Cyber Defense Organization

Fall 2018 - Intro to Cloud Security

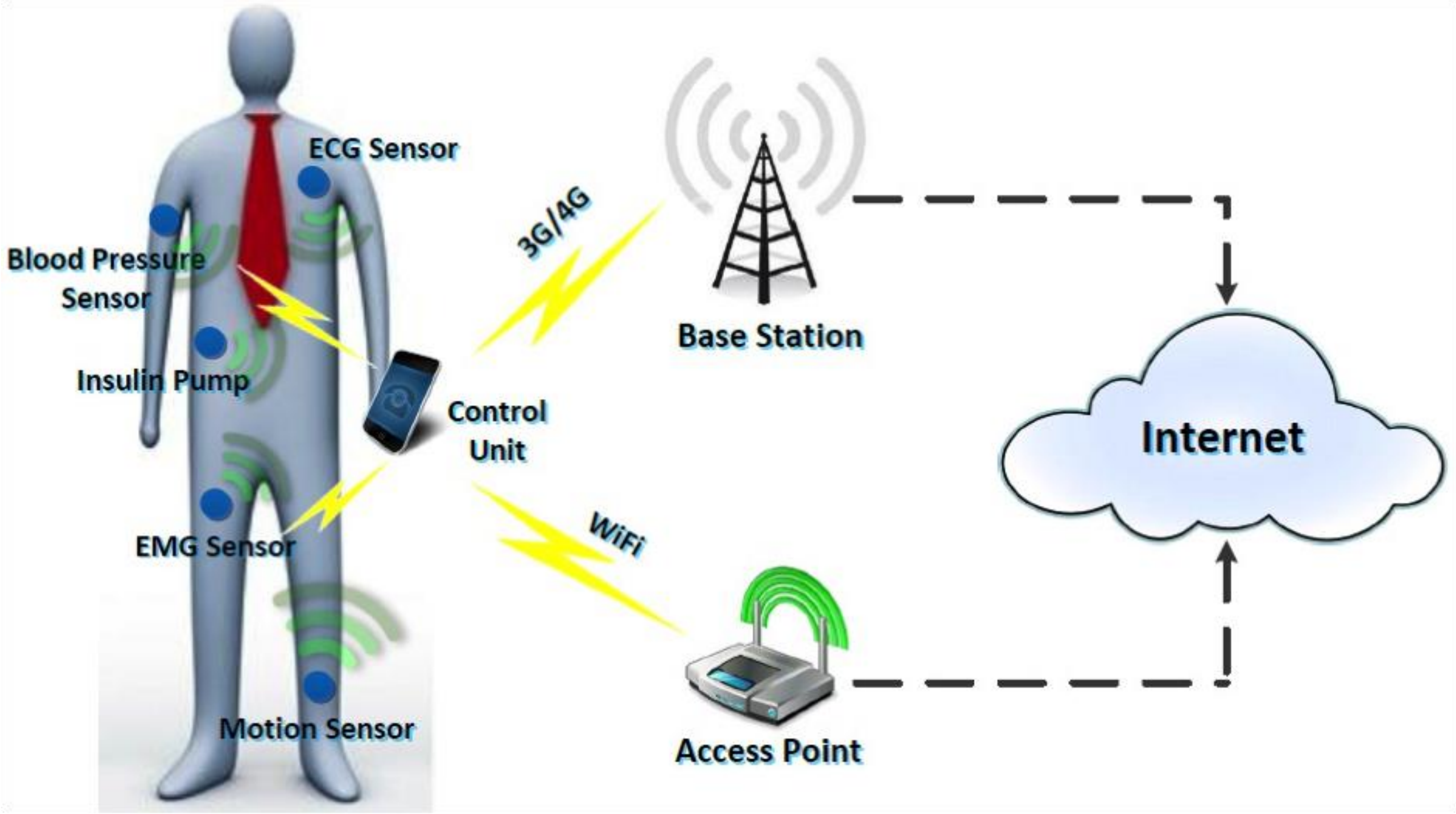
Agenda:

