Závěrečná zpráva

Projekt: **Monitorování bezdrátových sítí Internetu věcí pro zvýšení bezpečnosti**

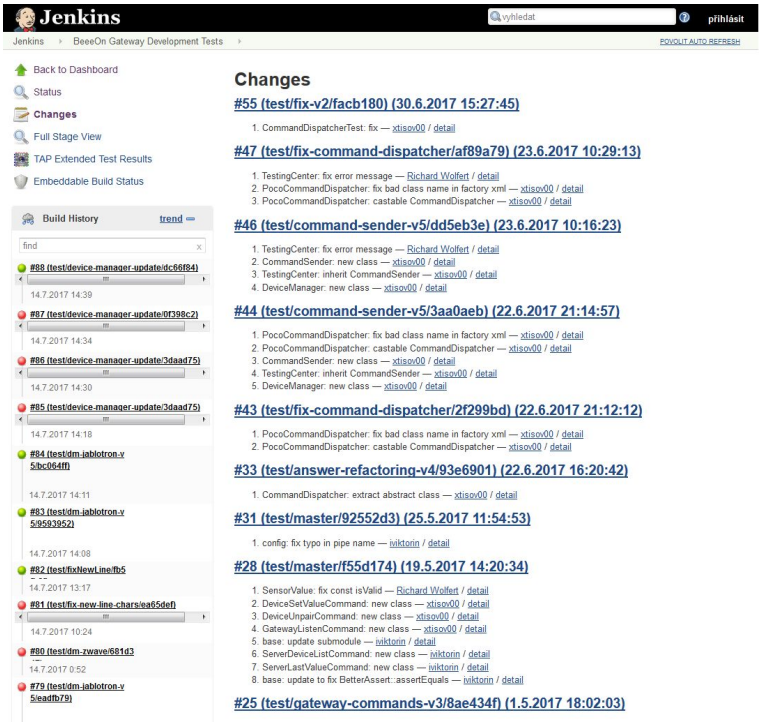
Hlavní řešitel: Ing. Pavol Korček, Ph.D. - FIT VUT v Brně

