SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
Fakulta elektrotechniky a informatiky

Juraj Matejka

.

Autoreferát dizertačnej práce

Security Manažér pre služby HbbTV a IoT

na získanie akademického titulu „doktor“ („philosophiae doctor“, v skratke „PhD.“)

v doktorandskom študijnom programe: Telekomunikácie

v študijnom odbore: 5.2.15 Telekomunikácie

Forma štúdia: externá

Miesto a dátum: Bratislava, 20.6.2017

Dizertačná práca bola vypracovaná na Ústave telekomunikácií FEI STU BA v Bratislave

Predkladateľ Ing. Juraj Matejka
Ústav multimediálnych informačných a komunikačných technológií
Fakulta elektrotechniky a informatiky
Slovenská technická univerzita v Bratislave
Ilkovičova 3, 812 19 Bratislava

Školiteľ: prof. Ing. Pavol Podhradský, PhD.
Ústav multimediálnych informačných a komunikačných technológií
Fakulta elektrotechniky a informatiky
Slovenská technická univerzita v Bratislave
Ilkovičova 3, 812 19 Bratislava

Oponenti: doc. Ing. Ján Papaj, PhD.
Katedra elektroniky a multimediálnych telekomunikácií
Fakulta Elektrotechniky a informatiky TU v Košiciach,
Letná 9, 042 00 Košice

Ing. Tomáš Zeman, PhD.
Katedra telekomunikační techniky FEL ČVUT
Technická 2, CZ-166 27 Praha 6
Czech Republic

Autoreferát bol rozoslaný: .....

Obhajoba dizertačnej práce sa bude konať dňa.....

na .....

.....
dekan FEI STU v Bratislave
Prof. Dr. Ing. Miloš Oravec

Obsah

1 Úvod

Spektrum zariadení pripojených k internetu prudko rastie najmä v priebehu posledných rokov. Zahŕňa široký rozsah PC, pripojených televíznych prístrojov a set-top boxov (STB), domácich mediálnych brán, herných konzol a prenosných zariadení, ako sú tablety či inteligentné telefóny. Prístup k internet TV, videu na požiadanie (VOD), k internetovým službám a k sociálnym sieťam sa stal ľahkým a pohodlným na používanie a to pre všetky vekové skupiny.

S narastajúcim vplyvom internetových služieb a neustálej implementácie podpory internet konektivity aj pre aplikácie v TV a multimediálnych zariadeniach, sa bude svet vysielania a internetu postupne zbližovať. Predtým odlišné svety, ktoré sa svojimi službami skôr neprekrývali, dnes konvergujú a tento proces je čoraz rýchlejší. Zbližujúce sa služby internetovej a TV zábavy teda kladú nároky aj na technológie, ktoré musia podporiť konvergenciu služieb, a to tak, aby prišlo k štandardizácii definovania hybridných architektúr tak, aby sa zachovali atribúty otvorenosti, možnosti prepoužiteľnosti existujúcich komponentov a bezpečnosti. Úspech závisí na dobrej definícii používania služieb. Ako také sú ovplyvnené aj atribútmi použitých technológií. Môžu sa odlišovať v rôznych konceptoch definície identity užívateľov, zariadení či služieb, alebo v ich správe. Otázka prispôsobenia služieb v prostredí internetu a v prostredí domáceho prostredia sa odlišuje a pre jej konvergenciu musí byť dôkladne analyzovaná. V neposlednom rade sa toto týka aj problematiky bezpečnosti a nových spôsobov autentizácie a autorizácie užívateľov, ktoré so sebou služby v multimediálnej domácnosti prinášajú.

IoT (Internet of Things) je rapídne rozvíjajúce sa odvetvie a nepochybne aj „horúca“ téma, na ktorej základe sú (a budú) budované moderné služby. Výraznou výhodou IoT je generovanie veľkého množstva príležitostí pre inovácie, prostredie domácnosti nevynímajúc. Z dôvodu exponenciálneho rastu tzv. „wearables“ zariadení, mobilných aplikáciách aj pre domáce použitie sa zdá, že technológie na báze IoT budú transformovať tradičné technológie v domácnostiach smerom k výraznej personalizácii jednotlivých služieb a tiež k vysokému stupňu interakcie služieb v domácnosti navzájom. Úspešné využívanie IoT v prostredí domácností užívateľov bude reprezentované hlavne v doméne inteligentných domácností (SH- Smart Home). Tieto budú predstavovať nielen výhodu pre svojich užívateľov, či už na poli zvýšenia komfortu, šetrenia nákladov na energie, či zvýšenia bezpečnosti domácností, ale budú predstavovať aj výraznú výzvu v oblasti bezpečnosti samotnej technológie, ochrany dát a súkromia užívateľov nevynímajúc. Je preto otázkou, ako na tieto výzvy odpovedať a ako adresovať ich riešenie tak, aby bolo možné dosiahnuť aj synergické efekty prameniace pre problémy, ktoré sú v oboch doménach podobné.

Táto dizertačná práca sa venuje jednému z problémov uvádzaných v našom dizertačnom projekte - problému bezpečnosti v prostredí HbbTV. Práca rozpracováva túto problematiku v podrobnostiach, a nadväzuje tak na moju prácu v rámci projektu FP7 HBB-NEXT, v ktorom som bol členom riešiteľského tímu. Táto práca v medzinárodnom riešiteľskom kolektíve bola nesporne zaujímavá a svojimi závermi prospela k výskumu hybridného širokopásmového vysielania. Práca reflektuje najnovšie trendy v oblasti a zameriava spracovanie riešenej problematiky aj na oblasť IoT, zvlášť na oblasť Smart Home. Obe tieto technológie sú dnes v popredí záujmu poskytovateľov služieb aj vďaka záujmu užívateľov (GfK, 2017). Služby sa stávajú viac komplexnými, prichádza k snahe čím ďalej tým viac prepájať služby navzájom, kde daňou za zvýšený užívateľský komfort sa stáva vyššia komplexnosť technológií za týmito službami stojacimi. Žiaľ nevyhýbajú sa ani záujmu

tých, ktorý chcú tieto služby zneužiť a či už preniknúť k citlivým údajom osobnej potreby, alebo zneužiť služby samotné.

2 Ciele dizertačnej práce

Úlohou našej dizertačnej práce je potreba navrhnutia systému, ktorý bude súčasťou architektúry HBB-Next, s presne definovanou funkcionalitou pokrývajúcou potrebu autentizácie a autorizácie užívateľov služby, aj z pohľadu možností požitia ďalších faktorov autentizácie, a zároveň aj interných softvérových komponentov HbbTV, pre dosiahnutie požadovaného stupňa bezpečnosti, dôveryhodnosti a privátnosti dát samotných užívateľov týchto služieb. Ako už bolo konštatované, multimediálne služby sa neustále rozvíjajú aj v oblasti kombinácii vzájomnej interakcie užívateľov služieb, preto našim cieľom bude aj návrh systému s perspektívou rozširovania funkcionality hybridných služieb televízie a širokopásmového vysielania smerom k IoT. Je nutné zdôrazniť, že IoT je vo všeobecnosti veľmi široký pojem a náš pohľad na vzájomný prienik multimediálnych a IoT služieb je práve v aplikáciách tz. Smart Home. Ďalším dôležitým aspektom je aj univerzálnosť návrhu, ktorá by mala spočívať v budúcej flexibilite nasadenia rôznych autentizačných protokolov, hoci pre účely tejto práce vyberieme jeden konkrétny. Náš návrh bude musieť spĺňať aj podmienky nasadenia na moderných cloud-ových infraštruktúrach. Výsledok nášho výskumu budeme ďalej v texte označovať ako Security Manager (SM).

Na základe urobenej analýzy a jej vyhodnotenia sme definovali nasledovné ciele dizertačnej práce:

1. Návrh mechanizmu a funkčného modelu implicitnej identifikácie užívateľov vrátane softvérových (sw) modulov a riadenia prístupu ku zdrojom aj s využitím viacfaktorovej autentizácie
2. Návrh mechanizmu a funkčného modelu využívania rôznych poskytovateľov identity pre užívateľov či softvérové moduly HbbTV služieb
3. Návrh systémového a funkčného modelu architektúry Security Manager (SM) ako možnej súčasti architektúry HBB-Next
4. Implementácia navrhnutej architektúry SM a testovanie jeho vybraných funkcionalít.

3 Teoretické a praktické predpoklady

V dnešnom svete je informácia vlastníctvom zákonného vlastníka. Jednotlivec, alebo organizácia si môže zvoliť ochranu takéhoto vlastníctva v prípade, že prístup k nemu, jeho úprava a/alebo nedostupnosť by mohli spôsobiť neželanú situáciu. Preto väčšina jednotlivcov či organizácií chráni svoj najdôležitejší majetok pred možným poškodením. Bezpečnosť teda predstavuje metódy ochrany vlastníctva pred možnou hrozbou (Moosavi, 2015).

3.1.1 Koncepcia bezpečnosti a základné pojmy

Primárnym cieľom bezpečnosti je chrániť "dôvernosť", "integritu" a "dostupnosť" vlastníctva. ***Dôvernosť*** je pojem, ktorý sa používa vtedy, keď je vlastníctvo prístupné len autorizovanému užívateľovi. ***Integrita*** znamená, že vlastníctvo nebolo upravované (modifikované) neautorizovanou osobou ani počas prenosu či vzniku, zatiaľ čo ***dostupnosť***

znamená, že vlastníctvo je prístupné oprávnenému vlastníkovi vtedy, keď je to potrebné (Clapauch, 2012). ***Hrozba*** je čokoľvek, čo môže systému spôsobiť poruchu či škodu.

Typickým bezpečnostným prístupom k vlastníctvu je identifikácia veľkej hrozby a vyhľadanie spôsobov na jej minimalizáciu. Napríklad: významnou hrozbou pre odhalenie informácií je hrozba typu *man in the middle attack* (MITM) / teda odpočúvanie; pre ochranu je možné takúto informáciu zakódovať ešte pred jej prenosom, aby sa útok typu MITM minimalizoval. Vo väčšine prípadov býva bezpečnostná kontrola nastavená bezpečnostnými expertmi na ochranu informácií. Takéto kontroly zahŕňajú užívateľskú autentizáciu a identifikáciu (Choudhary, 2012). Teda existujú tri hlavné bezpečnostné procesy, ktoré kooperujú pri zabezpečovaní prístupu ku konkrétnemu vlastníctvu: autorizácia (*authorization*), autentizácia (*authentization*) a auditovanie (*accounting*) (Garcia-Carrillo, 2016).

- Autentizácia zahŕňa overovanie platnosti identifikácie danej entity
- Autorizácia zahŕňa zabezpečenie prístupu užívateľa k povoleným informáciám
- Auditovanie zahŕňa vedenie záznamov udalostí, ktoré sa vyskytli

3.1.2 Autentizačné mechanizmy

Autentizácia je proces overovania toho, čo o sebe tvrdí užívateľ. Užívateľská identifikácia vždy predchádza užívateľskej autentizácii, pretože identifikácia je to, "čo" užívateľ predstavuje pre bezpečnostný systém, zatiaľ čo autentizácia je proces overovania identity užívateľa. Autentizácia sa obyčajne zakladá na určitých faktoroch (Sha Liu, 2015): čo táto osoba vie - poznanie založené na autentizácii napríklad v podobe hesla; čo táto osoba má - autentizácia založená na vlastníctve, napríklad v podobe ID; a čím táto osoba je - biometricky založená autentizácia ako napríklad odtlačok prsta, alebo zosnímanie dúhovky oka. V závislosti od požadovanej úrovne bezpečnosti môže byť využitý jeden alebo kombinácia viacerých autentizačných faktorov.

3.1.3 Autorizačné mechanizmy

Cieľom autorizácie je určiť, či užívateľ má povolenie k prístupu k dátam/prostriedku (Alrawais, 2015). Inými slovami: ide o proces určovania, či už identifikovaný a autentizovaný používateľ je oprávnený k prístupu k špecifickým informáciám špecifickým spôsobom (More, 2011). Dôvernosť je motivačným faktorom pre autorizáciu, ktorá zabezpečuje, že informácia je prístupná len autorizovanej strane. Autorizačné koncepty sa zakladajú na vopred nakonfigurovanom systéme požiadaviek a užívateľských profilov.

Osobná identifikácia

Ako používateľ preukáže, že je tým, kým je? Osobná identifikácia je v autentizačnom procese tzv. faktorom "niečím si" (Sha Liu, 2015). Osobná identifikácia vždy predchádza autentizačnému procesu, pretože ide o informáciu, ktorú užívateľ preukazuje autentizačnému systému k svojej autentizácii. Pri identifikácii preukazuje užívateľ informácie, aby sa verifikoval či identifikoval, ako napr. užívateľské meno, či ID, alebo biometrické údaje. Užívateľské meno a ID sú všeobecne rozšírené spôsoby identifikácie, avšak vývoj počítačových technológií umožňuje celkom jednoducho zneužiť užívateľské meno a ID, preto sú v dnešnom svete dôležitejšími biometrické údaje než tradičné užívateľské meno a ID (Ishengoma, 2014) (Choudhary, 2012). Dôvodom je aj fakt, že biometrické údaje, akými sú

vzor odtlačku prsta či snímok sietnice oka, svoje hodnoty nemenia a tak môžu byť použité pre identifikáciu jednotlivca.

