Univerzita Komenského v Bratislave

Fakulta matematiky, fyziky a informatiky

Návrh komunikačného protokolu pre inteligentnú zásuvku

diplomová práca

2017

Bc. Tomáš Kubla

Univerzita Komenského v Bratislave

Fakulta matematiky, fyziky a informatiky

Návrh komunikačného protokolu pre inteligentnú zásuvku

diplomová práca

Študijný program:	Informatika
Študijný odbor:	2508 Informatika
Školiace pracovisko:	Katedra informatiky
Školiteľ:	RNDr. Richard Ostertág PhD.

Bratislava, 2017

Bc. Tomáš Kubla

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Bc. Tomáš Kubla
Študijný program: informatika (Jednoodborové štúdium, magisterský II. st., denná forma)
Študijný odbor: informatika
Typ záverečnej práce: diplomová
Jazyk záverečnej práce: slovenský
Sekundárny jazyk: anglický

Názov: Návrh komunikačného protokolu pre inteligentnú zásuvku.
Design of communication protocol for smart socket.

Cieľ: Cieľom diplomovej práce je:

* preskúmať najznámejšie protokoly pre komunikáciu medzi zariadeniami v inteligentných domácnostiach

* analyzovať bezpečnosť existujúceho riešenia inteligentnej zásuvky a prípadne určiť možné zraniteľnosti

* v prípade nájdenia zraniteľností navrhnúť bezpečný komunikačný protokol pre inteligentnú zásuvku

Vedúci: RNDr. Richard Ostertág, PhD.
Katedra: FMFI.KI - Katedra informatiky
Vedúci katedry: prof. RNDr. Martin Škoviera, PhD.

Spôsob sprístupnenia elektronickej verzie práce:
bez obmedzenia

Dátum zadania: 06.04.2016

Dátum schválenia: 07.04.2016 prof. RNDr. Rastislav Kráľovič, PhD.
garant študijného programu

.....
študent

.....
vedúci práce

Poďakovanie:

Chcel by som sa poďakovať RNDr. Richardovi Ostertágovi PhD. za odbornú pomoc pri tvorbe práce a prípadné korektúry.

Ďalej chcem poďakovať prof. Ing. Viere Stopjakovej PhD. za umožnenie spolupráce s vývojovým tímom, Ing. Jurajovi Brenkušovi PhD. za dlhodobú spoluprácu a sprístupnenie inteligentnej zásuvky a doc. RNDr. Martinovi Stanekovi PhD. za veľké množstvo vedomostí z oblasti kryptológie, ktoré boli zúžitkované v tejto práci.

Tiež by som sa chcel poďakovať za poskytnutie priestorov, v ktorých vznikala táto práca, a to Univerzitnej knižnici v Bratislave, pohostinstvám rýchleho občerstvenia a vlakom Železničnej spoločnosti Slovensko.

A nakoniec, ale nie v poslednom rade: svojej rodine, spolužiakom, kamarátom, kolegom (najviac Peťkovi) a priateľke Majke, ktorí ma podporovali počas štúdia a mali so mnou trpezlivosť.

Abstrakt

Na internet vecí (IoT) sa v posledných rokoch hľadí skepticky kvôli veľkému množstvu bezpečnostných zraniteľností. Prinášame prehľad existujúcich protokolov používaných v IoT, spolu s popisom známych chýb v ich návrhu. Inteligentná zásuvka patrí medzi často používané komponenty IoT. V práci sme vykonali bezpečnostnú analýzu jedného konkrétneho riešenia takejto inteligentnej zásuvky. Hlavným prínosom práce je návrh bezpečného komunikačného modelu pre riadenie zásuviek a zber dát, ktoré zásuvky zaznamenali.

Kľúčové slová: internet vecí, inteligentná zásuvka, bezpečný komunikačný protokol

Abstract

In the last couple of years, the internet of things has been looked upon with scepticism because of a huge quantity of security vulnerabilities. We bring an overview of already existing protocols used in loT, with the description of known bugs in their proposal. The intelligent socket belongs to the commonly used components of loT. In this work, we executed the security analysis of one particular solution of an intelligent socket of this kind. The main contribution of this work is the proposal of a safe communicational model for controlling of sockets and collection of data, which were measured by the sockets.

Keywords: internet of things, smart socket, secure communication protokol

Obsah

Zoznam obrázkov

Úvod

V ostatnom čase sa začal často používať pojem Internet vecí. Tento termín pochádza z anglického *Internet of Things* respektíve *IoT*. Rovnako ako aj v ostatných častiach informatiky je dôležité klásť dôraz na bezpečnosť návrhov a implementácií, v *IoT* tomu nie je inak.

V prvej časti práce preskúmame protokoly, ktoré sa využívajú na komunikáciu v *IoT*. Budeme pátrať po princípoch, na ktorých sú založené komunikačné modely a k akým chybám prichádzalo pri návrhu týchto modelov.

V druhej kapitole spravíme bezpečnostnú analýzu inteligentnej zásuvky. Pokúsime sa bez hĺbkovej znalosti konkrétneho riešenia pasívnym spôsobom odpočuť komunikáciu a na základe nameraných údajov nájsť zraniteľnosť systému.

Posledná časť práce bude venovaná návrhu bezpečného komunikačného protokolu. Zadefinujeme, z ktorých častí sa systém zásuviek skladá, vyšpecifikujeme požiadavky na model a uvedenieme niekoľko aspektov, ktoré ovplyvňujú samotný model. Na záver popíšeme nami navrhnutý protokol pre komunikáciu zásuviek v systéme.

Kapitola 1

Súčasný stav problematiky

Vzhľadom k častému používaniu výrazu *IoT*, je potrebné vysvetliť daný pojem. V rámci dostupných zdrojov je možné sa dostať k veľkému počtu definícií. International Telecommunication Union[8] definoval v roku 2012 *IoT* ako *globálnu infraštruktúru informačnej spoločnosti, ktorá umožňuje pokročilým službám vzájomné prepájanie (fyzických aj virtuálnych) vecí, ktoré sú založené na existujúcich, ale aj vyvýjajúcich sa informačných a komunikačných technológiách.*

IoT zariadenia nachádzajú uplatnenie v priemyselnej sfére, ale často sa využívajú aj v domácnostiach. Aby sa zjednotil a zjednodušil prenos dát medzi zariadeniami, vzniklo niekoľko štandardov a komplexných riešení, ktoré sú ponúkané ako komerčné riešenia alebo sú zdieľané v rámci open-source komunity.

V oblasti *IoT* sú najrozšírenejšou skupinou komponenty spadajúce pod pojem *smart home*[1]. Ide o názov, ktorý je preferovaný v komerčnej sfére.

[1] slovensky inteligentná domácnosť

V takýchto domácnostiach sa využívajú predovšetkým kamery, pohybové senzory, inteligentné zásuvky, inteligentné žiarovky a iné.

1.1 IoT štandardy

Rozšírenie spomínaných *vecí* podnietilo vznik rôznych štandardov s cieľom zjednotiť komunikačné rozhranie. V porovnaní s bežne používaným OSI modelom alebo TCP/IP stackom, aj v *IoT* sa vytvárajú obdobné konštrukcie popisujúce komunikáciu na rôznych úrovniach. Nakoľko spomenuté modely nie su až tak odlišné, niektoré komunikačné protokoly použité v TCP/IP stacku sa uplatňujú aj v oblasti internetu vecí.

Obrázok 1.1 ilustruje podobnosti a rozdielnosti medzi TCP/IP a vybraným IoT stacku. Komunikačné modely sa môžu v rôznych *IoT* riešeniach podstatne líšiť.

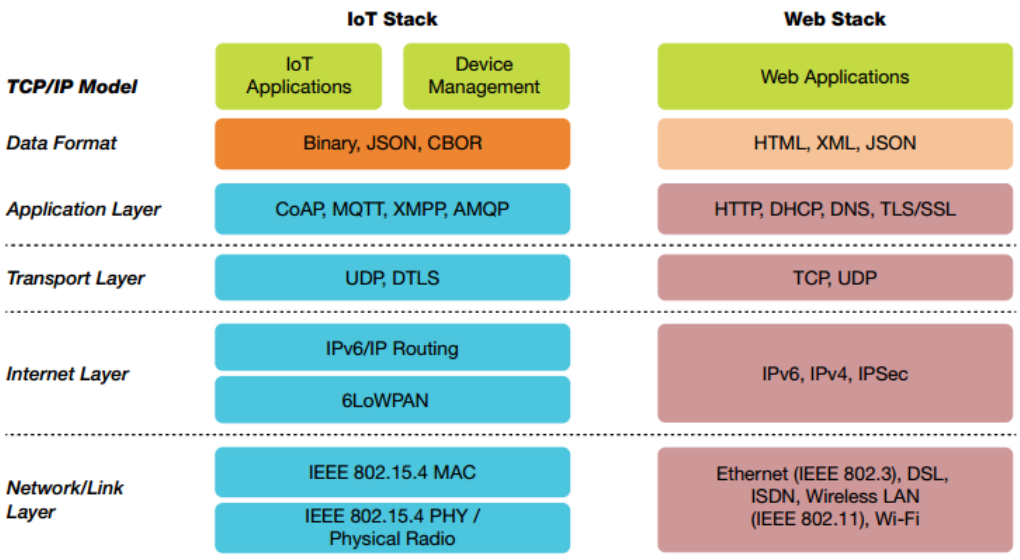
1.1.1 Komunikačný stack

V zariadeniach určených pre krátku vzdialenosť (hlavne v domácnostiach) sa využívajú štandardy radu *IEEE 802.15*. Spadajú sem protokoly kategórie WPAN[3], medzi ktoré patrí aj Bluetooth či IrDA. V oblasti internetu vecí sa využívajú hlavne ZigBee a Z-Wave. Tieto dva protokoly spadajú do kategórie domácej automatizácie[4].

[2]Zdroj: `https://www.linkedin.com/pulse/emerging-open-standard-protocol-stack-iot-aniruddha-chakrabarti` [citované 28.4.2017]

[3]wireless personal area network

[4]z anglického home automation



Obr. 1.1: Ukážka porovnania modelov[2]

Využívajú sa aj protokoly s veľkým dosahom, postavené na mobilných sieťach (GPRS, EDGE, HPSA+, LTE), WiFi (802.11n) alebo LoRa.

Niektoré protokoly nepokrývajú iba jednu úroveň, ale sú schopné pracovať s viacerými úrovňami naraz.

Okrem iného protokoly riešia aj bezpečnosť v oblasti autentifikácie a dôvernosti prenášaných dát. Príkladom je Bluetooth, v ktorom sa pri párovaní zariadení musí zadať zhodný predzdieľaný kľúč. V prípade zadania zhodného kľúču sa nadviaže spojenie. Pri komunikácii sa posielané dáta šifrujú za pomoci šifry E0 [9].

1.1.2 Chyby

Využitie štandardných protokolov však nezabezpečuje garanciu v oblasti bezpečnosti. V protokoloch sa nachádzajú chyby alebo dokonca niektoré na bezpečnostné aspekty vôbec nehľadia. Poukazuje na to aj článok [10], ktorý prináša prehľad útokov, ktoré je možné uplatniť na rôzne smart home riešenia.

Ďalším dôkazom toho, že sa v *IoT* riešeniach nie vždy prikladá dôraz na bezpečnosť je aj vytvorenie rebríčka desiatich najčastejších bezpečnostných chýb pri návrhu riešení z oblasti internetu vecí [7]. Spomenutý rebríček vytvorila komunita OWASP, uznávaná v oblasti bezpečnosti IT.

Rôzne riešenia implementujú šifrovanie pre zachovanie dôvernosti za pomoci všeobecne uznávanej symetrickej blokovej šifry AES. Výrobcovia zariadení používajú spomenutý fakt ako argument v otázkach riešenia bezpečnosti dát. Nie vždy je ale bezpečne realizovaná výmena kľúča, ktorý sa pre spomenuté šifrovanie využíva. Príkladom je protokol ZigBee, ktorý predpokladá predzdieľanie takzvaného *master key*. Tento kľúč sa do zariadenia dostane buď cestou, ktorej bezpečnosť nevieme garantovať alebo je do zariadenia nahraný ešte v továrni. Druhé z riešení nie je možné využiť v prípade dynamicky sa rozvíjajúceho systému. Spomenutú zraniteľnosť (ale aj rôzne ďalšie) demonštroval Joshua Wright na konferencii Toorcon [11].