Spoluřešitel: Ing. Tomáš Novotný - FIT VUT v Brně

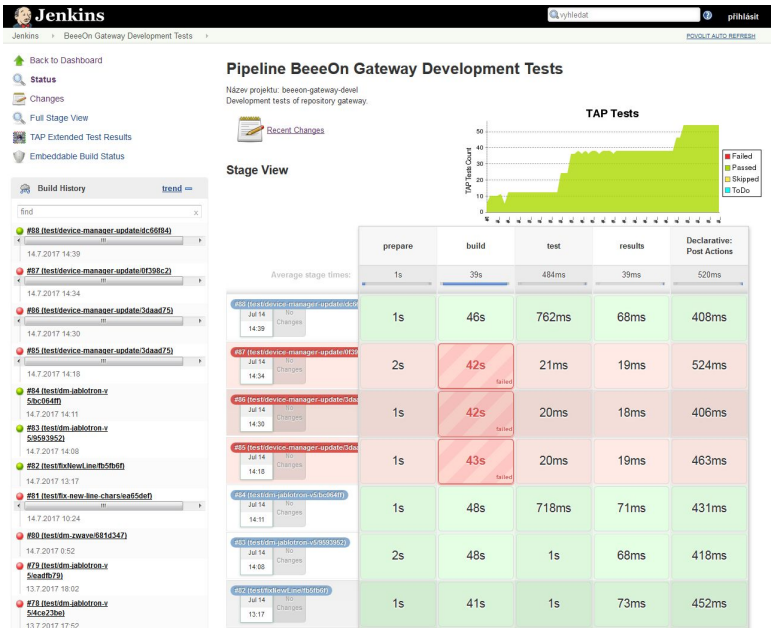
Obsah

1. Postup při řešení, způsob řešení

Řešení projektu bylo rozděleno do několika částí. V rámci přípravy byly nakoupeny 2 servery, na kterých byla uvedena do provozu dvě prostředí. První prostředí bylo určeno pro samotný vývoj softwarového řešení a druhé pro organizační zajištění tohoto projektu a podporu vývoje. Vzájemně pak byly tyto servery pravidelně zálohované. První prostředí poskytovalo pro členy týmu čistě linuxové prostředí spolu se základními nástroji, prostředím pro překlad zdrojových kódů software (tzv. křížovou kompilaci pro cílové architektury routerů ARM/MIPS) spolu se systémem pro správu verzí *(Git)*. Naopak druhé prostředí na druhém serveru bylo sice také postaveno nad linuxovým systémem, ale navíc byl instalován open-source systém *Redmine* pro řízení projektů, pro tzv. bug-tracking a pro uložení vývojářské dokumentace s kompletní historií změn. Také jsme využívali open-source systém *Jenkins* (viz Snímek č. 1 a Snímek č. 2) a to za účelem automatického testování vyvíjeného software.



Snímek č. 1: *Sledování změn kódu ve vybrané "úloze" systému Jenkins.*



Snímek č. 2: *Celkový přehled vybrané "úlohy" s historií v systému Jenkins.*

Dále bylo postupně v rámci řešení projektu nakoupeno několik bezdrátových senzorů a komunikačních USB donglů pro ně, dále součástky pro vývoj modulů a senzorů, které se postupně integrovaly a testovaly na vyvíjeném software.

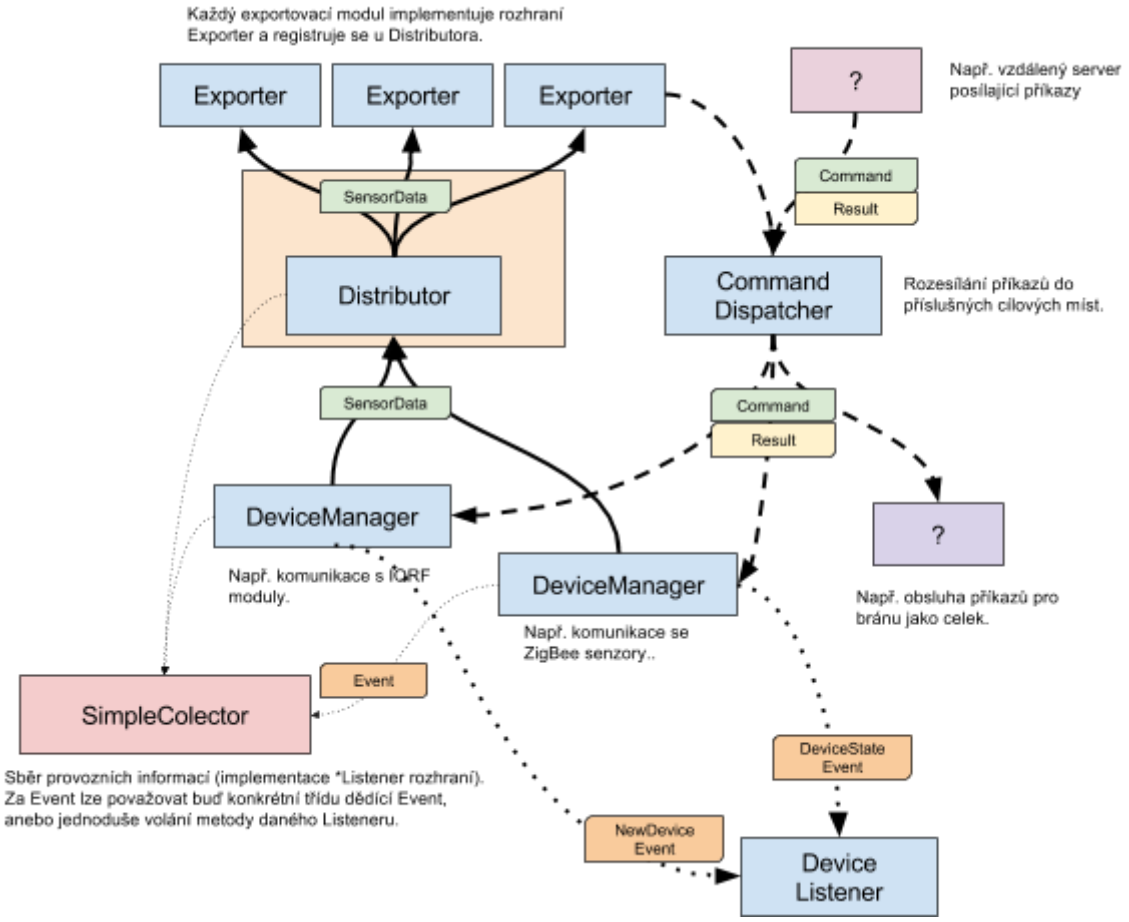
Se samotným vyvíjeným software byl plán využít vhodné části softwarového základu open-source zájmového projektu BeeeOn na FIT VUT v Brně (www.BeeeOn.org). Projekt BeeeOn si klade za cíl vyvinout kompletní systém, který je rozšiřitelný o podporu nových senzorů. Kompletním systémem je myšleno celé prostředí od senzorů, přičemž aktuálně má projekt BeeeOn jeden vlastní senzor (pro vlhkost a teplotu zároveň), až po vlastní, zdarma dostupnou, aplikaci pro mobilní telefony s OS Android. Tato aplikace je pak určená pro zobrazovaní dat z připojených senzorů. Mezičlánkem popisovaného systému je ještě adaptér, skrze který se připojují právě bezdrátové senzory. Adaptér odesílá všechna data do další části systému a to serveru pro sběr a uložení dat samotných. Samotný adaptér je postaven nad open-hardware platformou OLinuXino A10 od bulharské společnosti Olimex. Platforma s rozšiřující rádiovou deskou je vyobrazená na Snímku č. 3.

