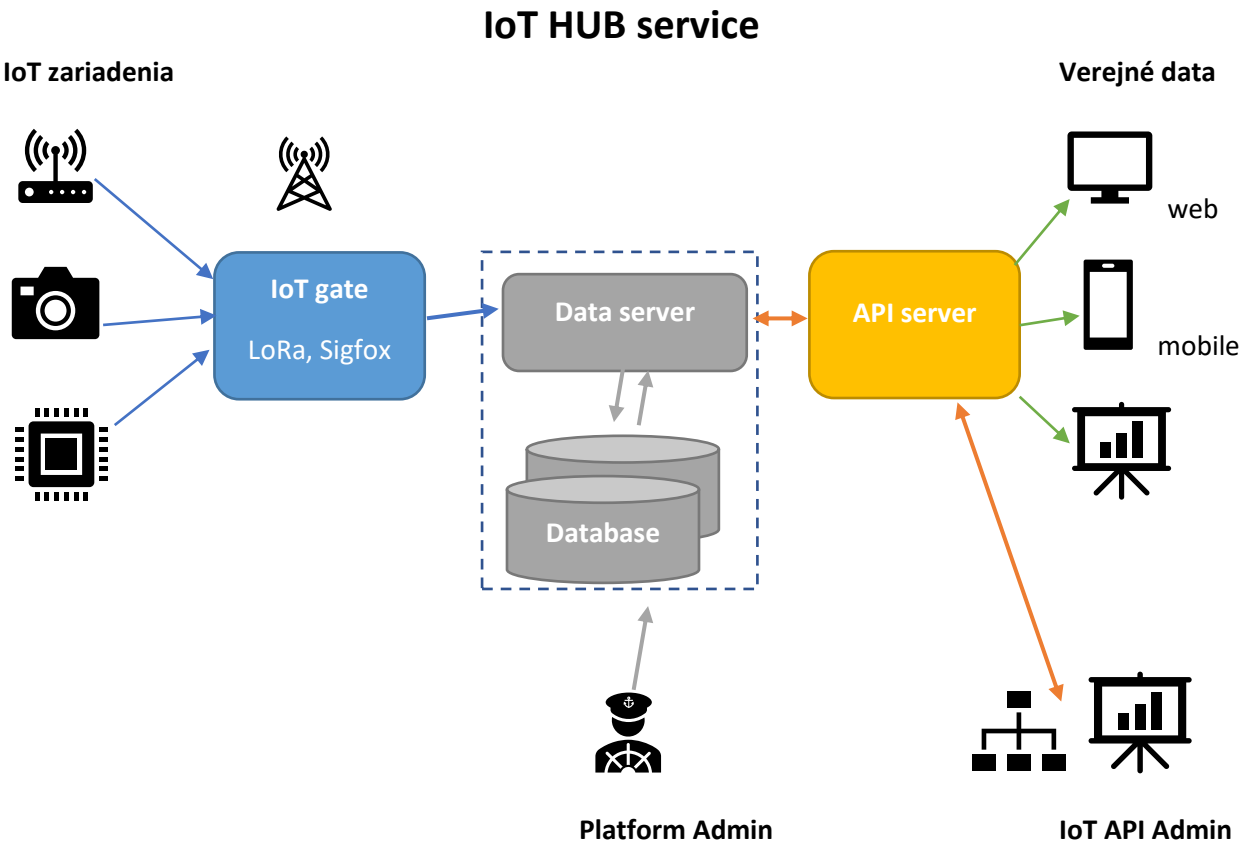
Úvod do počítačovej bezpečnosti FEI STU

Modelovanie hrozieb

[Zadanie 1]

