Cloud Computing (INFS3208)

Lecture 12: Security & Privacy

Guest Lecturer

Cheng Jiang

Lead Platform Engineer at Dabble

Cloud Computing at Scale

OUR PLAN

Part 1 – Cloud Computing at Scale

- Check-in
- Cloud foundations
- Containers & K8s
- IaC
- Live build -> deploy (fun project)
- Interactions & observations
- The future of cloud & you
- Wrap-up

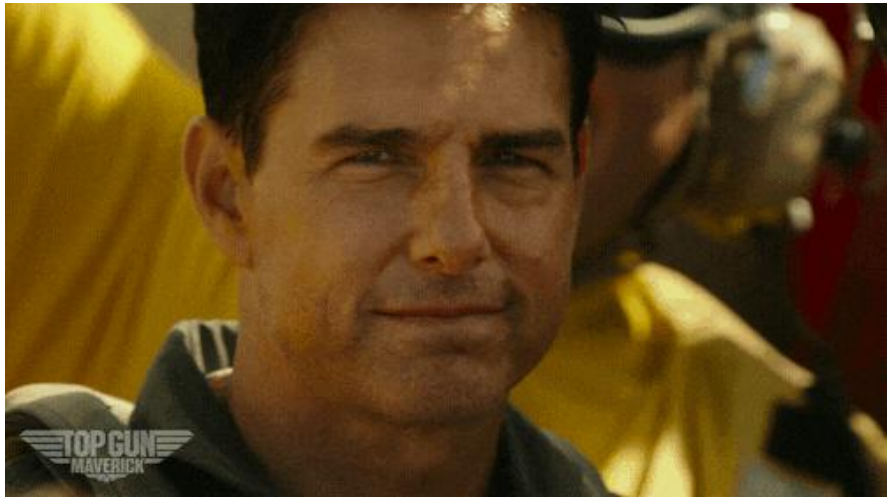
Part 2

- Security in cloud environments
- Privacy in cloud computing

CHECK IN

SHOUT OUT TO YOURSELF

What’s something you’re proud of. It doesn’t have to be course related.



SHOUT OUT TO SOMEONE ELSE

Anyone who has made your life fantastically and unbelievably better.

The Big Picture

Every tap you make travels through the cloud.

Cloud foundations

- What is “the cloud,” really?
- Why cloud?
- How it makes Netflix, Spotify, and gaming work at global scale
- How apps scale globally through regions and availability zones
- Why companies rely on it for speed and reliability

Containers & Kubernetes

- The secret behind how modern apps scale up instantly
- Containers: lightweight, portable mini-servers
- Kubernetes: the system that runs, scales, and heals thousands of containers automatically
- Why it matters?

IaC: Infrastructure as code

- Building cloud infrastructure…using code, not clicks
- Tools like Pulumi and Terraform keep cloud setups repeatable
- How IaC helps teams manage huge systems safely and more efficiently?
- Other benefits?

Let’s have fun

How powerful is AI + IaC?

Live build -> deploy (mini project)

- Together we'll deploy a mini web app to a local k8s cluster
- You'll be able to visit it from your own device
- Watch how real-world cloud infrastructure behaves in action

Interactions & Observations

- Post your shout-outs to the live app
- See how Kubernetes balances traffic and scales
- Observe how infrastructure “self-heals” when we break things 😈

What it means for your career?

Where cloud is headed - and how you can be part of it

What cloud computing means for your career

- Every industry now relies on cloud platforms — finance, healthcare, gaming, and AI all run on them
- Developers who understand both coding and infrastructure stand out in the job market
- Cloud knowledge bridges development and operations — enabling faster, safer releases
- Skills like Docker, Kubernetes, and Infrastructure as Code are becoming baseline expectations
- Building small cloud projects is the fastest way to learn and showcase real-world experience

The future of cloud & you

- AI and cloud computing are merging — training, inference, and data pipelines increasingly run on cloud systems
- Developer tools are simplifying cloud operations, making it easier to deploy and manage apps
- Global-scale systems are becoming common — multi-region, low-latency, always-on applications
- Security, efficiency, and sustainability will shape the next decade of cloud innovation
- Staying curious, experimenting, and understanding automation will keep your skills future-proof

Wrap-up: Key Takeaways

- **Cloud** is built on automation, scalability, and reliability — systems that adapt and recover on their own
- **Containers** make apps portable and consistent across different environments
- **Kubernetes** orchestrates and self-heals workloads at scale
- **Infrastructure as Code (IaC)** turns infrastructure into programmable, version-controlled code
- **Reflection:** Which part of cloud computing excites you most — building, deploying, or automating?
- **Looking ahead:** Cloud skills are shaping nearly every tech career path — the more you understand how it works, the more valuable you'll be
- **Next step:** Try hands-on tools like Docker Desktop, Orbstack, K3s, Minikube, etc

- Security in Cloud Computing
- Privacy in Cloud Computing

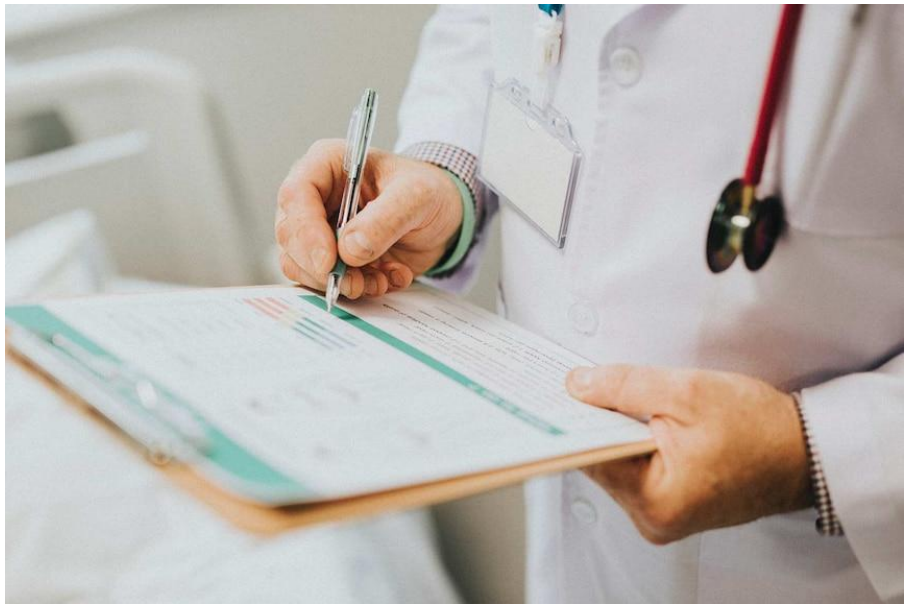
Security and Privacy Outline

- Security in Cloud Computing
  - Basic Terms and Concepts
  - Threats in Cloud Computing
  - Security Mechanisms:
    - Encryption: symmetric & asymmetric
    - Hashing
    - Digital Signature
    - PKI and CA
- Privacy in Cloud Computing
  - What is Privacy
  - Privacy Laws in Australia
  - Privacy Questions for Cloud Providers

Security News

Take a single year of 2020 as an example...

In July 2020, confidential information about WA patients from the state's Department of Health, including those with suspected COVID-19 infection, was published online. The data breach was associated with the use of a third-party pager system on which the messages exchanged were non-encrypted.



https://www.abc.net.au/news/2020-07-20/wa-health-department-investigates-confidential-data-breach/12475310

Security News

In August 2020, tens of thousands of NSW driver's licences were exposed online. The storage folder, which contained back-and-front scans of NSW licences, was mistakenly left exposed in an open cloud storage.

Tolling Notice Statutory Declaration – Companies

Use this form to give notice of the name and address of the driver who was in charge of the vehicle at the time of the trip.

- Print clearly in CAPITAL letters using black pen.
- The original Toll Notice or a copy **must** be enclosed.
- Completed form **must** be received at least 7 days before the due date on the toll notice. You must provide the name and address of the company you wish to nominate.

Toll Notice number: 1 6 7 9 [redacted] Vehicle registration number: [redacted]

I, *[full name of person completing this form on behalf of the Company/organisation named on the toll notice]*

PETER

am an authorised officer of

Company name: [redacted] PTY LTD

Company address: [redacted] ARTARMON NSW 2064

https://www.abc.net.au/news/2020-09-01/nsw-drivers-licence-data-breach-under-investigation/12611918

Security News

In September 2020, data breach at University of Tasmania affects 20,000 students. Due to the incorrect configuration of security setting, electronic files that contained students' personal information were inadvertently able to be accessed by all users with a utas.edu.au email address.

https://www.abc.net.au/news/2020-09-21/data-breach-at-university-of-tasmania/12685318

Outline

- Security in Cloud Computing
  - Basic Terms and Concepts
  - Threats in Cloud Computing
  - Security Mechanisms:
    - Encryption: symmetric & asymmetric
    - Hashing
    - Digital Signature
    - PKI and CA
- Privacy in Cloud Computing
  - What is Privacy
  - Privacy Laws in Australia
  - Privacy Questions for Cloud Providers

Security Goals

Security is a **generic** term, be **specific**

- specify what is the **goal**

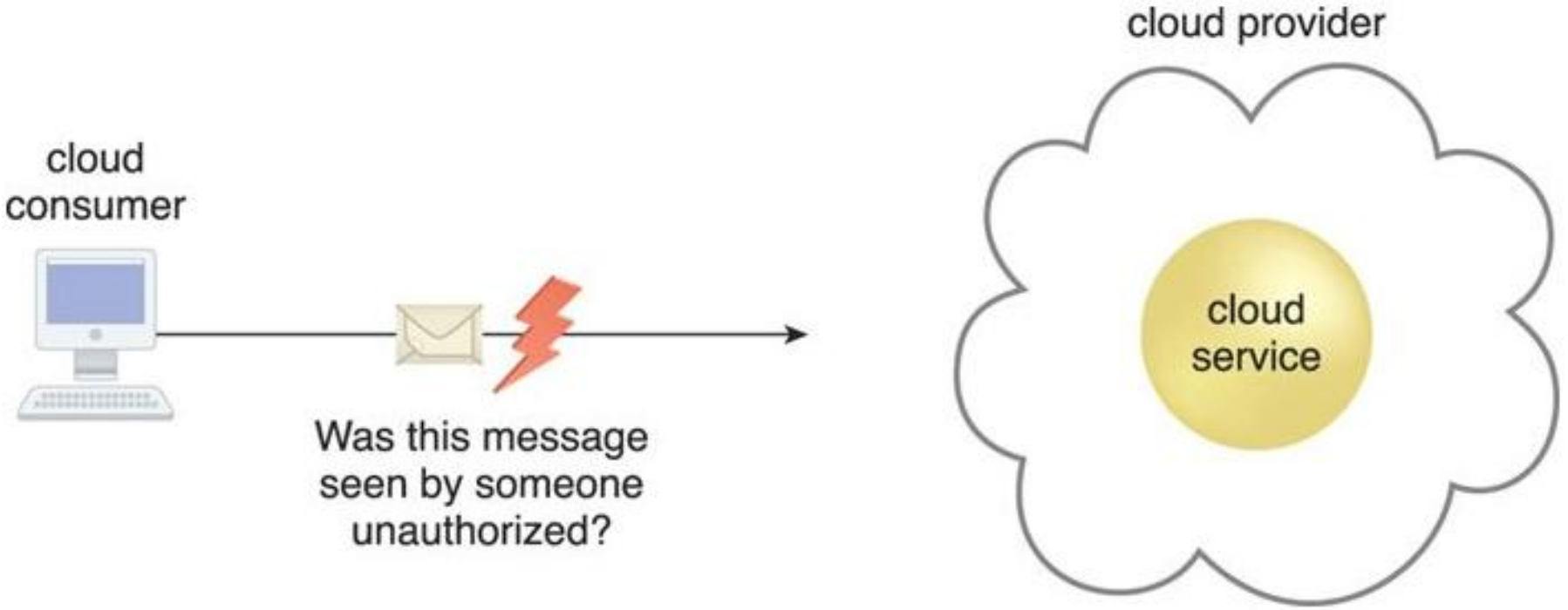
Security **Goals** *examples (Recap)*

- Secrecy / Confidentiality (CONF)
- Integrity (INT)
- Authentication (AUTH)
- Non-Repudiation (NR)
- Availability (AVL)

Terms and Concepts

Confidentiality

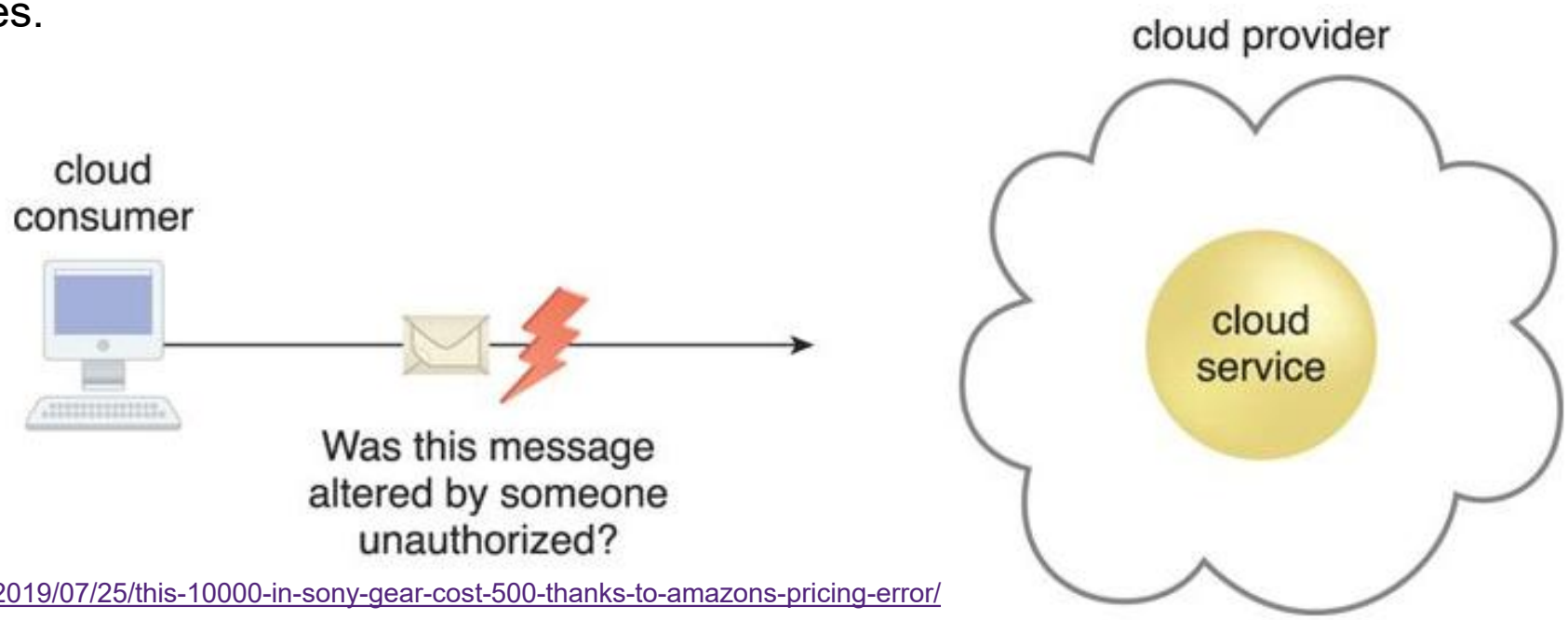
- Confidentiality is the characteristic of something being made accessible only to authorized parties
- Within cloud environments, confidentiality primarily pertains to restricting access to data in transit and storage.



Terms and Concepts

Integrity

- Integrity is the characteristic of not having been altered by an unauthorized party.
- An important issue that concerns data integrity in the cloud is whether a cloud consumer can be guaranteed that the data it transmits to a cloud service matches the data received by that cloud service.
- Integrity can extend to how data is stored, processed, and retrieved by cloud services and cloud-based IT resources.



https://petapixel.com/2019/07/25/this-10000-in-sony-gear-cost-500-thanks-to-amazons-pricing-error/

Terms and Concepts

Authenticity

- Authenticity is the characteristic of something having been provided by an authorized source.

Availability

- Availability is the characteristic of being accessible and usable during a specified time period.
- In typical cloud environments, the availability of cloud services can be a shared responsibility
  - VMs by cloud provider;
  - Applications by cloud consumer.

