UNIK4750 - Measurable Security for the Internet of Things

L17 – IDS and Cloud Security

György Kálmán,
DNB/UiO ITS
gyorgy.kalman@its.uio.no

Josef Noll
UiO ITS
josef.noll@its.uio.no

UNIK4750: Lecture plan

- 18.01 L1: Introduction
- 25.01
  - L2: Internet of Things
  - L3: Security of IoT + Paper list
- 01.02 --- No lecture because of sickness
- 08.02
  - L4: Smart Grid, Automatic Meter Readings
  - L5: Service implications on functional requirements
- 15.02
  - L6: Technology mapping
  - L7: Practical implementation of ontologies
- 22.02 --- Winter holiday
- 01.03
  - L8-9: Paper analysis with 15 min presentation
  - L10 if presentations do not fill the day
- 08.03 --- Held by Josef Noll
  - L11: Multi-Metrics method for measurable security
  - L12: Weighting in Multi-Metrics Method
- 15.03
  - L13: Guest Lecture, Mohammad Chowdhury from ABB
  - Paper analysis with 15 min presentation – continued
  - L14: System Security and Privacy analysis
- **22.03**
  - **L17: IDS and Cloud security**
  - **L18: Wrap-up of the course**
- 29.03 --- Easter holiday
- 05.04 ---- No lecture, consultation possibility
- 12.04
  - L15: Real world IoT service evaluation group work
  - L16: Real world IoT service evaluation group work
- 19.04 ---- No lecture, consultation possibility
- 27.04 ---- Exam ! This is a Friday!

Intrusion Detection and Prevention

- What is an Intrusion Detection System
- Flavours of IDS
- Industrial case
  - Comparison to generic cases
  - Physical process and safety
- Industrial examples
- Conclusion

Definitions – as requested – both definitions by ISACA

- Information security: "Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)
- Privacy: The rights of an individual to trust that others will appropriately and respectfully use, store, share and dispose of his/her associated personal and sensitive information within the context, and according to the purposes, for which it was collected or derived

- I think, both security and privacy is easier to see from the other way around:
- Losing security and privacy.

- If you loose information security: then you loose confidentiality of important data or the possibility to check its integrity or just can't access it.
- Same with privacy: if you loose it, then you can not control any more what is happening with private information

What is an Intrusion Detection System

- This is a practical example on fuzzy evaluation of different criteria and taking decisions by evaluating multi-dimension problems
- What is an intrusion: an attempt to break or misuse the system
- Might be internal or external source and can be physical, system or remote
- It is typically a set of entities distributed in the network and monitoring some network parameters

How an intrusion works

- Exploit different programming errors (e.g.: buffer overflow, no input validation)
- Unexpected input (e.g.: tamper with TCP checksum, fragmentation)
- Combination with creating special circumstances
- IDS need a baseline to work properly
- Baseline creation very much depends on the use
- We always assume, that they who attack behave differently

IDS flavours

- IDS can be based on:
  - Anomaly detection (heuristics) – challenge is good training and right set of sensitivity
  - Signature-based – challenge is to deal with new attacks
  - Typically we use a combination
- Or by location:
  - Host-based: the host os or application is running the logging, no additional hardware
  - Network-based: filters traffic, independent of clients

IDS in industrial environments

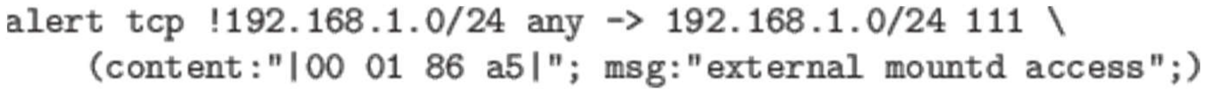
- Two important factors: much more clean traffic baseline is possible and relation to physical process and safety
- We can’t design a system to be secure forever – count with failure: fail-safe, fail-operational, graceful state changes
- Tamper detection and evidence
- The only difference between systems that can fail and systems that cannot possibly fail is that, when the latter actually fail, they fail in a totally devastating and unforeseen manner that is usually also impossible to repair(1)
- In an industrial environment the assumption that attackers will behave differently is not necessarely true

IDS in industrial environments

- IDS is a system: evaluation of logs, evaluation of network traffic, maintenance on firewall and IDS infrastructure (software+taps)
- Getting a reaction is actually easier in the industrial environment: typical to have 24 hours staffing somewhere, also physical security and safety
- Challenges with shared infrastructure and suppliers
- Possible approach: whitelisting, stateful payload analysis (operational envelope)

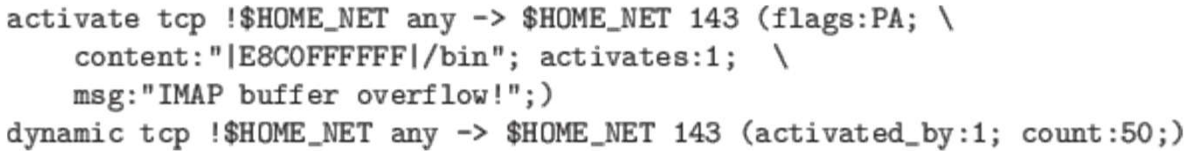
Example rules

- There are different ways, but take this snort rule as an example:



```
alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111 \
    (content:"|00 01 86 a5|"; msg:"external mountd access";)
```

- Dynamic rule example (both examples are from the snort manual):



```
activate tcp !$HOME_NET any -> $HOME_NET 143 (flags:PA; \
    content:"|E8C0FFFFFF|/bin"; activates:1;  \
    msg:"IMAP buffer overflow!";)
dynamic tcp !$HOME_NET any -> $HOME_NET 143 (activated_by:1; count:50;)
```

Industrial attacks

- No difference here: injection, man-in-the-middle, replay etc.
- Long life, high utilization of equipment and legacy support open for more attacks then in an office case
- SCADA compared to DCS/PCS
- Resilience and restoration
- Because of the use of COTS products, you actually might use the very same exploits, like windows on HMI

Industrial examples, from ICS-CERT (6)

Davis-Besse Nuclear Power Plant [2003]

- The Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant
- Disabled a safety monitoring system for nearly five hours
- Power plant was protected by a firewall
- In 1998 the same plant was hit by a tornado (natural disaster)

Industrial examples, from ICS-CERT (6)

Maroochy Shire Sewage Spill [2000]

- First recorded instance of an intruder that “deliberately used a digital control system to attack public infrastructure”
- Software on his laptop identified him as “Pumping Station 4” and after suppressing alarms controlled 300 SCADA nodes
- Disgruntled engineer in Queensland, Australia sought to win the contract to clean up the very pollution he was causing
- He made 46 separate attacks, releasing hundreds of thousands of gallons (264,000) of raw sewage into public waterways

Industrial examples, from ICS-CERT (6)

CSX Train Signaling System [2003]

- Sobig virus blamed for shutting down train signaling systems throughout the east coast of the U.S.
- Virus infected Florida HQ shutting down signaling, dispatching, and other systems
- Long-distance trains were delayed between four and six hours

Conclusions on Intrusion Detection

- Intrusion Detection is an example, where a collection of parameters will serve as an input to a fuzzy system
- Industrial systems might be quite well suited for «sharp» heuristics
- The main difference is the physical process back (both plus and minus)
- Evaluation of the detection system is very much in line with the classification examples shown in previous lectures: one can define a set of metrics and analyise which level the system is can reach.

Cloud – Security – IoT

- What is cloud computing
- Delivery models and shared responsibility
- AWS in general
- AWS security functions
- IoT in AWS
- Recommended additional resources

What is cloud computing

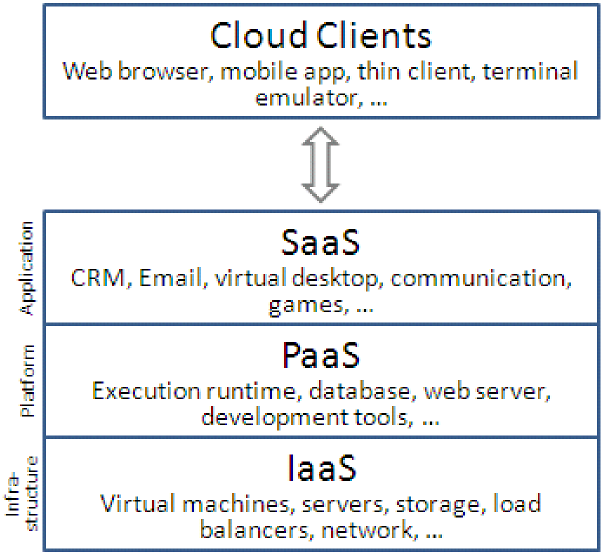
- A remote pool of (shared) resources on different levels
- Dynamic provisioning, elastic use of resources, pay-as-you-go
- A type of outsourcing

- Increased utilization of resources, economy of scale
- Multi-tenancy
- Global reach
- Flexible expense vs capital expense
- High availability
- Deployment: public, private, hybrid and community

Figure from https://www.slideshare.net/AmazonWebServices/awsome-day-nashville-2018training

Delivery models

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

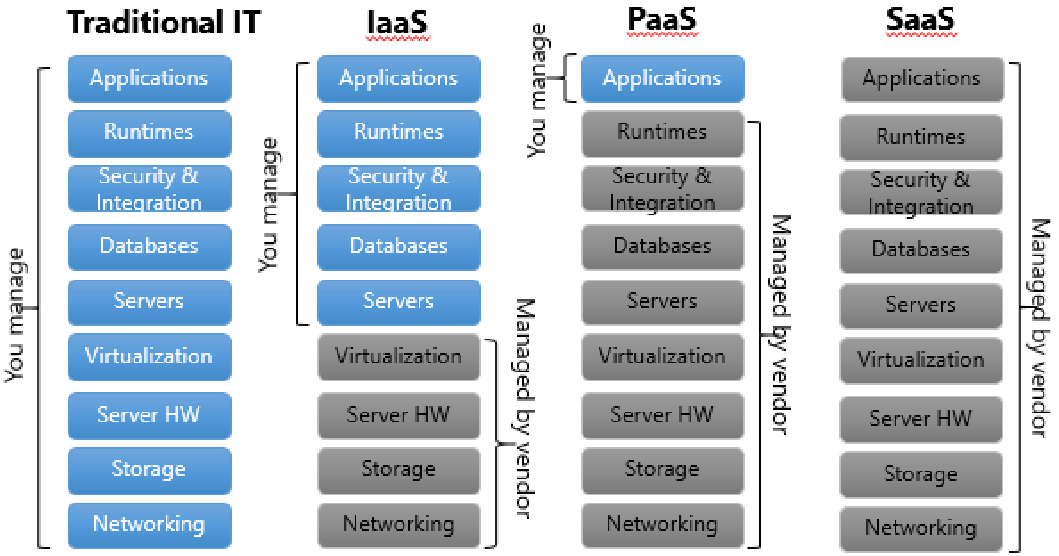


Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...

Application
SaaS
CRM, Email, virtual desktop, communication, games, ...

Platform
PaaS
Execution runtime, database, web server, development tools, ...

Infra-structure
IaaS
Virtual machines, servers, storage, load balancers, network, ...



Traditional IT
You manage
Applications
Runtimes
Security & Integration
Databases
Servers
Virtualization
Server HW
Storage
Networking

IaaS
You manage
Applications
Runtimes
Security & Integration
Databases
Servers
Managed by vendor
Virtualization
Server HW
Storage
Networking

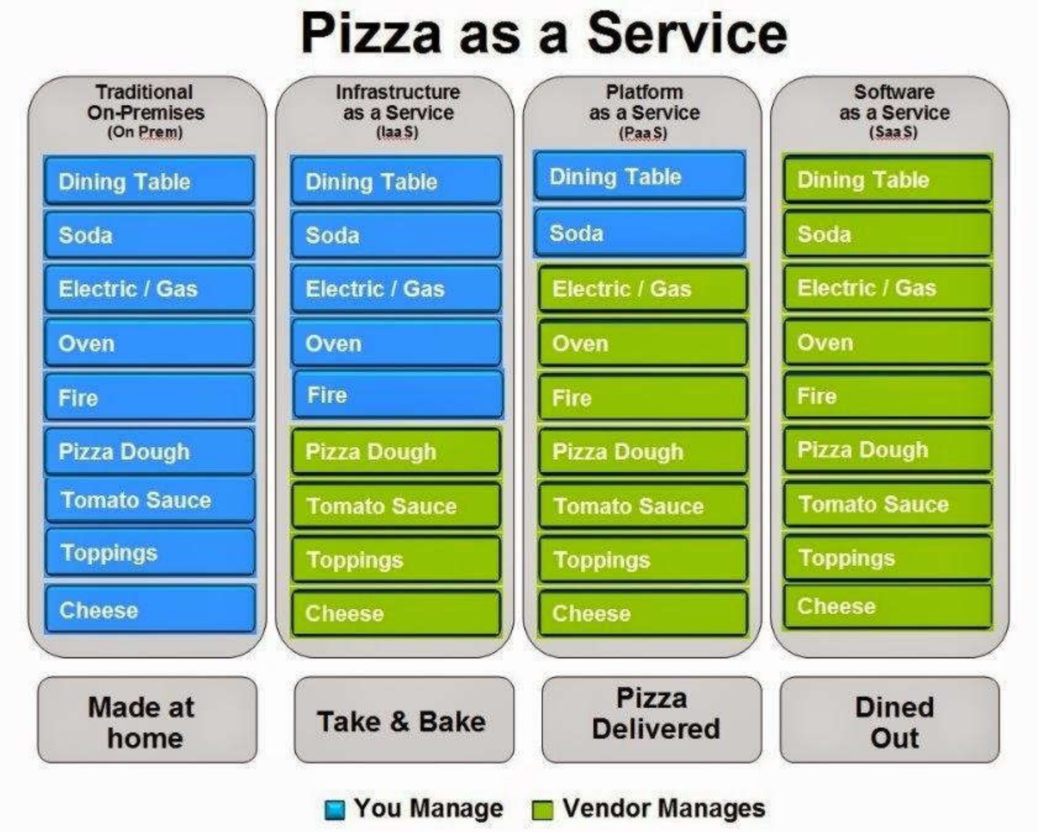
PaaS
You manage
Applications
Managed by vendor
Runtimes
Security & Integration
Databases
Servers
Virtualization
Server HW
Storage
Networking

SaaS
Managed by vendor
Applications
Runtimes
Security & Integration
Databases
Servers
Virtualization
Server HW
Storage
Networking

Both figures are from: http://oracle-help.com/oracle-cloud/cloud-computing-stack-saas-paas-iaas/

Delivery models contd.

- A perfect figure from Fred Bals at Episerver



Pizza as a Service

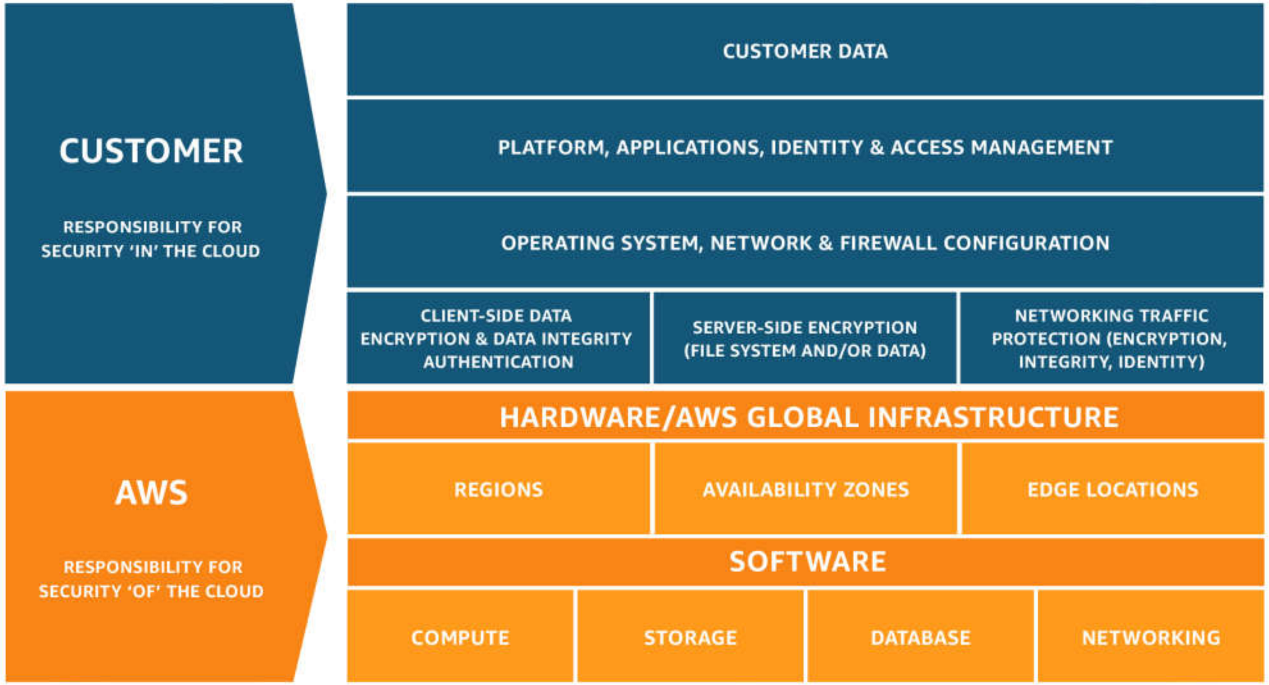
Traditional On-Premises (On Prem)	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
🟦 Dining Table	🟦 Dining Table	🟦 Dining Table	🟩 Dining Table
🟦 Soda	🟦 Soda	🟦 Soda	🟩 Soda
🟦 Electric / Gas	🟦 Electric / Gas	🟩 Electric / Gas	🟩 Electric / Gas
🟦 Oven	🟦 Oven	🟩 Oven	🟩 Oven
🟦 Fire	🟦 Fire	🟩 Fire	🟩 Fire
🟦 Pizza Dough	🟩 Pizza Dough	🟩 Pizza Dough	🟩 Pizza Dough
🟦 Tomato Sauce	🟩 Tomato Sauce	🟩 Tomato Sauce	🟩 Tomato Sauce
🟦 Toppings	🟩 Toppings	🟩 Toppings	🟩 Toppings
🟦 Cheese	🟩 Cheese	🟩 Cheese	🟩 Cheese
Made at home	Take & Bake	Pizza Delivered	Dined Out

🟦 You Manage 🟩 Vendor Manages

https://www.episerver.com/learn/resources/blog/fred-bals/pizza-as-a-service/

AWS Shared Responsibility Model

- AWS responsibility is to provide a reliable and secure infrastructure, where the customer services can be built on, a «foundation»
- Customer responsibility is determined by the services chosen
- Wide range of services
- And third party deliveries



