IOT'S CYBER SECURITY LUCKY 13

Jennifer Janesko

Presented at IoT People, August 2020

JENN JANESKO

- 20+ years in IT
- 6 years in Cyber Security
  - security testing (network, web, automotive, ICS)
  - architecture & risk analysis & secure design
  - application security / DevSecOps
  - cloud (GCP, AWS)
- Organizer: MUC:SEC and BSidesMunich
- running, hiking, ukulele playing, puzzling, tinkering, language learning, (bouldering)
- Twitter: @jennjanesko

OUR JOURNEY TODAY

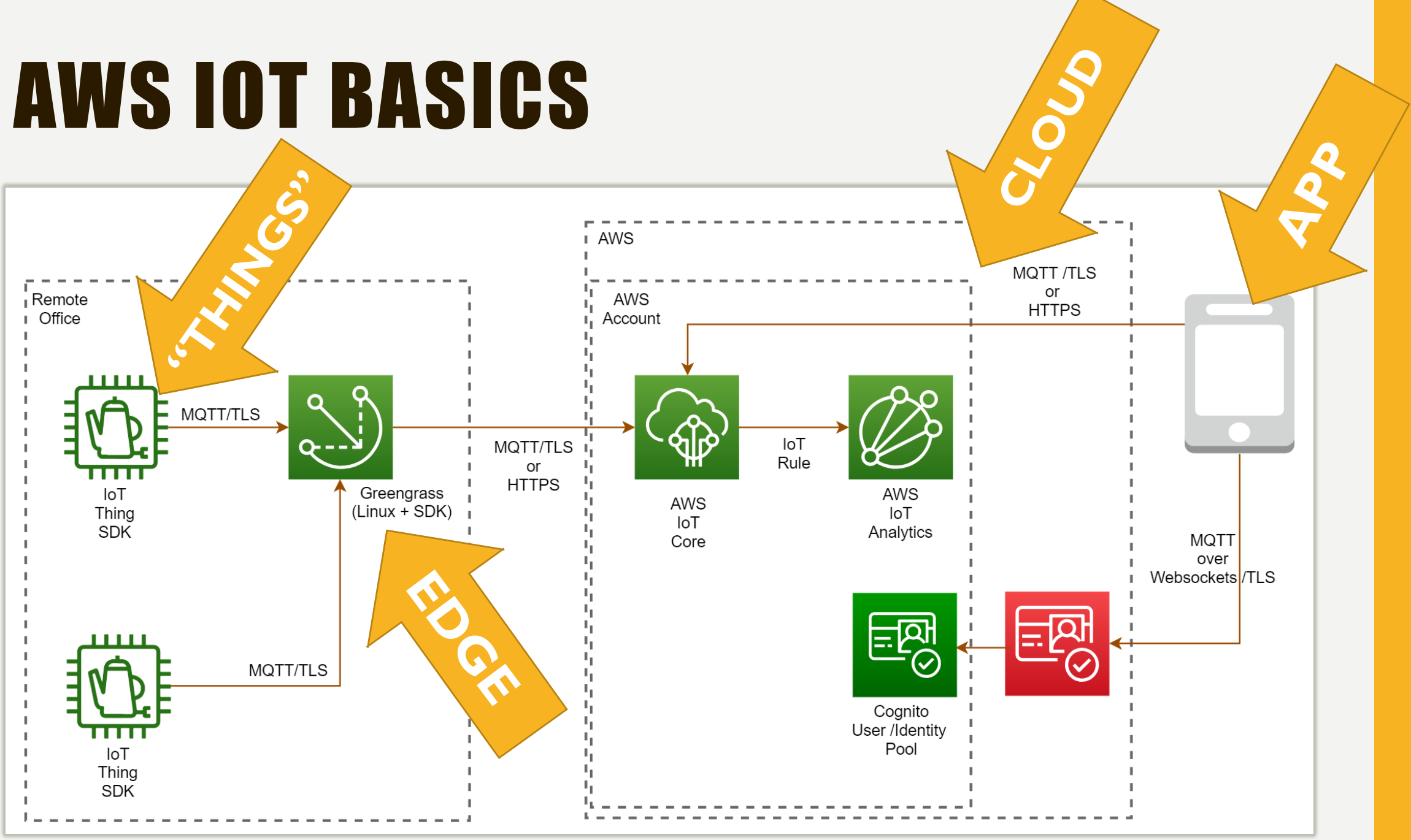
AWS IoT Stack

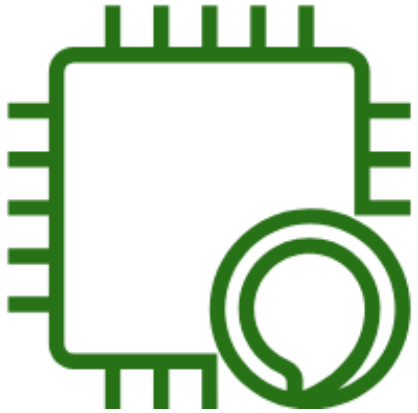
ETSI EN 303 645

EZTea & the Lucky 13

AWS IOT STACK

AWS IOT BASICS





Alexa & Skills

DeepLens

Dash Button

NOT IN SCOPE....

ETSI EN 303 645

CYBER SECURITY FOR CONSUMER IOT: BASELINE REQUIREMENTS

			Page	#of Provisions
5	**Cybersecurity Provisions for Consumer IOT**		13	
	5.1	No universal default passwords	13	5
	5.2	Vulnerability reporting	14	3
	5.3	Keep software updated	15	16
	5.4	Securely store sensitive security parameters	18	4
	5.5	Communicate securely	19	8
	5.6	Minimize exposed attack surfaces	20	9
	5.7	Ensure software integrity	21	2
	5.8	Ensure that personal data is secure	22	3
	5.9	Make systems resilient to outages	22	3
	5.10	Examine system telemetry data	23	1
	5.11	Make it easy for users to delete data	23	4
	5.12	Easy installation and maintenance	24	3
	5.13	Validate input data	24	1
6	**Data Protection Provisions for Consumer IoT**		24	5

