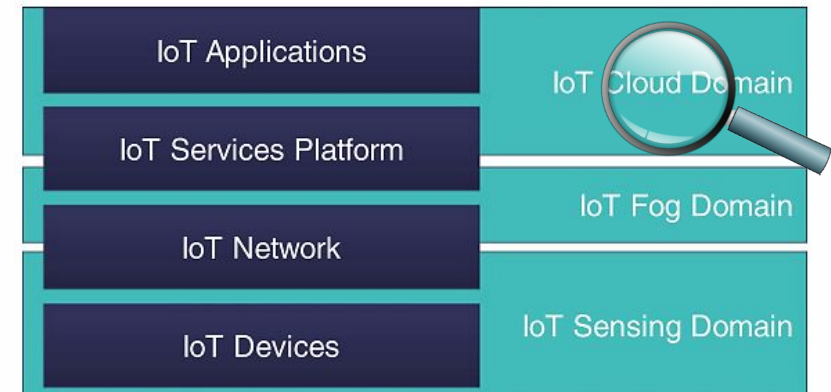


Ch. 14 - IoT Security and Privacy

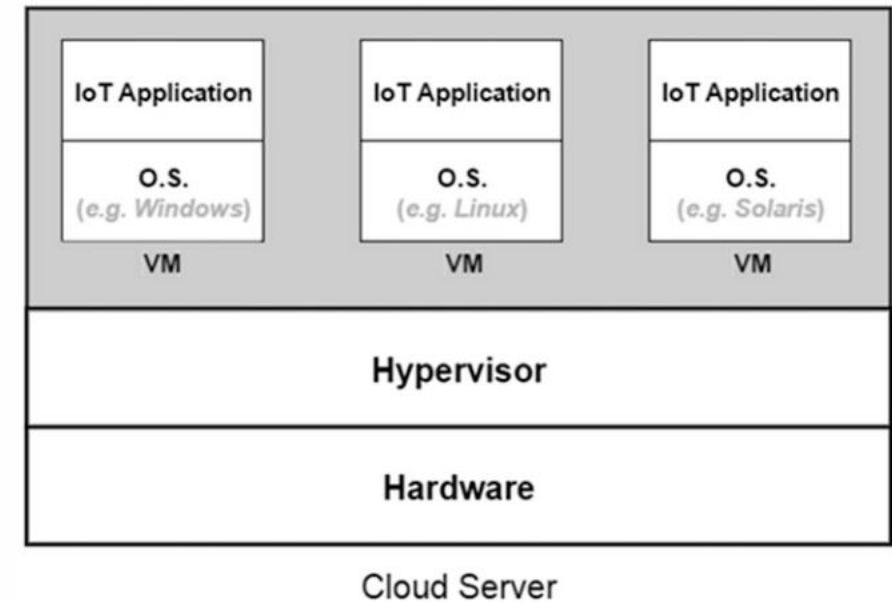
Sec 2 – Cloud Domain

COMPSCI 244p
Internet-of-Things; Software and Systems



Cloud Domain – Hypervisor based structure

- IoT application can have one or multiple dedicated virtual machines (VMs)
 - Cloud data center is made up of thousands of servers
 - Certain amount of CPU and memory resources are allocated
 - One server can accommodate several VMs
- Hypervisor
 - Manages how VMs share the server's hardware
 - Provides the logical separation among VMs
 - Migrates VMs on the server to another server



Cloud Domain – Attacks

Five categories of cloud domain attacks:

1. Hidden-Channel Attacks
2. VM Migration Attacks
3. Theft-of-Service Attack
4. VM Escape Attack
5. Insider Attacks



Cloud Domain – 1. Hidden-Channel Attacks

- Some hardware components are shared among VMs.
 - E.g. Cache, on-chip communication, etc.
- Opportunities for **data leakage** across the VMs on the **same** server.
- The steps for attack are as follows:
 - Step1: Mapping Target VM
 - Step2: Malicious VM Placement
 - Step3: Cross-VM Data Leakage