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

SOFTWARE

COMPUTE

STORAGE

DATABASE

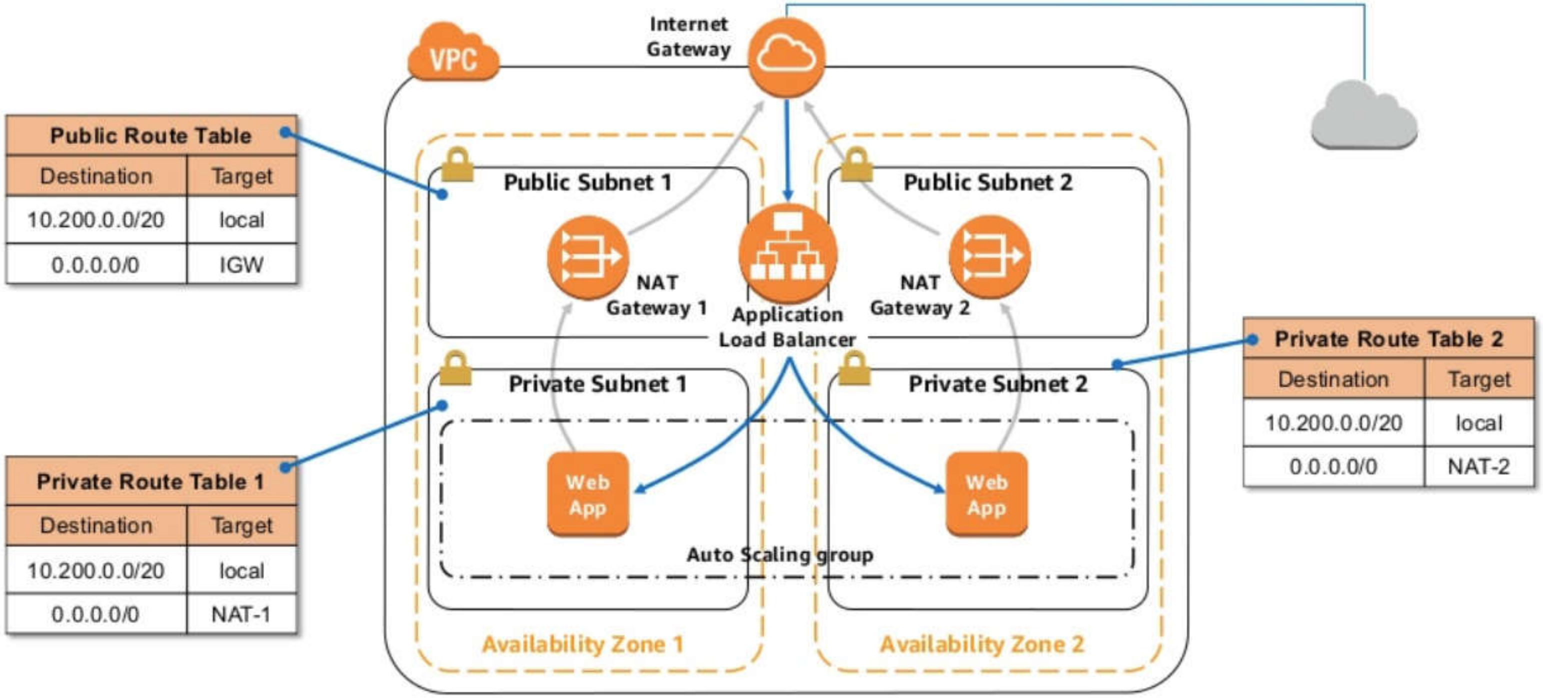
NETWORKING

https://aws.amazon.com/compliance/shared-responsibility-model/

Fundamentals

- Edge location
  - Border towards CloudFront, AWS' Content Delivery Network
  - Supports AWS DNS service (Route 53), WAF, Shield, Lambda@Edge
- Basic components
  - EC2
  - S3
  - VPC
- AWS Marketplace: a Play store for your cloud installation

Generic service architecture



Public Route Table

Destination	Target
10.200.0.0/20	local
0.0.0.0/0	IGW

Private Route Table 1

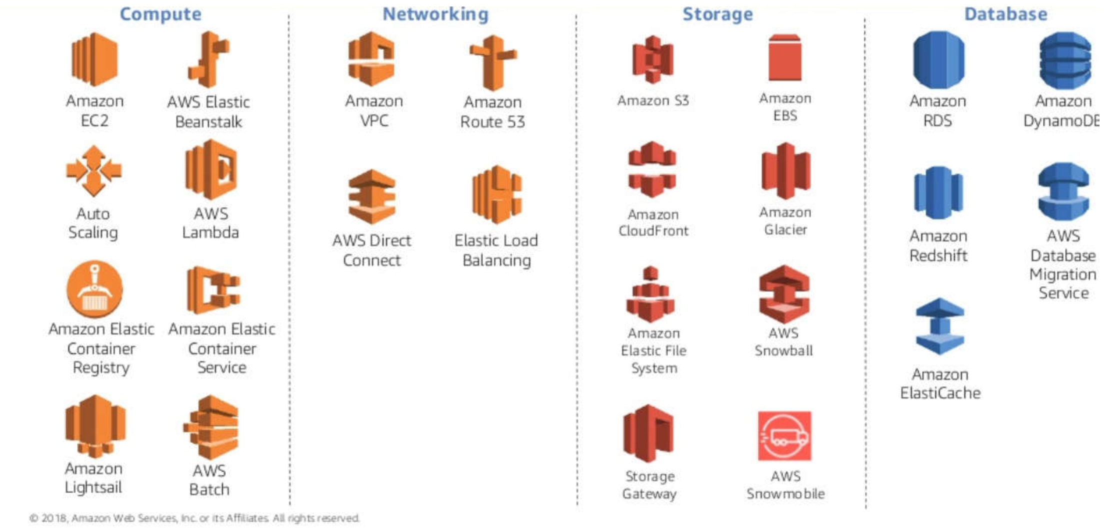
Destination	Target
10.200.0.0/20	local
0.0.0.0/0	NAT-1