Z-wave vznikol ako nasledovník ZigBee, ktorým mali byť odstránené známe nedostatky. Podľa Security evaluation of the Z-Wave wireless protocol[5] je prístup k z-wave špecifikácii a SDK[5] možný, ale až po zaplatení licen-

[5]software development kit – sada pre vývoj softvéru

cie a podpísaní NDA[6][3]. Avšak existuje open-source implementácia zvaná OpenZWave [1]. Behrang Fouladi a Sahand Ghanoun publikovali článok [5] v ktorom stojí, že napriek pridaniu šifrovania, ktoré zabezpečuje dôvernosť dát, protokol je zraniteľný na odchytenie kľúča, ktorý sa využíva pri samotnom šifrovaní. Kľúč síce nie je prenášaný v otvorenom formáte, avšak je zašifrovaný staticky preddefinovaným kľúčom.

Odvádzanie kľúča nebolo verejne publikované v žiadnej verejnej dokumentácii. Podarilo sa ho odhaliť vďaka podrobnej analýze komunikácie a analýze firmvéru. Pri uvedenom protokole sa znova potvrdilo, že *security by obscurity*[7] nie je vhodným riešením pri návrhu bezpečnostných častí ľubovoľnej komunikácie.

Do tretice uvádzame protokol X10, ktorý je predchodcom ZigBee a Z-wave. Štandard umožňuje ovládať zariadenia pomocou štandardnej elektrickej rozvodnej siete. Bolo postačujúce, aby zariadenia boli pripojené na rovnakej elektrickej fáze. K takejto sieti mohlo byť pripojených najviac 256 zariadení a protokol neumožňoval prenášané dáta šifrovať. Táto zraniteľnosť bola spomenutá na konferencii DEFCON 19, kde Rob Simon [2] odprezentoval Rob Simon X10 sniffer a X10 blackout nástroje, vďaka ktorým je možné odchytávať komunikáciu tohto štandardu alebo zahltiť komunikačnú linku natoľko, že nebude možné zariadenia ovládať.

[6]Non-disclosure agreement, slovensky Zmluva o mlčanlivosti

[7]slovensky bezpečnosť utajením – bezpečnostný model nie je verejne známy

1.2 Inteligentné zásuvky

Ako bolo spomenuté, medzi početnú skupinu *IoT* zariadení patria komponenty spadajúce pod súhrnný názov inteligentná domácnosť. Takého riešenia sa skladajú z rôznych komponentov ako dverový, pohybový či dymový senzor, inteligentná žiarovka alebo kamera. Jedným z najčastejšie využívaných komponentov sú inteligentné zásuvky. Zásuvky sa vyhotovujú v dvoch základných typoch:

- integrovaný obvod v redukcii, ktorý sa zasúva do bežnej zásuvky v stene
- integrovaný obvod, ktorý je zabudovaný v zásuvke nachádzajúcej sa v stene

V prvom prípade ide o zariadenie, s ktorým môže manipulovať aj zákazník bez elektrotechnického vzdelania. Nevýhodou je však menšia estetickosť[8]. Druhá alternatíva je priestorovo úspornejšia. Ale montáž musí previesť technik s elektrotechnickým vzdelaním[9].

[8] iba poznámka autora

[9] ide o vzdelanie popisované aj v podkapitole 3.3.2

[10] www.telekom.sk

[11] www.zwaveproducts.com

(a) Redukcia[10]

(b) Zásuvka pre zabudovanie do steny[11]

Obr. 1.2: Inteligentné zásuvky

Kapitola 2

Analýza bezpečnosti zásuvky

Aktívnemu vývoju inteligentných zásuviek sa venuje aj tím na Fakulte elektrotechniky a informatiky Slovenskej technickej univerzity. Pracujú na modely, v ktorom sa meracie zariadenie nachádza priamo v stene, a je súčasťou zásuvky ako takej. Pre komunikáciu uprednostnili bezdrôtovú technológiu umožňujúcu prenos dát na veľké vzdialenosti, na rozdiel od bežne predávaných riešení, ktoré využívajú technológie ako bluetooth alebo wifi. Spomenutá komunikačná technológia umožňuje zasielať dáta rádovo do niekoľkých kilometrov. Túto výhodu je možné využiť v hoteloch alebo v priemyselných zónach, prípadne na odľahlých miestach (chatové oblasti). Vývojový tím sa tiež zameral na minimalizáciu elektrickej energie, ktorú merač spotrebuje počas svojej prevádzky.

Sponenutý tím v televíznej relácii prezentoval a prakticky demonštroval možnosti spomenutej zásuvky na vyhotovenom prototype. V čase vysielania relácie zásuvka umožňovala len základnú funkcionalitu, a to zasielanie aktuálnej spotreby. Bolo spomenuté, že prenášané dáta sú šifrované, a teda

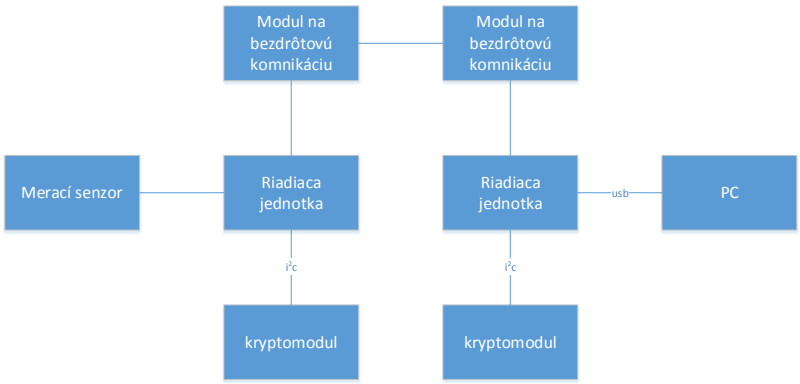
bezpečne prenášané zo zásuvky k zbernému bodu. Pre všetky kryptografické operácie bol využitý hardvérový kryptografický modul (ďalej len kryptomodul, kryptoelement alebo len modul).

Nakoľko sa pri návrhoch bezpečnostných protokolov objavujú chyby, zaujímalo nás, či sa neobjavili pri dizajne celého riešenia. Z uvedeného dôvodu sme kontaktovali vývojový tím za účelom spolupráce, kvôli prevereniu bezpečnosti použitého modelu. Tím súhlasil s ponukou vykonať audit celého riešenia.

Členovia tímu nás oboznámili so základanými informáciami o konštrukcii zásuvky, ktorá pozostáva z centrálnej riadiacej jednotky, meracieho senzoru, kryptografického modulu a modulu na bezdrôtovú komunikáciu. Zberané dáta sú ukladané do flash pamäte centrálnej jednotky a šifrovanie s následným odosielaním je vykonávané až po nazbieraní dostatočného množstva dát. Kryptomodul je od firmy NXP, model A7001, ktorý s centrálnou jednotkou komunikuje prostredníctvom komunikačného štandardu I^2C.

Celý audit bol vykonaný bez hĺbkovej znalosti riešenia. Nebola k dispozícii žiadna dokumentácia k zásuvke a ani k elementom, z ktorej je zásuvka zložená. Jediné informácie, s ktorými sme disponovali boli vyššie uvedené.

Nakoľko sa spomenutý modul používa na kryptografické operácie, výrobca nesprístupnil dokumentáciu k uvedenému modulu. Je k dispozícii len v prípade podpisu NDA.



Obr. 2.1: Komunikácia modulov

2.1 Popis auditu a informácie o komunikácii

Kryptoelement využíva na komunikáciu s centrálnou jednotkou protokol I^2C. Štandard tohto protokolu používa jednu dátovú linku (SDA) a jednu linku určenú na synchronizáciu času zápisu alebo čítania (SCL). Protokol predpokladá, že k linkám je pripojená práve jedna jednotka označovaná ako Master (riadi celú komunikáciu) a niekoľko[1] jednotiek Slave. V tomto kontexte je Masterom centrálna riadiaca jednotka a jedným zo Slave-ov je kryptoelement.

Pri analýze sme použili digitálny osciloskop Picoscope 6403D (obrázok 2.2). Softvérové vybavenie spomenutého zariadenia umožňuje automatické rozpoznávanie jednotlivých bajtov v komunikačnom protokole, v prípade, že

[1] najviac 128

budú o využívaní štandardu I^2C preddefinované informácie:

- ktorá sonda osciloskopu je pripojená na SDA
- ktorá sonda osciloskopu je pripojená na SCL
- aký rýchlostný štandard je použitý pri komunikácii[2]

Obr. 2.2: Osciloskop Picoscope 6403D[3]

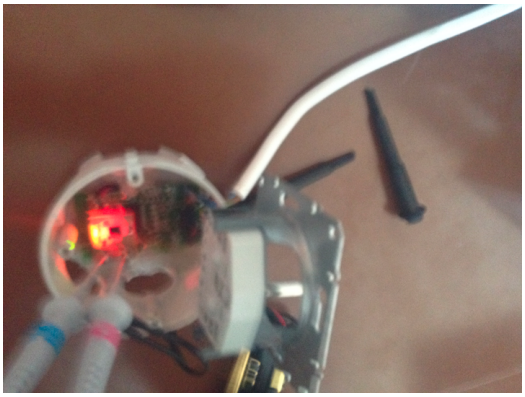
Keďže sme chceli predísť náhodnej chybe pri určovaní[4], ktorá linka je SDA a ktorá SCL, informovali sme sa, ktoré piny je možné využiť na pripojenie v prípade, že chceme odchytávať komunikáciu na uvedených linkách štandardu I^2C (obrázok 2.3). Namerané dáta sú k dispozícii ako príloha tejto práce.

Po meraní komunikačných dát sa pokračovalo ich analýzou. Nakoľko nie je zverejnená dokumentácia ku kryptomodulu, nebolo možné priamočiare dekódovanie obsahu komunikácie. Ukázalo sa, že v nameraných dátach je možné

[2]Štandard I^2C umožňuje komunikáciu s rôznymi prenosovými rýchlosťami

[3]www.picotech.com

[4]pripojením na nesprávne konektory by sme mohli spôsobiť poškodenie zásuvky alebo osciloskopu



Obr. 2.3: Osciloskop pripojený na I^2C

nájsť určité vzory, na základe ktorých sme stanovili hypotézu popisujúcu sémantiku jednotlivých príkazov nachádzajúcich sa v komunikácii.

Základný popis kryptomodulu[6] popisuje, že modul má širokú podporu pre rôzne kryptografické operácie. Predpokladali sme, že po zapnutí zásuvky sa vykoná určitá inicializácia a následne sa budú modulu zasielať len dáta potrebné na zašifrovanie. Hypotéza sa nepotvrdila, a teda vždy bola opakovane, každých 5 sekúnd, vykonaná rovnaká sekvencia príkazov.

2.2 Sémantika komunikácie

Komunikáciu v rámci jedného päť-sekundového intervalu sme si logicky rozdelili do siedmich častí. Delenie bolo podmienené dvoma aspektami:

- Z I^2C štandardu vieme, že pri komunikácii Master začne odoslaním čísla adresy, s ktorou chce komunikovať. Pokračuje odoslaním jedného bitu, popisujúceho či pôjde o zápis alebo čítanie. Ďalej v komunikáci nasleduje ACK bit. Ak je na linke pripojené zariadene pripravené na

komunikáciu, bit je rovný 0. V opačnom prípade (bit je rovný 1) zariadenie nie je pripravené alebo na zbernici sa žiadne zariadenie s touto adresou nenachádza. Dôvodom rozdelenia na jednotlivé časti bolo neodvysielanie ACK bitu rovného 0. Príčinou mohlo byť, že modul v tom čase ešte spracovával predchádzajúci príkaz obdržaný Mastrom a nebol pripravený prijať ďalšie dáta. Medzi časťou 5 a 6 sa tento jav dokonca zopakoval dva krát.

- Druhým aspektom delenia bolo, že každá časť (okrem prvej) sa začínala sekvenciou: WRITE 07, READ 01 07 a WRITE 02. Predpokladáme, že ide o určitú nadstavbu protokolu I^2C, ktorú využíva firma NXP pri komunikácii s jej modulmy. Táto sekvencia ohraničuje začiatok a koniec príkazu zasielaného kryptoelementu.