SECURITY BASELINE CHECKLIST

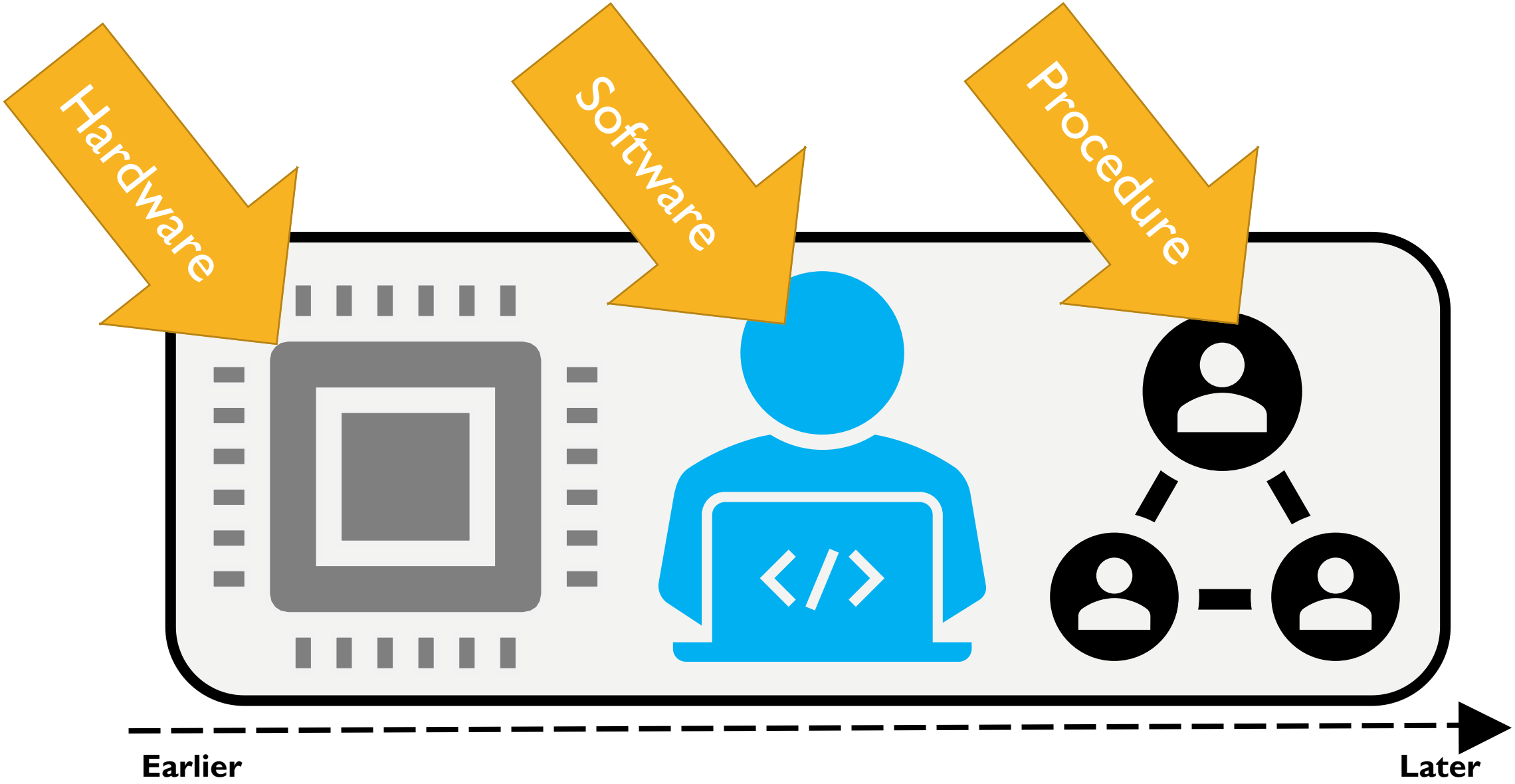
Table B.1: Implementation of provisions for consumer IoT security

Clause number and title			
Reference	**Status**	**Support**	**Detail**
5.1 No universal default passwords			
Provision 5.1-1	M C (1)		
Provision 5.1-2	M C (2)		
Provision 5.1-3	M		
Provision 5.1-4	M C (8)		
Provision 5.1-5	M C (5)		
5.2 Implement a means to manage reports of vulnerabilities			
Provision 5.2-1	M		
Provision 5.2-2	R		
Provision 5.2-3	R		
5.3 Keep software updated			
Provision 5.3-1	R		
Provision 5.3-2	M C (5)		
Provision 5.3-3	M C (12)		
Provision 5.3-4	R C (12)		
Provision 5.3-5	R C (12)		
Provision 5.3-6	R C (9, 12)		
Provision 5.3-7	M C (12)		
Provision 5.3-8	M C (12)		