Biometrické informácie sú zachytené a ukladané v serverových databázach ako podklad pre ďalšiu vyžiadanú autentizáciu. Biometrický systém obyčajne pozostáva zo zachytených biometrických dát, softvéru a hardvéru nevyhnutnému k ich zachyteniu, a softvéru, ktorý zachytené dáta vyhodnocuje. Biometria pre osobnú identifikáciu sa zvyčajne delí na dve kategórie - fyziologickú a behaviorálnu biometriu (Sae-Bae, 2012). Fyziologická biometria zahŕňa odtlačky prstov, snímok odtlačku prsta, geometriu ruky, snímok sietnice oka či snímok tváre, zatiaľ čo behaviorálna biometria zahŕňa užívateľove behaviorálne atribúty ako dynamiku podpisu, dynamiku pohybu myšou a hlasovú či rečovú verifikáciu. Biometria ponúka bezpečnostné vylepšenia oproti iným bezpečnostným kritériám, vrátane nepopierateľnosti, presnosti/bezpečnosti a previerky.

Zhrnutie: identifikácia, autentizácia a autorizácia sú tri bezpečnostné prvky, ktoré zabezpečujú naplnenie bezpečnostných cieľov. Bezpečnostné ciele zahŕňajúce dôvernosť, integritu a dostupnosť, chránia informácie pred neautorizovaným prístupom, neautorizovanou modifikáciou a zabezpečujú, že informácia je vždy dostupná, keď je to potrebné. Užívateľ sa preukazuje niektorou z foriem identifikácie ako je napr. ID, heslo, užívateľské meno alebo aj biometrická informácia pre autentizačný server, ktorý obratom autentizuje užívateľa za pomoci protokolov akými sú napríklad PKI a Kerberos, aby overil, či je užívateľ tým, kým tvrdí, že je. Následne, ak je užívateľ autentizovaný, potom overovateľ overí, či má užívateľ práva k prístupu ku konkrétnemu prostriedku konkrétnym spôsobom, a to použitím protokolov ako sú PMI a Zoznam riadenia prístupu (ACL). Ak overovateľ potvrdí užívateľove práva, potom je prístup povolený.

3.2 Riadenie identít

Systémom identity môžeme nazývať architektúry, ktoré definujú štandardizované mechanizmy umožňujúce zdieľanie atribútov identity užívateľov s aplikáciami či inými službami. Toto umožní

- zjednodušiť a optimalizovať tzv. „*on-line*“ skúsenosť užívateľov,
- zabezpečiť vyššiu ochranu identity pred tými, ktorý by ju chceli zneužiť
- iné príležitosti, ako napríklad vytvorenie možnosti prispôsobovania a personalizácie užívateľských profilov v službách bez potreby manuálnej konfigurácie zo strany užívateľa samotného

Z pohľadu definície súvislostí, rozlišujeme v systémoch správy identít nasledovné entity

Poskytovateľ identity IdP (*Identity Provider*) – je poskytovateľom špecifickej služby, ktorou danému užívateľovi vytvára, prevádzkuje a spravuje informácie o jeho identite, a na základe poverení ich poskytuje iným poskytovateľom služieb

Poskytovateľ služby SP (*Service Provider*) – Je to entita v systéme, ktorá poskytuje špecifickú službu a to aj na základe informácií od poskytovateľa identity IdP.

Užívateľ U – Osoba, ktorá používa informačný systém za účelom služby, pristupuje ku zdrojom či chce zdieľať časť informačných zdrojov s inými užívateľmi či službami.

Klient C (*Client*) – je to služba, ktorá asistuje užívateľovi pri vytváraní či používaní transakcií s jeho identitou

3.2.1 Federovaná správa identít

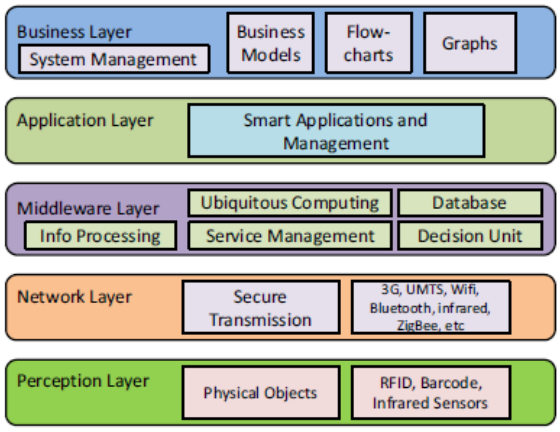
FIM sa teda zaoberá vytvorením vzťahu dôvery medzi rôznymi bezpečnostnými doménami, pre umožnenie zdieľania autentizačných dát pre zníženie komplexnosti riadenia prístupu a zároveň zníženia bezpečnostných rizík. Tiež prispieva k zjednodušeniu autentizačných procedúr pre koncových používateľov, (napríklad použitím SSO - *Single Sign On* (Shim, 2005)). Táto problematika bola skúmaná a aplikovaná v mnohých oblastiach, ako je napríklad web zdroje (Morgan, 2004), web služby (OASIS, 2009) a iných, s potvrdením vysokej relevancie FIM ako takej pre SSO. Avšak táto relevancia môže byť v narušená rizikom podvodu (napríklad krádežou bezpečnostného tokenu) na jednom IdP partnerovi, s následnou kapacitou afektovania ostatných IdP partnerov v rámci federácie (Jensen, 2012).

Technológia SSO bola vyvinutá za účelom riadenia prístupu ku zdrojom, ktorá prepája užívateľa s viacerými cloud službami (Fengming, 2012). SSO môže byť chápané ako podmnožina FIM. Užívateľ po zadaní svojich poverovacích údajov (anglicky: *credentials*) je overený a môže pristupovať k službám bez potreby opätovného prihlasovania sa. Z pohľadu poskytovateľov služieb tu prichádza k zjednodušeniu architektúry a manažmentu užívateľov, a tiež zavádza potrebu vytvorenia dôveryhodného vzťahu medzi autentizujúcimi systémami, teda IdP poskytovateľmi.

3.1 Internet vecí a inteligentné domy

Svet, v ktorom "všetko" komunikuje so "všetkým", zriaďujúci širokú prepojenosť každodenných vecí s ľudskými bytosťami a to spôsobmi, o ktorých sme mysleli, že sú nemožné. Táto prepojenosť "všetkého" odkazuje na tzv. internet vecí (*Internet of Things*, IoT) a ten bol všeobecne definovaný v niekoľkých výskumoch ako vzájomná prepojenosť a komunikácia "všetkého", vrátane ľudí, predmetov/vecí, umožňujúca bezprecedentnú použiteľnosť kedykoľvek a kdekoľvek, pri využití akéhokoľvek pripojenia k sieti či službe (Perera, 2014) (Khan, 2012).

Dnešná internetová architektúra predstavuje vrstvený model podľa TCP/IP modelu. IoT model, ako ukazuje Obrázok 1, je zložený z 5 vrstiev (Khan, 2012): vrstva zariadení/vnímania, sieťová vrstva, middleware vrstva, aplikačná vrstva a vrstva business modelu. Analyzujme jednotlivé vrstvy z hľadiska hlavných bezpečnostných útokov na každú vrstvu.



Obrázok 1: IoT architektúra (Khan, 2012)

Všeobecná architektúra bezpečnosti domácej siete je definovaná podľa ITU-T X.1111 (Arabo, 2012) Prostredie inteligentného domu tvorí komplex heterogénnych prostredí, ktoré

možno rozdeliť do troch kategórií (Brezovan, 2013): domáce spotrebiče, kontrolný systém a systém domovej automatizácie.
Bližšie je architektúra diskutovaná v dizertačnej práci v kapitole 3.

Môžeme konštatovať, že svety chytrých či inteligentných domov a moderných multimediálnych služieb vysielania a zábavy v domácnostiach, sú z pohľadu ich synergického potenciálu dosiaľ budované a rozvíjané do značnej miery osobitne. Chýba tu možnosť zdieľania služieb navzájom na úrovni samotných modulov služby, dosiaľ sa to štandardne deje na úrovni definovaných Push/Pop APIs medzi back-end cloudami jednotlivých služieb TV a IoT osobitne. Je preto z pohľadu bezpečnosti žiadúce analyzovať, ako je možné zdieľať vybrané komponenty TV a IoT/SH spoločne, a to aj s prihliadnutím na univerzálnosť implementácie tak, aby sme spoľahlivo využili ich jednotlivé silné stránky v oblasti identifikácie a autentizácie.

Podľa bezpečnostnej analýzy (OWASP project, 2014), je nedostatočná úroveň autentizácie a autorizácie zaradená medzi TOP10 bezpečnostných hrozieb vo svete IoT, SH nevynímajúc, s priemernou mierou zneužiteľnosti, častým výskytom, ľahkou detekciou zraniteľnosti a vážnym dopadom, aj v závislosti na službe, o ktorú sa jedná konkrétne. Jedná sa prevažne o nedostatky ako nízka úroveň ochrany poverení, neprítomnosť dvojfaktorovej autentizácie, nezabezpečená obnova hesla, neimplementovanie RBAC a podobne. Je preto žiadúce navrhnúť systém, ktorý by uvedené riziká minimalizoval aj s ohľadom na špecifické možnosti technológií moderných hybridných televíznych služieb a sveta internetu vecí.

Ďalej môžeme konštatovať, že uvádzané bezpečnostné štandardy neuvažujú s rôznou klasifikáciou obsahu zdieľaného (SH a HbbTV) informačného zdroja (napríklad aplikácie), a teda s potrebou diferenciácie prístupu k týmto zdrojom, a to flexibilne podľa potreby rôznych užívateľov. Pokiaľ využijeme vlastnosti protokolov tak, aby sme implementovali procedúru diferencovaného prístupu k informačným zdrojom na základe (pre oba svety spoločných) užívateľských preferencií, zavedieme tak silnejší bezpečnostný model pre autorizáciu a zabezpečenie privátnosti vybraných dát.

Pokiaľ sa na problematiku pozrieme z pohľadu poskytovateľa služieb, tak vidíme možnosť riešiť poskytovanie služieb nielen užívateľom vlastným, ale aj riešenie ako poskytnúť možnosť aktívne sa zapojiť do domácej zábavy aj pre návštevy týchto užívateľov, aj keď majú aj iného poskytovateľa služieb, a poskytnúť tak lepší komunitný rozmer služby ako takej. Aplikovaním metód federácií do prostredí HbbTV a IoT, definovaním vhodných procedúr interakcií medzi autentizačnými a autorizačnými entitami, môže byť požiadavka naplnená.

4 Zvolené metódy riešenia

Z analýzy súčasného stavu riešenia problematiky vyplýva, že pre splnenie stanovených cieľov dizertačnej je nutné si definovať a jasne ohraničiť skupinu požiadaviek, ktoré budú determinovať funkčnosť navrhovaného celku tak, aby zodpovedala stanoveným požiadavkám. Preto môžeme definovať nasledovné:

- požiadavka zjednotenej autentizácie a autorizácie užívateľov a modulov služieb
- požiadavka viacfaktorovej autentizácie
- požiadavka na diferenciáciu zdieľania a prístupu k užívateľským dátam

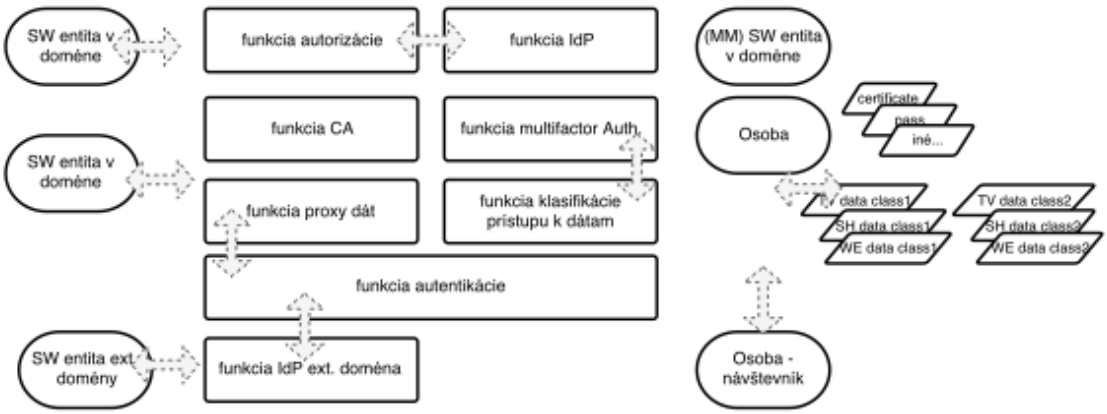
- požiadavka na vzájomnú interakciu navštevujúcich a navštívených užívateľov, v prostredí domáceho užívateľa služby
- požiadavka na zdieľanie bezpečnostných komponentov IoT služby v kontexte HBB-Next architektúry.