2.2.1 Predstavenie

Úvodnú časť komunikácie sme nazvali predstavenie, nakoľko jediné informácie, ktoré sa nám podarilo identifikovať boli v sekvencii *41 37 30 30 31 43 4D 20 32 34 32 52 31*, ktorá pri preklade do ASCII kódovania zodpovedá textovému reťazcu *A7001CM 242R1*. Uvedenú informáciu poslal kryptomodul centrálnej jednotke. Oznamuje tým o aký typ elementu ide. Ako odpoveď modul dostáva reťazec *41 37 30 42 4D*, ktorý v ASCII reprezentuje *A70CM*. Z verejne dostupných informácií[5] predpokladáme, že ide o element, ktorý spro-

[5]https://ebv.avnet.com/wps/wcm/connect/6ecf2c81-0c92-4ef1-b8aa-9dd0d2b91c83/F-039-E-05-2015-v1_NXP_A70CM_-_Cyber_Security_Solution_web.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-6ecf2c81-0c92-4ef1-b8aa-9dd0d2b91c83-lic-Se4 [citované 12.3.2017]

Tabuľka 2.1: Predstavenie

Packet	Start Time	R/W	ACK	Data
1	0.0239	W	0	0F
2	0.0319	W	0	1F
3	0.0322	R	0	01 00
4	0.0557	W	0	2F
5	0.0561	R	0	1E 00 B8 03 11 01 05 B9 02 01 01 BA 01 01 BB 0D 41 37 30 30 31 43 4D 20 32 34 32 52 31 BC 00
6	0.0745	W	0	FF
7	0.0748	R	0	01 CC
8	0.0829	W	0	00 0B 00 A4 04 00 05 41 37 30 43 4D 00

stredkováva dešifrovanie komunikácie na druhej komunikačnej linke, a teda na zbernom bode.

2.2.2 Inicializácia sedenia - definovanie použitia AES

Z dát v ďalšej časti sa nám nepodarilo identifikovať presný význam príkazu, ktorý sa centrálna jednotka pokúšala zadať modulu. Predpokladáme, že ide o inicializáciu sedenia[6], pri ktorom bude úlohou kryptomodulu šifrovanie symetrickou šifrou AES-128 v móde CBC. Fakt, že ide o šifru AES sme

[6] z anglického session

Tabuľka 2.2: Inicializácia sedenia

Packet	Start Time	R/W	ACK	Data
9	0.0921	Write	1	
10	0.1309	Write	0	07
11	0.1312	Read	0	01 07
12	0.1484	Write	0	02
13	0.1487	Read	0	07 02 02 05 01 02 90 00
14	0.1588	Write	0	10 0B 80 02 01 00 06 01 01 03 02 01 01

usúdili z informácií dostupných v krátkom popise modulu[7]. To, že ide práve o uvedené šifrovanie[8], zdôvodňujeme ďalej v práci.

2.2.3 Nahratie kľúča

Vychádzajúc z pozorovania sme predpokladali, že v častiach číslo 3 a 4 sa nachádza inicializačný vektor a kľúč pre šifrovane AES. Implicitne nebolo možné zistiť, ktorý z danej dvojice je prítomný v časti 3 a ktorý v časti 4. Z dĺžky príkazov sme usúdili, že pôjde o šifru AES-128 alebo AES-192. Šifru AES-256 sme vylúčili, nakoľko by sa kľuč nezmestil do poslaného packetu. Neskoršie zisťovanie ukázalo, že sa v tejto časti nachádza príkaz oznamujúci modulu, že má použiť kľuč *2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C*, z čoho expliticne vyplýva použitie šifry AES-128.

[7] http://www.nxp.com/documents/short_data_sheet/A700X_FAM_SDS.pdf [citované 12.3.2017]

[8] v CBC móde s dĺžkou kľúča

Tabuľka 2.3: Nahratie kľúča

Packet	Start Time	R/W	ACK	Data
15	0.1680	Write	1	
16	0.2068	Write	0	07
17	0.2071	Read	0	01 07
18	0.2243	Write	0	02
19	0.2246	Read	0	03 12 69 82
20	0.2344	Write	0	20 1D 80 06 01 00 18 02 01 00 16 01 01 0C 10 2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C

2.2.4 Nahratie IV

Ako bolo v predchádzajúcej časti uvedené, v časti číslo 4 sa predpokladala prítomnosť kľúča alebo inicializačného vektora. V packete sa nachádzala sekvencia končiaca aritmetickou postupnosťou *00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F*. Ak by sa ukázalo, že ide o kľuč, išlo by o zraniteľnosť typu *slabé heslo*. Záverečná analýza odhalila, že v tomto prípade ide o inicializačný vektor, u ktorého nie je kritické, pokiaľ má spomenutý tvar.

2.2.5 Zaslanie nezašifrovaných dát

Časť číslo 5 je s častou 6 najdlhšou v celej komunikácii. Pri analýze sme predpokladali, že ide o zasielanie nezašifrovaných dát kryptomodulu, ktoré boli určené na zašifrovanie. V tomto závere nás utvrdil aj fakt, že sa v ňom opakovala dvojica bajtov *33 EA*. Nakoľko sme počas celej doby odchytá-

Tabuľka 2.4: Nahratie IV

Packet	Start Time	R/W	ACK	Data
21	0.2454	Write	1	
22	0.2842	Write	0	07
23	0.2845	Read	0	01 07
24	0.3017	Write	0	02
25	0.3020	Read	0	03 22 90 00
26	2.0019	Write	0	30 1D 80 10 01 00 18 02 01 00 0F 01 01 10 10 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

vania komunikácie nemali pripojený žiaden spotrebič, v zásuvke sa nemenil odber elektrickej energie, čo viedlo k vygenerovaniu konštantnej postupnosti meraní. Uvedená hodnota(*33 EA*[9]) sa opakovala 32 krát, čo zodpovedá 4 blokom[10].

2.2.6 Čítanie zašifrovaných dát

V predposlednej časti kryptomodul zasielal zašifrované dáta. Ukázalo sa, že v tomto prípade dáta nie sú zarovnané na koniec celého príkazu, ale sú k nim pridané 2 bajty *90 00*. Vzhľadom na zarovnania predchádzajúcich packetov sme s takýmto zarovnaním nepočítali.

Za povšimnutie stoja až 2 packety naznačujúce, že kryptomodul nie je pri-

[9]V desiatkovom zápise by sa jednalo o hodnotu 13290 alebo 59955 v závislosti od toho, či bol pre zápis použitý little-endian alebo big-endian

[10]šifra AES vždy šifruje 16 bajtové bloky

Tabuľka 2.5: Zaslanie nezašifrovaných dát

Packet	Start Time	R/W	ACK	Data
27	2.0129	Write	1	
28	2.0517	Write	0	07
29	2.0520	Read	0	01 07
30	2.0692	Write	0	02
31	2.0695	Read	0	06 32 0E 01 01 90 00
32	2.0796	Write	0	40 47 80 10 02 01 42 11 40 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA 33 EA

Tabuľka 2.6: Čítanie zašifrovaných dát

Packet	Start Time	R/W	ACK	Data
33	2.0948	Write	1	
34	2.1337	Write	1	
35	2.1725	Write	0	07
36	2.1728	Read	0	01 07
37	2.1900	Write	0	02
38	2.1903	Read	0	45 42 12 40 F3 5A 3B B4 63 1A 37 C3 04 8D 41 4E 41 B0 58 6D C9 C2 EF 5C F3 F8 FE CF EA F6 1E D0 CE 21 70 1B 5B A9 4D F1 F4 5E DF 03 D5 10 C0 55 48 AC 84 8D CC EA 8B 1B C8 D5 5A AD B0 DC 85 F4 7C 90 38 2D 90 00
39	2.2062	Write	0	50 05 80 10 04 01 00

pravený na komunikáciu. Spomínaný fakt prisudzujeme vyťaženosti modulu. Podľa špecifikácie má modul hardvérovú podporu pre šifrovanie za pomoci AES. Keďže ale ide o nízko odberový čip stavaný pre malé riešenia (akým je aj inteligentná zásuvka), dĺžka šifrovania trvala dlhšie než centrálna riadiaca jednotka predpokladá.

2.2.7 Koniec sedenia

S popisom záverečnej časti sme mali problémy, vzhľadom na to, že si nie sme istí jej významom. Očakávame, že ide o príkaz oznamujúci kryptomodulu

Tabuľka 2.7: Koniec sedenia

Packet	Start Time	R/W	ACK	Data
40	2.2148	Write	1	
41	2.2536	Write	0	07
42	2.2539	Read	0	01 07
43	2.2711	Write	0	02
44	2.2714	Read	0	03 52 90 00

ukončenie sedenia, počas ktorého sa šifrovalo za pomoci AES.

2.2.8 Hľadanie šifry

Počas analýzy komunikácie nám vzniklo niekoľko hypotéz, ktoré sme museli preveriť. Išlo o konečný počet hypotéz, ktorých bolo rozumne málo, a tak nebol problém ich všetky vyskúšať. Zvažovali sme nasledujúce aspekty:

- je *00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F* kľúč alebo IV?
- ak je *00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F* kľúč, je skutočne *2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C* inicializačný vektor? Ak nie, je *2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C* kľúčom?
- ide o AES-128 alebo AES-192?
- v akom móde pracuje AES? ECB, CBC alebo úplne iný?

Napokon nebolo potrebné otestovanie všetkých možností. Zistili sme, že

ide o AES-128 v CBC móde s IV *00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F* a kľúčom *2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C*.

Ak by sa ani jedna z hypotéz nepotvrdila, museli by sme zvážiť, či sa v niektorých nami očakávaných parametroch nemýlime.

Všetkými uvedenými dôkazmi sme demonštrovali prelomitelnosť bezpečnosti použitej inteligentnej zásuvky v relatívne krátkom čase, bez znalosti dokumentácie.

Celá komunikácia v pôvodnej forme, ako aj v prekonvertovanej do čistých dát, je súčasťou príloh tejto práce.

Kapitola 3

Špecifikácia komunikačného modelu

Zámerom kapitoly je špecifikácia komunikačného modelu inteligentných zásuviek, pre potreby návrhu bezpečného komunikačného protokolu medzi jednotlivými zariadeniami.

3.1 Komunikačné entity

Pre úplnosť je potrebné definovanie komunikačných entít, ktoré v systéme vystupujú.

3.1.1 Zásuvky

Integrovaný obvod v zásuvke je schopný merať aktuálny odber elektrickej zásuvky. Namerané dáta si vie ukladať a v pravidelných intervaloch posielať. Obvod je schopný od zberného bodu alebo servisného zariadenia prijímať

riadiace príkazy. Komunikácia je teda obojsmerná. Definovanie príkazov ponechávame na vývojovom tíme, nakoľko neovplyvňujú samotný komunikačný model.

Zásuvka má v sebe umiestnený komunikačný modul pre výmenu dát na veľké vzdialenosti a komunikačný modul bluetooth pre konfiguráciu na krátke vzdialenosti.

3.1.2 Zberný bod

Zberný bod je samostatné zariadenie komunikujúce so zásuvkami iba v jednom systéme. Predpokladá sa, že pôjde o modul pripojený k PC. Môže však existovať aj samostatne. Jeho úlohou je zber dát zo zásuviek a posielanie príkazov zásuvkám.

V systéme zásuviek musí byť aspoň jeden zberný bod. Zákazník ich môže inštalovať viacero, v prípade záujmu používania záložných zberných bodov[1]. Ak je použitých viac zberných bodov, ich vzájomnou komunikáciou prebehne dohoda, ktorý z nich komunikuje s konkrétnou zásuvkou. Táto komunikácia je realizovaná po samostatnom nezávislom komunikačnom kanáli. Napríklad prostredníctvom pevnej káblovej siete alebo prostredníctvom mobilnej siete.

V prípade, že by bola zásuvka premiestnená a bolo by výhodnejšie, aby so zásuvkou komunikoval iný zberný bod, zberné body sa dohodnú na výmene. Tento výmenný mechanizmus siaha nad rámec tejto práce. Z pohľadu zásuvky nepríde k zmene.

