Cloud Computing Security and Privacy

A. Tassanaviboon
ECE University of Waterloo

Outline

- What is cloud computing
- What are Cloud’s Benefits
- Cloud Architecture
  - Characteristics
  - Layers
  - Service Models
- Cloud Security
  - Security Concern
  - Threats
  - Attacks
  - New direction

What is cloud computing

- Gartner

“a style of computing where massively scalable IT related capabilities are provided 'as a service' using Internet technologies to multiple external customers”

- NIST

“a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources and services, that can be rapidly provisioned and released with minimal management effort or service provider interaction"

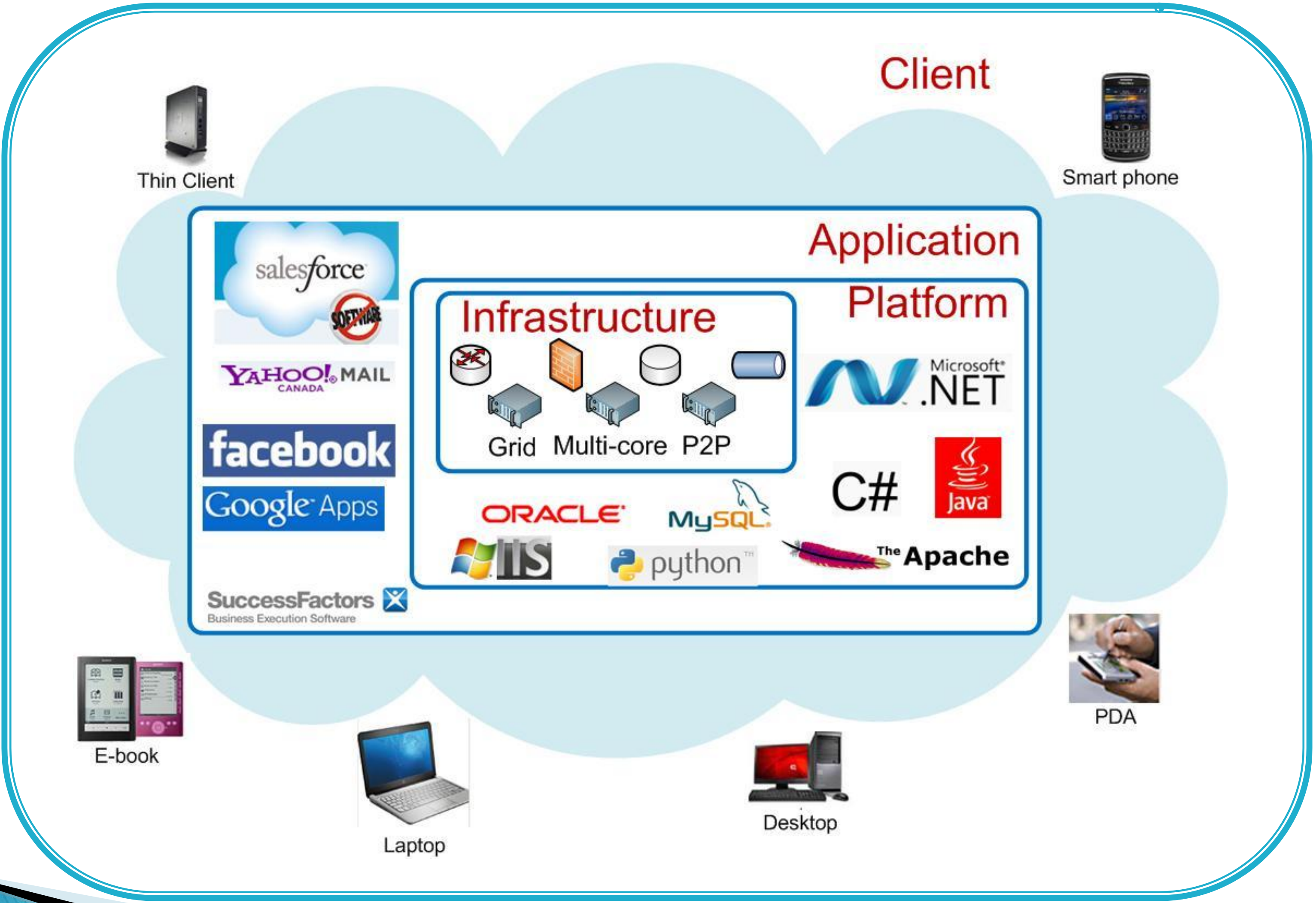
What are Cloud’s Benefits

- Business
  - Convert most expenditures to on-demand payment, aka. 5th utility.
