Slovenská technická univerzita

Fakulta informatiky a informačných technológií

Tímový projekt

Monitorovanie LoRa IoT zariadení

Inžinierske dielo

Akademický rok:	2022/2023
Vedúci tímu:	Ing. Valach Alexander
Členovia tímu (tím č. 3):	Bc. Gajdošová Dorota Bc. Greguš Michal Bc. Laš Matej Bc. Melicher Adam Bc. Minár Michal Bc. Ondov Adrián

Zoznam skratiek

TCP - protokol riadenia prenosu

IP - internetový protokol

TCP/IP - sada komunikačných protokolov

UDP - používateľský datagramový protokol

LoRa - fyzická rádiokomunikačná technika

SIEM - manažment bezpečnostných informácií a udalostí

ELK - skratka pre projekty Elasticsearch, Logstash, a Kibana

CWE - systém kategorizácie pre hardvérové a softvérové zraniteľnosti

MAC - riadenie prístupu k médiu (*angl. Media Access Control*)

LoRaWAN - LoRa rozľahlá sieť (*angl. Wide Area Network*)

Obsah

1. Úvod

Spolu s narastajúcim počtom IoT zariadení sa zvyšuje aj potreba efektívnych riešení pre ich komunikáciu. LoRa predstavuje takéto riešenie a slúži na komunikáciu medzi IoT zariadeniami pomocou LoRaWAN protokolu. Ide o pomerne novú technológiu, ktorej bezpečnosť doposiaľ nebola detailne analyzovaná a v rámci nášho projektu sa budeme venovať práve tejto problematike. Cieľom práce na projekte je navrhnúť a implementovať riešenie, pomocou ktorého bude možné identifikovať vybrané útoky na sieťovú infraštruktúru a čítať bezpečnostné incidenty priamo zo systému SIEM (Security Information and Event Management).

V rámci dokumentu sme si najprv stanovili ciele na zimný a letný semester. Nasledovala analytická časť, v ktorej sme sa zaoberali samotným protokolom LoRaWAN a jeho aktuálnym stavom zabezpečenia. Návrh a realizácia monitorovania zahŕňa spôsoby detekcie vybraných útokov na infraštruktúru a vymedzuje dáta, ktoré je pre vybrané útoky potrebné logovať ako aj ich prípadný dopad. Vo vlastnom riešení sme pracovali s modulmi hardvér, SIEM, ChirpStack architektúra, koncové zariadenie (firmvér) a Lora Gateway Packet Forwarder, ktorým je venovaná posledná kapitola.

Cieľom dokumentu je čitateľa v skratke oboznámiť s aktuálnou bezpečnostnou situáciou týkajúcou sa protokolu LoRaWAN a následne mu môže slúžiť ako dokumentácia k nami navrhnutému a realizovanému riešeniu.

2. Globálne ciele projektu

2.1. Zimný semester

- Analýza LORA a LORAWAN
- Analýza útokov a spôsobov obrany v LORA prostredí
- Výber určitých druhov útokov a spôsobov ich detekcii
- Spustenie demonštračného kódu na koncovom zariadení
- Spustenie Lora brán pre pripojenie koncových zariadení
- Spustenie Chirpstack softvéru
- Úprava softvéru UDP packet forwarder
- Nastavenie Chirpstack-u na odosielanie logov do SIEM pomocou logstash
- Prepojenie koncových zariadení s bránami a Chirpstack-om

2.2. Letný semester

- Vytvorenie škodlivého kódu pre vybrané útoky realizované na koncové zariadenia
- Vytvorenie pravidiel v SIEM nástroji na detekovanie vybraných útokov na základe ich spôsobu detekcie
- Testovanie pravidiel v SIEM nástroji realizáciou útokov na koncové zariadenia

3. Analýza existujúceho riešenia

LoRa je proprietárna technológia umožňujúca IoT zariadeniam vďaka chirp spread spectrum modulačnej technike komunikovať na veľké vzdialenosti pri zachovaní vysokej miery energetickej efektivity [7]. Samotná technológia LoRa však len definuje spôsob modulácie signálu na fyzickej vrstve a preto je potrebné pri prenose dát používať aj protokoly zodpovedajúce za komunikáciu na vyšších vrstvách RM/OSI modelu. Najpoužívanejším protokolom na MAC vrstve v rámci technológie LoRa je protokol LoRaWAN.

Tento protokol má vo svojom aktuálnom formáte aplikované isté formy zabezpečenia. Jeho najaktuálnejšia verzia je verzia LoRaWAN v1.1, vďaka ktorej boli v protokole aktualizované určité metódy zabezpečenia, ktoré sa v predošlých verziách (verzie 1.0.1, 1.0.2 a 1.0.3) považovali za kritické. Medzi tieto zraniteľnosti patrí nedostatočný manažment kľúčov, slabé šifrovanie, či slabá ochrana voči odchytávaniu a falšovaniu posielaných paketov [12]. Ich mitigácia je často realizovaná pomocou nových typov správ, ktoré si vymieňajú koncové zariadenia so serverami, prípadne pomocou vylepšenia systému kľúčov (konkrétne ich funkcionality, alebo distribúcie). Napriek úpravám, ktoré so sebou priniesla verzia LoRaWAN v1.1, je protokol náchylný na útoky, ktoré môžu narušiť očakávané fungovanie infraštruktúry. Týmto útokom sa bližšie venujeme v kapitole 4.1.

Bezpečnostné opatrenia LoRaWAN protokolu (v1.1) boli taktiež upravené vo fyzickej rovine, a to pridaním nového servera do infraštruktúry. Ide o tzv. *Join server*, ktorý celkovo zjednodušuje procedúru pridávania koncových zariadení do siete. Jeho výhodou je, že dokáže uložiť a spravovať rôzne kľúče, ako napr. koreňové kľúče (*angl. root keys*). Tieto kľúče následne je možné distribuovať z Join servera na potrebný sieťový/aplikačný server. Join server inými slovami zmenšuje hardvérové požiadavky na infraštruktúru (nie je potreba mať viacero priestorov pre kľúče, stačí iba jeden) a podporuje jej celkovú bezpečnosť za pomoci šifrovania [13].

Novým pojmom pre verziu v1.1 je aj *Roaming*. Táto funkcionalita je aplikovaná pomocou typového rozdelenia sieťových serverov - domáci (*angl. home*), preposielací (*angl. forwarding*) a obsluhujúci (*angl. serving*) server. Roaming takto umožňuje pripojenie koncových zariadení do siete, ktorá nie je ich domácou (lokálnou) sieťou [14].

