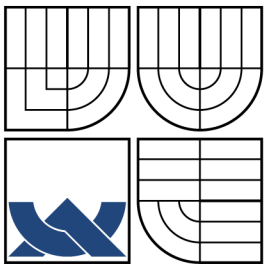
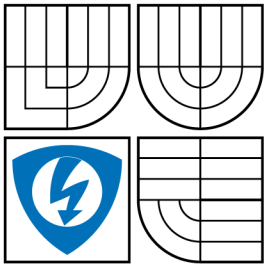


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND
COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

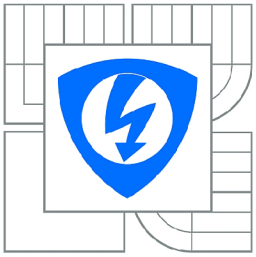
UŽITÍ PROTOKOLU ACP PRO PLATEBNÍ SYSTÉMY

BAKALÁRSKA PRÁCA
BACHELOR'S THESIS

AUTOR PRÁCE — ANDREJ NOVÁK
AUTHOR

VEDÚCI PRÁCE — Ing. IVO STRAŠIL
SUPERVISOR

BRNO 2013



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Andrej Novák	***ID:***	139287
Ročník:	3	***Akademický rok:***	2012/2013

NÁZEV TÉMATU:

Užití protokolu ACP pro platební systémy

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je vypracovat scénáře užití protokolu ACP v platebních systémech. Součástí práce bude zhodnocení vytvořených scénářů z hlediska bezpečnosti, univerzality a datové náročnosti.

DOPORUČENÁ LITERATURA:

[1] BURDA, K. Univerzální rámec pro řízení přístupu v počítačových sítích. Elektrorevue - Internetový časopis (http://www.elektrorevue.cz), 2011, roč. 2011, č. 9, s. 1-6. ISSN: 1213- 1539.
[2] BURDA, K.; LEŽÁK, P. Aplikace univerzálního rámce řízení přístupu. Elektrorevue - Internetový časopis (http://www.elektrorevue.cz), 2012, roč. 2012, č. 28, s. 1-5. ISSN: 1213- 1539.
[3] ČÍKA, P. Protokol pro zabezpečení elektronických transakcí - SET. Elektrorevue - Internetový časopis (http://www.elektrorevue.cz), 2006, roč. 2006, č. 45, s. 1 (s.)ISSN: 1213- 1539.

Termín zadání:	11.2.2013	***Termín odevzdání:***	5.6.2013

Vedoucí práce: Ing. Ivo Strašil
Konzultanti bakalářské práce:

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

SIX research centre
sensor, information and communication systems

Faculty of Electrical Engineering
and Communication

Brno University of Technology
Purkynova 118, CZ-61200 Brno, Czechia

http://www.six.feec.vutbr.cz

Výzkum popsaný v této diplomové práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

2007–13
OP Výzkum a vývoj pro inovace

ABSTRAKT

Bakalárska práca sa zameriava na protokol pre kryptografické systémy v platobných systémoch vyvinutý na ÚTKO. V práci je zhrnutý momentálny stav vývoja v oblasti systému pre platbu medzi dvoma zariadeniami a v práci bude názorne ukázané ako protokol umožňuje dvojici zariadení v rámci transakcie zjednať požadované aktivity, zjednať autentizačnú metódu, previesť autentizáciu, doručiť prístupové parametre a previesť vyúčtovanie.
Úlohou tejto práce je vypracovať scenáre užitia protokolu ACP v platobnom systéme a zhodnotiť ich z hľadiska bezpečnosti, dátovej náročnosti a univerzality.

KĽÚČOVÉ SLOVÁ

ACP, AAA, mobilné platby, elektronické platobné systémy

ABSTRACT

Bachelors work focuses on the protocol for the cryptographic systems in payment systems developed for ÚTKO. The work summarizes the current state of the system for payment between the two devices, and work will show how protocol allows for pair of devices within the required activities to negotiate the transaction, negotiate the authentication method, make an authentication, deliver the access parameters and transfer statement. The purpose of this work is to develop scenarios inclusive protocol ACP in the payment system and evaluate them from the aspect of safety, performance data and universality.

KEYWORDS

ACP, AAA, mobile payments, electronic payment systems

NOVÁK, Andrej *Užití protokolu ACP pro platební systémy*: bakalárska práca. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2013. 47 s. Vedúci práce bol Ing. Ivo Strašil

PREHLÁSENIE

Prehlasujem, že som svoju bakalársku prácu na tému „Užití protokolu ACP pro platební systémy“ vypracoval samostatne pod vedením vedúceho bakalárskej práce, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej bakalárskej práce ďalej prehlasujem, že v súvislosti s vytvorením tejto bakalárskej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/nebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona č. 121/2000 Sb., o právu autorském, o právoch súvisejúcich s právom autorským a o zmeně niektorých zákonov (autorský zákon), vo znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhé, hlavy VI. diel 4 Trestného zákoníka č. 40/2009 Sb.

Brno ....

