SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY
A INFORMATIKY

Ondrej Lábaj

Autoreferát dizertačnej práce

VIACÚROVŇOVÉ RIADENIE PRÍSTUPU V MULTIMEDIÁLNYCH APLIKÁCIÁCH

na získanie akademickej hodnosti doktor (philosophiae doctor, PhD.)

v doktorandskom študijnom programe: **Telekomunikácie**
v študijnom odbore 5.2.15 Telekomunikácie

Bratislava, 22.6.2015

Dizertačná práca bola vypracovaná v externej forme doktorandského štúdia

Na Ústave telekomunikácií FEI STU BA v Bratislave

Predkladateľ: Ing. Ondrej Lábaj
Ústav telekomunikácií
Fakulta elektrotechniky a informatiky
Slovenská technická univerzita v Bratislave
Ilkovičova 3, 812 19 Bratislava

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

Oponenti: prof. Ing. Stanislav Marchevský, CSc.
Fakulta Elektrotechniky a informatiky TU v Košiciach, Letná 9, 042 00 Košice

doc. Ing. Ján Dúha, PhD.
Elektrotechnická fakulta ŽU v Žiline, Univerzitná 1, 010 26 Žilina

Autoreferát bol rozoslaný: .....

Obhajoba dizertačnej práce sa koná: .....

Na FEI STU v Bratislave v zasadacej miestnosti Ústavu telekomunikácií FEI STU, Ilkovičova 3, 812 19 Bratislava

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

Obsah

1 Úvod

Za posledných 20 rokov zohrali informačné a telekomunikačné systémy prudký rozvoj smerom ku globalizácii a vzájomnej previazanosti poskytovaných aplikácií. Tento vývoj smeroval od špecializovaných, cez podnikové systémy až do domácností a súkromnej sféry v podobe multimediálneho obsahu, za ktorého rozmach vďačí stále narastajúcej popularite internetu.

Výrazný podiel na tomto vývoji predstavujú koncové zariadenia, ktoré sú pre používateľa cenou, funkčným vybavením a zlepšujúcou sa jednoduchosťou ovládania stále dostupnejšie pre široké spektrum ľudí s rozdielnym vekom a preferenciami.

Ďalším faktorom je taktiež mobilita pri využívaní akéhokoľvek typu multimediálnej služby, ktorá umožnila ľuďom nielen telefonovať mimo pracoviska, či domácnosti, ale v súčasnosti využívať celé spektrum doteraz využívaných služieb, ako sú sociálne siete, televízia, internetbanking, či nakupovanie prakticky kdekoľvek a to nezávisle od typu používaného koncového zariadenia.

Poskytované služby sa za posledných pár rokov snažia prispôsobiť ponúkaný multimediálny obsah prostrediu a okruhu záujmov používateľov služieb na základe ich zvyklostí, preferencií pri vyhľadávaní konkrétnej informácie na internete, priateľov v ich okolí a pod. Za týmto účelom vznikajú rôzne previazania služieb, ktoré boli predtým nezávislé. Tento trend zasiahol aj do oblasti súkromia používateľa, týkajúcich sa hlavne narábania s osobnými informáciami a dôvery, kde hranice nie sú vždy jasne stanovené a pre používateľa jasne zrozumiteľné. Vývoj nových multimediálnych aplikácií, systémov a ich vzájomné previazanie pravidiel je v informačnej bezpečnosti mnohokrát vnímané rozdielnym spôsobom alebo s nedostatočným ohľadom na súkromie používateľa. To sa nemusí nevyhnutne diať úmyselne, ale s cieľom poskytnúť používateľovi služby komfort obsluhy a zážitok z jej používania. Vývoj multimediálnych aplikácií tak často naráža na správne skĺbenie bezpečnosti a použiteľnosti tak, aby mal používateľ jednoduchú registráciu, prihlásenie sa do služby a jej používanie pri správnom aplikovaní bezpečnostných pravidiel vzhľadom na to aké koncové zariadenie používa, s akým typom informácie narába a kde sa v čase využívania služby nachádza.

1.1 Motivácia

V roku 1987, Brian Reid napísal *„Pohodlie programátora je protikladom bezpečnosti, pretože ide práve o pohodlie útočníka, ak je účet programátora ohrozený.“* [1]

Tento fundamentálny konflikt medzi silnými bezpečnostnými mechanizmami a použiteľnosťou systému prenikol do dnešného sveta informačných a komunikačných systémov, ktoré využívame čoraz častejšie. Začalo prevládať presvedčenie, ktoré tvrdí, že dostatočne sofistikované zabezpečenie znamená komplexnosť systému, ktorý je potom ťažké používať. [2]

V súčasnej dobre však rastie počet odborníkov, ktorí si uvedomujú, že toto presvedčenie obsahuje vnútorný rozpor. Hľadanie spôsobov ako maximalizovať použiteľnosť systému a zároveň jeho zabezpečenie bol a je dlhodobý problém. Saltzerov a Schroederov [3] princíp psychologickej akceptovateľnosti hovorí, že bezpečnostné mechanizmy by nemali pristupovať ku prostriedkom alebo vykonávať akciu zložitejšie ako keby tieto bezpečnostné mechanizmy neexistovali. V praxi to znamená, že bezpečnostné mechanizmy by mali pridať na obťažnosti obsluhy systému používateľom také minimum, ako je to len možné.

Aplikovanie tohto princípu však prináša zásadnú otázku - Obťažné pre koho? Pre mladého človeka dnešnej modernej doby nemusí byť prístup do aplikácie rovnako zložitý, ako

napríklad pre staršieho človeka. Aplikovanie princípu psychologickej akceptovateľnosti vyžaduje prihliadnutie na znalosti, vek a mentálne schopnosti ľudí, ktorý budú daný systém používať. [4]

2 Ciele dizertačnej práce

Kľúčovou úlohou dizertačnej práce je adresovať možnosti riadenia prístupu ku informačnému obsahu na základe jeho klasifikácie, a to podľa úrovne potrebného zabezpečenia. Dôležité je ale zároveň riešiť správu prideľovania oprávnení a spôsob vyhodnocovania žiadostí o prístup, zameraný na rôznych používateľov z pohľadu ich vzájomných vzťahov a prostredia, ktoré môže rozhodovanie priamo ovplyvniť.

V prípade štandardov neexistuje univerzálny protokol/protokoly adresujúci túto problematiku komplexne, ale len prostredníctvom viacerých protokolov. Systémy rozhodujúce o riadení prístupu sú často postavené pre konkrétne aplikácie primárne v podnikovom prostredí. Kritérium, ktoré je hlavnou motiváciou, a to komfort používateľa počas prístupu ku informačnému obsahu pri dodržaní stanovenej úrovne zabezpečenia, je v komplexných systémoch často obmedzené zložitými postupmi overovania identity.

Ciele dizertačnej práce sme si preto definovali nasledovne:

1. Návrh algoritmu viacúrovňového riadenia prístupu k informačnému obsahu, ktorý zároveň umožní využitie viacerých identifikačných a autentifikačných mechanizmov a zohľadňuje prostredie, v ktorom sa používateľ nachádza.
2. Návrh architektúry centralizovaného systému riadenia prístupu, jeho funkčných komponentov a definovanie potrebných rozhraní smerom do externého prostredia.
3. Návrh protokolu komunikácie medzi jednotlivými komponentmi architektúry a externým prostredím prostredníctvom sekvenčných diagramov. Sekvenčné diagramy musia zohľadniť hierarchiu používateľov, ich vzájomných vzťahov a prostredie v čase žiadosti o prístup ku konkrétnemu informačnému obsahu.
4. Implementácia centralizovaného systému riadenia prístupu do vybraného multimediálneho systému, využívajúceho a rešpektujúceho prístup používateľa k službám v závislosti od požadovaného stupňa zabezpečenia informačného obsahu v prostredí interaktívnych služieb.

3 Teoretické a praktické predpoklady

Problematika ochrany identity používateľa a jeho súkromia, vrátane riadenia prístupu ku službám a ich prostriedkom v rámci systému spadá do komplexnej problematiky sieťovej bezpečnosti, konkrétne časti zaoberajúcej sa prístupovou bezpečnosťou. Základnými piliermi prístupovej bezpečnosti sú autentifikácia používateľov a riadenie prístup ku systémových prostriedkom a službám. [5] Dôležitú úlohu v procese autentifikácie a riadenia prístupu však zohráva aj samotný používateľ.

3.1 Autentifikácia

Používateľov systému je možné autentifikovať na základe toho, že niečo **vedia** (memometrics), niečo **rozpoznajú** (cognometrics), niečo **vlastnia** alebo **čím sú** charakteristický (biometrics). Pri všetkých troch spôsoboch systém s používateľom zdieľajú tajomstvo (tzv. authentication key). [7] Počas registrácie sa používateľ a systém dohodnú, čo

tým tajomstvom bude. V prípade biometrie systém počas registrácie zaznamená digitálnu reprezentáciu niektorého aspektu používateľovej fyziológie alebo správania.
Výber vhodného autentifikačného mechanizmu alebo mechanizmov závisí od viacerých faktorov, ktorými sú:

