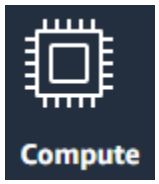
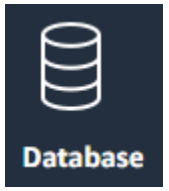
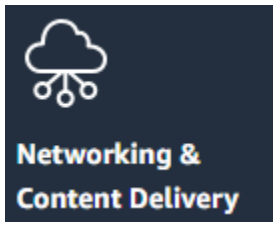
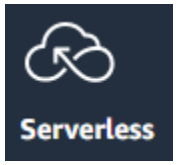
CS 240
Computer Systems

#23: Security and Authentication

Nov. 16, 2021 · Wade Fagen-Ulmschneider

Overview of Cloud Services (AWS)

	**Amazon EC2:** "Virtual Services in the Cloud" (Identical to your course VM in the UIUC private cloud, but EC2 provides public cloud access.)
	Amazon Elastic Container Registry: "Easily store, manage, and deploy container images" (Docker) **Amazon Elastic Container Service (ECS):** "Highly secure, reliable, and scalable way to run containers"
	**Amazon Aurora:** "High performance managed relational database" (SQL) **Amazon DynamoDB**: "Managed NoSQL database" (MongoDB-like) **Amazon ElastiCache: "**In-memory caching system" (Redis-like)
	**Amazon API Gateway:** "Build, deploy, and manage API's" **Amazon CloudFront:** "Global content delivery network" (CDN) **Amazon Route 53:** "Scalable domain name system (DNS)"
	**AWS Lambda:** "Run code without thinking about servers"
	Amazon Simple Storage Service (S3): "Scalable storage in the cloud" **Amazon Elastic File System (EFS)**: "Fully managed file system for EC2"

Security and Authentication

One advanced topic in cloud systems is security and authentication. Doing security correctly is **very hard** and the best practices change rapidly (what I learned 10 years ago is trash-tier security nowadays).

Token-Based ("Bearer") Authorization

One of the most fundamental pieces of cloud security is token-based authorization. You have seen this already:

-
-
-
-
-

Q: What is a **token**?

Assuming the token uses [a-zA-Z0-9], there are **62** possible character choices. What security against guessing the token does various token lengths provide?

Length	Combinations	Avg. Time to Find @ 1m guesses /sec
1	$62^1 = 62$	0.031 **ms**
2	$62^2 = 3{,}844$	1.9 **ms**
3		
4	$62^4 = 1{,}4776{,}336$	7.4 **seconds**
5	$62^5 = 916{,}132{,}832$	458 **seconds**
10	$62^{10} = 8.4 \times 10^{17}$	13 298 **years**
15	$62^{15} = 7.7 \times 10^{26}$	~12,182,899,300,000 **years**

The Google URL to this sheet worksheet:

1P061GTQYgMp0WOXqmJqh2ZzlK2AFZDPeJmWLWThtUlE
12345678901234567890123456789012345678901234 1 2 3 4

Total Length: _____ ⇒ Combinations: _____

Avg. Time to Find (at 1,000,000 guesses /sec):

Q: What happens if you leak the token?

...does that make token-based authentication insecure?

Token Storage
Nearly all datastores have optimizations around storing unique values, referred to as indexes in the database:

SQL Database: (Relational Datastore)	`CREATE INDEX UserToken ON tableUserTokens (token);`
MondoDB: (NoSQL Datastore)	`db.userTokens.createIndex( { "token": 1 }, { unique: true })`
Redis (Memory Datastore)	*(Every key acts like an index.)*

Tokens are stored in a BTree or HashTable-like structure, resulting in runtimes that are:

Authorization vs. Authentication
Tokens provide a form of authorization (access) to a specific resource, and are often used after a form of authentication (verification) is done.

Authentication as a Service
Many applications now rely on "Authentication as a Service" where the authentication is handled by a separate application.

- Ex: "Login with Google" / "Login with Instagram" / ...
- Ex: Queue@Illinois ⇒ Login w/ Illinois
  - Shibboleth (UIUC login technology) provides user authentication without revealing any details except that the user!

Advantages:

Disadvantages:

On Thursday: How does this all happen?

Project MIX - Week 2
https://courses.grainger.illinois.edu/cs240/fa2021/project/part2/

Deliverables:
(1): Extend your Microservice <-> IM interface to use age-based caching technologies, as specified in the HTTP standard.

(2): Create additional IMs so that you have a total of ***3p*** IMs.
- Update your IMs.md to document the new IMs.

(3): Ensure that at least one IM depends on the output of another IM.

Due Date: