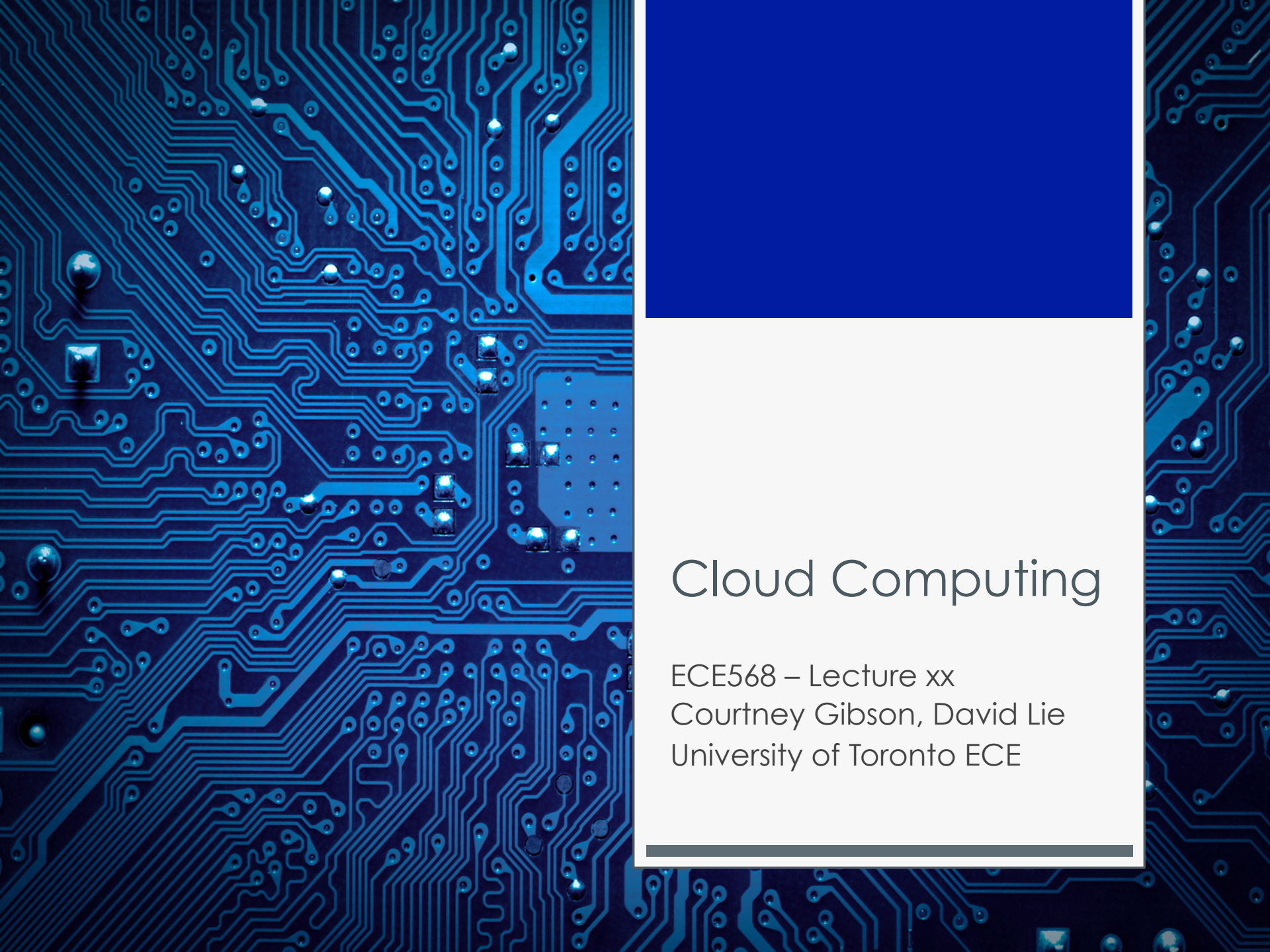


Cloud Computing

ECE568 – Lecture xx

Courtney Gibson, David Lie
University of Toronto ECE

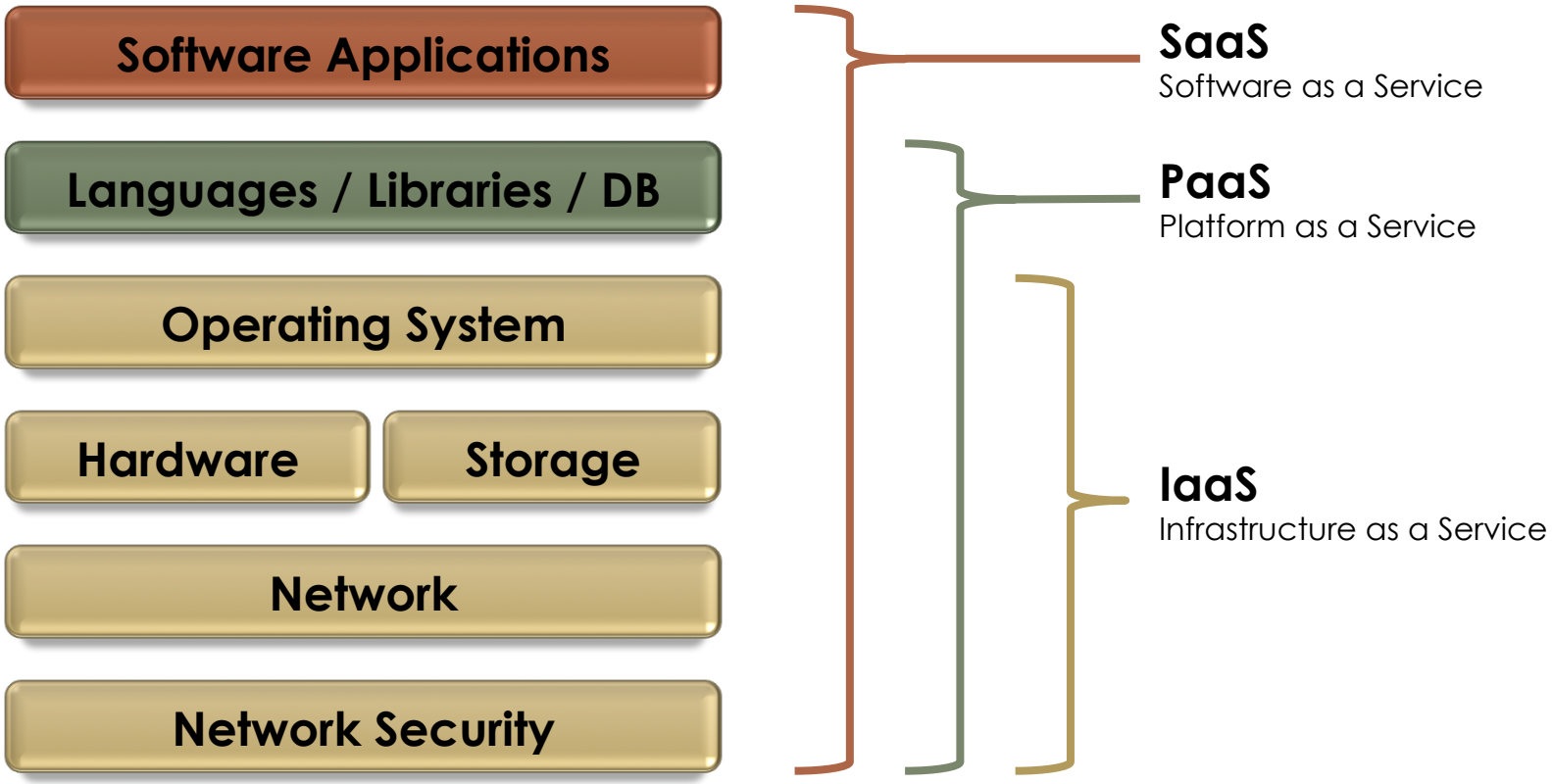
Credit

The State of Public Infrastructure-as-a-Service Cloud Security

W. Huang, A. Ganjali, B. Kim, S. Oh, D. Lie

Overview

Cloud Computing



Cloud Computing

SaaS: Software as a Service

- Salesforce, Marketo, Eloqua, etc.

