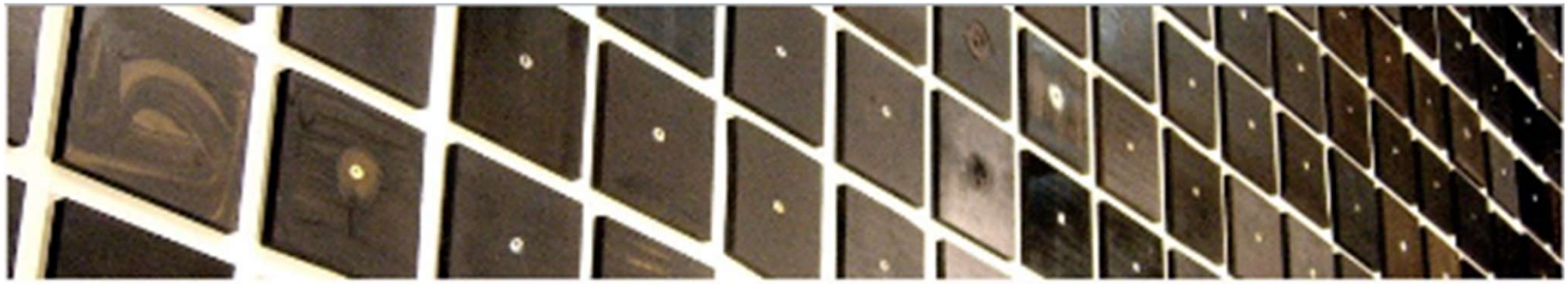


UiO : Universitetet i Oslo

TEK5370

Security, IoT and cloud

Shujun Zhang · 2nd
Associate Professor at Western Norway University of Applied Sciences,Høgskulen på Vestlandet (HVL)
Bergen, Hordaland, Norway · 500+ connections · Contact info

Josef Noll
Secretary General at the Basic Internet Foundation, Professor at the University of Oslo
Oslo Area, Norway · 500+ connections · Contact info

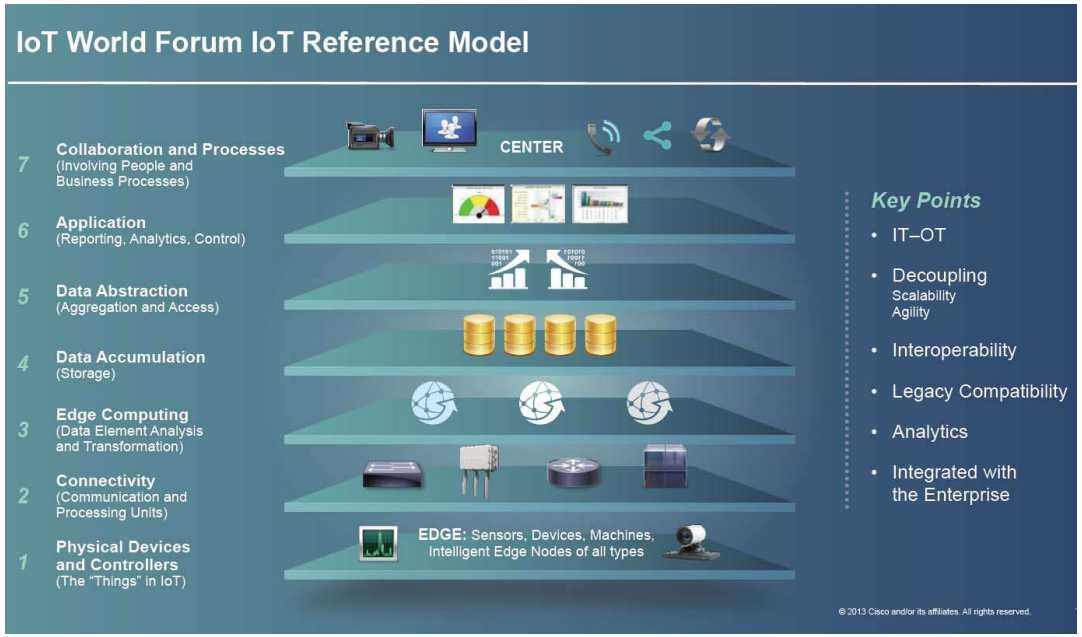
György Kálmán, Ph.D., CISM, CCSP
Vice President - Security Architecture Quality Assurance at Morgan Stanley
Budapest, Budapest, Hungary · 500+ connections · Contact info

Agenda

- Introduction to IT security
- Industrial IT and IoT security landscape
- IoT and cloud-related challenges
- Example incidents and vulnerabilities
- Introduction to cloud
- Cloud security fundamentals and IoT through the example of AWS

IoT, cloud, automation

- Heading toward a fully connected world, including most aspects of everyday life
- The substantial difference is, that these systems have a physical dimension
- Automation to a new connectivity level – the internet is coming to automation and home services
- Main challenges: how to join the physical and the logical world, how to achieve interoperability in a heterogeneous and conservative industry?
- How to secure services with long value chains?
- How to implement and keep configs secure?



Internet architecture fundaments

- Intelligence in the end nodes – this enables easier scaling – where to put the «end node»
- Best effort traffic – perfect for content delivery towards humans or other async traffic
- Infrastructure = network equipment, intelligence/processing in end nodes

- QoS: best effort, adopted to the human consumer: 10s of ms of drop is not a problem, stable delay is accepted, majority of applications are bursty, reaction time in 0.5-1s range
- Stochastic – resource allocation expect that only a fraction of users are active at a given timeslot

Internet of Things and automation type of applications

- Centralized intelligence – here, as with the end node, the choice of abstraction level is important
- Automation is traditionally operated independently as an island
- Direct connection with the physical world
- Is made for information gathering and processing by machines
- Economic press leads to adoption of internet-based services which *require* a paradigm change
- Additional field of interest is home automation, where heterogenous setups, privacy issues and security/configuration questions arise

Mine (Boliden)

ABB robots

http://www07.abb.com/images/librariesprovider104/Extended-Automation/control-room-consolidation-by-abb.png?sfvrsn=1

IoT

- «best of both worlds»: security threats of the internet world meet the security challenges of the automation industry, with exceptions
  - Billions of connected devices
  - Secure and insecure locations
  - Security may or may not be built in
  - Life cycle mismatch between IT and automation devices
  - Installed base
  - Clash between IT and OT, IT has to accept the traffic
- IoT is not necessarily something big: an IP camera, smart thermostat, door opener, remote controlled power outlet, all is part of the IoT.

IT Security intro

- What is security and why do we need it?
  - Technical and other controls to protect your information and other assets
- Where you meet with security controls?
  - Password policies, username policies, spam settings, the little padlock in your browser
- Why do we have these in place and how they relate to an IoT/automation scenario?
  - Think about the typical tip of disconnecting the device which you suspect is hacked: how would this work in an IoT/automation case?

CIA – Confidentiality, Integrity, Availability

- **Confidentiality:** ensures, that information remains confidential, only those, who should access information, can do it.
- **Integrity:** no one should be able to alter information without detection.
- **Availability:** information is available when needed
- **Balance between CIA:**
- **Confidentialy preferred:** disconnect – attacker wins if DoS was the goal, availability lost
- **Availability preferred:** proceed with operation even if integrity/confidentiality suffers

CIA – Confidentiality, Integrity, Availability

- **Confidentiality:** encryption, access control, physical security
- **Integrity:** encryption, checksum, hashing, signature, logs, audit trail
- **Availability:** firewall, load balancing, graceful degradation, out-of-band management, backup, redundancy

IT Security fields

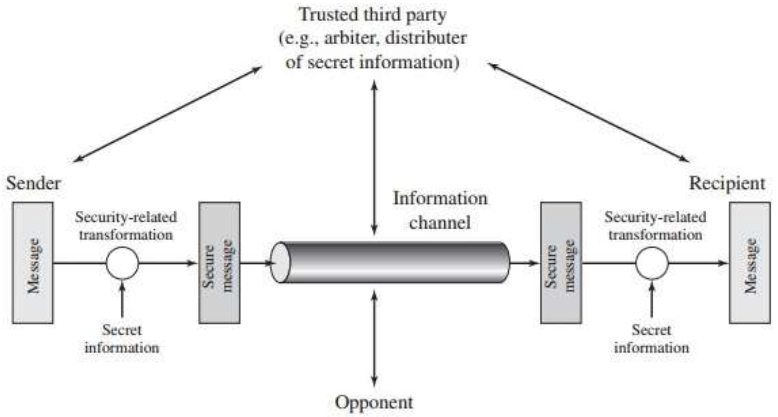
- Network security
  - Typically the first one we think about when talking IT sec: channel encryption, access control, authentication
- Internet security
  - Things around internet activity, e.g. the browsers. Firewalls, unified threat management
- Endpoint security
  - Device level protection, includes all the endpoints like tablets, sensors, laptops, phones. Network access, isolation, self-checks
- Application security
  - Secure coding, management of libraries, check for typical errors, peer-review