Snímek č. 3: *BeeeOn adaptér a jeho platforma OLinuXino s rozšiřující rádiovou deskou.*

Ze systému BeeeOn by byla v tomto projektu využitelná zejména softwarová část adaptéru (tzv. *adaapp*, dostupná zde: https://github.com/BeeeOn/gateway-app). Detailní analýzou bylo však zjištěno několik skutečností, kvůli kterým bylo nutné přistoupit na vlastní řešení. Mezi hlavní nedostatky existujícího software patřilo zejména:

- *Formát exportovaných dat ze senzorů není jednoduše definovatelný s jasně definovaným rozhraním. Navíc neexistuje podpora exportu dat ve standardním formátu*
- *Není umožněno získat a tedy i exportovat provozní data senzorické sítě (např. počet zahozených, chybných, přeposlaných apod.) rámců, které mohou být velice důležité z pohledu další analýzy bezpečnosti*

Pro vážnost uvedených problémů bylo přistoupeno na kompletní návrh vlastní architektury softwarového vybavení, které bude vycházet ze zkušeností z předchozí implementace a zároveň odstraňovat uvedené nedostatky. Byla tedy navržená a implementovaná nová aplikace "*Gateway"* (běžněji používaný název v oblasti IoT než "adaptér"), která sestává z několika ústředních komponent. Tyto komponenty umožňují sběr a distribuci dat ze senzorické sítě a senzorů samotných a řízení aktivních prvků na základě příkazu z řídicího serveru (tato část byla ponechána z původní implementace tak, aby nová implementace mohla být dále využívaná i v projektu BeeeOn). Řešení je vyobrazeno na Snímku č. 4.