Z bezpečnostného hľadiska má teda protokol LoRaWAN vo verzii v1.1 svoje výhody a nevýhody. Pridaním roamingu sa zlepšila univerzálnosť tohto protokolu, avšak na druhej strane môže dôjsť k zväčšeniu plochy útoku (*angl. attack surface*). Pridaním Join servera sa uľahčila manipulácia s kľúčmi, avšak je potrebné dobre zabezpečiť server pred útokmi. Inými slovami, ide o protokol, ktorý má veľké ambície, avšak stále ho nemôžeme považovať za plne bezpečný. Cieľom nášho projektu je predstaviť jedno z možných riešení zabezpečenia LoRaWAN infraštruktúry za pomoci monitorovania a logovania sieťovej premávky za účelom minimalizovania času potrebného na detekciu útoku. Týmto spôsobom sa vieme proti útokom včas brániť a vieme vytvoriť lepšie podmienky pre preventívne opatrenia.

4. Návrh a realizácia monitorovania

Protokol LoRaWAN je relatívne málo využívaný protokol, ktorý bol vytvorený len nedávno a zatiaľ nie sú dostupné detailné analýzy tohto protokolu z hľadiska bezpečnosti [4]. V rámci našej práce sme sa rozhodli preštudovať daný protokol (verziu 1.1) [7] a tak identifikovať pre nás dôležité informácie a postupy ako napríklad podporované typy správ, spôsob nadviazania spojenia, pripojenia do sieti a prenosu dát medzi koncentrátom a koncovými zariadeniami.

Zvýšenú pozornosť sme venovali bezpečnostným mechanizmom a prvkom protokolu LoRaWAN. Na základe analýzy protokolu a jeho prvkov sa nám počas tímových stretnutí podarilo identifikovať niekoľko zraniteľností v rámci návrhu protokolu LoRaWAN ako aj v dizajne komunikácie v sieťach. Identifikované zraniteľnosti sme sa rozhodli rozdeliť do niekoľkých kategórii pričom ku všetkým sme sa pokúsili priradiť aj útok, pomocou ktorého by mohli byť zneužité [1-7].

Počas tímových stretnutí sme taktiež navrhli spôsob akým by mohli byť jednotlivé útoky detekované a prípadne aj zastavené. Kvôli detekcii útokov bolo potrebné identifikovať polia na logovanie v hlavičkách správ prenášaných protokolom LoRaWAN. V nasledujúcej časti odprezentujeme niekoľko vybraných útokov, pričom charakterizujeme aj ich možné dopady a spôsoby detekcie.

4.1 Vybrané útoky

4.1.1 Jamming [3, 4, 6]

Stručná charakteristika útoku: Pri registrácii do siete metódou aktivácie zariadení bez vopred definovaných kľúčov, ktoré by vyžadovali ich uloženie v pamäti koncového zariadenia sa využíva metóda OTAA (over the air activation). Počas tejto sa využíva DEVNONCE, číslo, ktoré je súčasťou join request správy na generovanie kľúčov. Pričom toto 16 bitové číslo je generované koncovým zariadením náhodne a zároveň sa medzi niekoľkými join requestami nesmie opakovať. V prípade jeho opakovanie server zamedzí pripojeniu koncového zariadenia do siete zahodením prijatého join requestu. Teda v prípade, ak útočník zachytí join request resp. má znalosť o čase, kedy sa štandardne vybrané zariadenie pripája do siete. Je v prípade, že dokáže vysielať na vyššom vysielacom výkone alebo sa nachádza bližšie ku koncentrátoru schopný použiť identifikátor cieľového koncového zariadenia a odoslaním veľkého počtu join requestov pri vyčerpaní väčšej časti rozsahu (ideálne celého rozsahu) DEVNONCE čísel dosiahnuť, že sieťový server po prijatí join requestu od skutočného koncového zariadenia tento request odmietne pre opakujúce sa devNonce číslo. Iný typ jammingu môže spočívať v kontinuálnom vysielaní na dát na vybranej frekvencii s maximálnym vysielacím výkonom, čím môže dôjsť k rušeniu komunikácie ostatných koncových zariadení v okolí, ktoré následkom toho nebudú schopné úspešne odosielať uplink správy ku koncentrátorom resp. prijať downlink správy.

Možné dopady: Úspešná realizácia daného útoku vedie k zamedzeniu prístupu k službe pre koncové zariadenie, ktoré je cieľom útoku a má teda dopad na dostupnosť systému (Availability)

Navrhovaný spôsob realizácie: Úpravou firmvéru vytvoríme koncové zariadenie, ktoré v krátkom čase odošle veľké množstvo join requestov resp. odošle veľké množstvo join requestov pri ktorých bude DEVNONCE číslo sledovať určitý vzor teda vytvorená sekvencia nebude vyzerať náhodne. Prípadne vyčerpáme celý priestor 0 - 2^16 možných DEVNONCE. Vytvoríme koncové zariadenie, ktoré bude kontinuálne vysielať dáta vybranej frekvencii v blízkosti vybraného koncového zariadenia a predpokladáme, že tak dôjde k strate niekoľkých odosielaných správ z koncového zariadenia obete.

CWE identifikátor: CWE-799: Improper Control of Interaction Frequency

Návrh spôsobu detekcie: navrhujeme sledovať počet join requestov odoslaných z koncového zariadenia a ak tento presiahne určitý počet napr. 100 za posledných 24 hodín tak vygenerujeme alert a budeme predpokladať, že ide o replay resp. jamming útok. V prípade budeme disponovať dostatočným množstvom času navrhujeme implementovať KLD (kullback leibler divergence alg.) na analýzu niekoľko posledných prijatých DevNONCE čísiel a pomocou štatistickej analýzy tak vyhodnotiť, či sú skutočne náhodné alebo nie. Taktiež v prípade zariadenia, ktoré má odosielať dáta v pravidelných intervaloch ak nedôjde k prijatia dát navrhujeme vygenerovať alert a následne vykonať fyzickú kontrolu funkčnosti daného koncového zariadenia.

Možné zamedzenie/predchádzanie útoku: zmeny komunikačnej frekvencie koncovými zariadeniami. Relatívne časté zmeny komunikačnej frekvencie koncovými zariadeniami výrazne znižujú schopnosť útočníka odchytiť join request pôvodného koncového zariadenia a tak získať jeho identifikátor pod ktorým následne preposiela rogue join request správy. Ďalším možným spôsobom predchádzania tomuto typu útoku je namiesto odpojenia a pripojenia zariadenia zo siete ho nechať kontinuálne pripojené do siete, čo je možné dosiahnuť pravidelným odosielaním keepalive správ.