[1]pre prípad výpadku alebo nedostatočného dosahu v bezdrôtovom spojení

3.1.3 Servisné zariadenie

Servisné zariadenie je prístroj, ktorého účelom je inicializácia zásuvky po jej nainštalovaní a diagnostika pri riešení problémov. Týmto zariadením môže byť špecializovaný servisný box alebo zariadenie s bluetooth modulom (notebook, smartphone, tablet). Úlohou zariadenia je hlavne sprostredkovať prvotnú konfiguráciu a čítať logy zo zariadenia v prípade poruchy.

3.2 Systém zásuviek a jeho princípy

Systém zásuviek je množina pozostávajúca z najmenej jedného zberného bodu a ľubovoľného počtu zásuviek. Z hľadiska bezpečnosti nie je limitovaný počet zásuviek v systéme, avšak nevylučujeme prítomnosť iného technického alebo fyzikálneho limitu. V systéme sa žiadna zásuvka nachádzať nemusí. Z praktického hľadiska nemá takýto systém význam, ale je potrebný, aby sa dalo jednoduchšie definovať pridávanie zásuviek do systému. So zásuvkou môže komunikovať ľubovolný zo zberných bodov. Voľba stratégie určujúca komunikanta, ktorého náplňou je spárovanie sa so zásuvkou, nenarúša bezpečnostnú stránku protokolu, a preto sa s ňou nebudeme zaoberať.

Komunikácia je možná iba medzi zásuvkou a zberným bodom/servisným zariadením. Zásuvky vzájomne nekomunikujú a zásuvka sa vždy nachádza len v jednom systéme.

Prvotné spárovanie so systémom prevádza servisné zariadenie.

3.3 Aspekty ovplyvňujúce model

Pri tvorbe modelu sme sformulovali aspekty, ktoré sme museli zvážiť alebo ich potrebujeme, aby sme sa mohli o ne oprieť.

3.3.1 Zamedzenie čítania kľúčov

Kryptomodul, s ktorým pracujeme podporuje ochranu kľúčov, ktoré sú v ňom uložené.Výhodou tejto techniky je, že umožňuje šifrovať dáta týmto kľúčom bez možnosti jeho extrakcie užívateľom či útočníkom. Daná vlastnosť funguje za predpokladu, že sa nám nepodarí modul otvoriť. Na tento úkon sú potrebné špeciálne technológie. Otvorenie takéhoto modulu sa väčšinou prevádza leptaním jeho púzdra. Následne je nutné zistiť kde je potrebné sa pripojiť a použiť mikro-sondy a/alebo mikroskop. Napriek tomu môže byť zariadenie chránené mriežkou spojov, cez ktoré sa sondou nedá prejsť a nemôžu sa ani narušiť. Bezpečnosť modelu zakladáme na náročnosti vykonať takýto útok.

Aby sme umožnili komunikujúcim entitám čitanie dôvernych dát, je potrebné distribuovať symetrický kľuč určený na šifrovanie aj do druhého kryptomodulu. Ten je možné získať napríklad zašifrovaním za pomoci verejného kľúča partnera, ktorému chceme daný kľúč poslať. Asymetrické šifrovanie kľúča je jediná možnosť, ako je možné kľúč z modulu dostať.

3.3.2 Montáž špecializovaným technikom

Podľa vyhlášky 508/2009 Z.z.[2][3] môže s technickým zariadením[4] pracovať len vyštudovaný elektrotechnik, prípadne osoba s vyššou kvalifikáciou[5]. Z tohto dôvodu konštatujeme, že montáž, demontáž a servis nebudú môcť vykonávať bežní používatelia, ale špecializovaní technici. Napriek uvedeným aspektom je vhodné, aby nastavenie zariadení v systéme nebolo príliš zložité a aby zákazník nemusel disponovať hlbšou odbornou spôsobilosťou v oblasti elektrotechniky alebo kryptológie. Synchronizáciu zásuviek a jednoduché servisné úkony bude vykonávať samotný zákazník.

3.3.3 Fyzický prístup k zariadeniu

Počas bežnej prevádzky sa predpokladá, že užívateľ nemá fyzický prístup k elektronickej časti zásuvky, nakoľko je zásuvka z bezpečnostných dôvodov chránená plastovou krytkou. Berieme do úvahy riziko možného útoku, pri ktorom útočník odstráni spomenutý ochranný prvok a bude odchytávať komunikáciu na komunikačných linkách prostredníctvom osciloskopu. Z pohľadu modelu môže byť kritická práve komunikácia medzi riadiacou jednotkou a kryptomodulom, ktorú je možné odchytiť počas spomenutého útoku.

Za predpokladu, že útočník sa bude môcť pripojiť ku komunikačnej linke

[2]vyhláška Ministerstva práce, sociálnych vecí a rodiny Slovenskej republiky, ktorou sa ustanovujú podrobnosti na zaistenie bezpečnosti a ochrany zdravia pri práci s technickými zariadeniami tlakovými, zdvíhacími, elektrickými a plynovými a ktorou sa ustanovujú technické zariadenia, ktoré sa považujú za vyhradené technické zariadenia

[3]v znení neskorších predpisov

[4]ktorým zásuvka v zmysle tejto vyhlášky je

[5]podľa §21 musí byť osoba s dozorom, podľa §22-§24 bez dozoru

I2C, musíme počítať s tým, že bude môcť komunikáciu nielen pasívne sledovať, ale bude ju môcť aj riadiť. Keďže sa dáta medzi riadiacou jednotkou a kryptoelementom prenášajú v otvorenej neautentifikovanej podobe, útočníkovi je umožnené vystupovať voči kryptomodulu ako riadiaca jednotka bez toho, aby mohol modul takúto zámenu detegovať. Z tohto dôvodu sa z kryptomodulu stáva takzvané šifrovacie resp. dešifrovacie orákulum, teda jednotka, ktorú môžeme požiadať o zašifrovanie/dešifrovanie nami pripravených dát bez toho, aby sme poznali šifrovací kľúč. Uvedený útok považujeme za stredne náročný z hľadiska realizácie. Toto zaradenie ovplyvnili nasledujúce aspekty:

- k zariadeniu je potrebný fyzický prístup
- znalosti v oblasti elektrotechniky, nakoľko sa pracuje so zariadením ovládajúcim 230V
- schopnosť realizovať útok buď v samotnej zásuvke pri plnej prevádzke a pod prúdom alebo je potrebná demontáž vnútra zásuvky
- taktiež zdatnosť vyhotoviť zariadenie schopné simulovať činnosť riadiacej jednotky zásuvky

Ak útočník splní všetky spomenuté predpoklady, realizáciu simulácie považujeme za jednoduchšiu časť útoku.

3.3.4 Bezpečnostné profily

Vychádzajúc z niektorých predpokladov sme pre určité časti modelu definovali rôzne funkcie. Následne sme vedeli jednotlivým funkciám určiť ich

stupeň bezpečnosti. Z uvedeného dôvodu sme sa rozhodli vytvoriť takzvané bezpečnostné profily, ktoré sa odlišujú tým, z ktorých bezpečnostných scenárov pozostávajú. V kontexte profilov si užívateľ môže zvoliť, do akého akceptovateľného rizika je ochotný ísť[6]. Skúsení používatelia majú možnosť si definovať vlastné profily využijúc dostupné scenáre.

3.3.5 Riadenie komunikácie

Proces komunikácie medzi zásuvkami a zbernými bodmi cez bezdrôtové spojenie je modelom siahajúcim nad rámec práce. Pri návrhu bezpečného modelu však musíme počítať s niektorými vlastnosťami spomenutého procesu.

Jedným z týchto aspektov je, že komunikácia je v modely: 1 master – entita riadiaca komunikáciu a viac slave-ov – entita komunikujúca až po vyzvaní master-om. V kontexte systému zásuviek bude zberný bod master-om, ktorý bude inicializovať komunikáciu voči zásuvkám.

Kvôli úspore energie zásuvka nie je počas celej prevádzky pripravená vysielať. V pravidelných intervaloch sa zapína a prechádza do takzvaného majákového módu, kedy odvysiela informáciu o tom, že je pripravená komunikovať a následne čaká na vyzvanie. V prípade, že do určitého času nie je vyzvaná, znova sa prepne do režimu, kedy sa komunikačný modul stane neaktívnym.

[6]Pre porovnanie s bezpečnosťou v oblasti WiFi sieti – do štandardu pridaná možnosť pripojiť nové zariadenie za pomoci rozšírenia WPS. Táto funkcia zvýšila pohodlie pri pripájaní nových zariadení k sieti avšak poľavila v predpokladoch na bezpečnosť.

3.3.6 Dlhšia nedostupnosť

Vychádzajúc z faktu, že komunikáciu inicializuje master, nie je vylúčené, že v prípade jeho väčšej vyťaženosti alebo nedostupnosti z dôvodu iných fyzikálnych a technických anomálií či problémov bude potrebné nazbierané dáta dlhodobejšie ukladať. Takéto ukladanie je potrebné až do momentu, kým nebude zásuvka znova vyzvaná na zaslanie nazbieraných dát.

3.3.7 Nešifrovaný ukladací priestor

Počas nedostupnosti mastera sa neodoslané dáta musia ukladať do pamäte odolnej voči výpadku elektrickej energie. Pôjde o flash pamäť nachádzajúcu sa priamo v riadiacej jednotke alebo mimo nej[7]. Tieto dátové média nie sú šifrované. Uvedený fakt môže niektorým užívateľom zásuviek prekážať. Dôvodom môže byť možnosť extrakcie dát zo zásuvky servisným technikom[8], pričom zákazník nechce, aby technik vedel čítať informácie o spotrebe.

3.3.8 Kapacita ukladacieho priestoru

V prípade extrémne dlhej nedostupnosti master-a, môže pri ukladaní dát dôjsť k zaplneniu úložného priestoru. Bolo potrebné nájsť metódy, ktoré riešia daný problém. Zvážili sme možnosť zahadzovania[9] najstarších dát alebo kompresie dát vo forme ukladania aritmetických priemerov dát za dané časové obdobie. Uvedené postupy sú možnými riešeniami daného problému.

[7] napríklad microSD karta

[8] alebo políciou

[9] mazania

3.3.9 Práca so zašifrovanými informáciami

Scenár ukladania aritmetických priemerov nie je plne realizovateľný, ak požadujeme splnenie ostatných bezpečnostných aspektov. V prípade uplatnenia predpokladu, že chceme využívať kryptoelement v zásuvke len na šifrovanie s ohľadom na aspekt neprezradenia kľúča[10], je vhodné nepovoliť dešifrovanie dát. Ak by takáto funkcia bola povolená, z kryptoelementu sa stáva takzvané dešifrovacie orákulu, čo nie je žiadúce, lebo by bolo možné dešifrovať dáta z flash pamäte technikom.

Pokiaľ ale nie je umožnené dešifrovanie dát, ani riadiaca jednotka nebude môcť vykonať dešifrovanie so zámerom následného priemerovania uložených dát.

Riešením môže byť upustenie od požiadavky na zakázanie fungovania v režime dešifrovacieho orákula alebo od požiadavky dlhodobého ukladania dát[11]. Teoreticky by možným riešením bolo šifrovanie za pomoci iného algoritmu ako je AES, ktorý umožňuje so zašifrovanými dátami prevádzať aritmetické operácie ako sčítavanie a násobenie[12]. Tento algoritmus však nie je podporovaný kryptomodulom, ktorý máme k dispozícii.

Posledným možným riešením je priebežne ukladať aritmetické priemery za určité časové obdobie (napríklad 1 minúta, 10 minút, 1 hodina, 6 hodín, 24 hodín a 7 dní- t.j. 6 časových granularít). Tým by sa vytvorilo niekoľko nezávislých časových radov a každý z nich by bol šifrovaný. Po naplnení radu by sa uplatnil scenár zahadzovania najstarších dát. Tento scenár síce

[10] jedine prostredníctvom asymetrického zašifrovania, nám povoleným certifikátom

[11] po naplnení pamäte by boli najstaršie dáta mazané

[12] tieto operácie sú postačujúce na vypočítanie aritmetického priemeru

nepožaduje dodatočné dešifrovanie avšak úmerne znižuje kapacitu pamäte.