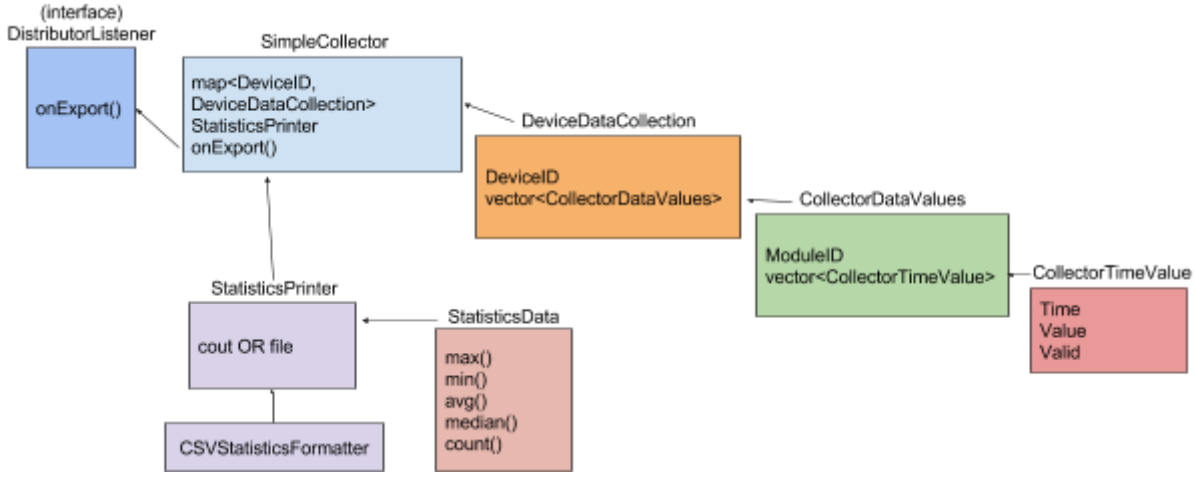


Snímek č. 4: *Navržená architektura software s vyznačením komunikace.*

Jádrem vyvíjené aplikace Gateway jsou potom především:

- **Distributor** - přijímá veškerý datový provoz ze senzorů a provádí export do různých exportovacích úložišť
- **CommandDispatcher** - rozesílá příkazy od řídicího serveru
- **DeviceManager** - spravuje konkrétní senzorovou síť (Z-Wave, IQRF, …), má znalosti o použité technologii, může generovat události týkající se dané sítě
- **SimpleCollector** - sbírá data z různých komponent systému a ukládá je dle nastavení

Samotná aplikace exportuje skrze *Exporter* čistá (raw) senzorická data. Navíc byl také implementován *SimpleColector* určen pro sběr jiných dat a událostí v celém systému (vyobrazen na Snímku č. 5).



Snímek č. 5: *Implementovaná architektura SimpleCollector.*

Ten obsahuje tzv. asociativní kontejner, kde klíčem je *DeviceID* (id zařízení) a obsahem struktura *DeviceDataCollection*. V této struktuře je pak vektor dalších struktur *CollectorDataValues*, kde jsou jednotlivé typy hodnot, jelikož jedno zařízení může poskytovat více veličin, označené *ModuleID*. *CollectorTimeValue* je nejnižší úroveň, kde jsou spojeny naměřené hodnoty s časem pořízení. SimpleCollector dle konfigurace vypisuje navíc průběžné statistiky (implicitně ve formátu CSV). Výpis zajišťuje *StatisticsPrinter*, který načte data z CollectorData pro vybrané období a předá je pro zpracování třídě *StatisticsData*. Ta nad daty vypočítá základní matematické operace a výsledky poskytuje dále.