Private Route Table 2

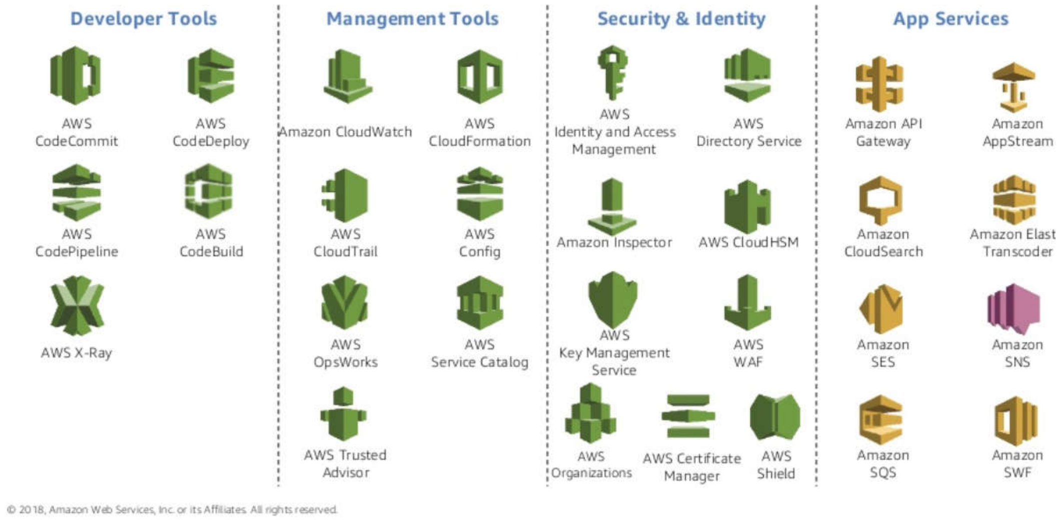
Destination	Target
10.200.0.0/20	local
0.0.0.0/0	NAT-2

AWS in a nutshell

- Launched in 2006, originally to utilize computing capacity investment for Christmas season
- More than 4000 features with around 1500 launched in ’17
- In Europe, Ireland is the main site and soon Sweden will also be an region



© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

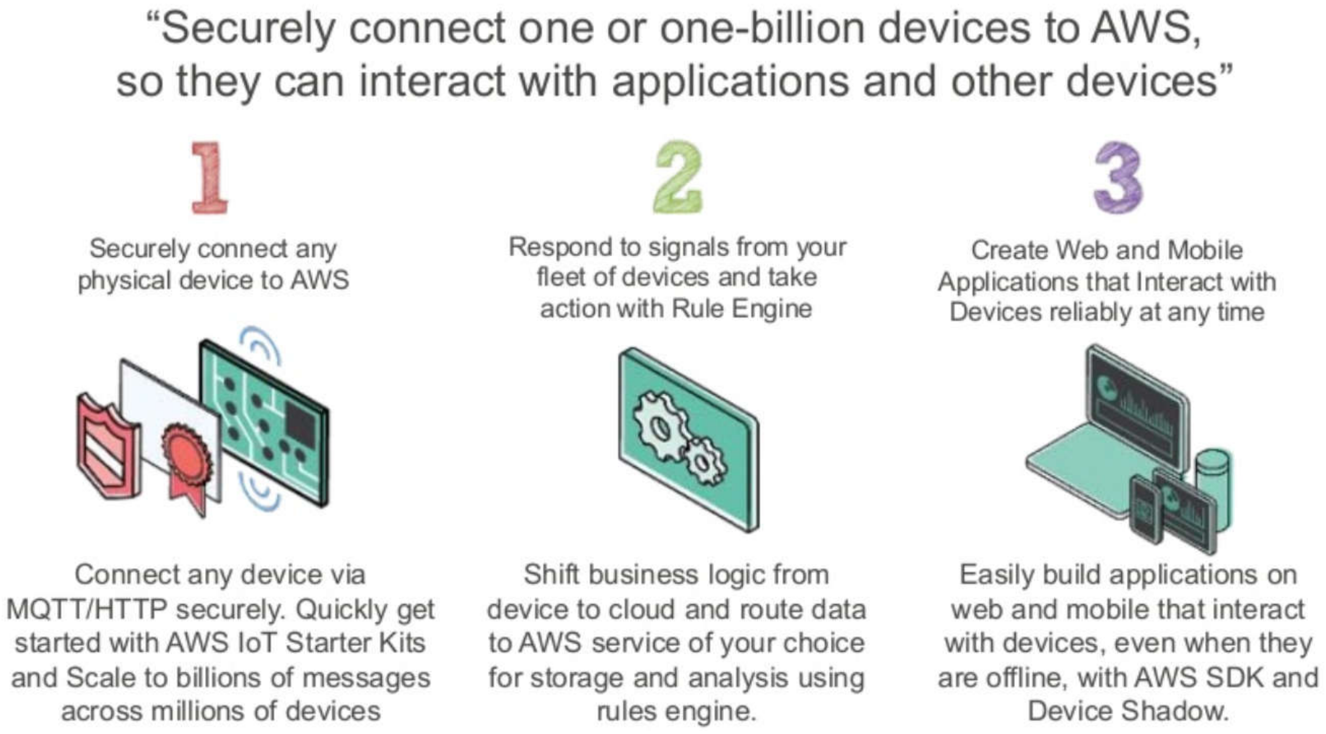
Based on https://www.slideshare.net/AmazonWebServices/awsome-day-nashville-2018training