Pre ilustráciu: hypoteticky sme ukladali do pamäte dáta po sekundových intervaloch a vedeli sme uložiť merania za posledných 24 hodín (86400 vzoriek). Rozhodli sme sa okrem pôvodných dát ukladať aj časove dáta agregované po minúte, hodine a dni, pričom ukladaná kapacita by bola v nasledujúcom pomere:

- 64% sekundové vzorky
- 30% minútové vzorky
- 5% hodinové vzorky
- 1% dňové vzorky

Dáta, ktoré by sme vedi takto uložiť na nasledovné obdobie:

- sekundové vzorky na 15 hodín, 21 minúť a 36 sekúnd
- minútové vzorky na 18 dní
- hodinové vzorky na 180 dní
- dňové vzorky na 2 roky a 134 dní

3.3.10 Aktuálny čas

Bezpečnosť komunikačného modelu, ktorý by mal využívať certifikáty, je založený (okrem iného) na overovaní platnosti — či nie je certifikát exspirovaný. Pre tento účel je potrebné požadovať od komunikačných entít udržovanie platného aktuálneho času. Od vývojového tímu vieme, že integrované

obvody v zásuvke obsahujú komponent určený na ukladanie aktuálneho času a v prípade výpadku elektrickej energie sa aktuálny čas zapamätá[13]. Ale čas, ktorý uplynul počas vypnutia nebude zaznamenaný.

3.3.11 Použitie multicast-u a broadcast-u

Pre zefektívnenie komunikácie sa na náš podnet pridala možnosť zasielania multicast-ových a broadcast-ových správ[14]. Výhoda plynie z možnosti zaslania rovnakého príkazu všetkým zásuvkám, bez potreby šifrovať správu pre každú zásuvku zvlášť. Takto vyhotovená správa môže ušetriť výpočtový výkon a čas na strane zberného bodu. Tiež ušetrí vyťaženosť prenosového kanálu, nakoľko obsahovo rovnaká správa nebude zasielaná viacnásobne.

Ako aj pri výmene ostatných dát usudzujeme, že pred šifrovaním správy symetrickou šifrou došlo k zaslaniu symetrického kľúča do modulu za pomoci zašifrovania asymetrickým kľúčom.

Funkcia multicast resp. broadcast môže byť použitá, len v prípade uplatnenia jedného zo nasledujúcich scenárov:

- symetrický kľúč je uložený len v jednom zbernom bode - v tomto prípade môže šifrovanie prevádzať len tento jeden modul a následne musí zašifrované dáta doručiť ostatným zberným bodom, aby mohlo dôjsť k ich odoslaniu zásuvkám

- symetrický kľúč vlastní každý zberný bod. Zberné body vzájomne nez-

[13]na rozdiel od iných realizácii pri ktorých v prípade výpadku sa čas vynuluje na prednastavenú hodnotu

[14]broadcast-ová správa je len špeciálny prípad multicast-ovej, ktorá nie je adresovaná len vybranej skupine príjemcov, ale všetkým príjemcom

dieľajú rovnaký kľúč a každý bod spravuje svoje vlastné broadcast-ové a multicast-ové domény. Predpokladá sa, že zberný bod, ktorý chce zaslať správu spomínaného typu nedoručí dáta len svojím doménam, ale zašle správu aj ostatným zberným bodom, aby zabezpečili doručenie zásuvkám v ich doménach.

3.3.12 Synchronizácia v továrni

Pre potreby jednoduchého nastavenia sa pri návrhu modelu zvažovala alternatíva, pri ktorej by boli zásuvky zosynchronizované s centrálnym zberným bodom priamo v mieste výroby komponentov.

Túto možnosť sme neuplatnili v implementácii modelu z nasledujúcich dôvodov:

- Nakoľko sa v modely plánovali použiť certifikáty, ktorých platnosť je ohraničená dátumom ich exspirácie, mohlo by dôjsť k situácii, keď by zásuvky a zberné body boli uložené na sklade dodávateľa alebo obchodu dlhšie, ako je platnosť certifikátu. Muselo by tak či tak dôjsť k situácii, že si komunikačné entity budú musieť znovu nadviazať dôveru.

- V prípade, že by zákazník mal záujem rozšíriť množstvo zásuviek v celom systéme, nemohlo by dôjsť k ich synchronizácii v továrni.

Kvôli spomenutým dôvodom sa pri tvorbe modelu uprednostnila alternatíva, kedy sa dôvera bude nadväzovať až po prvotnej inštalácii a spustení. Preto bolo potrebné dať dôraz na bezpečnosť práve v tejto fáze.

3.3.13 Možnosti sekundárnej komunikácie

Vzhľadom k vyššie uvedenému sme pri prvotnej synchronizácii museli rátať s využitím iného postranného kanála sprostredkujúceho výmenu dôvernej informácie, ktorá by garantovala bezpečnosť komunikácie medzi zúčastnenými stranami. Takáto výmena musí byť prevedená spôsobom, pri ktorom bude garantované, že nemohol do komunikácie vstúpiť útočník, respektíve, ak by vstúpil, bol by ľahko odhalený.

Počas vývoja bolo navrhnutých niekoľko možností:

- Využitie bluetooth s verejne známym heslom – ide o metódu, ktorá je užívateľsky jednoduchá a zvládne ju aj laický používateľ. Jej nevýhodou je, že bluetooth ma veľký dosah, čím uľahčuje pripojenie útočníka napriek tomu, že by sa nenachádzal explicitne pri zásuvke[15].

- Využitie bluetooth s unikátnym heslom – takéto heslo by muselo byť súčasťou balenia zásuvky. Táto metóda už je odolná voči útoku z prechádzajúceho bodu. Je však užívateľsky namáhavá a časovo náročná (v prípade veľkého systému).

- NFC – táto metóda umožňuje spárovanie pre extrémne malú vzdialenosť. Vývojový tím však neschválil použitie tejto technológie do zásuvky, kvôli komplikovanej inštalácii.

[15] je postačujúce, aby sa nachádzal na druhej strane steny

3.4 Protokol

Nasledujúca podkapitola sa venuje konkrétnemu návrhu protokolu, aby sme zabezpečili bezpečný prenos nazbieraných dát zo zásuvky a príkazov zo zberného bodu. Pri návrhu sme zohľadnili aspekty z podkapitoly 3.3.

Uvedieme akú úlohu majú certifikáty v našom systéme a ako vznikajú a popíšeme podstatu slotov, ktoré sa využívajú pri komunikácii medzi zariadeniami. Ďalej popíšeme životný cyklus zariadení, s čím sú spojené aj fakty, kedy certifikáty a sloty vznikajú a ako prichádza k ich aktualizácii.

3.4.1 Certifikáty

Nadväzujúc na Sahanda Ghanouna, ktorý na konferencii Black Hat USA 2013 povedal, že dlhodobým riešením pre problémy s výmenami kľúčov v *IoT* je použitie asymetrických konštrukcií [4], rozhodli sme sa použiť asymetrické kľúče, ktoré sú obsahom certifikátov. Certifikáty sú v kontexte zásuviek využité na autentifikáciu (aby zásuvka aj zberný bod mali istotu, že komunikujú s dôveryhodným partnerom z rovnakého systému) a na dôvernosť (pre výmenu symetrického kľúča).

Hlavným certifikátom je certifikát certifikačnej autority (ďalej len CA), ktorého súkromný kľuč sa nachádza na jednom zo zberných bodov. Tento zberný bod ako jediný môže vydávať certifikáty pre všetky entity v systéme.

Okrem CA certifikátu sa v systéme používajú ešte nasledovné druhy certifikátov:

- certifikát zberného bodu

- certifikát zásuvky
- certifikát pre multicastové a broadcastové správy

Certifikát CA, ktorý sa nachádza v zbernom bode, kde sídli CA nie je totožný s certifikátom zberného bodu. Na takomto zbernom bode sa teda nachádzajú dva certifikáty. Spomenuté rozdelenie je nutné, aby v prípade potreby[16] bolo možné certifikát CA jednoducho presunúť. V prípade nevyhnutnosti presunu CA na iný zberný bod, jeho súkromný kľúč musí byť presunutý bezpečným spôsobom.

V rámci celého systému je ako prvá potrebná inicializácia hlavného zberného bodu[17]. S týmto krokom je spojené vytvorenie certifikačnej autority a jej certifikátu. Parametre certifikátu CA podliehajú požiadavkám bezpečnostného profilu, ktorý si zvolí zákazník. Nakoľko sa predpokladá, že zberný bod je zriadenie, s ktorým je možná plnohodnotná interakcia s užívateľom, vytvorenie certifikátu nechávame na podnet zákazníka t.j. nevzniká automaticky nevyhnutne po zapnutí. Postup, ako má zákazník tento certifikát vytvoriť a ako si zvolí aj iné parametre systému bude súčasťou užívateľskej príručky k systému. Týmto vytvorením vzniká systém, v ktorom zatiaľ nie su žiadne zásuvky a iba jeden zberný bod.

Od momentu vytvorenia je možné, aby ostatné zariadenia, ktoré budú súčasťou systému požiadali o vytvorenie ich certifikátu. Táto tvorba podlieha štandardnému procesu za pomoci CSR[18], kedy entita vygeneruje vlastný pár

[16] napríklad ak príde k poškodeniu zberného bodu

[17] Hlavný zberný bod – ide o jednorázové pomenovanie zberného bodu čisto pre účel inicializácie. Môže ísť o ľubovoľný zo skupiny zberných bodov v systéme.

[18] Certificate signing request

kľúčov (súkromný a verejný) a požiada o vygenerovanie certifikátu pre novo vytvorený verejný kľúč. CA následne vygeneruje certifikát a zašle ho entite. Od tohto momentu môže entita pri komunikácii používať certifikát za účelom autentifikácie a dešifrovania dát, ktoré mu boli zaslané.

Samotné žiadanie o certifikát v našom kontexte je zložené z nasledujúcich krokov:

- žiadateľ (zberný bod alebo zásuvka) vygeneruje pár verejného a súkromného kľúča za pomoci kryptoelementu. Súkromný kľúč však zostáva v elemente a nie je možné ho exportovať.
- verejný kľúč element zabalí do CSR, ktorý si zásuvka/zberný bod prečíta a zašle certifikačnej autorite
- certifikačná autorita vygeneruje certifikát a zašle ho zásuvke/zbernému bodu späť
- zásuvka/zberný bod si zapíše certifikát do pamäte a kryptoelementu

Všetky certifikáty vydané CA majú obmedzenú platnosť. Aktualizáciu certifikátu je potrebné robiť pred skončením platnosti starého certifikátu. Jednotlivé entity majú rôznu dĺžku platnosti ich certifikátu a tiež dobu, po ktorej je stanovené, že majú svoj certifikát aktualizovať. Všetky časy sú uvedené v tabuľke 3.1.

Potreba obnovenia certifikátov je výrazne kratšia ako ich platnosť. Tento fakt sme určili so zámerom zachovať certifikáty platné aj keď sa nepodarí ich aktualizácia na prvý pokus. Príčiny, za ktorých môže dôjsť k neúspešnej aktualizácii sú popísané neskôr.

	Platnosť	Obnovenie od dátumu vydania
Zberný bod	2 roky	½ roka
Broadcast/multicast	2 roky	½ roka
Zásuvka	1 rok	1 mesiac

Tabuľka 3.1: Platnosť a potreba obnovy certifikátov

Všetky zariadenia v systéme majú svoje unikátne označenia definované v továrni. Pre zberné body ide o označenie *ZB_xxx*, pre zásuvky *Z_xxx* a pre servisné zariadenia *SZ_xxx*. Označenie 'xxx' reprezentuje 32 bitové číslo zapísané v hexadecimálnom formáte, napríklad Z_04ED4BA2. Uvedené označenie je aj súčasťou certifikátu.

3.4.2 Komunikačné sloty

Pre komunikáciu používajú všetky entity takzvané *komunikačné sloty*. Každý slot špecifikuje komunikačnú linku medzi dvojicou entít. Každá entita môže mať ľubovolný počet slotov. Slot je štruktúra v pamäti, ktorá je zložená z nasledujúcich častí:

- Identifikátor slotu
- Certifikát partnera
- Typ
- Symetrický kľúč

Identifikátor slotu určuje partner, ktorý ho inicializuje, teda zberný bod a môže byť dlhý najviac 4 bajty. Konkrétne pomenovanie, teda presný identi-

fikátor je poradové číslo slotu, ktoré v rámci systému vzniklo. Z tohto dôvodu je prideľovanie identifikátorov centrálne riadené a má ho na starosti certifikačná autorita. Identifikátor sa využíva, aby pri prijatí správy bolo možné jednoducho identifikovať, ktorým kľúčom je potrebné správu dešifrovať.

