SWINBURNE UNIVERSITY OF TECHNOLOGY

Theory of Blockchain

Session 1:

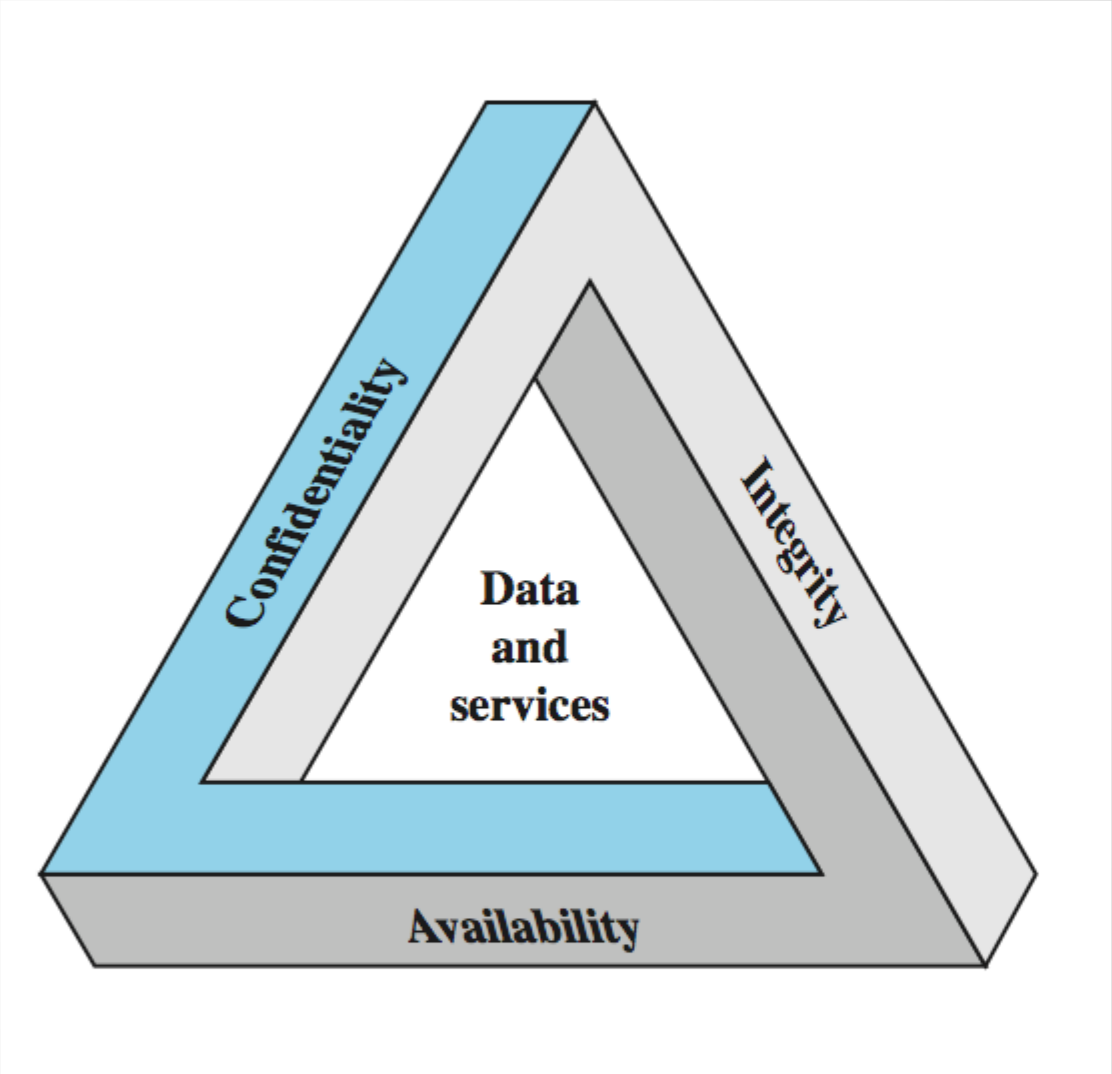
Fundamental Security Concepts

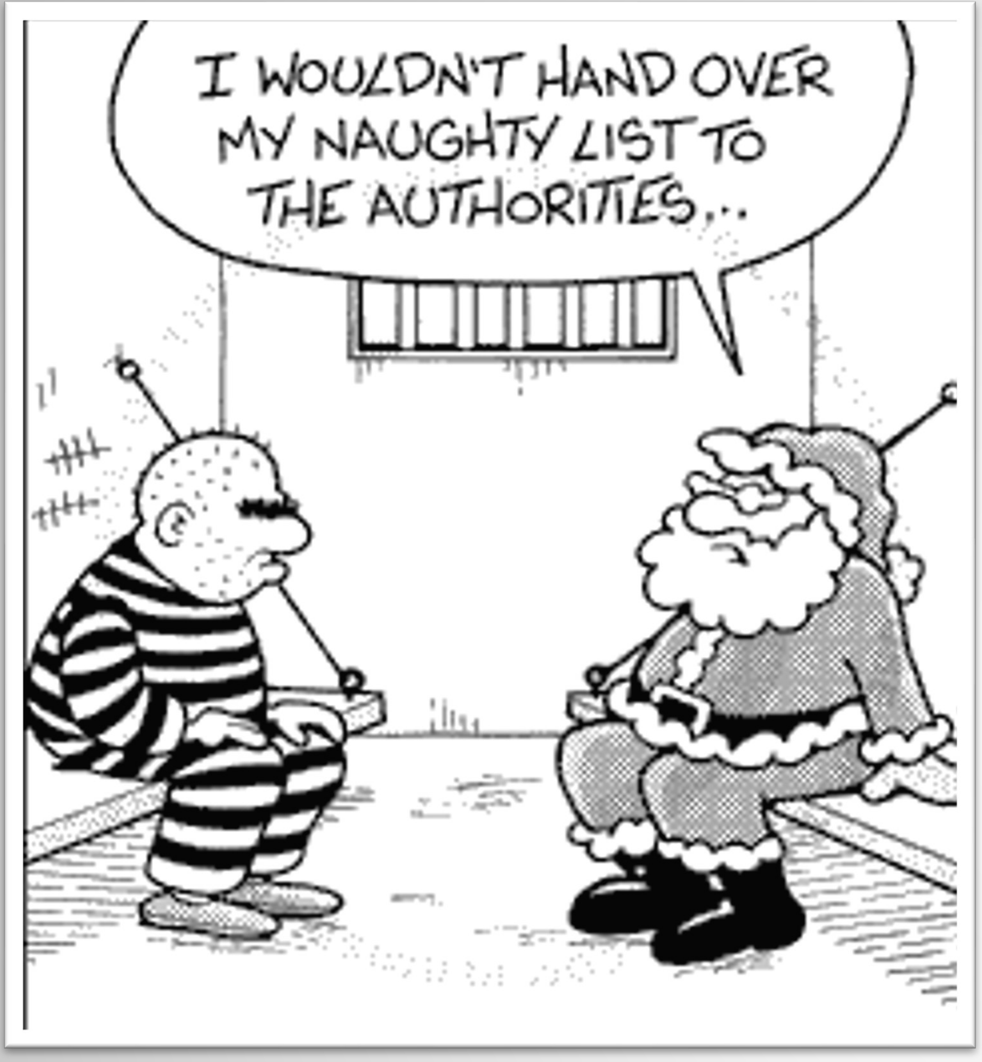
Module 2 - Basic Security Services + Definitions

Fundamental Security Services

1- Confidentiality
2- Integrity
3- Availability
4- Authentication
5- Authorization
6- Non-repudiation

The first three are fundamental (C.I.A.) , others are derivatives.





Confidentiality means keeping the information hidden from the eyes of others.