  - Less investment and operation cost
  - Quickly and flexibly react to market.
- Engineering
  - Rapidly scalable and unlimited resource.
  - No upfront engineer for peak load.
  - No restriction for access devices.

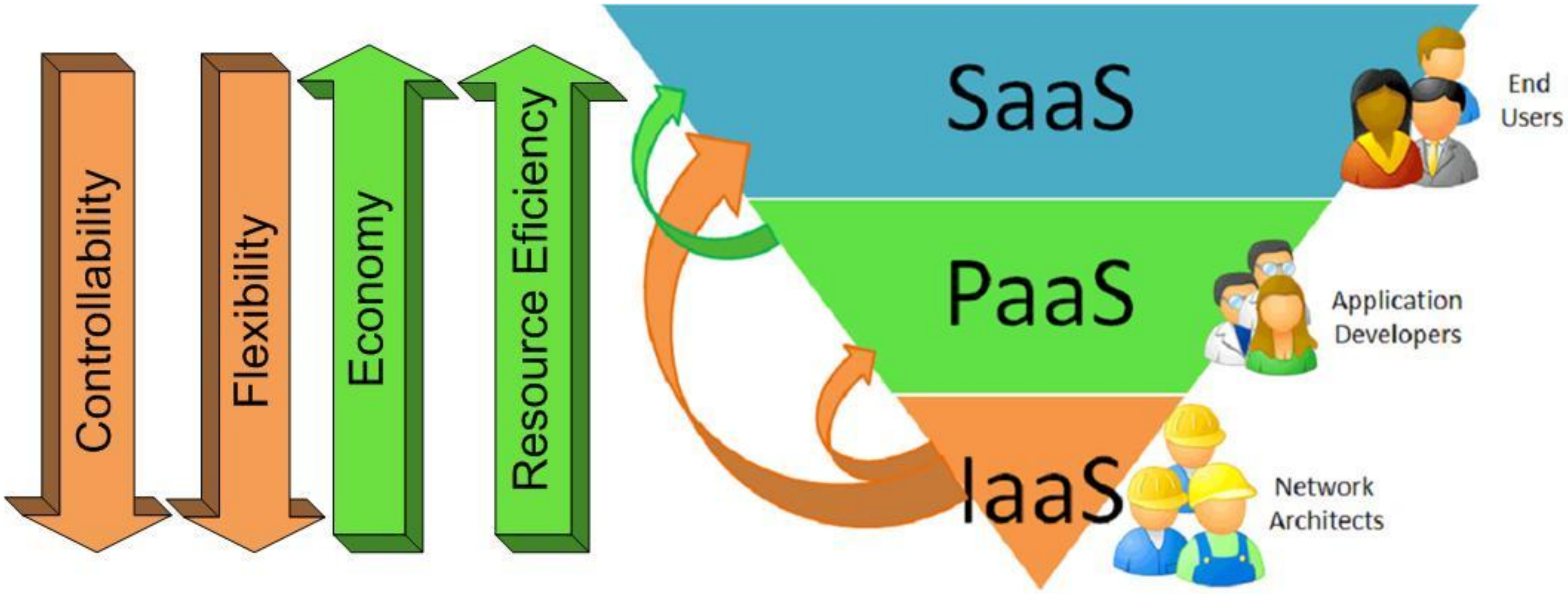
Cloud's Characteristics

- Elastic Capability
  - Resource capability scale according to user's request or automatically scale to the real load.
  - Scale with minimal effort or human interface.
- Virtualization
  - Shared resource pool
  - Isolation in multi-tenant environment,
  - Load balance, redundancy, disaster recovery
  - Transparency for user's perspective
- Measured Services
  - Cloud users: fine tune and optimization
  - Cloud providers: monitor, control, and prevent
- Broad Access
  - Internet access and standard protocols
  - Thick/ thin clients and mobile devices