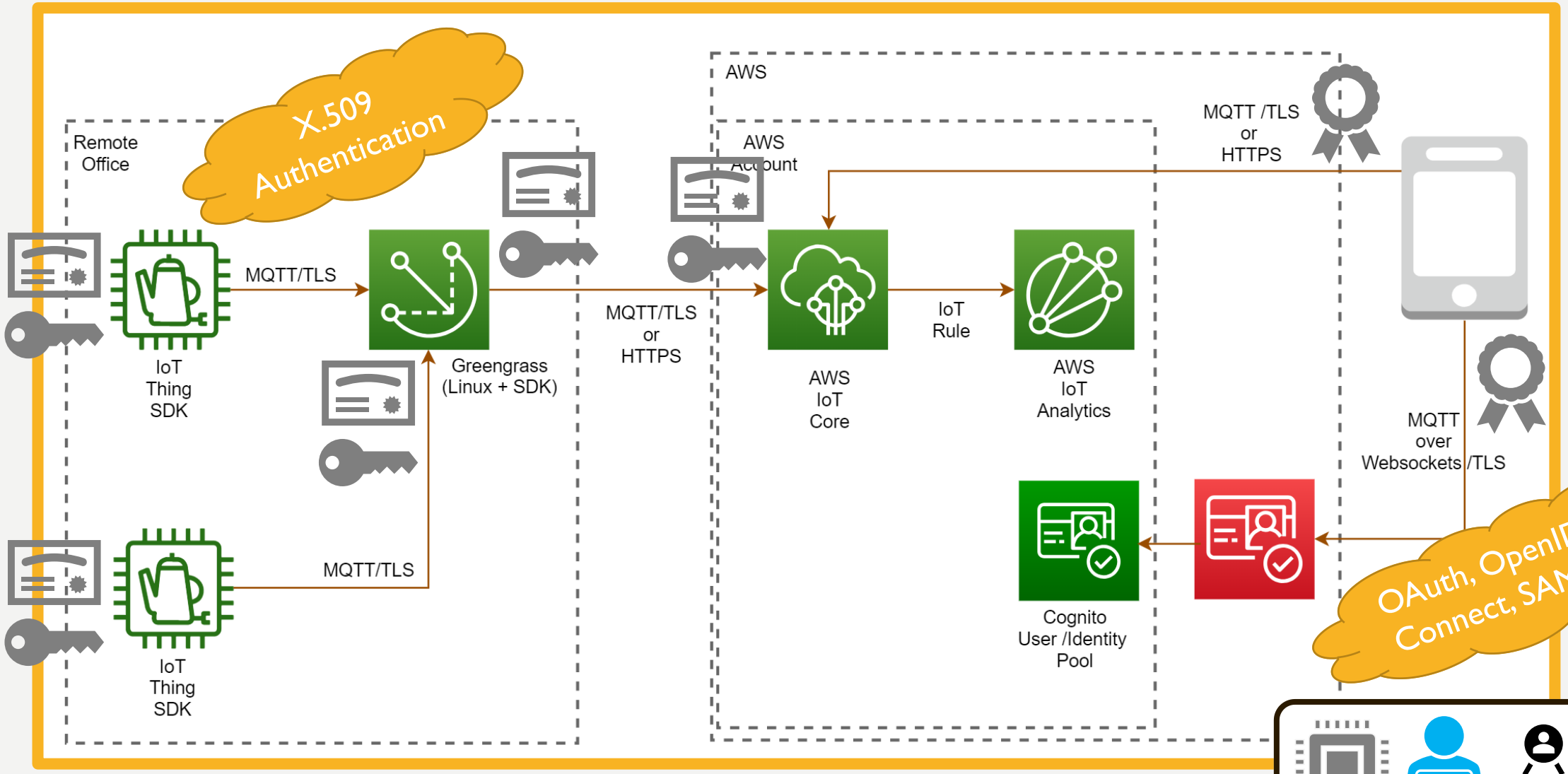
M	the provision is a mandatory requirement
R	the provision is a recommendation
M C	the provision is a mandatory requirement and conditional
R C	the provision is a recommendation and conditional

