Sem vložte zadání Vaší práce.

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Diplomová práce

Detekce anomálií v provozu IoT sítí

Bc. Dominik Soukup

Katedra počítačových systémů
Vedoucí práce: Tomáš Čejka

17. ledna 2018

Poděkování

Doplňte, máte-li komu a za co děkovat. V opačném případě úplně odstraňte tento příkaz.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval(a) samostatně a že jsem uvedl(a) veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 46 odst. 6 tohoto zákona tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou, a veškeré jejich dokumentace (dále souhrnně jen „Dílo“), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla, a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené. Každá osoba, která využije výše uvedenou licenci, se však zavazuje udělit ke každému dílu, které vznikne (byť jen zčásti) na základě Díla, úpravou Díla, spojením Díla s jiným dílem, zařazením Díla do díla souborného či zpracováním Díla (včetně překladu), licenci alespoň ve výše uvedeném rozsahu a zároveň zpřístupnit zdrojový kód takového díla alespoň srovnatelným způsobem a ve srovnatelném rozsahu, jako je zpřístupněn zdrojový kód Díla.

V Praze dne 17. ledna 2018 .....

Odkaz na tuto práci

Soukup, Dominik. *Detekce anomálií v provozu IoT sítí.* Diplomová práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2018.

Abstrakt

V několika větách shrňte obsah a přínos této práce v češtině. Po přečtení abstraktu by se čtenář měl mít čtenář dost informací pro rozhodnutí, zda chce Vaši práci číst.

Klíčová slova Nahraďte seznamem klíčových slov v češtině oddělených čárkou.

Abstract

Sem doplňte ekvivalent abstraktu Vaší práce v angličtině.

Keywords Nahraďte seznamem klíčových slov v angličtině oddělených čárkou.

Obsah

Seznam obrázků

Úvod

Koncept internetu existuje již několik desítek let a pro spoustu lidí se stal nedílnou součástí pracovního i osobního života. V poslední době je možné sledovat stále rostoucí počet zařízení, která jsou do něj zapojena. Tento trend by měl pokračovat i do budoucnosti, a dokonce v ještě větším měřítku. Odhadem je přes 30 miliard připojených zařízení do roku 2020 [1]. Důvodem zrychleného růstu je expanze síťového připojení na veškeré elektronické zařízení a senzory, která umožní vzdálené řízení a monitorování. Pro označení tohoto trendu se používá termín Internet věcí (Internet of Things, IoT).

Cílem IoT je usnadnit, zlepšit a ušetřit lidskou činnost napříč všemi odvětvími. Uplatnění se nachází zejména ve výrobních podnicích, dopravě nebo běžných domácnostech. Dále je upraven model komunikace, který již nevyžaduje zasílání zpráv centrálnímu serveru (north-south), ale podporuje přímou komunikaci mezi připojenými uzly (east-west). Oblast IoT nezahrnuje jen malá a nevýkonná zařízení, ale jeho součástí jsou i výkonná datová centra a pokročilé algoritmy, které vyhodnocují získané informace.

Hlavní hrozbou Internetu věcí je bezpečnost. Získaná data slouží k automatizovanému řízení dalších systémů, nebo dokonce k zabezpečovacím účelům. Důležité je tedy získávat validní data a mít možnost detekce útoků jako v běžných IP sítích.

Kapitola 1

Cíl práce

Cílem magisterské práce je analyzovat množinu aktuálně používaných protokolů pro komunikaci v IoT sítích a identifikovat jejich bezpečnostní zranitelnosti. Na základě získaných znalostí bude navžen, implementován a otestován algoritmus pro detekci anomálního provozu v IoT sítích. Algoritmus bude možné spustit v prostředí nově vznikající zabezpečené IoT brány BeeeOn.