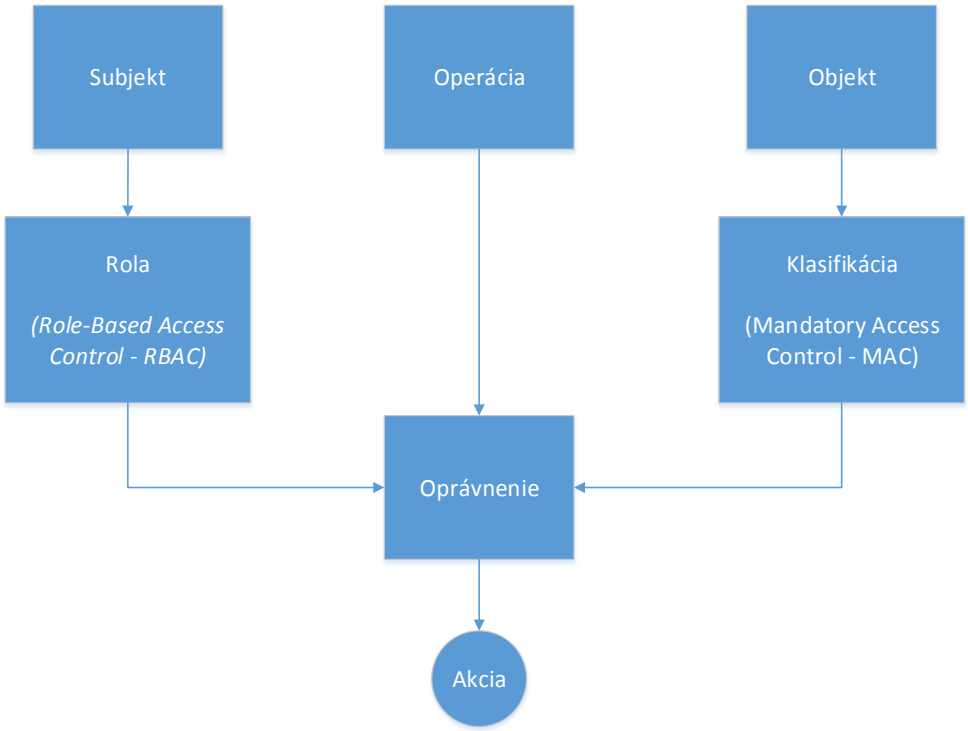
- Bariéry dostupnosti - príkladom sú ľudia trpiaci problémami s pamäťou, ľudia ktorí majú problém pri práci s textom alebo vykonávaním akcií, vyžadujúce dodržanie istých sekvencií v správnom poradí. Títo ľudia majú ťažkosti najmä pri použití autentifikačných metód založených na znalosti tajomstva.
- Niektoré autentifikačné mechanizmy požadujú vizuálnu aktivitu alebo pohyb, čo môže byť problém pre nevidiacich alebo starších ľudí.
- Ľudské faktory - Pretože mnohé autentifikačné mechanizmy vyžadujú kognitívnu aktivitu, je nevyhnutné mať na zreteli procesy ľudského zmýšľania a limitácie pamäti, ktoré sú predpokladom pre úspešné aplikovanie autentifikačných metód založených na znalosti tajomstva. Uložená správa môže časom zanikať alebo interferovať s inými alebo podobnými správami v pamäti alebo je jednoducho zabudnutá, pretože nebola v pamäti používateľa šifrovaná s vhodným vodítkom/vodítkami tak, aby túto správu bolo možné neskôr extrahovať. [11]
- Bezpečnosť - Používané autentifikačné mechanizmy musia byť úmerné tomu, aký prostriedok alebo aplikácia je používateľovi poskytovaný. To znamená, že napr. aplikácie internet bankingu požadujú oveľa silnejšiu autentifikáciu, ako aplikácie, ktoré zdieľajú rovnaký obsah s rôznymi používateľmi, ako napríklad predplatený obsah televíznych kanálov. Pred rozhodovaním sa aký autentifikačný mechanizmus bude použitý, je potrebné analyzovať, aká informácia bude chránená a aký prístup bude poskytovaný.
- Významný efekt zohráva samotné prostredie. Napríklad, organizácie používajú často bezpečnostné pravidlá, ktoré stanovujú obnovu hesla po určitom časovom období. Organizácie tým chcú zabrániť úniku firemných údajov v prípade uniknutého kľúča. Efekt tohto opatrenia je však často opačný a zamestnanci s cieľom ľahko si pamätať vždy nové heslo, volia si ľahko zapamätateľné kombinácie, pri ktorých menia iba poslednú časť hesla tak, aby vyhovovalo stanoveným pravidlám. Požiadavky na zložitosť hesla ich ku tomuto v podstate vedú. [12] Tieto reštriktívne pravidlá ale na druhej strane dokážu zabrániť katastrofe v neočakávaných situáciách, akým je napríklad hromadné odhalenie hesiel v systéme.

3.2 Autorizácia

Autorizácia je overenie oprávnení subjektu pri vstupe (do siete alebo služby), na základe prístupových práv. [25] Oprávnenia definujú, ku ktorým informáciám môže identifikovaný a autentifikovaný používateľ pristupovať a aké akcie môže vykonať.

Povolenia závisia na subjekte – používateľovi, pristupujúcom ku objektom a operácii, ktorú si želá vykonať. Prienikom role používateľa a klasifikácie objektu vzniká oprávnenie (viď. obr. 1).

V súčasnosti sa využíva niekoľko hlavných modelov riadenia prístupu.
Napríklad, Mandatory Access Control (MAC) používa na určenie toho, ku čomu môže subjekt (používateľ) pristupovať tzv. klasifikácie. Subjekt teda môže pristúpiť ku všetkým objektom, ktorých úroveň oprávnenia je nižšia alebo rovná, ako klasifikácia objektu.
Najrozšírenejším modelom je tvz. Role-Based Access Conrol (RBAC), ktorý používa na pridelenie oprávnení subjektom role a skupiny. Používateľ tak môže pristupovať ku objektom na základe rolí, ktoré má v oprávnení a tiež na základe svojej skupiny.



Obrázok 1 Modely riadenia prístupu

3.3 Bezpečnostné protokoly

Integrácia služieb z rôznych systémov je koncepčne podobná integrácii služieb v rámci jedného systému. Rozdielne požiadavky však nakoniec vedú k návrhu špecifického riešenia. Ide hlavne o rozdiely v bezpečnostných protokoloch, ich flexibilite a bezpečnostných funkcionalitách, ktoré vyžadujú interakcie týchto služieb, spravovaných v rámci rozdielnych administratívnych domén. V distribuovaných systémoch navyše narastá dôležitosť definovania a štandardizovania interakcií medzi službami, formátmi správ a ich obsahom. Adresovanie týchto problémov pomocou uzavretých a individuálnych riešení je nákladovo neefektívne a neposkytuje takmer žiadne možnosti flexibilného rozširovania funkcionalít a integrácie s ďalšími službami v budúcnosti. Okrem toho individuálne riešenia nie je možné opätovne aplikovať v inom prostredí. Z týchto dôvodov je bežné spoliehať sa na štandardizované bezpečnostné protokoly. Na obr.2 [32] je uvedených niekoľko protokolov, používaných v súčasnosti na autentifikáciu a autorizáciu používateľa do systému. Ich analýza je podrobnejšie opísaná v dizertačnej práci (kap.3).

Bezpečnostné riešenia aplikované na služby so vzájomne integrovanými scenármi sú často navrhované pre špecifický set technológií. Napríklad, niektoré riešenia môžu byť založené na XML alebo Web službách, zatiaľ čo iné môžu používať modernejšie technológie, ako je JSON, práve pre svoje schopnosti kódovať správy a REST architektúru, ktorá dovoľuje vzájomnú integráciu služieb. [32]
Je vhodné, aby boli bezpečnostné riešenia založené na rovnakom type technológií, inak sa tieto riešenia stanú ťažkopádnymi z dôvodu rôznych problémov s interoperabilitou.

Pohľad na obrázok a opísanú analýzu nám formuluje tieto otvorené problémy:

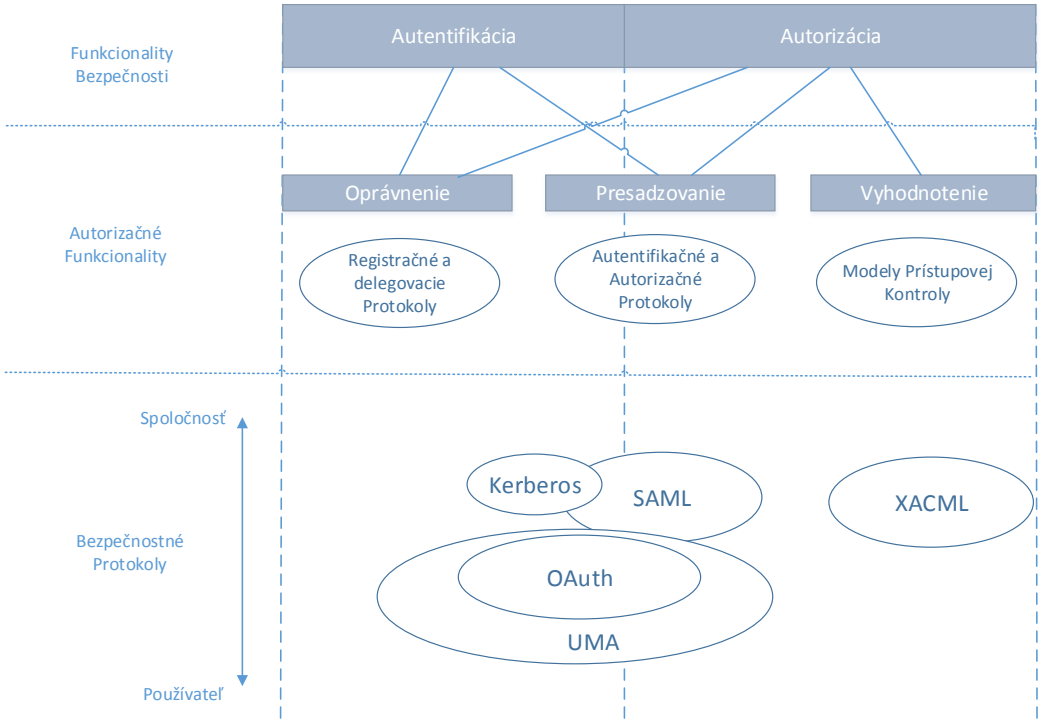
1. Z obrázku je zrejmé, že ani jeden z protokolov nie je univerzálne použiteľný v prípade, že je potrebné pokryť všetky základné autorizačné funkcionality, ktorými sú prideľovanie oprávnení, vyhodnocovanie prichádzajúcich požiadaviek na prístup a následné presadzovanie

pravidiel. Otázka znie, či je potrebná a aj možná vzájomná súčinnosť protokolov alebo je nevyhnutná potreba špecifikácie ďalšieho protokolu.

2. Ďalším rozmerom protokolov je vhodnosť ich použitia vzhľadom na účel nasadenia v prostredí podnikových systémov/aplikáciách alebo aplikáciách pre bežných koncových spotrebiteľov. Štandardizované modely riadenia prístupovú našli svoje uplatnenie práve v podnikových systémoch, zatiaľ čo aplikácie pre koncových spotrebiteľov v oblasti multimediálnej komunikácie využívajú často uzatvorené riešenia, ktoré neumožňujú ich univerzálne použitie, hlavne ak hovoríme o využití viacerých faktorov identifikácie a autentifikácie a taktiež viacúrovňovom riadení prístupu Posledný bod sa zároveň týka ďalšieho problému, ktorý s týmto problémom priamo súvisí.

3. Štandardy neuvažujú nad tým, že klasifikácia obsahu v rámci jednej aplikácie môže byť rozložená do viacerých úrovní, podľa úrovne potrebné zabezpečania poskytovaného obsahu. Ak sa forma klasifikácie obsahu zavedie aj do oblasti špecifikácie protokolu, poskytne sa tým možnosť univerzálneho nasadenia v konkrétnej implementácii.

4. Prostredie používateľa a jeho vzťah s inými používateľmi, resp. ich prítomnosť môže rozhodovanie o udelení prístupu ovplyvniť. Táto problematika úzko súvisí s novými technológiami, označovanými ako Smart Space alebo Internet of Things, ktoré sa v súčasnosti dostávajú do popredia a zásadným spôsobom ovplyvňujú informačnú bezpečnosť a potrebu tieto problémy riešiť.



Obrázok 2 Porovnanie bezpečnostných protokolov

4 Zvolené metódy riešenia

4.1 Návrh algoritmu viacúrovňového riadenia prístupu k informačnému obsahu

Pri návrhu algoritmu sme postupovali na základe nasledovných krokov:

1. Stanovenie vstupných predpokladov, ktoré definujú základné požiadavky na navrhovaný systém.

2. Návrh kontextového diagramu, definujúci vstupné premenné, ktoré musí systém pri rozhodovaní vziať do úvahy pri každej prichádzajúcej požiadavke na prístup.
3. Návrh klasifikácie informačného obsahu do úrovní, na základe stupňa zabezpečenia, čím sa zároveň v ďalšom návrhu naplní požiadavka zavedenia viacerých úrovní riadenia prístupu.
4. Výber vhodných identifikačných a autentifikačných metód/mechanizmov, ktoré budú v návrhu použité.
5. Výber vhodného autorizačného modelu a hierarchiu používateľov systému (tzv. role používateľov)
6. Predpoklady návrhu rozhodovacieho algoritmu, ktoré ohraničujú navrhované riešenie.
7. Samotný návrh rozhodovacieho algoritmu, ktorý narába s definovanými premennými, navrhovanými úrovňami riadenia a rolami používateľov, s využitím stanovených identifikačných a autentifikačných metód. Návrh diagramu musí všetky tieto skutočnosti zachytené v predošlých kapitolách reflektovať.
8. Návrh algoritmu je ukončený vysvetlením navrhovaného systému udeľovania oprávnení pre jednotlivé role používateľov.