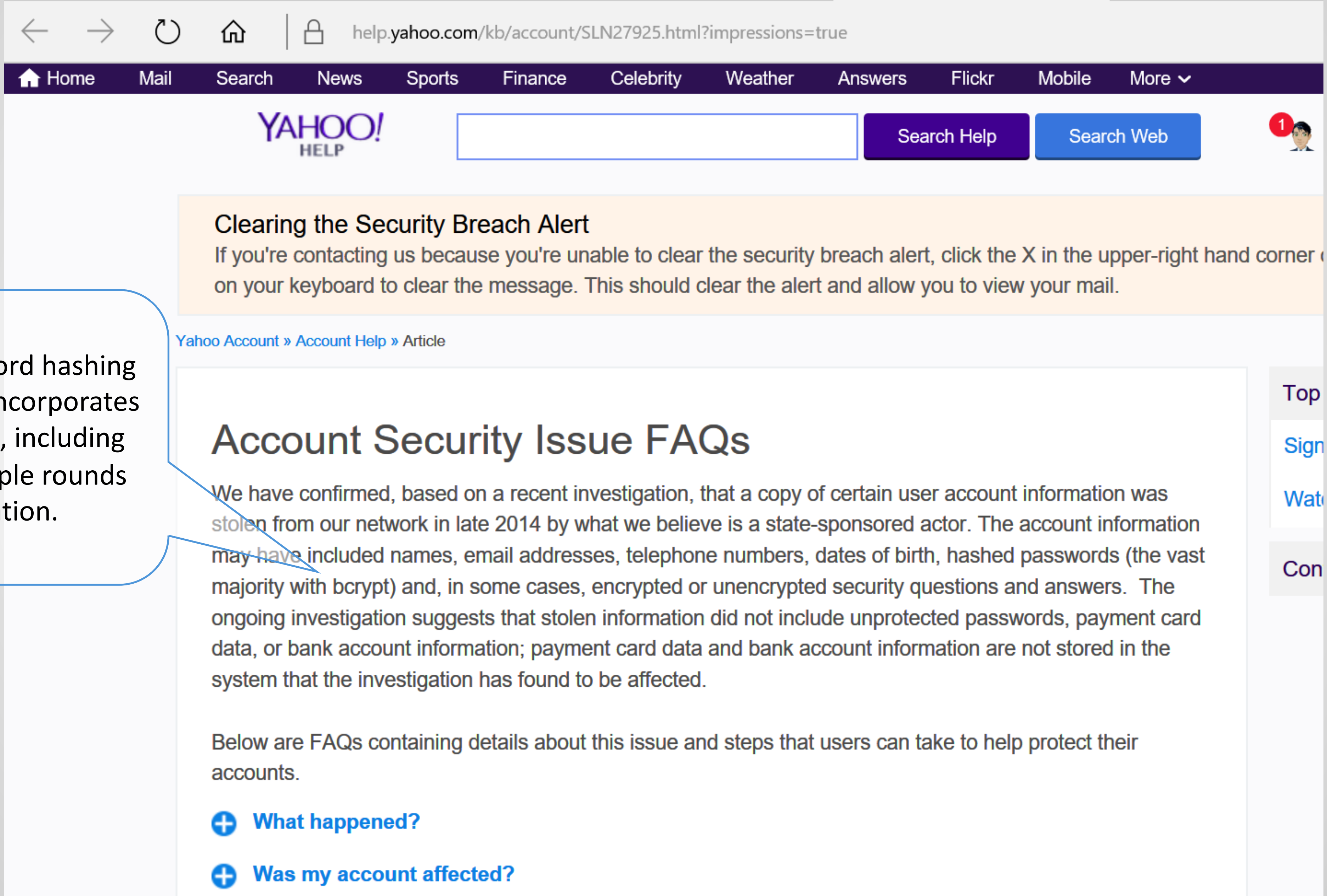
We usually encrypt the data to achieve this goal in the digital world.

Story of a Hack…

- November 24, 2014: A hacker group ("Guardians of Peace" (GOP)) leaked a release of confidential data from the film studio Sony Pictures Entertainment.
  - The data included personal information about Sony Pictures employees, e-mails between employees, executive salaries, and copies of unreleased Sony films.

(Wikipedia)

Yahoo Hack (publicized in 2016)



Clearing the Security Breach Alert

If you're contacting us because you're unable to clear the security breach alert, click the X in the upper-right hand corner
on your keyboard to clear the message. This should clear the alert and allow you to view your mail.

Yahoo Account » Account Help » Article

Account Security Issue FAQs

We have confirmed, based on a recent investigation, that a copy of certain user account information was stolen from our network in late 2014 by what we believe is a state-sponsored actor. The account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security questions and answers. The ongoing investigation suggests that stolen information did not include unprotected passwords, payment card data, or bank account information; payment card data and bank account information are not stored in the system that the investigation has found to be affected.

Below are FAQs containing details about this issue and steps that users can take to help protect their accounts.

⊕ **What happened?**

⊕ **Was my account affected?**

Bcrypt is a password hashing mechanism that incorporates security features, including salting and multiple rounds of computation.

