Cyber Security for IoT

Beveiliging Eenergie-efficiënt IoT luchtkwaliteitsmonitoring system met LoRa-communicatie

Opleiding: Internet of Things

Academiejaar: 2024-2025

Naam: Amir Hasanzada en Ieben Mens

AP HOGESCHOOL ANTWERPEN

AP.BE

Inhoud

1 Introductie

Dit project is het eindproject van Cyber Security. Als eindproject van Cyber Security zijn Amir en ik van plan om het het eindproject van IoT Projects te beveiligen a.d.h.v. de onderwerpen die we tijdens de les van Cyber Security hebben gezien. Het doel van het oorspronkelijke project is het meten van de luchtkwaliteit in twee verschillende lokalen.

2 Projectdoelstelling

Het doel van het project is het IoT Project project zo veilig mogelijk maken. Dit gaan we doen a.d.h.v. het zoeken naar de zwakke punten en de Threats ervan en deze oplossen m.b.v. een Risico Analyse. We kunnen dit fysiek niet realiseren maar we gaan het hier volledig uitleggen.

3 Risico Analyse

ID	Component	STRIDE threat	Description and Explanation	Damage	Reproducibility	Exploitability	Affected Users	Discoverability	Risk Rating
1	Doos	Tampering	Omdat de doos gemaakt is uit zacht materiaal kun je deze makkelijk stuk maken.	10	3	4	10	10	7,4
2	Doos	Dos	Doos is niet op slot dus iedereen kan die openen en draden/compnenten ontkoppelen.	9	3	3	9	9	6,6
3	Doos	Tampering	De doos is niet waterdicht. Als men er water over zou gieten is alles stuk.	10	6	5	10	6	7,4
4	LoRa Gateway TNT	Dos	Overbelasting. Overmatig verkeer blokkeert communicatie met de gateway.	9	5	6	10	7	7,4
5	LoRa Gateway TNT	Tampering	De hacker verandert de verzonden data tijdens het transport.	7	6	5	8	5	6,2
6	LoRa Gateway TNT	Tampering	De hacker kan met de gehackte keys zich voor doen als de gebruiker.	7	6	7	4	2	5,2
7	LoRa Communicatie	Information Leakage	Gevoelige gegevens die via LoRa worden verzonden, worden onderschept door de hacker.	8	7	6	9	6	7,2
8	MQTT Broker	Tampering	De hacker verandert berichten tijdens het transport, daardoor gebeuren er verkeerde acties.	7	6	5	8	5	6,2
9	MQTT Broker	Dos	Door te veel verbindingen of berichten kan de broker onbruikbaar worden.	9	6	8	9	4	7,2
10	MQTT Broker	Spoofing	Als je subscribed op het topic van de MQTT server kan je alle data zien.	7	3	7	9	4	6
11	MQTT Communicatie	Information Leakage	Een aanvaller kan gevoelige gegevens lezen als TLS(Transport Layer Security) ontbreekt.	8	6	7	8	6	7
12	ESP	Tampering	Andere code uploaden naar esp.	7	5	7	10	2	6,2
13	ESP	Dos	De hacker maakt de ESP fysiek kapot maken.	5	10	8	10	9	8,4
14	ESP	Spoofing	De hacker doet zich voor als een geldig apparaat om data te onderscheppen.	8	7	6	9	6	7,2
15	Raspberry PI3 server	Tampering	Andere gegevens instellen in de configuratie.	8	7	6	6	3	6
16	Raspberry PI3 server	Tampering	Het overbelasten van de Raspberry PI doormiddel van een Dos aanval.	8	6	5	7	6	6,4
17	Raspberry PI3 server	Dos	Overmatige netwerkenverzoeken of zware rekenprocessen die server onbruikbaar maken.	8	6	6	7	3	6
18	Raspberry PI3 server	Repudiation	Het ontbreken van logging kan leiden tot ontkenning van acties.	2	3	1	2	5	2,6
19	Raspberry PI3 server	Information Leakage	Onbeveiligde configuratiebestanden bevatten gevoelige informatie.	7	4	4	5	4	4,8
20	Raspberry PI3 server	Elevation of Privilege	Een aanvaller misbruikt een kwetsbaarheid in de software of configuratie om root-rechten te krijgen.	6	5	5	3	3	4,4

3.1 Doos

Tampering:

- Doos is gemaakt uit zacht materiaal dus makkelijk stuk te maken. (plastic PLA)
- Doos is niet waterdicht dus als men er water over giet is alles stuk.

Dos:

- Doos is niet op slot dus iedereen kan die openen en draden/componenten ontkoppelen.