Jednotlivé kroky, vrátane celého rozhodovacieho algoritmu sú vysvetlené v dizertačnej práci (kap.5). Zameriame sa na samotný princíp rozhodovacieho algoritmu, resp. jeho časti (krok 7).

Vývojový diagram na obr. 3 zachytáva návrh rozhodovacieho procesu, ktorý sa spustí pri každej požiadavke na prístup ku informačnému obsahu. Vyhodnotenie sa začína vždy od najnižšej úrovne, až po dosiahnutie úrovne, ktorá zodpovedá klasifikácii informačného obsahu, ku ktorému používateľ práve pristupuje. Dôvodom aplikovania takéhoto postupu vyhodnocovania je fakt, že používateľom zvolená aplikácia môže poskytovať informačný obsah na rôznych úrovniach. Používateľ má tak možnosť vstupu do aplikácie bez potreby zložitého overovania jeho identity v prípade, že to úroveň informačného obsahu nepožaduje alebo takúto možnosť aplikácia povoľuje. Tu je dôležité poznamenať, že tento spôsob môže generovať dodatočné požiadavky na strane multimediálneho systému, resp. aplikácie, ktorá tak musí podporovať viacúrovňový prístup, ak je poskytovaný obsah z hľadiska danej klasifikácie možné v aplikácii rozdeliť. Tento prístup nie je v súčasnosti trendom a zvyčajne sa uplatňuje overenie identity používateľa formou, ktorá zodpovedá najvyššej možnej úrovni informačného obsahu, ktorú aplikácie poskytuje, čo do značnej miery obmedzuje používateľa z hľadiska komfortu, ako je napr. potreba zadávania zložitého hesla alebo PIN-u, prípadne ich kombinácia.

Požiadavka na prístup do konkrétnej aplikácie tak vždy začína na úrovni 0. Ak aplikácia obsah tejto úrovne ponúka, môže používateľ k tomuto informačnému obsahu pristúpiť bez toho, aby sa ďalej musel preukázať svoju identitu, ktorá navyše nemusí byť známa, t.j. môže ísť aj o neregistrovaného používateľa.

Predpokladajme, že používateľ pristupuje ku informačnému obsahu klasifikovanému ako úroveň 1. V tomto prípade ide o obsah, pri ktorom je základná identifikácia používateľa žiadaná, za účelom poskytnutia tých informácií, ktoré preferuje alebo ku nim často pristupuje. Ide teda viac o komfort používateľa, ako o ochranu informácií, ku ktorým môže pri tejto úrovni pristupovať akýkoľvek iný používateľ. Na základnú identifikáciu používateľa sa v prvom kroku využije biometrická metóda rozpoznania tváre. Výsledok identifikácie je záležitosťou tzv. externého systému rozpoznávania [59], vykonávajúci porovnanie kamerou zachytenej vzorky s uloženými snímkami, na základe ktorých určí percentuálnu pravdepodobnosť zhody tváre s konkrétnym používateľom. Pravdepodobnosť reprezentuje

jediný číselný údaj, ktorý je vstupom pre vykonanie ďalšej akcie. Ak je pravdepodobnosť dostačujúca, obsah je používateľovi sprístupnený.

Za podmienky, že je pravdepodobnosť nedostačujúca na rozhodnutie, pokračuje sa procesom identifikácie hlasovej charakteristiky používateľa, ktorý je vyzvaný na prečítanie konkrétnej vety napr. prostredníctvom TV obrazovky.

Vstupom pre rozhodovací proces je znovu pravdepodobnosť, reprezentujúca zhodu s uloženou vzorkou hlasu. Tento číselný udaj je rovnako poskytnutý externým rozpoznávacím systémom. [59]

Ak je pravdepodobnosť zhody v prípade tváre alebo hlasu dostatočná, používateľ je v tomto kroku úspešne identifikovaný pre úroveň 1. Konkrétny informačný obsah na základe jeho preferencií sa však prístupní až po vyhodnotení práv, ktoré nasleduje sekvenciou 3 (detailne opísané v 3. časti vývojového diagramu, viď. Dizertačná práca, kap.5.6.2). Ak však ani druhá biometrická metóda nepreukázala dostatočnú zhodu s databázou známych používateľov, využije sa v ďalšom kroku autentifikácia používateľa prostredníctvom hesla, požadovaná pre úroveň 2. /Pokračovanie algoritmu v kap.5.6.2./

Dôležitým krokom v rozhodovaní je typ zariadenia, prostredníctvom ktorého používateľ pristupuje ku žiadanému obsahu. T.j. či ide o mobilné alebo fixné koncové zariadenie. Dôvodom zaradenie tohto parametra v ďalšom rozhodovaní je rozdielny charakter použitia vo vzťahu ku používateľovi. Vo všeobecnosti je možné povedať, že mobilné zriadenie je chápané ako osobné, teda určené predovšetkým konkrétnemu používateľovi. Tento fakt používateľ koncového zariadenia (nie služby) prirodzene berie na vedomie a následne sa tak aj vo vzťahu ku zariadeniu aj správa. T.j. dokáže prispieť k ochrane zneužitia koncového zariadenia vlastnými prostriedkami alebo prostriedkami, ktoré mu mobilné zariadenie ponúka ako štandardnú súčasť používateľského rozhrania operačného systému.

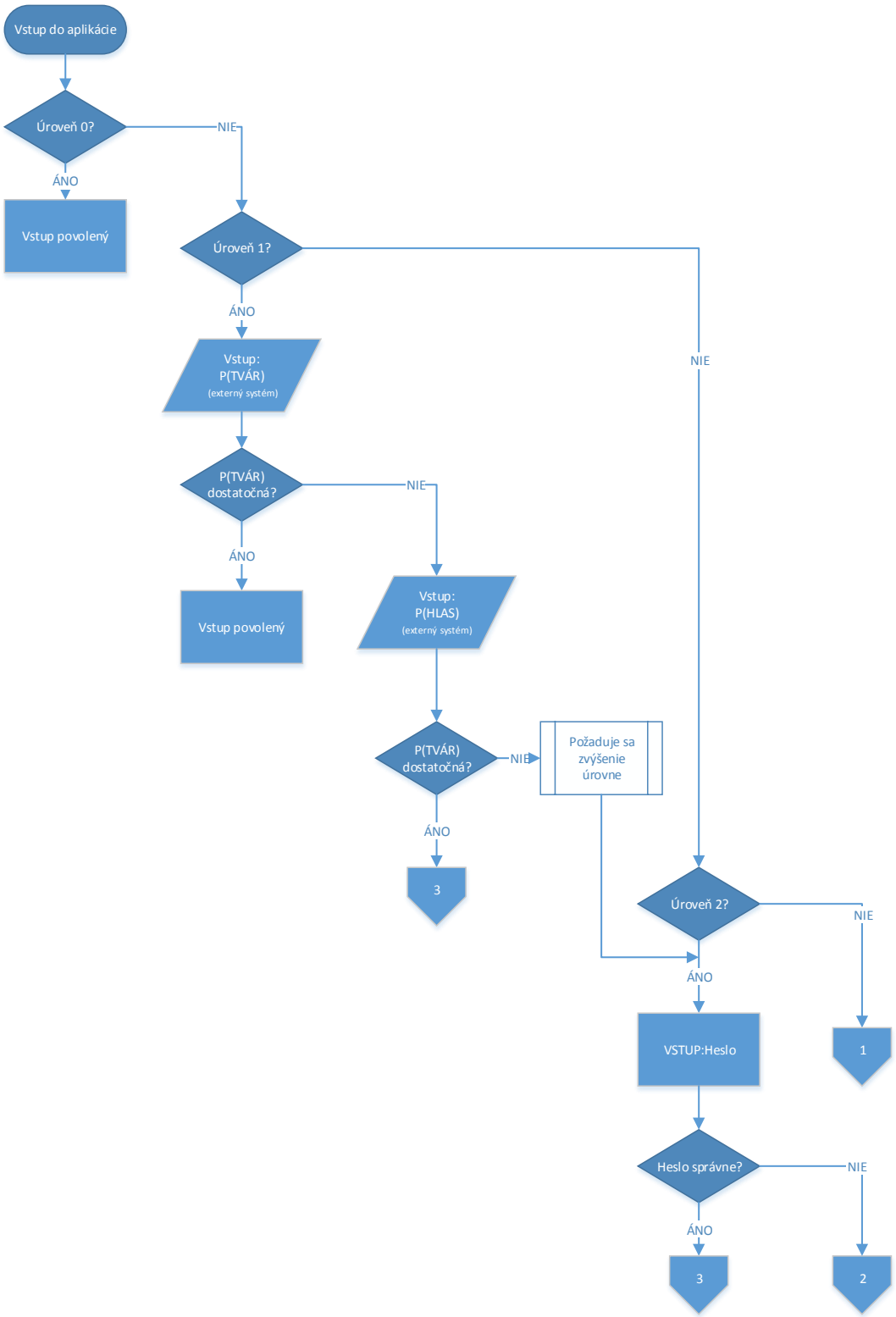
Zároveň je vo všeobecnosti možné povedať, že sprístupnený obsah je na displeji zariadenia zobrazovaný iba jednej osobe. Naproti tomu fixné koncové zariadenie môže byť svojim charakterom používateľovi určené jednému alebo viacerým používateľom. Môže ísť o zariadenie používané skupinou (napr. SmartTV v domácnosti) ale aj o zariadenie používané vo verejných priestoroch (napr. Deskop PC v knižnici). Na základe tohto je možné povedať, že použitie typu prístroja môže ovplyvniť požiadavky na bezpečnosť prístupu ku požadovanému informačnému obsahu.

O tom, aký typ zariadenia a pre ktorú úroveň môže používateľ použiť rozhoduje systémový správca v roli Administrátora systém. Oprávnenie je prideľované vždy iba používateľovi, ktorý figuruje v roli Vlastníka skupiny. Prakticky je tento krok možné vykonať automaticky počas registrácie sa používateľa do systému, pri ktorom dochádza ku prideleniu role Vlastníka skupiny.

Vlastník skupiny môže v rámci svojich kompetencií rozhodovať o tom, aký typ koncového zariadenia môže používať používateľ alebo viacerí používatelia v roli Používateľ dát .

V rozhodovacom procese (časť na obr. 23 v dizertačnej práci, str.62) sa posudzujú obe oprávnenia, nakoľko záleží či ku informačnému obsahu pristupuje už identifikovaný používateľ v roli Vlastníka skupiny alebo hierarchicky nižšie v roli Používateľa dát.

V čase procesu identifikácie používateľa žiadajúceho o prístup v predošlých krokoch sa v priestore pred zariadením môžu objaviť aj iné osoby, ktoré externý systém rozpoznávania pomocou tváre alebo hlasu zachytil a doručil vo forme pravdepodobnosti ako vstup pre ďalšie vyhodnocovanie. Avšak, v reálnom prostredí môže byť problematické ďalšie osoby identifikovať nakoľko sa v priestore pred zariadením iba pohybujú a nepožaduje sa od nich proces, ktorým práve prechádza žiadateľ o vstup. Súčasťou tohto procesu je napríklad na základe zobrazenej výzvy dostatočné priblíženie sa ku kamere rozpoznávajúcej tvár alebo zrozumiteľné vyslovenie definovaných viet.