Threat

- A threat is a potential security violation that can challenge defenses to cause harm.
- Both manual and automatic threats are designed to exploit known weaknesses (aka vulnerabilities).
- A threat results in an *attack*.

Security Goals examples

Security **Goals** *examples (Recap)*

- Secrecy / Confidentiality (**CONF**)
  - achieved by *encryption*
- Integrity (**INT**)
  - achieved by *Message Authentication Code* (MAC)
  - achieved indirectly by *digital signature*
- Authentication (**AUTH**)
  - achieved by *digital signature, biometrics, password*
- Non-Repudiation (**NR**)
  - achieved by *digital signature, biometrics*, …

Terms and Concepts

Vulnerability

- A vulnerability is a weakness that can be attacked.
- IT resource vulnerabilities can many reasons:
  - configuration deficiencies, security policy weaknesses,
  - user errors, hardware or firmware flaws,
  - software bugs, and poor security architecture.

Risk

- Risk is the possibility of loss when performing an activity.
- Risk is typically measured according to the threat level.
- Two metrics to determine risk for an IT resource:
  - the probability of a threat occurring to exploit vulnerabilities in the IT resource
  - the expectation of loss upon the IT resource being compromised

https://www.makeuseof.com/tag/meltdown-spectre-cpu-vulnerable-attack/
https://www.youtube.com/watch?v=bs0xswK0eZk
https://aws.amazon.com/security/security-bulletins/

Fundamental Cloud Security

Security Mechanisms

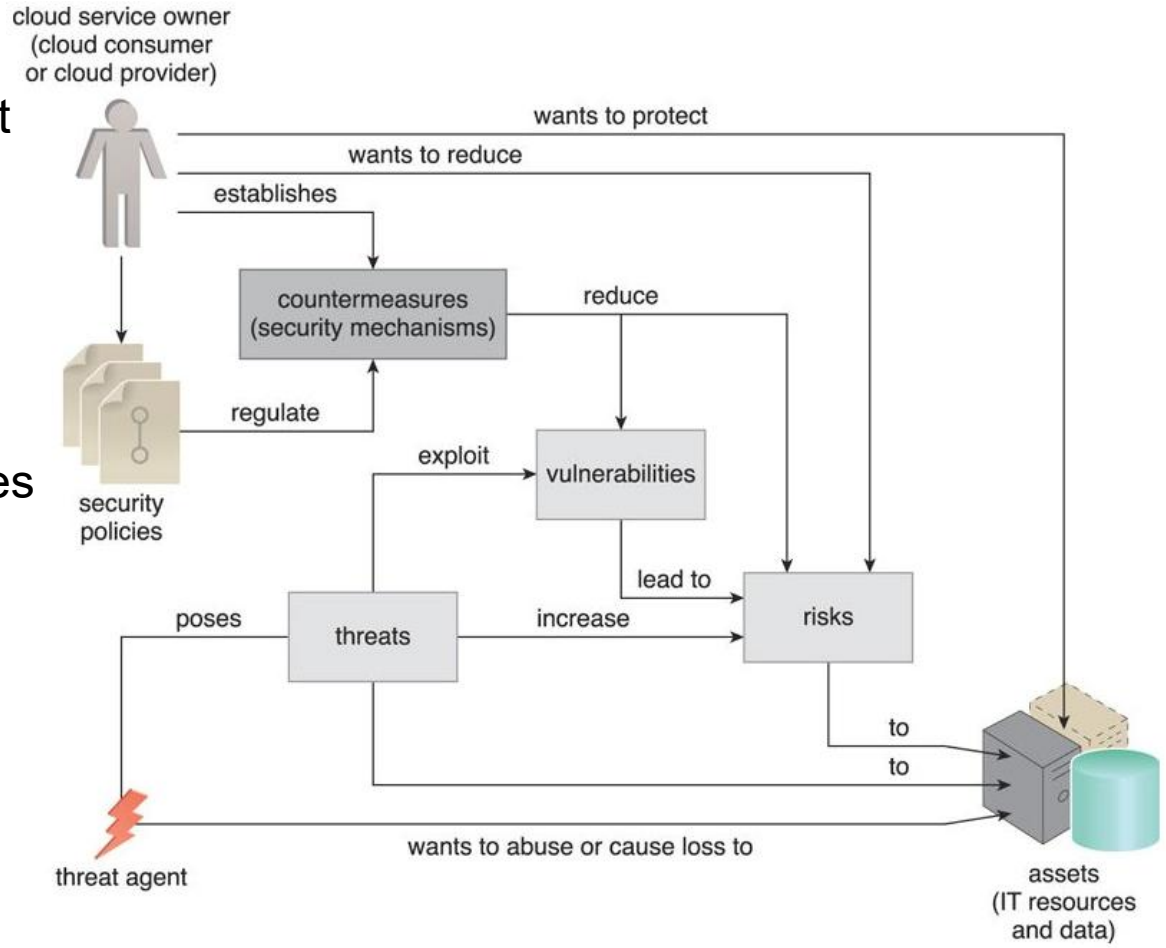
- Are components comprising a defensive framework that protects IT resources, information, and services.

Security Policies

- A security policy establishes a set of security rules and regulations.
- Often, security policies will further define how these rules and regulations are implemented and enforced.

Threat agent

- is an entity that poses a threat because it is capable of carrying out an attack.
- Cloud security threats can originate either internally or externally, from humans or software programs.



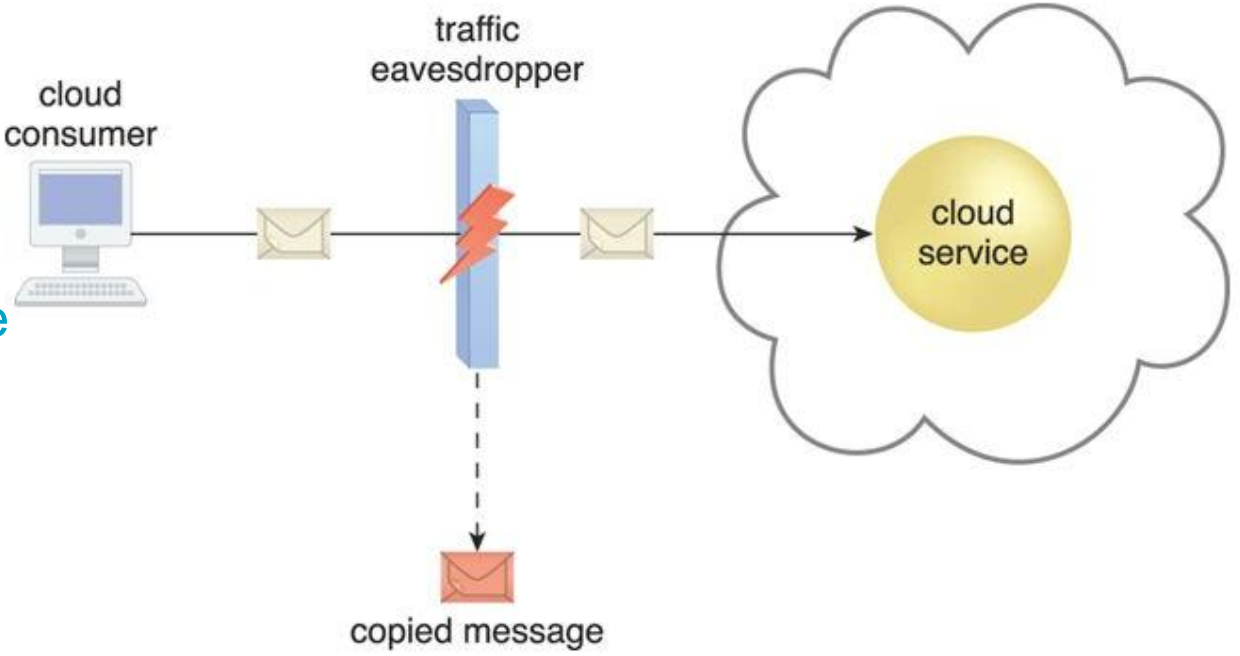
Outline

- Security in Cloud Computing
  - Basic Terms and Concepts
  - Threats in Cloud Computing
  - Security Mechanisms:
    - Encryption: symmetric & asymmetric
    - Hashing
    - Digital Signature
    - PKI and CA
- Privacy in Cloud Computing
  - What is Privacy
  - Privacy Laws in Australia
  - Privacy Questions for Cloud Providers

Cloud Security Threats

Traffic Eavesdropping

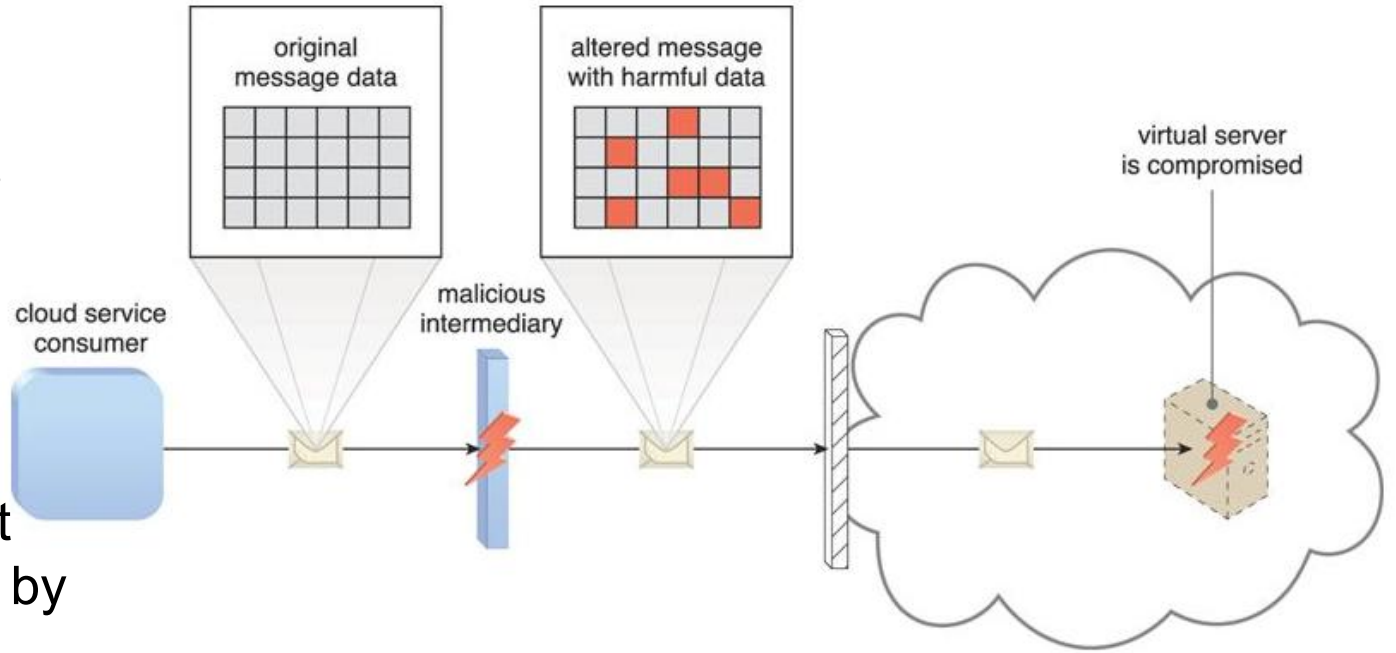
- occurs when data being transferred to or within a cloud
- is passively intercepted by a malicious service agent for illegitimate information gathering purposes.
- The aim of this attack is to directly compromise the confidentiality of the data.
- Because of the passive nature of the attack, it can more easily go undetected for extended periods of time.



Cloud Security Threats

Malicious Intermediary

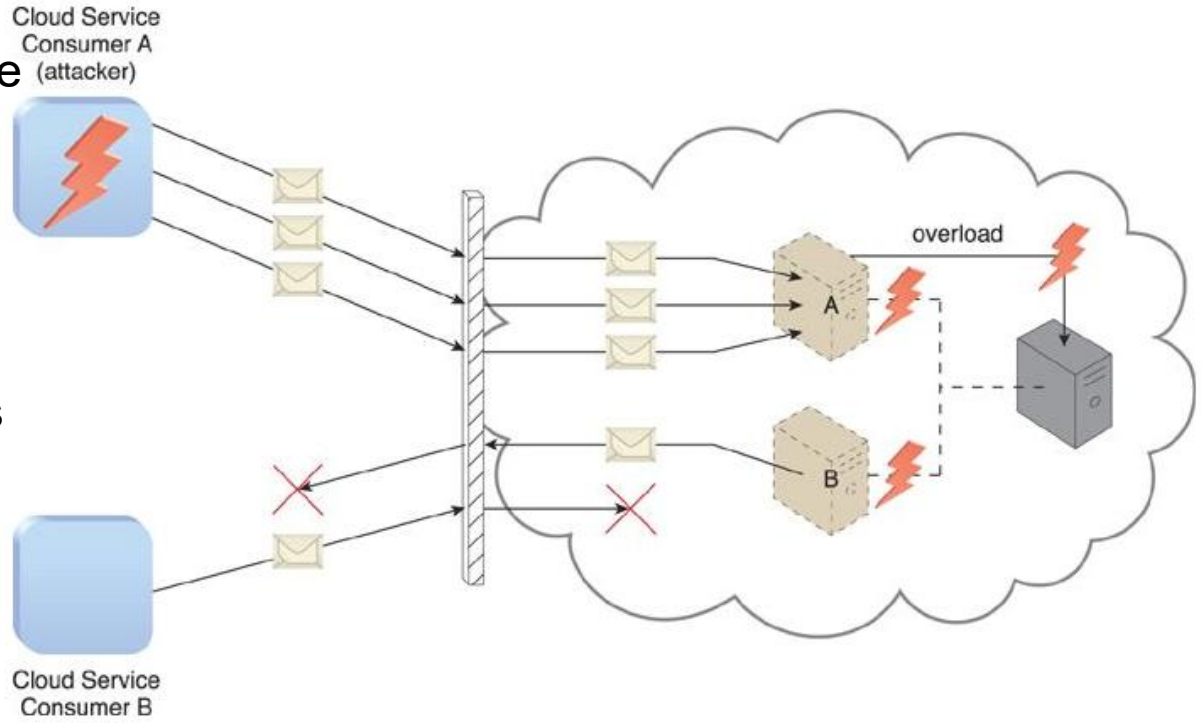
- The malicious intermediary threat arises when messages are intercepted and altered by a malicious service agent;
- potentially compromising the message's confidentiality and/or integrity.
- It may also insert harmful data into the message before forwarding it to its destination.
- In the figure, the malicious service agent intercepts and modifies a message sent by a cloud service consumer to a cloud service being hosted on a virtual server.



Cloud Security Threats

Denial of Service (DoS)

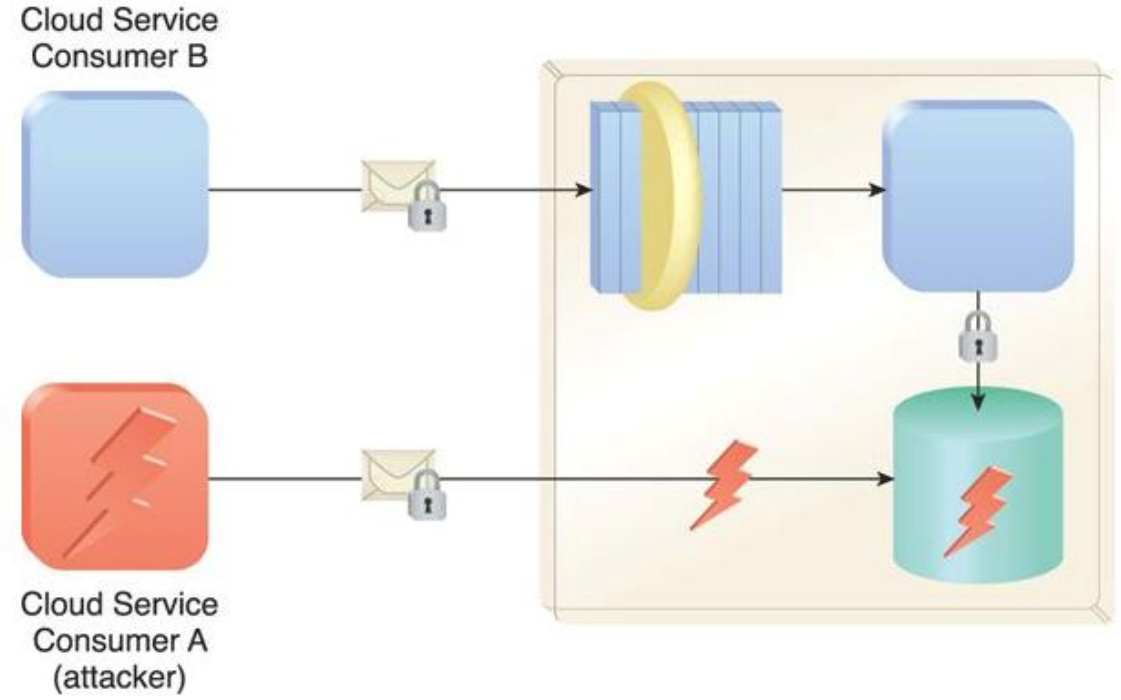
- DoS attack aims to overload IT resources to the point where they cannot function properly.
- This form of attack is commonly launched in one of the following ways:
  - The workload on cloud services is artificially increased with imitation messages or repeated communication requests.
  - The network is overloaded with traffic to reduce its responsiveness and cripple its performance.
  - Multiple cloud service requests are sent, each of which is designed to consume excessive memory and processing resources.