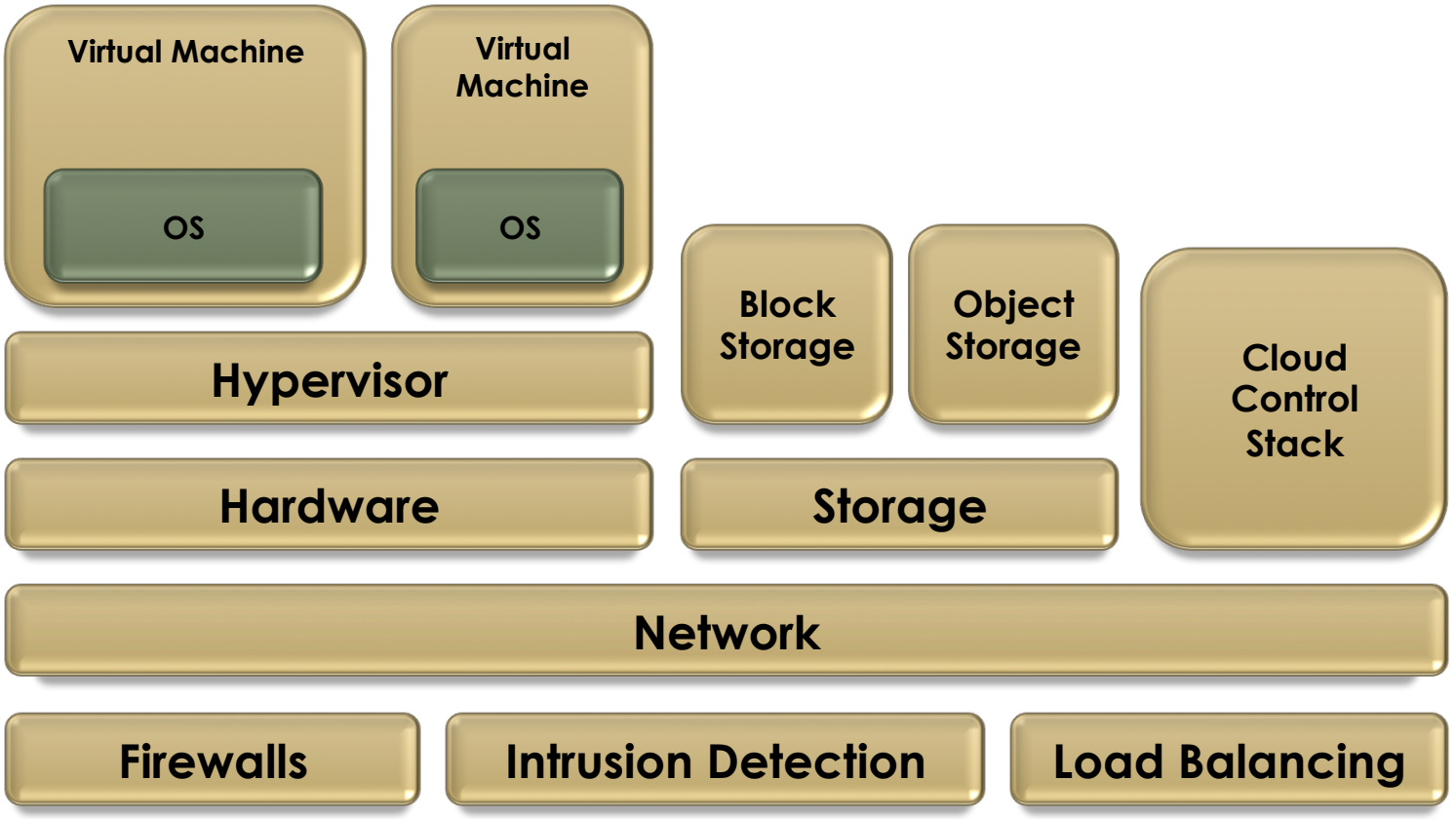
PaaS: Platform as a Service

- AWS, Google App Engine, etc.