Obrázok 3 Rozhodovací algoritmus (1.časť)

Uvedený návrh rozhodovacieho procesu nedefinuje konkrétne hodnoty pravdepodobností, na základe ktorých sa ďalej rozhoduje. Tomuto kroku by mohol byť venované rozsiahly výskum matematického modelu, ktorý nie je cieľom práce. Úlohou návrhu je poukázať na možnosti využitia takejto formy tvorby pravidiel v procese rozhodovania a ďalšom návrhu architektúry, ktorá musí zohľadniť komunikačné rozhrania

medzi externým rozpoznávacím systémom, poskytujúcim vstupy pre systém rozhodujúci o aplikovaní konkrétnych pravidiel.

5 Návrh architektúry centralizovaného bezpečnostného systému

Pri návrhu architektúry centralizované bezpečnostného systému sme postupovali na základe nasledovných krokov:

1. Výber vhodného bezpečnostného protokolu alebo protokolov z pohľadu ich funkčných komponentov.
2. Dátový model, definujúci formát každej požiadavky na prístup v kontexte zvoleného protokolu, definujúceho jej výrazový formát.
3. Návrh architektúry Manažéra riadenia prístupu ako centralizovaného systému riadenia vo forme funkčných komponentov, vrátane rozhraní smerom na externé prostredie (vzhľadom na navrhovaný systém).

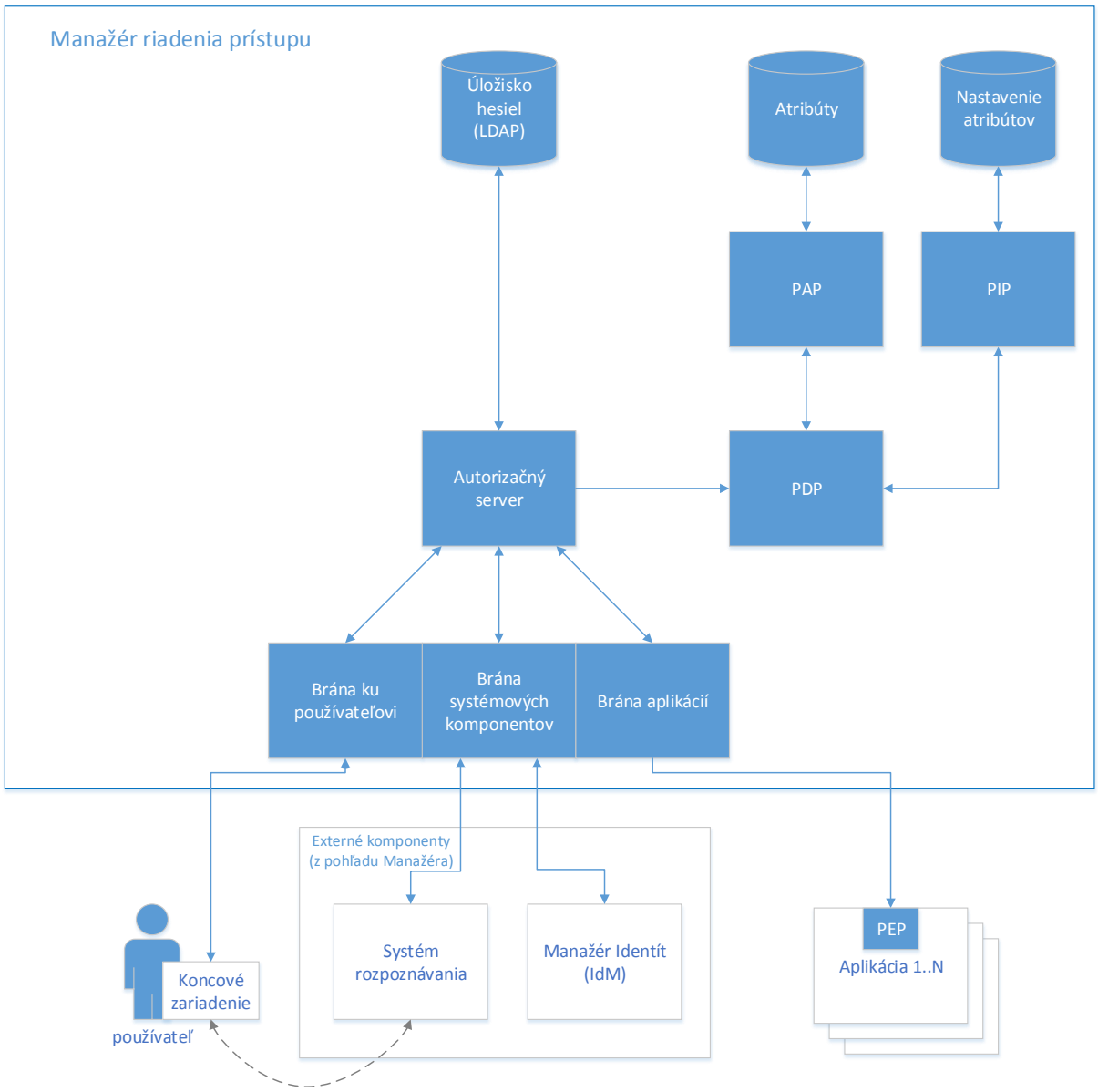
Návrh systému určeného na riadenie prístupu vychádza zo základného predpokladu, ktorým je definovanie centralizovaného rozhodovacieho prvku, riadiaci dodržiavanie pravidiel v multimediálnom prostredí. Centralizácia rozhodovacej logiky dokáže zabezpečiť riadenie prístupu ku obsahu rôznych typov aplikácií, ktoré nevyhnutne nemusia byť izolované v rámci jednej administratívnej domény. Doména môže predstavovať multimediálny systém poskytujúci napr. služby zdieľaného obsahu, pričom tento obsah sa nemusí obmedzovať iba na skupinu používateľov v rámci tohto multimediálneho systému. Cieľom práce nie je zamerať sa na popis vzťahov medzi administratívnymi doménami nakoľko ide o rozsiahlu tému pre ďalší výskum. Dôležité je ale pri návrhu systému riadenia prístupu tento fakt zohľadniť a počítať s modularitou systému a aplikovaním protokolov umožňujúcich takéto vzťahy podporiť. Účelom nasledujúcich podkapitol je návrh blokovej architektúry centrálneho riadenia prístupu ku obsahu aplikácií poskytovaných v rámci jedného multimediálneho systému, označovaný ďalej ako Manažér riadenia prístupu.

Nami navrhovaná architektúra Manažéra riadenia prístupu, uvedená na obr. 4 vychádza z centrálneho komponentu, ktorým je Autorizačný server (ďalej len AS), definovaný podľa UMA. Návrh oproti existujúcej špecifikácii počíta s jeho využitím v rozhodovaní podľa pevne definovaného procesu, nastaveného rozhodovacím algoritmom, opísaným v kap. 5.6.2 dizertačnej práce.
Komponenty prevzaté z XACML štandardu, konkrétne Policy Decission Point (PDP), Policy Administration Point (PAP) a Policy Information Point (PIP) vykonávajú úlohy správy oprávnení a atribútov pre definované role a následný proces rozhodovania, ktorý tieto role môžu v rámci svojich oprávnení ovplyvňovať svojim nastavením, popísané v kap. 5.6.3 dizertačnej práce. Databáza oprávnení musí preto podporovať formát, ktorý umožní tieto oprávnenia uložiť a následne prezentovať. Dôležitá nie je forma uloženia pravidiel, ale ich prezentácia komponentu PAP. Tá spočíva v uložení atribútov do formy tak, aby bolo možné komponentom PAP čítať, aké atribúty sa v procese rozhodovania musia posudzovať. Ako vhodná forma na reprezentáciu týchto nastavení môže slúžiť MySQL databáza, ktorá je dostatočné flexibilná z pohľadu variability tabuľkovej štruktúry.
Čítanie nastavených hodnôt pre jednotlivé atribúty je následne úlohou komponentu PIP.
Databázu určenú na uchovávanie atribútov je rovnako možné postaviť na MySQL formáte. Obe databázy sú však striktne oddelené nakoľko o atribútoch, ktoré sa posudzujú procese posúdenia požiadavky nerozhoduje používateľ. Používateľ má možnosť nastaviť iba ich hodnoty a to podľa možností jeho role v rámci systému.

Autorizačný server je za účelom overovania hesiel integrovaný s databázou typu LDAP, ktorá slúži ako ich úložisko. Tieto databázy môžu v praxi predstavovať externé logické komponenty v informačných systémoch, často postavané práve na protokole LDAP, vhodné práve na účel uchovávania prístupových údajov ako je login a heslo.

Dôležitými funkčnými komponentmi navrhovaného systému sú tzv. brány, ktoré prekladajú formáty prijatých žiadostí a následné odpovede na tieto požiadavky:
Brána ku používateľovi – komunikuje priamo s koncovým zariadením používateľa, resp. aplikáciami vo forme klientov služieb (inštalovaných na koncovom zariadení) multimediálneho systému.
Brána systémových komponentov – zodpovedá za komunikáciu s externými komponentmi v rámci multimediálneho systému, ktoré s Manažérom riadenia prístupu priamo komunikujú. Ide hlavne o komponenty, ktorých výstupy sú v ďalšom procese rozhodovania dôležité.
Rovnako dôležitý je externý komponent, poskytujúci výsledky biometrickej analýzy hlasu, tváre a sietnice vo forme pravdepodobnosti identifikovanej osoby/osôb, tvz. Systém rozpoznávania. Systém rozpoznávania je výsledkom celého tímu kolegov Ústavu telekomunikácií na FEI STU BA, ktorého výsledky boli pre ďalší postup návrhu použité.
Informácia o identite konkrétneho používateľa je uložená v tvz. Manažérovi Identít (IdM), s ktorým Systém rozpoznávania môže spolupracovať priamo (nie je uvedené na obr. 4) alebo prostredníctvom uvažovanej brány. IdM je rovnako komponentom, ktorý je výsledkom PhD výskumu kolegu, ktorý tieto výsledky sumarizuje v dizertačnej práci. [74]
Autorizačný server tak prostredníctvom IdM dostáva úplnú informáciu o pravdepodobnosti identifikácie konkrétneho používateľa/používateľoch alebo informáciu o neznámej osobe/osôb, žiadajúcej o prístup. Manažér riadenia prístupu tieto externé systémy v prípade potreby prostredníctvom brány systémových komponentov oslovuje. Medzi týmito komponentmi a Manažérom riadenia prístupu musí preto existovať vzťah založený na dôvere, nakoľko ide o výmenu veľmi citlivých informácií, ovplyvňujúcich proces rozhodovania.
Budovanie vzťahov na základe PKI modelu a šifrovaného spojenia nie je cieľom tejto práce. Ide však o nevyhnutný predpoklad pre návrh, ovplyvňujúci reťazec dôvery v rozhodovacom procese pre ďalšie štúdium.(viď. konkrétne závery pre ďalší rozvoj)
Brána aplikácií je určená výhradne na komunikáciu s aplikačnými servermi, resp. službami, ktoré sú v rámci multimediálneho systému poskytované pre používateľov. Medzi aplikáciou a Manažérom riadenia prístupu musí rovnako exitovať vzťah založený na dôvere.