V nasledujúcich kapitolách každú požiadavku analyzujeme z pohľadu charakteru HbbTV služieb ako takých, z pohľadu interakcie s ostatnými prvkami architektúry HBB-Next, ako aj z pohľadu klientov – teda užívateľov služby alebo softvérových modulov. Je dôležité uviesť, že budeme diferencovať medzi týmito dvoma užívateľskými entitami, keďže každá z nich má osobitné charakteristiky a potreby.

V návrhu budeme navrhovať funkcionality a architektúru, ktoré majú byť vo svojom princípe nezávislé od konkrétneho autorizačného protokolu.

4.1 Návrh funkčného modelu Security Manager

Z hľadiska súhrnu všetkých požiadaviek, môžeme tieto definovať na nasledujúcej schéme, spolu s entitami poskytovateľov či odoberateľov služieb. Zároveň načrtneme a popíšeme základné vzťahy medzi nimi.



Obrázok 2: Návrh funkčného modelu SM

Na obrázku 2 vidíme návrh funkcionalít SM v navrhovanej architektúre. Každá funkcionalita môže interagovať s ostatnými tak, aby prispela k naplneniu požadovaných funkčností ako celku podľa cieľov dizertačnej práce. Nepredstavuje však jeho praktickú realizáciu, ale deskriptívne popisuje jednotlivé funkcionality, ktoré sú nevyhnutné k napĺňaniu jeho poslania. Samotná praktická realizácia je popísaná v kapitole Implementácia.

Mapovanie základných funkcionalít

SW entita v doméne:

Jedná sa o softvérový modul, ktorý vykonáva vopred určenú funkciu v systéme. Môže to byť napríklad generovanie EPG, zobrazovanie zákazníckych dát, softvér pre riadenie svetiel v dome a podobne. Ako taký môže byť inštalovaný buď domácim poskytovateľom služby, alebo môže byť napríklad stiahnutý z aplikačného obchodu služby a môže byť vyrobený dodávateľom tretej strany. SW entít môže byť v službe niekoľko a môžu navzájom interagovať. Táto SW entita je spúšťaná výhradne v doméne poskytovateľa služby, a to napríklad na domácom STB alebo v prostredí vlastného cloudu domáceho poskytovateľa služby. Sw entitu niekedy nazývame aj sw modulom.

SW entita ext. domény:

V zásade môžeme konštatovať, že sa jedná o rovnakú funkcionalitu ako v prípade SW entity v doméne s tým, že SW entita ext. domény (teda mimo domácej domény) beží v prostredí (cloudu) iného poskytovateľa služby.

Osoba:

Jedná sa o ľudskú bytosť, ktorá používa službu od svojho poskytovateľa. Osoba má v systéme svoje vlastné jedinečné profily, ktoré uchovávajú nastavenia a ostatné dáta potrebné pre funkciu služby. Tieto môžu byť kategorizované tak, ako je naznačené ďalej v dizertačnej práci, podľa ich charakteru. Osoba ako taká je v systéme reprezentovaná klientom - to je modul, ktorý zastupuje klienta pri vybavovaní jeho požiadaviek voči ostatným SW entitám (modulom) služby. V kontexte ďalších použití pojmu Osoba v texte, bude vždy uvažované, že sa jedná o osobu navštívenú.

Osoba - návštevník:

Je to človek, ktorý sa nachádza mimo svojej domácej domény služby a zároveň používa/zdieľa službu u osoby, ktorú navštívil. Očakáva, že služba u navštívenej osoby bude schopná plniť niektoré funkcionality s využitím jeho vlastných preferencií či iných, pre neho charakteristických, nastavení. Osoba - návštevník zároveň môže byť (z pohľadu vzťahu voči navštívenej osobe) z domény rovnakého poskytovateľa služby, alebo iného poskytovateľa služby.

Funkcia IdP ext. domény:

Táto funkcionalita SM (Security Manager) znamená možnosť bezpečne komunikovať s inými poskytovateľmi identít. Jedná sa o funkcionalitu, ktorá bude využívaná pre entity ako Osoba - návštevník, či SW entita mimo domácej domény. Zabezpečí sa ňou spoľahlivé a dôveryhodné overenie identity žiadateľa, prostredníctvom aktívnej komunikácie s externým IdP. Je zjavné, že IdP a SM musia mať istý vzťah a definovaný spôsob komunikácie.

Funkcia Autentizácie:

Zabezpečuje funkcionalitu overovania identít pre sw entity a osoby.

Funkcia certifikačnej autority:

Táto funkcia je dôležitou pre vybrané procesy autentizácie pomocou technológie PKI pre proces vydávania a správy certifikátov sw entít.

Funkcia proxy dát:

Komunikácia medzi entitami služby, v prípade že prebieha v rámci rozličných domén, je zabezpečovaná funkciou proxy dát. Táto je zodpovedná za vybrané atribúty bezpečnosti komunikácie, teda na služieb na zaistenie dôvernosti a integrity komunikácie oboch strán.

Funkcia IdP:

Je to funkcia domáceho IdP pre všetky entity v doméne domáceho poskytovateľa služby. Vytvára, udržiava a riadi informácie o identitách pre vlastných užívateľov služby a poskytuje principiálnu autentizáciu aj pre iných poskytovateľov identity podľa potreby.

Funkcia viacfaktorovej autentizácie:

Požiadavka na viacfaktorovú autentizáciu vyplýva z multimediálne podstaty HbbTV služieb a zabezpečuje komunikáciu na ďalšie komponenty, ktoré sú schopné uskutočniť niektorú z viacfaktorových autentizačných metód, ako je hlasová analýza, analýza tváre, sietnice oka a podobne.

Funkcia klasifikácie prístupu k dátam:

Táto funkcionalita zabezpečuje transparentný a diferencovaný prístup k dátam každého užívateľa služby. Spolupracuje tiež s funkcionalitami ako Autentizácia, viacfaktorová autentizácia a pod. Obsahuje logiku kategorizácie dát, ich klasifikácie, užívateľské nastavenia a modifikácie, vrátane politiky prístupov k nim, aby tak zabezpečil užívateľovi služby požadovaný stupeň privátnosti zdieľania informácii avšak pri zachovaní plnej funkčnosti služby ako takej. Samotná definícia tejto funkcionality je vždy objektom konkrétnej definície služby zo strany poskytovateľa služby a jej prijímateľa - osoby, či modulu.

Návrh mechanizmu autentizácie prostredníctvom externého IdP s využitím federácie

V nasledujúcej časti budeme rozoberať (už vyššie spomínanú) možnosť (a zároveň jeden z cieľov dizertačnej práce) použitia externého IdP, čo znamená, že niektorí užívatelia - návštevy HbbTV služby môžu byť klientami iného poskytovateľa služby. Táto požiadavka kladie na nami navrhovaný modul SMIM vyššie nároky v zmysle

- rozpoznania klienta iného operátora
- správneho smerovania na externé IdP a komunikáciu s týmto elementom
- pripravenosť autorizácie prístupu k dátam navštívenej osoby/osôb podľa vopred stanovenej kategorizácie

Tretí bod diskutujeme v našej dizertačnej práci v kapitole 5.3.2.

Proces použitia externého IdP však musí byť navrhnutý komplexnejšie, aby bol univerzálnejší. Architektúra navrhovaného modulu SMIM pre použitie pre HbbTV a SH služby musí teda zohľadňovať aj nasledujúce:

- poskytnúť zoznam možných IdP poskytovateľov
- poskytnúť možnosť zistenia podporovaných autentizačných protokolov
- poskytnúť zoznam možných služieb pre danú identitu modulu či užívateľa
- upraviť proces pre užívateľa ako ľudskú osobu a pre modul služby

V našej dizertačnej práci popisujeme tento mechanizmus aj so zohľadnením horeuvedených bodov v detailoch.

Požiadavka na diferenciáciu zdieľania a prístupu k užívateľským dátam

Diferenciácia prístupu k užívateľským dátam je nevyhnutnou požiadavkou kladenou na služby HbbTV a SH, zvlášť v prostredí multiužívateľských služieb s vysokou mierou interaktivity.

Kategorizácia privátnosti dát

Užívateľské údaje môžeme vo všeobecnosti kategorizovať podľa potreby tej ktorej služby, my však za účelom popisu konceptu pre našu prípadovú štúdiu kategorizujeme dáta nasledovne (návrh):

- Súkromné dáta– sú to dáta, ktoré z pohľadu informačnej hodnoty predstavujú výrazné riziko pri ich zverejnení mimo vyhradený úzky okruh ľudí.
- citlivé - osobné dáta citlivosti vyššieho stupňa: tieto dáta obsahujú osobné informácie, ktoré sú obvykle zdieľané iba úzkym okruhom ľudí, najčastejšie rodinou alebo komunitou.
- citlivé - dáta domácnosti citlivosti vyššieho stupňa: tieto dáta obsahujú domáce informácie, ktoré sú obvykle zdieľané iba úzkym okruhom ľudí, najčastejšie rodinou alebo komunitou, či priateľmi. Pre opodstatnené prípady je možné zdieľať tieto dáta aj s externými službami.
- zdieľané - osobné dáta citlivosti nižšieho stupňa: sú to dáta, ktoré z pohľadu informačnej hodnoty nepredstavujú riziko pri zdieľaní, obyčajne obsahujú informácie, ktoré sú obvykle zdieľateľné širším okruhom.
- zdieľané - dáta domácnosti citlivosti nižšieho stupňa: sú to dáta, ktoré z pohľadu informačnej hodnoty nepredstavujú riziko pri zdieľaní.
- verejné dáta: Dáta, ktoré sú obyčajne známe širokému okruhu známych či neznámych ľudí.

Bližší popis kategórií uvádzame v našej dizertačnej práci.

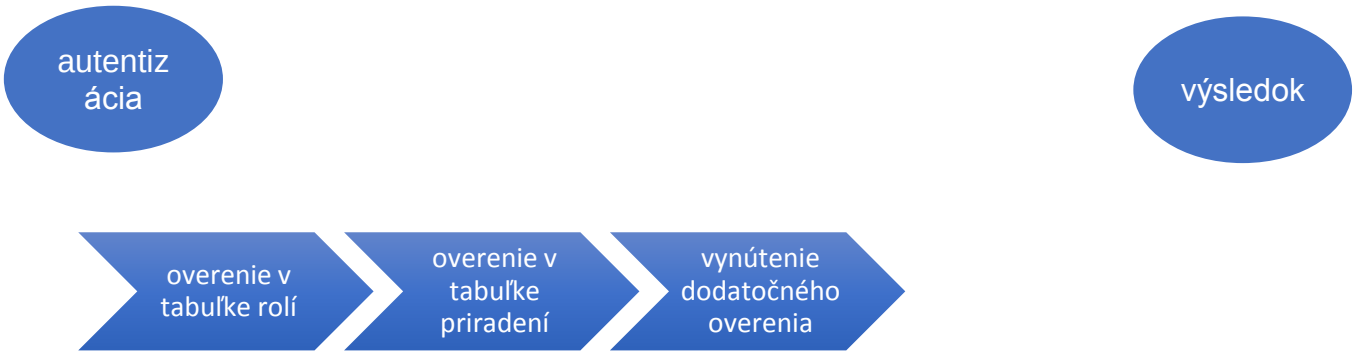
Návrh algoritmu pre diferenciáciu zdieľania a prístupu

Diferenciáciu zdieľania a prístupu k užívateľským dátam budeme vykonávať prostredníctvom funkcie autorizácie a funkcie klasifikácie prístupu k dátam (pozri obrázok 2). Tak, ako sme naznačili vyššie, za pomoci kategorizácie dát určíme možnosti pre ich zdieľanie pre požadujúcu stranu, a to prostredníctvom:

- overenia jej identity (softvérového modulu, či stupňa rozpoznania identity osoby)

- kontroly pridelenej užívateľskej roli
- kontroly dodatočných podmienok podľa priradenia
- ďalšími prípadnými akciami pre dosiahnutie požadovaného stupňa overenia identity

Algoritmus pre diferenciáciu zdieľania a prístupu k užívateľským dátam navrhujeme teda nasledovne, viď obrázok 3:



Obrázok 3: Algoritmus diferenciácie zdieľania prístupu k užívateľským dátam

Overenie identity – autentizácia, zabezpečí možnosť identifikácie role v dedikovanej **tabuľke rolí**, ktorá bola danému užívateľovi priradená. Toto priradenie sa obyčajne deje pri prvotnom nastavovaní služby na začiatku jej užívania. Tabuľka rolí je jednoduché priradenie preddefinovanej role (podľa modelu RBAC) pre každú registrovanú identitu užívateľa či softvérového modulu, a to zvlášť pre každú kategóriu privátnosti dát. V ďalšom kroku sa vykoná overenie v **tabuľke priradení,** čo má za účel určiť minimálny požadovaný stupeň overenia identity pre prístup k dátam, podľa kategórie ich privátnosti. **Výsledkom** je potom povolenie či zamietnutie prístupu pre žiadajúcu entitu. Povolenie samotné je žiadajúcej entite udelené formou zaslania prístupového tokenu s prístupovými právami podľa výsledku autorizácie, to prostredníctvom subsystému autentizácie a autorizácie SMIM [viď kapitola 5.3.1 v dizertačnej práci].