EZTEA
&
ETSI LUCKY 13

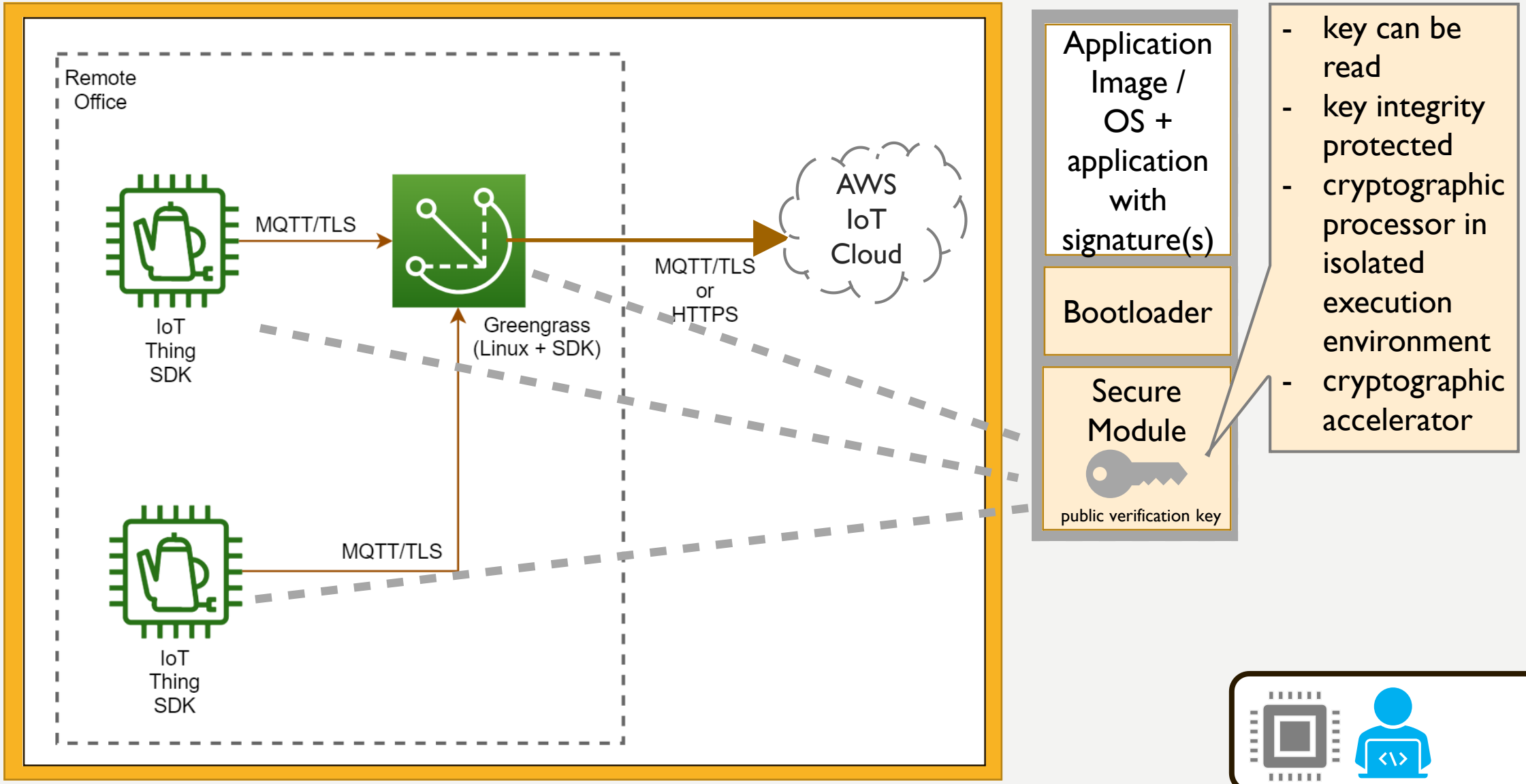
DESIGN DECISION TIMELINE



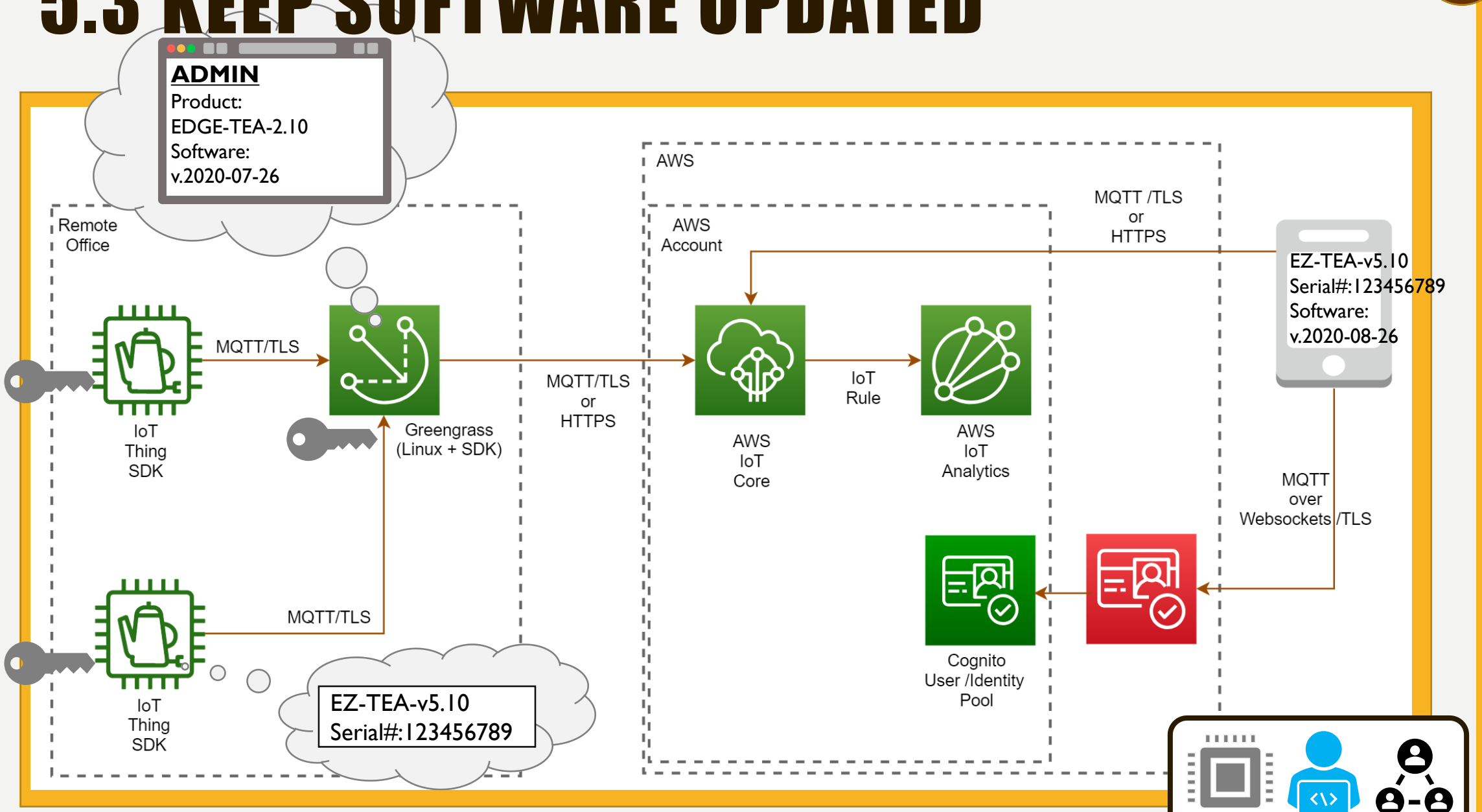
5.5 COMMUNICATE SECURELY



5.7 ENSURE SOFTWARE INTEGRITY



5.3 KEEP SOFTWARE UPDATED



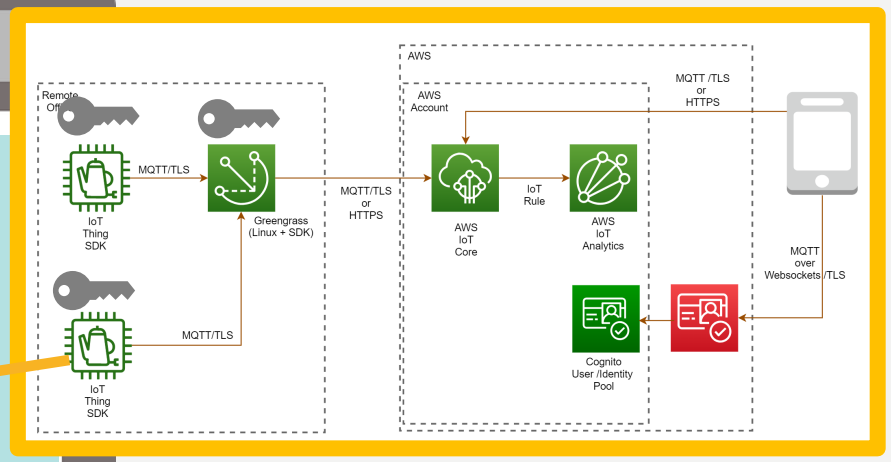
5.8 & 6 PROTECT PERSONAL DATA

ADMIN

User: jan-admin

Jan Madhatter
123 Darjeeling Ln.
73AA37 Somewhere

-Configure
-Kettle-Link
-Descale
-Privacy
-**Data Collection**
-Factory Reset
-System Update



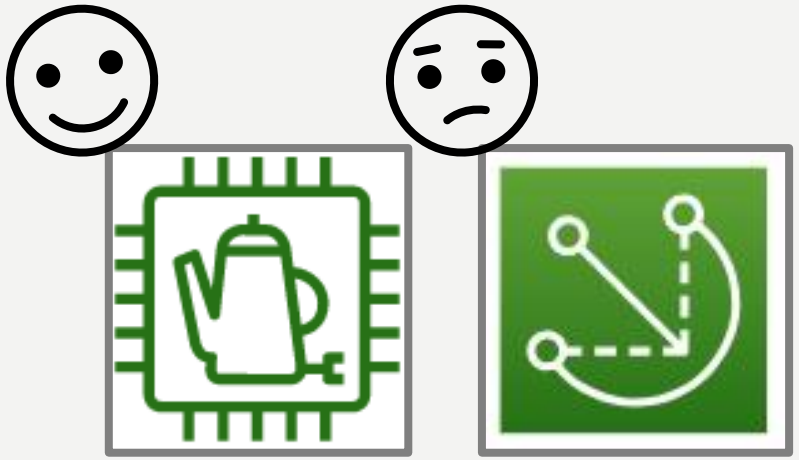
Data EZTea Collects

- Volume of water heated per use
- Water volume low alarm
- Times of device use
- Heating coil maximum temperature per use
- Heating coil heating pattern per use...