1 Návrh informačného systému

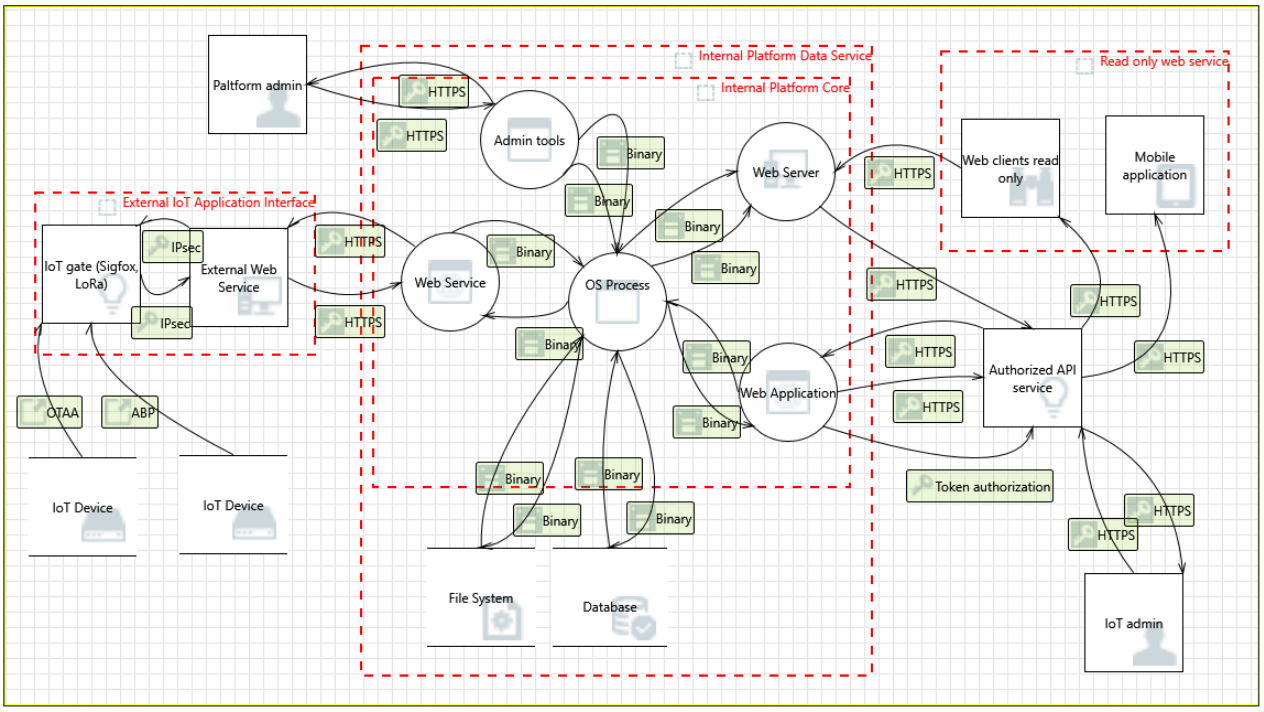
Pre svoj projekt som si vybral na modelovanie informačný systém **Centralizovaná platforma pre monitorovanie s právu zariadení Internetu vecí IoT.** Táto platforma bude poskytovať API rozhrania na zhromažďovanie informácií z IoT zariadení a na následný prístup k týmto údajom.



Systém ma fungovať ako webový service, ktorého správu ma pod kontrolou „Platform admin“. Platforma komunikuje priamo s IoT operátorom a zabezpečuje užívateľské prostredie na správu a monitorovanie vlastných IoT zariadení, ktoré sú u operátora registrované. Ak sa IoT admin rozhodne zverejniť svoje údaje, môže ich zdieľať pomocou web aplikácie a mobilnej aplikácie.

2 Data flow diagram a trust boundaries

Architektúra systému sa delí na 3 hlavné časti, a to sú prijatie a odšifrovanie prijatých dát z IoT zariadení, spracovanie a uloženie prijatých dát podľa užívateľských nastavení a nakoniec, vizualizácia dát.



3 Modelovanie hrozieb metodikou STRIDE

STRIDE – Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privileges

3.1 Spoofing

Pri spoofingu útočník predstiera svoj totožnosť pomocou IP, ARP za účelom získania autentifikačných oprávnení. V mojom informačnom systému je zraniteľný touto metódou hlavne prístupový portál pre IoT administrátora. Ak sa útočník dostane do IoT administrátorského účtu dokáže manipulovať s užívateľskými dátami.