Potrebné logovanie polí v hlavičke: Timestamp, DEVNONCE, GWID, NETID, DevAddr, JoinEUI, DevEUI

4.1.2 Replay útok [2, 4]

Stručná charakteristika útoku: Útočník preruší pôvodné spojenie resp. komunikáciu medzi koncovým zariadením a koncentrátorom pričom zároveň zachytí správu odoslanú z koncového zariadenia a túto sa následne pokúsi odoslať znovu. Tento útok je často vykonávaný práve v kombinácii s jammingom, kde útočník odosiela veľké množstvo join requestov s identifikátorom zariadenia, ktorému chce zabrániť pripojenie do sieti.

Možné dopady: Tento útok vie mať v prípade, že je vykonávaný v kombinácii s jamming útokom zabrániť pripojeniu legitímneho zariadenia do siete a tak dosiahnuť zneprístupnenie služby pre vybrané koncové zariadenia. Resp. v prípade úspešného znovuposlania dát (Availability).

Navrhovaný spôsob realizácie: Navrhujeme upraviť LMIC komunikačnú knižnicu vybraného koncového zariadenia tak, aby neakceptovalo joinAccept správy od koncetrátoru a neustále odosielalo join requesty z postupne sa zvyšujúcim DevNonce (number used only once), čo je 16 bitové náhodné číslo ktoré musí byť súčasťou každého join requestu. Toto číslo je dôležité nakoľko je využívané na generovanie kľúčov pri pripojení koncového zariadenia do siete s využitím OTAA metódy aktivácie zariadenia. V prípade znovupoužitia devnonce čísla ako aj v sieťový server neumožní pripojenie koncového zariadenia dos sieti a zahodí daný join request. Druhý možný spôsob realizácie je upraviť zdrojový kód tak aby koncové zariadenie pri odosielaní dátových správ odoslalo tieto správy s nevhodným framecounterom avšak podľa dokumentácie by tieto mali byť automaticky zahodené na sieťovom serveri a preto by sme ich neboli schopný v dostatočnej miere logovať.

CWE identifikátor: CWE-323: Reusing a Nonce, Key Pair in Encryption

Návrh spôsobu detekcie: navrhujeme sledovať počet join requestov odoslaných z koncového zariadenia a ak tento presiahne určitý počet napr. 100 za posledných 24 hodín tak vygenerujeme alert a budeme predpokladať, že ide o replay resp. jamming útok. V prípade budeme disponovať dostatočným množstvom času navrhujeme implementovať KLD (kullback leibler divergence alg.) na analýzu niekoľko posledných prijatých DevNONCE čísiel a pomocou štatistickej analýzy tak vyhodnotiť, či sú skutočne náhodné alebo nie. Taktiež v prípade ak budeme registrovať prijatie join requestu s identifikátorom zariadenia, ktoré už je pripojené v sieti, tak je možné predpokladať, že tieto requesty sú odoslané z rogue koncového zariadenia, ktoré sa snaží vyčerpať použiteľné DEVNONCE pre dané koncové zariadenie a tak v prípade potreby znemožniť jeho opätovné pripojenie do siete. Prípadne ako sofistikovaný spôsob detekcie v prípade statických koncových zariadení je možné na základe analýzy hodnôt RSSI a SNR správ prijatých z koncového zariadenia prostredníctvom niekoľkých koncentrátorov trianguláciu určiť približnú polohu koncového zariadenia odosielajúceho join requesty a v prípade ak sa poloha tohto zariadenia nezhoduje s polohou na ktorej by sa malo nachádzať zariadenie s týmto identifikátorom môže to byť do istej miery indikátorom kompromitácie.

Možné zamedzenie/predchádzanie útoku: Tomuto útoku nie je možné predchádzať nakoľko nevieme ovplyvniť a ani zabrániť rogue koncovým zariadeniam odosielať veľký počet falošných join requestov. Avšak relatívne časté zmeny komunikačnej frekvencie koncovými zariadeniami výrazne znižujú schopnosť útočníka odchytiť join request pôvodného koncového zariadenia a tak získať jeho identifikátor pod ktorým následne preposiela rogue join request správy.

Potrebné logovanie polí v hlavičke: Timestamp**,** FrameCNT, DevNONCE, RSSI, SNR

4.1.3 Nedovolený presun brány (zmena polohy brány) [6, 7]

Stručná charakteristika útoku: útočník presunie koncentrátor do inej lokality, pričom ho naďalej ponechá pripojený do siete, čím spôsobí, že napriek tomu, že sa toto zariadenie bude javiť ako bezproblémové a fungujúce v rámci sieťovej infraštruktúry tak z dôvodu novej

polohe je možné, že dané zariadenie už nebude schopné pokrývať spojením geografickú oblasť pre ktorú bolo určené.

Možné dopady: odstránenie resp. presun brány z vybranej lokality môže viesť k degradácii služby v danej lokalite, čo má za následok dopad na dostupnosť služby (Availability)

Navrhovaný spôsob realizácie: Prenos brány do inej fyzickej lokality a jej následné opätovné pripojenie do siete v novej lokalite.

CWE identifikátor: CWE-1263: Improper Physical Access Control

Návrh spôsobu detekcie: Prostredníctvom údajov latitude a longtitude, ktoré posiela brána v rámci polí LAT a LNG hlavičiek odosielaných správ na sieťový server. Pomocou týchto polí možno sledovať zemepisnú pozícii brány v čase a v prípade zmeny hodnôt budeme schopný spoľahlivo identifikovať presun brány resp. nedovolený presun brany.
Možné zamedzenie/predchádzanie útoku: Zabezpečenie bezpečného umiestnenia jednotlivých koncentrátorov. Teda zabezpečenie fyzickej ochrany pred neoprávneným prístupom resp. minimálne umiestnenie brány na zložito prístupných miestach.

Potrebné logovanie polí v hlavičke: Timestamp, LAT, LNG

4.1.4 Kompromitácia kľúčov (komunikačných) na sieťovom serveri

Stručná charakteristika útoku: V tomto smere si vieme predstaviť niekoľko vektorov útoku. Ako napríklad modifikácia daných kľúčov, ich nedovolené kopírovania a poskytnutie neoprávneným osobám, odstránenie kľúčov.

Možné dopady: úspešná realizácia daného útoku vedie k ohrozeniu dôvernosti odosielaných dát. Zároveň v istých prípadoch môže viesť k zamedzeniu funkčnosti služby. (Confidentiality, Availability)

Navrhovaný spôsob realizácie: zmazanie prípadne úprava kľúčov na sieťovom serveri.

