As a result, traditional network visibility tools are not suitable for cloud environments, making it difficult for you to gain oversight into all your cloud assets, how they are being accessed, and who has access to them

Cloud security risks and challenges

- Misconfigurations
  - Misconfigured cloud security settings are one of the leading causes of data breaches in cloud environments
  - Cloud-based services are made to enable easy access and data sharing, but many organizations may not have a full understanding of how to secure cloud infrastructure
  - This can lead to misconfigurations, such as leaving default passwords in place, failing to activate data encryption, or mismanaging permission controls
- Access management
  - Cloud deployments can be accessed directly using the public internet, which enables convenient access from any location or device
  - At the same time, it also means that attackers can more easily gain authorized resources with compromised credentials or improper access control

Cloud security risks and challenges

- Dynamic workloads
  - Cloud resources can be provisioned and dynamically scaled up or down based on your workload needs
  - However, many legacy security tools are unable to enforce policies in flexible environments with constantly changing and ephemeral workloads that can be added or removed in a matter of seconds
- Compliance
  - The cloud adds another layer of regulatory and internal compliance requirements that you can violate even if you don’t experience a security breach
  - Managing compliance in the cloud is an overwhelming and continuous process
  - Unlike an on-premises data center where you have complete control over your data and how it is accessed, it is much harder for companies to consistently identify all cloud assets and controls, map them to relevant requirements, and properly document everything.