Cloud's Layers



Cloud's Service Models



Cloud's Security Constaints

1. Our sensitive data and computing are controlled by cloud provider.

2. Must trust in the instance and storage isolation managed by cloud.

3. Must understand security function boundary between cloud user and provider.

Threats to Clouds

- External Threats
  - Spoofing, eavesdropping, MITM, flooding, DoS, etc.
  - Viruses, worms, Trojan horses, Rootkits, spywares, etc.
- Internal Threats
  - Side/covert channel
  - Malicious/illegal images
- Untrusted Providers
  - Manipulate our data and computing like their own.
  - Data Lock-in, unauthorized data mining
  - Audit difficulty, contractual obligation

Attacks on Clouds

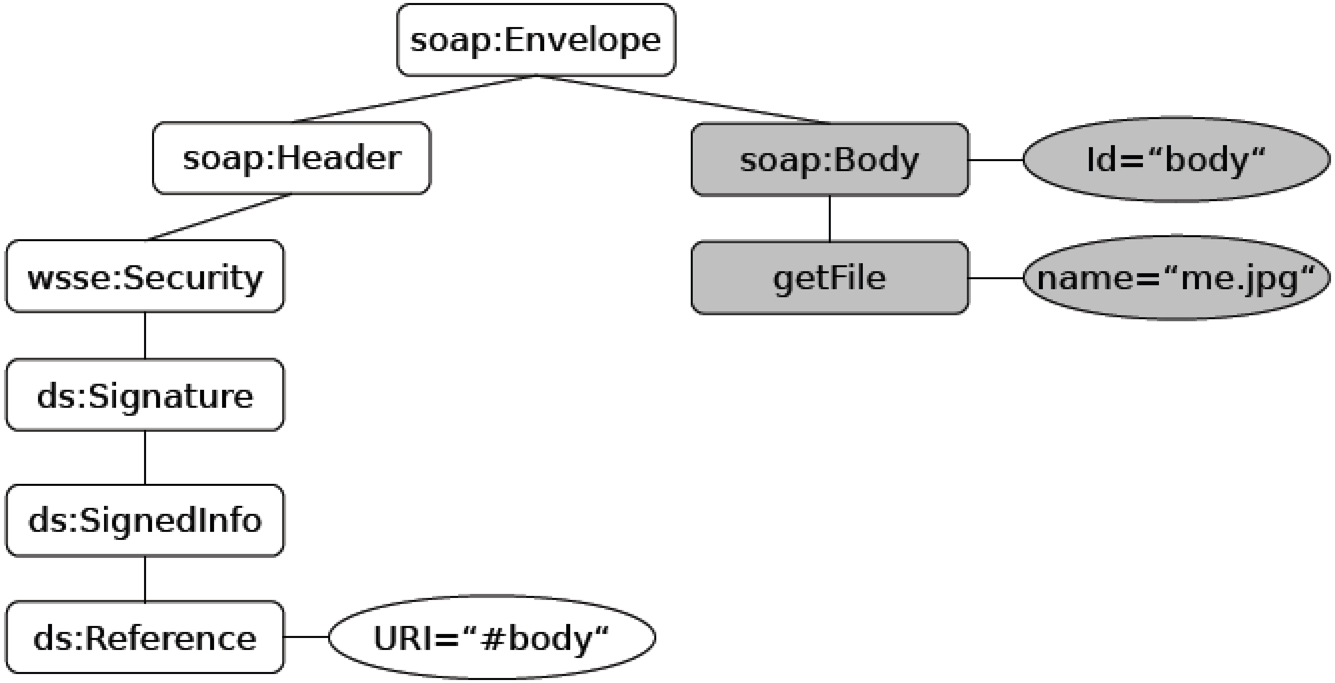
- Web Interface Attacks
- Malicious/illegal Image Attacks
- Cache Interference Attacks
- Metadata spoofing attacks
- Flooding attacks
- Etc.