CWE identifikátor (možné prípady): CWE-732: Incorrect Permission Assignment for Critical Resource; CWE-284: Improper Access Control

Návrh spôsobu detekcie: Detegovať daný útok navrhujeme implementáciou systému FIM (file integrity monitoring) nad súbormi obsahujúcimi komunikačné kľúče. Tento bude schopný v prípade neoprávnenej zmeny daného súboru vygenerovať alert systémovým administrátorom, ktorý následne môžu pristúpiť v vykonaniu nápravných opatrení.

Možné zamedzenie/predchádzanie útoku: V rámci proaktívnych opatrení na predchádzanie útokom navrhujeme implementovať vhodnú prístupovú politiku spolu v zmysle politiky

minimálnych oprávnení a tak zabezpečiť, aby mali možnosť akejkoľvek manipulácie (čítanie aj zápis) so súbormi obsahujúcimi komunikačné kľúče len oprávnený používatelia v ideálnom prípade obmedzené množstvo serverových administrátorov. Zároveň navrhujeme logovať všetky prístupy k daným súborom (čítania aj zápis, zmeny) aby bolo možné skontrolovať všetky činnosti vykonávané nad týmito súbormi a v prípade potreby ich auditovať.

Potrebné logovanie údajov: Timestamp, správa/alert z file integrity checker aplikácie, prístupy k daným súborom a ich modifikácie

4.1.5 Man in the middle medzi sieťovým serverom a aplikačným serverom

Stručná charakteristika útoku: útočník zachytáva komunikáciu medzi sieťovým serverom a aplikačným serverom s cieľom zistiť obsah dát odoslaných z koncového zariadenia prípadne zmeniť ich obsah. Toto by napr. bolo možné, ak by zmenil obsah poľa framepayload na localhoste lora.fiit.stuba.sk
Možné dopady: úspešné prevedenie útoku má za následok získanie prístupu k citlivým údajom, ktoré nie sú prenášané v šifrovanej podobe resp. za istých okolností umožňuje dokonca aj ich manipuláciu a teda má dopad na dôvernosť a integritu dát.
(Integrity, Confidentiality)

Navrhovaný spôsob realizácie:

CWE identifikátor: žiadne konkrétne CWE

Návrh spôsobu detekcie: tento typ útoku neplánujeme detegovať v systéme SIEM.

Možné zamedzenie/predchádzanie útoku: Pridanie vlastného MIC nad dáta odoslané medzi sieťovým serverom a aplikačným serverom. V prípade potreby možný prenos dát medzi sieťovým serverom a aplikačným serverom v šifrovanej podobe, pričom dáta by boli aj podpísané kryptografickým podpisom.

Potrebné logovanie údajov: Timestamp, vlastné MIC (message integrity check)

4.1.6 Porušenie vysielacích regulácii koncovým zariadením [10, 11]

Stručná charakteristika útoku: Na koncové zariadenie je nahratý firmvér ktorý nesprávne kontroluje dodržiavanie pracovného cyklu (maximálneho vysielacieho času) koncového zariadenia, ktoré následne nadmerne zaťažuje komunikačnú frekvenciu a to dokonca v niektorých prípadoch nad rámec platnej legislatívy regulujúcej rádiovú komunikáciu. Ďalším možným problémom z tejto kategórie je odosielanie dát na inej vysielacej frekvencii ako je vysielacia frekvencia povolená v rámci legislatívy o rádiovej komunikácii v danom regióne.

Možné dopady: V prípade nadmerného vysielania jedného koncového zariadenia môže dôjsť k rušeniu komunikácie iných koncových zariadení, čo môže mať za následok zneprístupnenie služby teda dopad na jej dostupnosť. (Availability)

Navrhovaný spôsob realizácie: Navrhujeme zámerne nahrať na vybrané koncové zariadenia chybný firmvér, ktorý im umožní vysielať dáta kontinuálne bez dodržovania platných obmedzení vzťahujúcich sa na maximálny vysielací čas. Ďalej navrhujeme zámerne nahrať na vybrané koncové zariadenia chybný firmvér, ktorý im umožní vysielať dáta na vysielacej frekvencii, ktorá nie je povolená v rámci SR, kde je rádiová komunikácia pre technológiu LoRa regulovaná komunikačným plánom EU433. Pričom tieto zmeny plánujeme vykonať vhodnou úpravou zdrojového kódu komunikačnej knižnice LMIC, ktorá tvorí súčasť firmvéru koncových zariadení využívaného na odosielanie a prijímanie dát.

CWE identifikátor: žiadne konkrétne CWE

Návrh spôsobu detekcie: Daný útok navrhujeme detegovať v rámci systému SIEM na základe pravidla, ktoré porovná vysielaciu frekvenciu koncového zariadenia voči zoznamu povolených vysielacích frekvencii pre daný región a následne vyhodnotí súlad s platnými vysielacími pravidlami. Ďalej budeme po prijatí dát z koncového zariadenia kontrolovať množstvo prijatých dát z daného koncového zariadenia za posledných 24 a toto množstvo vzhľadom na komunikačnú rýchlosť koncového zariadenia prepočítame na vysielací čas a ten porovnáme s maximálnym možným vysielacím a opäť sa pokúsime vyhodnotiť, či sú v prípade komunikácie z daného koncového zariadenia dodržané požiadavky na maximálnu možnú dĺžku komunikácie.

Možné zamedzenie/predchádzanie útoku: V tomto prípade v podstate neexistuje spôsob zabránenia danému útoku okrem fyzického znefunkčnenia koncového zariadenia vysielajúceho nad rámec platných regulácii. K lokalizácii by bolo možné prispieť na základe hodnôt RSSI a SNR správ prijatých z daného koncového zariadenia rôznymi koncrentrátormi v okolí a tak približne pomocou triangulácie identifikovať jeho polohu čo môže do istej miery uľahčiť jeho lokalizáciu a umožniť jeho znefunkčnenie avšak toto považuje ako miernu nadprácu a preto to nebudeme realizovať. My ako opatrenie navrhujeme odpojiť dané zariadenie z našej siete a tak mu znemožniť odosielané dáta prijať na koncrentrátore resp. sieťovom serveri pokiaľ majiteľ nevykoná nápravu firmvéru.