Cloud Domain – 1. Hidden-Channel Attacks

Step 1: Mapping Target VM

- **Gaol:** To locate where the target VM resides
- Cloud data center is divided into multiple clusters
 - Each cluster is in a certain **geographical location** and is made up of **thousands** of **servers**
- To know where a target VM resides, the attacker needs only to know the **external IP** address of that VM
 - External IP address => geographical location
- To identify in what zone within the cluster the target VM resides the target VM's **internal IP** address is needed
 - VMs within the same zone have the same network prefix
 - The attacker rents a VM in the same cluster
 - Query the DNS server of the cloud cluster from the rented VM => fetch internal IP address of the target VM

Cloud Domain – 1. Hidden-Channel Attacks

Step 2: Malicious VM Placement

- **Goal:** To place a malicious VM on the same server where the target VM resides
- The following process is needed:
 - The attacker rents a VM in the same cluster as the target VM
 - The scheduling algorithm places the rented VM on one of the servers within one of the cluster's zones
 - The attacker performs a **traceroute** from the rented VM to the target VM
 - **Multiple hops** from the target VM to the rented VM => the rented VM and target VM are **NOT** in the same server
 - The attacker **releases** the rented VM and requests a **new** one
 - Do it repeatedly to succeed

Cloud Domain – 1. Hidden-Channel Attacks

Step 3: Cross-VM Data Leakage

- **Goal:** To learn some information about the target VM by exploiting the shared server's hardware
- For example, learn what lines of cache (data or instruction) the target VM has **accessed** recently
 - The attacker **fills** the whole shared cache by **dummy** data
 - Observing the time it takes to access each chunk of the dummy data after the target VM changes some chunks
 - Short time => cache access
 - Long time => memory access
 - Extracting addresses the target VM has accessed recently
 - Access pattern partially recovers the security keys

Cloud Domain – 1. Hidden-Channel Countermeasures

- Hard Isolation
 - To separate the cache dedicated for each VM
 - To assign only one VM to each server
 - Both facing cloud underutilization problem!
 - Cloud client specify a list of trusted cloud users (**white list**), and sharing the server with only the VMs in the white list
 - New scheduling algorithms are needed.
 - VM must have a list of identified untrusted VMs (**black list**)
- Cache Flushing
 - To flush the shared cache every time the allocation of the cache is switched from a VM to another
 - Performance degradation!

Cloud Domain – 1. Hidden-Channel Countermeasures II

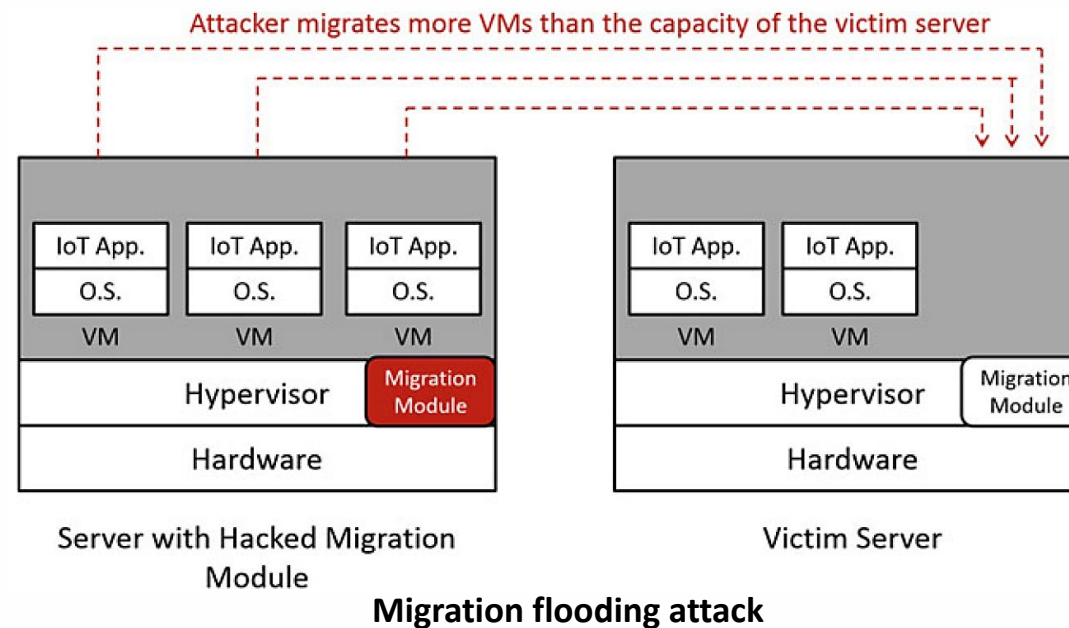
- Noisy Data Access Time
 - Adding **random noise** to the amount of **time** needed to fetch data
 - Fetched data gets delayed due to the noise
- Limiting Cache Switching Rate
 - Limiting how often the cache is switched from a VM to another
 - i.e., the cache is not switched too soon