Implementovaný software byl dále rozšířen o sadu testů, které se v pravidelných intervalech a po změně zdrojových kódu spouštěly (jako tzv. úlohy v systému Jenkins), čímž se testovala integrita po provedení změn. Software se ale také nasadil do testovacího prostředí v laboratoři na FIT VUT v Brně, které simulovalo reálné využití senzorů. Za tímto účelem se využívalo již hotové prostředí ostatních částí systému BeeeOn (výše uvedená serverová část a Android aplikace).
Kromě integračních testů a testů v reálném prostředí byl pro experimentální a testovací účely reimplementován také systém tzv. virtuálních senzorů, což je simulace senzorického

zařízení. Virtuální senzor periodicky generuje hodnoty dle nastavení v konfiguračním souboru, kde je jich možno definovat neomezený počet.

Následně jsme se dle plánu věnovali portaci vyvinutého software pro otevřenou platformu OpenWRT (https://openwrt.org/), který se používá v síťových zařízeních a domácích routerech. Protože byl však OpenWRT v průběhu řešení nahrazován postupně novějším projektem LEDE (https://lede-project.org/) vycházejícím z OpenWRT, rozhodli jsme se vytvořit instalační balík právě do prostředí LEDE.

2. Dosažené cíle

V projektu se podařilo dosáhnout cílů, které byly určeny při návrhu projektu. Hlavním cílem řešení projektu bylo vytvořit systém pro monitorování bezdrátových sítí IoT a připravit tak vhodné prostředí pro detekci bezpečnostních incidentů. Byl vytvořen software umožňující monitoring IoT zařízení, sběr provozních informací z různých zařízení v IoT síti. Funkcionalita systému a implementovaný software byly průběžně testovány a také ověřeny v pilotním provozu a to v rámci vytvořeného testovacího prostředí. Celé řešení je nasaditelné pomocí vytvořeného instalačního balíčku.

3. Zdůvodnění případných změn v projektu

V projektu nebyly provedeny zásadní změny a výsledky projektu odpovídají tomu, co bylo navrhováno při podání projektu. Jedinou změnou v projektu je nákup 2 ks serverů z prostředků FIT VUT v Brně místo původně plánovaného 1 ks, a to pro účely rozdělení administrativní a vývojové části řešení projektu na nezávisle avšak vzájemně zálohované servery.

4. Konkrétní výstupy, další využitelnost

Hlavním výstupem projektu je software umožňující monitoring IoT zařízení a to pomocí sběru různých typů dat. Tím prvním typem dat jsou **čistá data ze senzorů,** kterých ukázka následuje v podporovaném formátu JSON:

{"device_id":"0xff00000000000001","timestamp":1500452407,"data":[{"module_id":0,"value":-4.99293}]}
{"device_id":"0xff00000000000002","timestamp":1500452407,"data":[{"module_id":0,"value":0.00707212}]}
{"device_id":"0xff00000000000003","timestamp":1500452407,"data":[{"module_id":0,"value":5.00707}]}
{"device_id":"0xff00000000000001","timestamp":1500452417,"data":[{"module_id":0,"value":6.9928}]}
{"device_id":"0xff00000000000002","timestamp":1500452417,"data":[{"module_id":0,"value":11.9928}]}
{"device_id":"0xff00000000000003","timestamp":1500452417,"data":[{"module_id":0,"value":16.9928}]}

a taká ukázka exportu v podporovaném formátu CSV:

sensor;1500452556;0xff00000000000001;0;-4.99;
sensor;1500452556;0xff00000000000002;0;0.00;
sensor;1500452556;0xff00000000000003;0;5.00;
sensor;1500452566;0xff00000000000001;0;6.99;
sensor;1500452566;0xff00000000000002;0;11.99;
sensor;1500452566;0xff00000000000003;0;16.99;

V obou případech jsou exportovány informace o typu zprávy, časová značka (timestamp), identifikátor modulu a samotná hodnota. Samotné formáty výstupu jsou nastavitelné (v *conf/gateway-startup.in*i).