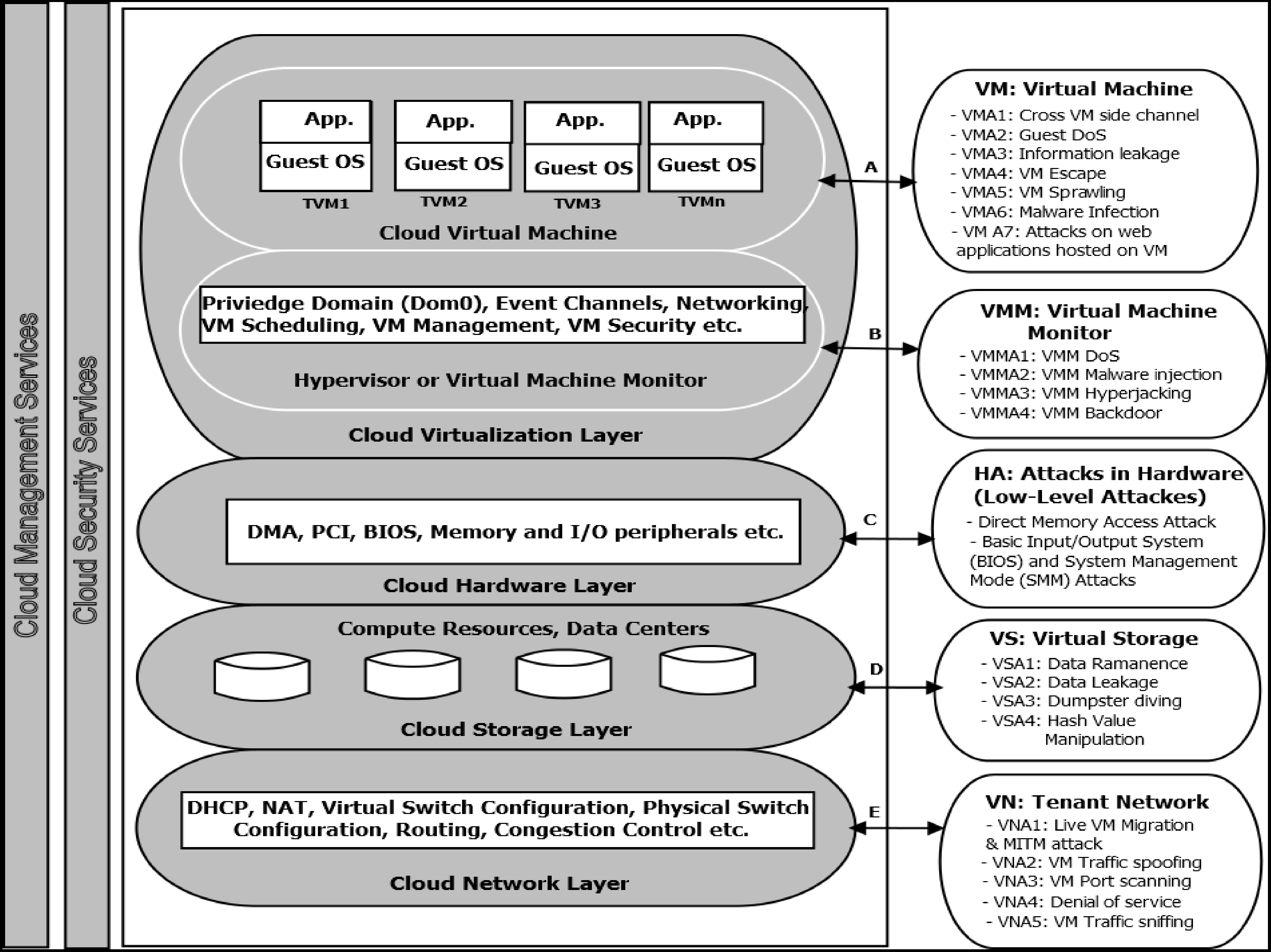


- Vulnerabilities
  - VM Applications
    - Memory Management
      - Runtime variable type checking
      - Memory deallocation
      - Kernel inference in userspace
      - Development software flaw
    - Software Interfaces
      - Access control
      - Code injection
      - Concurrency
  - VM Guest OS
    - Software Management
      - Dependency solving error
      - Service degradation during mgmt
      - Configuration issue
    - OS Kernel Oversight
      - Kernel criticality
      - Inapplicable security mechanism
      - Access to userspace
      - Hardware exposure
  - Hypervisor
    - Inter-VM Crosstalks
      - Co-residence
      - Shared networking infrastructure
      - Other resource sharing
    - VM-Hypervisor Crosstalks
      - Resource sharing with the host
      - Implementation of the virtualization method
      - Hypervisor oversight
    - Management Console
      - Management console oversight
      - Non-linear/non-monotonic VM execution
  - Hypervisor Execution Environment
    - Host OS (*refer to guest operating system*)
    - Hardware
      - Oversight
      - Physical property
      - Upgradibility
      - Physical access

