MIST Guide - Einführung

Nachfolgend findet sich eine Beschreibung des Mandl IoT Security Testing Guide (MIST-Guide) für Protokolle vor. Dadurch kann eine Bewertung der Sicherheit stattfinden, wodurch auch neue Protokolle einfach und schnell geprüft werden können. Als Grundlage dient ein Bewertungssystem nach Punkten. Sobald ein gewisser Wert erreicht wird folgt eine Empfehlung oder ein Abraten. Dadurch ist es für Entwickler und Entwicklerinnen möglich zu erkennen, welche Schwere eine Sammlung von mehreren Schwachstellen hat und ab wann es ein gravierendes Problem darstellt.

Vorbereitung – Phase 1

Der MIST-Guide begeht nicht den Fehler wie viele Testing Guides davor, indem erst nach einer Entwicklung, ein Test der Sicherheit durchgeführt wird. Sieht man sich den generischen Software Development Life Cycle in Abbildung 1 an, so hat man die verschiedensten Möglichkeiten in den Entwicklungsprozess einzugreifen und dadurch hohe Kosten zu vermeiden, wenn das falsche Protokoll gewählt wurde. Der Ansatz in dem Guide von CSA kommt somit zu tragen. Für den MST-Guide sind zwei Phasen, nämlich Define und Design, von Relevanz. Im ersten Abschnitt werden die Anforderungen definiert. Hierbei ist wichtig zu wissen, was geschützt werden muss (Assets) und was die Software für Forderungen an die Security stellt (Schutzziele).

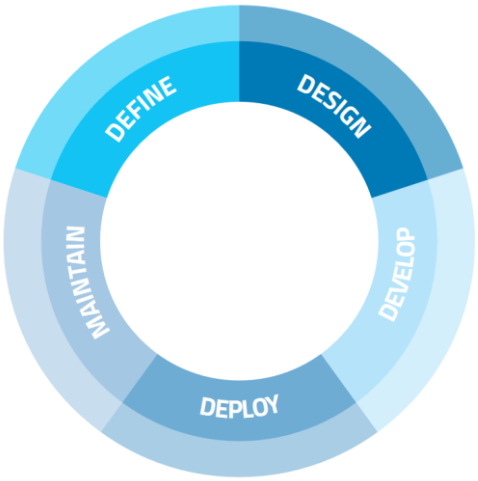

Abbildung 1: Software Development Life Cycle

Dabei muss beachtet werden, dass grundsätzliche Sicherungen enthalten sein müssen und nur eine höhere Sicherheit beschrieben werden muss, also wäre z.B. Non Repudiation ein weiteres Ziel was erfüllt werden muss. Der Guide definiert folgende Ziele als grundsätzlichen Securitystandard für IoT-Protokolle:

- Confidentiality
- Integrity
- Availability
- Authenticity

Die ersten drei Punkte sind auch unter dem Begriff C.I.A. Dreieck bekannt und stellen die wichtigsten Punkte dar, die unter allen Umständen eingehalten werden müssen. Authenticity ist ein zusätzliches Ziel, das in der IoT zwingend erforderlich ist, da die Identität von Nodes zur Kommunikation benötigt wird. So wird erkannt, welches Endgerät angesprochen werden muss. Deswegen ist es zusätzlich angeführt.

Zusammenfassend für die Vorbereitung müssen nun alle Assets definiert werden. Das ist jeglicher Teil, der durch das Protokoll geschützt werden muss und allgemein das Protokoll betreffen. In der Regel sind das zum Beispiel die Daten beim Transport. Im Fall von LoRaWAN würde noch der Schutz der Schlüssel durch das Protokoll selbst hinzukommen und die Zeitslots der Nodes. Zusätzlich ist eine Definition der erforderlichen Schutzziele notwendig. Hierbei sind nur die zusätzlichen Ziele notwendig. Die Grundsätzlichen müssen immer vorhanden sein. Diese sind in diesem Kapitel oberhalb genau definiert. Die Assets werden in einer späteren Phase benötigt, um zu differenzieren, was das Protokoll betrifft, und was das Design des Produkts.