IaaS: Infrastructure as a Service

- Amazon EC2, Google Compute Engine, etc.
- Focus of this talk

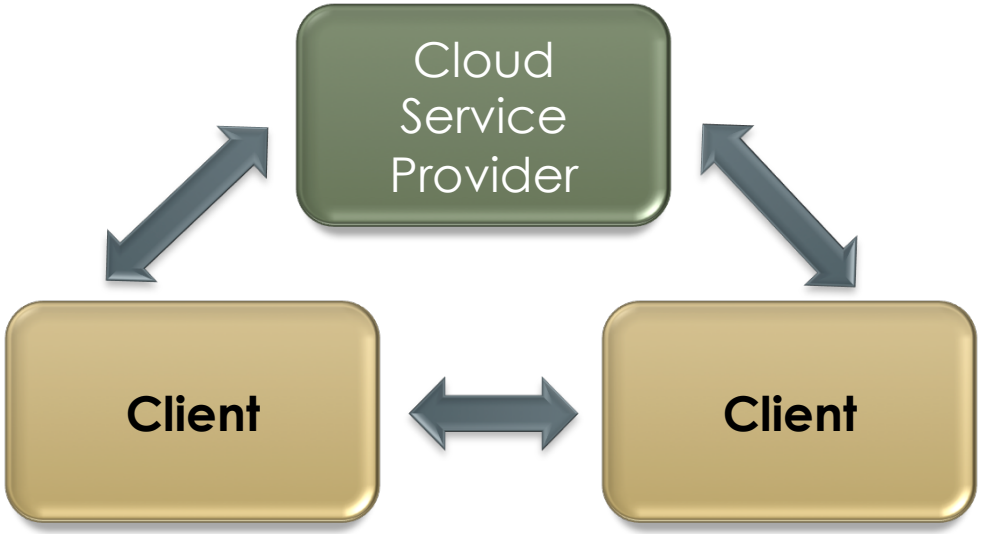
IaaS


Virtual Machine
OS
Virtual Machine
OS
Block Storage
Object Storage
Cloud Control Stack
Hypervisor
Hardware
Storage
Network
Firewalls
Intrusion Detection
Load Balancing

Security Best Practice

- The Cloud Computing ecosystem is still rapidly evolving
  - **2008:** Amazon EC2, Rackspace
  - **2009:** Joyent, GoGrid
  - **2010:** Fujitsu, Microsoft Azure
  - **2011:** Tier 3, Dimension Data
  - **2012:** HP Public Cloud, Savvis Direct
  - **2013:** Google Compute Engine
  - **2014:** Verizon Public Cloud
- Industry is still defining "best practice"
- Much research on overcoming the security challenge of shared infrastructure

Trust in Cloud Environments



- Clients trust CSP to provide confidentiality, integrity, availability
- CSP trusts clients not to behave badly (spam, DoS, etc.)
- CSP needs to ensure malicious clients don't interfere with or exploit one another

Confidentially

Confidentiality concerns can include:

- Customer software and data
- Usage statistics / patterns

Threats

- Observing access patterns of storage and VMs (even if encrypted)
- Side-channel leakage: recovery of data from previously-running VMs

Integrity

Integrity concerns can include:

- Customer software and data

Threats

- Race conditions: exploits of weaknesses in data caching, data consistency
- Manipulation of block/object storage
- Integrity of the VM image

Availability

Availability concerns can include:

- Uptime of hypervisor and virtual machines
- Durability of client data
- Geolocation of data (*e.g.*, legal jurisdictions)

Threats

- Attacks on hypervisor and storage layer

Components and Threats

Hypervisors

- Low-level software component that allows commodity compute hardware to be virtualized and partitioned into VMs, which can then be rented to customers
  - Xen, KVM, VMWare, Hyper-V
- Trusted to isolate VMs from one another, from a security and a performance standpoint

Hypervisors

Problem: How can CSPs and customers detect a compromised hypervisor?