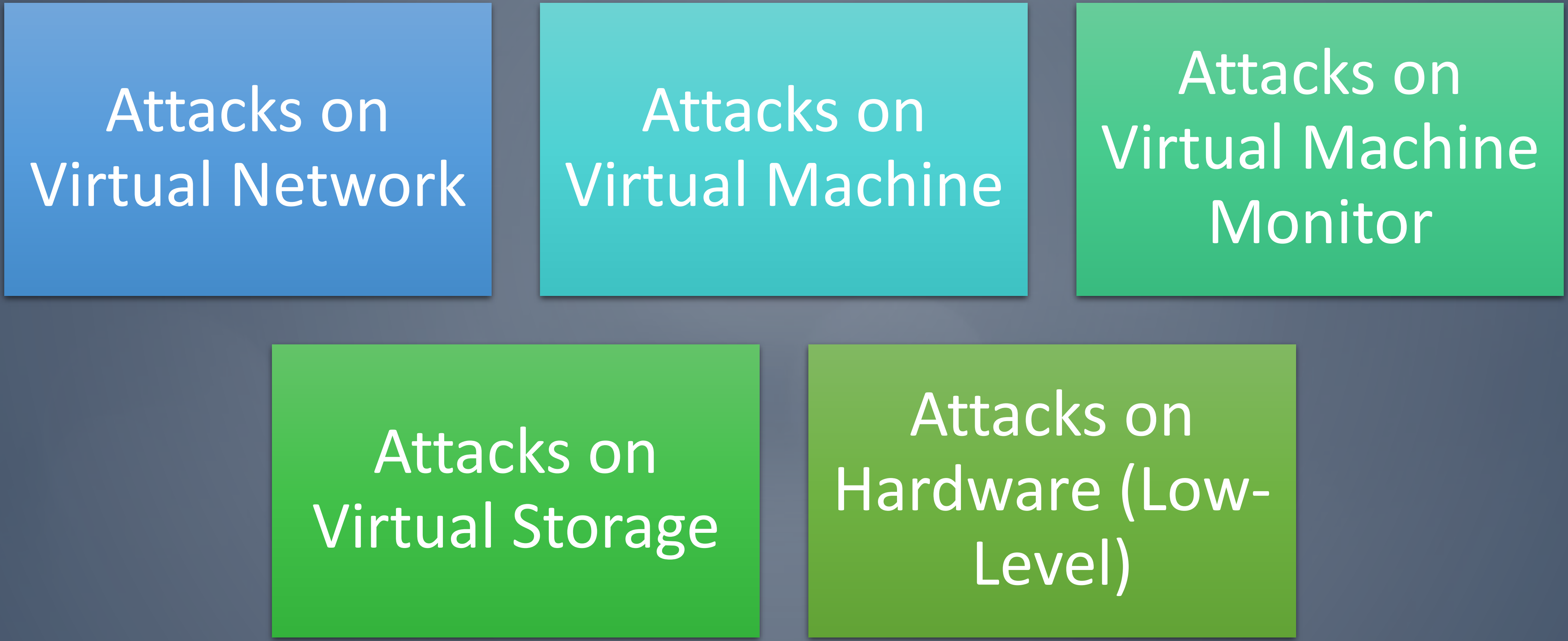
Classification of considered vulnerabilities

From virtualization security issues to cloud protection opportunities: An in-depth analysis of system virtualization models

Attacks on Cloud Computing Environment


Cloud Management Services
Cloud Security Services
App.
Guest OS
TVM1
App.
Guest OS
TVM2
App.
Guest OS
TVM3
App.
Guest OS
TVMn
Cloud Virtual Machine
Priviedge Domain (Dom0), Event Channels, Networking, VM Scheduling, VM Management, VM Security etc.
Hypervisor or Virtual Machine Monitor
Cloud Virtualization Layer
DMA, PCI, BIOS, Memory and I/O peripherals etc.
Cloud Hardware Layer
Compute Resources, Data Centers
Cloud Storage Layer
DHCP, NAT, Virtual Switch Configuration, Physical Switch Configuration, Routing, Congestion Control etc.
Cloud Network Layer
A
B
C
D
E
VM: Virtual Machine
- VMA1: Cross VM side channel
- VMA2: Guest DoS
- VMA3: Information leakage
- VMA4: VM Escape
- VMA5: VM Sprawling
- VMA6: Malware Infection
- VM A7: Attacks on web applications hosted on VM
VMM: Virtual Machine Monitor
- VMMA1: VMM DoS
- VMMA2: VMM Malware injection
- VMMA3: VMM Hyperjacking
- VMMA4: VMM Backdoor
HA: Attacks in Hardware (Low-Level Attackes)
- Direct Memory Access Attack
- Basic Input/Output System (BIOS) and System Management Mode (SMM) Attacks
VS: Virtual Storage
- VSA1: Data Ramanence
- VSA2: Data Leakage
- VSA3: Dumpster diving
- VSA4: Hash Value Manipulation
VN: Tenant Network
- VNA1: Live VM Migration & MITM attack
- VNA2: VM Traffic spoofing
- VNA3: VM Port scanning
- VNA4: Denial of service
- VNA5: VM Traffic sniffing