Cloud Security Threats

Insufficient Authorization

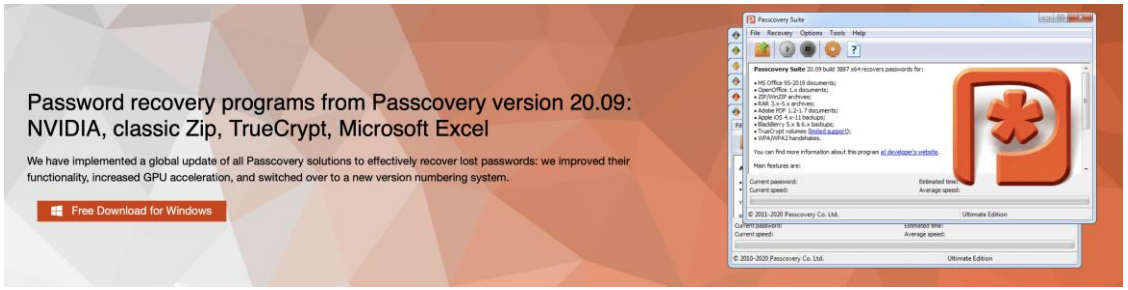
- The insufficient authorization attack occurs when access is granted to an attacker erroneously or too broadly, resulting in the attacker getting access to IT resources that are normally protected.
- This is often a result of the attacker gaining direct access to IT resources that were implemented under the assumption that they would only be accessed by trusted consumer programs.

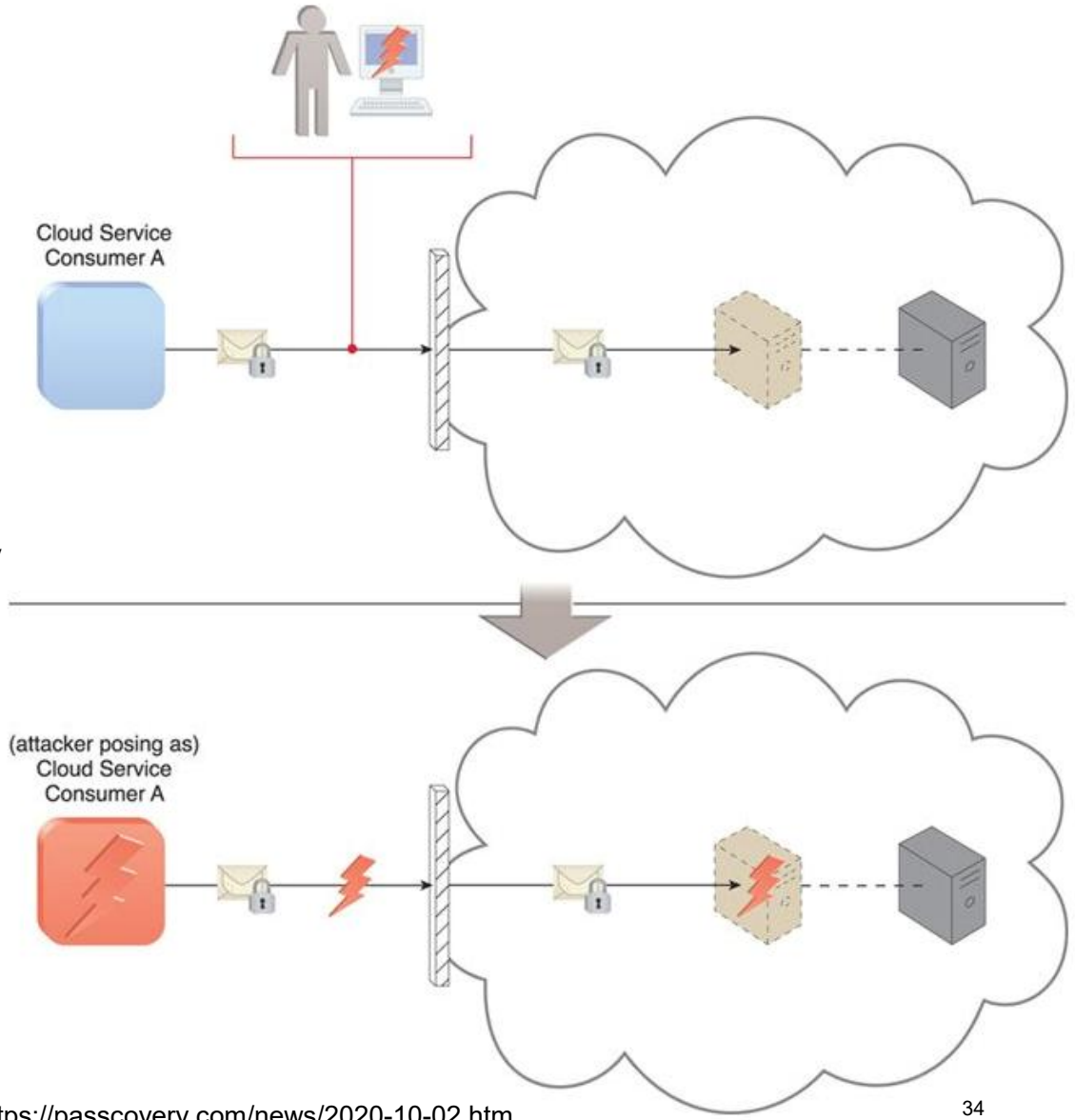


Cloud Security Threats

A variation of this attack, known as weak authentication:

- can result when weak passwords or shared accounts are used to protect IT resources.
- significant impacts depending on the range of IT resources and the range of access to those IT resources the attacker gains.
- E.g. An attacker has cracked a weak password used by Cloud Service Consumer A. As a result, a malicious cloud service consumer (owned by the attacker) is designed to pose as Cloud Service Consumer A in order to gain access to the cloud-based virtual server.





https://passcovery.com/news/2020-10-02.htm

Outline

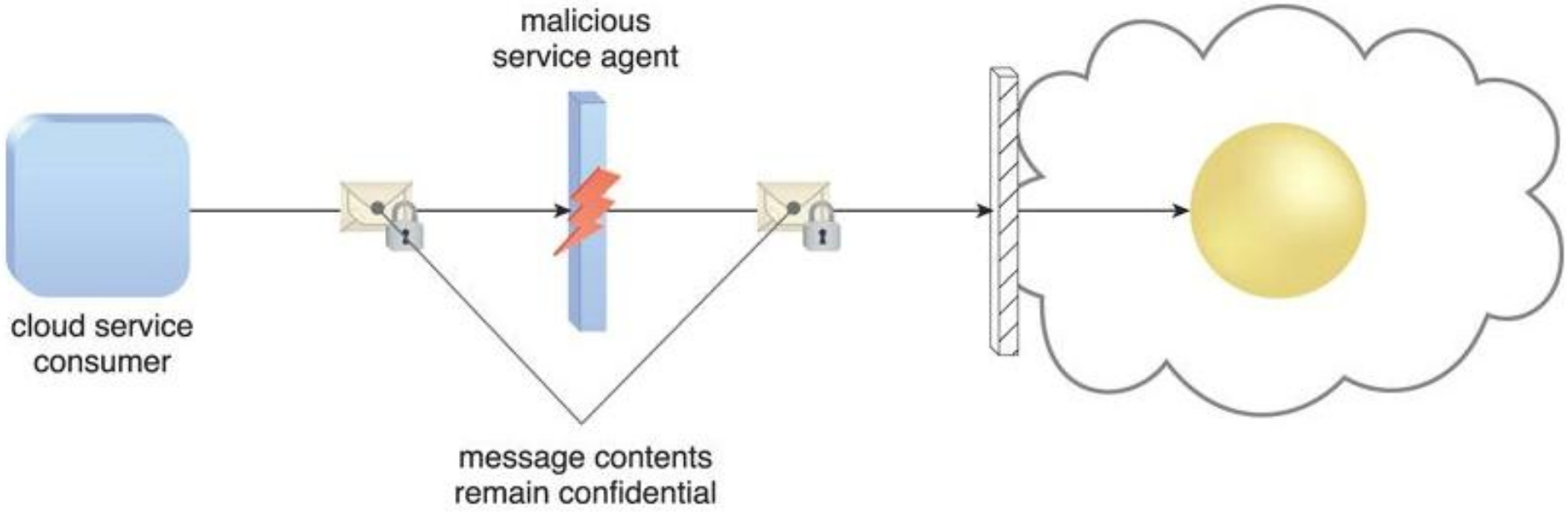
- Security in Cloud Computing
  - Basic Terms and Concepts
  - Threats in Cloud Computing
  - Security Mechanisms:
    - Encryption: symmetric & asymmetric
    - Hashing
    - Digital Signature
    - PKI and CA
- Privacy in Cloud Computing
  - What is Privacy
  - Privacy Laws in Australia
  - Privacy Questions for Cloud Providers

Cloud Security Mechanisms

- Data, by default, is coded in a readable format known as *plaintext*.
- When transmitted over a network, plaintext is vulnerable to unauthorized and potentially malicious access.
- The *encryption* mechanism is a system dedicated to preserving the confidentiality and integrity of data.
  - It is used for encoding plaintext data into a protected and unreadable format.
  - Relies on a standardized algorithm called *a cipher* to transform original **plaintext data** into **encrypted data** (referred to as *ciphertext)*.
  - Access to ciphertext does not expose the original plaintext data.
  - The encrypted data is paired with a string of characters called an *encryption key*.
  - The encryption key is used to decrypt the ciphertext back into its original plaintext format.

Cloud Security Mechanisms

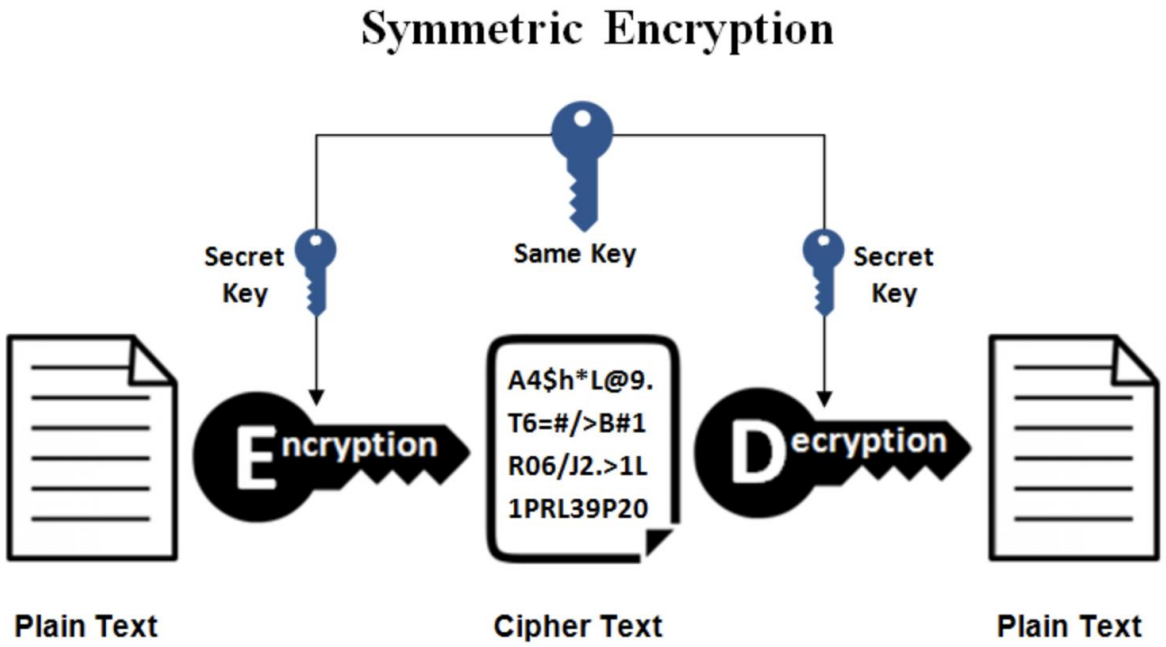
- The encryption mechanism can help counter the security threats:
  - traffic eavesdropping,
  - malicious intermediary,
  - insufficient authorization
- E.g. malicious service agents that attempt traffic eavesdropping are unable to decrypt messages in transit if they do not have the encryption key



Cloud Security Mechanisms – Encryption

There are two common forms of encryption known as *symmetric encryption* and *asymmetric encryption*.

- **Symmetric Encryption**
  - Symmetric encryption uses the same key for both encryption and decryption, both of which are performed by authorized parties that use the one shared key.
  - Parties that rightfully decrypt the data are provided with evidence that the original encryption was performed by parties that rightfully possess the key.
  - A basic authentication check is always performed.
  - Typical algorithms: DES, AES, RC4/RC5, etc.