Typical security threats

- Intrusion: some entity trying to get access to systems to reach some goal
- Virus&similar threats: some malicious code with the aim of typically destroy information, exfiltrate information or grant access to attackers to the system
- Spyware: more recent than the previous two, mostly just listening and sending out data
- Phishing: aimed towards the user, using typically fake emails or fake websites to get information and use it in e.g. economid fraud or identity theft
- Spam: no typical primary damage, mass sent email or other messages. Can carry or can help phishing attacks or help deploy virus/spyware
- Ransomware: special emphasis on this category since the widespread use of crypto-currencies

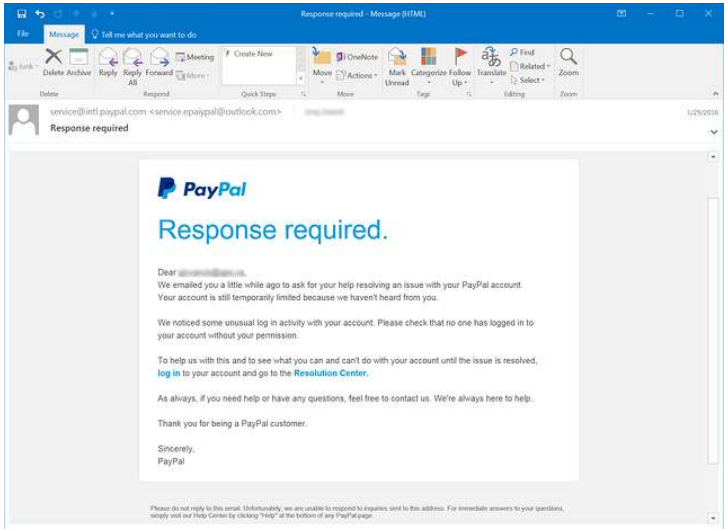
Network Security

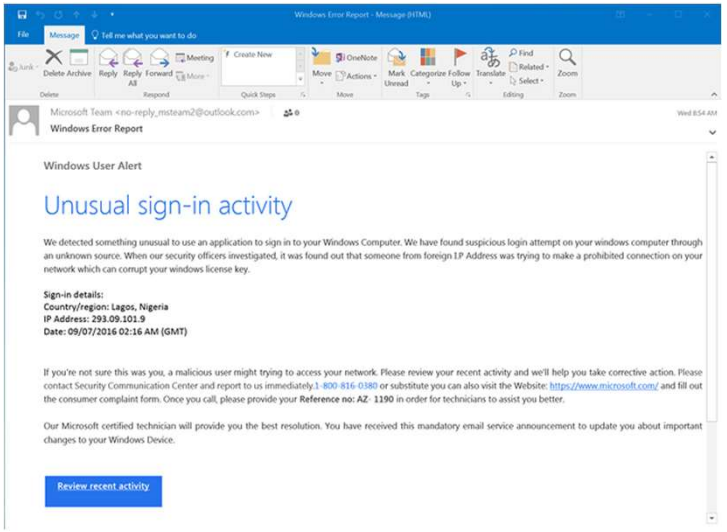
- Example on communication security
- Normal flow has no additional controls, end nodes and channel «trusted»
- Possible attacks here:
  - Interruption: DoS, availability
  - Interception: Confidentiality, data exfiltration, private information, industrial espionage, replay attack
  - Modification: Integrity, somebody modifies data underway
  - Fabrication: masquerade, somebody creates data which looks like coming from sender



https://www.brainkart.com/article/A-Model-For-Network-Security_8384/

Phishing example

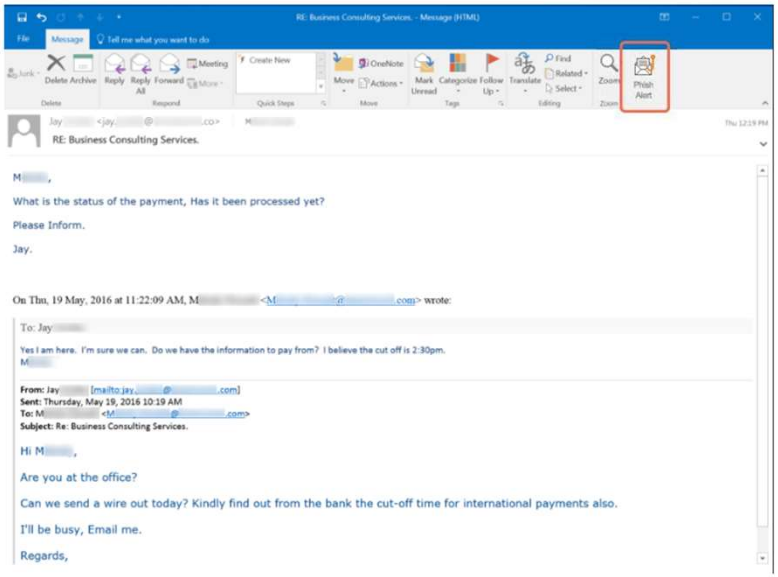




Can aim for e.g. important data directly or carry payload

https://www.phishing.org/phishing-examples

Phishing example – special emphasis in Norway



RE: Business Consulting Services.

M,

What is the status of the payment, Has it been processed yet?

Please Inform.

Jay.

On Thu, 19 May, 2016 at 11:22:09 AM, M <M .com> wrote:

To: Jay

Yes I am here. I'm sure we can. Do we have the information to pay from? I believe the cut off is 2:30pm.
M

From: Jay [mailto:jay. .com]
Sent: Thursday, May 19, 2016 10:19 AM
To: M <M .com>
Subject: Re: Business Consulting Services.

Hi M,

Are you at the office?

Can we send a wire out today? Kindly find out from the bank the cut-off time for international payments also.

I'll be busy, Email me.

Regards,

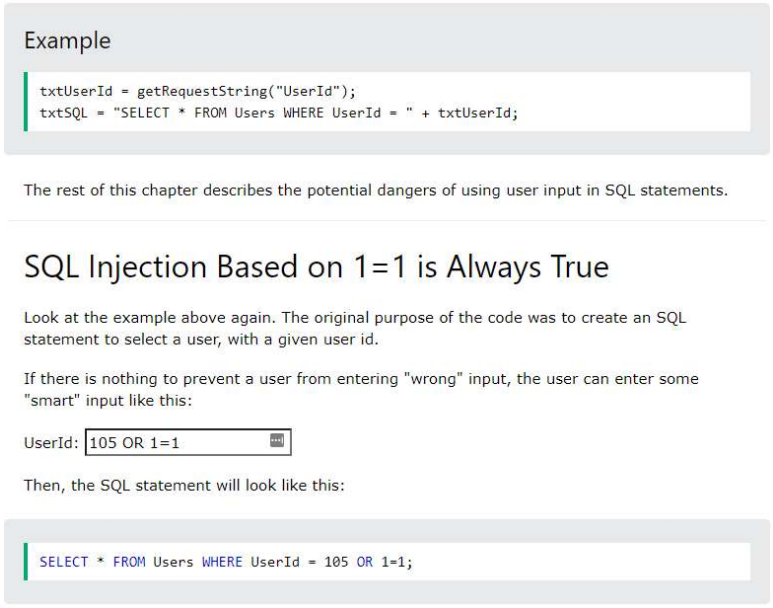
CEO fraud exploits trust in the society
https://www.phishing.org/phishing-examples

https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/varsler-fra-ncsc/sentralt-ansatte-i-hoyteknologiske-norske-bedrifter-mal-for-e-postsvindel

https://norsis.no/download/20115/

https://nsm.no/aktuelt/risiko-2021-helhetlig-sikring-mot-sammensatte-trusler

SQL injection example



Example

```
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
```

The rest of this chapter describes the potential dangers of using user input in SQL statements.

SQL Injection Based on 1=1 is Always True

Look at the example above again. The original purpose of the code was to create an SQL statement to select a user, with a given user id.

If there is nothing to prevent a user from entering "wrong" input, the user can enter some "smart" input like this:

UserId: 105 OR 1=1

Then, the SQL statement will look like this:

```
SELECT * FROM Users WHERE UserId = 105 OR 1=1;
```

- From https://www.w3schools.com/sql/sql_injection.asp
- The SQL above is valid and will return ALL rows from the "Users" table, since **OR 1=1** is always TRUE.