Integrity

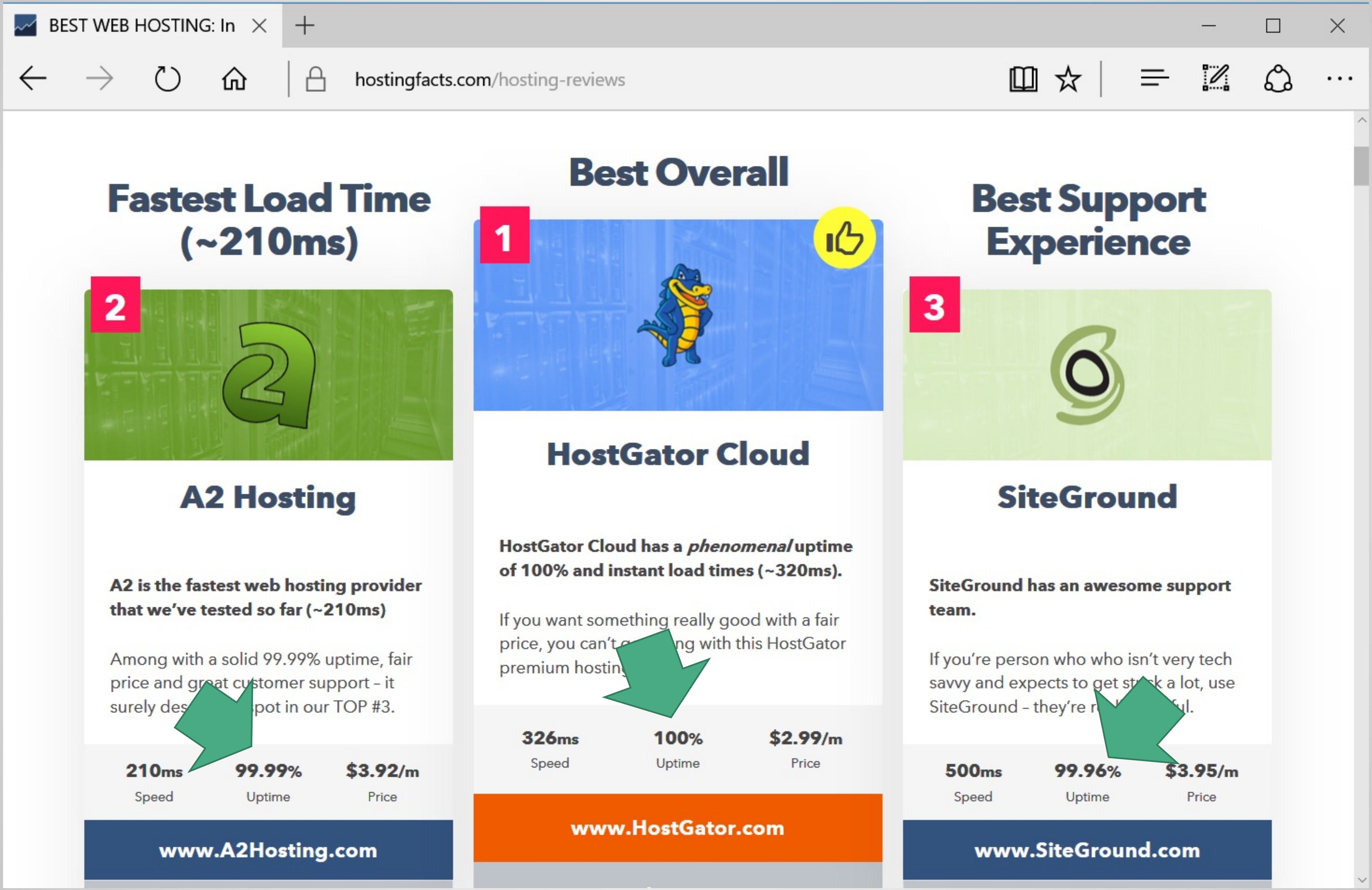
Means making sure the data is not modified or tampered with.

Even if the data is encrypted and is confidential, it can be modified.

Availability

Availability means the service should be up and available.

Some service provider show their availability rate by up-time:
e.g. 99.9% up time



Fastest Load Time (~210ms)

2

A2 Hosting

A2 is the fastest web hosting provider that we've tested so far (~210ms)

Among with a solid 99.99% uptime, fair price and great customer support – it surely des pot in our TOP #3.

210ms	99.99%	$3.92/m
Speed	Uptime	Price

www.A2Hosting.com

Best Overall

1

HostGator Cloud

HostGator Cloud has a *phenomenal* uptime of 100% and instant load times (~320ms).

If you want something really good with a fair price, you can't g ng with this HostGator premium hostin

326ms	100%	$2.99/m
Speed	Uptime	Price

www.HostGator.com

Best Support Experience

3

SiteGround

SiteGround has an awesome support team.