- Word of the Week
- What is the “Cloud”?
- Types of cloud services and cloud providers?
- AWS
- Open up AWS, and go to the management console
- Creating the virtual pentest lab with Kali and *Ubuntu.
- Messing with IAM and creating a real life example “datajanitor”
- Looking at AWS GuardDuty
- Reading CloudTrail
- Closing thoughts

Word of the Week

Body Area Network

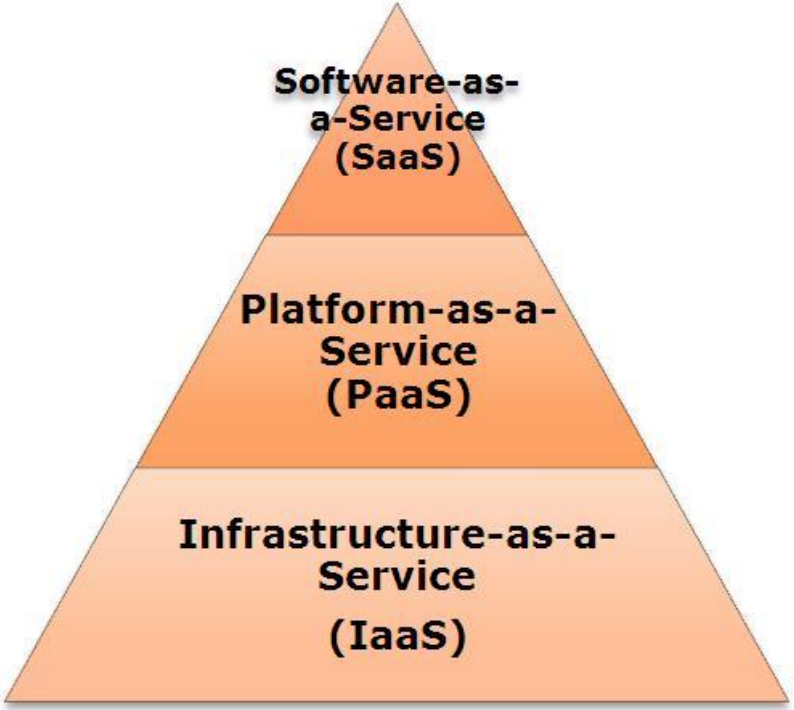
A body area network (BAN) is the interconnection of multiple computing devices worn on, affixed to or implanted in a person’s body. A BAN typically includes a smartphone in a pocket or bag that serves as a mobile data hub, acquiring user data and transmitting it to a remote database or other system.


ECG Sensor
Blood Pressure Sensor
Insulin Pump
EMG Sensor
Motion Sensor
Control Unit
3G/4G
WiFi
Base Station
Access Point
Internet

What is a “Cloud”

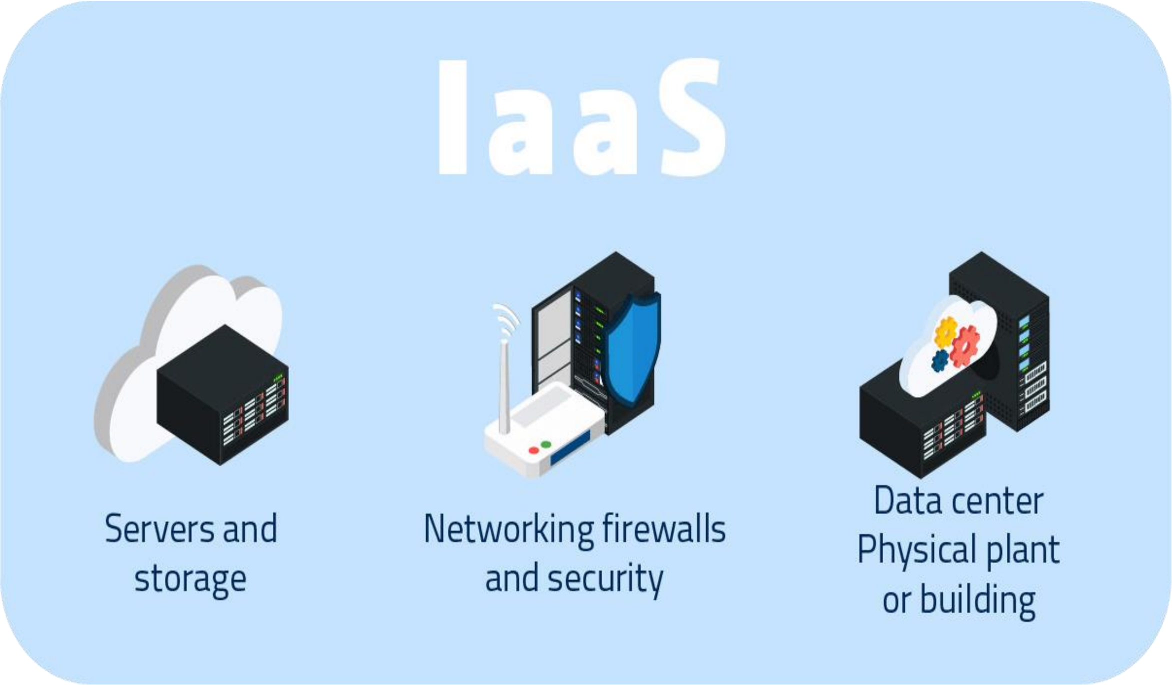
Cloud computing is taking services (*"cloud services"*) and moving them outside an organization's firewall. Applications, storage and other services are accessed via the Web. The services are delivered and used over the Internet and are paid for by the cloud customer on an as-needed or pay-per-use business model.