AWS IoT

- In general: exploit the global reach, flexible infrastructure

- Larger operations are especially interesting: predictive maintenance, traffic management, logistics, demand estimation
- Provides infrastructure to get information from the edge and process it with AWS services.
- An interesting feature is the Rules engine, which can be queried with SQL-like expressions
- Higher-level services built on the acquired data (e.g. traffic stats -> prediction)
- Device Shadow, use Lambdas

Main steps in AWS IoT



“Securely connect one or one-billion devices to AWS, so they can interact with applications and other devices”

1

Securely connect any physical device to AWS

Connect any device via MQTT/HTTP securely. Quickly get started with AWS IoT Starter Kits and Scale to billions of messages across millions of devices

2

Respond to signals from your fleet of devices and take action with Rule Engine

Shift business logic from device to cloud and route data to AWS service of your choice for storage and analysis using rules engine.

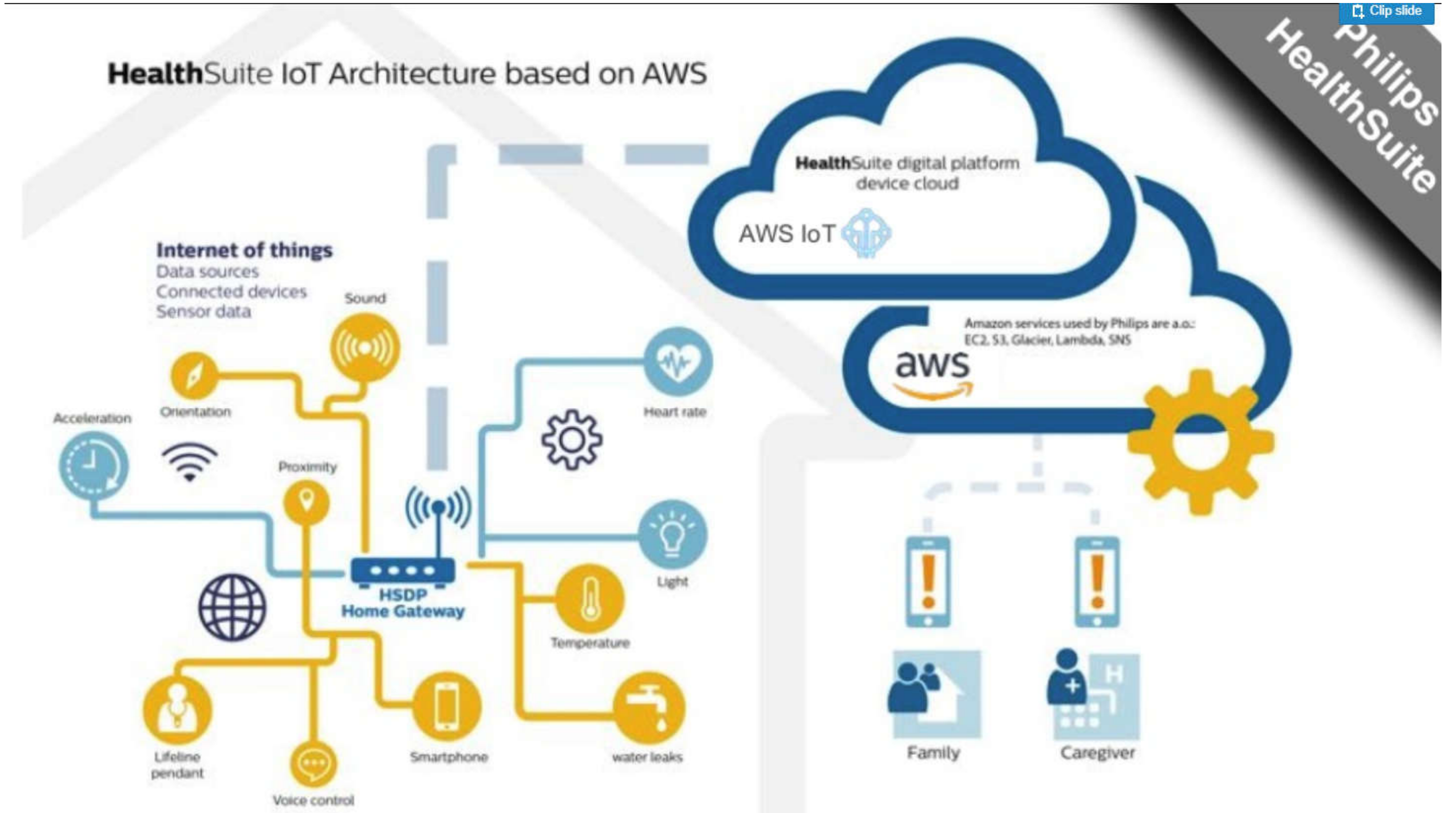
3

Create Web and Mobile Applications that Interact with Devices reliably at any time