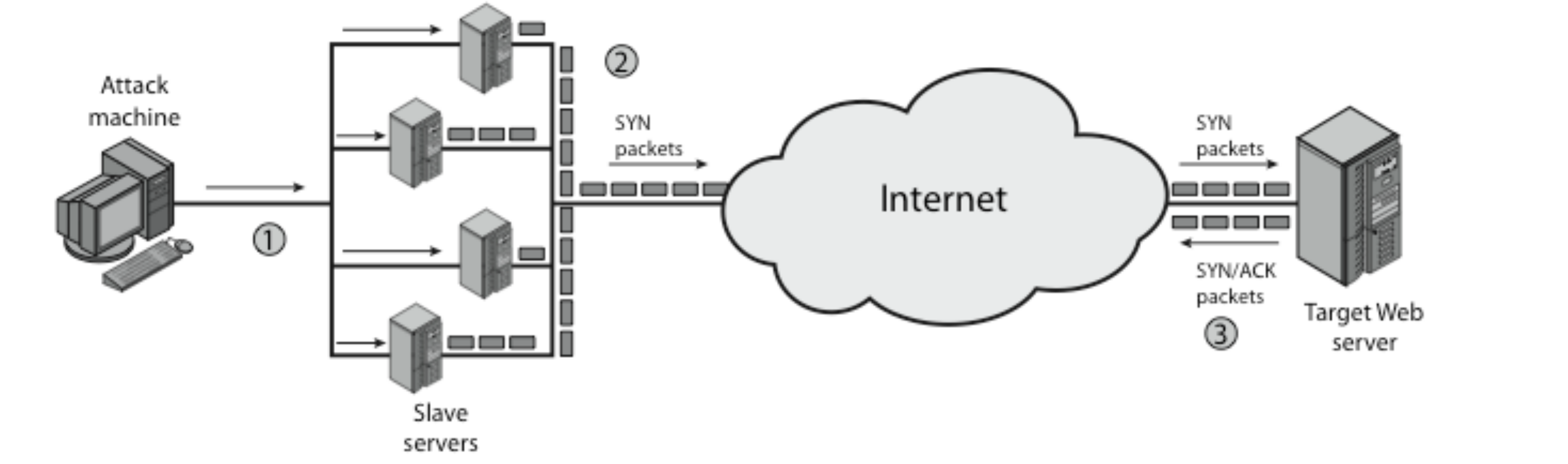
If you're person who who isn't very tech savvy and expects to get st k a lot, use SiteGround – they're r ful.

500ms	99.96%	$3.95/m
Speed	Uptime	Price

www.SiteGround.com

Distributed Denial of Service Attacks (DDoS)

Distributed SYN Flooding Attack

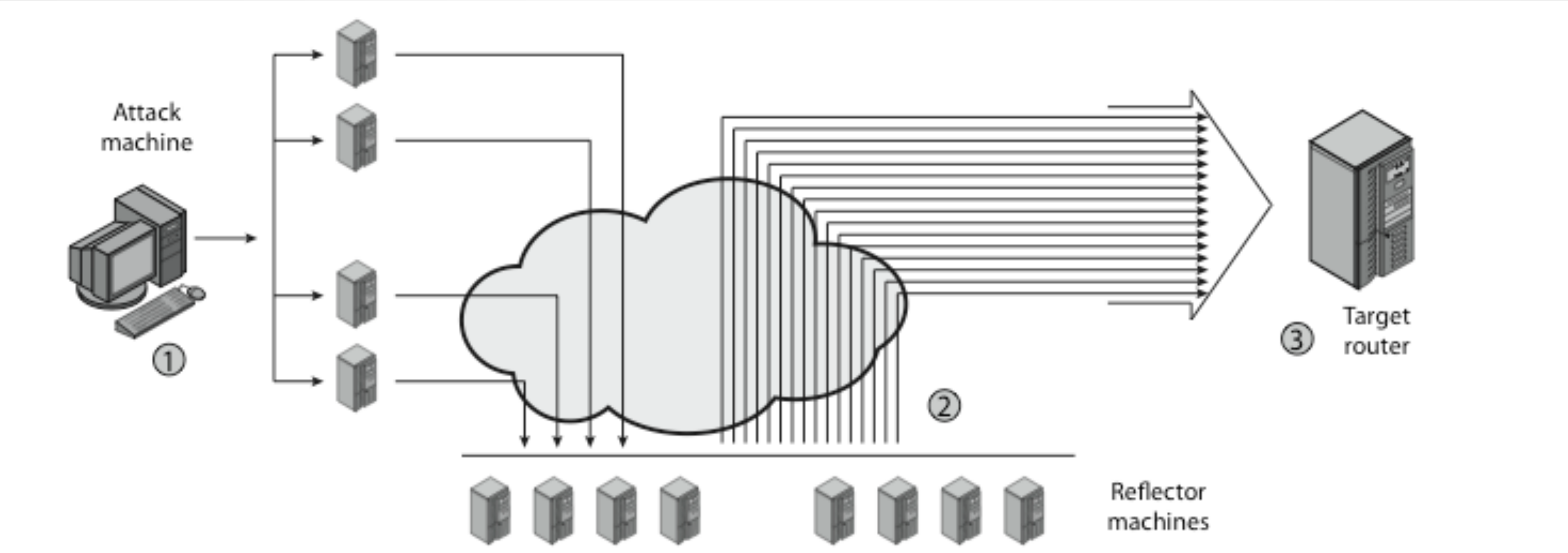


1. The attacker takes control of multiple hosts over the Internet 2. The slave hosts begin sending TCP/IP SYN (synchronize/initialization) packets, with erroneous return IP address information, to the target 3. For each such packet, the Web server responds with a SYN/ACK (synchronize/acknowledge) packet. The Web server maintains a data structure for each SYN request waiting for a response back and becomes bogged down as more traffic floods in.