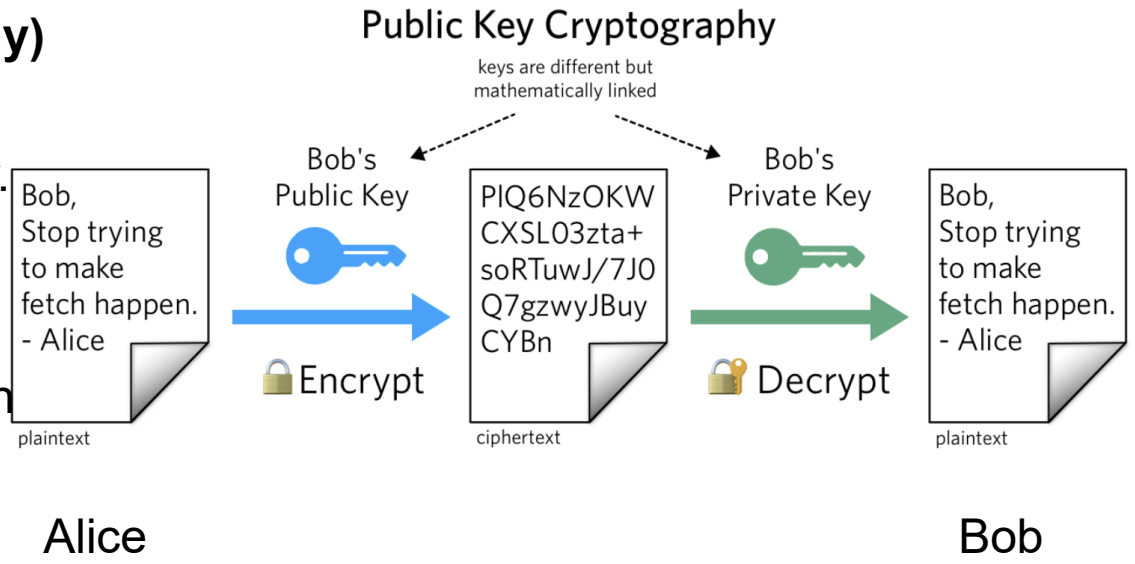


https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

Cloud Security Mechanisms – Encryption

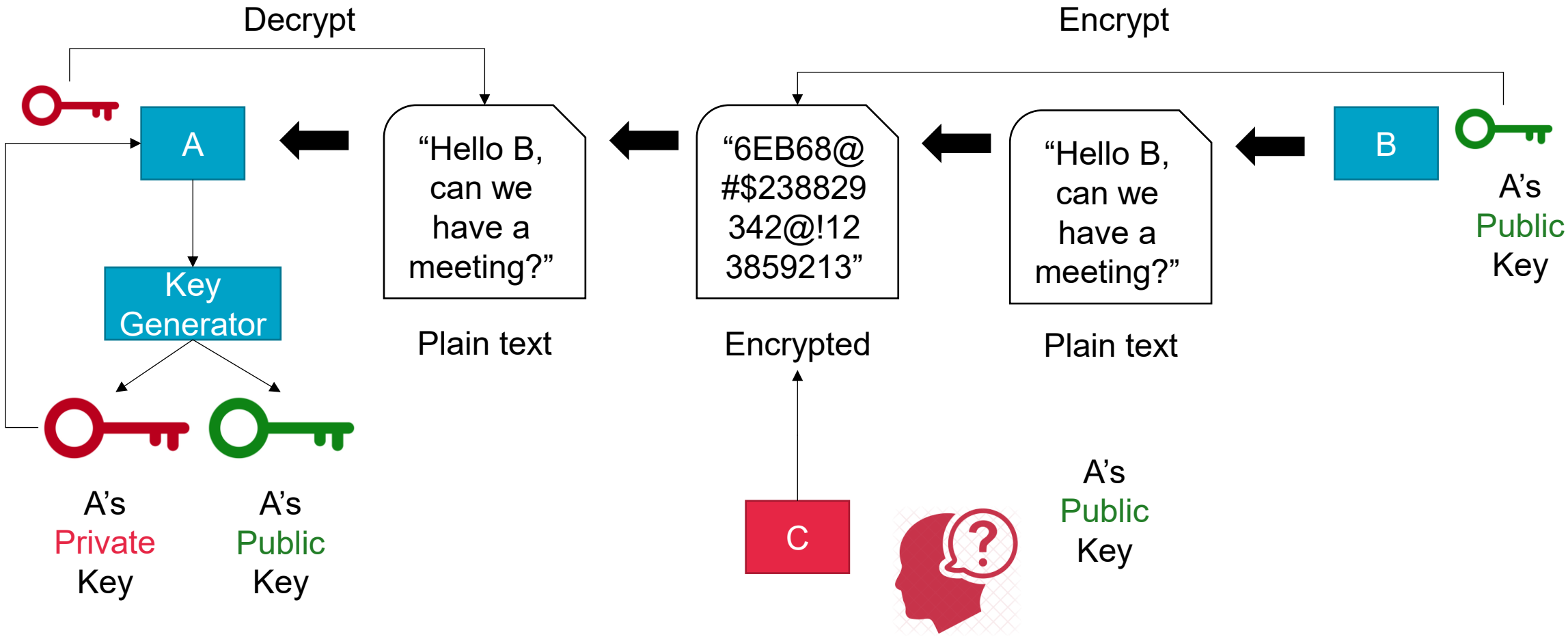
There are two common forms of encryption known as *symmetric encryption* and *asymmetric encryption*.

- **Asymmetric Encryption (aka public key cryptography)**
  - Asymmetric encryption relies on the use of two different keys, namely a private key and a public key.
  - The private key is known only to its owner
  - the public key is commonly available.
  - A document that was encrypted with a public key can only be correctly decrypted with the corresponding private key.
  - asymmetric encryption is almost always computationally slower than symmetric encryption.
  - Typical algorithms: RSA and etc.



Cloud Security Mechanisms – Encryption

- **Asymmetric Encryption (aka public key cryptography)**



Symmetric vs. Asymmetric

Symmetric	*Asymmetric*
Shared secret	PK/SK pair
80 bit key for high security (2010)	2048 bit key for high security (2010)
~1,000,000 ops/s on 1GHz proc	~100 signs/s & ~1,000 verifies/s on 1GHz proc
10x speedup in HW (AES-NI)	Limited speedup in HW

Combining Symmetric and Asymmetric Crypto

Example: TLS/SSL

Uses certificate authority to provide public key

Uses asymmetric crypto to establish symmetric key

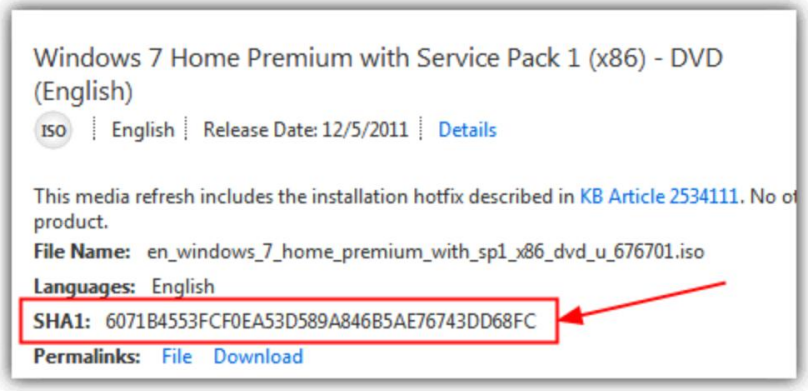
Uses symmetric crypto for data encryption

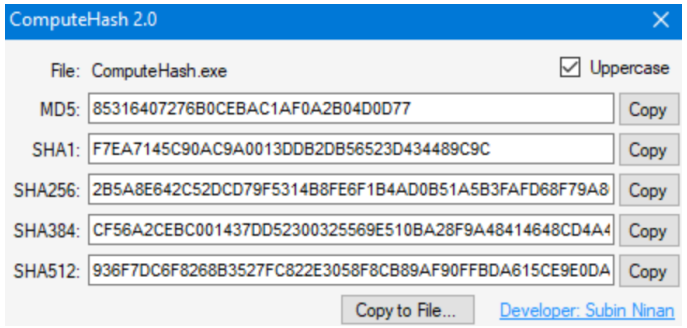
Cloud Security Mechanisms – Hashing

Hashing "Alex" -> a08372b70196c21a9229cf04db6b7ceb

- The *hashing* mechanism is used when a one-way, non-reversible form of data protection is required.
- Once hashing has been applied to a message, it is locked and no key is provided for the message to be unlocked.
- Hashing technology can be used to derive a hashing code or *message digest* from a message, which is often of a fixed length.
- The message sender can then utilize the hashing mechanism to attach the message digest to the message.
- The recipient applies the same hash function to the message to verify that the produced message digest is identical to the one that accompanied the message.
- Any alteration to the original data results in an entirely different message digest and clearly indicates that tampering has occurred.
- E.g. the storage of passwords, data integrity validation
- Typical algorithm: MD5, SHA-1, and SHA-2 (224, 256, 384, or 512 bits)

Microsoft

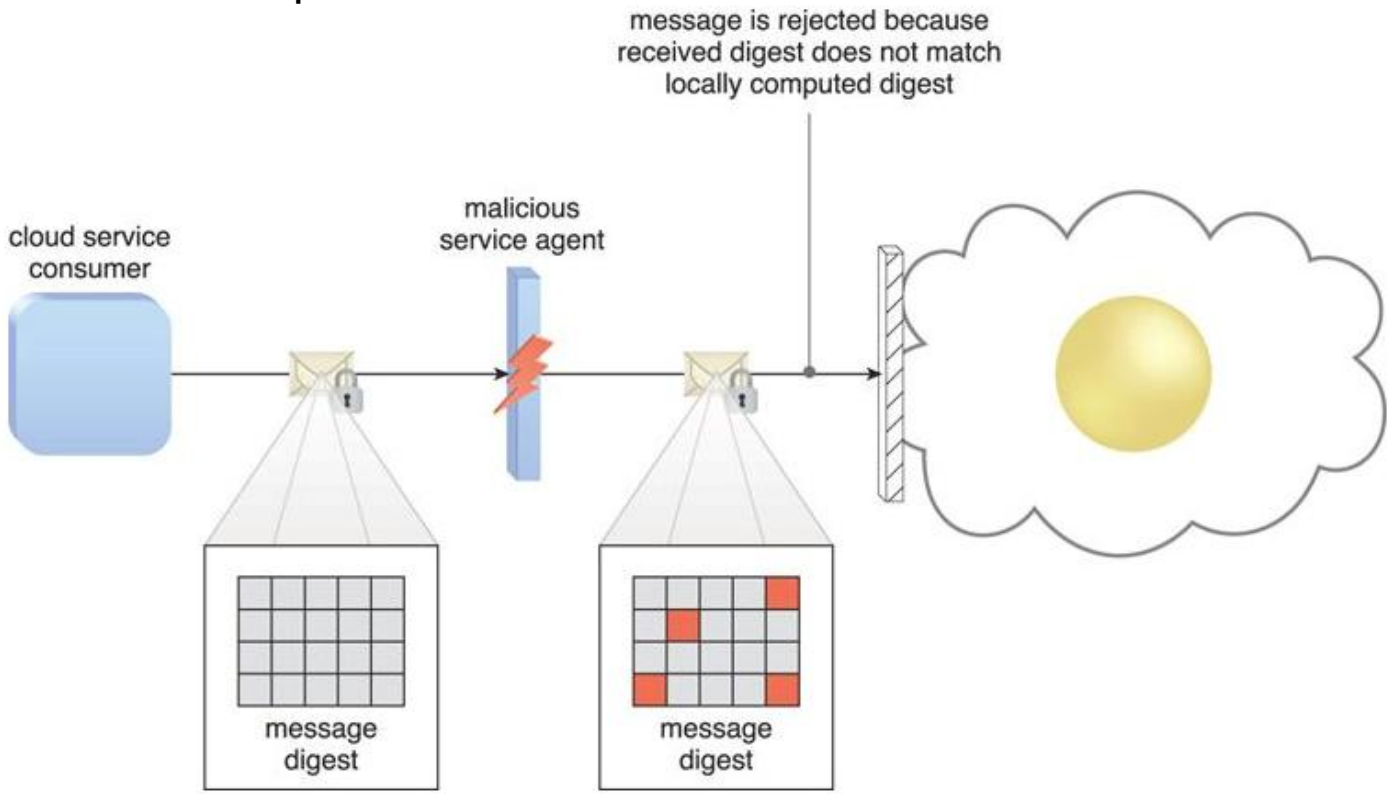




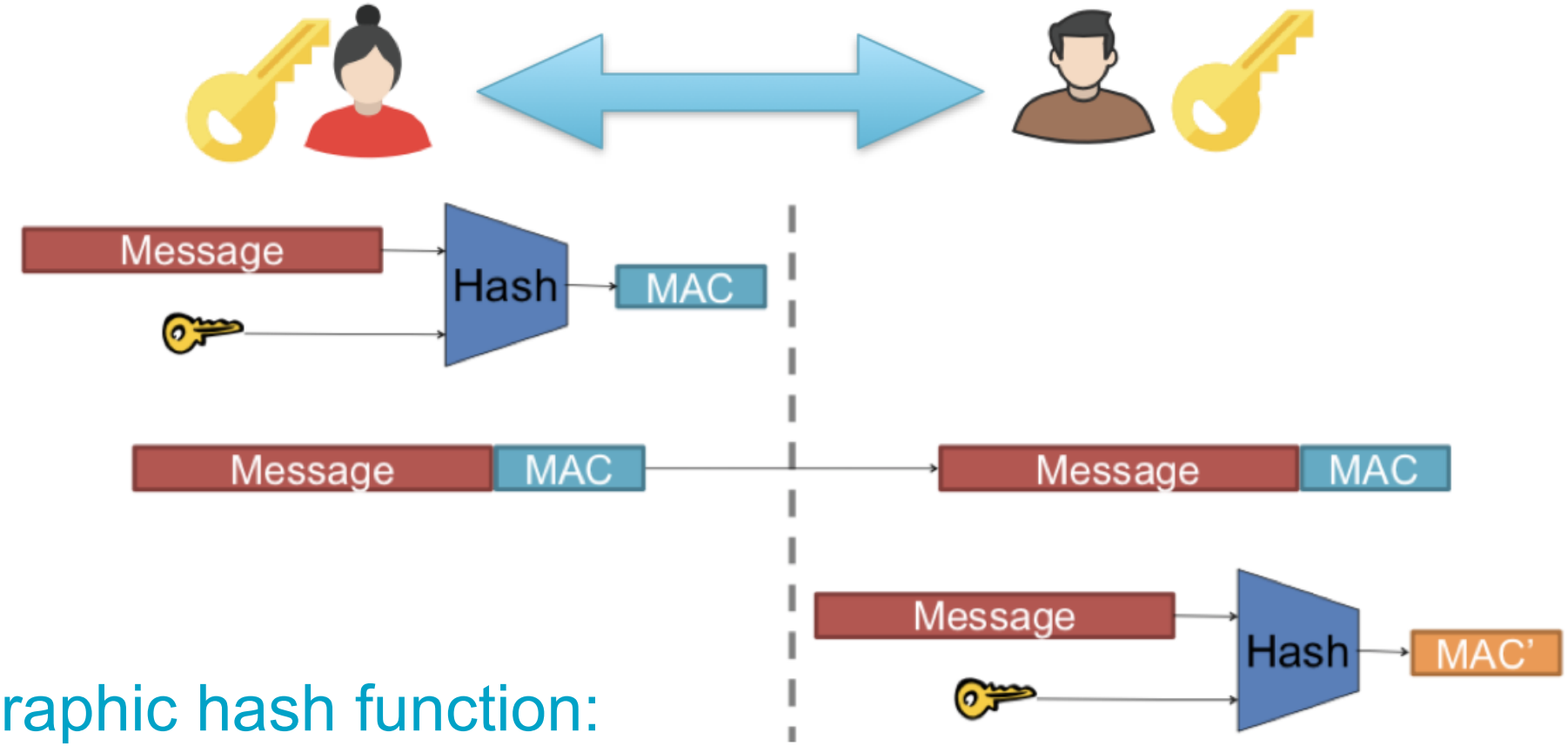
https://www.raymond.cc/blog/7-tools-verify-file-integrity-using-md5-sha1-hashes/

Cloud Security Mechanisms – Hashing

- A hashing function is applied to protect the integrity of a message that is intercepted and altered by a malicious service agent, before it is forwarded.
- The firewall can be configured to determine that the message has been altered, thereby enabling it to reject the message before it can proceed to the cloud service.



Symmetric Key: Hash Message Authentication Code for Integrity

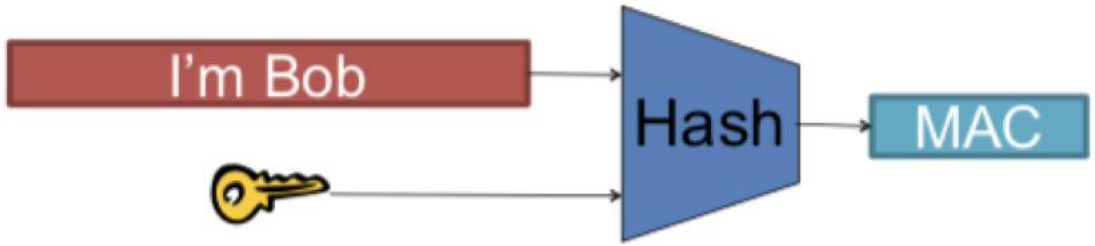


Cryptographic hash function:

- one-way, and collision resistance

Q: what is the difference with encryption?