Attacks on Cloud Environment



Attacks on Virtual Network

Attacks on Virtual Machine

Attacks on Virtual Machine Monitor

Attacks on Virtual Storage

Attacks on Hardware (Low-Level)

Attacks on Virtual Network

- Man-In-The-Middle attack
- VM Traffic Sniffing
- VM Traffic Spoofing
- VM Port Scanning
- Denial of Service

Attacks on Virtual Network

Man-In-The-Middle attack:

- Adversary may sit between two VM machines and may try to sniff the packets passing through it when VM is migrated, or when VMs communicate with each other.
- An attacker can modify the data in communication by generating its private key and sending to the CSP on behalf of the legitimate user.

VM Traffic Spoofing:

- All VMs on the same network segment are open to attacks and compromise from other VMs present on the same network.
- A malicious user on one VM can perform IP spoofing in which attack traffic is generated on behalf of legitimate tenant user and sent to destination VM

Attacks on Virtual Network

VM Port Scanning:

- Port scanning is an attack that does not cause any harm on the VMs, but it gives the attacker some specific information about the status of the ports that can be used for further attacks such as DoS attacks.

Denial of Service:

- Attacker floods with spoofed packets to the broadcast address. The sender address is target VM's IP address providing a service on the cloud.
- On receiving the packet, each node responds to the server hosting the VM with particular spoofed IP, consuming the resources so that it can no longer provide its intended service.

Attacks on Virtual Network

- VM Traffic Sniffing:
  - VMs are connected via virtual switches, packet sniffing is done at the virtual switch level.
  - Physically the VMs share the same hardware resources.
  - Attacker can exploit this vulnerability in sniffing the virtual network to gain sensitive information of VMs.

Attacks on Virtual Machine

- VM Cross Side Channel
- Guest Denial-of-Service
- VM Escape
- VM Information leakage
- VM Sprawling
- Malware Infection
- Attack on Web Applications Hosted on VM

Attacks on Virtual Machine

Cross VM Side Channel:

- Time, cache, heat and power used to extract confidential information

Guest Denial-of-Service:

- A VM can consume all the resources causing DoS to other applications

VM Escape:

- An attack in which attacker gain access to the memory that is beyond access of compromised tenant VM. Its breaking out of a VM and interacting with VMM / host Operating System

Attacks on Virtual Machine

VM Information leakage:

- This can be caused by VMI functions and access hardware states, system call information or breakpoint injection

Malware Infection:

- Attacker can inject malware in a VM to gain root access. Malware can be a worm or can be malicious code injected into normal program

Attack on Web Applications Hosted on VM:

- Cross Site Scripting, Phishing, Cookie Manipulation

Attacks on Virtual Machine Monitor

- VMM DoS
- VMM Malware Injection
- VMM Hyperjacking
- VMM Backdoor

Attacks on Virtual Machine Monitor

VMM DoS:

- Resource starvation of RAM, CPU and bandwidth cause DoS resulting in shutdown of the VM or restart each time.

VMM Malware Injection:

- Injected Malware can disable or infect critical component like VMM

Attacks on Virtual Machine Monitor

VMM Hyperjacking:

- Installing a rogue hypervisor that can take complete control of a server. Hypervisor level root kits exploit hardware virtualization features.

VMM Backdoor:

- An attacker can take a backdoor entry into hypervisors privilege domains by overwriting the hypervisor code and manipulating kernel data structures of guest OS