Doplnkové autentizačné mechanizmy pre autorizáciu

Overenie identity osôb (teda overenie deklarovanej identity voči skutočnej) je zo svojej podstaty komplexnou problematikou. Samotné overenie identity je dôveryhodné vždy iba do istej miery, a závisí hlavne na metóde, ktorou autentizácia prebehla. Môžeme teda konštatovať, že to, či je stupeň zistenia identity subjektu dostatočný, závisí na druhu dát, ku ktorým subjekt chce pristúpiť. V predchádzajúcej časti sme si zadefinovali kategorizáciu privátnosti dát. V **tabuľke priradení** budeme potom definovať, aký minimálny spôsob zisťovania totožnosti užívateľa budeme požadovať pre konkrétnu kategóriu privátnosti dát. Ešte predtým však popíšeme, akými ďalšími možnosťami, okrem užívateľských poverení (*credentials*), zisťovania identity subjektu – osoby disponujeme.

V dizertačnej práci opisujeme autentizačné možnosti užívateľa podrobnejšie. Na tomto mieste iba skonštatujeme, že že tieto možnosti sa s vývojom technológie zväčšujú a okrem „tradičných metód“ sa do popredia dostávajú aj metódy založené jednak na multimediálnych

technológiách, biometrických technológiách, respektíve na internetových technológiách, hlavne z prostredia IoT/SH.

Multimodálna identifikácia ako doplnkový autentizačný mechanizmus pre autorizáciu

Rozpoznanie hlasu, tváre, mimiky či gest, patrí do rodiny **multimodálnej identifikácie**. Možnosť identifikácie užívateľa resp. užívateľov prostredníctvom multimodálnych algoritmov znamená rozšírenie nášho komunikačného modelu so SM entitou o nové prvky. V samotnej podstate zavedenie viac-úrovňovej užívateľskej identifikácie, definične vyžadovanej v tabuľke priradení, znamená zavedenie viacerých stupňov úrovne bezpečnosti a autorizácie v službe ako takej.

Tabuľka priradení

V **tabuľke priradení** definujeme, aký minimálny spôsob resp. úroveň zisťovania totožnosti užívateľa budeme požadovať pre konkrétnu kategóriu privátnosti dát.

Pre popis konceptu pre našu prípadovú štúdiu budeme uvažovať s nasledovnými faktormi pre dodatočnú autentizáciu:

- rozpoznanie hlasu
- rozpoznanie tváre
- PIN

Samotné priradenie metód viacfaktorovej autentizácie, multimodálnu identifikáciu nevynímajúc, k jednotlivým stupňom citlivosti osobných údajov užívateľa služby, musí byť definované pre každú službu osobitne, samozrejme s cieľom minimalizovať náročnosť použitia ďalších faktorov pri autentizácii, avšak pri zachovaní požadovanej úrovne bezpečnosti.

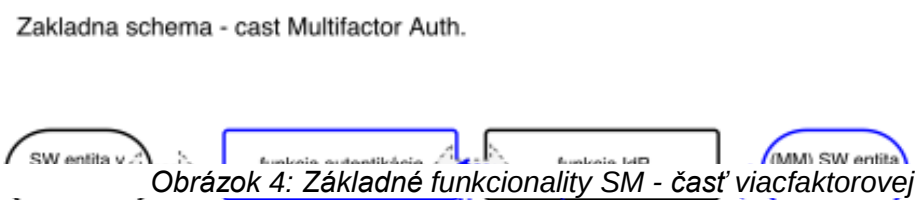
Bližší popis tabuľky priradení uvádzame v našej dizertačnej práci.

Pre každú kategóriu privátnosti dát je určená Primárna autentizácia užívateľa, a v prípade potreby (teda pre vyššie kategórie privátnosti dát) aj tzv. ďalší faktor. Oba môžu byť neskôr modifikované podľa potreby konkrétnych služieb, pre ktoré bude návrh využitý. V nadväznosti na existujúci stupeň autentizácie, vyhodnotí algoritmus prípadnú potrebu **dodatočného overenia identity**, a ak je potrebné, vynúti od žiadajúceho subjektu autentizáciu určeným spôsobom podľa tabuľky priradení (prostredníctvom funkcie viacfaktorovej autentizácie, popísanej v ďalšej časti dizertačnej práce).

4.1.1 Požiadavka viacfaktorovej autentizácie

Z definície viacfaktorovej autentizácie vyplýva, že overenie identity môže byť aj viacnásobné, zodpovedajúce stupňu privátnosti či zabezpečeniu dát, ku ktorým sa pristupuje.

Na nasledujúcej schéme funkcionalít architektúry SM (Obrázok 4), z ktorej s odvíjame v celej práci, sú navrhujeme funkcionality aktívne sa podieľajúce na viacfaktorovej autentizácii.



Obrázok 4: Základné funkcionality SM - časť viacfaktorovej autentizácie

Popis: 1: Osoba z domácej domény poskytovateľa služby požiada o prístup k istej službe. V tejto chvíli nastane teda aj požiadavka na jeho samotnú autentizáciu [bez uvedenia detailov, viď kapitola 5.3.1], ale po vyhodnotení požiadavky k prístupu ku konkrétnym zdrojom služby (prostredníctvom funkcie klasifikácie prístupu k dátam) aj k aktivácii funkcie viacfaktorovej autorizácie (2:). Následne je oslovená špecifická MM SW entita v doméne, venujúca sa napríklad multimodálnej autentizácii, a požiada o dodatočné rozpoznanie žiadajúcej osoby (3:). Špecifické dáta (4:), v tomto prípade napríklad heslo (*pass*), prislúchajúce osobnému profilu zákazníka, sú použité pre výsledné vyhodnotenie.

V prípade návštevy (5:) sa jedná o rovnaký vektor autentizačnej sekvencie s tým, že dáta vzťahujúce sa k identite návštevníka, sú vyhodnocované v spolupráci s jeho poskytovateľom identity (6:) a jeho osobným profilom v jeho doméne.

Pre príklad vynútenej viacfaktorovej užívateľskej autentizácie, pre autorizáciu prístupu domácej osoby k dátam domácnosti vyššej citlivosti služby Smart Home, bola navrhutý sekvenčný diagram, ktorý je bližšie uvedený v našej dizertačnej práci.

4.1.2 Požiadavka na zdieľanie bezpečnostných komponentov IoT a HBB-Next

V tejto kapitole budeme popisovať naplnenie požiadavky na zdieľanie komponentov architektúry HBB-Next slúžiacich na autentizáciu a riadenie prístupu ku zdrojom aj pre prvky IoT.

V predchádzajúcich kapitolách sme uviedli definície IoT, jej funkcie a základné atribúty. Z nej vyplýva, že rozsah a zameranie služieb IoT je skutočne rozmanité, a skladba či použitie konkrétnej architektúry je predovšetkým definované účelom IoT služby. Je preto zrejmé, že nie je našou ambíciou popísať možnosti zdieľania všetkých IoT služieb, ale zameriame sa na tie, ktoré sú späté s prostredím, v ktorom sa používajú služby HbbTV. V nasledujúcom texte sa preto sústredíme na charakteristický prípad IoT v prostredí domácností užívateľov, a to je služba „Smart Home“ (v ďalšom texte budeme používať skratku SH), rozšírenú o funkcionality starostlivosti o staršie osoby. Pomenujeme základné prvky, navrhneme modelový príklad a na ňom popíšeme možnosti zdieľania autentizačných a autorizačných komponentov v prostredí HbbTV.

Táto časť práce nebola riešená v projekte FP7 HBB-NEXT, a je rozšírením dizertačnej práce v projekte smerom ku svetu IoT. Náš príspevok k rozšíreniu architektúry bol navrhnutý s cieľom navrhnúť maximalizáciu synergických efektov medzi týmito dvoma typmi služieb s cieľom definovať využitie vybraných komponentov bezpečnosti tak, aby boli prepoužité a tak sa dosiahla vyššia možnosť vytvárania omnoho prepojenejších služieb z prostredia hybridných širokopásmových služieb vysielania a internetu vecí.

Modelový príklad služby SmartHome

Vychádzajúc z architektúry IoT, a zvlášť z SH architektúry, navrhujeme uvažovať s nasledovným modelovým príkladom. Tento príklad má za cieľ zahrnúť do úvahy hlavné charakteristické prvky SH služby, vrátane prvkov, ktoré sú využívané pri starostlivosti o starších.

Príklad služby SH bude službou poskytujúcou

- Služby optimalizácie energetickej spotreby
- Služby zabezpečenia poplachovej bezpečnosti domu (alarm)
- Služby komfortu bývania
- Služby integrovanej zábavy
- Služby starostlivosti o starších, o deti

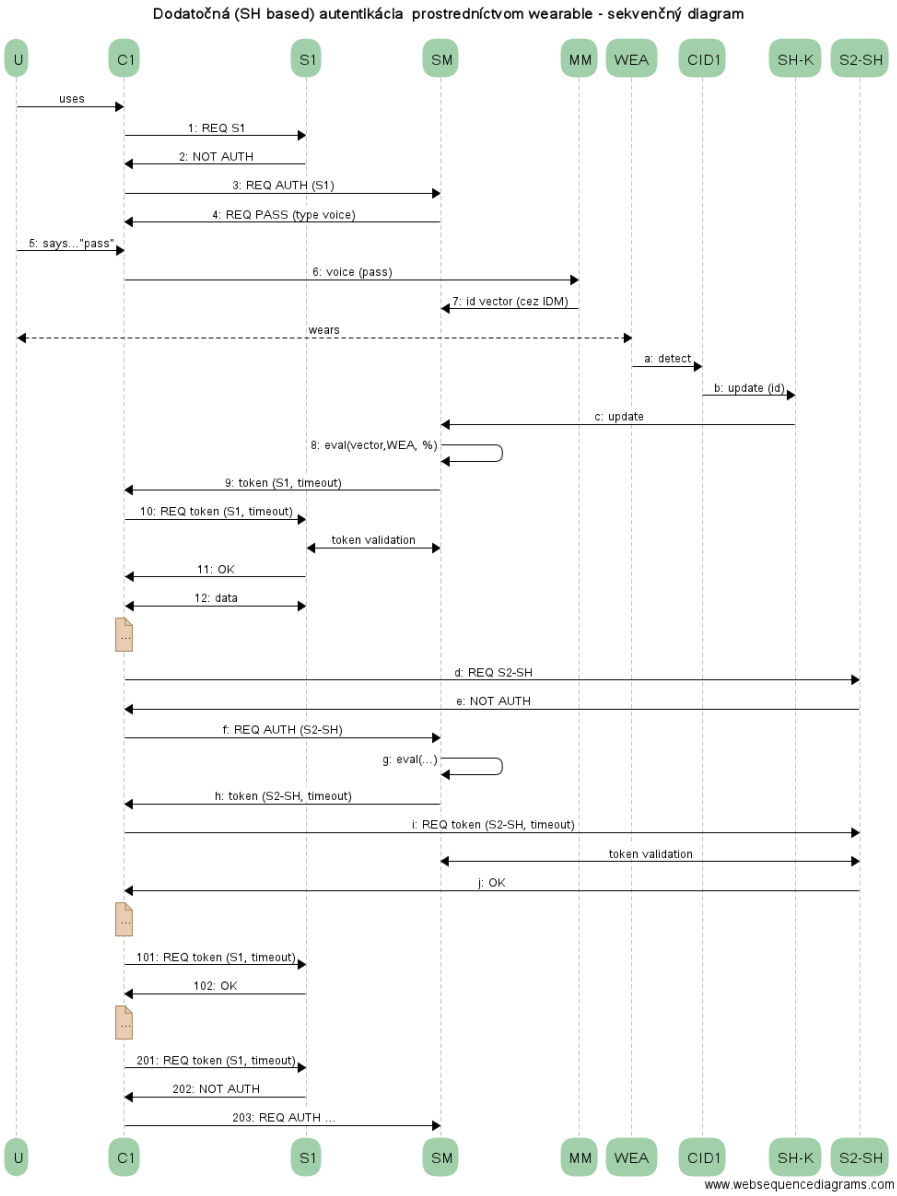
Uvažujme, že služba je inštalovaná na SH kontroléri, prostredníctvom ktorého prichádza ku komunikácii so senzormi S. V priestoroch inštalácie SH systému sa bude nachádzať IP kamera, pripojená prostredníctvom protokolu IP a LAN siete vytvorenej prostredníctvom protokolu Wifi. Súčasťou SH nech je aj pripojenie hudobných zariadení pripojených prostredníctvom protokolu Bluetooth. V rodine sa nachádzajú aj starší členovia, ktorí používajú zariadenie tele medicíny pre meranie srdcového rytmu a zároveň používajú monitorovacie zariadenia pre detekciu núdzových situácií (SOS náramok), detekciu pádu a nečinnosti. Pre zjednodušenie príkladu nebudeme uvažovať o použití nezávislého systému pre starostlivosť o starších, ale budeme uvažovať, že tento je integrovaný priamo do kontroléra systému SH.