Certifikát partnera je samo-popisujúci parameter.

Typ je vlastnosť spojenia, ktorá určuje, či je komunikačný slot určený k posielaniu príkazov alebo prenosu dát. Rozdelenie je spôsobené potrebou pracovať so synchrónnymi linkami, kde musíme garantovať, že obe komunikujúce strany majú šifrovacie komponenty v rovnakom stave[19], a tiež s linkami, ktoré sa v prípade rozsychronizovania vedia vrátiť do zhodeného stavu za pomoci synchrónnych liniek (napríklad aktualizáciou inicializačného vektora).

Symetrický kľúč je kľúč obdržaný za pomoci zašifrovania asymetrickým kľúčom pri inicializácii slotu. Tento kľúč je uložený iba v kryptoelemnte a zásuvka si pamätá len jeho poradové číslo. Platnosť kľúča je limitovaná na jeden týždeň. Následne sa prechádza k jeho aktualizácii. Za akých podmienok prichádza k aktualizácii kľúča je uvedené v podkapitole 3.4.6.

3.4.3 Bezpečnostné profily

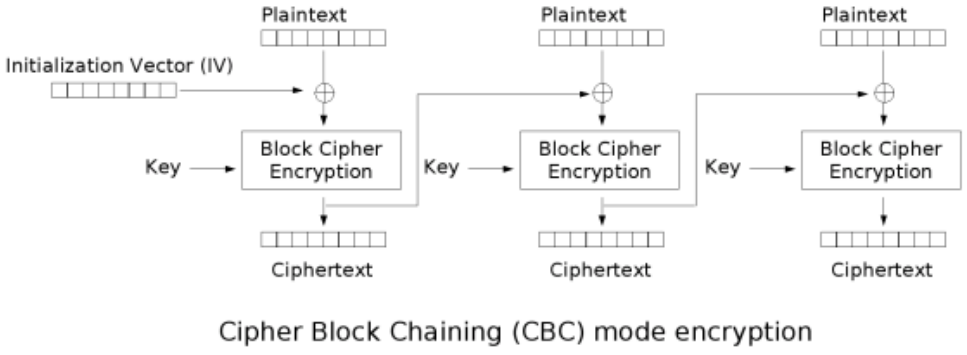
Ako bolo v práci uvádzané, zásuvka dokáže fungovať s rôzne nastavenými bezpečnostnými funkciami v závislosti od toho, ako si zákazník praje. Tieto nastavenia podliehajú skupine nastavení, ktorá sa vola bezpečnostný profil. Boli vytvorené 2 štandardné profily, ktoré v sebe nesú odporúčanú skupinu nastavení. Je však možné si zvoliť vlastný profil. Všetky zariadenia podliehajú rovnakému bezpečnostnému profilu a teda nie je možné, aby napríklad 2

[19] rovnaký inicializačný vektor a rovnaký šifrovací kľúč

zásuvky mali nastavené svoje bezpečnostné funkcie v rôznych módoch. Obsah profilov je uvedený ako príloha tejto práce.

3.4.4 Štandardná komunikácia

Zariadenia, ktoré majú vytvorené komunikačné sloty sú pripravené na výmenu štandardných dát a príkazov. Na šifrovanie týchto dát sa používa symetrická bloková šifra AES-128, AES-192 alebo AES-256, závislosti od toho, aký bezpečnostný profil si zvolí zákazník. Šifrovanie prebieha v CBC móde[20] (obrázok 3.1). Inicializačný vektor pre šifrovanie volí zberný bod náhodne a oznamuje ho zásuvke pri akciách A2 a A6. Pre šifrovanie jednotlivých dát sa nevyužíva vždy ten istý inicializačný vektor obdzržaný zberným bodom, ale posledný zašifrovaný blok. Túto funkciu nie je potrebné explicitne programovať, nakoľko vychádza z princípu CBC módu. Pri šifroví sa využíva výplňová schéma PKCS#7.



Obr. 3.1: CBC mód šifrovania[21]

[20]Cipher Block Chaining

Namerané dáta sú šifrované po skupinách, ako sú pripravované meracím senzorom. Predpokladáme, že to bude 32 dvoj-bajtových hodnôt, ako tomu boli pri analýze pôvodného protokolu. V prípade zásuviek sú počas prevádzky namerané dáta šifrované a ukladané do flash pamäte do momentu, kedy bude zásuvka vyzvaná zberným bodom, aby dáta zaslala.

Každá správa počas komunikácie je zložená z 2 častí a to z nešifrovanej a šifrovanej. Nešifrovanú časť tvorí identifikátor slotu, aby pri prijatí správy bolo možné určiť, ktorému slotu je správa pridelené.

Obsahom šifrovanej časti správ je vždy 1 bajt určujúci príkaz a následne jeho parametre.

Ak je príkaz rovný nule, ide o nazbierané dáta zo zásuvky. Parametrami v tomto kontexte sú časová pečiatka zodpovedajúca času, kedy bolo vykonané meranie[22], ako dlho trvalo meranie (v sekundách) a koľko jednotlivých meraní bolo realizovaných. Pečiatka zodpovedá počtu sekúnd od 1.1.1970[23] a je uložená ako neznamienkové číslo dĺžky 32 bitov. Dĺžka merania je uložená v 24 bitovom neznamienkovom čísle, z čoho vyplýva, že časové okná zasielané môžu mať dĺžku najmenej jednu sekundu a najviac 194 dní[24]. Počet meraní je 8 bitové číslo vyjadrujúce, koľko 16-bitových čísel bude nasledovať[25]. Nakoniec sú uvedené samotné namerané dáta.

Obsah príkazov rôznych od nuly je nad rámec tejto práce.

[21] Zdroj: `https://commons.wikimedia.org/wiki/File:Cbc_encryption.png` [citované 28.4.2017]

[22] kedy meranie začalo

[23] podľa štandardu POSIX

[24] po zaokrúhlení na dol

[25] vychádzame z faktu, že aktuálne sú merané dáta dvoj-bajtové hodnoty

Nešifrované d.	Šifrované dáta				
ID slotu (4B)	*Príkaz (1B)*	*parameter 1*	*parameter 2*	*parameter 3*	...

Tabuľka 3.2: Všeobený tvar komunikačnej správy

Nešifrované d.	Šifrované dáta				
ID slotu (4B)	*Príkaz (1B) = 0*	*časová pečiatka (4B)*	*dĺžka merania (3B)*	*# meraní (1B)*	*dáta*

Tabuľka 3.3: Posielanie nameraných dát

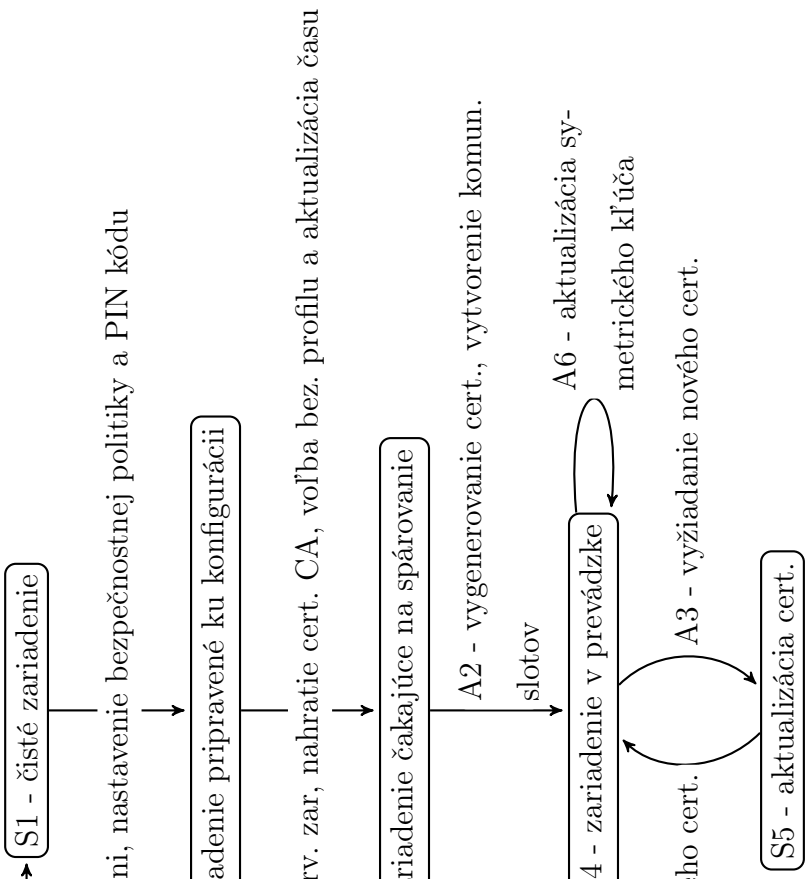
3.4.5 Životný cyklus entít

Všetky entity použité v systéme majú definovaný svoj životný cyklus. Za entitu respektíve zariadenie považujeme zberný bod, servisné zariadenie alebo zásuvku. Životný cyklus sa skladá z nasledujúcich stavov a prechodov medzi nimi, ktoré špecifikujeme ďalej v práci:

- S1 – čisté zariadenie – zariadenie bolo vyrobené v továrni avšak nebola vykonaná inicializácia jeho kryptomodulu. V prípade, že zberný bod alebo servisné zariadenie nebude používať kryptomodul, uvedený stav sa automaticky preskakuje. Zariadenie v tomto stave nesmie opustiť továreň.

- S2 – zariadenie pripravené ku konfigurácii – zariadenie prešlo úvodnou inicializáciou kryptoelementu, bol mu nastavený autentifikačný PIN kód, identifikátor a je pripravené k distribúcii k zákazníkovi. Zariadenie sa do tohto stavu mohlo dostať aj po vynútenom resete do továrenský nastavení. Zariadenie v tomto stave nie je súčasťou žiadneho systému.

- S3 – zariadenie čakajúce na spárovanie – po tom, ako bolo do zariadenia v stave S2 nahratý certifikát CA a bezpečnostný profil, zariadenie



Obr. 3.2: Životný cyklus entít

čaká na výzvu niektorého zo zberných bodov, aby bolo pripárované k systému.

- S4 – zariadenie v prevádzke – po spárovaní (vygenerovaniu certifikátu a vytvorení komunikačného slotu) je zariadenie pripravené ku štandardnej prevádzke a teda meranie aktuálnej spotreby, šifrovanie týchto dát a odosielanie zbernému bodu.

- S5 – aktualizácia certifikátu – v prípade, že dôjde k situácii, kedy entita potrebuje nový certifikát, požiada si oň a čaká v tomto stave na jeho vyhotovenie.

Časové limity

V nasledujúcich podkapitolách budeme okrem iného definovať prechody medzi stavmi, ktoré sme si už definovali. Pri niektorých prechodoch sa bude očakávať, že komunikační partneri budú musieť čakať na odpoveď od oponenta. Ak nebude stanovené inak, pri všetkých akciách, ktoré očakávajú odpoveď môže zariadenia čakať najviac 60 sekúnd. V prípade, že do tohto času nepríde očakávaná odpoveď, zariadenia sa vracajú do stavu, v ktorom sa naposledy nachádzali a pokúšajú sa celú akciu opakovať o 5 minút neskôr.

3.4.6 Akcie

Prechody medzi stavmi sú nazvané ako akcie, pričom každá z nich má označenie Ax.

Rozlišujeme nasledovné akcie:

A0 - inicializácia v továrni, nastavenie bezpečnostnej politiky, PIN kódu a označenia

V tomto kroku je potrebná inicializácia všetkých kryptoelementov. Ako bolo uvedené v podkapitole 3.3, kryptoelement musí počas prevádzky spĺňať niekoľko atribútov. Tie budú vynútené nastavením parametrov modulu. Ďalej uvedené parametre sú nezávislé od toho, v akom režime sa zákazník rozhodne používať systém zásuviek.Parametre závislé od zákazníkom zvoleného bezpečnostného profilu sa nastavujú neskôr (akcia A2).

