VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Excel@FIT 2022

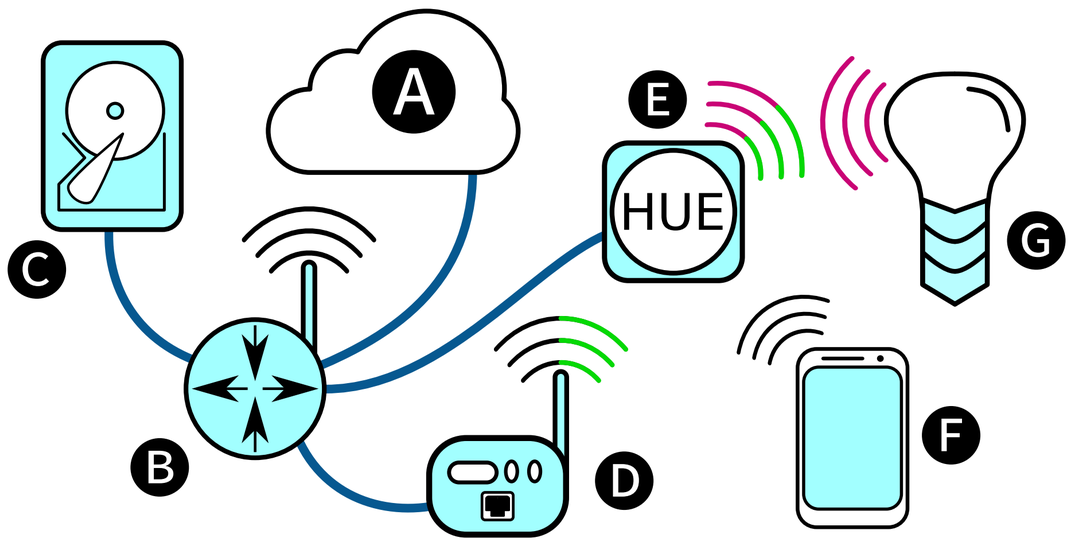
Analýza síťové komunikace IoT bran

Jan Zbořil, xzbori20@stud.fit.vutbr.cz
vedoucí: Mgr. Kamil Malinka, Ph.D. EasyChair submission ID: 1

Cíle

- Analyzovat síťový provoz IoT bran pro domácí použití
- Navrhnout a diskutovat možné útoky
- Vytvořit otisky komunikace
- Demonstrovat význačné prvky chování

Prostředí



A = Cloud, B = Turris Router,
C = Externí SSD,
D = tesotvaná IoT brána,
E = Phillips Hue Bridge,
F = smartphone s ovládací aplikací,
G = žárovka Phillips Hue

Testované brány: Aeotec Smart Home Hub, Amazon Echo, Google Nest Mini, Home Assistant SW gateway

Postup

1. Sestavení prostředí
2. Sbírání dat
   - pasivní režim - 7 bez vnějšího zásahu
   - aktivní režim – Opakovaně manipulovat s chytrou žárovkou
3. Analýza pomocí Zeek, Wireshark, Excel
4. Prezentace výsledků
5. Porovnání výsledků s existujícími studiemi

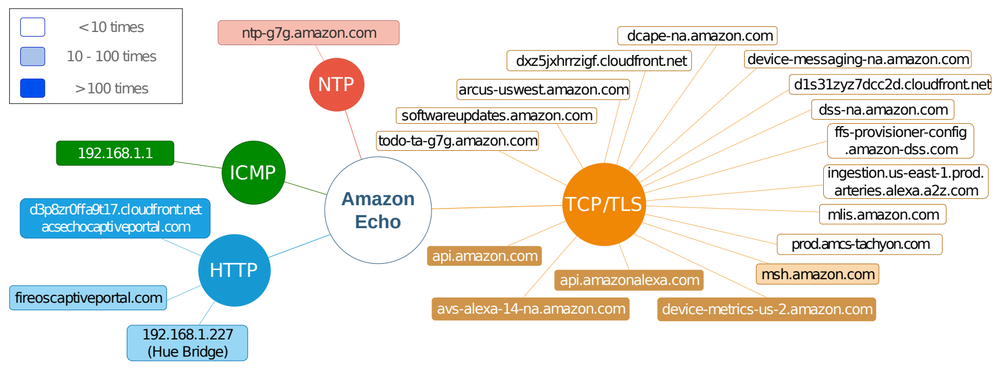
Analýza

Aeotec Hub

- Zachycen provoz při manipulaci se žárovkou
- Pakety: TLS 28.6 %, UDP 9.8 %, DNS 6.2 %
- služby Aeotec hostovýny na Amazon AWS

Amazon Echo

- Nejvíce provozu ze všech testovaný bran



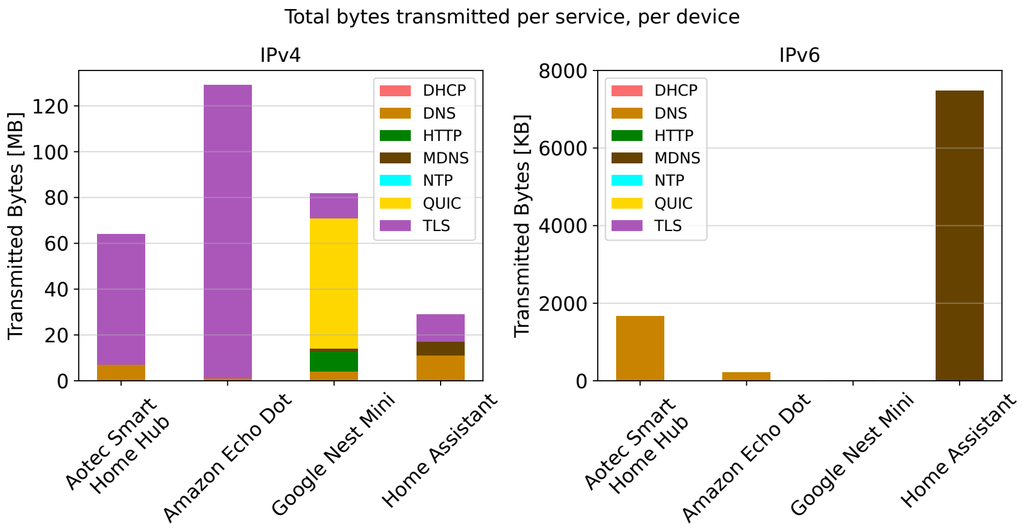
Google Nest

- Využívá DNS servery Google (8.8.8.8)
- Využívá protokol QUIC
  - vlastnosti HTTPS, TLS a TCP přes UDP

Home Assistant

- Open Source → nesbírá mnoho uživatelských dat → nejnižší naměřený objem dat
- Připojení k nejméně koncovým bodům

Výsledky



- Možnost vytvořit otisk zařízení z vlastností provozu
- Ne všechny studie v oblasti IoT jsou 100% správné
- Využívání šifrované komunikace TLS je na vzestupu a nyní tvoří základ komunikace