Design – Phase 2

Nachdem die Vorbereitungsphase abgeschlossen ist, hat man eine Übersicht aller Ziele und Assets. Nun muss mit dem Design der Software begonnen werden und somit auch eine Auswahl eines Protokolls stattfinden. Dahingehend muss die Spezifikation über den Aufbau des Protokolls selbst verfügbar sein. Am besten ist auch über den Hintergrund alles bekannt. Also das gesamte Ecosystem des Protokolls. In dem Fall von LoRaWAN ist diese Information notwendig, da eines der definierten Assets die Synchronisation der Nodes betrifft. Man muss zwischen zwei Protokollen unterscheiden, wenn man den Hintergrund analysieren möchte. Einerseits gibt es jene, die selbst verwendet werden können und kein anderes Gerät eine Übertragung oder dergleichen durchführt. Das ist zum Beispiel ZigBee[1], wobei hier die Kommunikation vollständig lokal durchgeführt wird und somit kein anderer betroffen ist. Andererseits gibt es wieder Protokolle, die auch eine Beteiligung Dritter erfordert. Dafür ist nun LoRaWAN ein Beispiel, denn die Kommunikation wird durch ein Netzwerk anderer geleitet und ist deswegen durchaus auch von diesen abhängig. Zusätzlich muss in diesem Schritt geklärt werden, ob das Protokoll für den drahtlosen Einsatz gedacht ist oder kabelgebunden arbeitet. Auch das wird nun festgeschrieben, da es in einer späteren Phase notwendig ist. Man hat also vier Werte definiert:

1. Ist es ein abhängiges IoT-Protokoll
2. Ist es ein unabhängiges IoT-Protokoll
3. Ist es ein drahtloses IoT-Protokoll
4. Ist es ein kabelgebundenes IoT-Protokoll

Bewertung – Phase 3

Nachdem die Auswahl zwischen abhängig und unabhängig erfolgt ist, muss die eigentliche Analyse stattfinden. Dafür muss die Spezifikation genau durchgegangen werden und ein Security Assessment des gerade definierten Designs findet statt. Dieses ist ähnlich zu jenem in Abschnitt 3. Dabei müssen unter anderem folgende Fragen beantwortet werden:

- Ist die Integrität vom Sender bis Empfänger gewahrt?
    - Wird ein aktuelles Signaturverfahren verwendet?
    - Können beteiligte Dritte etwas an der Nachricht unbemerkt verändern?
    - Werden fest definierte Kryptographische Schlüssel verwendet?
- Ist die Vertraulichkeit vom Sender bis Empfänger gewahrt?
    - Kann ein Angreifer Informationen aus der Übertragung gewinnen?
    - Besteht eine Forward–Secrecy?
    - Wird ein aktuelles Verschlüsselungsverfahren verwendet?
- Kann die Verfügbarkeit durch Angreifer beeinträchtigt werden?

[1] https://zigbeealliance.org

    - Kann ein Angriff auf Dritte verantwortlich für einen Ausfall sein?
    - Ist das Protokoll für eine drahtlose Anwendung gedacht?
- Ist die Authentizität der Endgeräte gegeben?
    - Ist es möglich zu erkennen, welches Gerät eine Nachricht übermittelt?
    - Ist die Identität der Geräte eindeutig nachweisbar?
    - Werden aktuelle Authentifizierungsmethoden eingesetzt?

Wenn in Phase 1 ein weiteres Security Ziel festgelegt wurde, so erweitern sich diese Fragen. Zusätzlich muss ein Augenmerk auf alle relevanten Schwachstellen der OWASP Top 10 liegen. Sonst werden nur die vier Grundsatzziele behandelt. Diese wurden im Zuge des Assessments auch durch diese Arbeit beantwortet. Durch das Assessment hat man nun einen Katalog an Schwachstellen, die in dem geplanten Design auftreten. Diese müssen nun, mithilfe der CVSS Scores bewertet werden. Dafür wird ebenfalls die Version 3.1 herangezogen. Andere Versionen funktionieren nicht, da der errechnete Base Score später abweicht. Das liegt daran, dass bei unterschiedlichen Versionen auch unterschiedliche Schemata angewendet werden und somit verschiedene Werte als Ergebnisse erscheinen. Der Guide legt am Ende Grenzen fest, die durch eine andere Berechnung nicht mehr gültig sind. Es wird nochmals hervorgehoben, dass diese Scores normalerweise für Anwendungen verwendet werden. Da das Design eine theoretische Anwendung darstellt, kann man einen Base Score errechnen und dadurch proaktiv Fehler erkennen. Es werden viele Schwachstellen auftreten, wofür das IoT-Protokoll aber nicht verantwortlich ist. Deswegen muss vor der Berechnung, nach dem MIST-Guide Schema, einige davon aussortieren und ermitteln welche Probleme für das Protokoll relevant sind und welche in anderen Bereichen des Produktes auftreten. Dafür kommen nun die in Phase 1 definierten Assets zum Einsatz. Alle Assets, die durch eine gefundene Schwachstelle betroffen sind, betreffen somit das IoT-Protokoll. Diese werden in eine gesonderte Tabelle geschrieben und für die weitere Berechnung verwendet.