- Ak príde k systémovej zmene, všetky uložené certifikáty a symetrické kľúče musia byť odstránené. Za takúto zmenu považujeme napríklad pokus o úpravu kritických nastavení (zamedzenie čítať symetrické kľúče).
- Certifikát certifikačnej autority bude nahraný do modulu ako prvý. V tomto kroku nie je nahrávaný samotný certifikát CA, nastavuje sa len spomenutá vlastnosť, aby počas zvyšnej prevádzky zariadenia bola daná podmienka splnená.
- Certifikáty, ktoré budú do zariadenia nahraté musia byť podpísané CA, ktorý je v pamäti kryptomodulu.

V tomto stave sa taktiež v továrni nahráva unikátny PIN kód, ktorý bude neskôr potrebný pre úvodnú konfiguráciu servisným zariadením cez Bluetooth.

Taktiež je definované označenie spomenuté v podkapitole 3.4.1.

Spätný prechod zo stavu S2 do stavu S1[26] nie je možný.

[26]teda opačná akcia k akcii A0

A1 - nadviazanie prvého spojenia so servisným zariadením, nahratie certifikátu CA, voľba bezpečnostného profilu a aktualizácia času

Po zakúpení a nainštalovaní častí systému[27] je potrebné ich spárovanie. Zberným bodom a zásuvkám je potrebné bezpečne nahrať certifikát CA. Nahratie do zberných bodov a servisných zariadení prebieha po sieti protokolom, ktorého obsah je nad rámec našej práce. Pre tento úkon je potrebné jednotlivým zberným bodom a servisným zariadeniam nastaviť IP adresu zberného bodu, na ktorom sa nachádza certifikačná autorita. Spomenutý protokol neslúži len na nahratie certifikátu CA, ale aj pre ďalšiu komunikáciu – žiadosti o certifikáty alebo zasielanie nameraných dát na spoločné úložné miesto.

Pre správne fungovanie je potrebné nahranie certifikátu CA aj do zásuviek. Tento úkon je potrebné previesť bezpečným spôsobom. V našom protokole je zabezpečený prostredníctvom protokolu Bluetooth. Servisné zariadenie, ktoré už vlastní certifikát CA sa pripojí cez bluetooth k zásuvke. Pre autentifikáciu je použítý PIN kód, ktorý bol do zásuvky nahraný počas výroby (akcia A0) a je súčasťou balenia. Servisné zariadenie tento PIN kód musí poznať a predpokladá sa, že ho zákazník vopred do zariadenia nahral (prepísal z balenia alebo ho iným automatizovaným spôsobom načítal, napríklad naskenovaním QR kódu). Po nadviazaní spojenia cez Bluetooth servisné zariadenie nahrá certifikát CA do zásuvky, ktorá si ho uloží do pamäte a kryptomodulu.

Nakoniec servisné zariadenie nahrá zoznam parametrov bezpečnostného

[27] v tomto kontexte sa pod inštaláciou myslí namontovanie zásuviek do steny alebo pripojenie zberných bodov k počítaču alebo k počítačovej sieti (ak ide o samostatný modul)

CA		žiadateľ
1	$\leftarrow SYNC$	
2	$ACK \rightarrow$	
3	$\leftarrow CSR$	
4	$C_z \rightarrow$	
5	$\leftarrow ACK$	

Tabuľka 3.4: Proces generovania certifikátu

profilu, ktorý si zvolil zákazník a zásuvke sa oznámi aktuálny čas. Tento profil získalo servisné zariadenie pri nahrávaní certifikátu CA z hlavného zberného bodu.

A2 - vygenerovanie certifikátu a vytvorenie komunikačných slotov

Zariadenie nachádzajúce sa v stave S3 je pripravené na spárovanie. V prvom rade je potrebné vytvorenie certifikátu pre zariadenie, ktoré sa má do systému pripojiť (ďalej ako žiadateľ). Následne si komunikujúce strany vytvoria sloty. Celý proces je vizualizovaný v grafoch 3.4 a 3.5.

Spárovanie vždy iniciuje zariadenie, ktoré sa chce do systému pripojiť. Túto správu budeme označovať ako SYNC. V prípade zberného bodu zasiela žiadosť druhému zbernému bodu, na ktorom sa nachádza CA. IP adresu, kde sa zberný bod s CA nachádza zadáva zákazník do žiadajúceho zberného bodu.

Žiadosť zásuviek je v pravidelných intervaloch vysielaná[28]. Na žiadosť o spárovanie odpovedá zberný bod, ktorého úlohou je v budúcnosti komuni-

[28]je použitý majákový mód popísaný v podkapitole 3.3.5

zberný bod		zásuvka
1	$C_{zb}, N, E_{C_z-pub}(nonce, K, IV)$ →	
2	← $E_K(nonce)$	
3	$E_K(nonce + 1)$ →	

Tabuľka 3.5: Proces tvorby slotu

kovať so zásuvkou.

V oboch prípadoch je odpoveďou akceptovanie žiadosti správou ACK. Ak žiadateľ vysiela žiadosti, kým neobdrží správu ACK.

Odpoveďou je zaslanie CSR. Postupuje sa podľa popisu uvedeného v podkapitole 3.4.1 a teda sa predpokladá, že žiadateľ už má vytvorený súkromný a verejný asymetrický kľúč. Následne žiadateľ obdrží podpísaný certifikát. V tomto kontext je označený ako C_z.

Na záver musí žiadateľ potvrdiť prijatie certifikátu, aby druhá strana vedela, že prišlo k úspešnej výmene.

V prípade, že je žiadateľom zásuvka, celá výmena CSR a certifikátu s CA je sprostredkovaná zberným bodom, ktorý zaslal správu ACK. Pod sprostredkovaním rozumieme preposlanie CSR certifikačnej autorite, keď ho pošle zásuvka a opačne v prípade certifikátu.

Týmto krokom žiadateľ obdržal svoj certifikát. Ďalej budeme opisovať proces vytvorenia komunikačného slotu.

Nakoľko komunikácia medzi zbernými bodmi je riadená protokolom nezávislým od tejto práce, vytvorenie slotov sa týka len komunikácie medzi zbernými bodmi a zásuvkami. Vytvorenie slotu iniciuje zberný bod a to hneď

po odoslaní certifikátu do zásuvky[29]. Zašle správu obsahujúcu certifikát zberného bodu, N pre názov slotu a ďalšej časti správy, ktorej obsah je zašifrovaný verejným kľúčom zásuvky[30]. Zašifrovaná časť obsahuje:

- nonce - unikátne číslo zložené z časovej pečiatky (4 bajty vyjadrujúce aktuálny čas od 1.1.2017) a 28 bajtov, ktoré budú náhodne zvolené[31]
- kľúč K vytvorený zberným bodom, ktorým bude za pomoci AES šifrovaná komunikácia[32] medzi týmto zberným bodom a zásuvkou
- inicializačný vektor IV tiež vytvorený zberným bodom, ktorým bude potrebný pri šifrovaní AES v CBC móde

Zásuvka následne overí:

- či ide o certifikát zberného bodu[33]
- či bol certifikát podpísaný spoločnou CA
- či nie je certifikát exspirovaný

Ak neprebehla kontrola korektne, zásuvka odošle správu *fail*, v inom prípade odošle ako odpoveď *nonce* zašifrovaný kľúčom K a inicializačným vektorom, ktorý zásuvka obdržala od zberného bodu.

[29] krok číslo 4 predchádzajúceho procesu

[30] tento kľúč zberný bod pozná, nakoľko certifikát s týmto kľúčom už zásuvke zasielal

[31] na tento účel je možné použiť kryptomodul, ktorý podporuje generovanie náhodných čísel

[32] po úspešnom vytvorení slotu

[33] či sa útočník nepokúsil použiť certifikát kompromitovanej zásuvky, využije sa označovanie zariadení spomenuté v podkapitole o certifikátoch

Po obdržaní si môže zberný bod vytvoriť vo svojej pamäti slot. Naviac, aby si zásuvka potvrdila, že celá výmena prebehla korektne, je potrebné, aby zberný bod odoslal zásuvke potvrdzovaciu správu. Pôjde o *nonce* zväčšený o 1 a zašifrovaný kľúčom K a inicializačným vektorom IV. Hodnota je zväčšená o 1, aby nemohol útočník vykonať replay attack už známou správou.

Následne si aj zásuvka môže z dohodnutých parametrov vytvoriť komunikačný slot a prejsť do stavu S4.

A3 - žiadosť o nový certifikát a A4 - použitie nového certifikátu

V prípade, že nastane čas, po ktorom je potrebná obnova certifikátu (hodnota je uvedená v tabuľke 3.1), vlastník certifikátu je povinný si požiadať o aktualizáciu certifikátu. Proces žiadania je zhodný s popisom procesu 3.4 v akcii A2.

Počas presunu zo stavu A4 do stavu A5 zodpovedá prvému kroku zo spomenutého popisu a to zaslaniu príkazu *SYNC*. Následne zariadenie čaká v stave S5 na odpoveď ACK, aby mohol žiadateľ zaslať CSR. Po obdržaní certifikátu sa žiadateľ vracia akciou A4 do bežnej prevádzky, pričom prichádza k aktualizácii certifikátu na slote, na ktorom bol pôvodný certifikát.

Avšak, ak by počas čakania na akciu 2 (odpoveď ACK) alebo akciu 4 (zaslanie nového certifikátu) uplynulo viac ako tri minúty, zásuvka sa bez zmeny vracia do stavu S4 a žiadosť znova zopakuje o 24 hodín. Neúspech tejto akcie môže byť spôsobený krátkodobým či dlhodobým výpadkom komunikácie zberného bodu so zásuvkou.

Počas celého procesu aktualizácie funguje zariadenie bez zmeny, ako by sa stále nachádzalo vstave S4 t.j. zásuvka naďalej meria a šifruje namerané

dáta kľúčom K respektíve zberný bod komunikuje so všetkými zásuvkami bez zmeny.

A5 - exspirácia certifikátu

Ak sa zariadeniu mnohonásobne nepodarilo zaktualizovať certifikát, mohlo dôjsť až k jeho exspirácii. V tomto prípade sa zariadenie vracia do stavu S3 a je znovu potrebné vygenerovanie certifikátu a vytvorenie komunikačného slotu. Spomenutým prechodom zariadenie opúšťa stav bežnej prevádzky a teda nevykonáva naďalej štandardné úlohy – napríklad zásuvka naďalej nemeria spotrebu a nešifruje namerané dáta.

A6 - aktualizácia symetrického kľúča

Ako bolo spomenuté, platnosť symetrického kľúča, ktorým sa šifrujú dáta potrebné na prenesenie partnerovi, je jeden týždeň. Následne je potrebná aktualizácia tohto kľúča. Proces aktualizácie iniciuje zberný bod a je zhodný s procesom 3.5. Nakoľko proces začína zberný bod, nie je potrebný vznik špeciálneho stavu, v ktorom by musela zásuvka čakať na odpoveď, ako tomu bolo pri aktualizácii certifikátu. V prípade, že proces nezačne po uplynutí týždňovej lehoty, zásuvka je naďalej povinná namerané dáta šifrovať pôvodným kľúčom.

I keď aktualizáciu začína zberný bod, zásuvka môže ku kroku 2 procesu 3.5 pristúpiť až v momente, kedy zariadenie nemá vo flash pamäti uložené dáta, ktoré ešte neboli odoslané. Ak je pamäť prázdna, je možné pristúpiť k aktualizácii kľúča.

Dáta, ktoré vzniknú počas aktualizácie kľúča nebudú dočasne šifrované

a budú uložené v operačnej pamäti. Po treťom kroku procesu, kedy zberný bod potvrdí akceptáciu aktualizácie, zásuvka nahradí v komunikačnom slote (a teda v kryptoelemente) starý kľúč novým a dáta nazbierané v operačnej pamäti dodatočne zašifruje. Ak by počas čakania prišlo k zaplneniu pamäte, postupuje sa stratégiou zahadzovania najstarších dát.

Reset do továrenských nastavení

Zo všetkých stavov S2-S5 je možné vykonať ešte akciu resetovania do továrenských nastavení. Táto akcia nebola uvedená grafe komunikáciu[34]. Akcia je podnietená zopnutím resetovacieho tlačidla. V prípade zásuvky je tlačidlo umiestnené v jej tele a teda je možné ho zopnúť len v prípade odstránenia chrániaceho plastového krytu. Preto tento zásah môže vykonávať len elektrotechnik.