Tento návrh poslúži ako základ pre následný návrh protokolu komunikácie medzi Manažérom riadenia prístupu, externými komponentmi, ďalej používateľom (resp. klientskou aplikáciou) a službou (resp. aplikačným serverom).

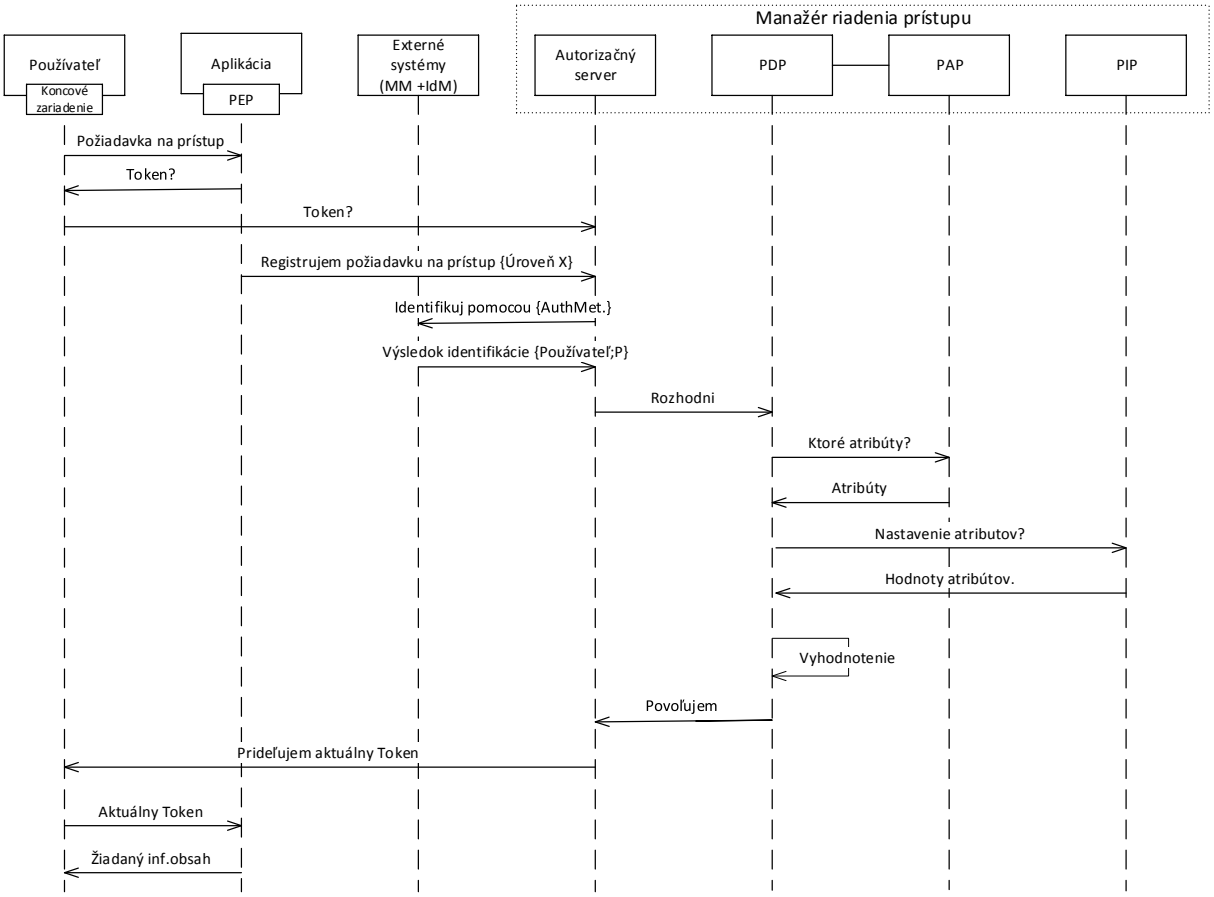


Obrázok 4 Architektúra Manažéra riadenia prístupu

6 Návrh protokolu komunikácie prostredníctvom sekvenčných diagramov

Návrh protokolovej komunikácie je vysvetlený prostredníctvom sekvenčných diagramov, ktoré ozrejmujú navrhovanú protokolovú komunikáciu medzi vnútornými komponentmi Manažéra riadenia prístupu a taktiež aj s entitami multimediálneho systému. Za tieto entity sa považuje používateľ, aplikácia, ku ktorej obsahu používateľ pristupuje a externé systémy, nevyhnutné v procese vyhodnocovania konkrétnej požiadavky. Koncové zariadenie je v uvedených diagramoch chápané ako rozhranie medzi používateľom a aplikáciou. Jednotlivé sekvencie sú opísané jednoduchou formuláciou požiadaviek a odpovedí, s cieľom vysvetliť základný princíp.
Uvedené sekvenčné diagramy zároveň detailnejšie prezentujú navrhovanú interakciu funkčných elementov UMA a XACML.
Sekvenčný diagram obr. 5 znázorňuje príklad povolenia prístupu používateľa ku žiadanému informačnému obsahu konkrétnej aplikácie.

Proces vyhodnocovania sa začína oslovením konkrétnej aplikácie prostredníctvom koncového zariadenia (ďalej len KZ), ktoré daný prístup umožňuje. Bez ohľadu na to, akej úrovne klasifikácie sa informačný obsah týka, požaduje aplikácia prvotné prihlásenie sa používateľa. Keďže používateľ mohol byť v čase požiadavky už úspešne prihlásený do systému a overený na dostatočnej úrovni, zodpovedajúcej žiadanému obsahu, je od neho požadovaný platný token. Týmto si aplikácia overí platnosť prihlásenia a používateľ nie je znovu žiadaný o vykonanie krokov potrebných pre úspešné prihlásenie sa.
V tomto prípade sa však používateľ neprezentuje platným tokenom, ktorý preto potrebuje získať. Za týmto účelom osloví (prostredníctvom klientskej aplikácie na KZ) autorizačný server, ktorý token môže vydať. Autorizačný server (ďalej len AS) sa týmto zároveň dozvie, aký typ zariadenia zamýšľa používateľ používať, t.j. či ide o zriadenie mobilné alebo fixné.
Okrem požiadavky prichádzajúcej z KZ prijíma AS informáciu o požiadavke na prístup aj od konkrétnej aplikácie. Aplikácia v informácii oznamuje o akú úroveň informačného obsahu ide, t.j. na akej úrovni klasifikácie sa žiadaný obsah nachádza.



Obrázok 5 Sekvenčný diagram - kladné vyhodnotenie požiadavky

Na základe týchto vstupov a nastaveného procesu rozhodovania (viď. Rozhodovací algoritmus, kap. 4.1) požiada AS externý systém rozpoznávania o pokus o identifikáciu používateľa prostredníctvom určeného mechanizmu. Zistený výsledok vo forme pravdepodobností osôb práve identifikovaných v priestore pre koncového zariadením je v odpovedi doručený AS. Informácia doplnená o identifikované osoby (nemusí isť nevyhnutne o známych používateľov) je posunutá v rámci Manažéra riadenia prístupu komponentu PDP. PDP sa prostredníctvom PAP dozvie, aké atribúty je potrebné zohľadniť v procese rozhodovania. Po ich zistení kontaktuje PIP, ktorý poskytuje používateľmi

nastavené hodnoty týchto atribútov (podľa privilégií jednotlivých rolí). PDP sa následne rozhoduje o povolení alebo zamietnutí žiadosti o prístup. Predpokladajme, že v tomto príklade bola požiadavka používateľa vyhodnotená kladne a doručená v odpovedi AS. AS na základe rozhodnutia generuje pre používateľa aktuálne platný token, ktorý môže uplatniť v požiadavke na prístup. Doručený token prezentuje používateľ aplikácii očakávajúcej odpoveď na výzvu vo forme prezentovania platného tokenu, na základe čoho mu bude poskytnutý prístup ku požadovanému informačnému obsahu.

V dizertačnej práci (kap.5.8) sú uvedené ďalšie dva príklady, pri ktorých je vidieť správanie sa Manažéra riadenia prístup pri opätovnom posúdení požiadavky s pomocou využitia ďalšej biometrickej metódy a prostredníctvom zadania hesla.

7 Implementácia navrhnutého systému

Výber vhodného multimediálneho systému bol závislý na cieľoch projektu, ktorého úlohou bolo konkrétny multimediálny systém vybudovať. Predpokladom výberu musela byť zároveň časť týkajúca návrhu bezpečnostnej architektúry.
Kapitola stručne opisuje implementáciu Manažéra riadenia prístupu v rámci projektu FP7 s projektovým číslom ICT-2011-7-287848 [61], v rámci ktorého bol začlenený do prostredia architektúry multimediálneho systému HBB-NEXT.

7.1 Manažér riadenia prístupu v prostredí HBB-NEXT WP3 architektúry

Začlenenie navrhovaných funkcionalít Manažéra riadenia prístupu do architektúry SecM (Security Manager) je uvedené v kap. 5.7.3 dizertačnej práce. SecM je výsledkom niekoľkých riešiteľov [85], použitý v bezpečnostnej architektúre HBB-NEXT WP3. Opis všetkých jeho funkcionalít nie je predmetom dizertačnej práce, zameriame sa preto na funkcionality súvisiace s riadením prístupu.
Lepšiu predstavu o intergrácii navrhovaných funkcionalít Manažéra riadenia prístupu do architektúry SecM v kap. 5.7.3 dizertačnej práce je vidieť na obr.6.