Web Service Attacks

- Web is a common tool:
  - SaaS: Web browsers
  - PaaS: Web APIs
  - IaaS : Web portals
- Legacy Same Origin Policy
  - Origin: (*domain name, protocol, port*)
  - DNS cache poisoning
- Unsecure Browser Authentication
  - Username/password
  - Token-based authentication
    - e.g. Microsoft Passport and REST

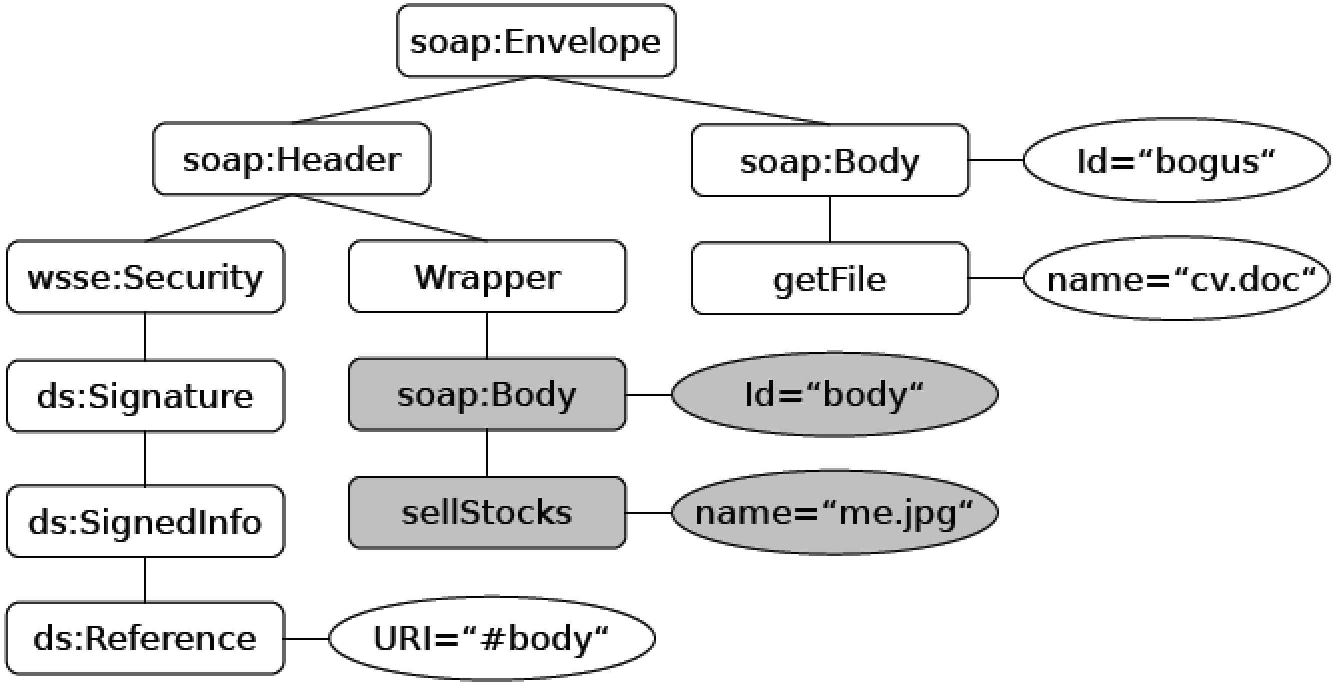
Web Service Attacks (Cont.)

- XML Signature Element Wrapping



Web Interface Attacks (Cont.)

- XML Signature Element Wrapping



Web Service Attacks (Cont.)