Attacks on Virtual Storage

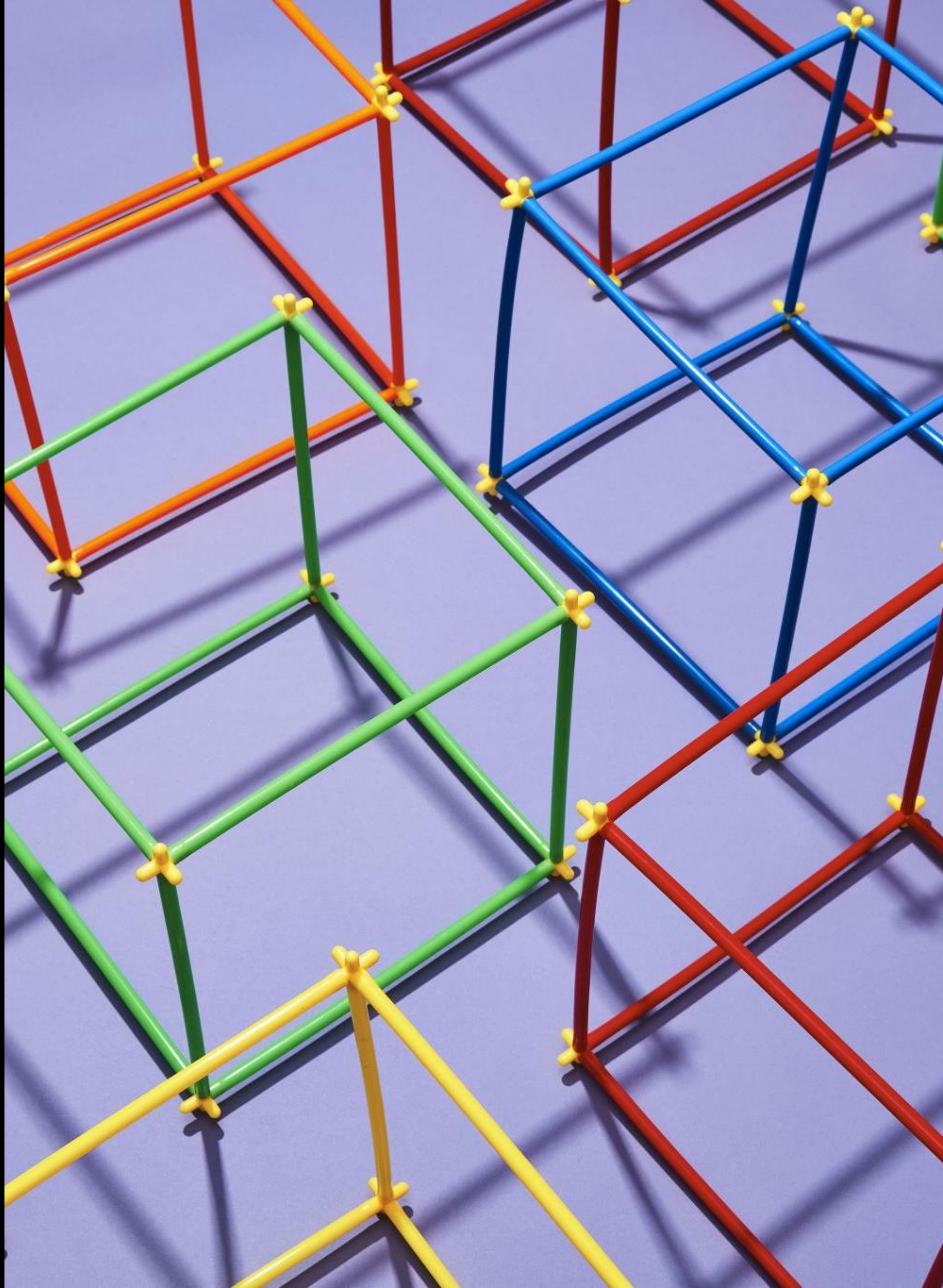
- Data Leakage
- Data Remanence
- Dumpster Diving
- Hash Value Manipulation