Potrebné logovanie polí v hlavičke: Timestamp, Channel, FREQ, SF, Payload size, Data rate

DataRate	Modulation	SF	BW	bit/s
0	LoRa	12	125	250
1	LoRa	11	125	440
2	LoRa	10	125	980
3	LoRa	9	125	1’760
4	LoRa	8	125	3’125
5	LoRa	7	125	5’470
6	LoRa	7	250	11’000
7	FSK 50 kbps			50’000

4.1.7 Service degradation + anomálie v dátových hodnotách [4, 5]

Stručná charakteristika útoku: napríklad manipuláciou prostredia v okolí koncového zariadenia napr. ak ide o meracie zariadenie teploty prípadne splodín môže útočník dosiahnuť odoslanie nesprávnych dát z koncového zariadenia. Ďalej umiestnením blokujúceho objektu napr. veľký kus kovu alebo betónu do blízkeho okolia koncového zariadenia možno ovplyvniť schopnosť koncového zariadenia úspešne vysielať dáta ku koncentrátorom.

Možné dopady: úspešná realizácia daného útoku môže viesť k odoslaniu chybných dát z koncového zariadenia čo má dopad na integritu dát. Obmedzenie schopnosti koncového zariadenia vysielať dáta ku koncentrátorom s dostatočne silným signálom pre ich prijatie môže spôsobiť výpadok služby a jej následné zneprístupnenie teda môže mať dopad na dostupnosť (Integrity, Availabilty)

Navrhovaný spôsob realizácie: Do okolia koncového zariadenia budeme postupne umiestňovať plech pomocou ktorého budeme blokovať signály odosielaného z koncového zariadenia. V prípade ak sa nám podarí získať prístup aj ku koncovému zariadeniu so senzorom merajúcim hodnotu určitej veličiny pokúsime sa nejakým spôsobom manipulovať daný senzor tak aby zaznamenal chybné dáta, ktoré budú následne odoslané koncovým zariadením.

CWE identifikátor: žiadne konkrétne CWE

Návrh spôsobu detekcie: V rámci systému SIEM budeme detekovať na základe hodnôt RSSI a SNR degradáciu signálu. V prípade anomálii v dátových hodnotách navrhujeme vytvoriť model detekcii anomálii v dátach na základe predchádzajúcich hodnôt (báza) a taktiež v prípade viacerých senzorov merajúcich hodnotu rovnakej veličiny korelovať hodnotu tejto veličiny medzi jednotlivými senzormi.

Možné zamedzenie/predchádzanie útoku: fyzická kontrola okolia koncových zariadení. Fyzická kontrola stavu a správneho fungovania senzorov koncových zariadení ako aj koncových zariadení ako celku.

Potrebné logovanie polí v hlavičke: Timestamp, RSSI, SNR (až na sieťovom serveri aby sme mali deduplikované dáta), SF, Payload(aplikačný server resp. až dešifrovaný payload)

4.1.8 Bit flipping [1, 4, 5]

Stručná charakteristika útoku: je to typ útoku, pri ktorom je možné zmeniť špecifické časti (bity) kryptogramu bez znalosti dešifrovacieho kľúču. Prevedenie tohto útoku umožňuje útočníkovi znehodnotiť odoslané dáta. Avšak na zmysluplné využitie útoku okrem dosiahnutia DOS útoku je nutná znalosť štruktúry plaintextu ako aj vedomosť o tom, kde v rámci kryptogramu sa nachádzajú jednotlivé bity plaintextu, tak aby ich bolo možné meniť zmysluplným spôsobom.

Možné dopady: v prípade úspešnej realizácie útoku môže dôjsť k zmene dát a teda dopadu na ich obsah resp. integritu. (Integrity)

Navrhovaný spôsob realizácie: vzhľadom na fakt, že v rámci knižnice LMIC, ktorú plánujeme využívať v rámci firmvéru koncových zaridení je využívaný šifrovací algoritmus AES-128, v rámci ktorého nedochádza k priamemu mapovaniu bitov vstupu na bity výstupu resp. ani nie je možné jednoznačne určiť ktorý bit vstupu zodpovedá vybranému výstupnému bitu preto nie je možné daný útok realizovať.

CWE identifikátor: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking

Návrh spôsobu detekcie: anomálie v dátových hodnotách. Nevhodný formát prijatých dát z koncového zariadenia napr. zmenené znaky v texte a tak podobne.

Možné zamedzenie/predchádzanie útoku: útoku nie je možné zamedziť. Avšak využitím šifrovacieho algoritmu v ktorom neexistuje priame mapovanie medzi bitmi vstupu a bitmi výstupu je možné dosiahnuť jeho efektívnu zmysluplnú neaplikovateľnosť pre útočníka. Taktiež možno implementovať dodatočný vlastný CRC alogritmus prípadne MIC mechanizmus, nad payloadom, ktorý bude jeho súčasťou a eventuálne by mohol byť využitý aj na detegovanie daného útoku.

Potrebné logovanie polí v hlavičke: Timestamp, MIC, CRC

Po vykonaní analýzi možných útokov na LoRa sieť, ako aj navrhovaných metódach je detekcie sme dospeli k záveru, že súčasný stav UDP packet forwarder-u ako aj chip stack-u nevykonávaná dostatočné logovanie a sledovanie nami zvolených metrík a polí hlavičiek potrebné pre spoľahlivú detekciu identifikovaných útokov na LoRa infraštruktúru. Preto sme sa rozhodli upraviť zdrojový kód UDP packet forwarder-u ako aj chirpstacku tak aby sme boli schopný potrebné údaje logovať a následne agregovať v rámci systému SIEM a v ňom s využitím vytvorených pravidiel identifikovať škodlivú aktivitu alebo premávku v rámci LoRa infraštruktúry. V nasledujúcej časti popisuje zmeny vykonané v rámci zdrojového kódu.

Pričom sme identifikovali nasledovné polia resp. údaje, ktorých hodnoty musia byť zaznamenané a postúpené na ďalšiu analýzu do systému SIEM: **DEVNONCE, GWID, NETID, Device ID, JoinEUI, DevEUI, Frame Counter, LAT, LNG, FREQ, SF, Payload size, RSSI, SNR, MIC, Timestamp**

SEM TREBA DOPISAT CO SA UPRAVILO NA CHIRPSTACKU A UDP PACKETe resp. ako sme dosiahli logovanie a zobrazenie tých dát v sieme, ktoré sme zistili, že chceme a potrebujeme logovať. pripadne screenshoty zo siemu

