Fakulta Informatiky a Informačných Technológii
Slovenská Technická Univerzita

ZÁPISNICA 15

04.04.2023

Monitoring of LoRa IoT Devices
Tím č. 3 Molid

Miestnosť 1.19

Prítomní Ing. Alexander Valach

Bc. Michal Greguš

Bc. Adrián Ondov

Bc. Adam Melicher

Bc. Matej Laš

Bc. Dorota Gajdošová

Bc. Michal Minár

Neprítomní

Obsah stretnutie

- Opäť došlo k výpadku systému Siem, po porade s vedúcim, ktorý nám poradil, že problémom by mohla byť tentokrát expirácia pravidla na FW sme skontrolovali pravidlá na FW a skutočne sme potvrdili, že dôvodom výpadku bola expirácia pravidla a teda blokovanie premávky z brán a chirpstacku
- Po náprave sme však zistili, že do Siemu stále netečú logy z niektorých brán
- Michal upravil zdrojový kód zariadení tak aby odosielali dáta o teplote, pričom vytvoril aj jedno koncové zariadenie, ktoré odosielalo chybné dáta, čo malo symbolizovať anomáliu v nameraných dátach
- Adrián a Dorka analyzovali zdrojový kód zariadení a odprezentovali postup plánovanej úpravy zdrojového kódu ako aj spôsob detekcie útoku typu replay ako aj porušenia vysielacích regulácii
- Následne sme viedli diskusiu o spôsobe realizácie útoku porušenia vysielacích regulácii. V zmysle plánu EU868 môžu jednotlivé koncové zariadenia vysielať denne len určité množstvo dát tak aby nedošlo k porušeniu regulácie vysielacieho pásma. Pôvodne sme plánovali navrhnúť detekčne pravidlá schopné identifikovať zaradenia porušujúce vysielacie regulácie. Aby sme však vedeli otestovať správnosť fungovania detekčného pravidla museli by sme sami porušiť vysielacie regulácie. Toto sme však v rámci diskusie vyhodnotili ako nekorektné a preto sme sa rozhodli navrhnúť si vlastný model, kde budú koncové zariadenia odosielať dáta každých 30s a v systéme Siem budeme identifikovať zariadenia odosielajúce dáta častejšie čo môže signalizovať porušenie vysielacích regulácii ako aj menej často čo môže signalizovať slabnutie batérie na zariadení alebo prítomnosť nejakého rušenia v okolí daného zariadenia.
- Michal a Matej úspešne nainštalovali file integrity monitoring, pričom zároveň vytvorili aj detekčné pravidlo na identifikáciu alertov pri neoprávnenej zmene sledovaných súborov

Úlohy a poznámky

- Zdebugovať brány a identifikovať prečo nie sú logovacie správy korektne odosielané a logované v systéme Siem (Matej, Michal, Adam)

- Dokončiť úpravu zdrojového kódu zariadení a nahrať zdrojový kód na zariadenia (Adrián, Dorka)
    - Vytvoriť návrh pravidiel pre kontrolu vysielacích regulácii resp. Metodiku vytvárania návrhu týchto pravidiel vzhľadom na vybrané veľkosti dátovej časti a zahrnúť ho do dokumentácie
- Napísať detekčné pravidlá na vysielacie regulácie, detekciu anomálie a replay útok (Adam, Michal)
- Postupne začať spisovať dokumentáciu k riešeniu projektu (Všetci)
- Vykonať útok zmeny polohy brány a tak otestovať úspešnosť implementácie

Autor Bc. Michal Greguš