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

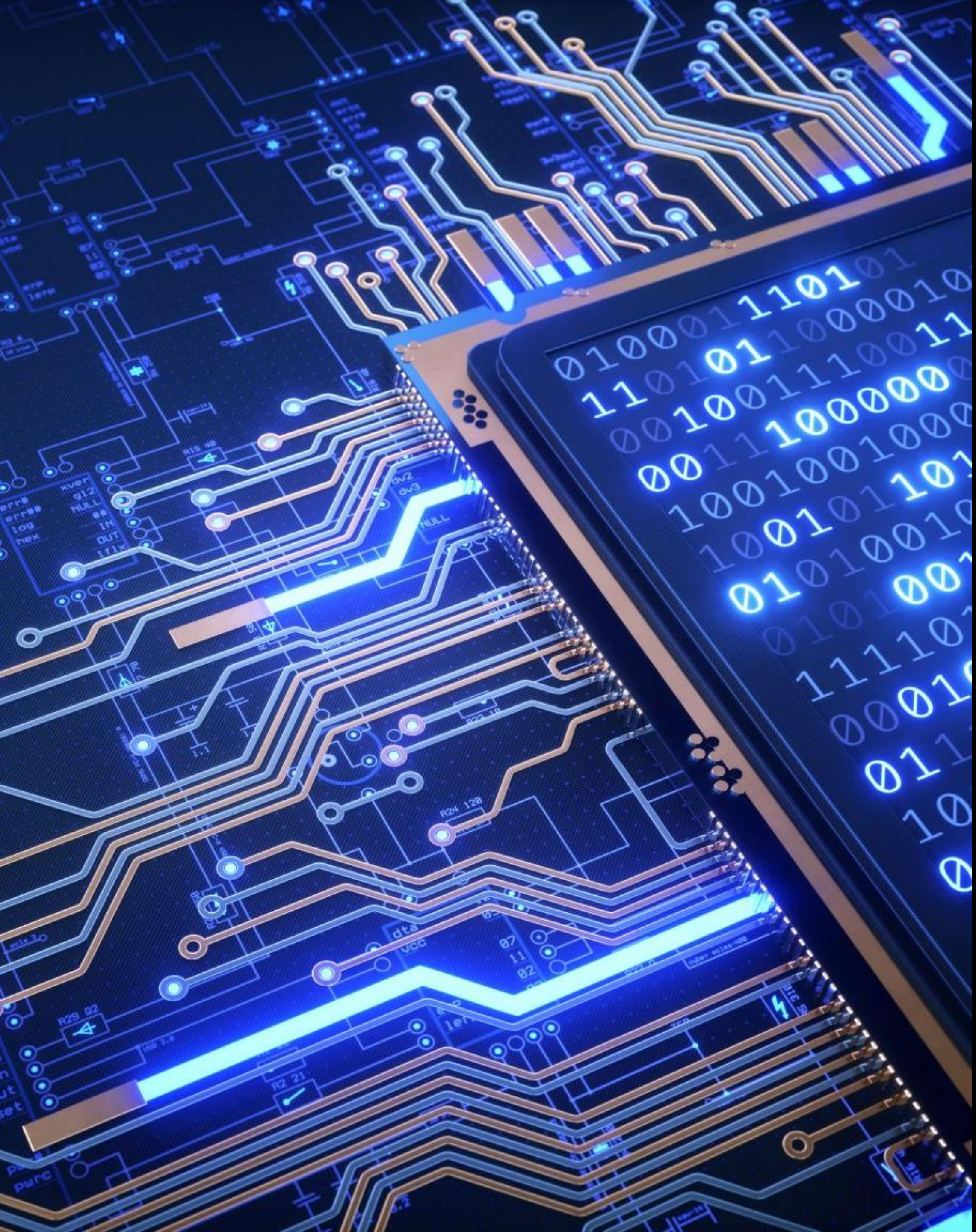
- Dumpster Diving
  - Dumpster diving is an attempt of deriving information from data which is declared as waste.
  - The data is recovered by the attacker that is discarded by cloud users or admin to gain useful information out of it.

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.