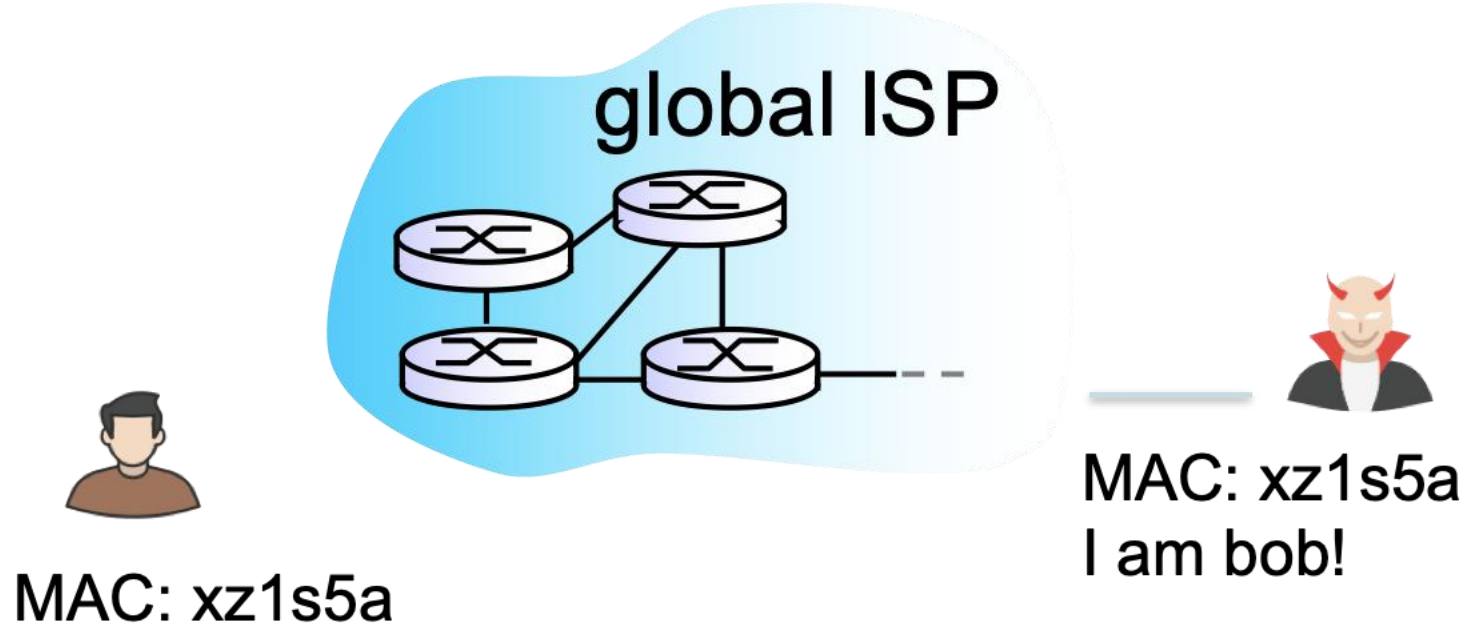
Hash Message Authentication Code for Authentication?



- Alice checks the MAC sent from Bob:
  - identify the sender is Bob

Q: is it secure in the network environment?

MAC Replay Attack and Countermeasure



If the attacker obtains Bob's MAC and replays it?
Countermeasure: nonce + challenge-response protocol

MAC Challenge- response Protocol

1. Alice sends a nonce (i.e., challenge) to Bob every time Bob would like to communicate
2. Bob then computes: Hash(key, “I’m bob”||nonce)
3. Alice receives the above hash value and re-computes it for verification

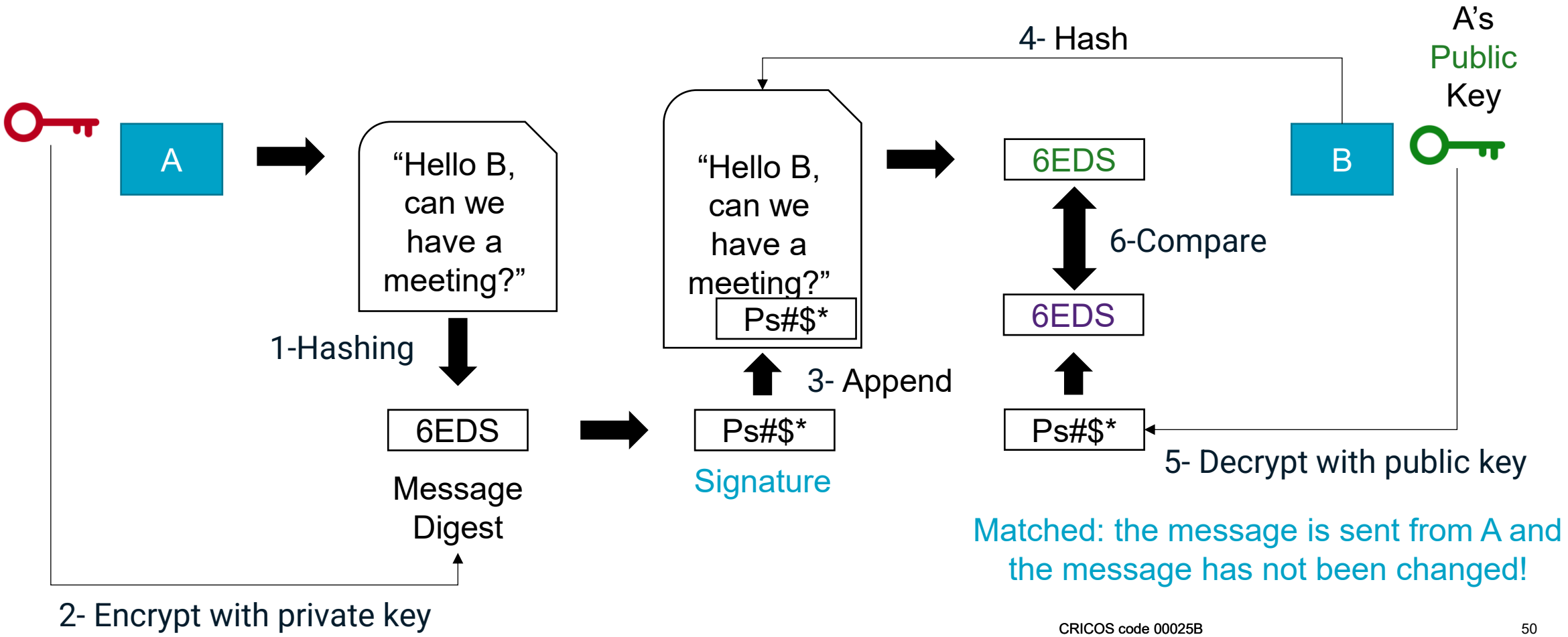
As each time the hash value will be different due to the nonce, the replay attack is mitigated.

Cloud Security Mechanisms – Digital Signature

- The *digital signature* mechanism is a means of providing data authenticity and integrity through authentication and non-repudiation.
  - A message is assigned a digital signature prior to transmission,
  - The signature will become invalid if the message has unauthorized modifications.
  - A digital signature provides evidence that the message received is the same as the one created by its rightful sender.
- Both hashing and asymmetrical encryption are involved in the creation of a digital signature
  - a message digest is encrypted by a private key and appended to the original message.
  - The recipient verifies the signature validity and uses the corresponding public key to decrypt the digital signature, which produces the message digest.
  - The hashing mechanism can also be applied to the original message to produce this message digest. Identical results from the two different processes indicate that the message maintained its integrity.

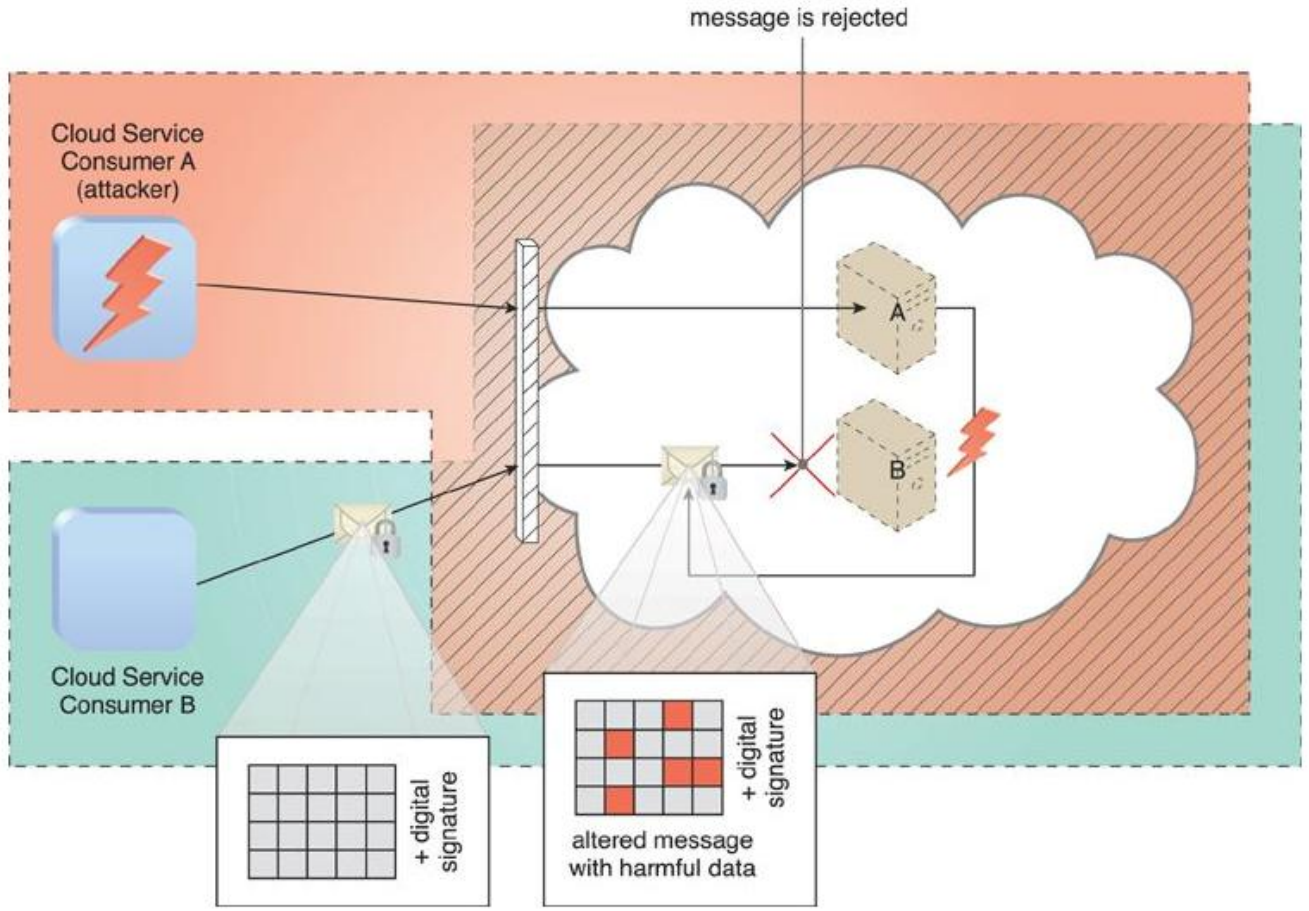
Cloud Security Mechanisms – Digital Signature

- The *digital signature* mechanism



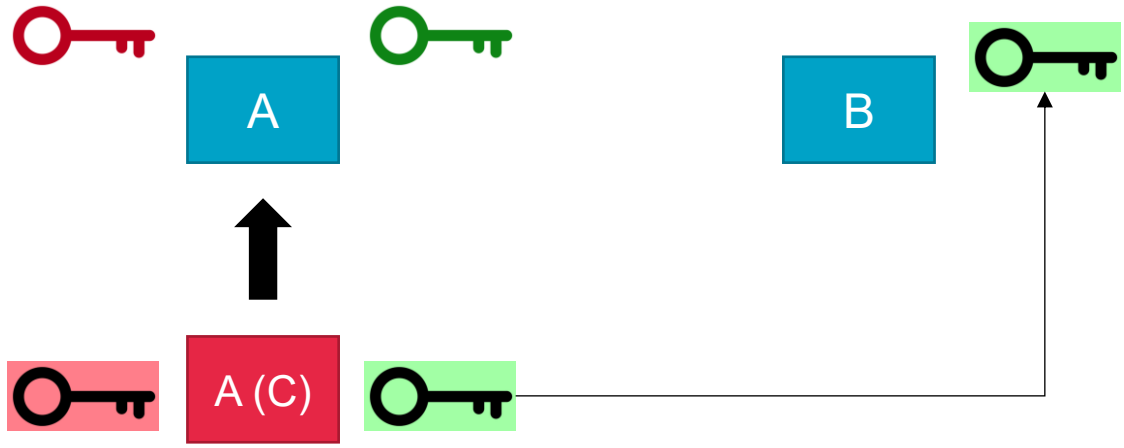
Cloud Security Mechanisms – Digital Signature

The digital signature mechanism helps mitigate the malicious intermediary, insufficient authorization, and overlapping trust boundaries security threats.



Cloud Security Mechanisms – Digital Signature

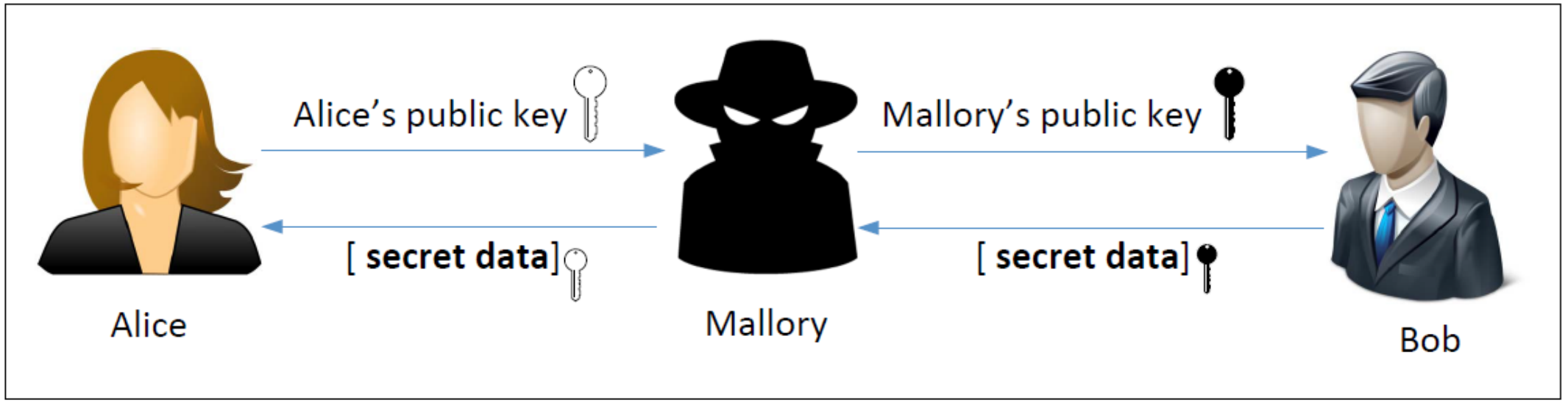
- False identity when receiving public keys



Why do we need Public Key Infrastructure (PKI)?

- *recap: public-key encryption*

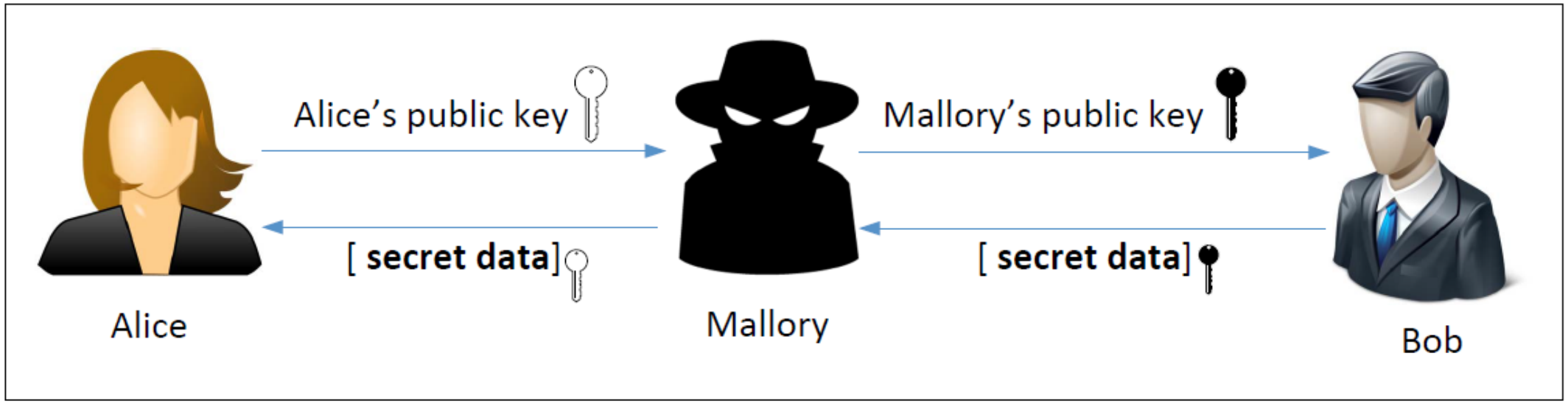
Man-in-the-Middle (MITM) Attack



Public-key encryption can defeat an adversary who can eavesdrop the communication

Q: can public-key encryption address a more powerful adversary who can intercept the communication?