Cloud Domain - 2. VM Migration Attacks

- **Live** VM migration allows moving a VM transparently from a server to another
 - live => only hundreds of milliseconds disruption
 - Useful for maintenance, patch installation, or load balancing
- 1. Copying the VM's memory content
- 2. If the destination server is the same local network, VM will keep the same IP address
- 3. An ARP (Address Resolution Protocol) reply packet is sent to the routing devices within the cloud to inform about the VM's new physical address

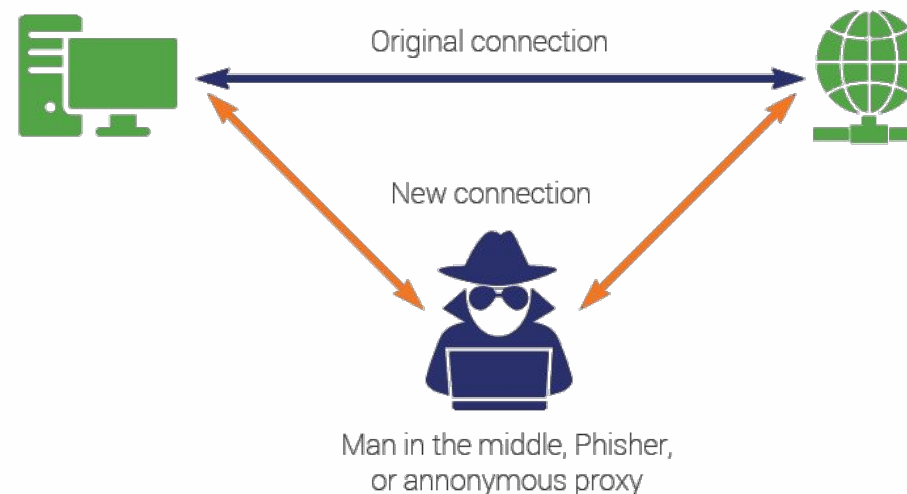
Cloud Domain - 2. VM Migration Attacks II

- **Control Plane Attacks** (taking control over the migration module):
 - Migration Flooding:
 - Overloading the victim server to cause a DoS
 - False Resource Advertising:
 - Claiming that it has a large resource slack
 - Some VMs are off-loaded to the hacked server



Cloud Domain - 2. VM Migration Attacks III

- **Data Plane Attacks** (targeting the network links over which the VMs are moved):
 - Sniffing Attack:
 - Reads migrated memory pages via sniffing the exchanged packets
 - Man-In-The-Middle Attack:
 - Fabricating an ARP Reply packet to receive the victims VM data by the attacker's malicious VM
 - The attacker continues to forward the packets to the victim VM to hide the attack