Purpose ...

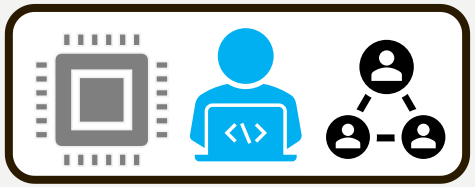
5.4 PROTECT SENSITIVE SECURITY PARAMETERS

Crypto Material	Confidentiality	Integrity
CA Certificate for Authentication		X
Private Keys for Authentication	X	X
Public Keys (secure boot, software update)		X
Encryption keys (private data)	X	X



IoT Thing Greengrass

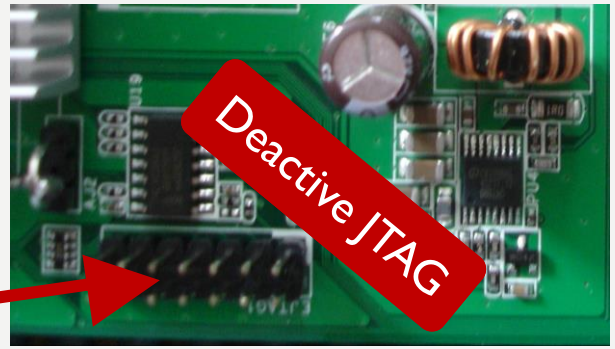
- Tamper resistant (physical, electrical)
- Use open, peer reviewed standards
- Sensitive security measures should be "stored securely"



5.6 MINIMIZE ATTACK SURFACES

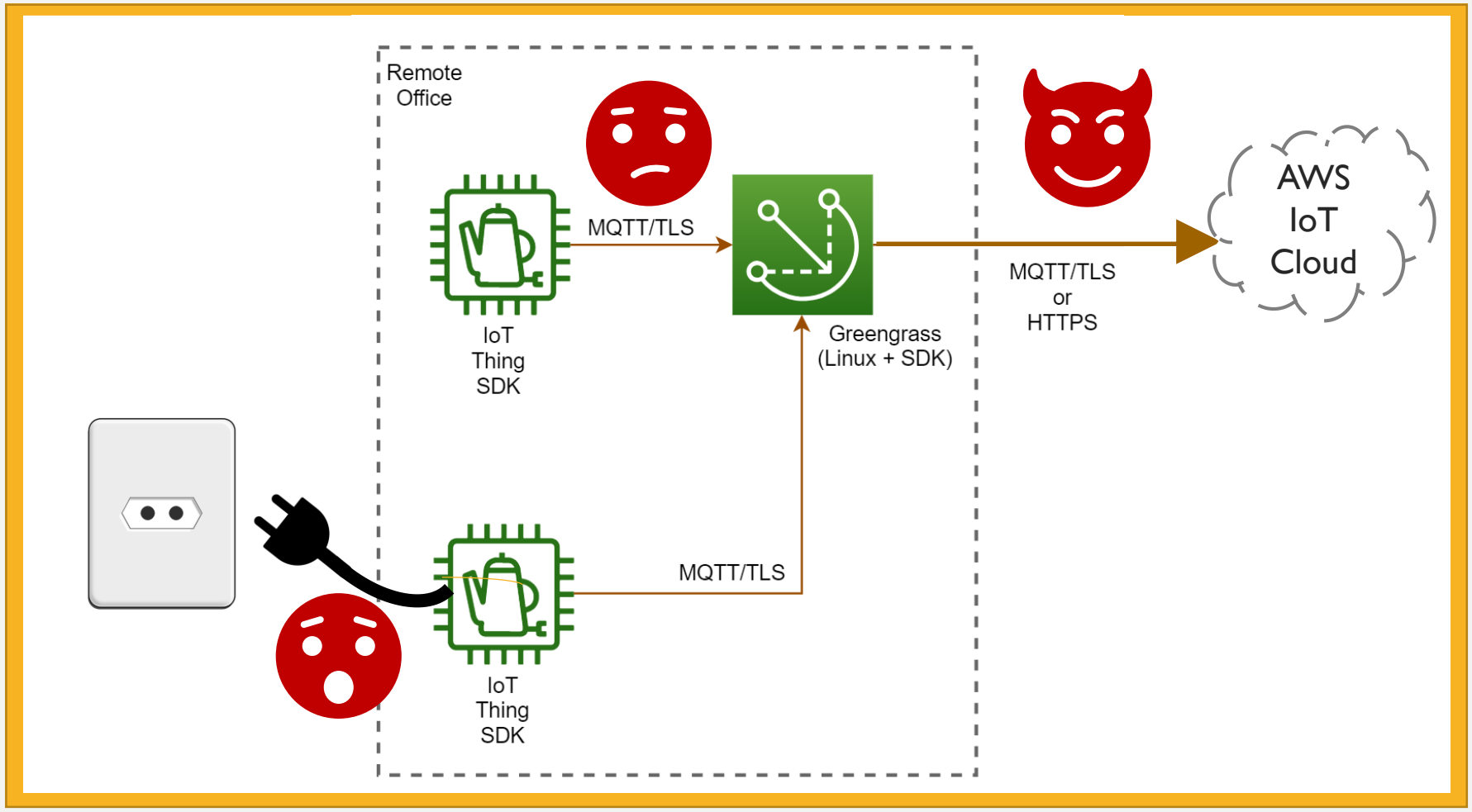
```
root@eztea:~$ ps -ef
UID      PID PPID    TIME        CMD
root     1   0       00:00:01    /sbin/init
.
.
root     123 1       00:00:03    [watchdogd]
.

eztea-D 897 0        00:05:45    tea-service
eztea-D 900 0        00:05:47    smtpd
eztea-D 987 1        00:06:01    nginx
```