Dále je možné pomocí software možné nad čitými daty počítat **statistiky.** Ukázka statistických hodnot následuje v tabulce:

DeviceID	ModuleID	Min	Max	Avg	Median	Count	NonValid
0x90000000019664a	2	100	100	100	100	34	0
0x90000000019664a	1	1	2	1.41	1	34	0
0x90000000025607e	2	100	100	100	100	60	0
0x90000000025607e	0	25.8	26.3	26.13	26.15	30	0
0x90000000025607e	1	10	40	28.92	30.25	30	0
0x900000000640280	2	100	100	100	100	66	0
0x900000000640280	0	1	1	1	1	64	0
0x900000000640280	1	1	2	1.5	1.5	2	0
0x9000000007f3862	2	100	100	100	100	5	0
0x9000000007f3862	1	1	2	1.2	1	5	0
0xff00000000000001	0	-4.99	10	2.78	2.93	360	0
0xff00000000000002	0	0.01	15	7.78	7.93	360	0
0xff00000000000003	0	5.01	20	12.78	12.93	360	0

Architektura implementovaného software ale také umožňuje sbírat **metadata (např. provozní informace) či jiné události** z ostatních částí systému (např. z rozhraní napojení na konkrétní bezdrátovou síť - komponenta *DeviceManager*) a to také pomocí komponenty *SimpleCollector.* Konkrétní data/události jsou ponechány na uživateli, protože to vždy závisí od konkrétní bezdrátové sítě.

Všechna data je možné dále zpracovávat a formátovat dle požadavků přijímací strany. Takovou stranou může být monitorovací nebo jiné analyzační prostředí, které tato data dále zpracováva.

Dalším výstupem projektu je zabalení uvedeného software pro systém LEDE (https://github.com/BeeeOn/lede-packages-frc), čímž je umožněno tento software provozovat na široké škále síťových zařízení a také na domácích routerech.

5. Přínosy projektu, vlastní hodnocení

Přínos projektu: Projekt řeší velice podstatnou část tzv. monitoringu, který souvisí s bezpečností bezdrátových sítí využívaných nejen v rámci konceptu IoT. Až na základě kvalitního monitoringu je totiž možné vykonávat další analýzy a z té pak vyvozovat incidenty/události související s bezpečností. Uvedený postup je dnes znám např. i z běžných IP sítí a v rámci sdružení CESNET je využit v rámci projektu NEMEA (https://www.liberouter.org/technologies/nemea/).
Aktuálně se vyvinutý software integruje do již běžícího projektu *"Zabezpečená brána pro Internet věcí"* (SIoT), který sdružení CESNET řeší jako hlavní řešitel v druhé veřejné soutěži ve výzkumu, experimentálním vývoji a inovacích programu "Bezpečnostního výzkumu České republiky 2015 - 2020 (BV III/1 – VS)" vyhlášené Ministerstvem vnitra České republiky dne 21. října 2015. Cílem uvedeného projektu je sestavovat modely chování jednotlivých uzlů bezdrátové sítě, vytvářet systémy detekce anomálií v prostředí projektu NEMEA a sekundárně pak řídit prvky a procesy pro obranu jednotlivých uzlů. Systém vyvinutý v tomto projektu poskytuje právě monitorovací část uvedeného komplexního řešení.

Vlastní hodnocení: Projekt zpracoval a vyřešil všechny body z návrhu projektu. Podařilo se navrhnout a implementovat komplexní systém, který již je využíván přímo sdružením CESNET. Osobně tedy hodnotím výsledky a přínos projektu pozitivně.

6. Tisková zpráva – 2 řádky textu (cca 300 znaků) s odkazem na web řešitele

FIT VUT v Brně ve spolupráci se sdružením CESNET vytvořil software pro OpenWRT/LEDE směrovače, který umožňuje poskytovat data k zajištění lepší bezpečnosti sítí Internetu věcí. Uvedený software je využít sdružením CESNET v běžících projektech pro další analýzu získaných dat a pro detekci incidentů.

Odkaz na web hlavního řešitele: http://www.fit.vutbr.cz/~ikorcek/