Kapitola 2

Analýza

Kapitola se zabývá analýzou celkové architektury IoT sítí a způsoby pro jejího zabezpečení. Postupně je prozkoumán komunikační model, možné bezpečnostní hrozby, a existující řešení pro obranu. Na základě analýzy jsou uvedeny funkční a nefunkční požadavky, které jsou kladeny na výsledný program. V závěru jsou vybrány konkrétní technologie pro realizaci.

2.1 Architektura IoT sítí

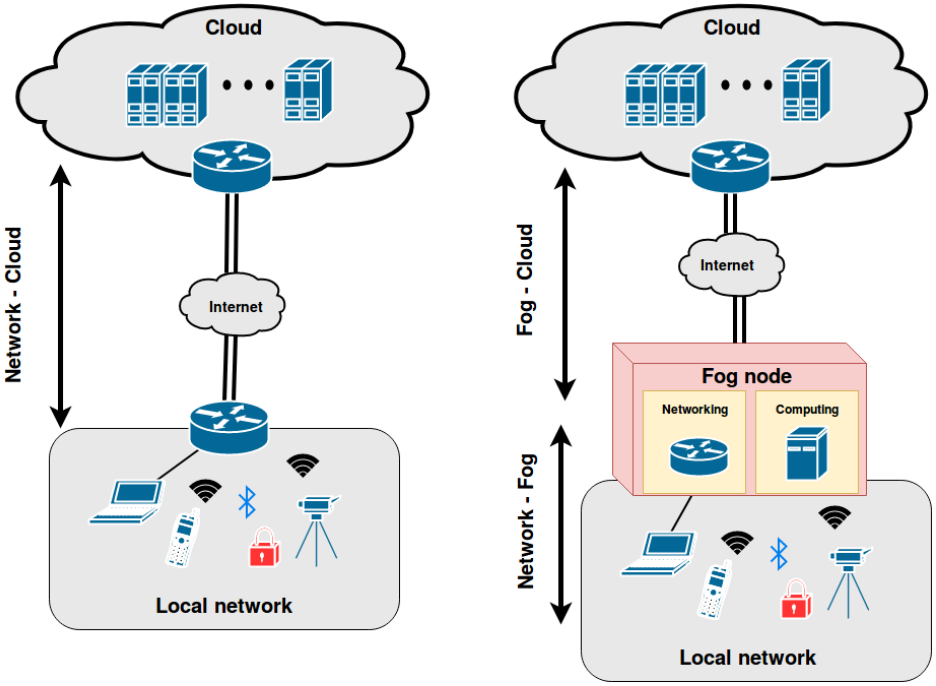
V blízké době se očekává stále větší nárůst zařízení, která jsou připojena k internetu. Dle odhadů by jejich počet měl v roce 2020 překročit 30 miliard [1]. Pro takové množství připojení už není možné, aby každé zařízení komunikovalo přímo se vzdáleným datovým centrem, protože nároky na potřebnou šířku pásma by byly obrovské [2]. Dalším problémem je často velmi omezený výkon připojených prvků, který je nezbytný pro použití bezpečnostních funkcí umožňujících kompletně zabezpezpečenou komunikaci.

Řešení těchto problémů je do probíhající komunikace přidat několik podvrstev, které umožní přesunout výpočetní výkon blíže ke koncovým zařízením, a tím celý proces zpracování dat provést efektivněji.

2.1.1 Fog computing

Fog computing je rozšíření Cloud computingu, které spočívá v přesunutí výpočetního výkonu blíže k okraji sítě. Rozšíření je umožněno pomocí přidání síťových zařízení, které kromě síťových funkcionalit nabízí i výpočetní výkon pro běh programů. Programy je často možné nasadit pomocí konterjnerů nebo samostatných virtuálních strojů, což velmi usnadňuje jejich distribuci [2].

Porovnání klasické a Fog architektury se nachází na obrázku 2.1. V reálném nasazení může být použito i více Fog vrstev, kde každá provádí určitý stupeň předzpracování a řízení dat. Zavedením principů Fog computingu vznikají pro síť následující výhody:



Obrázek 2.1: Porovnání klasické a Fog architektury

- **Zlepšení bezpečnosti** [2]

  Síťové prvky jsou trvale napájené a připojené k internetu. Podporují pokročilé bezpečnostní funkce, a proto je možné například vytvářet šifrované tunelové spojení pro bezpečný přenos dat.