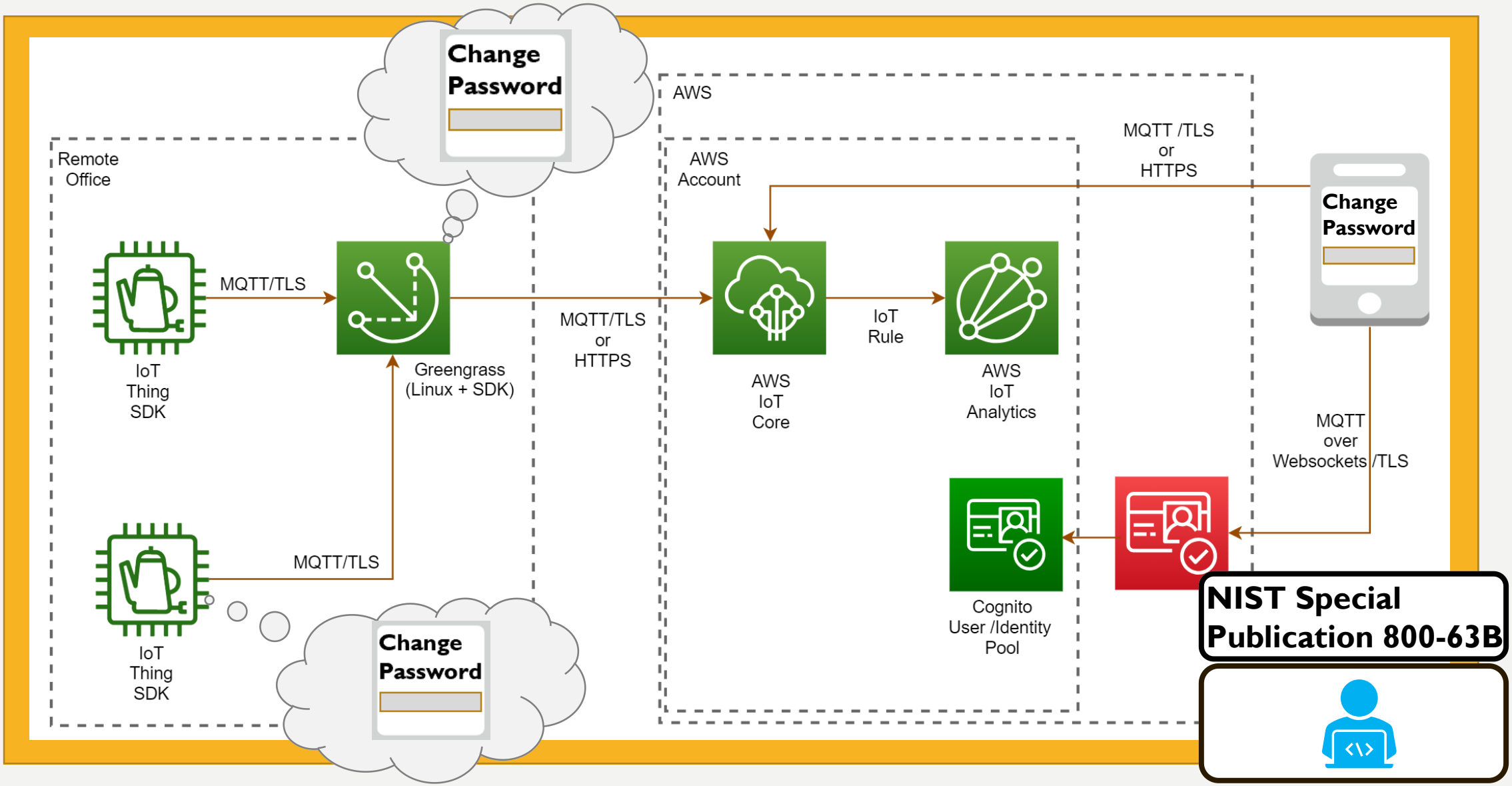


5.12 EASY DEVICE MAINTENANCE

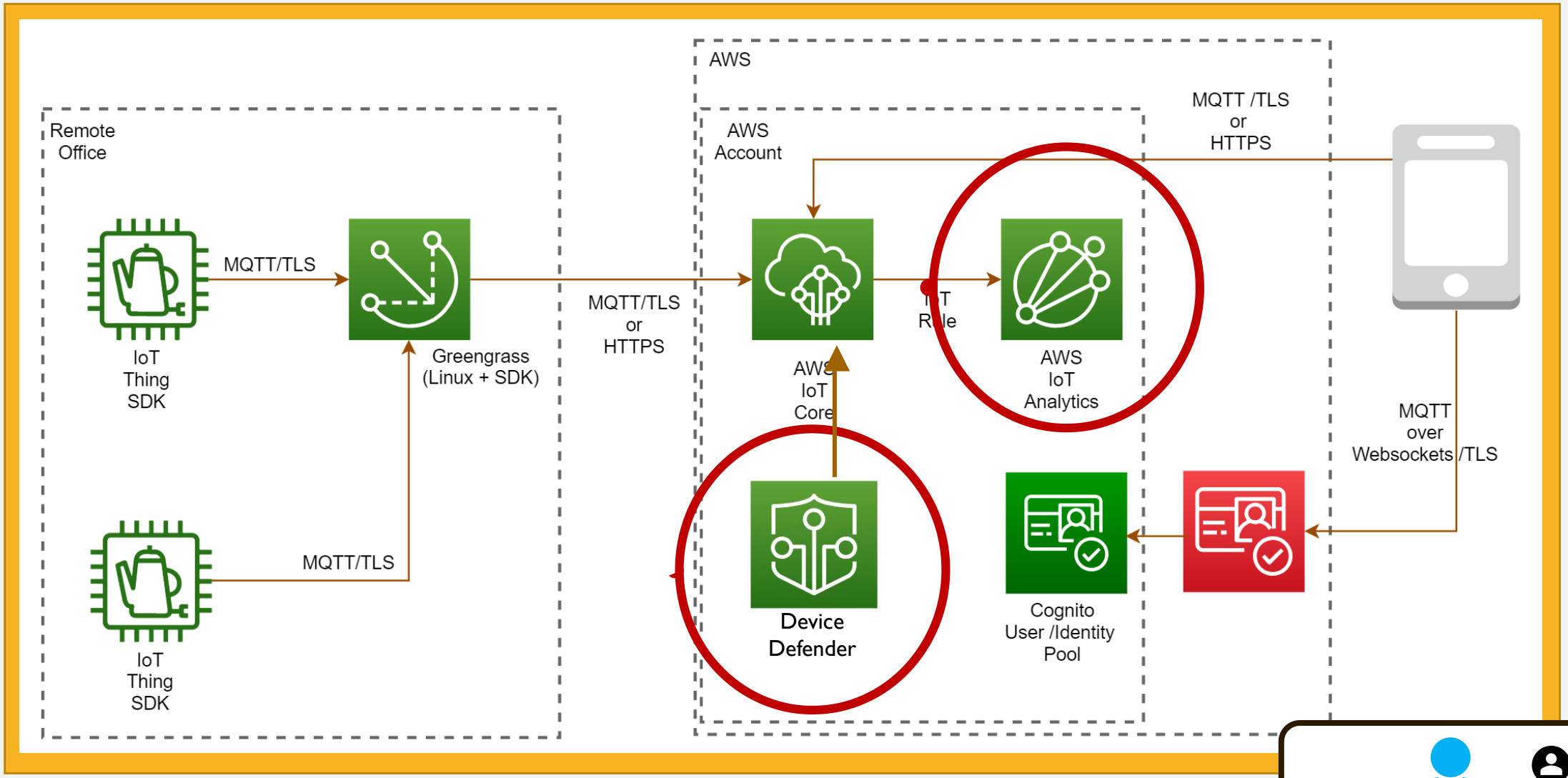
5.9 MAKE SYSTEMS RESILIENT



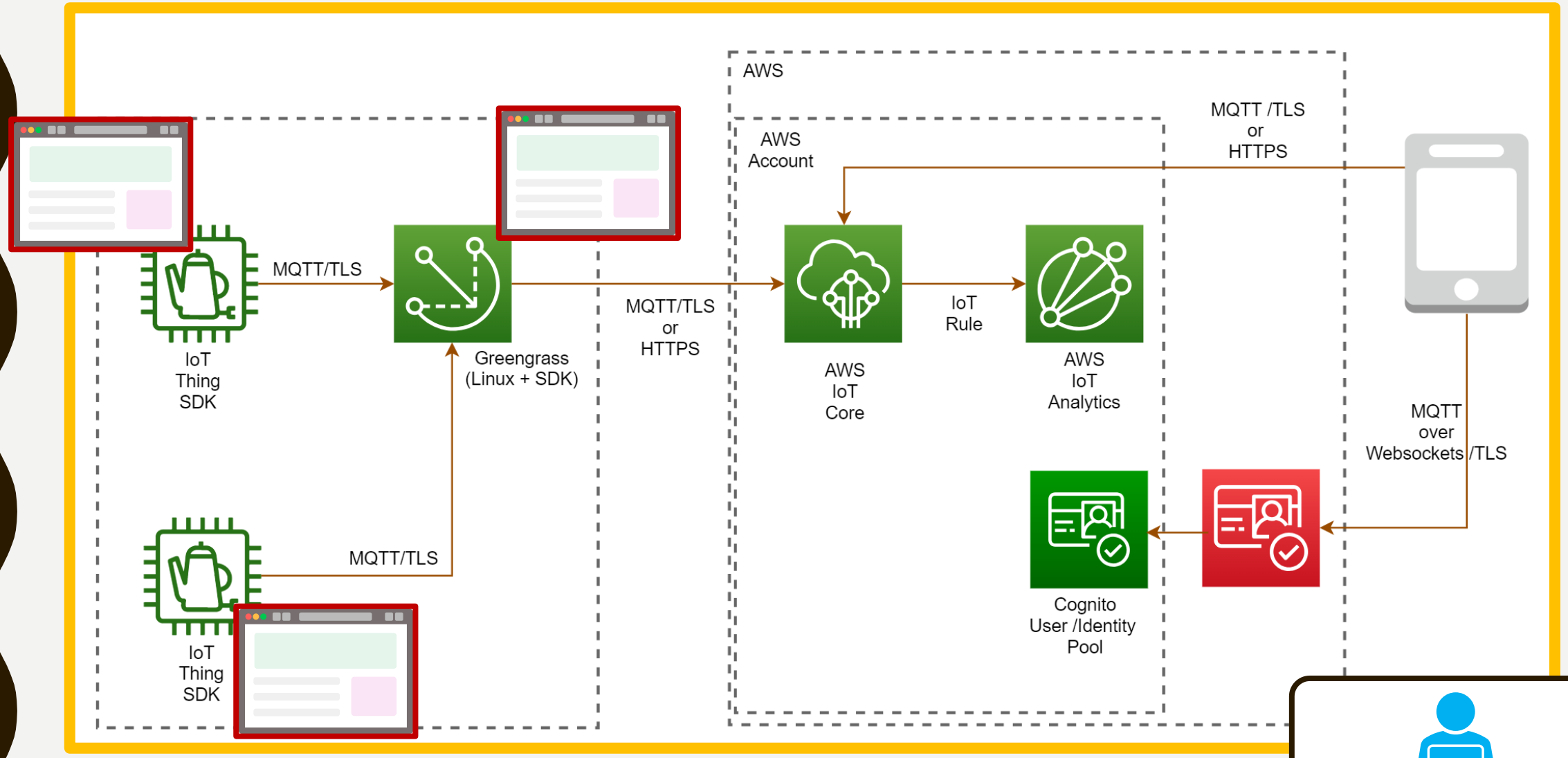
5.1 NO UNIVERSAL DEFAULT PASSWORD



5.10 EXAMINE SYSTEM TELEMETRY DATA



5.13 VALIDATE INPUT DATA



5.2 ENABLE VULNERABILITY REPORTING

Hacking a Smart Kettle

Earlier this year, Packetlabs was asked by the Hackable podcast to investigate a smart, WiFi enabled kettle and create some working exploits to demonstrate on the podcast. After our research we found a way to steal the WiFi password of a user's home network from the kettle, the only requirement is to be within WiFi range of the kettle. The episode, number 26, is titled "Malicious Brews" and can be listened to here.

Here's how it works at a high-level:

- Send crafted WiFi messages to the kettle to deauthenticate it from its current WiFi network
- Create a fake WiFi network that mimicks the original WiFi network
- The kettle joins the rogue WiFi network
- Connect to the kettle using the default password of "000000"
- Enter a command to display the WiFi passwords the kettle has stored.