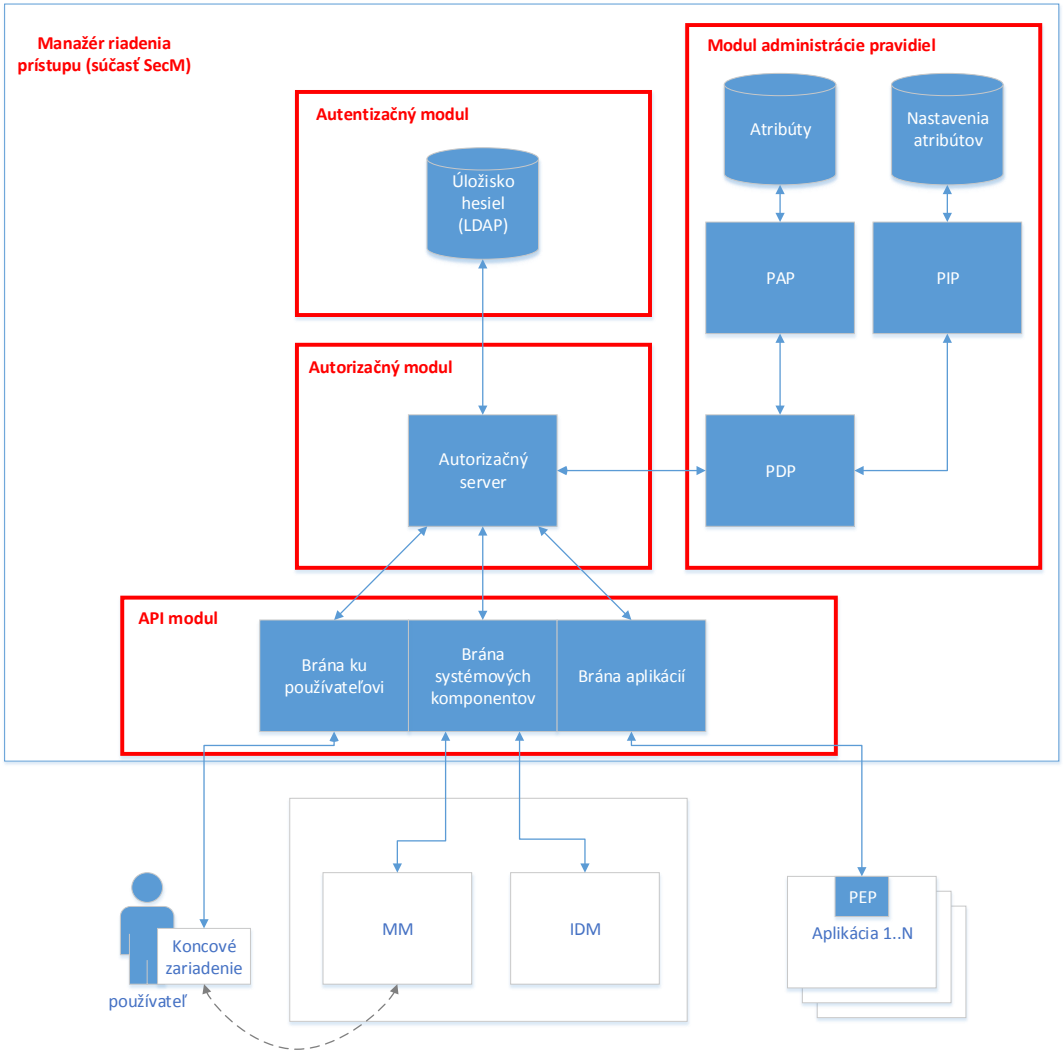
Autorizačný modul – zodpovedný za správu tokenov a ich distribúciu klientom, ktorých predstavuje napríklad web prehliadač alebo aplikácia inštalovaná v používanom koncovom zariadení. Modul zároveň zodpovedá za validáciu pridelených tokenov, vychádzajúc pri tom zo špecifikácie Autorizačného servera podľa UMA protokolu, konkrétne:

- Vydanie RPT (tvz. Requesting Party Token) tokenu
- Verifikácia RPT tokenu
- Registrácia oprávnenia
- Vydanie oprávnenia

Zodpovednosť za delegovanie prístupových oprávnení je ale už súčasťou modulu administrácie pravidiel, ktorý s Autorizačným modulom v rozhodovaní spolupracuje.
V prípade potreby overenia prístupových hesiel alebo PIN kódov, spolupracuje autorizačný modul s autentifikačným modulom.

Autentifikačný modul – je v podstate LDAP databázou, uchovávajúcou prístupové údaje používateľov registrovaných do systému . Modul prostredníctvom ďalšieho API modulu zodpovedá za proces registrácie nového používateľa. Modul zároveň uchováva osobné informácie, ktoré sa počas registrácie zapisujú do systému, nevyhnutné v ďalšom procese obsluhy požiadaviek.

Modul Administrácie Pravidiel – Modul mapuje pravidlá pre účely rozhodovacieho procesu a rozhoduje o povolení alebo zamietnutí prístupu, pracujúci v úlohe RBAC kontrolera. Poskytuje odpovede na žiadosti autorizačnému modulu, ktorý na základe výsledku vydáva platný token.
Ústredným komponentom tohto modulu, rovnako ako v prípade architektúry XACML je Policy Decission Point (PDP), rozhodujúci o požiadavkách na povolenie prístupu. Za uchovávanie atribútov jednotlivých pravidiel je zodpovedný Policy Administration Point (PAP), ktorý spolu s Policy Information Point (PIP) uchovávajúcom hodnoty atribútov mapujú podmienky rozhodovania.



Obrázok 6 Začlenenie funkcionalít Manažéra riadenia prístupu do architektúry SecM

Modul API – poskytuje rozhrania na komunikáciu SecM s ostatnými entitami HBB-NEXT domény a koncovým zariadením používateľa. Keďže entity systému môžu mať rozdielne požiadavky na zabezpečené rozhranie, disponuje troma rozdielnymi rozhraniami:

- Systémová brána – rozhranie smerom ku systémovým modulom HBB-NEXT architektúry. Vzhľadom na SecM ide o externé moduly v systéme. Konkrétne, správu identít používateľov IDM (Identity Manager), systém biometrického rozpoznávania MM (Multi-

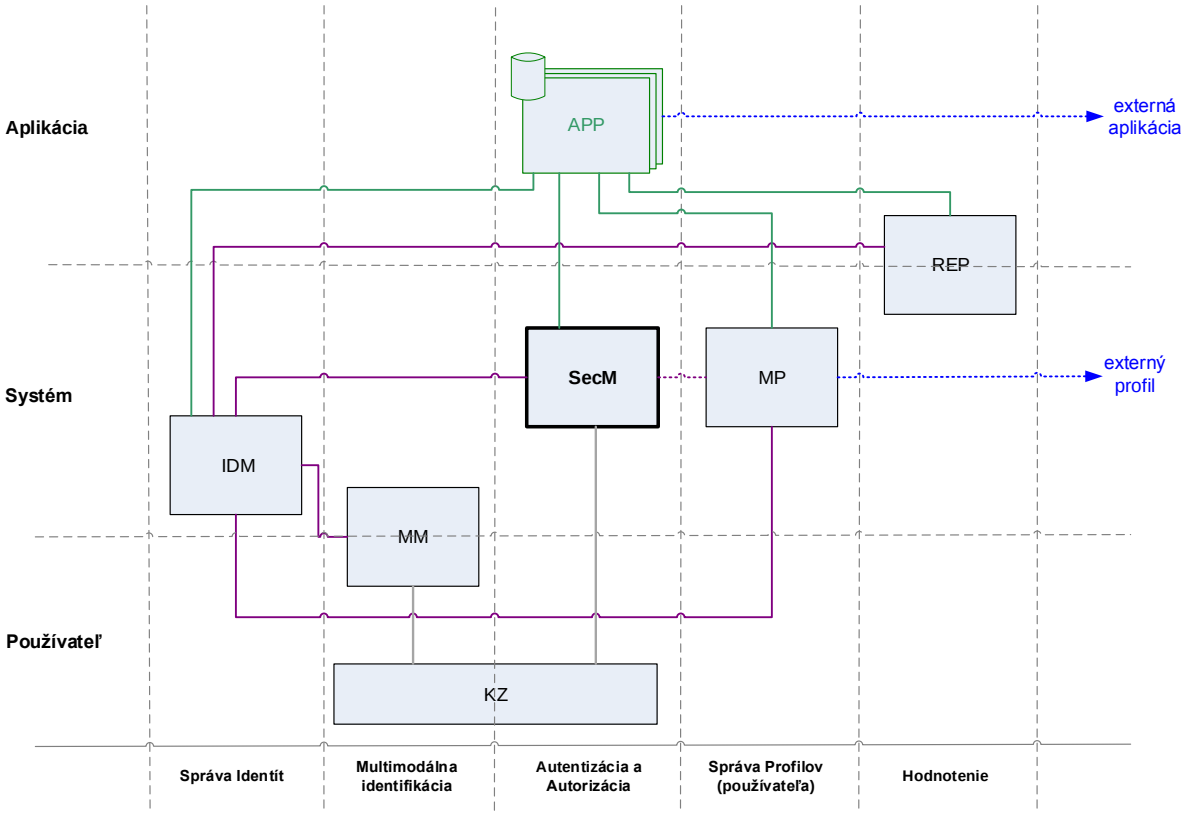
modal), správu používateľských profilov a modul určený na hodnotenie aplikácií používateľmi (Reputation).

- Aplikačná brána – rozhranie slúžiace na komunikáciu s aplikáciami, poskytujúcimi pre používateľa multimediálny obsah. V implementácii sa uvažuje s aplikáciami poskytovanými v rámci jednej HBB-NEXT domény, t.j. aplikácie sú súčasťou jedného multimediálneho systému. V praxi sa však rovnako musí uvažovať aj s externými aplikáciami, poskytovanými tzv. tretími stranami a ich vzájomná interakcia so systémom.
- Terminálová brána – rozhranie určené výhradne na komunikáciu s terminálmi alebo koncovými zariadeniami používateľov systému. Ide o rozhranie, ktoré je vystavené do tvz. nedôveryhodnej zóny, nakoľko používatelia môžu používať akýkoľvek typ koncového zariadenia a ako prenosové prostredie internet.

Modul záznamu udalostí – slúži na záznam a uchovávanie všetkých akcií, vykonaných SecM, ukladajúci zároveň históriu všetkých požiadaviek na prístup. Modul v súčasnosti neanalyzuje správanie sa systému alebo používateľov v doméne, čo môže byť pre riadenie pravidiel v budúcnosti veľmi dôležité. Ako jediný z modulov neposkytuje obojsmernú interakciu s ďalšími modulmi.

7.2 Vzťah SecM s entitami systému HBB-NEXT

Úlohu pracovnej skupiny WP3 v projekte HBB-NEXT bol návrh bezpečnostnej architektúry, pozostávajúci z niekoľkých entít / subsystémov, dôležitých aj z pohľadu riadenia prístupu ku aplikáciám a ich obsahu. [68] Vzťah SecM s ďalšími entitami bezpečnostnej architektúry je uvedený na obr. 7.



Obrázok 7 Klasifikácia komponentov bezpečnostnej architektúry a ich vzťah

SecM <-> IDM
IDM (Identity management) zodpovedá za správu identít všetkých používateľov v rámci HBB-NEXT domény. Keďže SecM nemá znalosť o tom, aký používateľ alebo používatelia môžu prostredníctvom konkrétneho koncového zariadenia pristupovať do systému, požiada o list aktívnych používateľov IdM. V PIP profile SecM je udržiavaná iba hodnota typu zariadenia, prostredníctvom ktorého môže používateľ do systému vstupovať, nie jeho ID číslo.
SecM komunikuje s IdM aj v prípade potreby získania výsledkov biometrickej identifikácie a verifikácie v konkrétnom čase, keďže MM modul nemá so SecM priamy vzťah. Dôvodom tohto kroku je normalizácia výsledkov z MM.

SecM <-> PM
V súčasnosti je časť profilu používateľa uložený v IdM, ktorý má s Manažérom profilov priamy vzťah. Ich interakcia je detailne opísaná v [68]. Ide o plánovanú funkcionalitu, ktorej cieľom je zlúčiť hodnoty o uložených atribútoch pravidiel súvisiacich s používateľom v PIP profile s ostatnými údajmi do jednej databázy.

SecM <-> APP
Základným predpokladom v prípade bezpečnostných požiadaviek na aplikáciu je pri každej žiadosti o prístup do jej obsahu žiadať o rozhodnutie SecM. Keďže v návrhu sú použité elementy XACML architektúry, musí aplikácia spĺňať požiadavky kladené na PEP Policy Enforcement Point), ktorý je spravidla súčasťou služby, poskytujúcej prístup ku obsahu.
Registrácia používateľa do systému ale aj aplikácie je rovnako veľmi dôležitá, v implementácii však nie je tento krok analyzovaný, nakoľko ide o ďalšiu komplexnú tému.