HTTP basic authentication

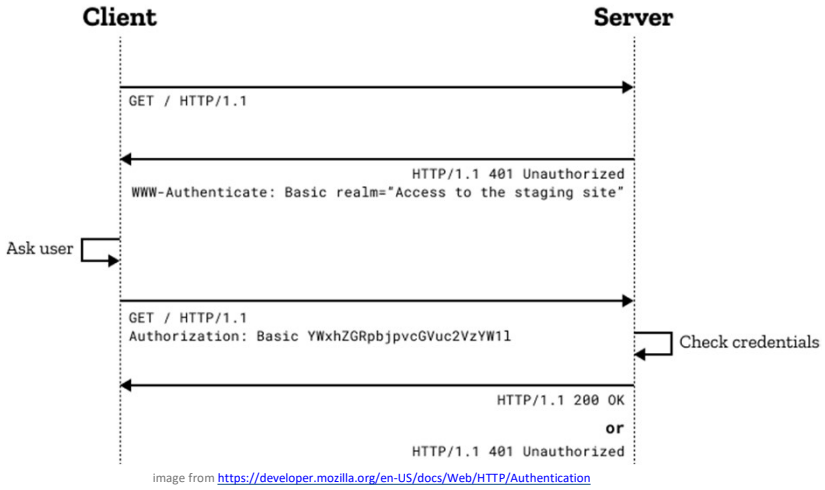
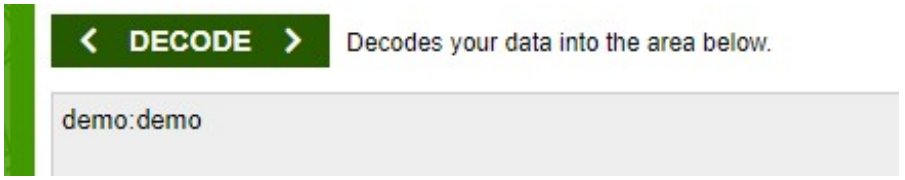


image from https://developer.mozilla.org/en-US/docs/Web/HTTP/Authentication

- Basic authentication is communicating using an encoding and not an encryption to hide credentials from trivial reading
- Base64 is used.
- A Base64 encoded string looks like this: ZGVtbzpkZW1v
- Paste into any Base 64 decoder, e.g. https://www.base64decode.org/:



IoT and automation scenarios

- Smart home
- Rail operations: passenger security, route optimization, maintenance
- Smart city: efficient city services, parking, lights, traffic signals
- Self-driving car: online services, connected sensors, traffic engineering

Selected incidents

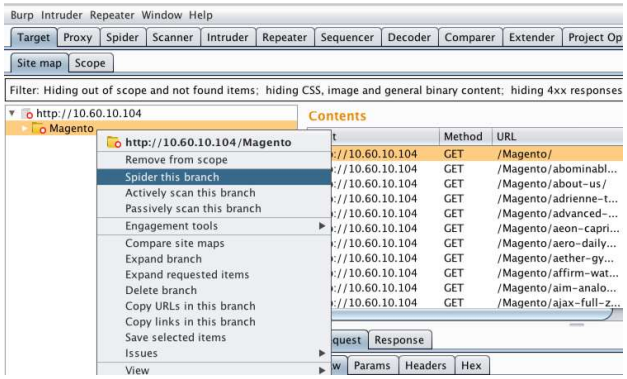
- Ukraine blackout
- Ransomware e.g. https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/ (LockerGoga) or Mondelez in 2017 (NotPetya)
- Spike botnet: DDoS attacks, ARM platform, infected devices included routers, smart thermostats, dryers, freezers, raspberry pi appliances.
- Mirai botnet: cameras (http://www.welivesecurity.com/2016/10/24/webcam-firm-recalls-hackable-devices-mighty-mirai-botnet-attack/)
- Meris botnet: https://krebsonsecurity.com/2021/09/krebsonsecurity-hit-by-huge-new-iot-botnet-meris/ attack against Yandex and Cloudflare

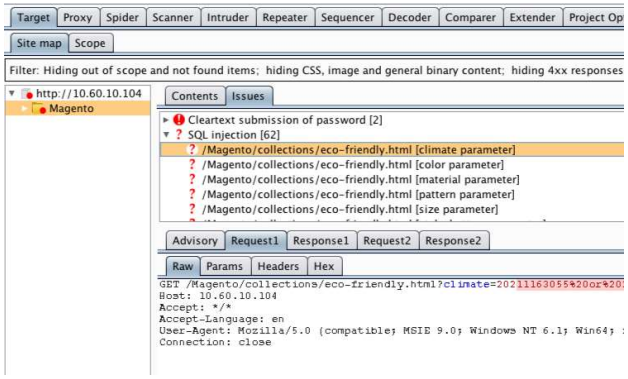
Threat landscape

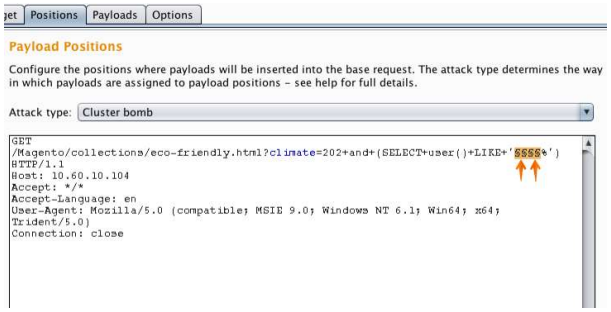
- Vectors:
  - Physical access (e.g. USB drive – Stuxnet)
  - Authenticated attacks
  - Unauthenticated attacks
  - Trivial access – http Basic Auth or scan
- Types of attackers
  - Hack – typically exploits vulnerability in the system (might be trivial)
  - System analysis – side channel attacks, analysis of the running environment and runtime
  - Lab-based attack – highly skilled attacker supported with special equipment
  - Inside job
- Types of attacks
  - DDoS, botnet, malware, perimeter weakening, data breach, just for fun
- Defense:Tamper resistance, monitoring

Local proxy

- Good example is Burp by PortSwigger, a widely used tool for security testing







https://portswigger.net/blog/using-burp-suite-to-audit-and-exploit-an-ecommerce-application

Security challenges

- IoT introduces a dramatically larger attack surface
- Wide range of technologies involved:
  - Sensors: AV, positioning, acceleration, temperature, proximity
  - Communication: cellular, wireless, wired, light
  - Identification: rfid, barcodes, tags, biometry
  - Localization: gps, indoor solutions
- From closed networks to cloud computing:
  - Security solutions should not build on and depend on the network technology (heterogeneous infrastructure)
- Cost of security:
  - Possible mismatch between the value of the device and the data handled
- Misconception: device focus. IoT has many attack surfaces, each of these shall be evaluated.
- All elements of the system have to be considered:
  - End devices, cloud infrastructure, the application, network intefaces, software environment, use of crypto
- Public acceptance of IoT depends on security of the systems

Security analysis

- It's not about the device. One shall see the big picture

- Structured approach with well-known steps: e.g. securing a web interface, analysis and setup of protocol parameters (avoid fallback to weak crypto), analysis of data to select correct protection
- Insecure network services: unfortunately, typical for industrial applications
- Transport encryption: use appropriate technological solutions
- Cloud interface
- Mobile interface
- Appropriate granularity in security configuration: e.g. monitoring, logging, password and lockout parameters
- Insecure software
- Physical security

Security needs of IoT

- User identification
- Identity management
- Tamper resistance
- Secure storage
- Secure content
- Secure software execution
- Secure communication
  - Over-the-air updates
- Secure network access

- Gateway as a key customer component: edge device for the LAN, concentrator

The CIS top 20 critical controls

1. Inventory of authorized and unauthorized hardware.
2. Inventory of authorized and unauthorized software.
3. Secure Configurations for Hardware and Software For Which Such Configurations Are Available.
4. Continous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance and Analysis of Complete Security Audit Logs
7. E-mail, web and other online service protection
8. Malware Defenses
9. Limitation and Control of Ports, Protocols and Services
10. Data Recovery Capability
11. Secure Configurations of Network Devices Such as Firewalls And Routers.
12. Boundary Defense
13. Data Protection
14. Controlled Access Based On Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Training To Fill Gaps
18. Application Software Security
19. Incident Response Capability
20. Penetration tests and Red Team Exercises