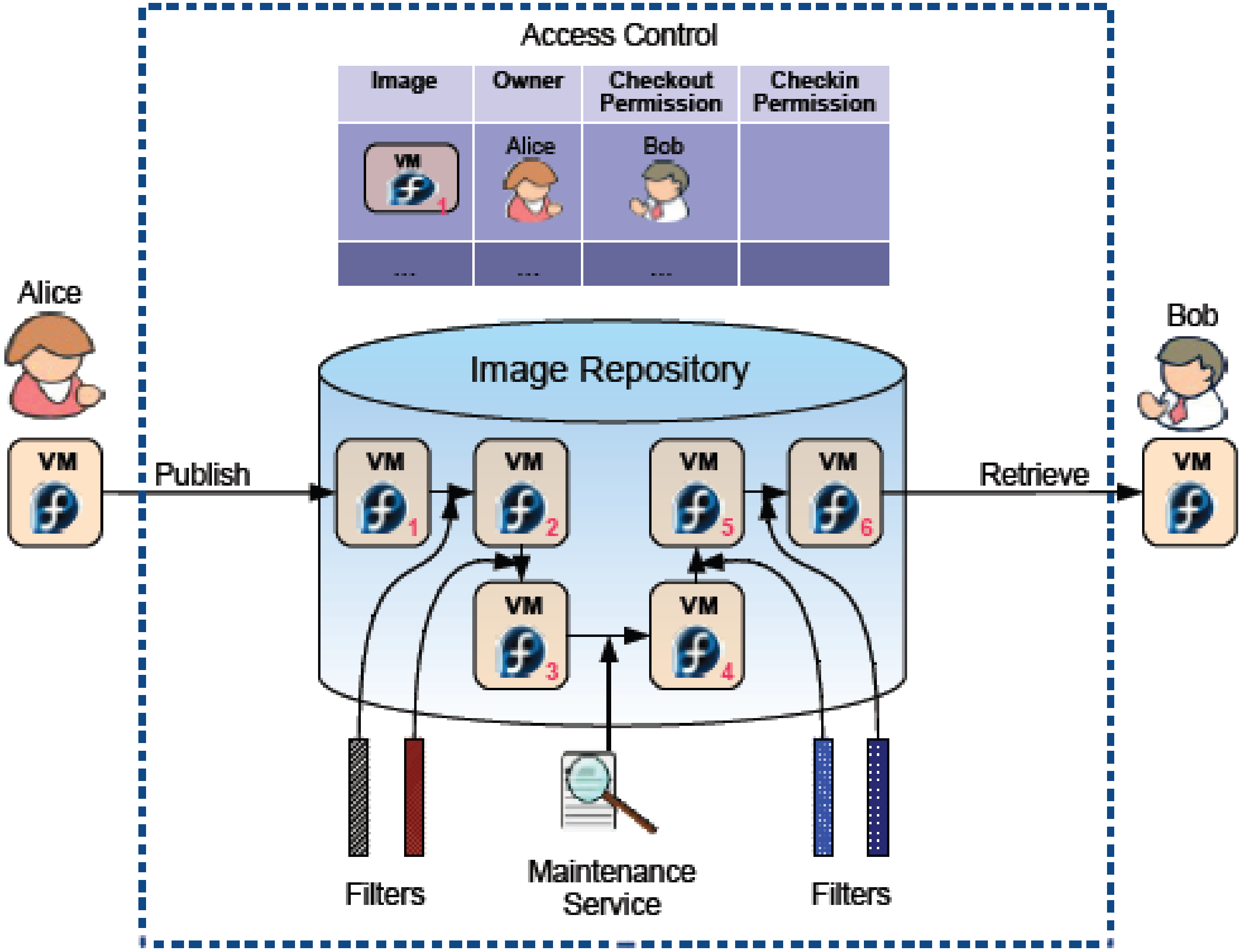
- Existing (ad-hoc) Solutions
  - TLS Federation
  - SAML 2.0 Holder-of-key Assertion Profile
  - Strong Locked Same Origin Policy
  - TLS session binding

- Long-term Solutions
  - Build XML signature and encryption API in Web browser.