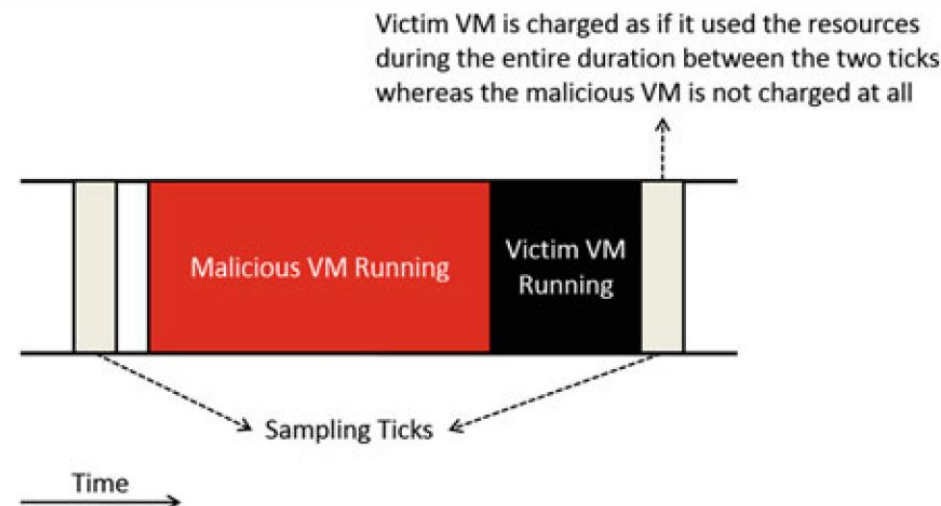


Cloud Domain - 2. VM Migration COUNTERMEASURES

- ✓ **Mutual authentication** between the source and destination servers prior to migration.
- ✓ Control messages should be encrypted and signed by the respective entity
 - ✓ Avoids fabricating fake control messages
- ✓ Sequence numbers for control messages
 - ✓ Prevent a malicious entity from **replaying** an **old** control message
- ✓ ARP reply packets should be accepted only after authentication

Cloud Domain - 3. Theft-of-Service Attack

- A malicious VM misbehaves to obtain more resources than its share from the hypervisor
 - Victim VMs get allocated less share of resources than what they should obtain.
 - **Xen** is a well-known hypervisor that is susceptible to this attack
 - Xen samples every 10 ms VMs core utilization
 - It assumes the VM has had the core during the entire 10 ms



Cloud Domain - 3. Theft-of-Service Countermeasures

1. To **log more accurately** the start and end time when each VM was utilizing the cores
 - Using accurate clocks
2. To randomize the sampling times

Cloud Domain - 4. VM Escape Attack and Countermeasures

- **Attack**: Software bugs can be exploited to **break the isolation** and **escape the hypervisor layer** and **reaches** the server's **hardware**
 - VM can **gain root access** to the whole server where it resides
- **Countermeasure**: **CloudVisor** adds an extra isolation layer between the hardware and the hypervisor through **nested virtualization**
 - Prevents obtaining the root privileges even if hypervisor is bypasses

Cloud Domain - 5. Insider Attacks and Countermeasures

- **Attack**: Someone with access to the cloud server can perform the attack
 - Data center **administrators** might be the risk!
 - **Sensitive applications** may have serious concerns about hosting their information on the cloud.
- **Countermeasures**:
 - Homomorphic encryption: Allows cloud servers to perform certain computing operations on **encrypted input** data to generate **an encrypted result**.
 - Only the **smart objects** and the **user** running the IoT application can **interpret** these data.
 - Data storage: Data is broken down into multiple chunks and sorted with permutations defined by a secret key. Data is uninterpretable for the administrators.

Cloud Domain - Summary of the security attacks

Attack	Vulnerability Reason	Security Violation	Countermeasures
Hidden-Channel Attack	Shared hardware components (e.g. cache) among the server's VMs	Confidentiality	<ul style="list-style-type: none">- Hard Isolation- Cache Flushing- Noisy Data Access Time- Limiting Cache Switching Rate
VM Migration attacks	<ul style="list-style-type: none">- VM Migration software bugs- VM Migration is performed without authentication- Memory pages copied in clear	Confidentiality Integrity Availability	<ul style="list-style-type: none">- Server authentication- Encrypting migrated memory pages
Theft-of-Service Attack	Periodic sampling of VMs' used resources	Availability Non-Repudiation	<ul style="list-style-type: none">- Fine-grain sampling using high precision clocks- Random sampling
VM Escape Attack	Hypervisor software bugs	Confidentiality Availability Integrity	<ul style="list-style-type: none">- Add an isolation domain between the hypervisor and hardware
Insider Attacks	Lack of trust in cloud administrators	Confidentiality Integrity	<ul style="list-style-type: none">- Homomorphic Encryption- Secret storage through data chopping and permutation based on a secret key