One solution is a **TPM**: *Trusted Platform Module*

- A secure co-processor, on the motherboard of the host running the hypervisor
- TPM signs a hash of the software running at boot (an "attestation"), which it can make available to the client or CSP, to verify the integrity of the code that's running

Firewalls

- Customer-controlled firewalls allow customers to restrict traffic to and from their VMs
- All CSPs have opted to implement firewalls outside of the VMs, so that an attacker who compromises a VM doesn't automatically gain the ability to change its firewall settings
  - Similar protection to that of a physically-separate, non-virtualized firewall in a traditional configuration

Cryptography

Cryptographic mechanisms can be divided into those used to protect customer data while in transit and those used to protect customer data while at rest.

While in transit:

- Customer data and commands are protected by SSL/TLS
- Public-facing CSP servers have certificates signed by well-known CAs

Cryptography at Rest

No agreed-upon best practice as yet:

- **Amazon:** Object storage is encrypted and signed, block storage is plaintext.
- **OpenStack:** Block storage can be encrypted and signed, object storage cannot.
- **Joyent:** No encryption. They argue that encryption managed by CSPs shouldn't be trusted, and that customers should be responsible for their own encryption.

Do you agree or disagree with Joyent's stance?

Networking

- Customer VMs run customer code, but use IP addresses belonging to the CSP. A customer who sends malicious traffic can cause a CSP IP address to be banned or blacklisted.
- Since IPs may be rotated among CSP customers, a customer who causes an IP to be banned could adversely affect the next customer who later uses the same IP.
- **Defenses:** monitoring for spoofed packets, blocking some outbound services (*e.g.*, spam)

Information Leakage

- One of the greatest concerns that customers face when deciding whether or not to move privately owned infrastructure to the public cloud is the loss of the confidentiality of their data and computations.
- Leakage channels include shared caches, storage channels and covert channels.

Cache Timing Exploits

An attacker who is able to run code on the same processor as a victim can use the shared cache as a timing channel to infer information about data being used in computation by the victim

- The attack consists of alternating “prime” and “probe” phases

Cache Timing Exploits

Prime Phase

- The attacker fills the shared cache with her data, thus evicting all the victim's data from the cache.
- She then lets the victim execute their code, which uses the shared cache.
- Loads by the victim will cause the attacker's data to be evicted from the cache.

Cache Timing Exploits

Probe Phase

- Attacker reads her data from the cache and times how long each read takes.
- Some accesses will take longer because they will miss in the cache and go to memory, and so the attacker can infer which cache lines the victim accessed between the prime and the probe phases.
- Experimentally shown that this channel leaks enough info to allow an attacker to recover a victim's AES key. (Bernstein, 2005)

Cache Timing Exploits

Defenses

- Allocate memory such that there is no overlap in cache lines used by different customers. (Raj et al., 2009)
- Allocate memory so that cache lines that contain sensitive information cannot be evicted from the cache and thus do not affect the timing of the attacker's memory accesses. (Kim et al., 2012)

Covert Channels

One scenario for this is an attacker who compromises a VM and tries to covertly exfiltrate information without the victim knowing.

- Experiments have achieved 2-10 bits per second on cache-based covert channels (Xu et al., 2011)
- More advanced methods using the memory bus have achieved 100bps on Amazon EC2 (Wu et al., 2012)

Data Security

Data Security

Goal: prove with high probability that a CSP has maintained the integrity, availability and durability of customer data

Solution: probabilistic algo, where customers make specially-constructed queries on their data