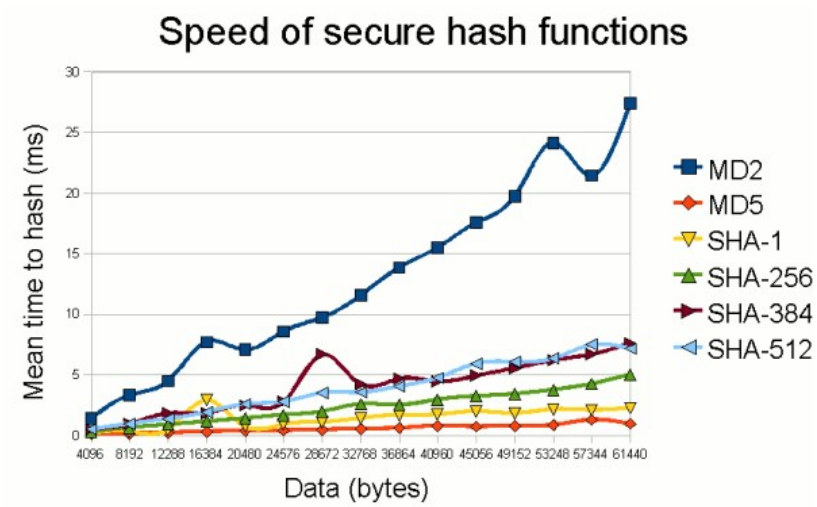
IoT and cloud-related challenges

- CIA balance
- AMS attack surface
- Exploiting cloud-elasticity
- Smart home – Always online
- Autonomous vehicles
- Unauthorized resource usage (e.g. mining)
- Privacy: many of the devices require e.g. to use a Google account for setup
- Lack of resources amongst other factors may lead to weak password policies
- Confidentiality: using no security is the widest adapted method
- Outdated solutions: UI is poorly implemented and is prone to vulnerabilities found several years ago

Resource constraints

- Required strength security/integrity protection depends on the data protected – classify with resurce need, typically cycle time
- This is a tradeoff between resource usage and importance/lifetime
- See hash example: delay vs security, in IoT a ms can be long time
- Some benchmark examples: https://www.wolfssl.com/docs/benchmarks/

MD5 25 kB took 0.003 seconds, 8.138 MB/s
POLY1305 25 kB took 0.004 seconds, 6.104 MB/s
SHA 25 kB took 0.006 seconds, 4.069 MB/s
SHA-256 25 kB took 0.014 seconds, 1.744 MB/s
SHA-512 25 kB took 0.042 seconds, 0.581 MB/s



http://www.javamex.com/tutorials/cryptography/HashTime.png

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

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

An example – Secure gateway vulnerability

- **eWON Reference: Password visibility (https://ewon.biz/support/news/support/ewon-security-enhancement-7529-01)**
- **Affected devices:** eWON Flexy/CD
- **Affected versions:** All firmware versions
- **Impact/description:**
- It is possible to “sniff” passwords when the firmware website is accessed through standard non-secure HTTP.
- Furthermore the autocomplete feature integrated with the evergreen browsers might suggest in clear text previous passwords in the eWON User Setup creation/edition page.
- **Mitigating factors:**
- Connections to eWON devices should only be done through a point-to-point LAN, a secured LAN or a secured VPN. Sniffing is thus not a valid attack use case as it concerns closed work environment (limited connectivity) or secure environment.
- Regarding the second issue the internet browser is supposed to be manipulated by the eWON administrator only as the page that leaks passwords requires configuration management right.
- **Solution / Advice:**
- Always connect to eWON using a closed work environment (limited connectivity) using a point-to-point LAN, a secured LAN or a secured VPN (for instance using Talk2M).
- Since eWON firmware version 10.1s0 we disable password fields auto completion.

An example – glibc vulnerability affecting ICS

- Embedded devices also use code from other IT systems
- Vulnerabilities can be valid across platforms

Technical FAQs

Question	Moxa Statement on "GHOST" Vulnerability (CVE-2015-0235)
Question Type	Other
Updated	6/1/2016 1:54:36 PM
Hits	1
Products	

Suggestions

Background and Impact
According to ICS-CERT, the "GHOST" vulnerability (CVE-2015-0235) in the "glibc" library could affect industrial systems. An authenticated local administrator could cause a denial of service of the targeted system by exploiting this vulnerability. ICS-CERT recommends the three following general defensive measures to protect against this and other cybersecurity risks:

"Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.

Locate control system networks and remote devices behind firewalls, and isolate them from the business network.

When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices."

Impacted Products
Some Moxa devices are impacted by the "GHOST" vulnerability. Refer to the table below for a list of impacted products.

Category	Industrial Ethernet	Serial Connectivity	Industrial Computing	Remote Automation	IP Surveillance
Impacted Products	EDR-810 Series EDR-G900 Series	W2X50A, W1 MGate 5101-PBM-MN MGate 5101-PBM-PN MGate 5101-MB-EIP	UC-8100 X86, IA240, IA3341, W315A, W325A, UC-7112 Plus, W311, W321, W341, W327, DA-661/662/663. UC-8430, UC-8481/8486, MAR-2000-LX, RNAS/FU, UC-7112 Plus, W315, W325, W345, IA241, DA-660, W406, IA261-I/IA262-I, IA260, EM-2260	ioPAC 8500 ioPAC 8600 ioPAC 5500	VPort 06-1MP Series VPort 16-1MP Series VPort 26A-1MP Series VPort 36-1MP Series VPort 56-2MP VPort 66-2MP VPort 36-2MP VPort 461A VPort 06-2MP

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

ICS-CERT selected alerts:

- ICS-ALERT-19-225-01 : Mitsubishi Electric Europe B.V. smartRTU and INEA ME-RTU (Update A)

--------- Begin Update A ---------

CISA is aware of a public report of vulnerabilities with proof-of-concept (PoC) exploit code affecting Mitsubishi Electric Europe B.V. smartRTU (Versions 2.02 and prior) and INEA ME-RTU (Versions 3.0 and prior), remote terminal unit products. According to this report, there are multiple vulnerabilities that could be exploited to gain remote code execution with root privileges. CISA has notified Mitsubishi Electric Europe B.V. of the report and has asked them to confirm the vulnerabilities and identify mitigations. CISA is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks.

--------- End Update A ---------

The report included vulnerability details and PoC exploit code for the following vulnerabilities:

Vulnerability Type	Exploitable Remotely	Impact
OS command injection	Yes	Possible remote code execution with admin privileges
Improper access control	Yes	Possible remote code execution with admin privileges
Stored cross-site scripting	Yes	Possible to run arbitrary code on the client target system
Hard-coded cryptographic keys	Yes	Possible unauthorized access/disclosure of encrypted data
Hard-coded credentials	Yes	Possible unauthorized access/execution of admin commands
Plaintext password storage	Yes	Possible disclosure of usernames and plaintext passwords
Incorrect default permissions	No	Possible disclosure of usernames and plaintext passwords by a logged in user

smartRTU

Remote Terminal Unit based Monitoring and Control

Communicate securely to SCADA systems, the smartRTU addresses requirements for 100 % reliable remote surveillance and control of distributed assets, even in extreme climates. With powerful functions like diagnostics, alarm and event-storage and time trend data buffering, it meets the challenges of managing massively distributed assets such as data security, interfacing issues, data continuity and reliable communications.

Mitsubishi Electric's meets these demands with the smartRTU. It supports protocols such as DNP3 and IEC 60870. The smart- RTU combines the reliability and robustness of our standard PLC technology with a smart communication gateway, the ME-RTU gateway. Depending on the size and complexity of the application, select the required smartRTU power, pairing the ME-RTU with either an FX-, L-, or Q-Series PLC.