(Stallings Net. Sec. Essentials)

Distributed Denial of Service Attacks (DDoS)

Distributed ICMP DoS Attack / Reflection DoS Attack



1. The attacker takes control of multiple hosts over the Internet, instructing them to send ICMP ECHO packets with the target's spoofed IP address to a group of hosts that act as reflectors 2. Nodes at the bounce site receive multiple spoofed requests and respond by sending echo reply packets to the target site. 3. The target's router is flooded with packets from the bounce site, leaving no data transmission capacity for legitimate traffic.

(Stallings Net. Sec. Essentials)

Authentication

Authentication means making sure the one who claims an ID, is really the one he says.

© 2013 Union of Concerned Scientists

Authorization means giving permission to access resources.

This is directly related to the access-control topic.

Examples are keys (to doors) in the real world.

Non-repudiation

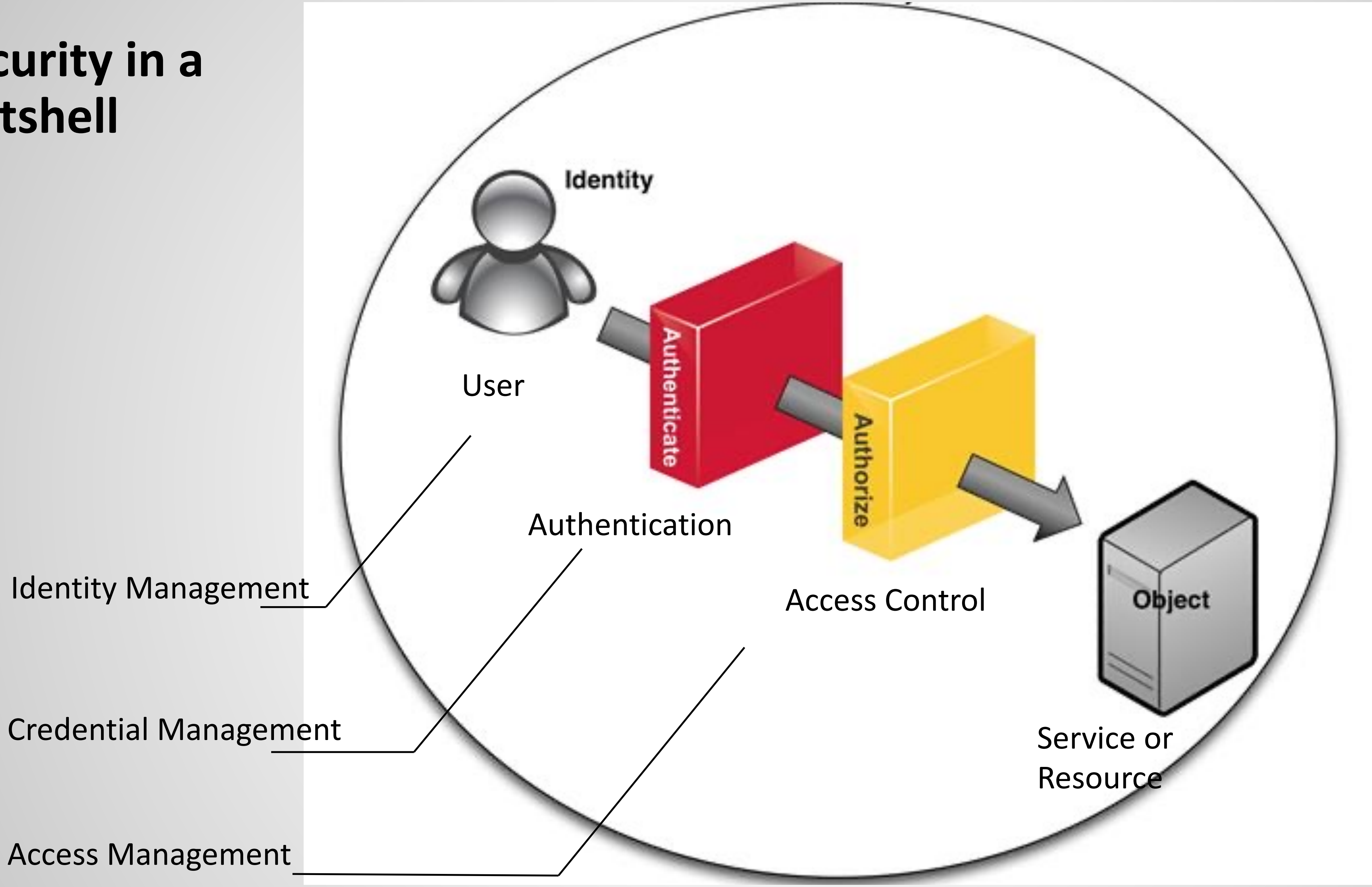
"First off, I'd like to categorically deny any wrongdoing...."