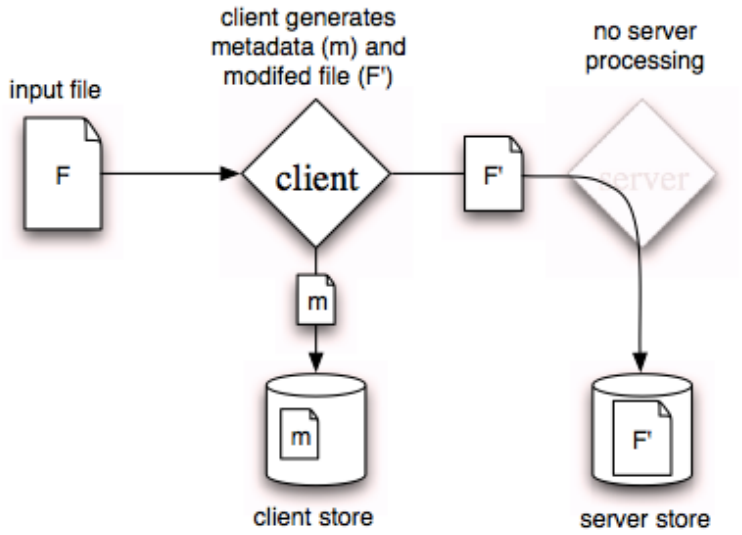
- If the queries are answered correctly by the CSP, it proves with high probability that the integrity, availability and durability of the customer data has been maintained.

Proof of Retrieval (POR)

- The customer encrypts the file and randomly embeds a set of randomly-valued check blocks called *sentinels*
  - The use of encryption renders the sentinels indistinguishable from other file blocks
- The customer later challenges the CSP by asking the for a random collection of the sentinel blocks
  - If the CSP has modified or deleted a substantial portion of the file, then with high probability it will also have suppressed a number of sentinels
- Checksums are used to detect the possibility of small changes having been made

Provable Data Possession (PDP)

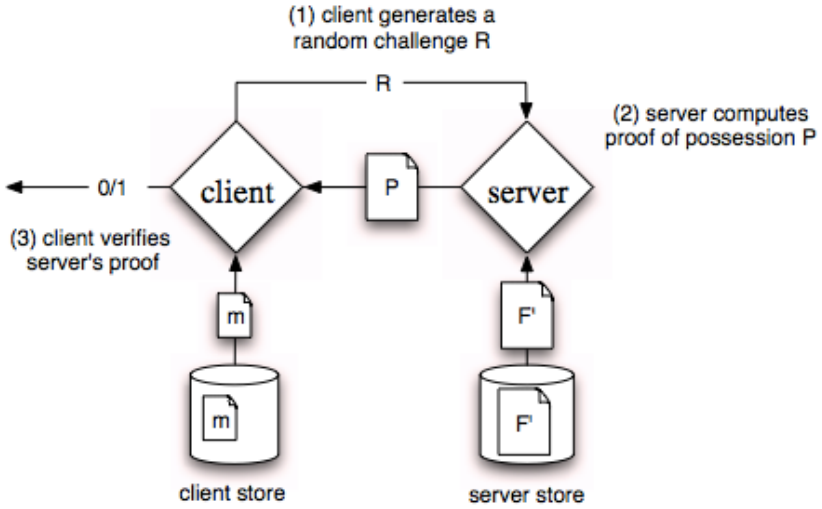
- The client pre-computes tags for each block of a file and then stores the file with a server
- Tags are computed using *homomorphic encryption*: this means that tags computed for multiple, arbitrary file blocks can be combined into a single value



Source: *Provable Data Possession at Untrusted Sources*, Ateniese et al.

Provable Data Possession (PDP)

- At a later time, the client can verify that the server possesses the file by generating a challenge against a randomly selected set of file blocks.
- The server calculates a result for the requested blocks, and sends it back as a proof of possession.
- The client is thus convinced of data possession, without actually having to retrieve the file blocks.