Types of Cloud Services


Software-as-a-Service (SaaS)
Platform-as-a-Service (PaaS)
Infrastructure-as-a-Service
(IaaS)

Iaas (Hardware)

You’re base, the physical stuff.


IaaS
Servers and storage
Networking firewalls and security
Data center Physical plant or building

PaaS

Geared towards Software Developers

The application stack of the Infrastructure

“Middleware”

A placeholder for your php or javascript.

SaaS

For the End User (Customers)

Google Docs..

Application for you delivered over the internet.

OS-agnostic, you can access it anywhere.

SaaS
SOFTWARE AS A SERVICE

Other types of Services

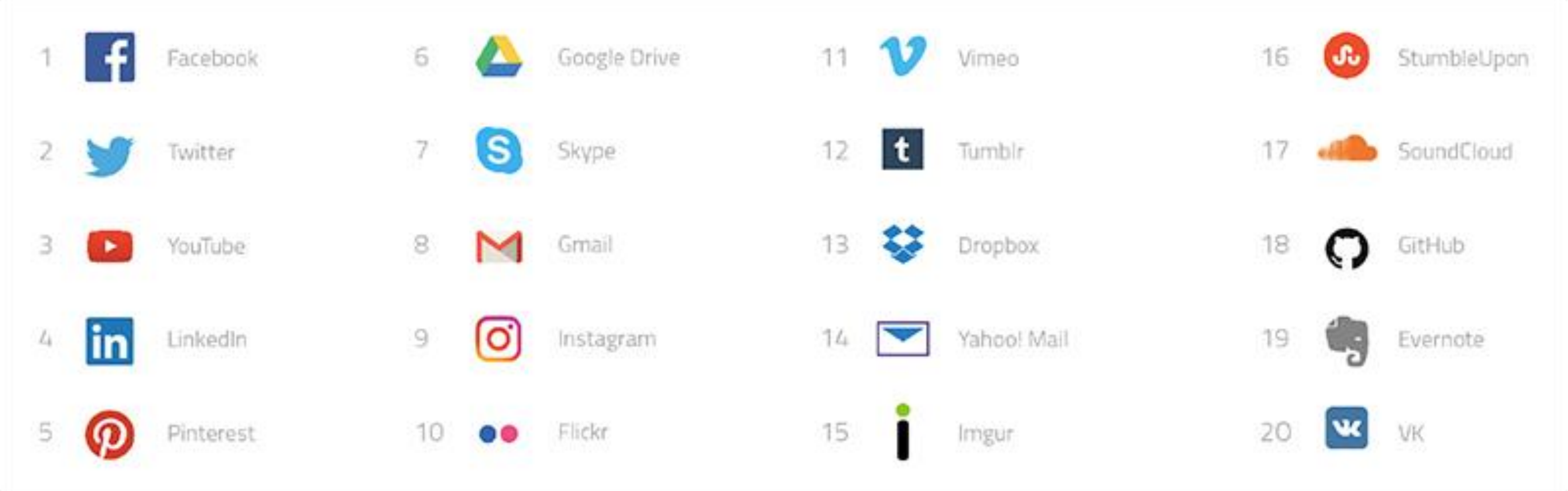
CaaS - Communication as a Service

DaaS - Data as a service

XaaS - Anything as a service

Top Cloud Providers

Who uses the Cloud?