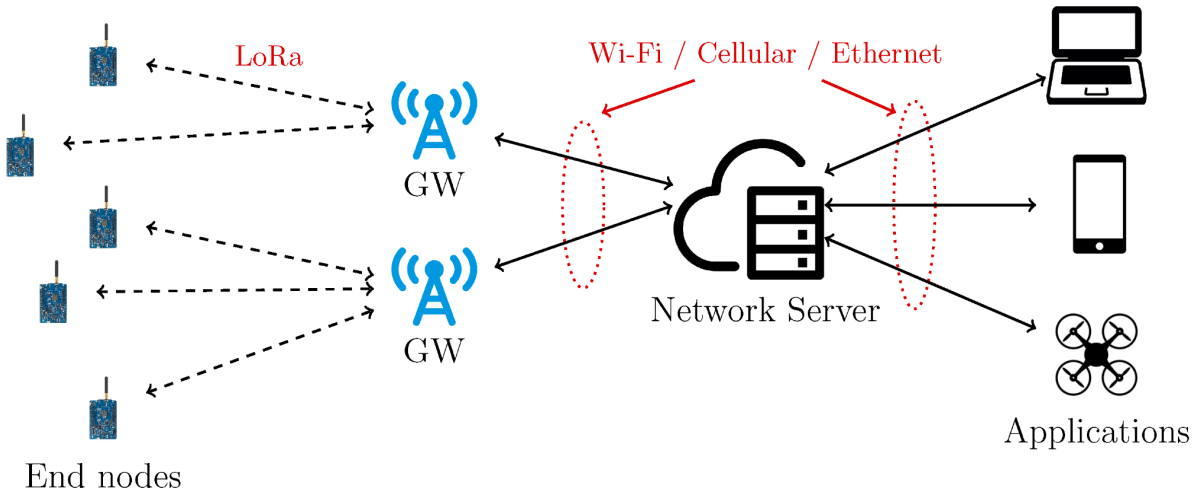
5. Moduly

V nasledujúcej kapitole sú uvedené hlavné moduly použité v projekte.

5.1 Hardvér

Pre testovanie a preukázanie funkčnosti jednotlivých monitorovacích systémov navrhovaných v projekte, sú potrebné 3 rôzne typy hardvéru.

1. Koncové zariadenie - vysiela informácie z prostredia aplikačnému serveru,
2. Lora Brána - prijíma dáta z koncových zariadení a posiela na hlavný server,
3. Server - spracováva a obsahuje aplikácie postavené na informáciach, ktoré koncové zariadenia odosielajú.



Obrázok 1: Architektúra LORAWAN sietí

5.2 SIEM

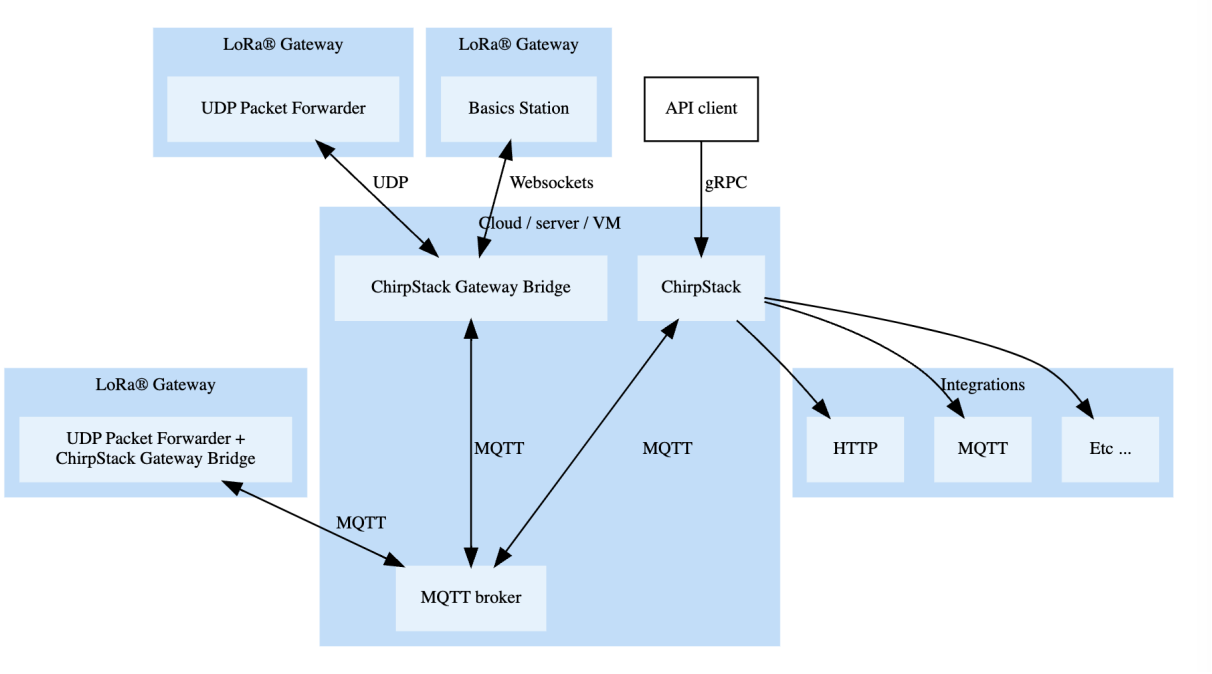
https://www.elastic.co/what-is/elk-stack

SIEM je monitorovací a auditný nástroj, ktorý používa IT bezpečnostný tím na monitorovanie relevantných informácii z IT infraštruktúry. Vzhľadom na charakter projektu je použitý nástroj ELK pozostávajúci z viacerých aplikácii, ktoré v kombinácii tvoria open-source SIEM riešenie.

5.3 ChirpStack architektúra

https://www.chirpstack.io/

Server použitý na spracovanie premávky z koncových zariadení je, podobne ako v prípade SIEM, open-source riešenie ChirpStack. Uvedený server slúži ako LoRAWAN sieťový server, s možnosťami pridávania a odoberania koncových zariadení.



Obrázok 2: Architektúra Chirpstack softvéru

5.4 Koncové zariadenie (firmvér)

Koncové zariadenie bude spomínané TTGO LoRa 32. Jadro skriptu na odosielanie rámcov je použité z otvoreného repozitára (https://github.com/lnlp/LMIC-node), kde je funkčný kód, ktorý slúži ako príkladné LoRa koncové zariadenie. Používa Arduino framework, knižnicu LMIC LoRaWAN a PlatformIO. Je tam vytvorený priestor pre používateľský kód, kde je možné definovať čo bude zariadenie robiť podľa toho na čo má slúžiť.