Repudiation: None

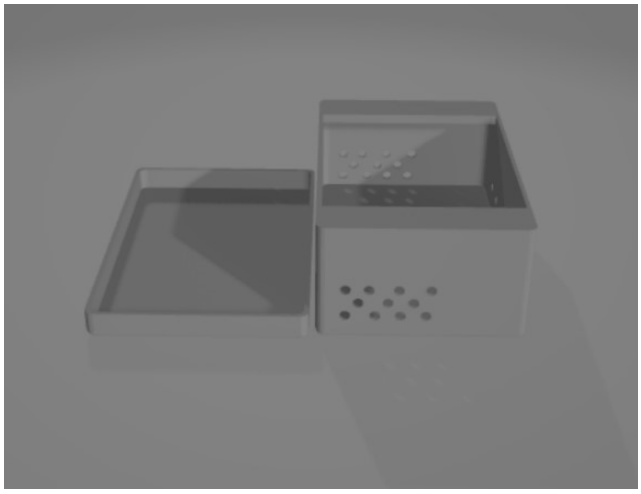
Spoofing: None

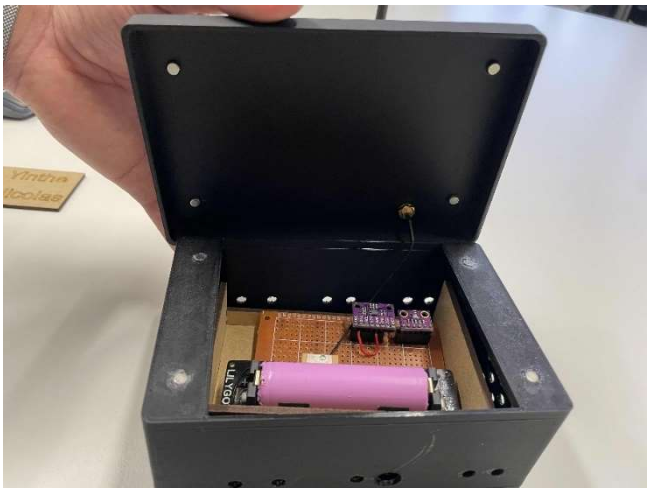
Information Leakage: None

Elevation of Privilege: None

3.1.1 Oplossing Doos

Andere materiaal van doos voorzien BV metaal en slot voorzien voor de opening en temper contact voor de doos voorzien voor het melding of extra automatisatie functies bv als de doos open gaat dat er melding gestuurd word of foto van uit de doos zou getrokken worden.





3.2 LoRa Gateway TNT

Tampering:

- De hacker verandert de verzonden data tijdens het transport.
- De hacker kan met de gehackte keys zich voor doen als de gebruiker.

Dos:

- Overbelasting. Overmatig verkeer blokkeert communicatie met de gateway.

Repudiation: None

Spoofing: None

Information Leakage: None

Elevation of Privilege: None

3.2.1 Oplossing LoRa Gateway TNT

Voorzien van eigen LoRa Gatway en communiceren op eigen frequentie.

3.3 LoRa Communicatie

Tampering: None

Dos: None

Repudiation: None

Spoofing: None

Information Leakage:

- Gevoelige gegevens die via LoRa worden verzonden, worden onderschept door de hacker.

Elevation of Privilege: None

3.3.1 Oplossing LoRa Communicatie

Op eigen frequentie communiceren.

3.4 MQTT Broker

Tampering:

- De hacker verandert berichten tijdens het transport, daardoor gebeuren er verkeerde acties.

Dos:

- Door te veel verbindingen of berichten kan de broker onbruikbaar worden.

Repudiation: None

Spoofing:

- Als je subscribed op het topic van de MQTT server kan je alle data zien.

Information Leakage: None

Elevation of Privilege: None

3.4.1 Oplossing MQTT Broker

Gebruik maken van extra beveiliging en login gegevens voor mqtt configuraties en authenticatie.

Extra: Hashing van logins of veilige ww langer dan 12 karakters met min 1 hoofdletter + cijfer + symbool = 34 000 jaar voor het kraken van de ww.

3.5 MQTT communicatie

Tampering: None

Dos: None

Repudiation: None

Spoofing: None

Information Leakage:

- Een aanvaller kan gevoelige gegevens lezen als TLS(Transport Layer Security) ontbreekt.

Elevation of Privilege: None

3.5.1 Oplossing MQTT communicatie

Gegevens minimaliseren of versleutelen hiervan

IP-whitelisting sta alleen bepaalde IP-adressen toe om verbinding te maken met de broker.

3.6 ESP

Tampering:

- Andere code uploaden naar esp.

Dos:

- De hacker maakt de ESP fysiek kapot.