3.4.7 Výnimočné udalosti

Počas prevádzky môže dôjsť k niektorým výnimočným udalostiam. Ďalej uvádzame, ako tieto udalosti rieši náš protokol.

Výpadok času

Ako je v živote bežné, v elektrickej sieti nastávajú výpadky elektrického prúdu. Nakoľko naša zásuvka nemá vlastný záložný zdroj energie, ľahko môže dôjsť k výpadku merania a tiež pozastaveniu čipu, ktorý má na starosti udržovanie aktuálneho času. Aj kvôli tomuto faktu zberné body zasielajú v pravidelných intervaloch zásuvkám informáciu o aktuálnom čase.

[34] z dôvodu lepšej prehľadnosti

V prípade, že ak dôjde k výpadku elektrického prúdu, zásuvka po opätovnom zapnutí zistí, že došlo k výpadku. Aby mohla zásuvka čo najvierohodnejšie oznámiť stav spotreby, namerané dáta od času opätovného zapnutia označí v pamäti špecifickým príznakom. Keď zásuvka znova obdrží informáciu o aktuálnom čase, zásuvka posunie čas nameraných dát na skutočný čas, kedy bolo meranie prevedené. Ak by prišlo znova k výpadku skôr, ako by sa zásuvka dozvedela informáciu o aktuálnom čase, žiaľ dáta by nebolo možné posunúť o požadovanú časovú hodnotu. V tomto prípade nebude v nameraných dátach rozpoznateľné, že prišlo k 2 alebo viacerým výpadkom. Všetky namerané dáta budu po sebe idúcou postupnosťou meraní.

Krátkodobá nedostupnosť

Ako bolo v popise protokolu uvedené, v prípade krátkodobých výpadkov môže zásuvka pracovať bez akýchkoľvek obmedzení. Aktualizácia certifikátu bude odsunutá na nasledujúci deň a aktualizácia symetrického kľúča bude vykonaná hneď opätovnom nadviazaní spojenia a vyzvaní zberným bodom.

Dlhodobá nedostupnosť

Za dlhodobý výpadok považujeme stav, kedy sa namerané dáta nezmestia do flash pamäte. V prípade týchto výpadkov je situácia zložitejšia. Je možné uplatniť jeden z dvoch scenárov uvedených v podkapitole s aspektami a to:

- ak nám to bezpečnostný profil dovoľuje, môžeme zašifrované dáta znova rozšifrovať a uložiť ich vo forme aritmetického priemeru
- budeme automaticky odstraňovať najstaršie dáta

Keďže naše šifrovanie funguje v CBC móde, ľahko príde k rozsynchronizovaniu komunikačných slotov, nakoľko odstraňovaním najstarších dát prichádza k strate informácie, ak inicializačný vektor je potrebné použiť. V týchto prípadoch je potrebné, aby po obnove spojenia boli pred zaslaním nameraných dát zosynchronizované inicializačné vektory prostredníctvom existujúceho synchrónneho komunikačného slotu.

S dlhodobou nedostupnosťou je spojená možnosť aj exspirácie certifikátu. V tomto prípade sa zariadenie vracia do stavu S2 a všetky uložené štruktúry a namerané dáta odstráni z pamäte. Zostáva mu jedine bezpečnostná politika z továrne, PIN kód, názov zariadenia, certifikát CA a nastavenia bezpečnostného profilu.

Viac časových radov

Ako bolo uvedené v podkapitole 3.3.9, v protokole uvažujeme s možnosťou, kedy budú do pamäte ukladané dáta v rôznych paralelných časových radoch, aby v prípade dlhodobého výpadku bolo možné zabezpečiť obnovu starších dát v priemerovanej podobe. Pre tento účel je potrebné vytvorenie viacerých komunikačných slotov a teda pre každý časový rad jeden slot. Množstvo slotov a ich granularitu určuje bezpečnostný profil.

3.4.8 Broadcast a multicast správy

Na náš podnet boli do systému zaradené aj broadcastové a mulicastovné správý. Našim zámerom bolo ušetrenia veľkého množstva šifrovania v prípade, že sa v systéme generujú príkazy s rovnakým obsahom. Príkladom môže byť pravidelné zasielanie aktuálneho času všetkým zásuvkám.

zberný bod		zásuvka
1	$C_{bc/mc}, N, E_{C_z-pub}(nonce, K)$ →	
2	← $K(nonce)$	
3	$K(nonce + 1)$ →	

Tabuľka 3.6: Proces tvorby slotu - broadcast a multicast

Rozhodli sme sa, že v modely uplatníme druhý spomenutý scenár z podkapitoly 3.3.11, a teda, že každý zberný bod bude spravovať vlastné broadcastové a multicast-ové domény.

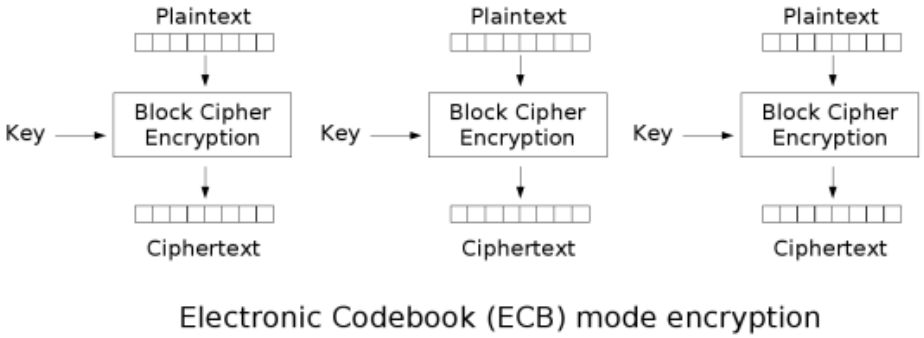
Pre uvedené správy sú v systémoch zriadené samostatné certifikáty. Na komunikáciu sa taktiež využívajú komunikačné sloty a vznikajú podobný spôsobom. Na rozdiel od vytvárania slotu so zbernom bodom, v tomto prípade je v prvej fáze zasielaný certifikát multicastovej respektíve broadcastovej domény. Tento certifikát je odlíšiteľný iným názvom (namiesto *ZB_xxx* je použité *MC_xxx*). Pre broadcast nie je potrebné vytváranie špeciálneho názvu, nakoľko ide len o typ multicastu.

Taktiež v šifrovanej v tele šifrovanej časti správy sa nenachádza IV, nakoľko pri multicastových správach sa bude využívať šifrovanie v ECB móde (obrázok 3.3). Týmto dôvodom je potreba nezávislosti od predchádzajúcich správ.

Taktiež na rozdiel od štandardných komunikačných slotov, v tomto prípade neiniciuje aktualizáciu symetrického kľúča zásuvka, ale zberný bod.

V našom návrhu existujú 2 typu multicast-ových správ: správy vyžadu-

[35]Zdroj: `https://commons.wikimedia.org/wiki/File:Ecb_encryption.png` [citované 28.4.2017]



Obr. 3.3: ECB mód šifrovania[35]

júce odpoveď a správy nevyžadujúce odpoveď. V prvom prípade ide napríklad o príkazy na aktualizáciu nastavenia v zásuvke. Akceptačnú správu zasiela zásuvka prostredníctvom komunikačného slotu, ktorý bežne používa na štandardnú komunikáciu. Potvrdenia sú v systéme potrebné, aby zberný bod vedeľ, ktoré zásuvky obdržali informáciu o aktualizácii a ktorým treba aktualizáciu osobitne zopakovať.

V prípade správ, ktoré nevyžadujú odpoveď môže ísť napríklad o aktualizáciu času.

3.4.9 Dokumentácia ku kryptoelementu

Pri návrhu protokolu sme vychádzali z voľne prístupných informáciach o kryptoelemente[6]. Mali sme snahu kontaktovať aj firmu NXP, ktorá je výrobcom samotného elementu. Naše úsilie však bolo v priebehu šiestich mesiacov márne a žiaľ napriek veľkému množstvu žiadostí o prístup k podrobnej dokumentácii nám nebolo zo strany NXP vyhovené. Podrobnú špecifikáciu

sme chceli využiť na čo najpresnejšie definovať požiadaviek, ktoré musia byť zahrnuté v bezpečnostnej politike a bezpečnostných profiloch. Žiaľ, ako bolo spomenuté aj v kapitole 1.1.2, firmy stále tvoria produkty podľa hesla *security by obscurity*.

Záver

V našej práci sme priniesli prehľad známych chýb, ktoré sa objavili v *IoT* protokoloch. Tento prehľad ukázal, že aj bežne nasadzované systémy, ktoré sú denne používane, majú chyby vo svojich návrhoch.

Spravili sme bezpečnostnú analýzu aj konkrétneho riešenia inteligentnej zásuvky. Podarilo sa nám nájsť zraniteľnosti, ktoré by mohli spôsobiť ľahký prístup neautentifikovanému útočníkovi k dôverným informáciám alebo by bolo možné v mene zásuvky odosielať dáta.

V poslednej časti práce sme zhrnuli požiadavky na inteligentnú zásuvku a tiež aspekty, ktoré ovplyvňujú návrh bezpečného komunikačného protokolu. Všetky tieto informácie, spolu s informáciami o zraniteľnostiach iných zariadení sme využili pri návrhu nového komunikačného modelu, ktorého cieľom je zabezpečiť dôverný prenos dát o spotrebe elektrickej energie a tiež riadiacich príkazov zo zberných bodov jednotlivým zásuvkám.

Navrhnutý protokol môže byť použitý nie len pre inteligentné zásuvky, ale aj iné zariadenia internetu veci, ktoré majú podobné komunikačné požiadavky.

Literatúra

[1] Opensource comunity. Open-ZWave Library. https://github.com/openzwave/.

[2] Kennedy D and Simon R. Pentesting over Power lines. *Defcon*, 2011. https://www.defcon.org/images/defcon-19/dc-19-presentations/Kennedy/DEFCON-19-Kennedy-Pentesting-Over-Powerlines-2.pdf.

[3] Sigma Designs, 2017. http://z-wave.sigmadesigns.com/design-z-wave/embedded-development-kits/.

[4] Behrang Fouladi and Sahand Ghanoun. Honey, I'm home!!-Hacking Z-Wave Home Automation Systems. *Black Hat USA*, 2013.

[5] Behrang Fouladi and Sahand Ghanoun. Security evaluation of the Z-Wave wireless protocol. *Black hat USA*, 1:1–6, 2013. https://sensepost.com/cms/resources/conferences/2013/bh_zwave/Security%20Evaluation%20of%20Z-Wave_WP.pdf.

[6] NXP. A700x family - Secure authentication microcontroller. http://www.nxp.com/documents/short_data_sheet/A700X_FAM_SDS.pdf.

[7] OWASP. Top IoT Vulnerabilities, 2015. `https://www.owasp.org/index.php/Top_IoT_Vulnerabilities`.

[8] International Telecommunication Union. Overview of the Internet of things ITU-T Y.4000/Y.2060 (06/2012). `http://handle.itu.int/11.1002/1000/11559`.

[9] Juha T Vainio. Bluetooth security. In *Proceedings of Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory, Seminar on Internetworking: Ad Hoc Networking, Spring*, 2000. `http://www.yuuhaw.com/bluesec.pdf`.

[10] Jeroen Vollenbrock. Hacking the Neighbor's Home: How Secure are Proprietary Wireless Home Automation Protocols?, 2016.

[11] Joshua Wright. Killerbee: practical zigbee exploitation framework. In *11th ToorCon conference, San Diego*, 2009. `http://www.willhackforsushi.com/presentations/toorcon11-wright.pdf`.

Bezpečnostné profily			
Bezpečnostná funkcia	Štandardný profil	Paranoidný profil	Užívateľský profil (možnosti naviac)
Použite sym. šifry	AES-128	AES-256	AES-192
Kompresia dát vs šifrovanie	priebežná tvorba aritmetických priemerov	dáta budú šifrované, nebude umožnené ich dešifrovanie a po naplnení pamäte budú najstaršie dáta mazané	povoliť vytvorenie dešifrovacieho orákula alebo priebežná tvorba priemerov, ale s vlastne definovanými intervalmi