Do každého zariadenia je so skriptom potrebné nahrať aj OTAA kľúč a identifikátor zariadenia, podľa nastavenia v Chirpstacku. Bez toho Chirpstack nevie identifikovať koncové zariadenie a spracovávať jeho komunikáciu. Pred odoslaním každého rámca zo zariadenia prebieha šifrovanie dát pomocou jeho relačných kľúčov. V Chirpstacku je pridaný kód na dešifrovanie, aby posielané dáta mohli byť analyzované v SIEM-e.

Úlohou skriptu je generovanie a posielanie dát, aby sme mohli simulovať útoky. Samotný obsah dát nebude hrať veľkú úlohu, takže budeme posielať len nasledovné údaje:

- nameranú teplotu zo senzorov,

- číslo, ktoré bude inkrementované každým odoslaním (mod. 10 000),
- statický string “Hello from LoRa device!”.

Zariadenia nebudú priamo do SIEM-u posielať nič, o to sa postará Chirpstack.

5.5 Lora Gateway Packet Forwarder

https://github.com/Lora-net/packet_forwarder

Ako je možné vidieť na obrázku s Chirpstack architektúrou, tak jedným z hlavných častí funkčného odosielania dát je UDP Packet Forwarder. Spomenutý softvér slúži na posielanie správ prijatých na LORA rozhraní, zmeniť kódovanie a pomocou TCP/IP architektúry odoslať serveru.

6. Implementácia

6.1 Realizované útoky

V rámci implementácie sa nám podarilo zrealizovať útoky jamming, porušenie vysielacích regulácií, nedovolený presun brány, kompromitácia kľúčov na sieťovom serveri a anomálie v dátových hodnotách. Na každý z úspešne zrealizovaných útokov sme na úrovni SIEMu napísali pravidlo, detekujúce prebiehajúci útok. Ich implementácia a celkový priebeh bude popísaný nižšie.

Zvyšné útoky sa nám nepodarilo zrealizovať z nasledujúcich dôvodov:

- replay - z dôvodu, že realizácia bola príliš náročná a ChirpStack spolu s knižnicou majú mechanizmy blokujúce tento typ útoku,
- man in the middle - z dôvodu, že ChirpStack integruje funkcionality sieťového aj aplikačného servera a tak nebola možná simulácia tohto útoku,
- bit flipping - z dôvodu, že v knižinici je používaný AES šifrovací algoritmus a keďže v ňom nie je možné priame mapovanie medzi bitmi šifrovaného a otvoreného textu tak sa nedá sa odhadnúť, ktoré bity flipnúť.

6.1.5 Jamming

Konfigurácia: V rámci našej implementácie bežne kontrolujeme počet odosielaných správ za vybrané obdobie. Tento konkrétny útok má za následok zníženie kvality až zneprístupnenie služby spôsobený nedostatkom doručených správ. Takýto útok vieme simulovať rôznymi

spôsobmi, kde budeme rušiť signál a správy sa nebudú môcť odoslať v normálnom počte (okolo 2880 správ).

Zachytenie: Pravidlo je vytvorené tak aby kontrolovalo počet správ každých 24 hodín za posledných 24 hodín a pokiaľ tento počet zoskupených na základe identifikátora zariadenia bude menší ako 2700 tak sa vygeneruje upozornenie.

– text pravidla –

Tento útok sme simulovali tak, že sme presunuli zariadenie mimo dosahu signálu do vzdialenej miestnosti. Upozornenie bolo vygenerované, pretože počet správ bol iba XX správ a je zobrazené na obrázku nižšie. Správy boli odosielané z koncového zariadenia číslo XX.

– obrazok alertu –

6.1.2 Nedovolený presun brány

Konfigurácia: Brána ma GPS modul, pri čom polohu odosiela na ChirpStack. V prípade, že dôjde k zmene polohy je vygenerované upozornenie. Poloha je reprezentovaná parametrami “lan” a “lot” ako latitude (zemepisná šírka) a longitude (zemepisná dĺžka).

Zachytenie: Pravidlo je implementované tak, aby sa pri zmene zaregistrovanej polohy (lat - 49.153 a lon - 17.072) vygenerovalo upozornenie. Poloha brány sa kontroluje každú minútu a kontroluje sa poloha za posledných 90 sekúnd.

Pôvodná poloha brány bola zmenená na lat - 48.153419494628906 a lon - 17.071544647216797. Obsah správy so zmenenou polohou je zobrazený nižšie.

6.1.3 Kompromitácia kľúčov

Konfigurácia: ChirpStack používa na ukladanie citlivých údajov databázu Redis. V nej sú uložené komunikačné kľúče. Útok je zameraný na to, že ak k databáze pristúpi nová IP adresa (doteraz nepoznaná) vygeneruje sa v SIEMe upozornenie. Cieľom je zabrániť aby k databáze nepristupoval nikto iný okrem hlavného stroja (ChirpStack).

Zachytenie: Pravidlo každú minútu kontroluje prístupy za posledných 90 sekúnd. Kontrolovaný parameter je “ip.keyword”. Pokiaľ je hodnota tohto parametru nová bude vygenerované upozornenie.

{"id":"5321df10-dc70-11ed-a1ab-5dee06af8c3c","updated_at":"2023-04-16T19:53:33.921Z","updated_by":"elastic","created_at":"2023-04-16T16:04:11.659Z","creat

ed_by":"elastic","name":"KEYS","tags":["private-keys"],"interval":"1m","enabled":true,"description":"Watch for Private key reads from Redis database on chirpstack","risk_score":21,"severity":"low","license":"","output_index":"","meta":{"from":"30s","kibana_siem_app_url":"http://10.0.130.124:5601/app/security"},"author":[],"false_positives":[],"from":"now-90s","rule_id":"d203f28c-c568-4da7-bd1e-a36350d23690","max_signals":100,"risk_score_mapping":[],"severity_mapping":[],"threat":[],"to":"now","references":[],"version":3,"exceptions_list":[],"immutable":false,"related_integrations":[],"required_fields":[],"setup":"","type":"new_terms","query":"*","new_terms_fields":["data.ip.keyword"],"history_window_start":"now-1d","filters":[],"language":"kuery","data_view_id":"90ef18c3-04a0-412f-b19f-f51e27273074","throttle":"rule","actions":[{"group":"default","id":"6d4d7dc0-cd31-11ed-a1ab-5dee06af8c3c","params":{"documents":[{"name":"private_key"}]},"action_type_id":".index"}]}

{"exported_count":1,"exported_rules_count":1,"missing_rules":[],"missing_rules_count":0,"exported_exception_list_count":0,"exported_exception_list_item_count":0,"missing_exception_list_item_count":0,"missing_exception_list_items":[],"missing_exception_lists":[],"missing_exception_lists_count":0}

Na obrázku je zobrazené upozornenie z prípadu, kedy sme sa pokúsili k databáze pristúpiť zo súkromného stroja s neznámou IP adresou 172.29.0.1.