Malicious/illegal Image Attacks

- Initial State and Security State
  - Instance → VM image
  - Application → Implementation module
- Security Risks
  - Publisher
    - Sensitive or private information leak
    - Unauthorized retrievers
  - Retriever
    - Malicious or illegal software
  - Repository administrator
    - Dormant images
    - Malicious and illegal software

Image Management System (Mirage)



Access Control

Image	Owner	Checkout Permission	Checkin Permission
VM 1	Alice	Bob	
...	...	...	

Alice

VM

Publish

Image Repository

VM 1

VM 2

VM 3

VM 4

VM 5

VM 6

Retrieve

Bob

VM

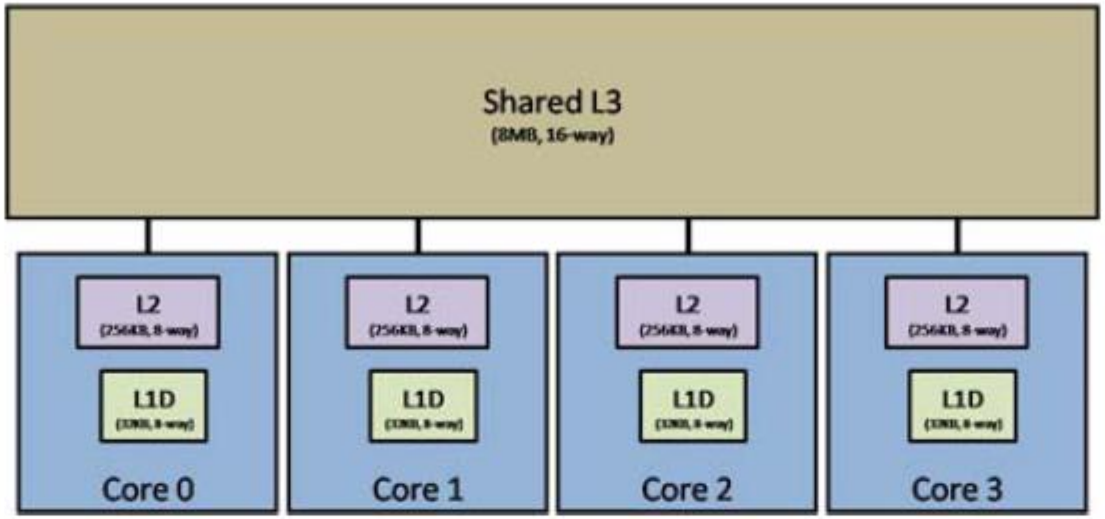
Filters

Maintenance Service

Filters

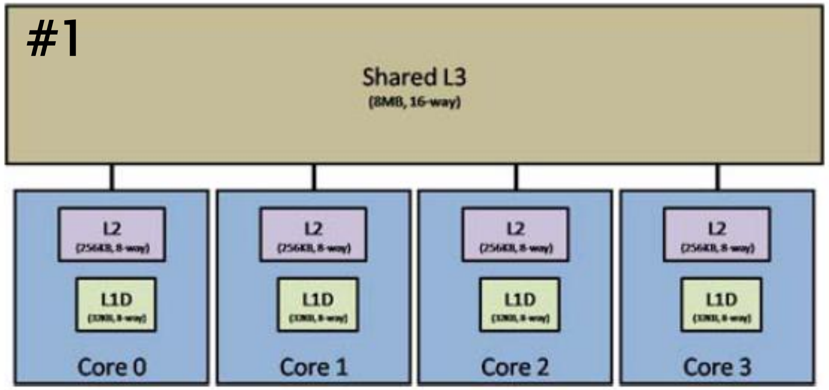
Cache Interference Attacks

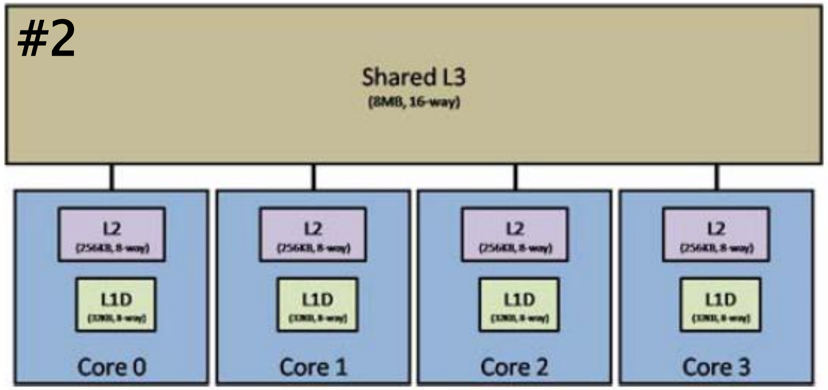
- Shared Resource on multi-core environment
  - Low Level Cache (LLC)
  - Memory bandwidth
- Memory/cache management technique
  - Cache hierarchy aware core assignment
  - Page-coloring based cache partitioning

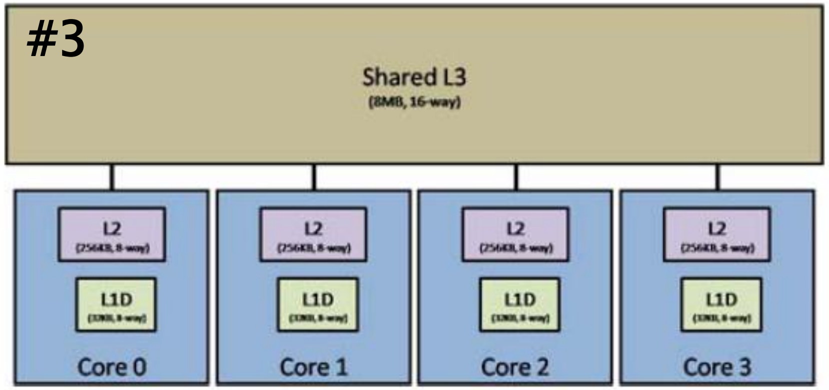


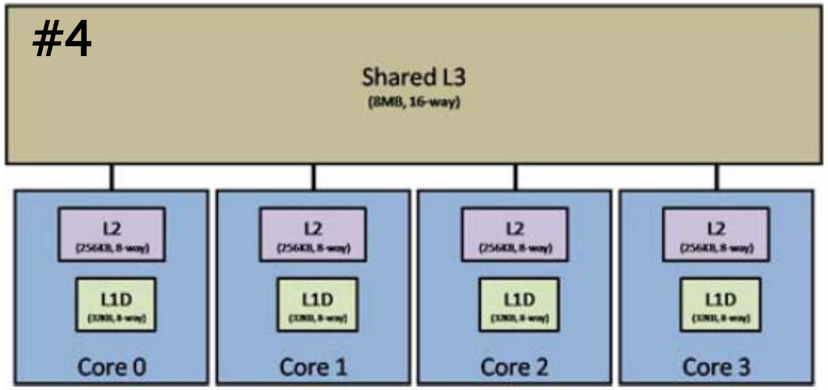
Cache Interference Attacks (cont.)