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

Interesting resources in ICS security attacks:

- https://www.osti.gov/servlets/purl/1505628
- https://www.nist.gov/industry-impacts/industrial-control-systems-cybersecurity
- https://inl.gov/critical-infrastructure-protection-training/
- https://us-cert.cisa.gov/ics
- https://www.dsb.no/globalassets/dokumenter/rapporter/sikkerhet-i-kritisk-infrastruktur.pdf

What is cloud computing

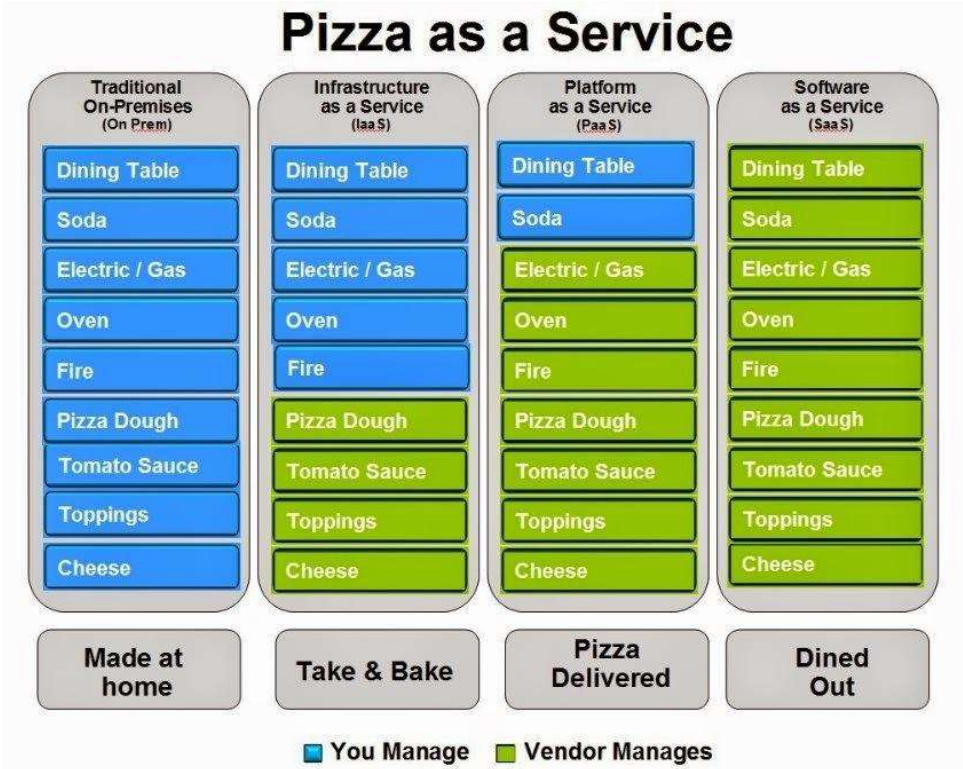
- A remote pool of (shared) resources on different levels
- Dynamic provisioning, elastic use of resources, pay-as-you-go
- A type of outsourcing

- Increased utilization of resources, economy of scale
- Multi-tenancy
- Global reach
- Running expense vs capital expense
- High availability – but assumes (fast) internet connectivity
- Deployment: public, private, hybrid and community

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

Delivery models

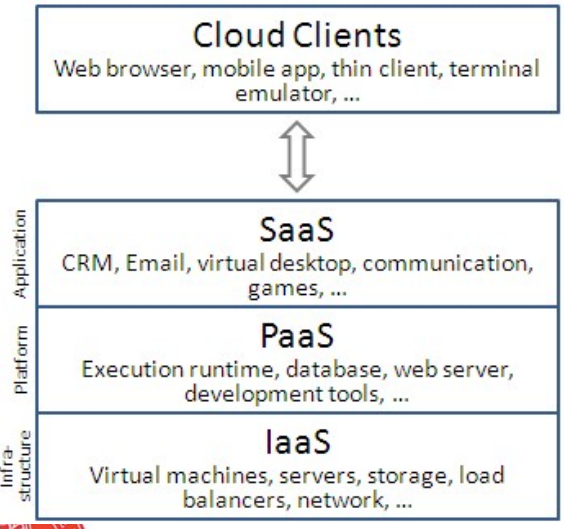
- A perfect figure from Fred Bals at Episerver

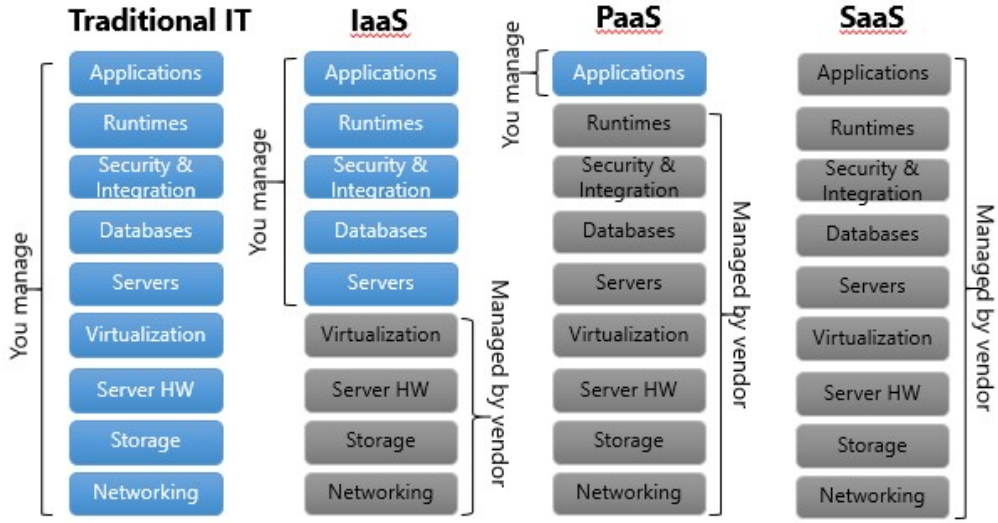


https://www.episerver.com/learn/resources/blog/fred-bals/pizza-as-a-service/

Delivery models

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

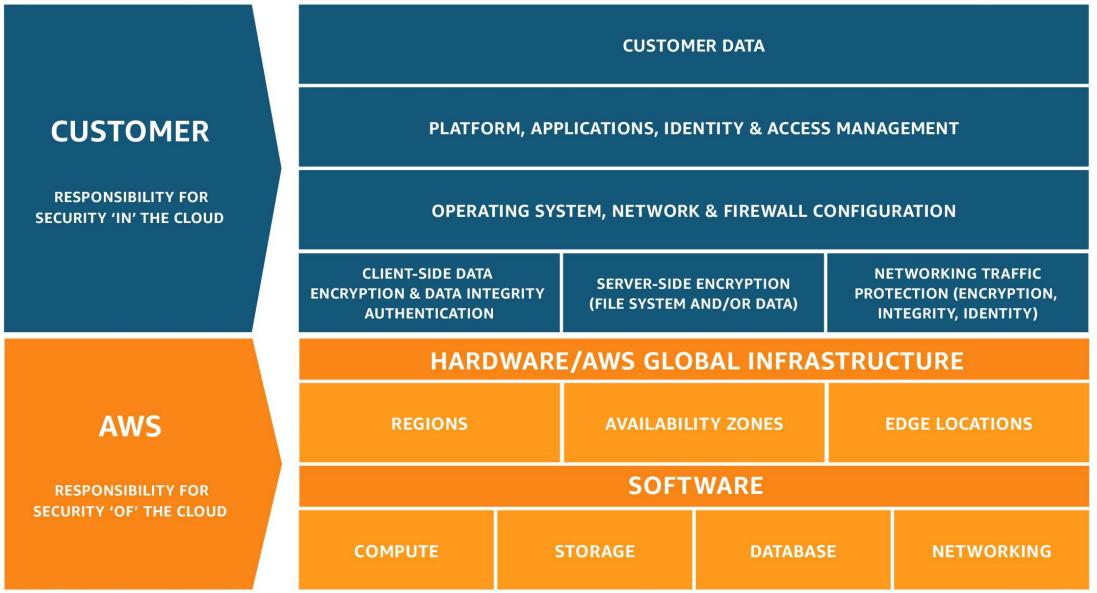




Both figures are from: http://oracle-help.com/oracle-cloud/cloud-computing-stack-saas-paas-iaas/