Man-in-the-Middle (MITM) Attack



1. Mallory intercepts pk_alice, and forwards pk_mallory to Bob
2. Bob uses pk_mallory to encrypt messages, as he cannot tell the difference
3. Mallory intercepts BoB's encrypted messages and decrypts them

What is the Fundamental Problem?

Fundamental Problem: Bob has no way to tell whether the public key he has received belongs to Alice or not.

Solution:

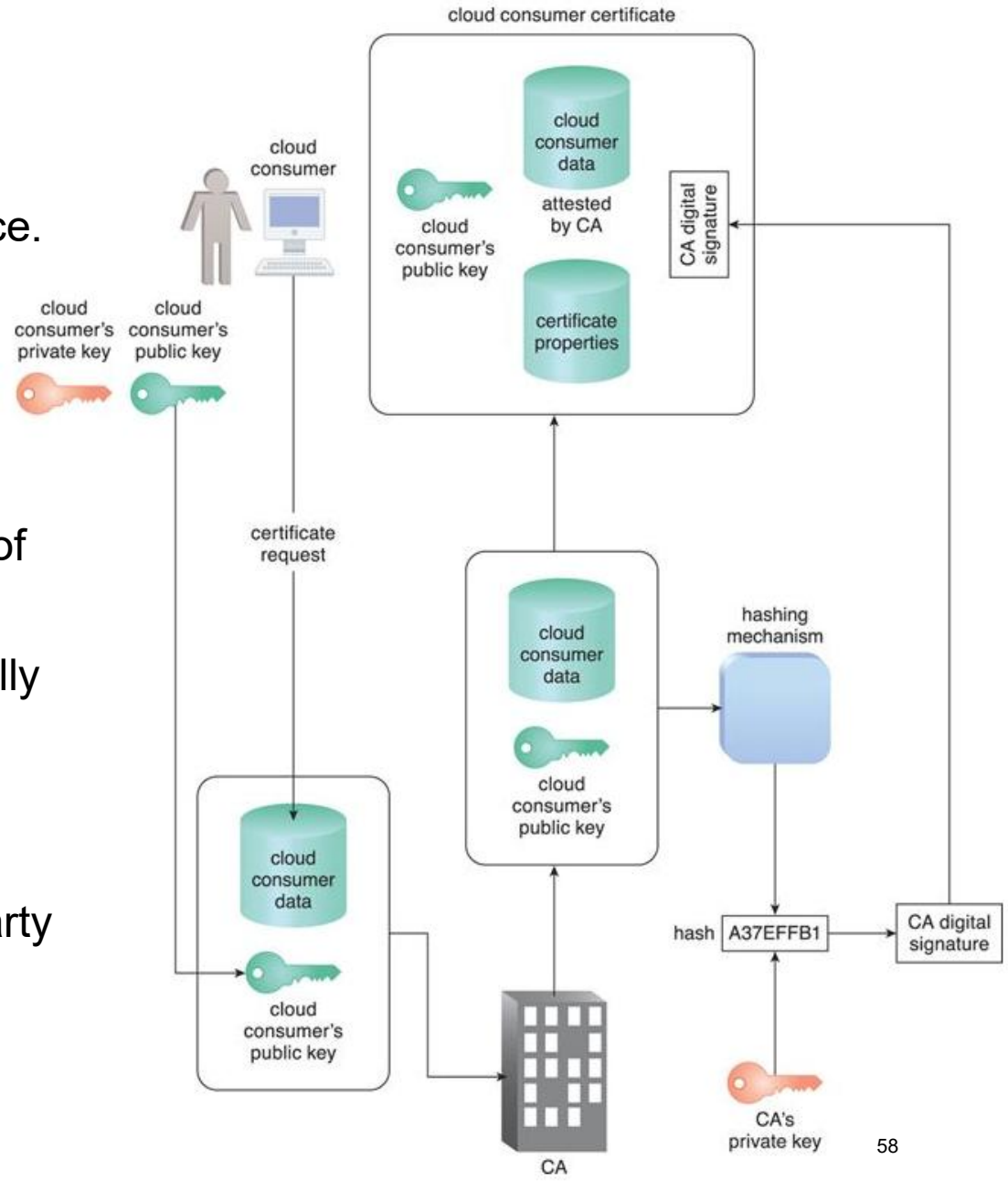
- Find a trusted party to verify the identity
- Bind an identity to a public key in a certificate
- The certificate cannot be forged or tampered with (using digital signature)

Defeating MITM Attacks using Digital Signature

- Alice needs to go to a trusted party to get a certificate.
- After verifying Alice's identity, the trusted party issues a certificate with Alice's name and her public key.
- Alice sends the entire certificate to Bob.
- Bob verifies the certificate using the trusted party's public key.
- Bob now knows the true owner of a public key.

Public Key Infrastructure (PKI)

- PKI is the cornerstone of secured Internet and e-commerce.
- PKI mechanism exists as a system of protocols, data formats, rules, and practices that enable large-scale systems to securely use public key cryptography.
- This system is used to associate public keys with their corresponding key owners while enabling the verification of key validity.
- PKIs rely on the use of digital certificates, which are digitally signed data structures that bind public keys to certificate owner identities, as well as to related information, such as validity periods.
- Digital certificates are usually digitally signed by a third-party certificate authority (CA).



Certification Authority (CA) – A trusted party

Certification authority (CA): issues **digital certificate** and binds public key to particular entity E (e.g., Jennifer).

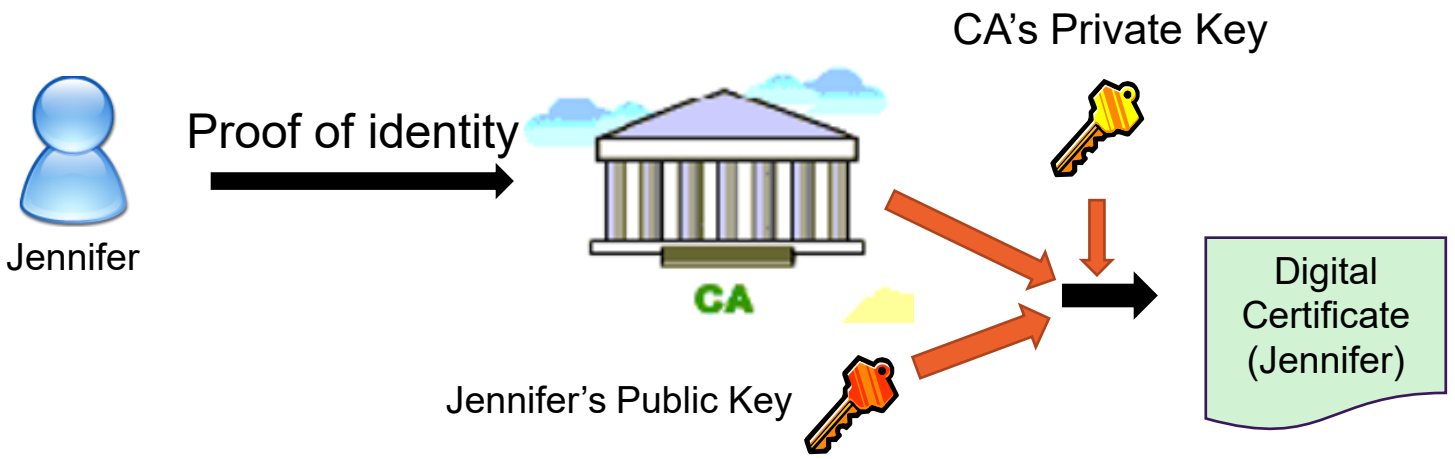
E (e.g. person, router) registers its public key with CA.

E provides "proof of identity" to CA.

CA creates certificate binding E to its public key.

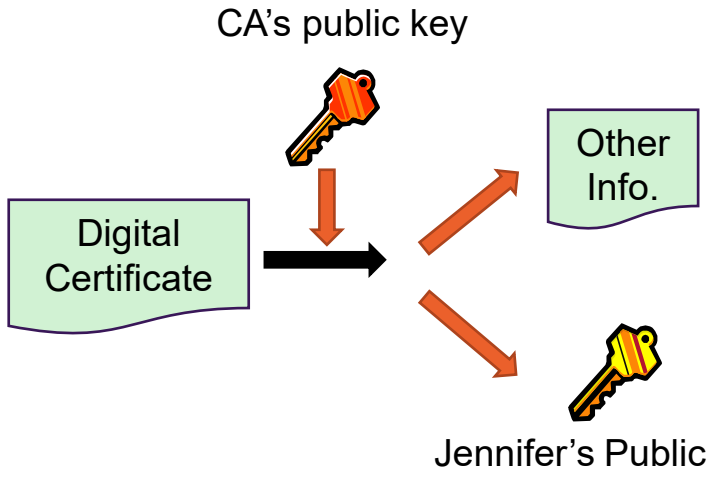
Certificate containing E's public key digitally signed by a specific CA

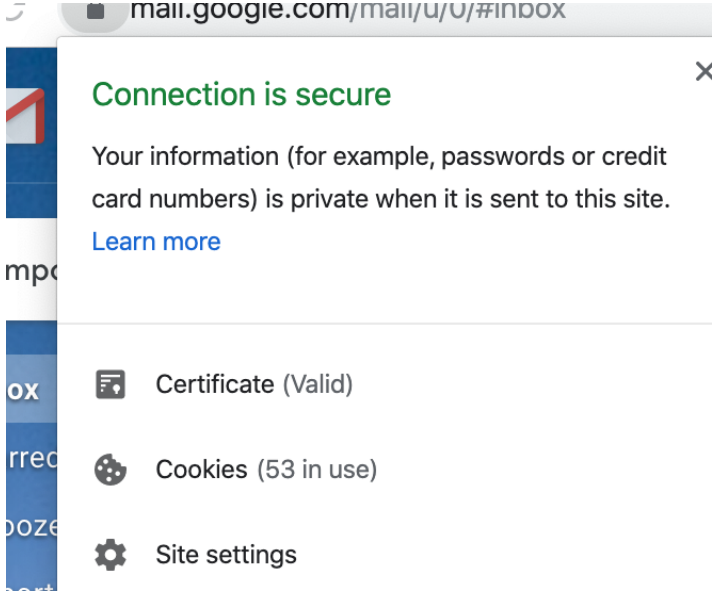
- CA says "this is E's public key"

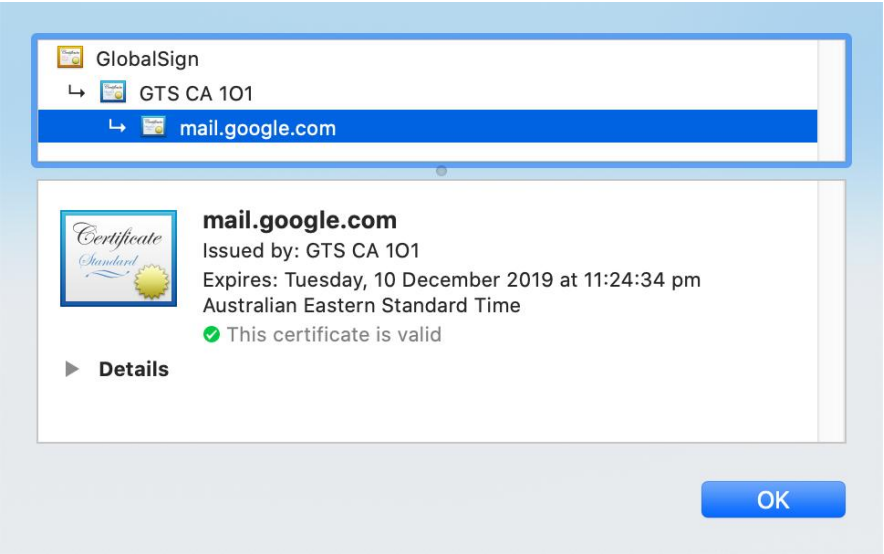


Obtaining a Public Key

In order to get the public key of Jennifer:







For Example: In google chrome, go to the https web page (say https://mail.google.com), click on the lock next to the URL, then click on "certificate information", click on the "Details" tab, and then find "Subject Public Key Info".

https://security.stackexchange.com/questions/16085/how-to-get-public-key-of-a-secure-webpage

Types of Digital Certificates

- Domain Validated Certificates (DV)
- Organisational Validated Certificates (OV)
- Extended Validated Certificates (EV)

Domain Validated Certificates (DV)

- Most popular type of certificate.
- The CA verifies the domain records to check if the domain belongs to applicant.
- Domain Control Validation (DCV) is performed on domain name in the certificate request.
  - DCV uses information in the WHOIS database
  - DCV is conducted via Email, HTTP, DNS

Organisational Validated Certificates (OV)

- Not very popular type of certificate.
- CAs verify the following before issuing OV certificates:
  - Domain control validation.
  - Applicant's identity and address.
  - Applicant's link to organisation.
  - Organisation's address.
  - Organisation's WHOIS record.
  - Callback on organisation's verified telephone number.

Extended Validated Certificates (EV)

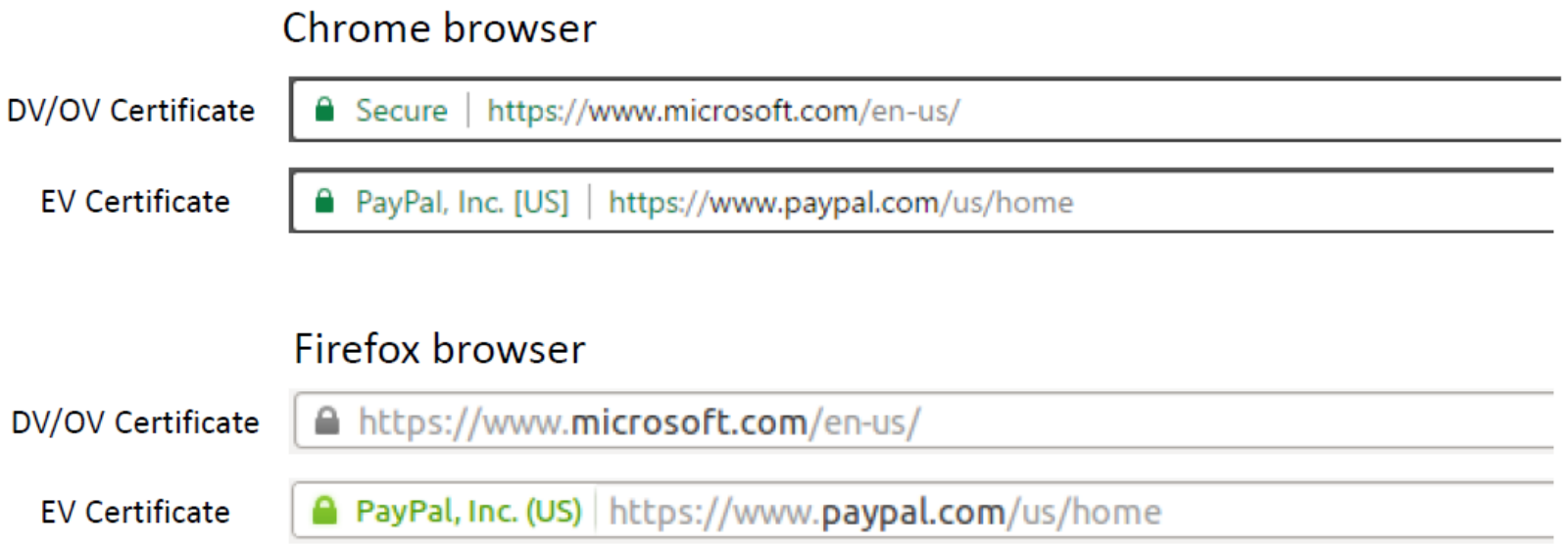
CAs issuing EV certificates require documents that are legally signed from registration authorities.

EV CA validate the following information:

- Domain control validation.
- Verify the identity, authority, signature and link of the individual.
- Verify the organisation's physical address and telephone number.
- Verify the operational existence.
- Verify the legal and proper standings of the organisation.