Non-repudiation is the service that makes sure no one can deny what he/she has done.

e.g. when you sign a contract digitally, you can’t say I haven’t done it.

How are these services used in practice?

Security in a Nutshell



User

Authentication

Access Control

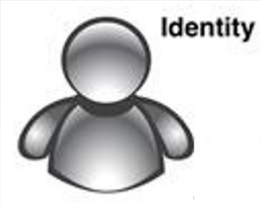
Service or Resource

Identity Management

Credential Management

Access Management

ID



Real World

Virtual World

Whatever unique code or tag for a person or thing

SOCIAL SECURITY

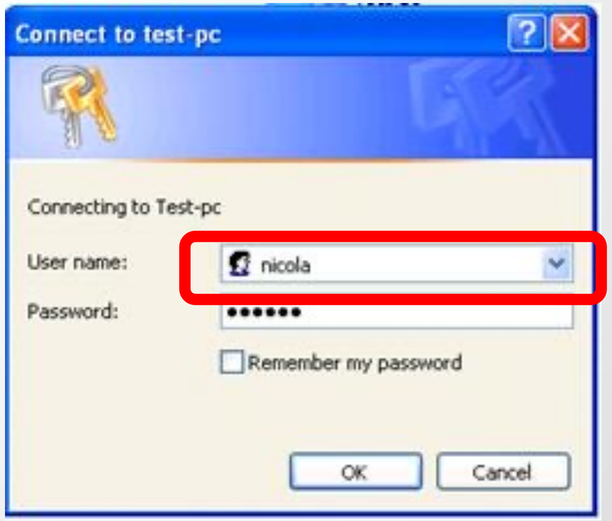
000 - 00 - 0000

THIS NUMBER HAS BEEN ESTABLISHED FOR

JOHN DOE

John Doe

username



Connecting to Test-pc

User name: nicola

Password: ••••••

□ Remember my password

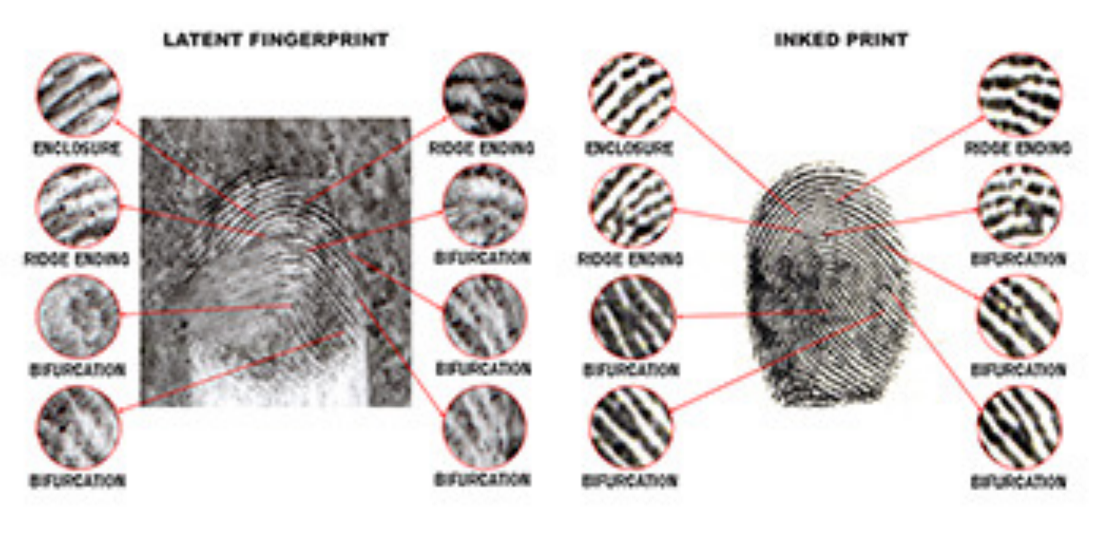
Employee code #128340

barcode

5 012345 678900

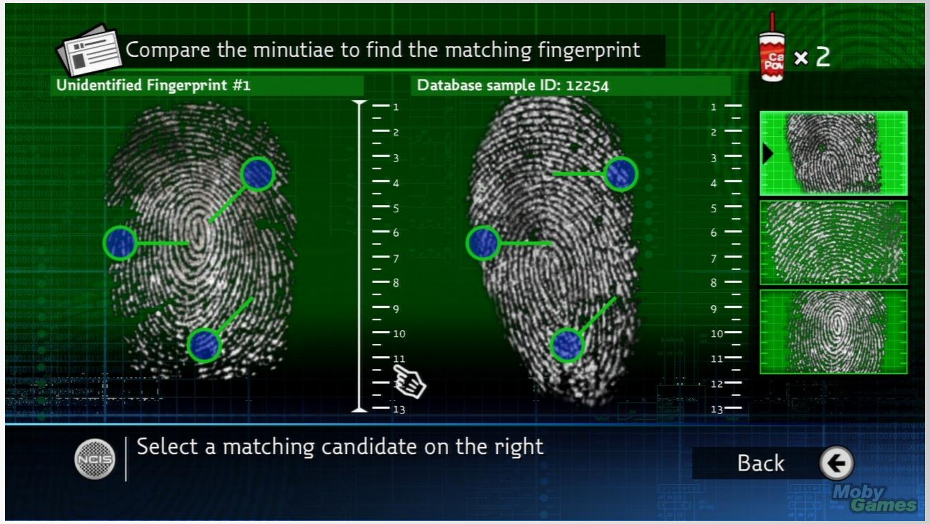
Authentication

Fingerprint matching



Real World | **Virtual World**

biometric fingerprint (what I am)



Compare the minutiae to find the matching fingerprint

Unidentified Fingerprint #1

Database sample ID: 12254

Select a matching candidate on the right

Face matching

Secret word

Password (what I know)

Password

****

Forgot your password?

Token (what I have)

User name: john_smith

Password: ••••••••••

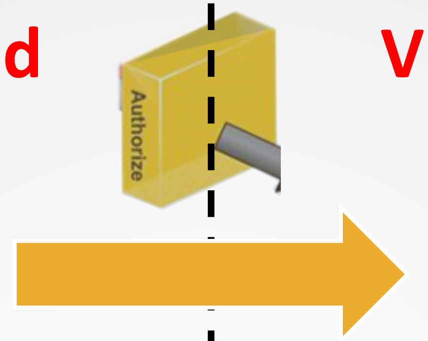
PASSCODE:

Log On