Praktické realizácie architektúr SH bývajú navrhované ako tzv. „*standalone*“ – tj. bez priamej závislosti na komponentoch iných architektúr či služieb (Brezovan, 2013). To znamená, že pre správne základné fungovanie nie je nutná komunikácia s inými komponentami mimo domény SH (pripojené služby, ako sú ukladanie dát v cloud-ových dátových úložiskách, aplikácie tretích strán pre optimalizáciu spotreby el. energie a pod., neuvažujúc). Z pohľadu zamerania dizertačnej práce však táto vlastnosť znamená to, že pri takejto realizácii služieb HbbTV a SH v prostredí vybranej domácnosti, by musel poskytovateľ služieb:

1. Definovať pre každú (HbbTV a SH) doménu rovnaké funkcionality autentizácie a autorizácie, pre rozpoznávanie účastníkov, ich oprávnení vykonávať rôzne činnosti a pristupovať ku zdrojom informácií
2. Pre (požadovanú) interakciu služieb v oboch (HbbTV a SH) doménach definovať a implementovať ďalšie prvky a protokoly - na úrovni API, ktoré (okrem iného) zabezpečia napríklad kryptovanie dát pri komunikácii medzi prvkami domén (senzor, aktuátor, ...), zdieľanie a mapovanie identít, využívanie viacfaktorovej autentizácie služieb jednej domény v druhej a podobne
3. Pre každú službu HbbTV a SH riešiť osobitne požiadavku na interakciu užívateľov týchto služieb, pokiaľ sú z prostredia rôznych poskytovateľov služieb

Preto sa nám javí ako výhodné, v hore definovanej situácii sa zamerať na využitie už definovaných komponentov z architektúry HBB-Next tak, aby prišlo k zjednodušeniu implementácie HbbTV a SH služieb, k zvýšeniu stupňa interakcie užívateľov týchto služieb a aj k umožneniu výrazne vyššej prepojenosti HbbTV a SH služieb samotných.

Sekvenčný diagram príkladu navrhovaného zdieľania SM komponentov pre služby HbbTV a SH je naznačený na obrázku 5.



Obrázok 5: Sekvenčný diagram zdieľania bezp. komponentov z prostredí HbbTV a SH

Na uvedenom príklade v sekvenčnom diagrame na obrázku 5 sme znázornili rozšírenie navrhovanej možnosti z kapitoly 5.3.3 v dizertačnej práci o možnosť zahrnutia do autentizačného, a následne autorizačného mechanizmu o identitu z oblasti služby SH. Naznačuje, že autorizačný mechanizmus pre využitie služby S1 je obohatený o prvok rozpoznania niečoho, čo daná osoba vlastní. V tomto prípade sa jedná o BT náramok (wearable - WEA), ktorý je detegovaný čidlom CID1 a SH kontrolórom SH-K, a keďže služba SH využíva zdieľané komponenty autentizácie a autorizácie (pozri body a až c na obrázku 5), je tento fakt zohľadnený pri samotnej autentizačnej metóde [viď kapitola 5.3.1] (pozri body 8 až 12 na obrázku 5). Tým dosiahneme vyšší stupeň autentizácie užívateľa pre využitie v procese autentizácie prístupu k požadovaným zdrojom.

Nami navrhnutý spôsob zdieľania autorizačných a autentizačných komponentov HbbTV v IoT/SH prostredí prináša nasledovné výhody:

- Realizáciou horeuvedeného – teda zdieľania bezpečnostných funkcionalít vo forme jedného komponentu (teda SM), príde k možnosti prepoužiť bezpečnostné prvky systému HBB-Next

aj pre technologickú realizáciu služby SH. Ich zaradením do architektúry SH potom príde k zjednoteniu celého procesu autentizácie užívateľov, čo bude viesť k možnosti poskytovania komplexných (a kombinovaných) služieb pre domácnosti v rámci jednej technologickej bázy poskytovateľa služby. Príde k tým k zníženiu komplexnosti architektúry takýchto (kombinovaných) služieb a k zvýšeniu stupňa bezpečnosti aj z dôvodu zdieľania identít užívateľov a spôsobu ich overovania z oboch svetov – SH a HBB-Next.

- V prípade autorizácie, realizáciou horeuvedeného spôsobu zdieľania vybraných bezpečnostných komponentov, prichádza k možnosti rozšírenia riadenia prístupu užívateľov k zdrojom v službe SH.
- Navrhovaný model navštíveného a navštevujúceho užívateľa z architektúry HBB-Next je možné úspešne aplikovať aj v prostredí SH. Toto nebolo dosiaľ v takejto forme navrhované, pokiaľ je nám známe. Znamená to, že poskytovateľ služby dokáže 1. identifikovať, 2. autentizovať a 3. autorizovať návštevníka v domácnosti navštíveného, pokiaľ má návštevník službu z architektúry HbbTV (môže byť HbbTV služba, alebo SH služba, ale musí byť podľa navrhovanej architektúry HBB-Next). Návšteva teda preberá oprávnenia čítať/riadiť/nastavovať atribúty služby SH u navštíveného tak, ako tento vopred definoval. Realizáciou architektúry HBB-Next k tejto možnosti bude prichádzať automaticky, bez akýchkoľvek úprav technológie vopred.
- Veľmi výhodnou sa javí byť realizácia architektúry SH so zdieľaním bezpečnostných komponentov z HBB-Next aj z pohľadu rôznych poskytovateľov služieb. V predchádzajúcom odseku sme popísali východy z pohľadu jedného poskytovateľa služby, avšak navrhovaná architektúra sa dá s úspechom použiť aj vtedy, pokiaľ existuje požiadavka na vzájomnú interakciu služieb SH a HbbTV, keď je navštívená osoba a návšteva od rôznych poskytovateľov služieb. Opäť konštatujeme, že realizáciou navrhovanej architektúry HBB-Next k tejto možnosti bude prichádzať automaticky, bez akýchkoľvek úprav technológie vopred.

5 Implementácia a testovanie navrhnutého systému SM

Táto kapitola popisuje implementáciu komponentu Security Manager a testovanie jeho vybraných funkcionalít v prostredí architektúry HBB-Next tak, aby sa koncept overil v reálnych podmienkach.

Implementácia bola súčasťou výskumných aktivít v rámci projektu FP7 HBB-NEXT **(HBB-NEXT, 2012)** , číslo projektu: ICT-2011-7-287848. Časť Security Manager bola jednou z viacerých častí projektu, ktorý bol experimentálne overený a jeho výstupy sú verejne dostupné **(HBB-NEXT, Architecture, Final HBB-NEXT System, 2014)**. Naša časť spĺňala funkčnosti požadované v rámci celého konceptu architektúry HBB-Next a tak, ako bola navrhovaná, zabezpečovala bezpečnostné definované funkcie pre ostatné komponenty v systéme podľa ich požiadaviek. V prvej časti kapitoly uvedieme celkový koncept HBB-Next tak, aby sme čitateľa uviedli do komplexnej problematiky. Ďalej bude popísaný návrh architektúry Security Manager a na záver uvedieme funkčnosť na konkrétnom príklade.

5.1 Security Manager

V procese riešenia problematiky autentizácie užívateľov a modulov v prostredí hybridných služieb širokopásmového vysielania a prostredia inteligentných domov, ich autorizácie a riadenia prístupu k vybraným zdrojom, vychádzajúc z cieľov dizertačnej práce, navrhujeme vytvorenie špecializovanej entity vykonávajúcej menované funkcionality. Návrh

tejto entity bude súčasťou širšieho konceptu architektúry budúcich hybridných multimediálnych služieb vysielania, návrh bude teda zohľadňovať aj existenciu iných komponentov tak, aby spolu plnili účel plnohodnotnej a funkčnej architektúry.

V ďalších kapitolách popíšeme návrh koncepcie Security Manager (SM), vymedzíme funkcionality, ktoré bude napĺňať a navrhneme jeho jednotlivé funkčné bloky.

5.1.1 Návrh koncepcie Security Manager

Návrh Security Manager, ako jeden z výstupov dizertačnej práce, bude zodpovedať za nasledovné funkcionality:

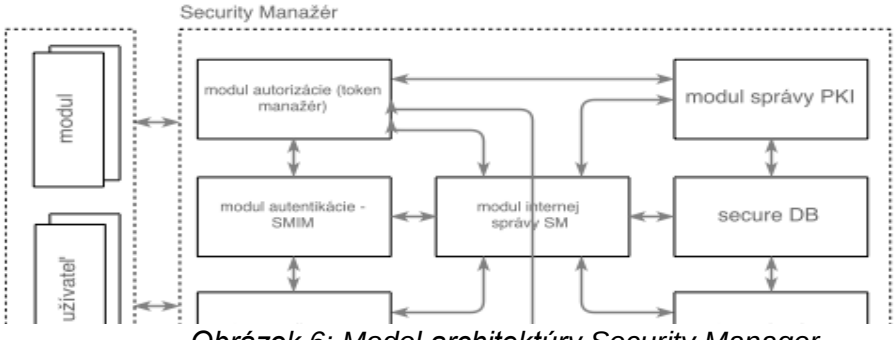
- vykonáva funkciu poskytovateľa identity domáceho poskytovateľa služby, spolupracuje pri zabezpečovaní autentizácie prostredníctvom federovanej správy identít
- riadi viacfaktorovú autentizáciu, autorizáciu a napĺňanie politík pre rôzne úrovne ochrany súkromia, privátnosti prístupu k dátam
- riadi vydávanie tokenov, vrátane vymedzenia rozsahu ich platnosti
- zabezpečuje služby PKI pre HBB-Next doménu, a to certifikačnú autoritu (CA), certifikačný zoznam odmietnutí (CRL)
- bezpečne ukladá SM špecifické dáta, ako sú heslá, vzorky hlasov, politiky prístupu k dátam, certifikáty a iné, pre každého užívateľa domovskej domény.
- poskytuje zoznam federovaných poskytovateľov identity, s ktorými má domáci poskytovateľ služby dohodnutý vzťah dôvery
- pre navštívených užívateľov a externé moduly vydáva autentizačné tokeny
- zabezpečuje bezpečnú komunikáciu lokálnych služieb a užívateľov do externých sietí
- komunikuje s ostatnými blokmi HBB-Next architektúry

5.1.2 Návrh systémového modelu architektúry SM

Navrhnutý model architektúry Security Manager je zobrazený na Obrázok 6. Navrhujeme spolu sedem funkčných blokov, z ktorých každý vykonáva špecifické úlohy popísané nižšie. Základné entity, ktoré s SM budú komunikovať, sú z pohľadu autentizovaných a autorizovaných entít užívateľ resp. softvérový modul, a z pohľadu funkčných aplikácií iné externé moduly či poskytovatelia identity.

Opis funkčných blokov Security Manager

Modul autorizácie (token manažér)
Má na zodpovednosti správu tokenov pre autorizáciu prístupu terminálov, klientov a modulov do domácej domény poskytovateľa služby. Modul buď udelí prístup žiadateľovi, alebo ho zamietne.



Obrázok 6: Model architektúry Security Manager

Z pohľadu napĺňania funkčných požiadaviek vykonáva funkcionalitu: autorizácie a viacfaktorovej autorizácie.

Modul autentizácie SMIM
Tento blok má na starosti riadenie procesu autentizácie užívateľov a modulov služieb. Je tiež zodpovedný za proces riadenia viacfaktorovej autentizácie. Pre rozhodovanie využíva aj modul politík prístupov.
Z pohľadu napĺňania funkčných požiadaviek vykonáva funkcionalitu: autentizácie, IdP a funkciu IdP externej doméne.

Modul manažovania API
Zabezpečuje komunikáciu samotného Security Manager s ostatnými HBB-Next entitami. Z pohľadu funkcionality obsahuje tri sub-moduly, každý pre špecifikovanú oblasť komunikácie.

Z pohľadu napĺňania funkčných požiadaviek vykonáva funkcionalitu: proxy dát a podieľa sa na vzájomnej interakcii navštevujúcich a navštívených, v prostredí domáceho užívateľa služby.

Modul internej správy SM
Je centrálnym modulom pre zber a vyhodnocovanie log-ov zo všetkých modulov SM. Jeho úlohou je aj vyhodnocovanie logov, klasifikácia, ich následné spracovanie a nadväzujúce akcie.

Modul správy PKI
Vykonáva funkcionalitu PKI spojenú s overovaním totožnosti respektíve pre šifrovanie komunikácie medzi modulmi architektúry HBB-Next pre doménu domáceho poskytovateľa služby, zabezpečuje zároveň certifikačnú autoritu pre túto doménu.
Z pohľadu napĺňania funkčných požiadaviek vykonáva funkcionalitu: CA

Modul Secure DB
Ukladá všetky citlivé PKI dáta, ako sú kryptografické kľúče, PKI certifikáty.