Easily build applications on web and mobile that interact with devices, even when they are offline, with AWS SDK and Device Shadow.

https://www.slideshare.net/AmazonWebServices/intro-to-aws-iot-80291679

Healthcare example



https://www.slideshare.net/AmazonWebServices/intro-to-aws-iot-80291679

AWS Greengrass

- Together with Amazon FreeRTOS: enable amazon IoT for a wider audience
- Offline operation with Lambda and device shadow support
- Local processing and reaction possiblity → QoS, criticality!

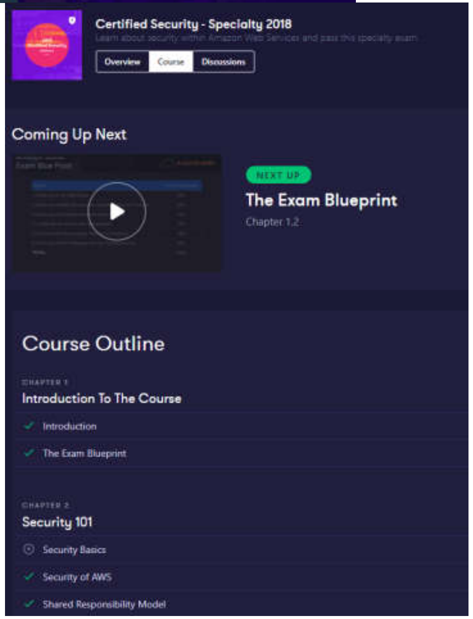
Additional resources

- ReInvent talk IOT201: The IoT Offering Explained in Plain English
- https://www.youtube.com/watch?v=A2BgY5VC4YI
- ReInvent talk IOT212: Amazon FreeRTOS
- https://www.youtube.com/watch?v=PerMQkl1QkE

Additional resources

TEACHING THE WORLD TO CLOUD

Join the 500,000+ engineers that have taken courses with A Cloud Guru.



Certified Security - Specialty 2018

Learn about security within Amazon Web Services and pass this specialty exam

Coming Up Next

The Exam Blueprint

Chapter 1.2

Course Outline

CHAPTER 1

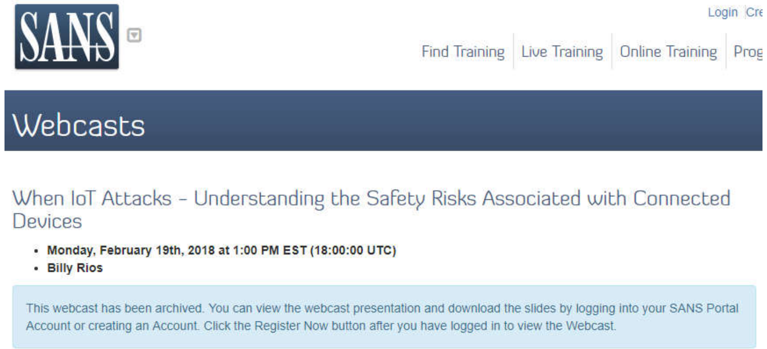
Introduction To The Course

- ✓ Introduction
- ✓ The Exam Blueprint

CHAPTER 2

Security 101

- Security Basics
- ✓ Security of AWS
- ✓ Shared Responsibility Model



Webcasts

When IoT Attacks - Understanding the Safety Risks Associated with Connected Devices

- Monday, February 19th, 2018 at 1:00 PM EST (18:00:00 UTC)
- Billy Rios

This webcast has been archived. You can view the webcast presentation and download the slides by logging into your SANS Portal Account or creating an Account. Click the Register Now button after you have logged in to view the Webcast.

https://www.sans.org/webcasts/106325?utm_medium=Social&utm_source=Twitter&utm_content=webcast+registration&utm_campaign=ICS+Webcasts

https://acloud.guru/course/aws-certified-security-specialty/dashboard

https://www.slideshare.net/AmazonWebServices/awsome-day-nashville-2018training

References - Classification

- Cybersecurity classes: http://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf
- IAEA: Computer Security at Nuclear Facilities: http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf
- Red Tiger Security: mapping security controls to standards: http://redtigersecurity.com/services/scadaics-security-consulting/scada-security-maturity-model/
- Standards for Security Categorization of Federal Information and Information Systems, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

References – Intrusion Detection

1. https://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Zanero.pdf
2. http://www.digitalbond.com/tools/quickdraw/
3. https://www.sans.org/reading-room/whitepapers/ICS/challenges-ids-ips-deployment-industrial-control-systems-36127
4. http://commons.erau.edu/cgi/viewcontent.cgi?article=1071&context=discovery-day
5. https://www.truststc.org/conferences/10/CPSWeek/papers/scs1_paper_8.pdf