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

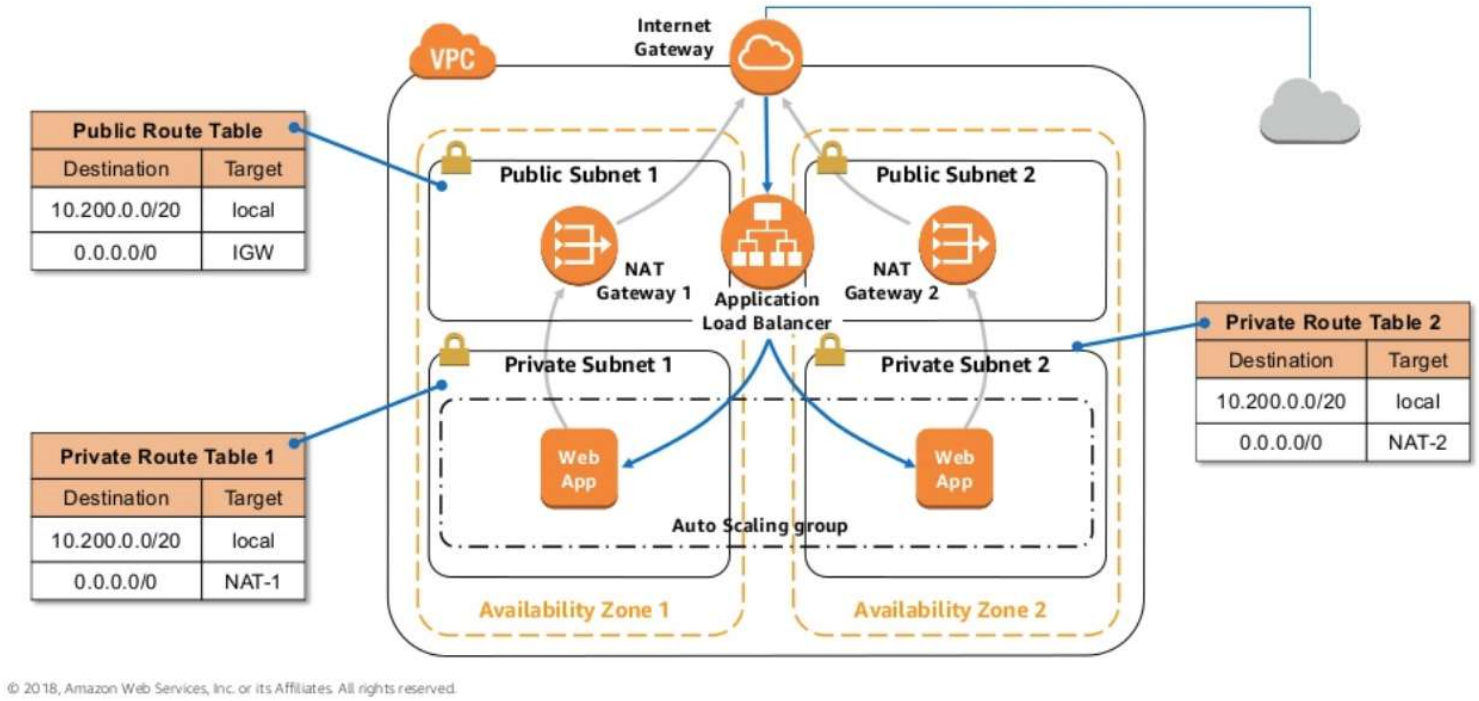


https://aws.amazon.com/compliance/shared-responsibility-model/

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



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.

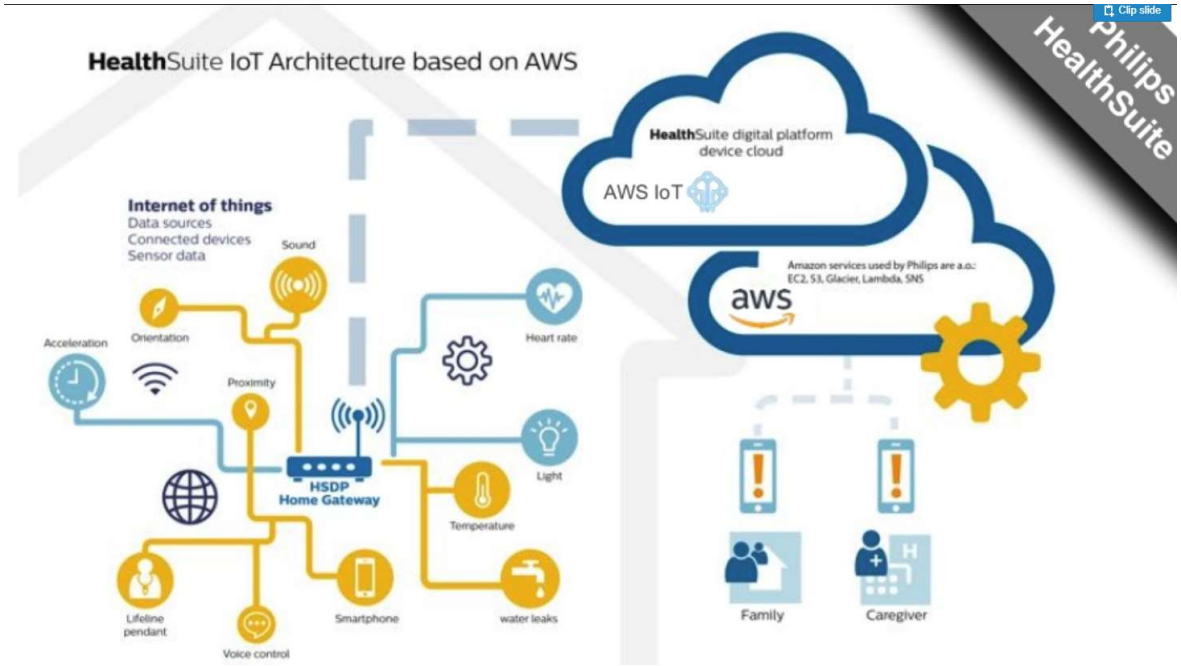
3

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.

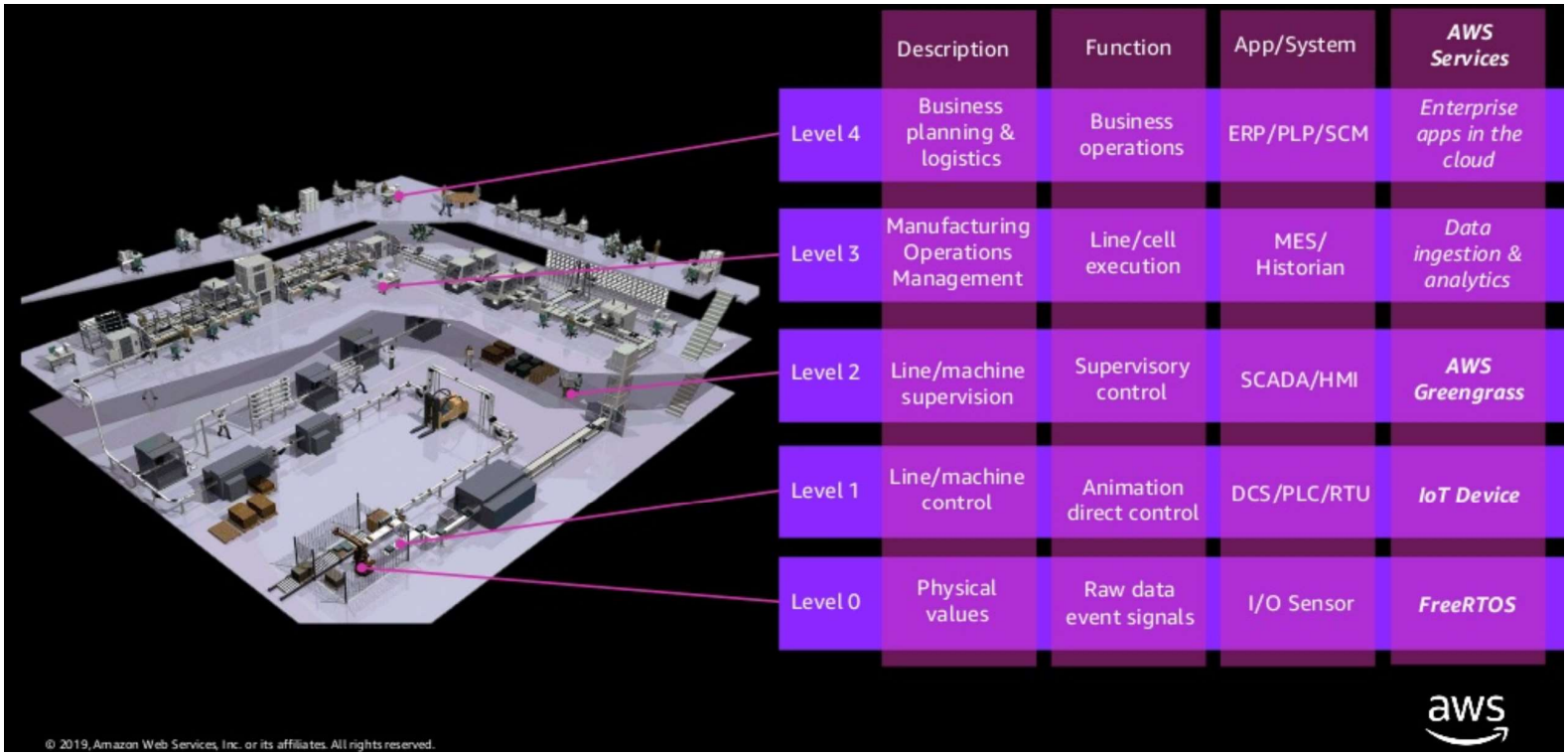
https://www.slideshare.net/AmazonWebServices/intro-to-aws-iot-80291679