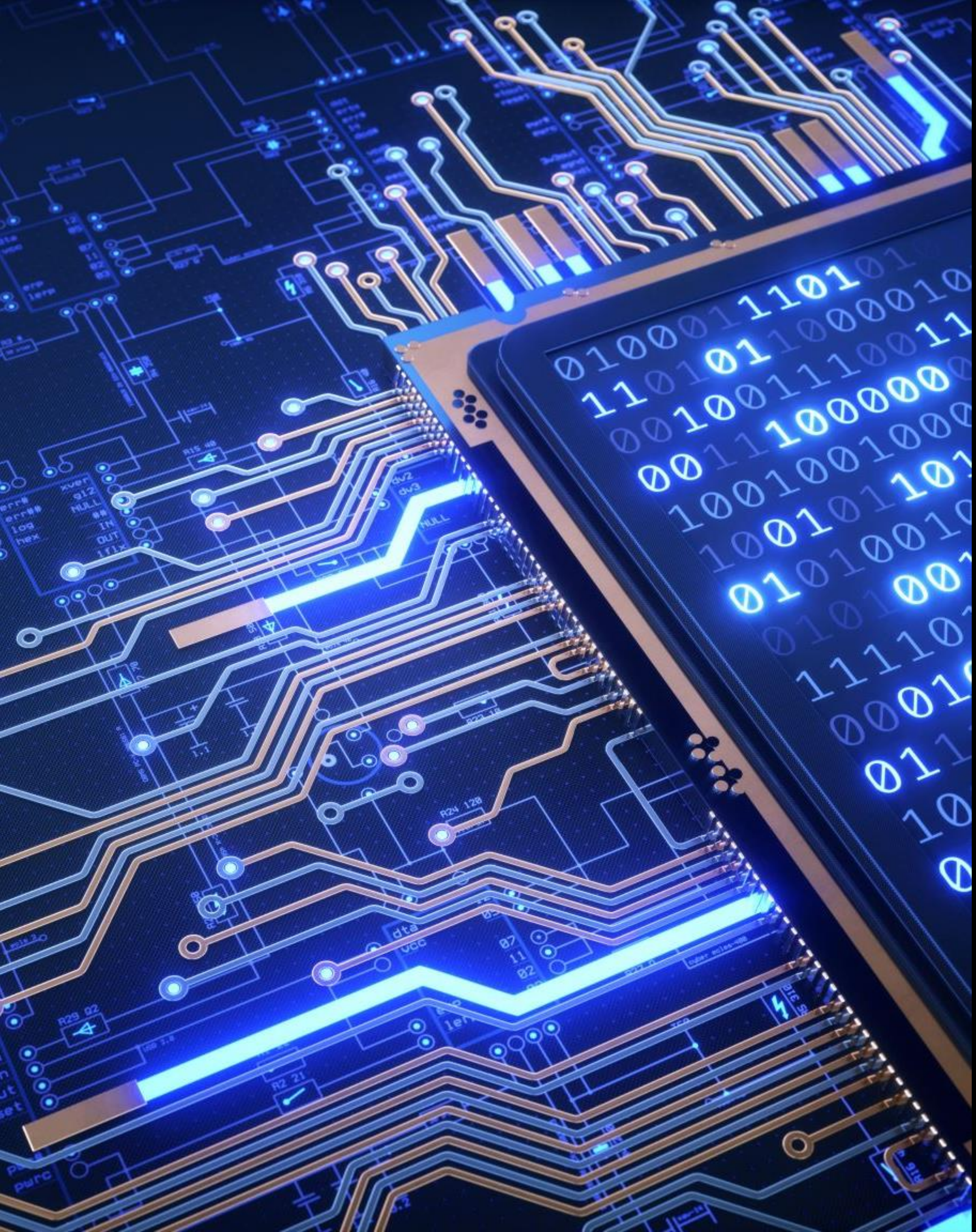
Attacks on Hardware (Low-Level)