- **Nižší nároky na šířku pásma a latency** [2]

  Odeslaná data z koncových zařízení jsou zpracovávána a filtrována na okraji sítě. Tím je možné rychleji reagovat na přijaté zprávy a snížit nároky na latency a šířku pásma. Zároveň krátkodobá data mohou být uložené ve Fog vrstvě a centrální datové cetrum může být využito pro dlouhodobé údaje, které se zpracovávají pokročilými algoritmy pro analýzu dat.

- **Jednotná správa** [2]

  Při správě sítě už se nemusí přistupovat přímo na koncové prvky, které často komunikují různými protokoly, ale stačí pouze řídit síťová zařízení v jednotlivých Fog vrstvách, které odstiňují různorodost protokolů a nabízí standardizovaný přístup. Díky této abstrakci je zároveň zjednodušeno zpracování získaných dat a je umožněno přímé zasílání zpráv mezi koncovými prvky, které používají odlišné komunikační protokoly.

2.1.2 IoT brána

IoT brána je síťové zařízení, které je umístěno velmi blízko koncových zařízení a představuje vstup do Fogové vrstvy. Jejím hlavním cílem je získávat data z připojených zařízení a poskytovat je vyšším vrstvám. Pokud je brána reprezentována výkonnějším síťovým prvkem, tak v rámci brány může probíhat i základní zpracování dat.

Pro IoT sítě je typické, že obsahují velké množtví koncových prvků komunikujících různorodými způsoby. Zejména senzory používají protokoly, které nepodporují IP (Internet Protocol) spojení. Důvodem použití této komunikace je často velký důraz na nízkou spotřebu a specifické požadavky na způsob zasílání zpráv. Příkladem protokolů pro senzorové sítě ne například: Z-Wave, Bluetooth a Zigbee. Jejich detailní popis se nachází v kapitole 2.3. Tato různorodost vyžaduje od brány, aby obsahovalo dodatečná rozhranní, které umožní připojení nejrůznějších bezdrátových i drátových koncových prvků.

2.1.3 Komunikační model a jeho hrozby

Při použití principů popsaných v předchzích kapitolách lze model komunikace do následujících vrstev [3]:

- Aplikační vrstva
- Síťová vrstva
- Senzorová vrstva

Jednotlivé vrstvy budou popsány v následujích podkapitolách.

2.1.3.1 Senzorová vrstva

2.1.3.2 Síťová vrstva

2.1.3.3 Aplikační vrstva

2.2 Analýza síťových protokolů

2.3 Analýza senzorových protokolů

2.4 Způsoby obrany

2.5 BeeeOn brána

2.6 NEMEA framework

2.7 Existující řešení

2.8 Analýza požadavků

2.9 Zvolené řešení

Kapitola 3

Návrh

Kapitola 4

Realizace

Kapitola 5

Testování

Závěr

Literatura

[1] Statista: Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025. Statista. [online], 2016 [cit. 2018-01-14]. Dostupné z: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[2] Statista: Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are. Cisco. [online], 2015 [cit. 2018-01-15]. Dostupné z: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf

[3] Zhao, K.; Ge, L.: A Survey on the Internet of Things Security. In *2013 Ninth International Conference on Computational Intelligence and Security*, 2013, s. 663–667.

Příloha **A**

Seznam použitých zkratek

GUI Graphical user interface

XML Extensible markup language

Příloha **B**

Obsah přiloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `exe` ..... adresář se spustitelnou formou implementace
- `src`
  - `impl` ..... zdrojové kódy implementace
  - `thesis` ..... zdrojová forma práce ve formátu LaTeX
- `text` ..... text práce
  - `thesis.pdf` ..... text práce ve formátu PDF
  - `thesis.ps` ..... text práce ve formátu PS