Healthcare example



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

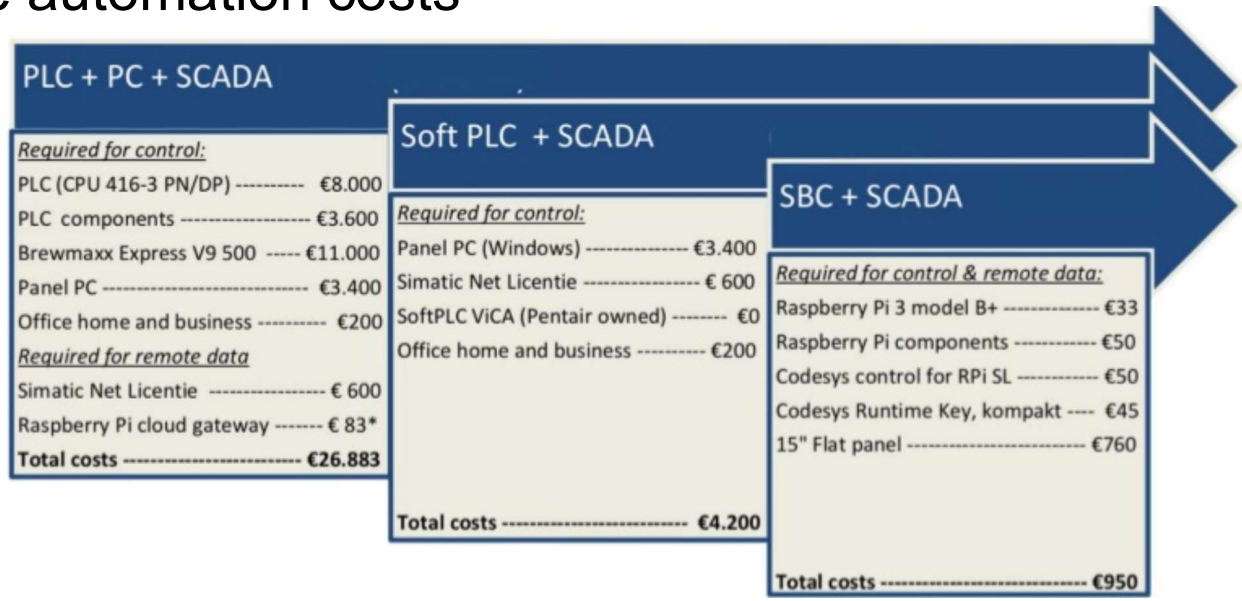
AWS in relation to ISA-95



https://www.slideshare.net/AmazonWebServices/aws-intelligent-at-edge-for-iot

Be careful!

- Slide from the same presentation as on the previous one
- One must be careful: the system is getting cheaper, but the capabilities and the environment, where they can be operated is changing
- It is _not this easy_ to cut the automation costs

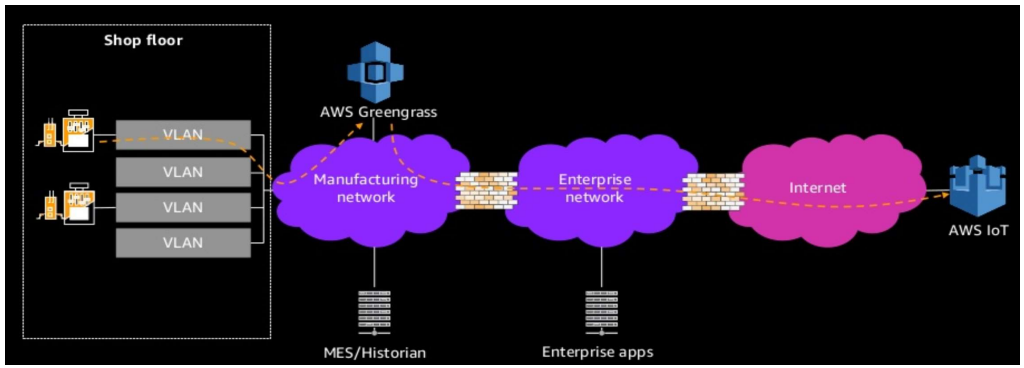


AWS FreeRTOS

- A free RTOS with extensions to connect to AWS services
  - Key importance for getting market share
  - OS is important in the budget of embedd projects
  - https://aws.amazon.com/freertos/

AWS Greengrass

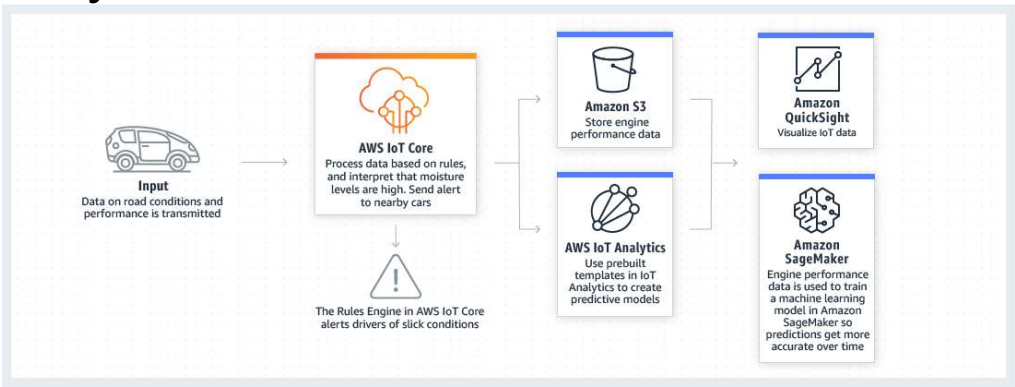
- Together with Amazon FreeRTOS: enable amazon IoT for a wider audience
- Offline operation with Lambda and device shadow support
- Local extraction, processing and reaction possiblity → QoS, criticality!
- Forwards information to AWS IoT core → which can then serve them as SaaS to Enterprise IT
- Secrets manager
- HW security