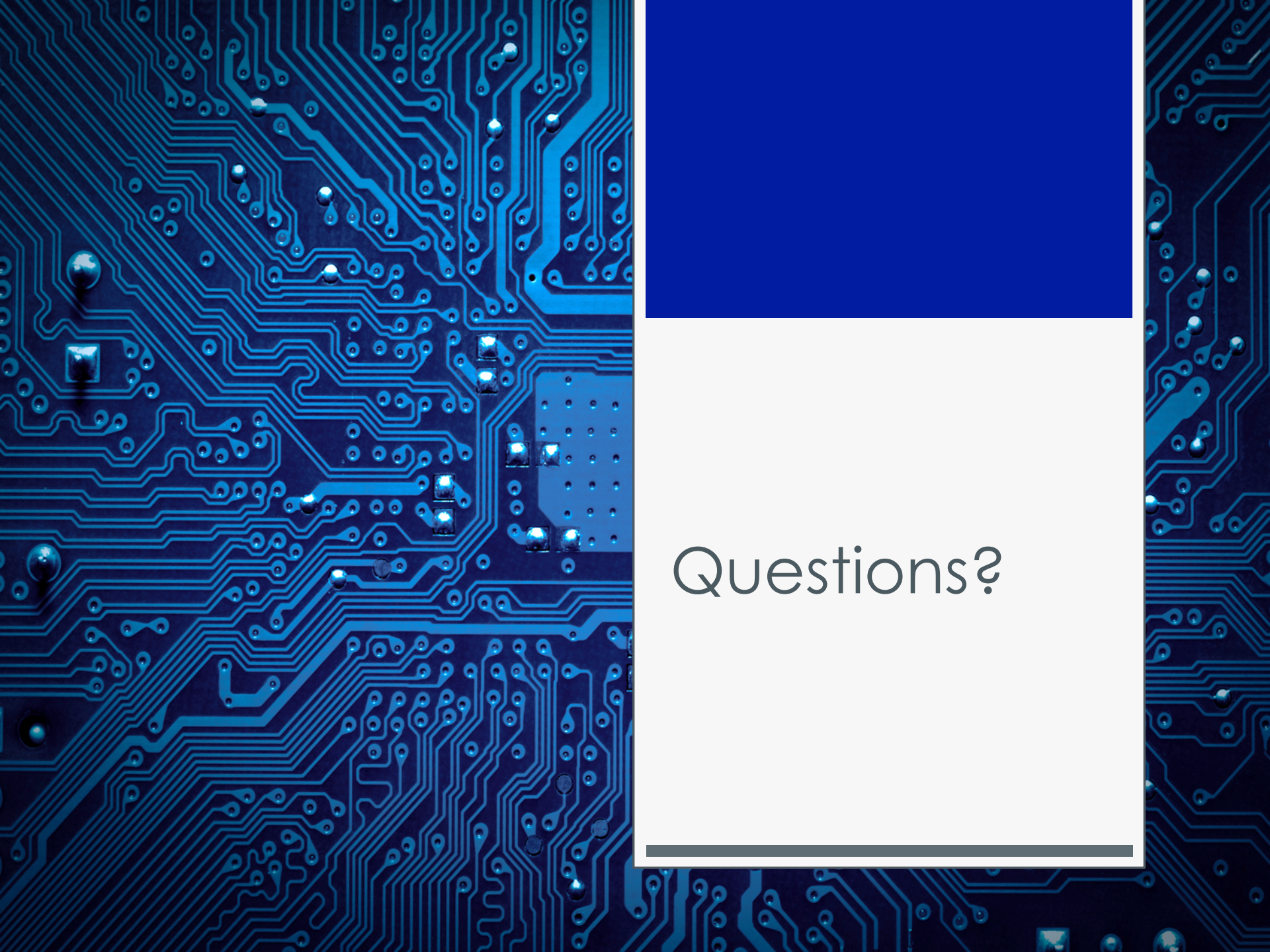
Source: *Provable Data Possession at Untrusted Sources*, Ateniese et al.

Conclusion

Role of Academia

It is not in the commercial interest of CSPs to publicly describe potential weaknesses, attacks or solutions: as a result, information about problems is fragmented.

- An interesting question is how academic research may interact with industrial IaaS cloud deployments going forward
- The primary interaction, thus far, has been in academia identifying threats, and industry reacting to provide solutions
- There has yet been little tangible transfer of the solutions explored by academia to industrial IaaS cloud deployments


Questions?