Modul politík prístupov
Zabezpečuje funkcionalitu politiky prístupu k dátam účastníkov či ostatných modulov, prostredníctvom spolupráce s modulom autorizácie a autentizácie, zvlášť v prípadoch viacfaktorovej autentizácie.
Z pohľadu napĺňania funkčných požiadaviek sa podieľa na funkcionalite diferenciácie zdieľania a prístupu k užívateľským dátam

Externé entity (mimo záberu SM) - výber:

Modul identity (IdM)
Tento externý modul zabezpečuje rolu identity manažmentu v architektúre HBB-Next. Ukladá a riadi identity dáta všetkých užívateľov služby a zároveň ich poskytuje ostatným entitám služby - s výnimkou bezpečnostných dát. Tieto poskytuje výhradne cez SM modul. SM modul zároveň ukladá a aktualizuje tieto informácie. Z pohľadu funkcionality, slúži IdM ako back-end modul pre SM.

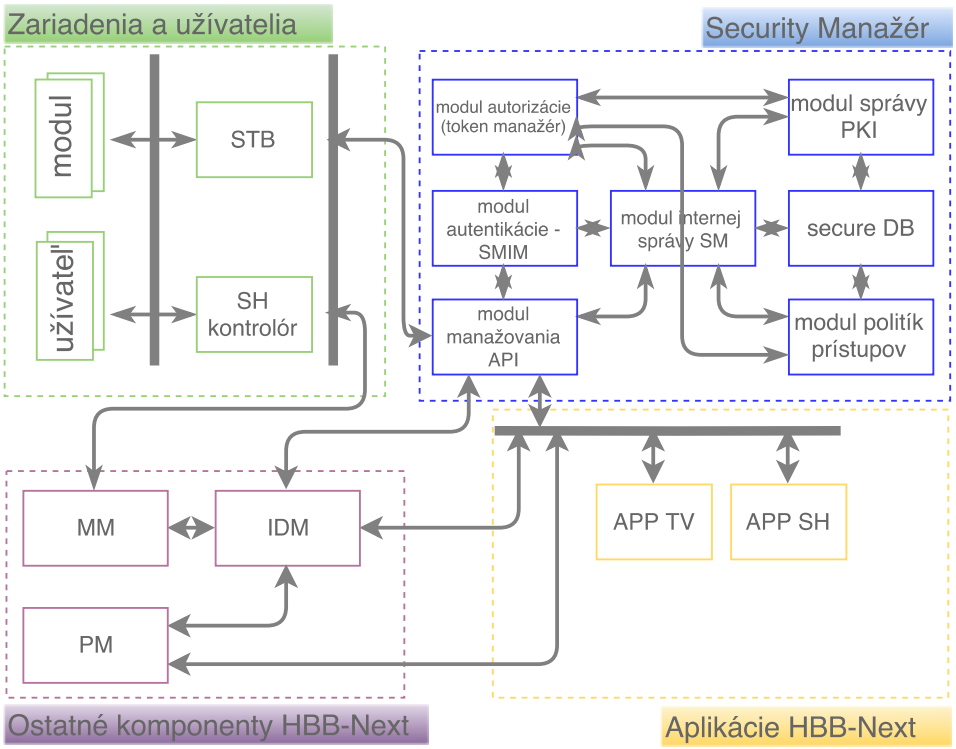
Multimodálny modul (MM)

Tento externý modul je zodpovedný za identifikáciu a rozpoznanie subjektov, ktoré sa nachádzajú v určitej vymedzenej oblasti a to buď prostredníctvom hlasu alebo vizáže. Navyše, modul MM poskytuje SM (ako entite zabezpečujúcej autentizáciu) prostredníctvom IDM dáta, ktoré sú potrebné pre rozhodovaní o priradení vyššieho stupňa autorizácie prístupu k citlivým dátam. Security Manager teda môže aplikovať niekoľko postupov na to, ako overiť užívateľovu identitu, a to podľa aktuálnej situácie respektíve potrieb jednotlivých služieb, k nim sa pristupuje.

EPG
Tento externý modul ponúka služby tzv elektronického sprievodcu programami (Electronic Program Guide - EPG) pre užívateľov HBB-Next. V závislosti na tzv. metadátach a ďalších aktívnych službách, generuje informačné dáta ktoré sú následne zobrazované užívateľom. Rozsah programov je obyčajne vysoko subjektívna vec, navyše spojená aj s aspektom vhodnosti programov v závislosti na veku užívateľa, resp. najmladšieho užívateľa k skupine, ktorá TV práve sleduje. Security Manager tu potom plní rolu, ktorá dodáva EPG službe informáciu, či daný užívateľ je dostatočne autentizovaný na to, aby mohol autorizovaný pre sledovanie konkrétneho programu či relácie, a to aj prostredníctvom spolupráce s MM a IdM modulom.

5.1.3 Vzťahy medzi modulmi architektúry

Každý modul architektúry vykonáva úlohy, ktoré boli popísané v predchádzajúcej podkapitole. Účelom tejto kapitoly je popísať vzťah medzi jednotlivými modelmi tak, aby sme objasnili základnú interakciu medzi modulmi na konkrétnom príklade. Na obrázku 7 sú znázornené vzťahy medzi samotným Security Manager a ostatnými komponentami architektúry HBB-Next.



Obrázok 7: SM a jeho vzťahy v rámci architektúry HBB-Next

Tak, ako bolo popísané, Security Manager komunikuje s ostatnými komponentami architektúry prostredníctvom modulu manažovania API. To znamená, že systémová brána je zodpovedná ka komunikáciu so systémovými modulmi, ako sú MM, PM respektíve IDM, tak ako je naznačené na Obrázok . Aplikačná brána modulu manažovania služieb komunikuje s aplikáciami, čo môžu byť jedna aplikácie vysielania, internetu, respektíve aj SH. Na obrázku 7 sú naznačené žltou farbou pre sprehľadnenie schémy tak, že komunikujú navzájom prostredníctvom naznačenej zbernice. Pre zariadenia a užívateľov platí, že rôzni užívatelia môžu používať rôzne zariadenia, ktoré komunikujú s SM prostredníctvom terminálovej brány, ktorá vykonáva funkciu rozhrania voči tzv. nedôveryhodnej zóne, pretože táto je mimo kontroly používateľa služby a ako také sa nemôže považovať za dôveryhodnú. V prípade modulov na strane zariadení sa môže jednať o špecializované softvérové moduly, ktoré sú vykonávané v koncových zariadeniach a podliehajú politike autentizácie a autorizácie tak, ako sme popísali v predchádzajúcich kapitolách.

Rozhranie SM voči modulu IDM zabezpečuje komunikáciu s IDM, ktorý v prostredí HBB-Next zodpovedá za správu identít užívateľov. Pre SM zabezpečí zoznam identifikovaných resp. neidentifikovaných (ale prítomných) užívateľov, resp. ich identít. IDM pre MM zároveň zabezpečuje tiež poskytnutie vzorky (napríklad hlasu) pre samotný proces spracovania multimodálnej analýzy. To je naznačené prepojením MM a IDM. Samotný SM rozhraním s MM nedisponuje.

Rozhranie SM a MM slúži na príjem výsledku autentizácie užívateľa podstupujúceho jednu z foriem multimodálnej identifikácie. Rozhranie voči aplikáciám slúži pre autentizáciu aplikácie samotnej, a pre autorizáciu prístupu užívateľov k informačným zdrojom služieb, ktoré poskytujú. V našom prípade je to aplikácia prezerania obsahu z internetu na TV a aplikácia pre SH. Aplikácie môžu navzájom interagovať, pristupovať ku zdrojom navzájom, preto v tomto prípade architektúra umožňuje rovnaké služby autorizácie v SM prostredníctvom interných modulov SM ako pri iných užívateľoch (samozrejme prostredníctvom aplikačnej brány modulu manažovania API).

Rozhranie SM voči PM slúži pre budúce zjednotenie informácií o profile užívateľa z prostredia IDM a prostredia PM do jednej funkčnej entity, ktorá bude reprezentovať úplný profil užívateľa.

5.1 Modelová aplikácia využitia - AppStore

V rámci architektúry HBB-Next je ponúkaných niekoľko nových konceptov, a medzi nimi aj koncept aplikačného obchodu (*AppStore*). Aplikačný obchod je novým prvkom v portfóliu možných služieb budúcich poskytovateľov HBB-Next produktov, ktorý prináša možnosť výberu rôznych aplikácií, dodávaných buď poskytovateľmi služieb alebo aplikačnými vývojármi z tretích strán, podľa preferencií samotného užívateľa. Tieto aplikácie sú vztiahnuté k samotných službám hybridného širokopásmového TV a vysielania či službám SH, a ako také obyčajne poskytujú vyššiu pridanú hodnotu, zameranú na špecifickú oblasť záujmu užívateľa, ale s výrazným aspektom využitia ponúkaných nových vlastností HBB-Next architektúry, a to napríklad v oblasti biometrickej autentizácie, viacúrovňovej autorizácie, rozpoznávania gest, rozšírenej bezpečnosti či užívateľských odporúčaní.

V rámci realizácie modelovej aplikácie využitia SM v prípade aplikačného obchodu HbbTV, uvádzame v praktickej časti našej dizertačnej práce niekoľko sekvenčných diagramov, prostredníctvom ktorých je detailne vysvetlená rola Security Manager ako takého, vrátane interakcie s externými entitami. Pre vizualizáciu uvedeného príkladu, ako aj pre demonštráciu praktických výsledkov, uvádzame referenciu na príslušný video záznam (HBB-

NEXT, YouTube, 2014). Uvedený algoritmus je možné využiť aj v prípade, ak by sa Alica identifikovala ďalším faktorom napríklad svojím chytrým náramkom (*wearable*), či iným vhodným identifikátorom z rodiny zariadení SH.

6 PÔVODNÉ VEDECKÉ PRÍNOSY

Dizertačná práca prináša nasledovné pôvodné vedecké prínosy:

1. Navrhnutý mechanizmus a funkčný model implicitnej autentizácie užívateľov
   1a) Navrhnutý mechanizmus a funkčný model SM – časť autentizácia
   1b) Navrhnutý algoritmus pre diferenciáciu zdieľania a prístupu k užívateľským dátam
   1c) Navrhnutý mechanizmus a funkčný model SM - časť klasifikácie prístupu
   1d) Navrhnutý mechanizmus a funkčný model SM - časť viacfaktorovej autentizácie
2. Navrhnutý mechanizmus a funkčný model využitia rôznych IdP
   2a) Navrhnutý mechanizmus a funkčný model SMIM (Security Manager's Identity module)
   2b) Navrhnutý mechanizmus zdieľania bezpečnostných komponentov architektúry HBB-Next a IoT
3. Návrh systémového a funkčného modelu architektúry Security Manager (SM)
   3a) Navrhnutý systémový a funkčný model architektúry SM
   3b) Navrhnutá koncepcia vzájomných vzťahov medzi internými modulmi SM
   3c) Navrhnutá koncepcia vzájomných vzťahov s modulmi externých subsystémov v kontexte architektúry HBB-NEXT
   3d) Navrhnutý mechanizmus zdieľania bezpečnostných komponentov IoT a HBB-Next
   3e) Aplikácia systémového a funkčného modelu SM v prostredí IoT (Smart Home)
4. Implementácia navrhnutej architektúry SM a testovanie jeho vybraných funkcionalít
   4a) Implementácia Security manažéra do aplikácie „Smart AppStore" a testovanie jeho vybraných funkcionalít v rámci riešenia FP7 projektu HBB-NEXT

7 Konkrétne závery pre ďalší výskum

Dizertačná práca rozpracúva tematiku Security Manager v prostredí služieb hybridného širokopásmového vysielania a SH, čo je témou aktuálnou a tiež komplexnou. Niekoľko tém, ktoré môžu byť predmetom ďalšieho výskumu, uvádzame v tejto kapitole.

1. V oblasti Modulu internej správy, ktorý vykonáva klasifikáciu jednotlivých udalostí, je možnosť orientovať ďalšie výskumné aktivity do oblasti detailnej špecifikácie konkrétnych metód a postupov pre čo najefektívnejšie vyhodnocovanie udalostí, s dôrazom na monitorovanie a vyhodnocovanie bezpečnostných incidentov a hrozieb v reálnom čase, berúc do úvahy všetky komponenty komunikujúce v ekosystéme HBB-Next.

2. Osobitným prípadom scenára možného nasadenia SM budúcich služieb (aj napr. mimo oblasti HbbTV) je oblasť tele medicíny. Táto oblasť je charakterizovaná vysokými nárokmi na bezpečnosť a privátnosť užívateľských dát, ako aj vysokými nárokmi na štandardizáciu integračných rozhraní. SM a jeho funkcionality sa javia ako vhodné pre

napĺňanie bezpečnostných požiadaviek aj v tejto oblasti. Vidíme tu preto priestor pre ďalší výskum.

3. Obrazové dáta môžu byť súčasťou súboru informácií o osobe, ktoré môžu byť v HbbTV a SH službách zaznamenávané a ukladané. Keďže môžu mať charakter privátnych dát, a zároveň môže existovať umožniť ich kontrolované a bezpečné zdieľanie, je možné na túto oblasť aplikovať mechanizmus DRM. Predmetom ďalšieho výskumu preto môže byť aj úloha SM vo vzťahu k týmto subsystémom manažmentu digitálnych práv.