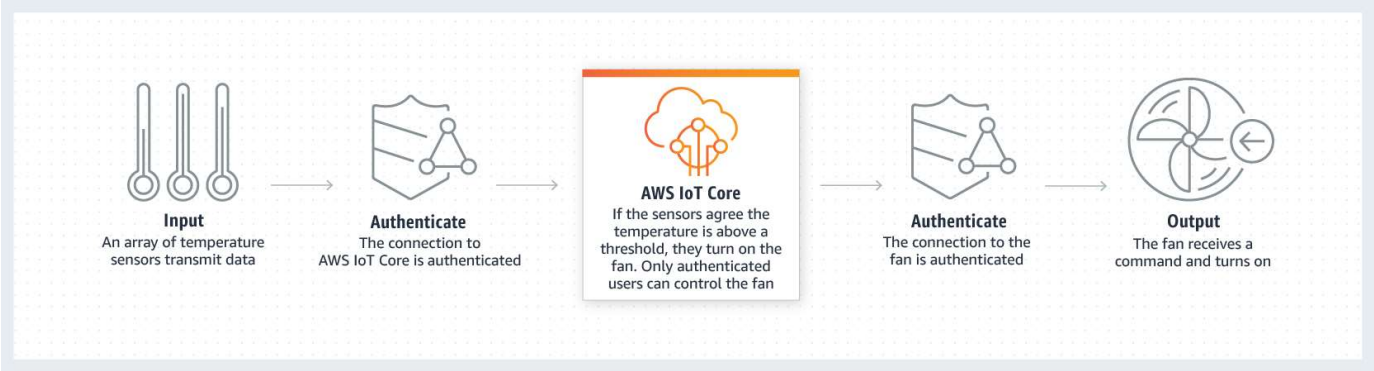


https://www.slideshare.net/AmazonWebServices/aws-intelligent-at-edge-for-iot

AWS IoT Core

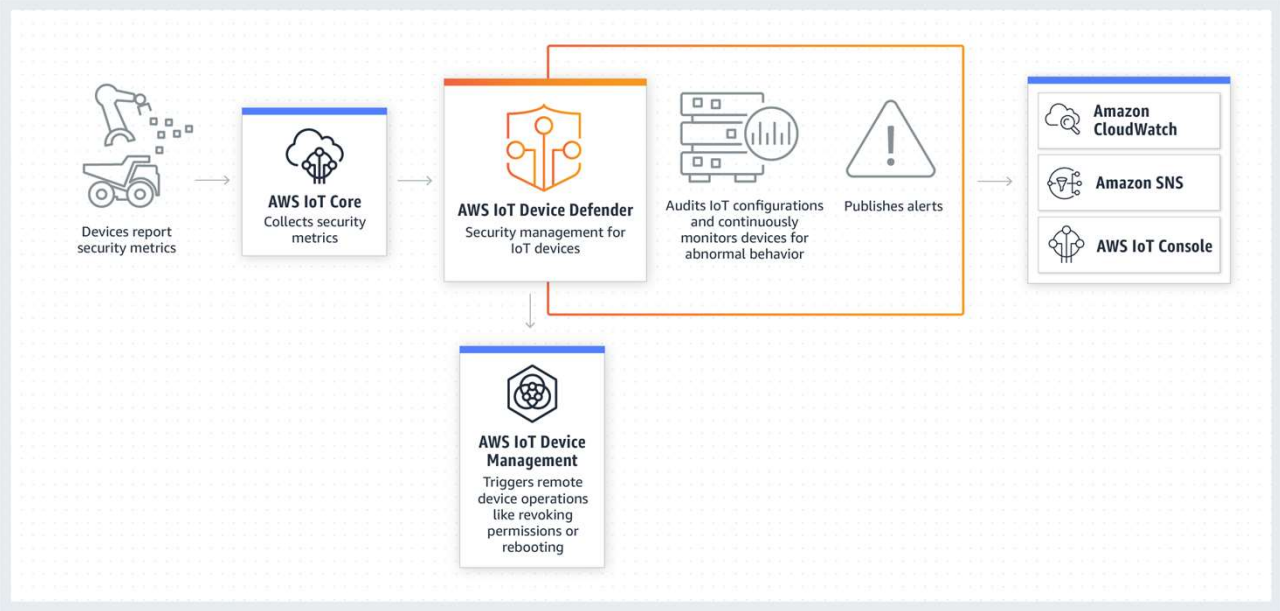
- Is a managed service to allow connectivity from the field to cloud services



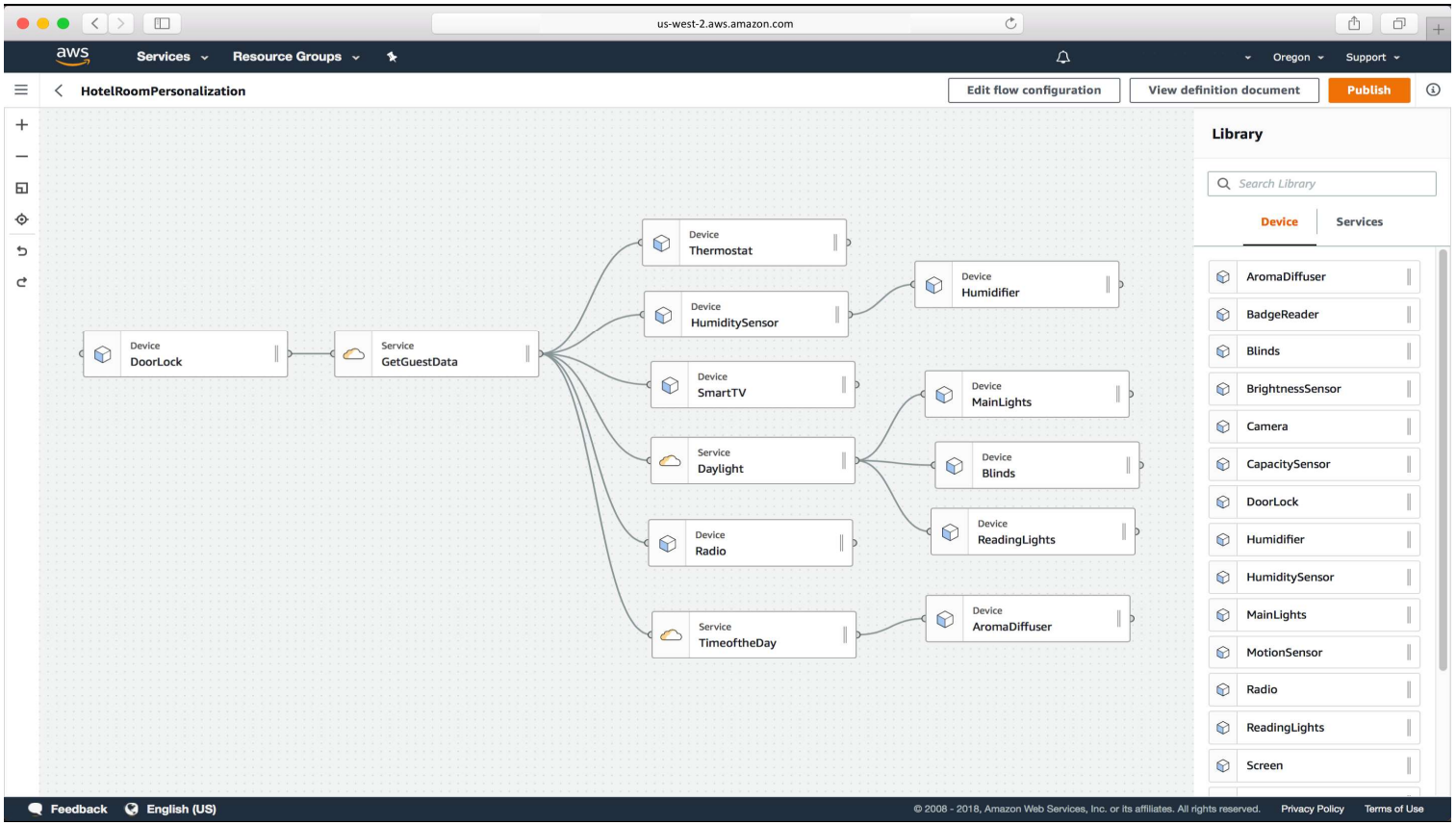


AWS IoT Device Defender

- Supports IoT Core with auditing the configuration against best practice and company policy
- Continous compliance, Attack surface evaluation, Threat impact analysis



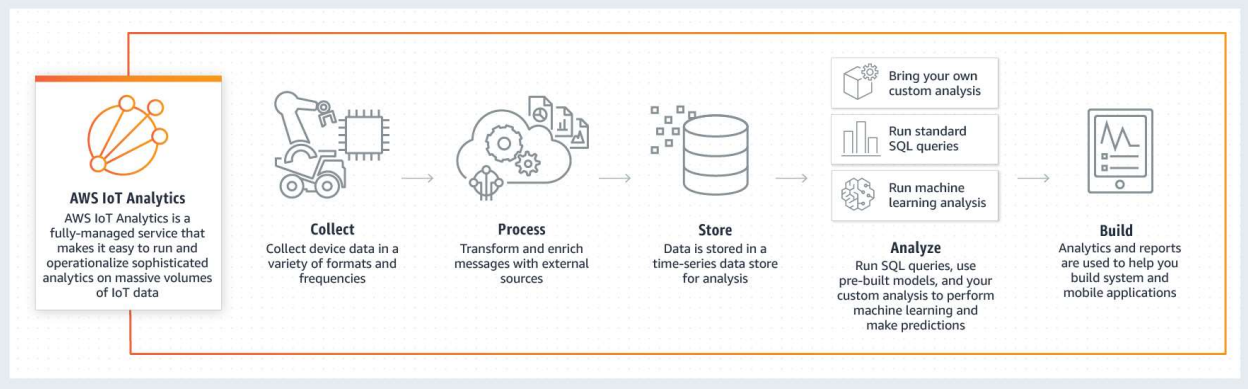
IoT ThingsGraph



IoT and analytics - SiteWise

- A combination of insight into IoT and processing power and analytics in cloud allows us to work on optimizations in different fields:
  - Classification
  - Route optimization
  - Anomaly detection
  - Prediction and forecast
  - Language processing
  - KPI identification

- Data lake: store unstructured data and run analytics on it



Security resources

- https://aws.amazon.com/security/videos/
- https://aws.amazon.com/security/penetration-testing/
- https://aws.amazon.com/blogs/industries/reinvent-2020-manufacturing-and-industrial-recap/
- https://pages.awscloud.com/GLOBAL-In-GC-700-The-Industrial-Executives-Guide-to-Cloud-Security-2021-learn.html

Worth reading

- OWASP Internet of Things project
  https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
- Amazon Web Services IoT
  https://aws.amazon.com/iot/