1 Facebook
2 Twitter
3 YouTube
4 LinkedIn
5 Pinterest
6 Google Drive
7 Skype
8 Gmail
9 Instagram
10 Flickr
11 Vimeo
12 Tumblr
13 Dropbox
14 Yahoo! Mail
15 Imgur
16 StumbleUpon
17 SoundCloud
18 GitHub
19 Evernote
20 VK

So, what's the big deal with AWS?

-The AWS platform was launched in July 2002, but maybe you are just hearing of it now?

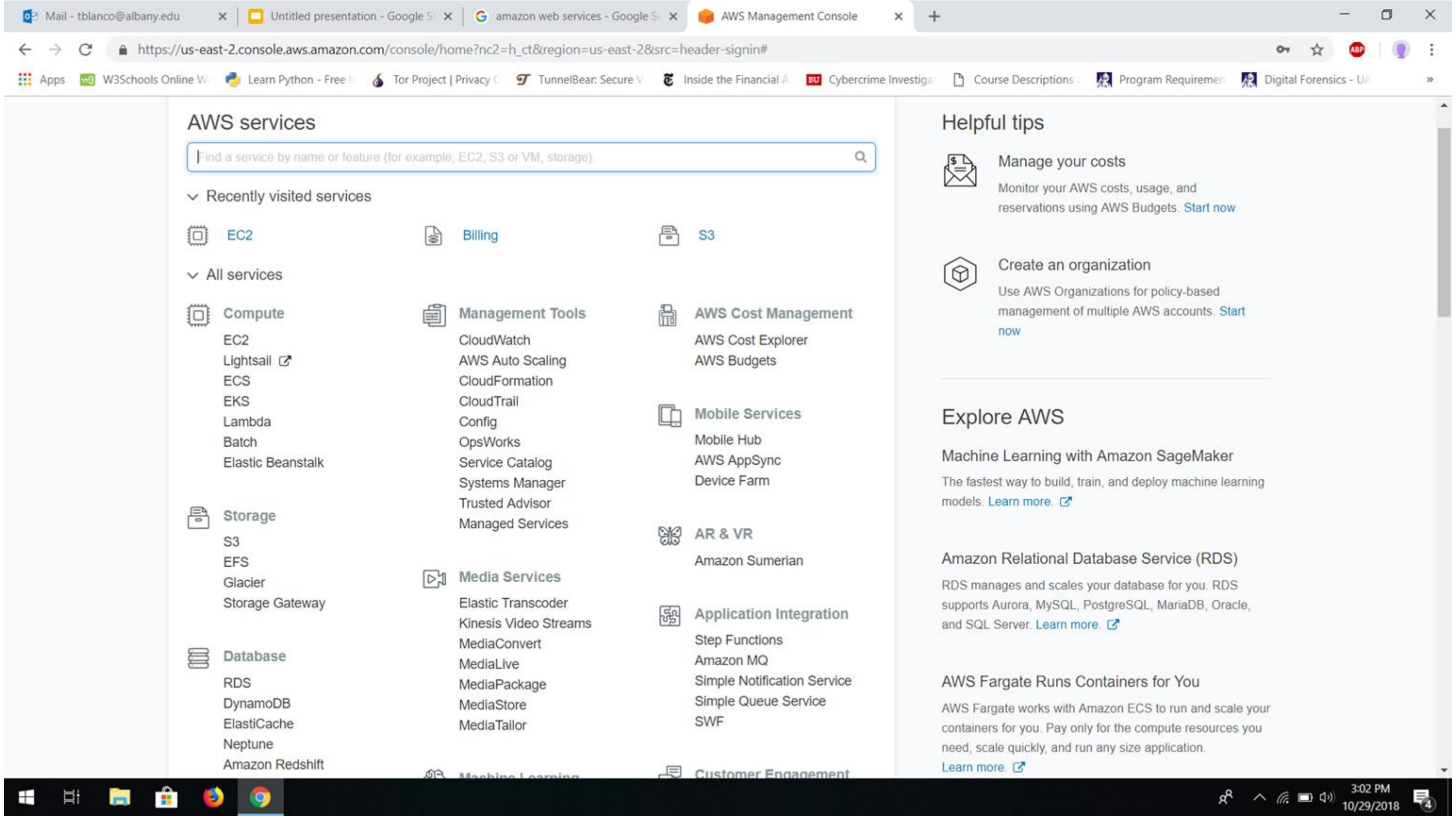
-Do you like Netflix?