Zoznam použitej literatúry

Clapauch, J. (04 2012). *A Survey of Smart House Security.* Cit. 2015. Dostupné na Internete: University of British Columbia: http://blogs.ubc.ca/computersecurity/files/2012/04/JClapauch_571B.pdf

Choudhary, J. (2012). Survey of Different Biometrics Technique. *International Journal of Modern Engineering Research (IJMER), 2*, 3150-3155 .

Alrawais, A. A. (2015). X. 509 Check: A Tool to Check the Safety and Security of Digital Certificates. *International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI)* (s. 130-133). Peking: IEEE.

Arabo, A. B.-M. (2012). Privacy in the age of mobility and smart devices in smart homes. *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom)* (s. 819-826). Amsterdam: IEEE.

Armbrust, M. e. (2010). Comm's of the ACM. A View of Cloud Computing., (s. 50-58).

Bagüés, S. Z. (2007). Sentry@Home : Leveraging the Smart Home for Privacy in Pervasive Computing. *International Journal of Smart Home, 1*(2).

Brezovan, M. e. (09 2013). *An Overview of Smart Home Environments: Architectures, Technologies and Applications.* Cit. 2016. Dostupné na Internete: Penn State University: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.478.7241&rep=rep1&type=pdf

D. Guinard, M. F. (2010). Sharing using social networks in a composable web of things. *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference on* (s. 702 - 707). Mannheim: IEEE.

D. Levický. (2010). *Kryptografia v informačnej a sieťovej bezpečnosti.* Košice: ELFA.

Das, S. (2013). Technology for SMART HOME. In Y. J. Veena S. Chakravarthi, *Proceedings of International Conference on VLSI, Communication, Advanced Devices, Signals & Systems and Networking (VCASAN-2013)* (s. 7-12). Springer India.

David W. Chadwick, K. S. (2014). Adding Federated Identity Management to OpenStack. *Journal of Grid Computing , 12*(1), 3-27.

EC. (22. 10 2014). *HBB-NEXT: TV evolution leaves no one behind*. Cit. 2016. Dostupné na Internete: European Commision: https://ec.europa.eu/digital-single-market/en/news/hbb-next-tv-evolution-leaves-no-one-behind

ETSI. (October 2015). *ETSI TS 102 796 V 1.3.1.* Cit. 2016. Dostupné na Internete: ETSI TS: http://www.etsi.org/deliver/etsi_ts/102700_102799/102796/01.03.01_60/ts_102796v010301p.pdf

ETSI. (Jun 2016). *ETSI TS 102 796.* Cit. 2016. Dostupné na Internete: ETSI TS: http://www.etsi.org/deliver/etsi_ts/102700_102799/102796/01.01.01_60/ts_102796v010101p.pdf
Fengming, N. F. (2012). SAML-based single sign-on for legacy system. *IEEE International Conference on Automation and Logistics (ICAL)* (s. 470-473). IEEE.
Foundation, O. C. (2015). *Providing the Software Linking the Internet of Things*. Cit. 2015. Dostupné na Internete: http://openconnectivity.org/
G. Rozinaj, J. K. (2013-2015). *Integration of Multimedia Signal Processing Methods into Multimodal Interface and Network Applications - IMUROSA.* VEGA 1/0708/13.
Gantz John, D. R. (2012). *The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east.* IDC iView: IDC Analyze the Future.
Garcia-Carrillo, D. &.-L. (2016). Lightweight CoAP-Based Bootstrapping Service for the Internet of Things. *Sensors 2016*(16(3)), 358.
GfK. (2017). *Report: Tech Trends 2017.* Cit. 2017. Dostupné na Internete: Tech Trends 2017 - Smart home: insights.gfk.com/report-tech-trends-2017
Goel, A. w.-A. (2016). *How to Easily Identify Your Federated Users by Using AWS CloudTrail*. Dostupné na Internete: http://blogs.aws.amazon.com/security/post/Tx2VW7TIKH1TY5E/How-to-Easily-Identify-Your-Federated-Users-by-Using-AWS-CloudTrail
Google. (2015). *CLOUD IDENTITY & ACCESS MANAGEMENT*. Cit. 2015. Dostupné na Internete: https://cloud.google.com/iam/
Google API. (2015). *SAML-based Federated SSO*. Dostupné na Internete: https://support.google.com/a/answer/6087519?hl=en
Group, I. O. (2014). *OAuth 2.0*. Dostupné na Internete: http://oauth.net/2/
Gómez Mármol, F. R. (June 2014). Smart AppStore: widening the frontiers of smartphone ecosystems. *IEEE Computer*, 42-47.
Harry, J. (2003). Federated Identity Management, Federated Single Sign-On and Web Services Security. *FIM 6.1 MBP Workshop.*
HBB-NEXT. (03 2012). *ANALYSIS: State of The Art on Identity, Security and Trust.* Dostupné na Internete: HBB-Next: http://www.hbb-next.eu/documents/HBB-NEXT_D3%201.pdf
HBB-NEXT. (09 2012). *DESIGN AND PROTOCOL (High Level Architecture): User ID, Profile, Application Reputation Framework.* Dostupné na Internete: HBB-Next: http://www.hbb-next.eu/documents/HBB-NEXT_D3.2.pdf
HBB-NEXT. (10 2014). *Architecture, Final HBB-NEXT System*. Dostupné na Internete: hbb-next.eu: http://www.hbb-next.eu/documents/HBB-NEXT_D6.1.3.pdf
HBB-NEXT. (27. May 2014). *YouTube.* Dostupné na Internete: Demo of Smart App Store: https://www.youtube.com/watch?v=CdtkFb4s8Kc
hbbTV.org. (2015). *www.hbbtv.org*. Dostupné na Internete: HbbTV services and devices at IBC 2013: http://www.hbbtv.org/wp-content/uploads/2015/07/HbbTV-Handout_IBC2013.pdf
Herfurt, M. (1. Jún 2013). *Security concerns with HbbTV.* Cit. 2015. Dostupné na Internete: Martin Herfurt's blog: https://mherfurt.wordpress.com/2013/06/01/security-concerns-with-hbbtv/
internet2. (2014). *Shibboleth: Trust & Identity* . Dostupné na Internete: http://www.internet2.edu/products-services/trust-identity/shibboleth/
iotivity. (2015). *iotivity*. Cit. 2015. Dostupné na Internete: https://www.iotivity.org/about
Ishengoma, F. R. (2014). Authentication System for Smart Homes Based on ARM7TDMI-S and IRIS-Fingerprint Recognition Technologies. *Programmable Device Circuits and Systems , 6*(6), s. 162-167.

Jensen, J. (2012). Federated Identity Management Challenges. *Seventh International Conference on Availability, Reliability and Security (ARES)* (s. 230-235). CPS.
Keoh, S. L. (2014). Securing the internet of things: A standardization perspective. *Internet of Things Journal, 1*(3), 265-275.
Khan, R. K. (2012). Future internet: the internet of things architecture, possible applications and key challenges. *In Frontiers of Information Technology (FIT), 10th International Conference on* (s. 257-260). Islamabad: IEEE.
Kim, J. B. (2012). Seamless integration of heterogeneous devices and access control in smart homes. *Proceedings of the 8th International Conference on Intelligent Environments (IE 2012).* Guanajuato.
Kokolevsky, T. (2013). *Diplomová práca - Rozšírenie platformy Hybrid Broadcast Broadband TV.* STU BA, FEI.
konzorcium, H. (2. 2 2016). *HBBTV.* Cit. 2016. Dostupné na Internete: https://www.hbbtv.org/membership/
Kozlov, D. V. (2012). Security and privacy threats in IoT architectures. *In Proceedings of the 7th International Conference on Body Area Networks* (s. 256-262). ICST.
Lindsay-Davies, R. (3 2016). *HbbTV Symposium 2015, London.* Dostupné na Internete: hbbtv.org: https://www.hbbtv.org/wp-content/uploads/2015/12/HbbTV-Symposium-Europe-2015.pdf
Lábaj, O. (2015). Dizertačná práca - Viacúrovňové riadenie prístupu v multimediálnych aplikáciách. Bratislava.
Magazine, C. (24. March 2010). *CED magazine.* Cit. 2015. Dostupné na Internete: http://www.cedmagazine.com/news/2010/03/broadband-briefs-03-24-10
Mahmoudi, O. &. (2013). Contribution to intelligent environment's security. *Advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference on* (s. 1878-1883). Mysore: IEEE.
Mainka, C. M. (2014). *Do not trust me: Using malicious IdPs for analyzing and attacking Single Sign-On.* (a. p. arXiv:1412.1623, Ed.) Cit. 2015. Dostupné na Internete: http://arxiv.org/abs/1412.1623
Marco Ghiglieri, F. O. (14. Máj 2013). *HbbTV – I Know What You Are Watching.* Cit. 2015. Dostupné na Internete: SIT TU Darmstadt: https://www.sit.tu-darmstadt.de/fileadmin/user_upload/Group_SIT/Publications/05_Ghiglieri_Oswald_Tews_HbbTV-I_Know_What_Your_Are_Watching.pdf
Matejka, J. (05 2011). Bezpečnosť v sieťach pre vytváranie a riadenie multimediálnych služieb a relácií. *Písomná práca k dizertačnej skúške*. Bratislava.
Moosavi, S. R. (2015). SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. . (52), s. 452-459.
More, V. N. (2011). Authentication and Authorization Models. *International Journal of Computer Science and Security (IJCSS)*(5(1)), 72-84.
Morgan, R. L. (2004). Federated Security: The Shibboleth Approach. *EDUCAUSE Quarterly, 27*(4), 12-17.
Morris R., T. K. (1979). Password security: a case history. *Commun. ACM, 22(11)*, s. 594–597.
Neuman, B. T. (1994). Kerberos: an authentication service for computer networks. *Communications Magazine, 32*(9), s. 33-38.
News, B. T. (9. December 2009). *EBU General Assembly backs HBB.* Cit. 2016. Dostupné na Internete: http://www.broadbandtvnews.com/2009/12/07/ebu-general-assembly-backs-hbb/

OASIS. (2008). *Security Assertion Markup Language (SAML) V2.0 Technical Overview*. Cit. 2014. Dostupné na Internete: https://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf

OASIS. (2009). *Web Services Federation Language (WS-Federation) Version 1.2*. Cit. 2015. Dostupné na Internete: http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.html

O'Malley, J. (13. 03 2016). *Smart TV in 2016: How Android TV, webOS + others are changing the game.* Dostupné na Internete: techradar.com: http://www.techradar.com/news/television/how-android-tv-webos-firefox-os-and-tizen-powered-smart-tv-into-a-new-age-1279578

OWASP project. (2014). *Internet of things - top ten.* Cit. 2015. Dostupné na Internete: Open Web Application Security Project: https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf

Perera, C. Z. (2014). *Context aware computing for the internet of things: A survey.Communications Surveys & Tutorials 16(1).* IEEE.

Riu Wang, S. C. (2012). *Signing Me onto Your Accounts through Facebook and Google: a Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services.* Cit. 2015. Dostupné na Internete: http://research.microsoft.com/pubs/160659/websso-final.pdf

Schneier, B. (2004). *Sensible Authentication, ACM Queue 1.*

Schumann, S. (2015). Dizertačná práca - Next generation identity management to enable converged personalized services. Bratislava.

Sae-Bae, N. A. (2012). Biometric-rich gestures: a novel approach to authentication on multi-touch devices. *SIGCHI Conference on Human Factors in Computing Systems* (s. 977-986). Austin: ACM.

Sha Liu, S. Z. (2015). Page 1 A Novel QR Code and mobile phone based Authentication protocol via Bluetooth. *International Conference on Materials Engineering and Information Technology Applications (MEITA 2015)* (s. 41-49). Hong Kong: atlantis-press.com.

Sharma, A. S. (2015). Identity and access management- a comprehensive study. *Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on* (s. 1481-1485). Noida: IEEE.

Shim, S. B. (2005). Federated identity management. *Computer vol. 38 (12)*, 120-122.

Smith, D. (2008). Federated ID: The Challenge of Federated Identity Management. *Network Security*(4), s. 7-9.

ThingSpeak. (2015). *ThingSpeak: Internet of things - application platform*. Cit. 2015. Dostupné na Internete: https://thingspeak.com/

Vaidya, B. P. (2011). Robust one-time password authentication scheme using smart card for home network environment. *Computer Communications, 34*(3), s. 326-336.

van Deventer, M. O. (2013). Towards next generation Hybrid broadcast broadband, results from FP7 and HbbTV 2.0. *IBC2013 Conference* (s. 12.3). Amsterdam: IBC.

Wanpeng Li, C. J. (2014). Security Issues in OAuth 2.0 SSO Implementations. *17th International Conference, ISC 2014, Hong Kong, China, October 12-14, 2014. Proceedings* (s. 529-541). Hong Kong: Springer International Publishing.