Als Ergebnis dieser Phase hat man eine Liste aller Schwachstellen, die für das Protokoll in Frage kommen und deren zugehörigen Base Scores nach dem CVSS v3.1. Diese Liste kann wie folgt aussehen:

Nummer	*Schwachstelle*	*Base Score - v3.1.*	*MIST-Punkte*
1	Mögliche Veränderung des Klartextes am Weg	10.0 - Critical	X
2	Replay Angriff	4.8 - Medium	X
3	Angriffe auf die Synchronisierung der Nodes	5.9 - Medium	X
4	Bit Flipping Angriff	7.5 - High	X

Tabelle 1: Beispiel einer Schachstellenliste für IoT-Protokolle

Berechnung – Phase 4

Nach der Bewertung des Designs und Errechnung der Base Scores muss das Punktesystem dieses Guides verwendet werden, um die Einstufung durchzuführen. Der Ansatz liegt darin, dass es für viele Entwicklerinnen und Entwickler schwer ist mit den Scores etwas anzufangen. Man hat zwar eine farbliche Darstellung mit einem Zahlenwert verbunden, aber das reicht oftmals nicht aus, um eine endgültige Entscheidung zu fällen. Somit bietet der MIST-Guide die Möglichkeit eine Summe aller Probleme zu bilden und durch festgelegte Grenzwerte zu bewerten, ob diese Schwachstellen eine grobe Verletzung der Security darstellen, oder ein Risiko vertretbar ist.

Zur Berechnung der MIST-Guide Punkte muss der Wert des Base Scores nach dem CVSS v3.1 nun durch zehn dividiert werden und immer eine Aufrundung auf eine Kommastelle

stattfinden. Der Grund hierfür ist, dass aufgrund einer höheren Sicherheitsanforderung des MIST-Guides kleine Fehler in der Bewertung durch Entwickler und Entwicklerinnen entgegengewirkt wird. Beim CVSS ist außerdem durch externe Firmen oft eine geringere Bewertung angesetzt, als die Schwachstelle eigentlich hat. Das kommt von Bug Bounty Programmen, wo die Unternehmen weniger Geld als Belohnung bezahlen wollen und oftmals durch einen geringeren Score sparen können. Wenn ein Techniker oder eine Technikerin nun eine Schwachstelle im Netz findet, die auf das Protokoll zutrifft, und diese Werte direkt übernimmt, wird das Endergebnis verfälscht. Als Berechnung folgt nun folgende Formel:

$$MIST - Guide\ Punkte = \left\lceil \frac{Base\ Score}{10} \right\rceil \quad (8)$$

Beispielrechnungen zur Anwendung der Formel (8):

Der Base Score für eine Schwachstelle liegt bei 7,5. Nach Anwendung der Rechnung liegt er bei 0,8, da 7,5/10 = 0,75 und 0,75 aufgerundet auf eine Stelle 0,8 ist.

Der Base Score für eine Schwachstelle liegt bei 6,4. Nach Anwendung der Rechnung liegt er bei 0,7, da 6,4/10 = 0,64 und 0,64 aufgerundet auf eine Stelle 0,7 ist.

Nach der Berechnung der Werte füllt man diese in diesem Beispiel an die Stelle „MIST-Punkte“ in Tabelle 6 ein. Das ist das Ergebnis und wird in Phase 6 weiterverwendet und repräsentiert einen Wert für schlechte Punkte. Am Ende der Arbeit findet sich eine leere Liste, die nochmals den Vorgang des Guides abbildet und in die alle Informationen eingetragen werden.