SecM <-> KZ
Koncové zariadenie (KZ) používateľa alebo inak Terminál, ktorý reprezentuje stranu používateľa. Z hľadiska implementácie reprezentuje časť systému, na ktorom je inštalovaná aplikácia-klient, komunikujúca s aplikáciou-server (APP). Klient zohráva v komunikácii SecM úlohu žiadateľa o token, ktorý neposkytuje serverová strana aplikácie, ale Autorizačný modul SecM.
Problematika bezpečnostných požiadaviek na KZ je veľmi široká. Ide o zariadenie, ktoré môže byť pripojené do systému prostredníctvom internetu, čím vznikajú dodatočné nároky na zabezpečenie komunikačných kanálov a distribúciu certifikátov. Táto téma je však mimo rozsahu tejto práce, čiastočne analyzovaná v [84].

7.3 Smart AppStore

V rámci projektu HBB-NEXT bol predstavený nový model appstore, ktorého zámerom bolo priniesť koncept distribúcie aplikácií na rôzne typy koncových zariadení, nezávisle od ich typu. V kontraste klasicky chápaných appstore, zameraných na špecifický segment ide o možnosť inštalácie vybraných aplikácií na mobilný telefón, tablet a SmartTV bez ohľadu na výrobcu zariadenia, pod názvom Smart AppStore.

Okrem iného sa rovnako aj tradičné chápané smartstore zameriavajú na bezpečnosť v oblasti prevencie proti inštalácii malware aplikácií a zamedzenia prístupu neautentifikovaným používateľom, avšak často za cenu obmedzenia používateľského komfortu. Smart AppStore predstavil v tejto oblasti nové funkcionality v podobe [72]:

- využitia biometrie pri identifikácii a autentifikácii používateľa,
- riadenia prístupu na viacerých úrovniach,

- centralizovanej správy identít,

hodnotenia aplikácií podľa preferencií používateľa.

Manažér riadenia prístupu, ktorý je v rámci HBB-NEXT platformy integrálnou súčasťou aplikácie Smart AppStore, zohráva svoju úlohu pri prvých dvoch funkcionalitách, uvedených na predošlej strane. V texte je uvádzaný ako Security Manager (SM).

Úlohu spracovateľa biometrických dát a poskytovateľa pravdepodobnosti identifikácie používateľa prostredníctvom hlasu a tváre plnil multimodálny systém (MM), ktorého výstup bol použitý (okrem iného) aj pre účely rozhodovania SM. Okrem podpory v oblasti rozhodovania bol využitý aj na rozpoznávanie giest používateľov pri ovládaní v prostredí SmartAppStore.

Manažment identít (Identity management) bol v prípade Smart AppStore určený na správu identít registrovaných používateľov, vrátane vzťahov medzi nimi. Pre SM zabezpečoval zároveň normalizáciu výsledkov pravdepodobností, získavaných v pravidelných intervaloch z MM tak, aby poskytol pre potreby SM jediný výsledok o identifikácii konkrétnych používateľa/používateľov v stanovenom čase, určený pre ďalšie rozhodovanie SM.

Uvedená trojica podporných systémov v HBB-NEXT doméne je v tomto prípade súčasťou jedného celku, označovaného ako IDSM.

Ďalším subsystémom, pracujúcim nezávisle od IDSM je modul určený na poskytovanie zoznamu hodnotenia aplikácií podľa preferencií používateľa. V texte je ďalej označovaný ako REP modul (Reputation). Výstup REP modulu je využívaný priamo požívateľom, pri rozhodovaní sa o inštalácii konkrétnej aplikácie zo Smart AppStore.

Ako bolo spomenuté vyššie, Smart Appstore predstavuje v rámci HBB-NEXT aplikáciu, ktorá je v podstate ďalšou entitou HBB-NEXT systému.
Pre demo Smart AppStore prezentované na IBC 2013 v Amsterdame [70] bolo použité koncové zariadenie Samsung SmartTV a senzor Kinect pre platformu Xbox360.

Sekvenčný diagram celej komunikácie je uvedený v dizertačnej práci, kap. 6.4.1.

8 Pôvodné vedecké prínosy

Za pôvodné vedecké prínosy výskumnej práce sa považujú nasledovné výstupy:

- Navrhnutý algoritmus riadenia prístupu podľa klasifikácie informačného obsahu do štyroch úrovní.
  - Algoritmus umožňuje používateľovi komfortný prístup do aplikácie/aplikácií a ich obsahu, bez potreby zložitej autentifikácie sa používateľa, ak to akcia nevyhnutne nepožaduje. Týmto inovatívnym návrhom bola zároveň splnená požiadavka na vytvorenie používateľsky komfortného prístupu ku multimediálnym službám.
  - Algoritmus zároveň umožňuje vytváranie pravidiel, pri ktorých sa do úvahy berie prostredie, v ktorom sa používateľ nachádza počas vykonávania akcie, typ použitého zariadenia a vzťah s ďalšími používateľmi.
  - V procese riadenia prístupu do aplikácie a jej informačnému obsahu sú využité v súčasnosti progresívne možnosti biometrických identifikačných a autentifikačných mechanizmov.

- Navrhnutá architektúra Manažéra riadenia prístupu, ktorý ako centralizovaný systém umožňuje riadenie prístupu ku informačnému obsahu v multimediálnych službách.
  - Špecifikovaním nových funkčných komponentov, tzv. brán bolo možné zaintegrovať Manažéra riadenia prístupu do architektúry príslušných multimediálnych platforiem.
  - Univerzálnosť nasadenia Manažéra riadenia prístupu sme dosiahli akceptovaním existujúcich štandardov.

- Navrhnutý protokol komunikácie medzi internými entitami Manažéra riadenia prístupu, ako aj s externými entitami v rámci multimediálneho systému.
  - Prostredníctvom sekvenčných diagramov sme navrhli interakciu funkčných entít existujúcich protokolov UMA a XACML a to z pohľadu komunikácie medzi internými entitami. Vzájomnou interakciou sme prezentovali možnú spoluprácu pri nahradení chýbajúcich funkcionalít oboch protokolov.
  - Navrhnutý protokol podporuje zároveň podporuje komunikáciu medzi internými a externými entitami. Vzájomná komunikácia externých entít medzi sebou je detailnejšie riešená v rámci [74]

- Implementácia navrhnutého centralizovaného systému riadenia prístupu do vybraného multimediálneho systému.
  - Manažér riadenia prístupu bol v rámci FP7 projektu začlenený do architektúry HBB-NEXT platformy.
  - Úloha Manažéra riadenia prístupu bola prezentovaná v reálnej aplikácii Smart AppStore.

Výsledky tohto výskumu boli prezentované v článku "Smart AppStore: widening the frontiers of smartphone ecosystems" vydanom v karentovanom časopise IEEE Computer. [75].

9 Konkrétne závery pre ďalší rozvoj

V tejto kapitole je uvedených niekoľko tém, ktoré sú návrhom pre ďalší výskum v tejto oblasti:

- Navrhnutý algoritmus opísaný v kap. 5.6.2 v dizertačnej práci využíva ako vstupné dáta výsledky biometrickej identifikácie a verifikácie vo forme pravdepodobností. Vetvenie podmienok na základe konkrétnej hodnoty je však potrebné stanoviť matematicky. Matematický model, ktorý by mal počítať s chybovosťou pri jednotlivých metódach môže byť predmetom ďalšieho výskumu do budúcnosti.
- Keďže Manažér riadenia prístupu uplatňuje rozhodnutia o povolení alebo zamietnutí prístupu aj na základe informácií, ktoré mu poskytujú externé systémy, musí medzi nimi existovať dôverný vzťah, vrátane zabezpečenia komunikácie medzi nimi. To isté platí aj v prípade komunikácie Manažéra riadenia prístupu s aplikáciou a tiež koncovým zariadením. Táto skutočnosť by mala byť zohľadnená v každej reálnej implementácii.
- V dizertačnej práci sme vychádzali z predpokladu, že používateľ je už v systéme zaregistrovaný. Procesu rozhodovania ale predchádza komplexná registrácia nového používateľa do multimediálneho systému, s ktorým súvisí aj získanie jeho biometrických dát. Tejto téme je venovaná práca [74].
- Komunikácia medzi externými entitami z pohľadu Manažéra riadenia prístupu je predmetom riešenia dizertačných prác kolegov (v štádiu finalizácie). [74] [75].

Zoznam použitej literatúry

[1] B. Reid, Reflections on Some Recent Widespread Computer Break-Ins, Communications of the ACM 30:2, Február 1987.

[2] L.F.Cranor a S.Garfinkel, Security and Usability, O'Reilly, ISBN 0-596-00827-9, August 2005.

[3] J. Saltzer a M.Schroeder, „The Protection of Information in Computer Systems, Proceedings of the IEEE 63:9," 1975.

[4] M. Bishop, Computer Security: Art and Science and Introduction to Computer Security (Addison Wesley).

[5] D.Levický, Kryptografia v informačnej a sieťovej bezpečnosti, Košice: elfa, ISBN 978-80-8086-163-6, 2010.

[6] B. Schneier, Sensible Authentication, ACM Queue 1, 2004.

[7] R. E. Smith, Authentication: From Passwords to Public Keys, Addison Wesley, 2002.

[8] H. Ebbinghaus, Memory: A Contribution to Experimental Psychology, New York: Dover Publications, 1964.

[9] E. Tulving a S. Osler, Effectiveness of Retrieval Cues in Memory for Words, Journal of Experimental Psychology 77, 1968.

[10] M. Eagle a E. Leiter, „Recall and Recognition in Intentional and Incidental Learning," *Journal of Experimental Psychology 68,* 1964.

[11] K. A. Ericsson a W. Kintsch, „Long-Term Working Memory," rev. *Psychological Review 102,* 1995.

[12] D. Povey, „Optimistic Security: A New Access Control Paradigm," rev. *Proceedings of the 1999 Workshop on New Security Paradigms,* ACM Press, 2000.

[13] „Biometric Technology Today," *Tomorrow's Markets,* Máj 2004.

[14] http://www.nist.gov.

[15] I. B. Group, „Comparative biometric testing," http://www.ibgweb.com/reports/public/comparative_biometric_testing.html.

[16] A. McCue, „Is Your Cat a Target for Password-Stealing Hackers?," *Silicon.com,* 11 August 2004.

[17] J. A. Haskett, „Pass-Algorithms: A User Validation Scheme Based on Knowledge of Secret Algorithms," *Communications of the ACM 27,* 1984.

[18] A. Madigan, „Picture Memory - Memory and Cognition: Essays in Honour of Allan Paivio," Erlbaum, 1983.

[19] S. Brostoff a A. Sasse, „Are Passfaces More Usable Than Passwords? A Field Trial Investigation," rev. *Proceedings of HCI, Springer,* 2000.

[20] R. Dhamija a A. Perrig, „Déjà Vu: A User Study Using Images for Authentication," rev. *USENIX, Security Symposium,* 2000.

[21] A. D. Angeli, M. Coutts, L. Coventry a G. I. Johnson, „VIP: A Visual Approach to User Authentication," rev. *AVI (Advanced Visual Interfaces),* 2002.

[22] G. E. Blonder, „Graphical Password," rev. *U.S. Patent 5559961,* 1996.

[23] I. Jermyn, A. Mayer, F. Monrose, M. K. Reuter a A. D. Rubin, „The Design and Analysis of Graphical Passwords," rev. *SENIX, Security Symposium,* 2000.

[24] „http://www.rsasecurity.com".

[25] ITU-T Y.2720, Y.2702, X.811.

[26] J. R. Vacca, Computer and Information Security Handbook, Morgan Kaufmann, ISBN 978-0-12-374354-1, 2009.