- 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



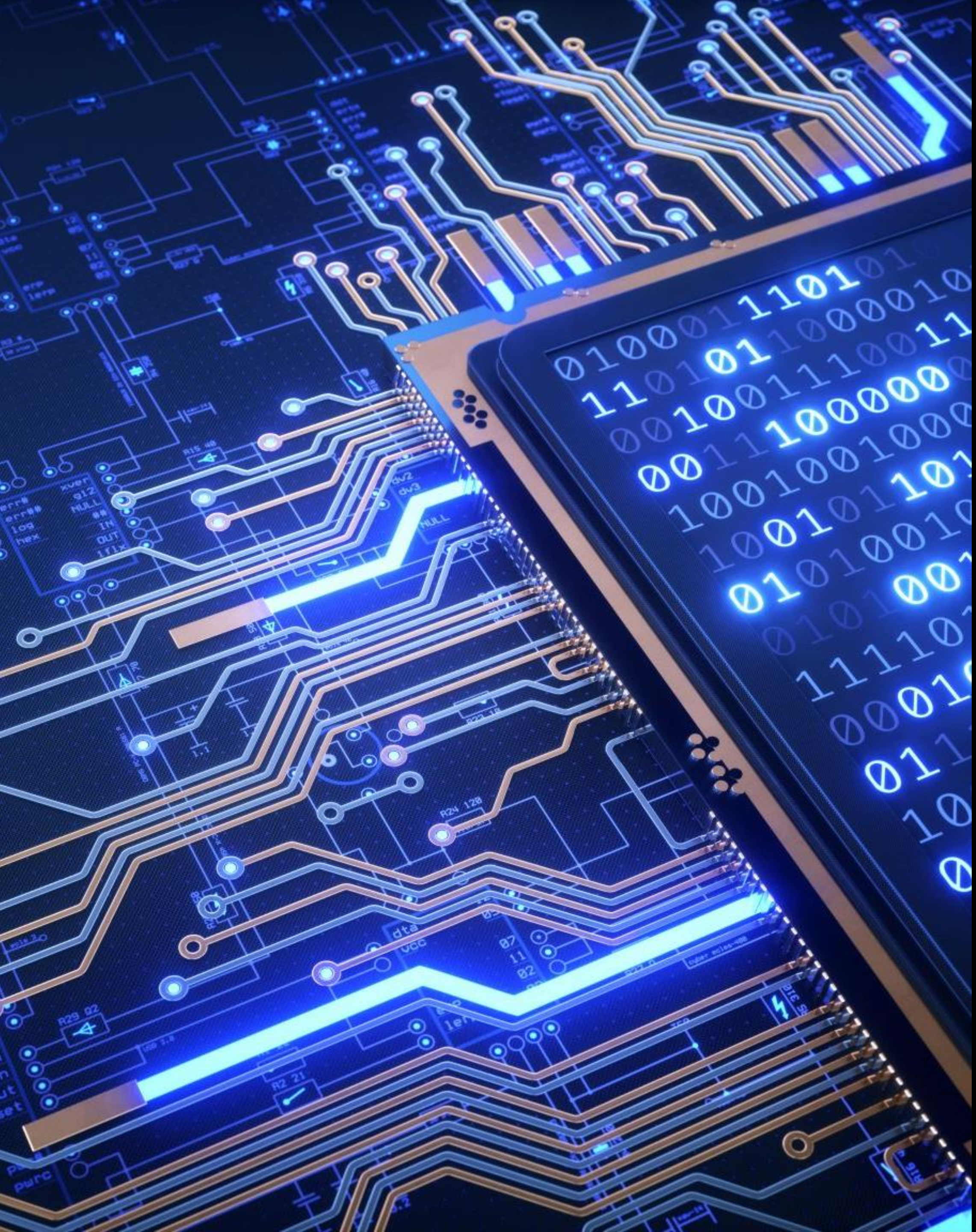
Attacks on Hardware (Low-Level)

- 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