Sonderregelungen – Phase 5

Da das Problem des Frequenzstörens bei drahtlosen Protokollen immer bestehen wird und ein abhängiges Protokoll immer ausfällt, wenn der Betreiber ein Problem hat, wurden fest definierte Werte gesetzt. Wenn diese Sonderregelung nicht existiert, gibt es von Beginn an, bei jedem abhängigen und drahtlosen Protokoll, ein negatives Ergebnis. Um nun die Schwere auf eine Stufe zu setzen wurden Werte definiert, die das Problem berücksichtigen, aber nicht überbewerten. Schwachstellen, die aufgrund der Abhängigkeit und der Übertragungsart bestehen, müssen mit der nachfolgenden Tabelle ersetzt werden und dürfen nicht entsprechend der CVSS Scores einfließen. In Phase zwei wurde schon abgeklärt, um welche Art von Protokoll es sich handelt. Zusätzlich dazu gibt es noch einen Wert von 0,3, der hinzukommt, wenn eine der Sicherheitsschwachstellen der OWASP Top 10 aufgefunden wird. Der Grund hierbei ist, dass diese Probleme bei sehr vielen IoT Geräten auftauchen und somit auch öfter auf diese getestet wird. Somit sind sie einem höheren Risiko ausgesetzt, was den Zusatzwert rechtfertigt. Dieser Wert von 0,3 ist nur einmal anrechenbar und darf nicht mehrmals addiert werden, auch wenn alle OWASP Top 10 auftreten.

Protokollart	**Punkte**
Abhängiges Protokoll	0,2 Punkte für Availability
Unabhängiges Protokoll	0,0 Punkte zusätzlich
Drahtloses Protokoll	0,2 Punkte für Availability
Kabelgebundenes Protokoll	0.0 Punkte zusätzlich

Tabelle 2: Fest definierte Werte für die jeweilige Protokollart

Summierung – Phase 6

Nach der Errechnung der MIST-Punkte hat die bewertende Person eine Liste aller Schwachstellen und die zugehörigen Werte. Diese müssen nun alle summiert werden. Sollten Sonderregelungen aus Phase 5 auftreten, so müssen auch diese hinzugerechnet werden. Sofern keine zusätzlichen Schutzziele erforderlich sind, gibt es nur vier Schutzziele, die berücksichtig werden müssen. Dafür wird ein Referenzwert von vier definiert. Wenn nun ein weiteres Ziel definiert wird, erscheint ein höherer Sicherheitsbedarf, was diesen Wert um 0,5 erhöht. Sollte zum Beispiel noch Non Repudiation hinzukommen, so steigt der Referenzwert um 0,5 und liegt in Summe somit bei 4,5.

Ob ein Protokoll nun eingesetzt werden kann, wird in Prozent vom Gesamtwert gemessen. Generell wird von einer Verwendung ab 80% abgeraten. Das heißt, dass bei keinen zusätzlichen Zielen der Wert von 3,2 nicht überschritten werden darf. Diese Grenzen und Referenzwerte wurden anhand eigener Beispiele gesetzt. Anderenfalls sollte das Protokoll überarbeitet werden und zusätzlicher Schutz wird benötigt. Ab 50% ist schon Vorsicht geraten, da es gröbere Probleme gibt. Eine Verwendung stellt aber noch keine unmittelbare Gefahr dar. Alles darunter ist in der Regel vertretbar, außer eine Schwachstelle allein hat einen Wert von 1. Dann tritt eine Sonderreglung in Kraft, die davon abrät, das Protokoll zu verwenden. Folgende Tabelle zeigt das endgültige Ergebnis nochmals. Dabei wird vier als Referenzwert genutzt.

Ergebnis	**Empfehlung**
Summe der MIST-Punkte > 80% (3,2)	Von einer Verwendung des Protokolls wird ohne zusätzliche Schutzmaßnahmen abgeraten.
Summe der MIST-Punkte >= 50% (2)	Eine Verwendung ist grundsätzlich möglich. Es wird aber geraten zusätzlichen Schutz einzubauen
Summe der MIST-Punkte < 50% (2)	Eine Verwendung ist ohne Bedenken möglich
Einzelwert einer Schwachstelle in MIST-Punkt = 1	Von einer Verwendung des Protokolls wird ohne zusätzliche Schutzmaßnahmen abgeraten.