[27] S. Harris, Mike Meyers' CISSP Certification Passport, McGraw-Hill Osborne Media, ISBN 0072225785, 2002.

[28] U. E. Gattiker, The Information Security Dictionary, KLUWER ACADEMICPUBLISHERS, ISBN 1-4020-7927-3, 2004.

[29] R. Housley, W. Ford, W. Polk a D. Solo, RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, IETF Network Working Group, The Internet Society, Január 1999.

[30] A. O. Freier, P. Karlton a P. C. Kocher, The SSL Protocol Version 3.0, IETF Transport Layer Security Working Group, November 1996.

[31] T. Dierks a C. Allen, RFC 2246, The TLS Protocol Version 1.0, IETF Network Working Group, Január 1999.

[32] D. Cabarkapa, „Authorization Architecture for SWoT," AALTO UNIVERSITY, Espoo, Fínsko, August 2013.

[33] A. Whitten a J. D. Tygar, „Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," rev. *USENIX Security Symposium*, 1999.

[34] P. Gutmann, „Plug-and-Play PKI: A PKI Your Mother Can Use," rev. *USENIX Security Symposium*, 2003.

[35] „http://en.wikipedia.org/wiki/Identity_management".

[36] C. Neuman, T. Yu, S. Hartman a K. Raeburn, RFC 4120, The Kerberos Network Authentication Service (V5), Network Working Group, Júl 2005.

[37] M. Benantar, „Access Control Systems: Security, Identity Management and Trust Models," Springer ISBN 9780387277165, Jún 2006.

[38] K. Wierenga, E. Lear a S. Josefsson, RFC 6595, A Simple Authentication and Security Layer (SASL) and GSS-API Mechanism for the Security Assertion Markup Language (SAML), IETF Internet Engineering Task Force, Apríl 2012.

[39] S. Cantor, J. Kemp, R. Philpott a E. Maler, Assertions and protocols for the OASIS security assertion markup language (SAML) v2.0, OASIS, http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf, Marec 2005.

[40] N. Ragouzis, J. Hughes, R. Philpott, E. Maler, P. Madsen a T. Scavo, Security assertion markup language (SAML) v2.0 technical overview, OASIS, Marec 2008.

[41] T. Dierks a E. Rescorla, RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2, Network Working Group, August 2008.

[42] T. Moses, eXtensible Access Control Markup Language (XACML) Version 2.0, OASIS, Február 2005.

[43] E. Hammer-Lahav, RFC 5849, The OAuth 1.0 protocol, IETF Internet Engineering Task Force, Apríl 2010.

[44] D. Hardt a D. Recordon, RFC 6749, The OAuth 2.0 authorization framework, IETF Internet Engineering Task Force, Október 2012.

[45] T. Hardjono, User-managed access (UMA) pro_le of OAuth 2.0, Internet-Draft (draft-hardjono-oauth-umacore-07b), Január 2013.

[46] M. P. Machulak, L. Moren a A. v. Moorsel, „Design and implementation of user-anaged access framework for web 2.0 applications," rev. *5th International Workshop*

on Middleware for Service Oriented Computing, New York, ACM, ISBN 978-1-4503-0452-8, 2010.

[47] User managed access work group, http://kantarainitiative.org/groups/user-managed-access-work-group/.

[48] „http://awareness.freeband.nl/“.

[49] „http://gaia.cs.uiuc.edu/“.

[50] „http://www.sensei-project.eu/“.

[51] D 3.5 - Security and Accounting for SENSEI, www.ict-sensei.org/index.php?option=com_chronocontact&chronoformname=SENSEI_WP3_D3.5.

[52] O.Lábaj, „Písomná práca ku dizertačnej skúške - Bezpečnosť multimediálnych služieb v prostredí konvergovaných komunikačných technológií,“ FEI STU BA, Bratislava, Jún 2011.

[53] „http://www.ericsson.com/uxblog/2012/04/a-social-web-of-things/“.

[54] „http://en.wikipedia.org/wiki/Smart-M3“.

[55] J. Kim, G. Boulous, J. Yackovich, C. Beckel a D. Mosse, „Seamless Integration of Heterogeneous Devices and Access Control in Smart Homes,“ Bosch Research and Technology Center, Pittsburgh, USA, 2012.

[56] „https://xively.com/“.

[57] R. Courtland, „ Radiation Monitoring in Japan Goes DIY, http://spectrum.ieee.org/tech-talk/energy/environment/radiation-monitoring-in-japan-goes-diy,“ IEEE Spectrum, 2011.

[58] „http://www.axiomatics.com/axiomatics-policy-server.html“.

[59] G. Rozinaj, J.Kacur a P.Podhradsky, „Integration of Multimedia Signal Processing Methods into Multimodal Interface and Network Applications - IMUROSA,“ VEGA 1/0708/13, 2013-2015.

[60] T.Hardjono, „User-managed access (UMA) profile of OAuth 2.0, draft-hardjono-oauth-umacore-07b,“ Kantara Initiative, Január 2013.

[61] HBB-NEXT project, (STREP) Small or medium-scale focused, FP7-ICT-2011-7, 2011-2014.

[62] Technická špecifikácia TS 102 796, Sofia Antipolis: ETSI, 2012.

[63] HbbTV, „https://www.hbbtv.org/pages/hbbtv_association/organisation_of_hbbtv.php“.

[64] HBB-NEXT, „http://www.hbb-next.eu/“.

[65] D6.1.1 - Initial Version of the HBB-NEXT System Architecture, http://www.hbb-next.eu/documents/HBB-NEXT_D6%20.1%20.1.pdf, Jún 2012.

[66] D2.2 - System, Service, and User Requirements, http://www.hbb-next.eu/documents/HBB-NEXT_D2.2.pdf, Marec 2012.

[67] ANALYSIS: State of The Art on Identity, Security and Trust, http://www.hbb-next.eu/documents/HBB-NEXT_D3%201.pdf, Marec 2012.

[68] DESIGN AND PROTOCOL (High Level Architecture): User ID, Profile, Application Reputation Framework, http://www.hbb-next.eu/documents/HBB-NEXT_D3.2.pdf, September 2012.

[69] T.Kokolevsky, „Diplomová práca - Rozšírenie platformy Hybrid Broadcast Broadband TV,“ Bratislava, 2013.

[70] „HBB-NEXT at the International Broadcasting Convention (IBC) 2013,

http://www.hbb-next.eu/publications/poster_IBC_2013_applications.pdf," Amsterdam, September 2013.

[71] Final HBB-NEXT System Architecture, http://www.hbb-next.eu/documents/HBB-NEXT_D6.1.3.pdf, Marec 2014.

[72] ETSI, Hybrid Broadcast Broadband TV, Sophia Antipolis Cedex FRANCE, 06/2010.

[73] HBB-NEXT project, (STREP) Small or medium-scale focused research, 2011.

[74] S. Schumann, „Dizertačná práca - Next generation identity management to enable converged personalized services", Bratislava 2015.

[75] J. Matejka, „Dizertačná práca – Bezpečnosť NGN sietí ", Bratislava 2015.

Zoznam publikácií autora

Vedecké práce v zahraničných karentovaných časopisoch

[75] Gómez Mármol, F., Rozinaj, G., Schumann, S., Lábaj, O., Kačur, J.: Smart AppStore: widening the frontiers of smartphone ecosystems. IEEE Computer, Jún 2014.

Knižné publikácie

[76] Podhradský, P., Mikóczy, E., Matejka, J., Lábaj, O., Tomek, R., Ďungel, M., Kotuliak, I.: Practical Experience with New Services and Applications Supported by NGN. In: Handbook of Research on Mobile Multimedia. - Hershey : IGI Global, 2008, ISBN 978-1-60566-046-2, Vol. 2, s.628-645 [1,852 AH]

[77] Podhradský, P., Mikóczy, E., Matejka, J., Lábaj, O., Tomek, R., Ďungel, M., Kotuliak, I.: Practical Experience with New Services and Applications Supported by NGN, Chapter in Handbook of Research on Mobile Multimedia Second Edition, Eds. by Ismail Khalil Ibrahim, Idea Group Publishing, 2008, ISBN: 978-1-60566-046-2, 2008, New York, USA

[78] Mikóczy, E., Podhradský, P., Matejka, J., Lábaj, O., Tomek, R., Kadlic, R., Schumann, S., Massner, S., Ďungel, M., Kotuliak, I., Mikula, J.: NGN Protocols, 2008, LdV projekt Train2Cert

Publikované príspevky na zahraničných vedeckých konferenciách

[79] Podhradský, P., Mikóczy, E., Matejka, J., Lábaj, O., Kotuliak, I.: NGN platform architecture and its adaptation to the evolution trends, In: 14th International Conference on systems, Signals and Image Processing IWSSIP 2007 and 6th EURASIP Conference Focused on Speech and Image Processing, Multimedia Communications and Services EC-SIPMCS 2007, 27. – 30. June 2007, Maribor, Slovinsko

[80] Lábaj, O., P. Podhradský, P.Truchly, E. Mikóczy: Exception violations in Voice over IP telephony, In: 50th International Symposium ELMAR-2008, 10-13 September 2008, Zadar, Chorvátsko

[81] Schumann, S., Lábaj, O., Podhradský, P.: Building complex Voice over IP (VoIP) applications based on open-source, 51th International Symposium ELMAR-2009, September 2009, Zadar, Chorvátsko

[82] Golha, M., Lábaj, O., Schumann, S., Podhradský, P.: Seamless WiFi-roaming in IMS network, 51th International Symposium ELMAR-2009, September 2010, Zadar, Croatia

[83] Matejka, J., Lábaj, O., Londák, J., Podhradský, P.: VoIP Protection Techniques, 52nd International Symposium ELMAR-2010, September 2010, Zadar, Chorvátsko

[84] Kadlic, R., Lábaj, O., Podhradský, P.: E/M-learning in IMS based NGN environment, 17th International Conference on Systems, Signals and Image Processing IWSSIP 2010, 2010, Florencia, Taliansko

[85] Matejka, J., Lábaj, O., Šupala, D., Kokolevský, T., Podhradský, P.: Security Aspects of Hybrid Broadband Broadcast Communication, 55th International Symposium ELMAR-2013, September 2013, Zadar, Chorvátsko

Publikované príspevky na domácich vedeckých konferenciách

[86] Lábaj, O., Podhradský, P., Kotuliak, I.: Zabezpečenie komunikácie NGN testovacej platormy, Elektrotechnika a informatika 2007, konferencia v rámci medzinárodného veľtrhu ELOSYS, 16. – 19. október 2007, Trenčín

Resumé

Title: Multi-level access control in multimedia applications

Keywords: identification, verification, authentication, authorization model, access control, rules, biometrics, security manager, architecture

A key task of the thesis is to address options for the management of access to information content based on its classification and the level of security required. An important part of the work is to design evaluation of access requests to the applications for different users in terms of their mutual relationship, user's environment and user-device facilities that can directly affect decision making process. The proposed solution for multi-level access control is combining several authentication factors based on defined rules.
The work focuses on the architecture and integration of the security system in the environment of platforms providing multimedia services for ordinary users, in order to present a possible solution for comfort access to applications and their content.
As a part of the proposed solution a protocol draft for communication among various functional components during access request is presented in this work. The protocol is explained through the sequence diagrams.
The proposed Access control manager as a part of Security Manager of the HBB-NEXT multimedia system was proven within the Smart AppStore application.