Ochrana

Administrátorky prístup bude pri registrácií vyžadovať silné heslo, navyše kontrola prihláseného užívateľa – session nebude prebiehať na základe **cookies** ale vždy bude generovaná **nová session**. Proti spoofingu som pre môj systém navrhol prídavnú **autentifikáciu pomocou tokenov**, ktorá umožní len oprávneným užívateľom pristúpiť na administrátorský portál.

Navyše v každej TCP komunikácií je použité SSL šifrovanie pomocou HTTPS, dokonca aj IoT zariadenia majú svoju alternatívu unikátnych identifikátorov na sieti – OTAA (Over the air activation) a ABP (Activation by personalization), táto komunikácia je teda šifrovaná 128 bitovým kľúčom.

3.2 Tampering

Útok metódou tamperingu prestavuje modifikáciu či odstránenie dát na ktoré sa systém spolieha alebo poskytujú funkčnosť iným funkcionalitám. Takýto útok mohol byť pre môj systém smerovaný na poškodenie databázy pomocou SQL injection alebo Js exploit na frontend – Cross site scripting.

Ochrana

Integrita databázy je chránená filtrami stringov vstupov do queries aby sme nedovolili útočníkovi obísť autentifikáciu pomocou **SQL injection**. Tento filter bude implementovaný na backend strane systému, aby mal útočník čo najmenej informácií o filtrovaní.

Proti Cross site scriptingu musíme dohliadnuť aby žiadny užívateľský vstup nemohol obsahovať JS/HTML exploit. To dosiahneme ďalšími filtrami a čítaním HTML zdrojov z databázy pri novom requeste.

Aby sme sa vyhli tragickým chybám v prípade prelomenia autentifikácie niektorého zo systémových administrátorov, títo budú rozdelený to skupín podľa oprávnení a najme podľa prístupu k súborom.

3.3 Repudiation

V prípade nejednoznačnosti vykonaných operácií alebo pokusu o neoprávnený vstup do systému bude každá anomália aj bežná činnosť zapisovaná do logov. Tieto logy budú mať podobný stupeň ochrany ako samotné užívateľské data.

V tejto súvislosti navrhnem pridať do systému redundantnú databázu, kedy výstup bude správny len v prípade ak oba redundantné údaje sú zhodné.

3.4 Information Disclosure

Tento problém nastane ak sa neoprávnený užívateľ alebo útočník dostane k informáciám ktoré mali byť pred ním skryté. V mojom systéme je zdieľanie a vizualizácia dát pravé kľúčovým produktom, preto musia byť aj prístupy k zdieľaným dátam obmedzené.

Ochrana

Napríklad ak IoT admin chce poskytnúť namerané údaje zo svojich IoT zariadení môže vďaka tokenovej autentifikácií vygenerovať unikátny prístupový kľúč pre jedného používateľa. Navyše bude portál admina kontrolovaný na činnosť a po nečnosti dlhšej ako pár minút bude automaticky odhlásený. Taktiež ma napadá feature na kontrolu z akej lokality sa užívateľ prihlasuje, ak to bude neobvyklá lokalita (svetový kontinent), podľa IP, užívateľ bude musieť potvrdiť prihlásenie na emaile.

3.5 Denial of service

Tento útok a riziká z neho plynúce sa vzťahujú takmer na všetky online služby a neexistuje 100% účinný spôsob ako sa ubrániť. Ak útočník vyčerpá naše prostriedky nedá sa už ani brániť.

Existujú spôsoby ako aspoň oslabiť tento útok, napríklad filtrovaním requestom na základe IP adresy, v poslednom rade je možnosť prispôsobiť infraštruktúru systému na zvládnutie útoku, čo sa prejaví na financiách.

3.6 Elevation of provileges

V prípade ak útočník získa práva nad systémom môže znefunkčniť celú infraštruktúru, preto je dobre rozdeliť a spravovať užívateľské práva a dodržiavať best practices pri správe produkčného systému. Best practise sa týkajú napríklad obmedzenia počtu užívateľov so sudo právami. Alebo nezdielať privátne SSH kľúče atď.