Tabelle 3: Ergebniseinstufung bei Referenzwert vier

Anhang 1: MIST-Guide Formulare

In diesem Abschnitt findet sich mehrere Formulare, die alle einen unterschiedlichen Zweck erfüllen und die Analyse unterstützen. Der Ablauf wird am Anfang definiert und zeigt in welcher Reihenfolge ein Formular ausgefüllt werden muss, um den Test sinnvoll durchzuführen.

Ablaufplan

Phase	Schritt	Aufgabenbeschreibung	Anwendbares Formular	Erledigt
Phase 1	1	Definition der Schutzziele.	1.1	☐
	2	Errechnung der Grenzwerte.	1.2	☐
	3	Definition der Assets.	1.3	☐
Phase 2	4	Protokoll Einstufung.	2.1	☐
Phase 3	5	Security Analyse, die alle Schwachstellen des Designs liefert.	-------	☐
	6	Übersicht über alle Schwachstellen wie in Tabelle 2 erstellen.	-------	☐
	7	Schwachstellen mit Assets vergleichen und in neues Formular bringen.	1.3 und 3.1	☐
Phase 4	8	MIST-Punkte errechnen	3.1	☐
Phase 5	9	Protokoll Einstufung nun anhand der Zusatzpunkte summieren.	2.1	☐
Phase 5	10	Alle Summen von 3.1 und 2.1 Summieren	-------	☐
Phase 6	11	Summe mit Formular 1.2 vergleichen und Ergebnis ablesen	1.2	☐

Tabelle 4: Checkliste

Schutzziel Formular 1.1

Mithilfe des Schutzziel Formulars ist es möglich alle grundsätzlichen Schutzziele schon vordefiniert zu finden. Alle weiteren Ziele werden mit dem Wert 0,5 erweitert und nur bei einem Eintrag zur Summe addiert. Standardmäßig ist der Referenzwert bei vier.

Referenzpunkte	Empfehlung
1	Confidentiality
1	Integrity
1	Availability
1	Authenticity
Referenzsumme =	----------

Tabelle 5: Schutzziel Formular 1.1

Errechnung der Grenzen Formular 1.2

Durch die Errechnung der Grenzen ist es möglich am Ende die Bewertung anhand des eigenen Referenzwertes durchzuführen.

MIST-Punkte Ergebnis	Empfehlung
Summe der MIST-Punkte >= 80% ( )	Von einer Verwendung des Protokolls wird ohne zusätzliche Schutzmaßnahmen abgeraten.
Summe der MIST-Punkte >= 50% ( )	Eine Verwendung ist grundsätzlich möglich. Es wird aber geraten zusätzlichen Schutz einzubauen
Summe der MIST-Punkte < 50% ( )	Eine Verwendung ist ohne Bedenken möglich

Tabelle 6: Errechnung der Grenzen Formular 1.2

Asset Definition Formular 1.3

In diesem Formular müssen die Assets definiert werden. Diese werden in Schritt 7 innerhalb der Phase 3 nochmals benötigt.

Assets

Tabelle 7: Asset Definition Formular 1.3

Protokoll Einstufung Formular 2.1

Dieses Formular ermöglicht die Einstufung, ob das IoT-Protokoll abhängig ist, und welcher Verbindungstyp Anwendung findet. Zusätzlich Schwachstellen, die in den OWASP Top 10 gefunden werden, markieren. Bei der Errechnung der Zusatzpunkte gilt darauf zu achten, dass der Wert 0,3 nur einmalig addiert werden darf, auch wenn alle vier Schwachstellen auftreten.

Einstufungen	Check	Zusatzpunkte
Abhängiges Protokoll	☐	0,2
Unabhängiges Protokoll	☐	0,0
Drahtloses Protokoll	☐	0,2
Kabelgebundenes Protokoll	☐	0,0
OWASP TOP 10	**Check**	**Zusatzpunkte**
Weak Guessable, or Hardcoded Passwords	☐	0,3
Insecure Ecosystem Interfaces	☐	0,3
Insecure Data Transfer and Storage	☐	0,3
Insecure Default Settings	☐	0,3
Summe:	----------	

Tabelle 8: Protokoll Einstufung Formular 2.1

CVSS Scores und MIST-Punkte Formular 3.1

Dieses Formular gibt eine Übersicht über alle Schwachstellen und die errechneten MIST-Punkte. Am Ende kann die Summe aller Werte errechnet werden.