Cache hierarchy aware core assignment



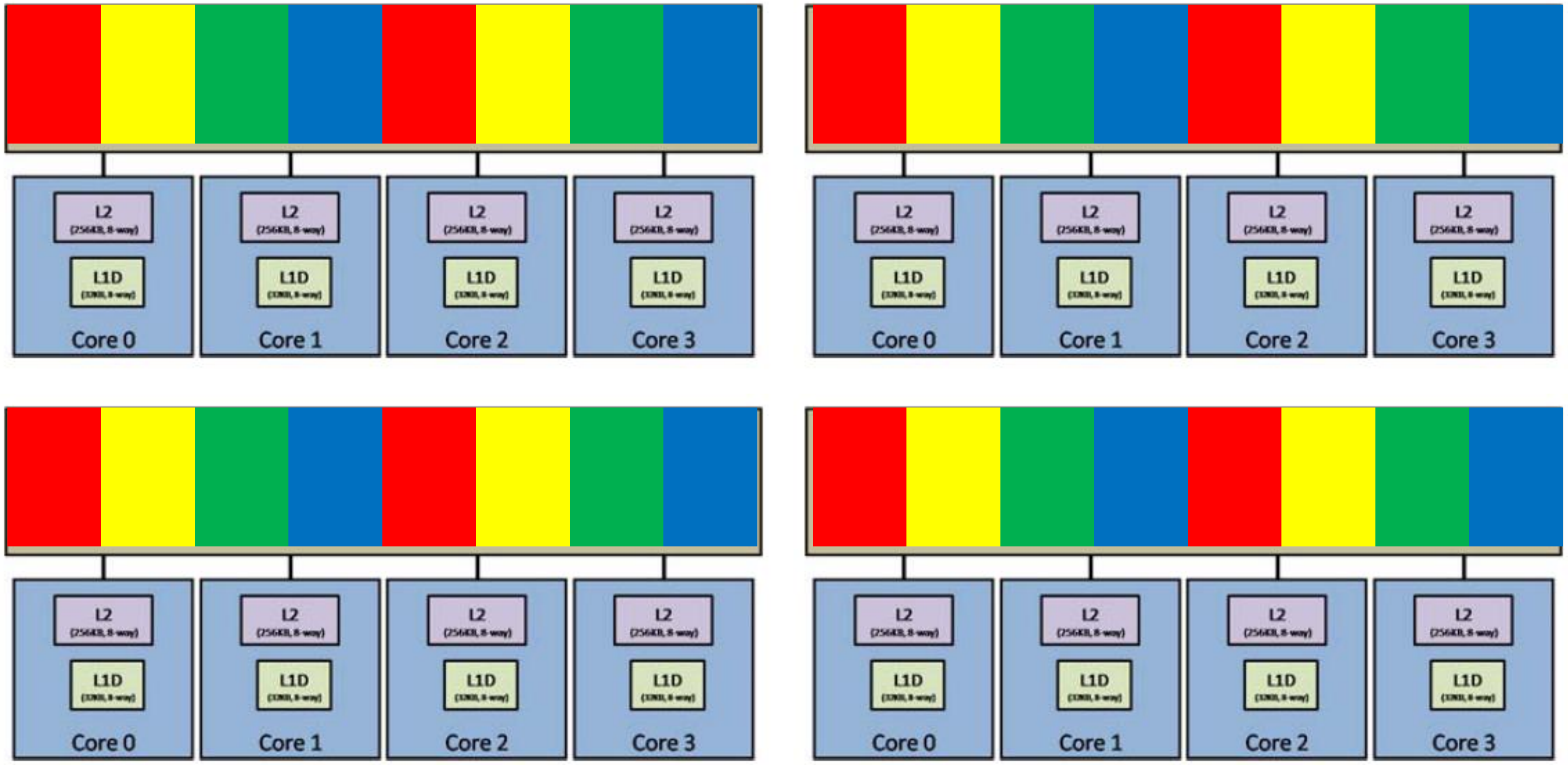






Cache Interference Attacks (cont.)

Page-coloring based cache partitioning



Other Attacks

- Metadata spoofing attacks
  - Attack by modification of Web Service Description Language (WSDL)
  - Address by binding between WSDL and Hash(image)

- flooding attacks
  - Elastic capability cause flooding effect disperse.
  - Downgrade/disable the victim service and service in the same core or the whole cloud.
  - Address by accounting and accountability.

New Direction in Cloud

- Privacy control
  - Data anonymity
  - Private information Retrieval
- Computation-supporting encryption
  - Searchable encryption
  - Homomorphic encryption
- Trust computing
  - High-assurance remote server
- Information-centric
  - Self-describing
  - Self-defending

Questions