6.1.1 Porušenie vysielacích regulácií

Konfigurácia: V tejto časti sme sa zamerali na zvýšenie frekvencie odosielania správ z koncového zariadenia tak aby sme navýšili počet join requestov odoslaných za posledných 24 hodín. Počet sa zvýšil niekoľkonásobne, keďže interval sa z 30 sekúnd zmenšil na 15 sekúnd. To znamená, že bežne bolo odoslaných okolo 2880 správ za 24 hodín a my sme pri realizácii útoku odoslali približne až 5760 správ z koncového zariadenia. Na to aby sme tento útok vedeli zrealizovať bolo potrebné upraviť kód knižnice a znovu ho nahrať na vybrané koncové zariadenie. Následne nám už len zostávalo vytvoriť pravidlo v SIEMe a overiť priebeh útoku.

Zachytenie: Detekcia tohto útoku je možná vďaka nižšie uvedenému pravidlu. Uvedené pravidlo kontroluje každých 24 hodín počet odoslaných správ za posledných 24 hodín, ktoré majú rovnaký atribút identifikátora zariadenia. Ak tento počet presahuje štandardne odoslaných 3000 správ, vygeneruje upozornenie.

Na obrázku môžeme vidieť ako vyzerá zachytenie útoku tohto typu spolu so štatistikami a počtami odoslaných správ s rovnakým identifikátorom zariadenia za posledných 24 hodín z koncového zariadenia číslo 2.

6.1.4 Anomálie v dátových hodnotách

Konfigurácia: Po prezretí správ z dlhšieho časového obdobia sme zistili, že LoRa koncové zariadenie v rámci korektnej bežnej prevádzky posielalo správy s teplotou nie vyššou ako 26 stupňov (štandardne išlo o 23 alebo 26 stupňov). My sme sa pri realizácii tohto útoku zamerali na to aby vybrané koncové zariadenie posielalo správy s niekoľkonásobne vyššou hodnotou pre premennú teploty. Konkrétne išlo o hodnotu 99 stupňov. Na to aby sme túto chybu spôsobili bolo nutné prepísať kód koncového zariadenia, v ktorom sme upravovali pole "temp" a následne opätovne nahrať tento upravený kód na vybrané zariadenie.

Zachytenie: Na detekciu tohto útoku slúži v rámci SIEMu nasledovné pravidlo:

Toto pravidlo kontroluje hodnotu premennej teploty a ak nespĺňa požadované podmienky, teda nie je vyššia ako 15 a nižšia ako 35, tak vygeneruje upozornenie.

Na obrázku môžeme vidieť ako vyzerá zachytenie takéhoto útoku a aj detaily škodlivej správy odosielanej koncovým zariadením číslo 5.

Bibliografia

1. JungWoon Lee, DongYeop Hwang, JiHong Park and Ki-Hyung Kim, "Risk analysis and countermeasure for bit-flipping attack in LoRaWAN," *2017 International Conference on Information Networking (ICOIN)*, 2017, pp. 549-551, doi: 10.1109/ICOIN.2017.7899554.
2. SeungJae Na, DongYeop Hwang, WoonSeob Shin and Ki-Hyung Kim, "Scenario and countermeasure for replay attack using join request messages in LoRaWAN," *2017 International Conference on Information Networking (ICOIN)*, 2017, pp. 718-720, doi: 10.1109/ICOIN.2017.7899580.
3. S. M. Danish, A. Nasir, H. K. Qureshi, A. B. Ashfaq, S. Mumtaz and J. Rodriguez, "Network Intrusion Detection System for Jamming Attack in LoRaWAN Join Procedure," *2018 IEEE International Conference on Communications (ICC)*, 2018, pp. 1-6, doi: 10.1109/ICC.2018.8422721.
4. X. Yang, E. Karampatzakis, C. Doerr and F. Kuipers, "Security Vulnerabilities in LoRaWAN," *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2018, pp. 129-140, doi: 10.1109/IoTDI.2018.00022.
5. N. Yakin, M. Zhitkov, A. Chernikov and P. Pepelyaev, "Security Threats and Service Degradation Detection in LoRaWAN Networks," *2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, 2021, pp. 0455-0458, doi: 10.1109/USBEREIT51232.2021.9455123.
6. M. Santamaria and A. Marchiori, "Demystifying LoRa WAN Security and Capacity," *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)*, 2019, pp. 1-7, doi: 10.1109/ITNAC46935.2019.9077997.
7. LoRa Alliance Technical Committee. (2020, November 17). *Lorawan® specification V1.1*. LoRa Alliance®. Retrieved November 28, 2022, from https://lora-alliance.org/resource_hub/lorawan-specification-v1-1/
8. Lnlp. (n.d.). *LNLP/LMIC-node: LMIC-node: One example to rule them all. LMIC-node is an example Lorawan application for a node that can be used with the things network. it demonstrates how to send uplink messages, how to receive downlink messages, how to implement a downlink command and it provides useful status information. with LMIC-node it is easy to get a working node quickly up and running. LMIC-node supports many popular (Lora) development boards out of the box. it uses*

the Arduino framework, the LMIC Lorawan Library and Platformio. GitHub. Retrieved November 28, 2022, from https://github.com/lnlp/LMIC-node

9. *What is the CIA triad and why is it important?* Fortinet. (n.d.). Retrieved November 28, 2022, from https://www.fortinet.com/resources/cyberglossary/cia-triad

10. *Frequency plans by country*. The Things Network. (n.d.). Retrieved November 28, 2022, from https://www.thethingsnetwork.org/docs/lorawan/frequencies-by-country/

11. *Regional parameters*. The Things Network. (n.d.). Retrieved November 28, 2022, from https://www.thethingsnetwork.org/docs/lorawan/regional-parameters/

12. Noura, Hassan, et al. "LoRaWAN security survey: Issues, threats and possible mitigation techniques." *Internet of Things* 12 (2020): 100303.
13. *The Things Industries launches Global Join Server with a series of device makers to simplify LoRaWAN® device provisioning.* The Things Industries. (January 31, 2020). Retrieved December 11, 2022, from https://thethingsindustries.pr.co/185845-the-things-industries-launches-global-join-server-with-a-series-of-device-makers-to-simplify-lorawan-device-provisioning
14. Vangelista, Lorenzo, and Marco Centenaro. "Worldwide connectivity for the internet of things through LoRaWAN." *Future Internet* 11.3 (2019): 57.