Nummer	*Schwachstelle*	*Base Score*	*MIST-Punkte*
1			
2			
3			
4			
5			
6			
7			
Summe:	----------	----------	

Tabelle 9: CVSS Scores und MIST-Punkte Formular 3.1

MIST-Guide Anwendung auf LoRaWAN

Der MIST-Guide für IoT-Protokolle geht davon aus, dass LoRaWAN für eine Entwicklung einer Produktionsumgebung, oder dergleichen, gebraucht wird. Es wird hier kein zusätzliches Schutzziel gewählt, weswegen nur die grundsätzlichen vier definierten Ziele genutzt werden. Das Formular 1.1 ist somit nicht erforderlich und die Grenzwerte bleiben beim Standardwert, wie in Tabelle 3 verzeichnet. Im nächsten Schritt müssen alle Assets definiert werden, um die relevanten Schwachstellen zu erkennen. Als Assets wurden folgende Objekte definiert:

Assets
Übertragene Daten des Protokolls
Synchronisierung des Protokolls
Schutz der Schlüssel durch das Protokoll

Tabelle 10: Definierte Assets für LoRaWAN

Nach der Definition muss die Einstufung erfolgen. Das Protokoll ist abhängig und drahtlos zugleich. Alle gefunden Schwachstellen wie „Frequenzstörer“ oder Dinge, die den Betreiber betreffen, fallen somit weg. Tabelle 10 zeigt das ausgefüllte Formular 2.1. Die Werte für die OWASP Top 10 können erst nach der Security Analyse ausgefüllt werden. Da es aber zu viel Platz verbrauchen würde nochmals das gleiche Formular zu zeigen, werden Sie an dieser Stelle entsprechend der Sicherheitslücken schon angekreuzt und summiert. Durch das mögliche Angriffe auf die Synchronisierung der Nodes und Bit Flipping Angriffe werden zusätzlich zwei der OWASP Top 10 markiert.

Einstufungen	Check	Zusatzpunkte
Abhängiges Protokoll	☒	0,2
Unabhängiges Protokoll	☐	0,0
Drahtloses Protokoll	☒	0,2
Kabelgebundenes Protokoll	☐	0,0
OWASP TOP 10	**Check**	**Zusatzpunkte**
Weak Guessable, or Hardcoded Passwords	☒	0,3
Insecure Ecosystem Interfaces	☒	0,3
Insecure Data Transfer and Storage	☒	0,3
Insecure Default Settings	☐	0,3
Summe:	----------	**0,7**

Tabelle 11: Einstufung des Protokolls für LoRaWAN

Die Summe errechnet sich aus den Werten von 0,4 für die Einstufung (0,2+0,2) und dem Zusatzwert von 0,3 durch die Verletzung der OWASP Top 10. Es wird nochmals angemerkt, dass dieser Wert nur einmal addiert werden darf. Auch wenn jede der vier Schwachstellen auftreten würde. Somit erhält man einen Zusatzwert von 0,7.

Es folgt nun die gesamte Security Analyse des Designs inklusive LoRaWAN. Dadurch lässt sich eine Tabelle aller Schwachstellen erstellen und deren zugehörigen CVSS Scores berechnen (Tabelle 13). Nun folgt die Reduzierung auf die Schwachstellen, die das Protokoll selbst betreffen. Dafür müssen die Assets in Tabelle 10 herangezogen werden. Somit finden sich vier eigentliche Probleme vor, die LoRaWAN betreffen. Tabelle 12 ist nun das ausgefüllte Formular 3.1. Zusätzlich werden alle MIST-Punkte berechnet. Hierbei wird Formel 8 angewendet

Nummer	*Schwachstelle*	*Base Score*	*MIST-Punkte*
1	Informationsgewinnung durch Analyse der Menge und Längen des Ciphertextes	5.3 - Medium	0,6
2	Replay Angriff	4.8 - Medium	0,5
3	Angriffe auf die Synchronisierung der Nodes	5.9 - Medium	0,6
4	Bit Flipping Angriff	7.5 - High	0,8
Summe	----------	----------	**2,5**

Tabelle 12: Relevante Schwachstellen für den Security Guide

Also Summe aller Schwachstellen errechnet in Tabelle 11 somit den Wert 2,5. Nun erfolgt eine Addition aller Schwachstellen Punkte und Sonderwerte. Diese wurden in Tabelle 11 schon errechnet.