EV certificate, hence, costs higher but is trustworthy

How Browers Display Certificate Types



Digital Certificate

Get Paypal's certificates via openssl

```
4b:a9:64:20:cc:77:0b:30:ab:69:50:d3:71:de:dc:7c:e2:1b:93:84:1d:
78:a7:06:e8:14:03:99:c0:e4:4a:ef:c3:5d:15:2a:81:a1:b9:ff:dc:3a:
... (omitted) ...
fb:00:3e:7d:6a:de:cb:9f:ff:ef:8c:65:35:e4:22:b5:88:b2:48:32:1e:
```

```
$ openssl s_client -showcerts -connect www.paypal.com:443 </dev/null
```

Save the above data to paypal.pem, and use the following command decode it (see next slide)

```
$ openssl x509 -in paypal.pem -text -noout
```

Example of X.509 Certificate

The CA's identity (Symantec)

The owner of the certificate (paypal)

```
Certificate:
Data:
  Serial Number:
          2c:d1:95:10:54:37:d0:de:4a:39:20:05:6a:f6:c2:7f
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network,
         CN=Symantec Class 3 EV SSL CA - G3
  Validity
     Not Before: Feb  2 00:00:00 2016 GMT
     Not After : Oct 30 23:59:59 2017 GMT
  Subject: 1.3.6.1.4.1.311.60.2.1.3=US/
          1.3.6.1.4.1.311.60.2.1.2=Delaware/
          businessCategory=Private Organization/
          serialNumber=3014267, C=US/
          postalCode=95131-2021, ST=California,
          L=San Jose/street=2211 N 1st St,
          O=PayPal, Inc., OU=CDN Support, CN=www.paypal.com
```

Example of X.509 Certificate

Public Key

CA's signature

```
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
            00:da:43:c8:b3:a6:33:5d:83:c0:63:14:47:fd:6b:22:bd:
            bf:4e:a7:43:11:55:eb:20:8b:e4:61:13:ee:de:fe:c6:e2:
            ... (omitted) ...
            7a:15:00:c5:01:69:b5:10:16:a5:85:f8:fd:07:84:9a:c9:
        Exponent: 65537 (0x10001)
Signature Algorithm: sha256WithRSAEncryption
4b:a9:64:20:cc:77:0b:30:ab:69:50:d3:7f:de:dc:7c:e2:fb:93:84:fd:
78:a7:06:e8:14:03:99:c0:e4:4a:ef:c3:5d:15:2a:81:a1:b9:ff:dc:3a:
... (omitted) ...
fb:00:3e:7d:6a:de:cb:9f:ff:ef:8c:65:35:e4:22:b5:88:b2:48:32:1e:
```

- Other fields:
  - Usage period: valid period of the certificate
  - Serial number

Other Security Mechanisms

- **Identity and Access Management (IAM)**
  - encompasses the components and policies necessary to control and track user identities and access privileges for IT resources, environments, and systems.
- **Single Sign-On (SSO)**
  - enables one cloud service consumer to be authenticated by a security broker, which establishes a security context that is persisted while the cloud service consumer accesses other cloud services or cloud-based IT resources.
- **Cloud-Based Security Groups**
  - Networks are segmented into logical cloud-based security groups that form logical network perimeters.
  - Each cloud-based IT resource is assigned to at least one logical cloud-based security group.
  - Each logical cloud-based security group is assigned specific rules that govern the communication between the security groups.
- **Hardened Virtual Server Images**
  - Use a template for virtual service instance creation
  - Template is more secure than the original standard image.

Outline

- Security in Cloud Computing
  - Basic Terms and Concepts
  - Threats in Cloud Computing
  - Security Mechanisms:
    - Encryption: symmetric & asymmetric
    - Hashing
    - Digital Signature
    - PKI and CA
- Privacy in Cloud Computing
  - What is Privacy
  - Privacy Laws in Australia
  - Privacy Questions for Cloud Providers

What is Data Privacy?

Data privacy: empowering users to make their own decisions about who can process their data and for what purpose

Data privacy is the relationship among (1) the collection & dissemination of data, (2) technology, (3) the public expectation of privacy, and (4) the legal and political issues surrounding them

The General Data Protection Regulation (GDPR) https://gdpr.eu

Sun, Yunchuan, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu. "Data security and privacy in cloud computing." *International Journal of Distributed Sensor Networks* 10, no. 7 (2014): 190903.
https://smallbiztrends.com/2017/01/data-protection-tips-for-data-privacy-day-2017.html
https://www.irishtimes.com/opinion/state-s-approach-to-data-privacy-is-a-national-scandal-1.3246055

Privacy – Legislative Protections in Australia

In Australia, there are two key laws that provide protection to consumers when using cloud services.

The *Privacy Act 1988* (Privacy Act)

- Regulates how most businesses handle personal information.
- Personal information is any information or opinion about an individual who is 'reasonably identifiable'.
- This includes information that could be reasonably linked with an indiviudal's identity,
  - E.g. a telephone number in many cases.

What you should expect from Cloud Providers (CPs) in terms of privacy:

- CPs must notify you as to what personal information will be collected;
- CPs must state the intended disclosure arrangements of personal information;
- CPs can only disclose personal information outside of Australia where they have taken reasonable steps to ensure the overseas recipient does not breach the Australian Privacy Principles (APPs);
- CPs must give you access to your personal information upon request – and take reasonable steps to correct any incorrect personal information on request;
- CPs must take reasonable steps to secure personal information from misuse, interference or loss and from unauthorised access, modification or disclosure, including security breaches that occur offshore;
- CPs must take reasonable steps to delete or de-identify personal information that is no longer needed for the purpose for which it was collected.

https://www.communications.gov.au/sites/g/files/net301/f/2014-112101-CLOUD-Consumer-factsheet.pdf

Privacy – Legislative Protections in Australia

The Australian Consumer Law (ACL).

- The ACL is technology neutral and provides consumers with protections against:
  - unfair contractual terms and conditions;
  - false or misleading representations;
  - unconscionable conduct; and
  - product guarantees.
- E.g. if a cloud service provider claims that a certain level of protection will apply to your data, and fails to live up to its promise, it might be in breach of the ACL.
- The ACL is enforced jointly by the Australian Competition and Consumer Commission (ACCC) and fair trading bodies in each state and territory.

https://www.communications.gov.au/sites/g/files/net301/f/2014-112101-CLOUD-Consumer-factsheet.pdf

Privacy – Questions You Should Ask

Key privacy related questions include:

Q1: Where will my data be stored?

- If you have a preference for onshore storage options, your provider should be able to clearly inform you of the physical location of their intended data storage facilities.
- You should be aware that different countries have different laws that may allow access to stored data for purposes of law enforcement and national security.

Q2: Will you encrypt my data? Do you offer encryption services?

- Some cloud providers offer encryption services to give customers an additional level of protection for their stored data.
- Encryption services may be offered as a standard feature, or as an additional feature (for a fee) upon request.

https://www.communications.gov.au/sites/g/files/net301/f/2014-112101-CLOUD-Consumer-factsheet.pdf

Privacy – Questions You Should Ask

Key privacy related questions include:

Q3: Will my data be deleted after my contract expires? If so, when?

- Some providers delete your data when your contract expires.
- Others will keep your data for reuse.
- You should also be aware that ‘data anonymization’ practices are not the same as ‘data deletion’ practices.

Q4: Do you back-up my data? If so, where is the back-up stored?

- Providers that back-up your data provide additional resilience in the event of data loss and offer increased chances for the preservation of your data in the event of a security attack.

https://www.communications.gov.au/sites/g/files/net301/f/2014-112101-CLOUD-Consumer-factsheet.pdf

Privacy – Questions You Should Ask

Key privacy related questions include:

Q5: How will my data be provided to me (in what format) upon my contract What are your exit clauses if I choose to migrate to another vendor?

- Knowing how your data will be returned to you will help you transition to an alternative arrangement.
- You should check whether migrating to an alternative provider will be an easy process and not complicated by complex contractual exit clauses.

Q6: Under what circumstances will data be disclosed to third parties?

- If you are uncomfortable with proposed disclosure arrangements, particularly where your express consent isn't required, you can shop around for a more suitable provider.

https://www.communications.gov.au/sites/g/files/net301/f/2014-112101-CLOUD-Consumer-factsheet.pdf

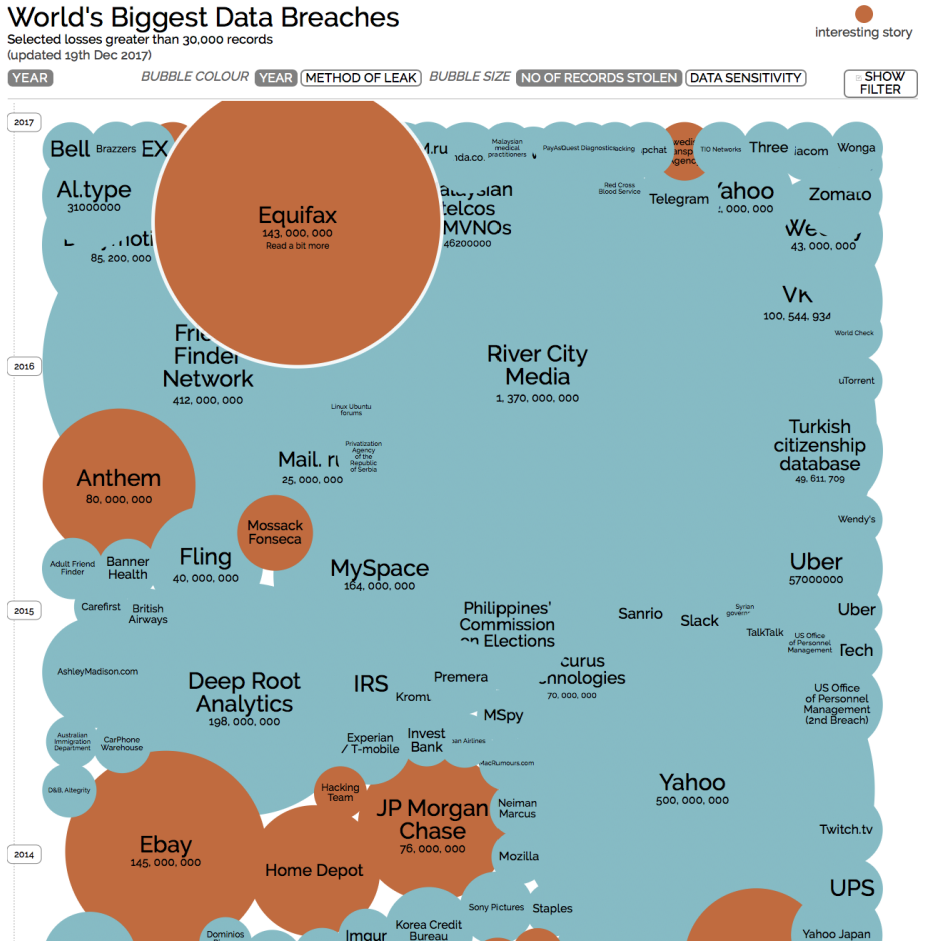
Data Leaks Raise Privacy Concerns

http://breachlevelindex.com/

Why Encrypted Database?

Sensitive data demands encrypted storage.

Encrypted search reduces risks of data breaches



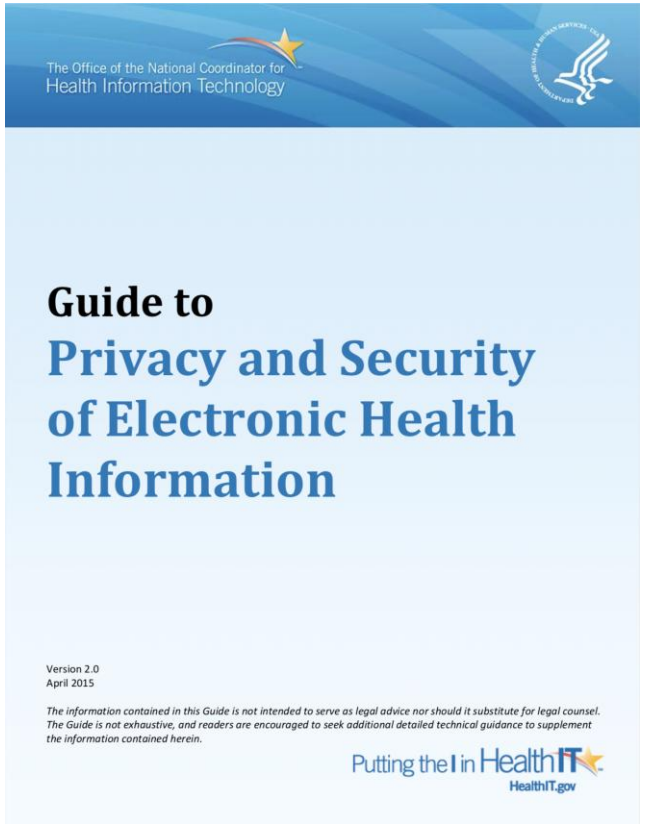
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Why Encrypted Search?

Data breaches involving 500+ patients must be reported by the recent HITECH US Health Care Law.

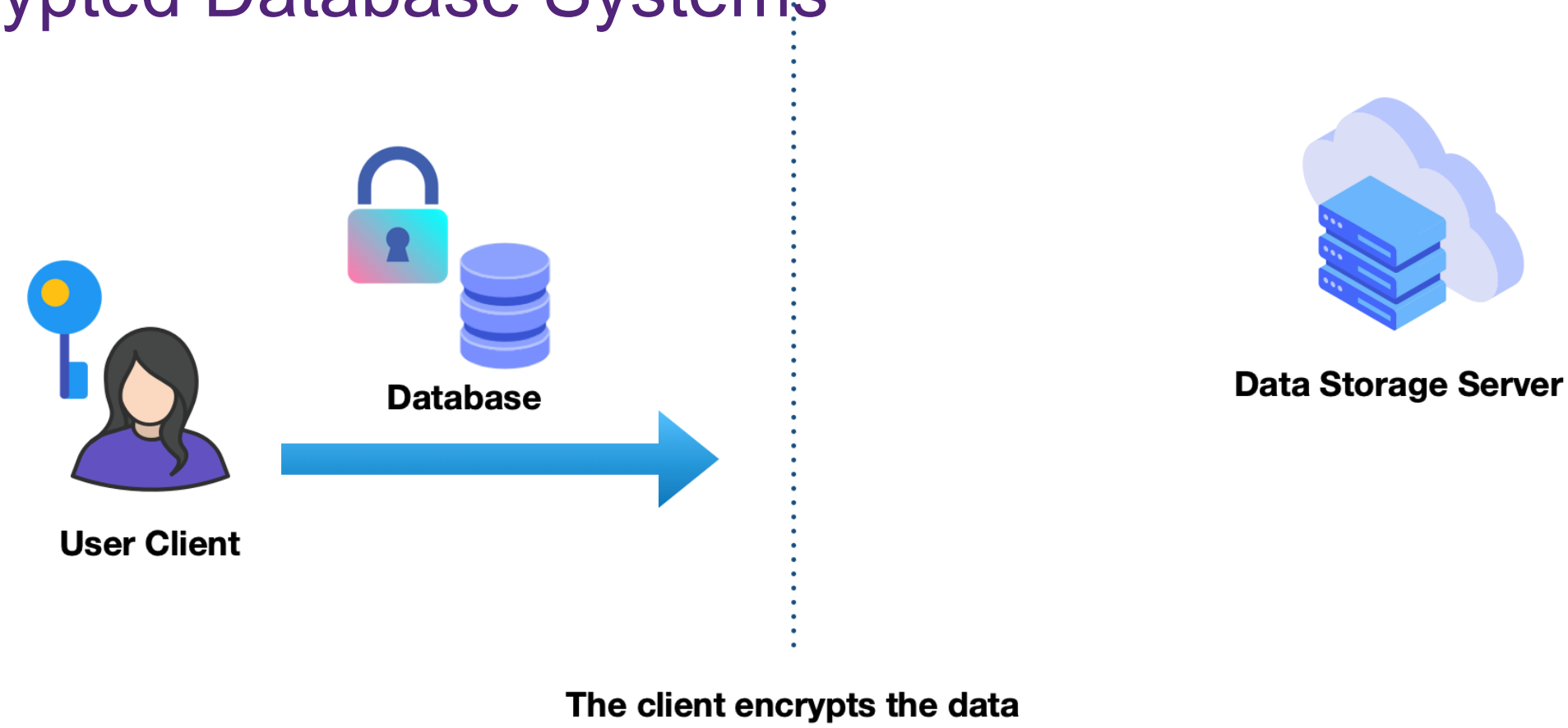
However,

"*if your practice has a breach of encrypted data [...] it would not be considered a breach of unsecured data, and you would not have to report it*"