- In regards to Security, the CIA offered 600 Million dollars to Amazon to create VPC's and host private network's for their data in July 2014.

- As of 2017, AWS owns a dominant 34% of all cloud (IaaS, PaaS) while the next three competitors Microsoft, Google, and IBM have 11%, 8%, 6% respectively according to Synergy Group

Questions?

AWS MANAGEMENT CONSOLE



AWS services

Find a service by name or feature (for example, EC2, S3 or VM, storage).

Recently visited services

EC2 Billing S3

All services

Compute
- EC2
- Lightsail
- ECS
- EKS
- Lambda
- Batch
- Elastic Beanstalk

Storage
- S3
- EFS
- Glacier
- Storage Gateway

Database
- RDS
- DynamoDB
- ElastiCache
- Neptune
- Amazon Redshift

Management Tools
- CloudWatch
- AWS Auto Scaling
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Systems Manager
- Trusted Advisor
- Managed Services

Media Services
- Elastic Transcoder
- Kinesis Video Streams
- MediaConvert
- MediaLive
- MediaPackage
- MediaStore
- MediaTailor

Machine Learning

AWS Cost Management
- AWS Cost Explorer
- AWS Budgets

Mobile Services
- Mobile Hub
- AWS AppSync
- Device Farm

AR & VR
- Amazon Sumerian

Application Integration
- Step Functions
- Amazon MQ
- Simple Notification Service
- Simple Queue Service
- SWF

Customer Engagement

Helpful tips

Manage your costs

Monitor your AWS costs, usage, and reservations using AWS Budgets. Start now

Create an organization

Use AWS Organizations for policy-based management of multiple AWS accounts. Start now

Explore AWS

Machine Learning with Amazon SageMaker

The fastest way to build, train, and deploy machine learning models. Learn more.

Amazon Relational Database Service (RDS)

RDS manages and scales your database for you. RDS supports Aurora, MySQL, PostgreSQL, MariaDB, Oracle, and SQL Server. Learn more.

AWS Fargate Runs Containers for You

AWS Fargate works with Amazon ECS to run and scale your containers for you. Pay only for the compute resources you need, scale quickly, and run any size application. Learn more.

Pentest Lab with EC2 Instances

KALI

vs

ubuntu®

IAM (Work-Place Scenario)

AWS GuardDuty

AWS CloudTrail

Event Logger

Type	Date	Time	Source
Info	6/16/2016	8:34 pm	.NET runtime
Info	6/16/2016	8:25 pm	Office 2016
Error	6/16/2016	7:30 pm	Office 2016
Info	6/15/2016	6:44 pm	Office 2016
Error	6/15/2016	4:35 pm	Application Hang
Info	6/15/2016	4:20 pm	MSiInstaller
Info	6/15/2016	4:03 pm	Application Hang

What did we cover?

❖ Amazon EC2 (Launching AMI’s and Working with Security Groups, Creating a virtual penetration testing lab utilizing Kali Linux AMI & Ubuntu Custom AMI, Explaining Key Pairs)

❖ IAM (Creating Policies, Users, Groups, Logging in with Alias/Link)

❖ Amazon GuardDuty (Analyzing Sample Entries, Severity rating and understanding metadata of threats)

❖ CloudTrail (Auditing and analyzing logs)

Cya Next week!

Thank you for participating in our workshops

Follow us on Twitter? Add on myInvolvement?

Join our Discord Group?

End of the semester Pizza Party, 3:00pm Next Friday (12/7)