$$MIST - WERT = Summe\ aller\ Schwachstellen + Summe\ der\ Zusatzpunkte \quad (9)$$

In Summe erhält man somit ein Ergebnis von 3,2. Das ergibt sich aus Formel 9 (2,5+0,7). Nun wird auf die definierte Sonderregel geprüft. Da in Tabelle 11 keiner der MIST-Punkte genau den Wert 1 trägt, fällt ein direktes Abraten aus und die Bewertung kann anhand Tabelle 8 durchgeführt werden. Dadurch, dass das Ergebnis genau auf 3,2 liegt, erhält man folgendes Ergebnis:

Eine Verwendung ist grundsätzlich möglich. Es wird aber geraten zusätzlichen Schutz einzubauen.

Somit wird grundsätzlich nicht abgeraten LoRaWAN einzusetzen. Dennoch wird empfohlen weitere Maßnahmen einzubauen. Dieser Schritt wird nochmals kurz umrissen indem TLS over LoRaWAN eingebaut wird. Gleicht man nun Tabelle 9 mit Tabelle 4 ab und befindet sich in der Spalte „LoRaWAN 1.0.3 mit LoRaTLS“, so fallen Schwachstellen 4,2 und 1 von Tabelle 11 weg. Zusätzlich sind alle bis auf eine OWASP Top 10 Verbindungen entfernt. Die neuen Werte sind also 0,6 als Summe für alle Schwachstellen und 0,7 als Zusatzpunkte. Dadurch erhält man einen neuen Wert von 1,3. Nach einer erneuten Einstufung nach Tabelle 8, ist dieses Ergebnis sogar unter 2,0 (50% vom Referenzwert 4) und die Empfehlung geht auf eine Verwendung ohne zusätzliche Schutzmaßnahmen über. Das Endergebnis ergibt genau die Einschätzung, die durch diese Arbeit schon anhand der Schlussfolgerungen in den anderen Kapiteln, vorzufinden war. Somit wurden die Bewertungskriterien gut gewählt. Als Future Work ist eine Anwendung auf weitere IoT-Protokolle angedacht.

Tabelle 13: Berechnung der CVSS

Nummer	*Schwachstelle*	*AV*	*AC*	*PR*	*UI*	*S*	*C*	*I*	*A*	*Base Score*
1	Repositories mit Quellcode und Schlüssel im Internet	Network	Low	None	None	Changed	High	High	High	10.0 - Critical
2	Hard gecodete Root – Keys	Physical	High	None	None	Unchanged	High	High	High	6.4 - Medium
3	Unsichere Implementierung der Server	Physical	High	High	None	Changed	High	High	High	6.9 - Medium
4	Ungesicherte Verbindung zwischen Application Server, Join Server und Network Server	Physical	High	High	None	Changed	High	High	High	6.9 - Medium
5	Kontrolle eines Gateways durch ungesicherte Fernwartungssoftware	Local	High	None	None	Changed	None	None	High	5.9 - Medium
6	Schlechte physische Sicherheit der Hardware	Physical	High	None	None	Unchanged	High	High	High	6.4 - Medium
7	Hard gecodete Session Keys	Network	High	High	None	Unchanged	High	High	High	6.6 - Medium
8	Informationsgewinnung durch Analyse der Menge und Längen des Ciphertextes	Network	Low	None	None	Unchanged	Low	None	None	5.3 - Medium
9	Keine Datenfilterung der Eingabewerte durch Nodes	Network	High	High	None	Changed	High	High	High	8.0 - High
10	Störung der Kommunikation zwischen Nodes und Gateways	Network	Low	None	None	Changed	None	None	High	8.6 - High
11	Replay Angriff	Network	High	None	None	Unchanged	None	Low	Low	4.8 - Medium
12	Zeitversetztes senden von Paketen	Network	High	None	None	Unchanged	None	Low	Low	4.8 - Medium
13	Angriffe auf die Synchronisierung der Nodes	Network	High	None	None	Unchanged	None	None	High	5.9 - Medium
14	Bit Flipping Angriff	Local	High	High	None	Changed	High	High	High	7.5 - High
15	Downgrade Angriff	Local	High	None	None	Unchanged	None	None	None	0.0 - None
16	Gültigkeitsdauer der Session Keys	Network	High	High	None	Changed	None	None	None	0.0 - None