"The Office of the National Coordinator for Health Information Technology", "Guide to privacy and security of electronic health information," 2015.
[Online] : https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

Encrypted Database Systems



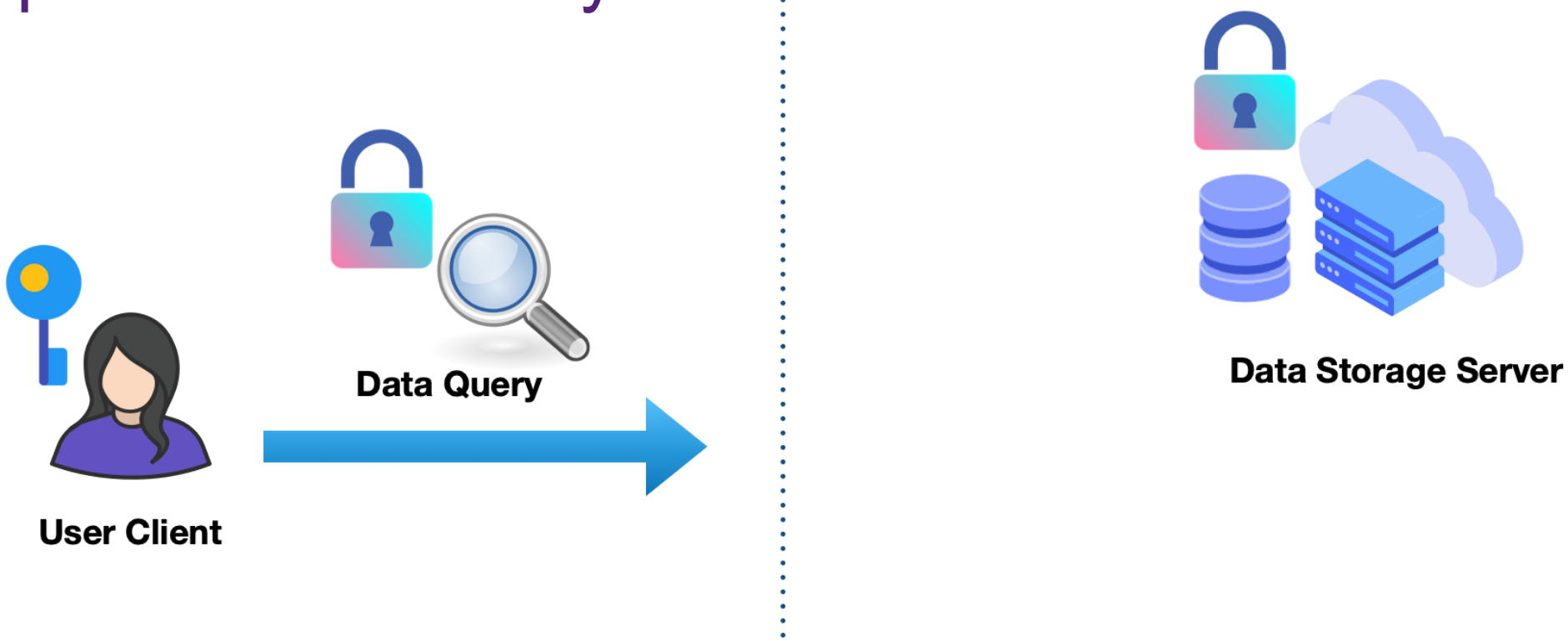
Encrypted Database Systems

User Client

Data Storage Server

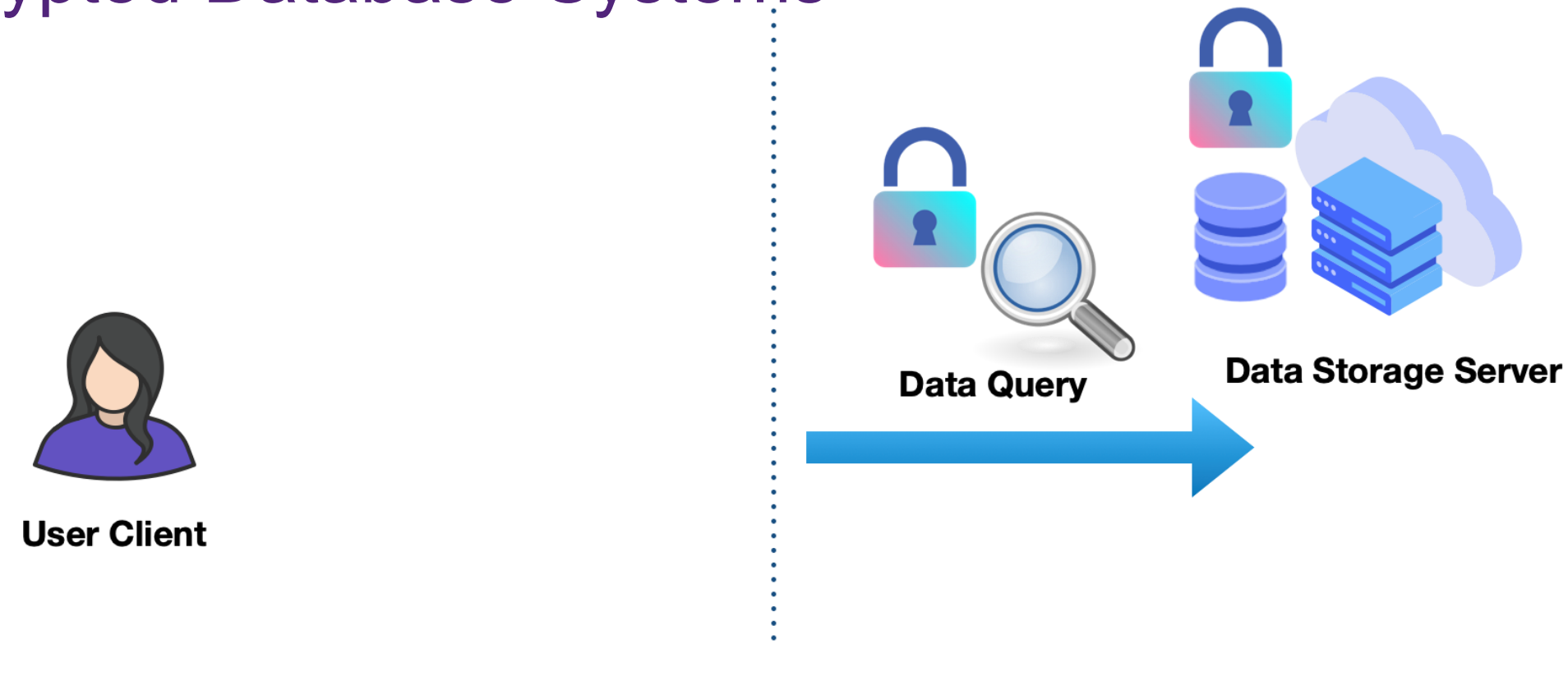
The server stores the encrypted data

Encrypted Database Systems



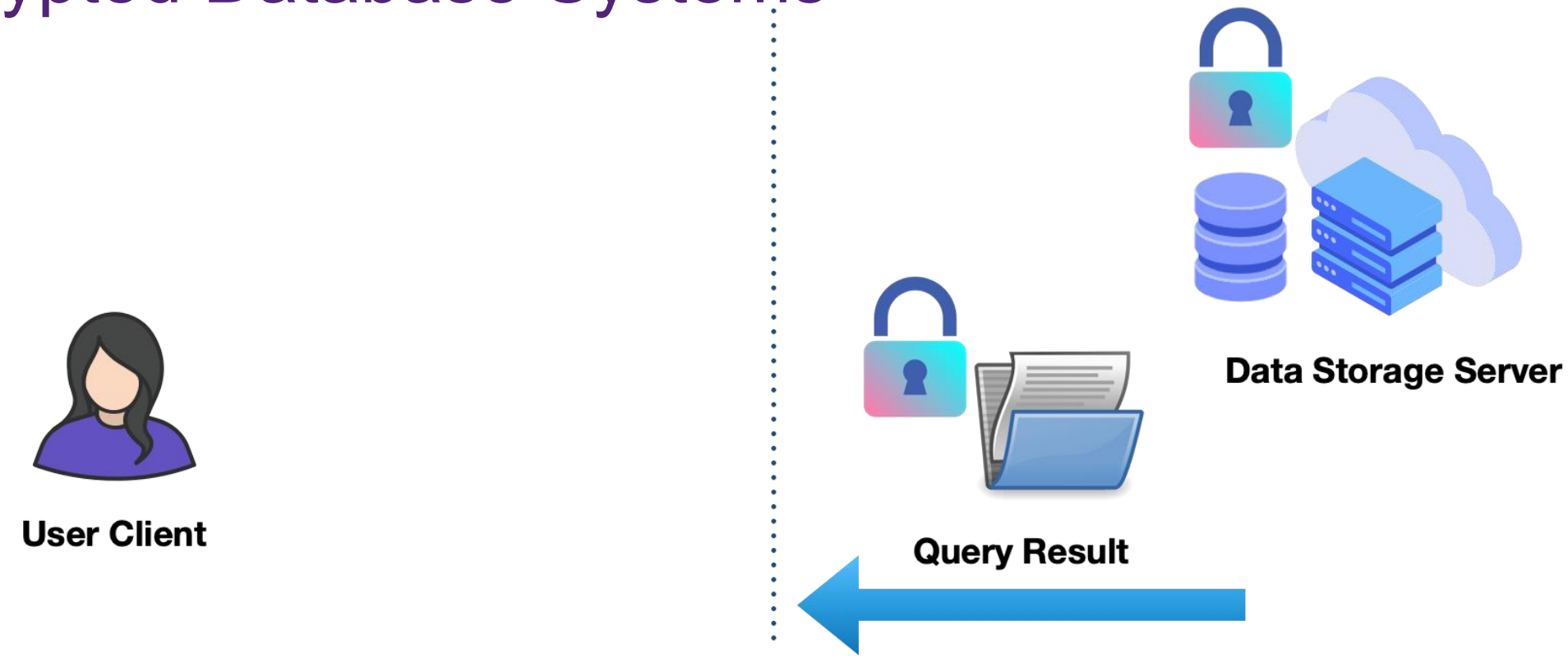
The client generates an encrypted query for search

Encrypted Database Systems



Encrypted database: the server processes the encrypted query

Encrypted Database Systems



The server processes the encrypted query and returns the encrypted result

Encrypted Database Systems

User Client

Query Result

Data Storage Server

Encrypted database: the client decrypts the result

Encrypted Database Systems

User Client

Query Result

Data Storage Server

Server can no longer access the cleartext of data and query !!!

The Area has Grown Rapidly

A wide variety of available crypto techniques

- **Property-preserving encryption, e.g., OPE, DET**
- **Searchable symmetric encryption (SSE)**
- **Trusted Execution Environment**
- **Oblivious RAM**
- Functional encryption that supports private test
- **Homomorphic encryption**
- **Secure multiparty computation**

But no best/dominant solutions

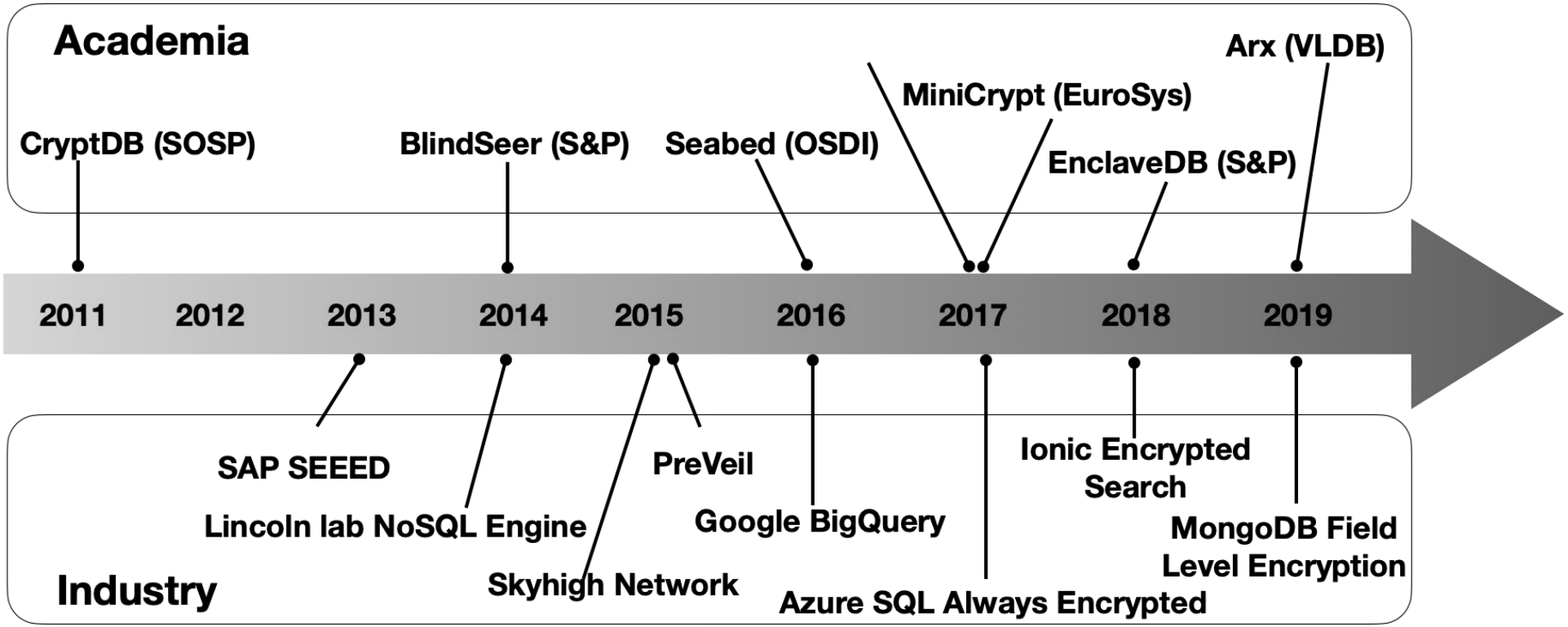
- Tradeoffs between functionality, security, and performance.

An Inflection Point in Maturity?

Rapidly growing interest in commercial space

- Bitglass
- Ciphercloud
- CipherQuery
- Crypteron
- IQrypt
- Kryptnostic
- Google's Encrypted BigQuery
- Microsoft's SQL Server 2016
- Azure SQL Database
- PreVeil
- Skyhigh
- StealthMine
- ZeroDB
- And more …

Roadmap of Encrypted Databases



References

1.“Cloud computing: concepts, technology & architecture”. Erl, Thomas, Ricardo Puttini, and Zaigham Mahmood. Pearson Education, 2013.

2.Jun Tang, Yong Cui, Qi Li, Kui Ren, Jiangchuan Liu, Rajkumar Buyya (2016) Ensuring Security and Privacy Preservation for Cloud Data Services. ACM Computing Surveys, Vol. 49, No. 1, 2016.

3.Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano (2004) Public key encryption with keyword search. In Advances in Cryptology (Eurocrypt’04). Springer, 506–522.

4.Cong Wang, Ning Cao, Jin Li, Kui Ren, and Wenjing Lou (2010) Secure ranked keyword search over encrypted cloud data. In Proceedings of IEEE 30th International Conference on Distributed Computing Systems (ICDCS’10). 253–262.

5.Seny Kamara, Charalampos Papamanthou, and Tom Roeder (2012) Dynamic searchable symmetric encryption. In Proceedings of the 2012 ACM Conference on Computer and Communications Security. IEEE, 965–976.

6.Cloud computing and privacy Consumer factsheet, https://www.communications.gov.au/sites/g/files/net301/f/2014-112101-CLOUD-Consumer-factsheet.pdf