Authorization / Access Control

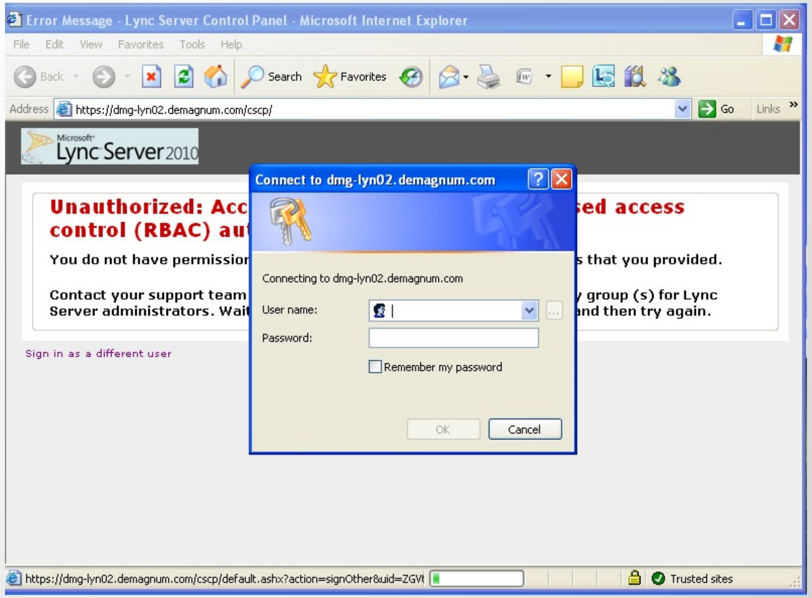
Door key is the access permission

Real World



Virtual World

Document
Classification


Error Message - Lync Server Control Panel - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
Microsoft Lync Server 2010

https://dmg-lyn02.demagnum.com/cscp/

Unauthorized: Acc… …sed access control (RBAC) au…

You do not have permissio… …s that you provided.

Contact your support team … …y group (s) for Lync Server administrators. Wai… …and then try again.

Sign in as a different user

Connect to dmg-lyn02.demagnum.com

Connecting to dmg-lyn02.demagnum.com

User name:

Password:

□ Remember my password

OK Cancel

https://dmg-lyn02.demagnum.com/cscp/default.ashx?action=signOther&uid=ZGVt

Trusted sites

Access to bank
account et.

Authentication

- Authentication can be done by any of these factors:

  - **What I know** (e.g. Password)
  - **What I have** (e.g. Card)
  - **What I am** (e.g. Fingerprint)

Main factors

  - Where I am
  - How I do stuffs
  - …

Supporting factors

What Comes Next …

- So far we have learned the basics of security services. We will use them all along the way.

- In the next video, we will also learn about the terms used in the cyber security domain, including blockchain.

See you in the next video …