Once the attacker has the victims WiFi password, they can connect to the network and attack any devices on the network. In the podcast, the attacker ends up compromising Geoff's Facebook credentials; an attacker could also hack into laptops and smartphones to install malware, steal documents, or monitor any traffic on the network to steal account credentials for email and online banking.

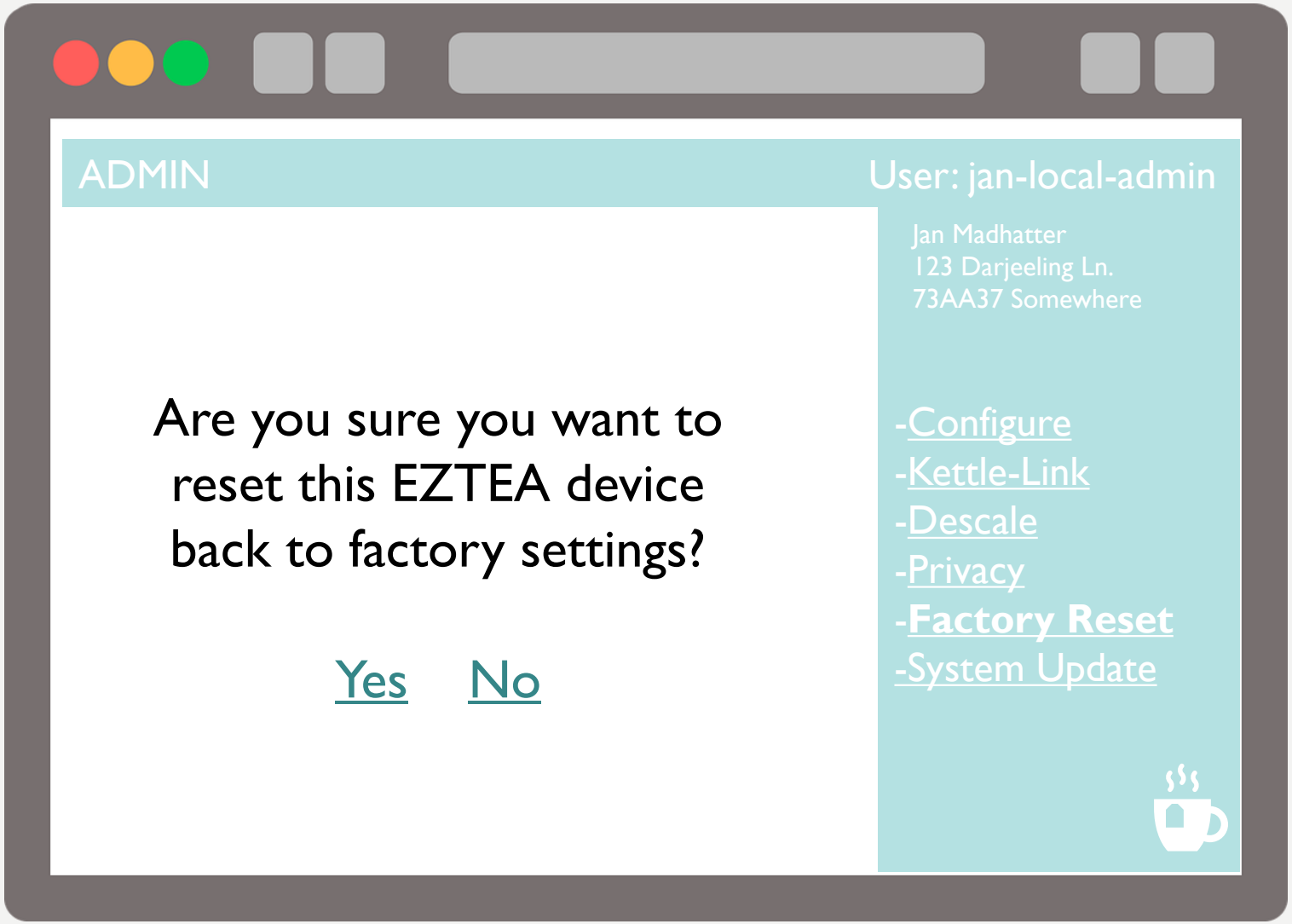
ISO/IEC 29147:2018

OWASP

https://www.packetlabs.net/hackable-podcast-kettle/

https://hackablepodcast.com/episodes/malicious-brews

5.11 EASY USER DATA DELETION



DESIGN DECISION MATRIX: HARDWARE, SOFTWARE, PROCEDURE

ID	Provisions Category	Hardware	Software	Procedure
5.1	No universal default passwords		✓	
5.2	Vulnerability reporting			✓
5.3	Keep software updated	✓	✓	✓
5.4	Securely store sensitive security parameters	✓	✓	✓
5.5	Communicate securely	✓	✓	✓
5.6	Minimize exposed attack surfaces	✓	✓	
5.7	Ensure software integrity	✓	✓	
5.8 & 6	Ensure that personal data is secure	✓	✓	✓
5.9	Make systems resilient to outages	✓	✓	
5.10	Examine system telemetry data		✓	✓
5.11	Make it easy for users to delete data		✓	✓
5.12	Easy installation and maintenance	✓	✓	✓
5.13	Validate input data		✓	

ETSI LUCKY 13: GREAT START, AND…

- **API**
  https://owasp.org/www-project-api-security/
- **Mobile App**
  https://owasp.org/www-project-mobile-security/
- **Web**
  https://owasp.org/www-project-top-ten/
- **Logging**
  https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Logging_Cheat_Sheet.md
- **Device-Device Authentication & Authorization…**
- **Cloud…**

THANK YOU!

Jennifer Janesko
@jennjanesko

Image References

- https://pixabay.com/vectors/citrus-juicer-cup-fork-garlic-press-1296432/
- https://pixabay.com/vectors/browser-web-internet-technology-4026002/
- Zuzu, https://commons.wikimedia.org/wiki/File:Netgear_ProSafe_Dual_WAN_VPN_Gigabit_Firewall_FVS336G_JTAG_interface.jpeg
- https://pixabay.com/photos/usb-outlet-connection-informatica-2327518/
- https://pixabay.com/illustrations/mobile-phone-smartphone-2468068/