Xuguang R., X.-W. W. (2012). A novel dynamic user authentication scheme. In I. Symposium (Ed.), *Communications and Information Technologies (ISCIT)*, (s. 713-717).

Yossef Oren, A. D. (2014. Máj 2014). *From the Aether to the Ethernet – Attacking the Internet using Broadcast Digital Television.* Cit. 2015. Dostupné na Internete:

Columbia University: http://www.cs.columbia.edu/~angelos/Papers/2014/redbutton-usenix-sec14.pdf

Yuan, E. &. (2005). Attributed based access control (ABAC) for Web services. *ICWS 2005. Proceedings. 2005 IEEE International Conference on.* (s. 569). IEEE.

Zhu, B. F. (2014). Loxin — A solution to password-less universal login. *Computer Comm's Workshops (INFOCOM WKSHPS)* (s. 488-493). IEEE Conference.

ZOZNAM PUBLIKÁCIÍ AUTORA

AAB Vedecké monografie vydané v domácich vydavateľstvách

AAB01 BRÍDA, Peter - DÚHA, Ján - GALAJDA, Pavol - GAMEC, Ján - KOTULIAK, Ivan - LAVRIN, Anton - MARCHEVSKÝ, Stanislav - MATEJKA, Juraj - MIKÓCZY, Eugen - PILLAR, Slavomír - POČTA, P. - PODHRADSKÝ, Pavol - RÓKA, Rastislav - TRÚCHLY, Peter - WIESER, Vladimír. *NGN, technológie v prístupových sieťach, služby a aplikácie*. Bratislava : Tonada, 2007. CD-Rom. ISBN 978-80-89299-08-9.

AAB02 BRÍDA, Peter - DÚHA, Ján - GALAJDA, Pavol - GAMEC, Ján - KOTULIAK, Ivan - LAVRIN, Anton - MARCHEVSKÝ, Stanislav - MATEJKA, Juraj - MEDVECKÝ, Martin - MIKÓCZY, Eugen - PILLAR, Slavomír - POČTA, P. - PODHRADSKÝ, Pavol - RÓKA, Rastislav - WIESER, Vladimír. *NGN, technológie v transportných sieťach, služby a aplikácie*. Bratislava : Tonada, 2007. CD-Rom. ISBN 978-80-89299-12-6.

AAB03 DÚHA, Ján - GAMEC, Ján - KOTULIAK, Ivan - MATEJKA, Juraj - MEDVECKÝ, Martin - MIKÓCZY, Eugen - PODHRADSKÝ, Pavol - RÓKA, Rastislav. *NGN, technológie v transportných sieťach a spojovacie technológie*. Bratislava : Tonada, 2007. CD-Rom. ISBN 978-80-89299-09-6.

AAB04 GAMEC, Ján - KOTULIAK, Ivan - LEVICKÝ, Dušan - MATEJKA, Juraj - MEDVECKÝ, Martin - MIKÓCZY, Eugen - PODHRADSKÝ, Pavol - RIDZOŇ, Radovan. *Multimédiá, NGN a spojovacie technológie*. Bratislava : Tonada, 2007. CD-Rom. ISBN 978-80-89299-14-0.

AAB05 MATEJKA, Juraj - MIKÓCZY, Eugen - PODHRADSKÝ, Pavol. *Konvergencia sietí a NGN*. Bratislava : STU, 2007. 86 s. ISBN 978-80-227-2607-8.

ABC Kapitoly vo vedeckých monografiách vydané v zahraničných vydavateľstvách

ABC01 PODHRADSKÝ, Pavol - MIKÓCZY, Eugen - MATEJKA, Juraj - LÁBAJ, Ondrej - TOMEK, Róbert - ĎUNGEL, Michal - KOTULIAK, Ivan. Practical Experience with New Services and Applications Supported by NGN. In IBRAHIM, Ismail Khalil.*Handbook of Research on Mobile Multimedia : Vol.1.,2*. 2.ed. Hershey : Information Science Reference, 2008, s.Vol. 2, s.628-645 [1,852 AH]. ISBN 978-1-60566-046-2.

AFC Publikované príspevky na zahraničných vedeckých konferenciách

AFC01 MATEJKA, Juraj - LÁBAJ, Ondrej - LONDÁK, Juraj - PODHRADSKÝ, Pavol. VoIP Protection Techniques. In *Proceedings ELMAR-2010 : 52nd International Symposium ELMAR-2010. Zadar, Croatia, 15.-17.9.2010*. Zadar : Croatian Society Electronics in

Marine, 2010, s.219-224. ISBN 978-953-7044-11-4.

AFC02 MATEJKA, Juraj - LÁBAJ, Ondrej - ŠUPALA, Dušan - KOKOLEVSKÝ, Tomáš - PODHRADSKÝ, Pavol. Security Aspects of Hybrid Broadband Broadcast Communication. In *Proceedings ELMAR-2013 : 55th International Symposium. Zadar, Croatia, 25-27 September 2013*. Zadar : Croatian Society Electronics in Marine, 2013, s.223-226. ISBN 978-953-7044-14-5.

AFC03 MIKÓCZY, Eugen - PODHRADSKÝ, Pavol - KOTULIAK, Ivan - MATEJKA, Juraj. Experimental NGN Lab Testbed for Education and Research in Next Generation Network Technologies. In *Personal Wireless Communications : 12th IFIP International Conference on Personal Wireless Communications. Prague, Czech Republic, 12.-14.9.2007*. New York : Springer Verlag, 2007, s.174-183. ISBN 978-0-387-74158-1.

AFC04 PODHRADSKÝ, Pavol - MIKÓCZY, Eugen - MATEJKA, Juraj - LÁBAJ, Ondrej - KOTULIAK, Ivan. NGN Platform Architecture and Its Adaptation to the Evolution Trends. In *2007 IWSSIP & EC-SIPMCS. 14th International Workshop on Systems, Signals & Image Processing and EURASIP Conference Focused on Speech & Image Processing, Multimedia Communications & Services : Maribor, Slovenia, 27.-30.6.2007*. Maribor : University of Maribor, 2007, 2007), s.CD-Rom. ISBN 978-961-248-029-5.

AFC05 PODHRADSKÝ, Pavol - MIKÓCZY, Eugen - MATEJKA, Juraj - LÁBAJ, Ondrej - KOTULIAK, Ivan - TOMEK, Róbert. Practical Experience with New Services and Applications Supported by NGN Platform. In *Proceedings Elmar-2007 : 49th International Symposium Elmar-2007 focused on Mobile Multimedia. Zadar, Croatia, 12.-14.9.2007*. Zadar : Croatian Society Electronics in Marine, 2007, s.CD-Rom. ISBN 978-953-7044-05-3.

AFC06 MATEJKA, Juraj - PODHRADSKÝ, PAvol - LONDÁK, Juraj. Security Manager for Hybrid Broadcast Broadband Architecture Evolution. In *Proceedings of. 58th International Symposium ELMAR 2016, Zadar, September 2016*. Zadar : Croatian Society Electronics in Marine, 2016, s.223-226. ISBN 978-953-184-221-1.

AFD Publikované príspevky na domácich vedeckých konferenciách

AFD01 PODHRADSKÝ, Pavol - LONDÁK, Juraj - LÁBAJ, Ondrej - MATEJKA, Juraj. Security Challenges in Next Generation HBB TV. In *Proceedings of 2012 5th Joint IFIP Wireless and Mobile Networking Conference : Bratislava, Slovakia, September 19-20, 2012*. Piscataway : IEEE, 2012, s.130-132. ISBN 978-1-4673-2994-1.

AFD02 LONDÁK, Juraj - PODHRADSKÝ, Pavol - MATEJKA, Juraj. Security of IMS Architecture Using Session Border Controller. In *Redžúr 2009 : proceedings; 3rd International Workshop on Speech and Signal Processing. Bratislava, Slovak Republic, 24.9.2009*. Bratislava : STU v Bratislave FEI, 2009, s.CD-Rom. ISBN 978-80-227-3137-9.

BCI Skriptá a učebné texty

BCI01 BRÍDA, Peter - DÚHA, Ján - GALAJDA, Pavol - GAMEC, Ján - KOTULIAK, Ivan - LAVRIN, Anton - MARCHEVSKÝ, Stanislav - MATEJKA, Juraj - MEDVECKÝ, Martin - MIKÓCZY, Eugen - PILLAR, Slavomír - POČTA, P. - PODHRADSKÝ, Pavol

- TRÚCHLY, Peter - WIESER, Vladimír. *NGN, spojovacie technológie, služby a aplikácie*. Bratislava : Tonada, 2007. CD-Rom. ISBN 978-80-89299-03-4.

BCI02 BRÍDA, Peter - DÚHA, Ján - GALAJDA, Pavol - GAMEC, Ján - LAVRIN, Anton - LEVICKÝ, Dušan - MARCHEVSKÝ, Stanislav - MATEJKA, Juraj - MIKÓCZY, Eugen - PILLAR, Slavomír - POČTA, P. - PODHRADSKÝ, Pavol - RIDZOŇ, Radovan - TRÚCHLY, Peter - WIESER, Vladimír. *Multimédiá, NGN, služby a aplikácie*. Bratislava : Tonada, 2007. CD-Rom. ISBN 978-80-89299-05-8.

BCI03 BRÍDA, Peter - DÚHA, Ján - GALAJDA, Pavol - GAMEC, Ján - LAVRIN, Anton - LEVICKÝ, Dušan - MARCHEVSKÝ, Stanislav - MATEJKA, Juraj - MIKÓCZY, Eugen - PILLAR, Slavomír - POČTA, P. - PODHRADSKÝ, Pavol - RIDZOŇ, Radovan - WIESER, Vladimír. *NGN, služby a aplikácie, informačná bezpečnosť*. Bratislava : Tonada, 2007. CD-Rom. ISBN 978-80-89299-02-7.

BCI04 DÚHA, Ján - GAMEC, Ján - KOTULIAK, Ivan - LEVICKÝ, Dušan - MARCHEVSKÝ, Stanislav - MATEJKA, Juraj - MIKÓCZY, Eugen - PODHRADSKÝ, Pavol - RIDZOŇ, Radovan - RÓKA, Rastislav - TRÚCHLY, Peter - WIESER, Vladimír. *NGN, technológie v prístupových sieťach a informačná bezpečnosť*. Bratislava : Tonada, 2007. CD-Rom. ISBN 978-80-89299-06-5.

BCI05 DÚHA, Ján - GAMEC, Ján - KOTULIAK, Ivan - MATEJKA, Juraj - MEDVECKÝ, Martin - MIKÓCZY, Eugen - PODHRADSKÝ, Pavol - RÓKA, Rastislav - TRÚCHLY, Peter - WIESER, Vladimír. *NGN, technológie v prístupových sieťach a spojovacie technológie*. Bratislava : Tonada, 2007. CD-Rom. ISBN 978-80-89299-04-1.

BCI06 DÚHA, Ján - GAMEC, Ján - KOTULIAK, Ivan - LEVICKÝ, Dušan - MARCHEVSKÝ, Stanislav - MATEJKA, Juraj - MIKÓCZY, Eugen - PODHRADSKÝ, Pavol - RIDZOŇ, Radovan - RÓKA, Rastislav - TRÚCHLY, Peter - WIESER, Vladimír. *Multimédiá, NGN a technológie v prístupových sieťach*. Bratislava : Tonada, 2007. CD-Rom. ISBN 978-80-89299-10-2.

ACB01 MIKÓCZY, Eugen - PODHRADSKÝ, Pavol - MATEJKA, Juraj - LÁBAJ, Ondrej - TOMEK, Róbert - KADLIC, Radovan - SCHUMANN, Sebastian - MASSNER, Stephan - TRÚCHLY, Peter - KOTULIAK, Ivan - MIKULA, Juraj - LONDÁK, Juraj. NGN Protocols. In *NGN Architectures and Protocols, Information and Network Security, Internet Protocol, Optical Networks, Digital Television, Traffic Engineering in Mobile Networks*. Bratislava: Nakladateľstvo STU, 2011, s.DVD-Rom [179 s.]. ISBN 978-80-01-04949-5.

AFC Publikované príspevky na zahraničných vedeckých konferenciách

AFC01 LONDÁK, Juraj - MATEJKA, Juraj - PODHRADSKÝ, Pavol. IMS Security and OpenSBC Testing. In *RTT 2010. Research in Telecommunication Technology : 12th International Conference. Velké Losiny, Czech Republic, 8.- 10.9.2009*. Ostrava : VŠB - Technical University of Ostrava, 2010, s.CD-Rom. ISBN 978-80-248-2261-7.

Resumé

Title: Security Manager in HbbTV and IoT

Keywords: HbbTV, authentication, identification, authorization, Security Manager, HBB-Next, IoT, Smart Home

The subject of the thesis is design of security subsystem as part of HBB-Next architecture, that is responsible for authentication, authorization, differentiation of sharing and access to the user's data, including control of multifactor authentication. Research is focused on selected security challenges from the area of multimedia TV services and IoT. This work also address challenges of federated identity management in the HbbTV area.