Repudiation: None

Spoofing:

- De hacker doet zich voor als een geldig apparaat om data te onderscheppen. (hacker doet zich als LoRa Gateway TNT)

Information Leakage: None

Elevation of Privilege: None

3.6.1 Oplossing ESP

Data poort beveiliging van ESP (na het programmeren van esp de micro usb poort van de esp los solderen of zelf saboteren)

Voorzien van extra authenticatie voor toegang tot esp programmaties.

Door extra beveiliging van de doos word de ESP ook extra beveiligt.

3.7 PI3 (server)

Tampering:

- Andere gegevens instellen in de configuratie.
- Overbelaste van de PI door middel van DoS aanvallen

Dos:

- Overmatige netwerkverzoeken of zware rekenprocessen die de server onbruikbaar maken

Repudiation:

- Het ontbreken van legging kan leiden tot ontkenning van acties, bijvoorbeeld een gebruiker kan ontkennen dat hij een wijziging heeft aangebracht.

Spoofing:

- Een aanvaller doet zich voor als een legitieme gebruiker of apparaat om toegang te krijgen tot de server.

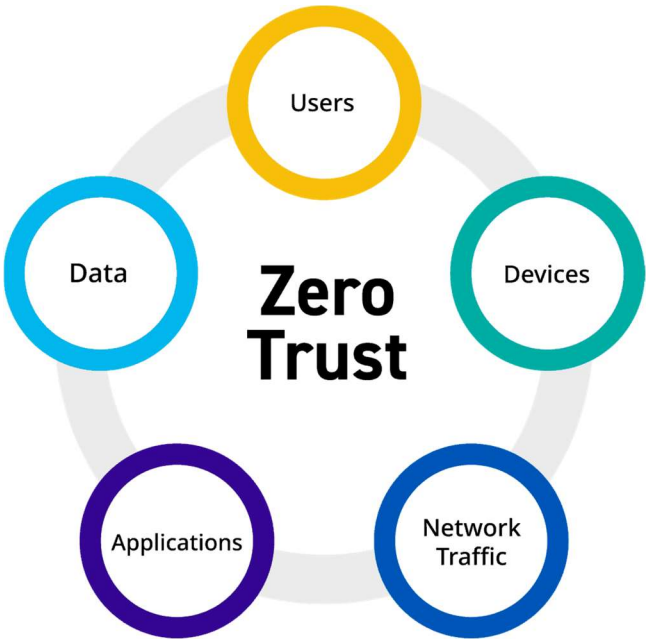
Information Leakage:

- Onbeveiligde configuratiebestanden bevatten gevoelige informatie zoals API-sleutels, wachtwoorden of databasegegevens.

Elevation of Privilege:

- Een aanvaller misbruikt een kwetsbaarheid in de software of configuratie om root-rechten te verkrijgen.

3.7.1 Oplossing PI3 (server) (Zero Trust)



- Users: Gebruik Multi-Factor Authentication (MFA) en sterke wachtwoorden of login uitzetten en enkel en alleen toegang toelaten via ssh key.
  veilige ww langer dan 12 karakters met min 1 hoofdletter + cijfer + symbool = 34 000 jaar voor het kraken van de ww.
  Juiste gebruiker juiste rechten geven zo dat niet iedereen sudo rechten heeft of enkel en alleen toegang tot de benodigde instellingen of data.
- Devices: Sta alleen geregistreerde en veilige apparaten toe toegang te krijgen tot de server. (zoveel hardware matige verbinding als netwerk verbindingen worden geweigerd bv uitzetten van alle usb poorten voor toegang tot data of verbindingen)
- Network Traffic: Gebruik TLS/SSL om gegevens tijdens verzending te beschermen.
- Applications: Laat applicaties of software en scripts alleen toegang hebben tot bronnen die absoluut noodzakelijk zijn.
- Data: Versleutel zowel opgeslagen gegevens als gegevens in transit.
  Beperken van opgeslagen van gevoelige gegevens tot wat nodig is voor operationele doeleinden en visualisatie.

4 Conclusie

We hebben redelijk veel risico’s gevonden zowel hardware- als softwarematige en qua configuratie waarvan er een aantal makkelijk zijn om op te lossen als we een groter budget hadden. De zwakke plek waar men het meeste schade kan aanrichten ligt bij de doos zelf en onze server. Het materiaal waar de doos uit gemaakt is niet veilig genoeg om te gebruiken in het werkveld. Het design is niet veilig want deze kan niet op slot en ook geen temper contact hiervoor voorzien is.
Er zijn ook een aantal risico’s op vlak van het data verlies of de lekkage en Availability aanwezig waar we zelf zo goed als weinig tot niets aan kunnen doen omdat deze worden beheerd door de externe partij bv. de TNT broker en de TNT gateway waardoor het risico aanwezig is op vlak van data lekkage(Information Leakage), verlies van data (Spoofing) en toegankelijkheid tot data (Availability).