(podpis autora)

POĎAKOVANIE

Rád by som poďakoval vedúcemu bakalárskej práce pánovi Ing. Ivovi Strašilovi, za odborné vedenie, konzultácie, trpezlivosť a podnetné návrhy k práci.

Brno ....

(podpis autora)

OBSAH

ZOZNAM OBRÁZKOV

ÚVOD

Dôsledkom vývoja ľudstva na tejto planéte je tiež nepochybne prirodzený pokrok v oblasti obchodovania. Myšlienka platenia za tovar a služby elektronickou cestou nie je už dnes nič nové ani prevratné. Všade okolo nás môžeme vidieť veľa obchodných transakcií, pri ktorých je aspoň časť z tohto procesu prenášaná elektronicky. Dnes je už celkom bežný nákup platobnou kartou či sťahovanie aplikácií z portálov. Od prelomu rokov sedemdesiatych a osemesiatych, kedy vznikali prvé návrhy toho, ako využívať počítačové siete v oblasti bankovej, išiel vývoj v tomto odbore neskutočne dopredu a jednou z hlavných príčin je určite rozvoj internetu ako globálneho komunikačného média.

Počas pár rokov sa elektronické platby ukázali ako nový a relatívne úspešný spôsob nakupovania tovaru a služieb. Každou metódou nakupovania, v ktorej sa platba uskutočňuje za pomoci elektronickej reprezentácie platobných nástrojov - obvykle cez sieťové spojenie, môžeme nazvať elektronickou platbou. Elektronické platby sú uchovávané a zasielané v elektronickej podobe, ktorá prináša nové problémy vývojárom bezpečných platobných systémov. Rovnako ako sa vyvíja oblasť elektronických platieb, menia sa tiež bezpečnostné požiadavky, ktoré na tieto platby máme.

Presun peňazí elektronickou cestou cez zabezpečené finančné siete je logicky bezpečná (ak neberieme do úvahy útoky z vnútra siete), ale platobná operácia vedená otvorenými sieťami ako je internet, vytvára nové možnosti pre potenciálnych zlodejov. Preto sa musela vytvoriť taká architektúra platobných systémov, ktorá je bezpečná voči všetkým možným útokom a v tejto súvislosti tiež vznikajú rôzne bezpečnostné štandardy, ktoré sa bankové inštitúcie a firmy snažia implementovať do svojich počítačových a platobných systémov. Je prirodzené, že útoky na tieto platobné systémy sú a budú rôzne a tiež rozdielne úspešné. Z tohto dôvodu nemôžeme prehlásiť žiadny model za úplne bezpečný.

V dnešnej dobe sa spolu s rozšifrovaním tzv. „múdrych“ mobilných telefónov s operačným systémom a podporou technologie NFC, viacero typov platobných terminálov a rôznych druhov koncových zariadení, opäť dostáva do popredia otázka technického riešenia a zabezpečenia platobných systémov.

Čo sa týka sveta počítačov, v tejto oblasti už boli vyvinuté a aplikované platobné systémy, v prvom rade systémy typu *Paypal*[5] a systém *3D Secure*, no v oblasti mobilných platobných systémov sa zatiaľ nepodarilo nájsť vhodný univerzálny systém, ktorý by spĺňal bezpečnostné požiadavky, bol by podporovaný čo najväčším množstvom poskytovateľov výrobkov a služieb a bol by ľahko prístupný pre zákazníkov, ktorí užívajú rôzne typy prístrojov a rôzne siete rôznych operátorov.

Kedže dnes je už koncových zariadení pomerne veľa, je problém vytvoriť systém, ktorý by podporoval ich vzájomnú komunikáciu. Môžme začať od mobilných tele-

fónov, ktoré nemajú operačný systém alebo jednoduchých POS terminálov po viac moderné prístroje, napríklad najnovšie kompatibilné počítače, mobily typu smartphone s viacjadrovými procesormi a iné. Aj keď sa môže zdať, že mnohé z týchto prístrojov sú bezpečné, spoľahlivé a technicky bezpečné, nemusia spĺňať požiadavky kompatibility a univerzálnosti. Väčšinou majú tieto prístroje systémy, ktoré boli vytvárané pre daný prístroj bez myšlienky kompatibility s inými druhmi prístrojov, aj inej značky, bez potenciálu ďalšej rozšíriteľnosti.

Táto práca sa teda zaoberá návrhom scenárov pre bezpečné elektronické platby. Práca je orientovaná na návrh jednotlivých scenárov s prihliadnutím na bezpečnosť, univerzalitu a dátovú náročnosť, pričom sa predpokladá, že prevádzka tohto systému bude aplikovateľná na rôzne hardwarové a komunikačné platformy.

1 PLATOBNÉ SYSTÉMY A ICH PROBLEMATIKA

1.1 Platobné systémy

Implementácia elektronických platieb je odbornou verejnosťou uznávaná ako jedna z najviac rastúcich oblastí v elektronickej komercii, čo si uvedomujú hlavne obchodníci, a snažia sa čo najviac uprednostňovať svoje elektronické platobné systémy. Táto skutočnosť má za následok to, že je na trhu niekoľko riešení a ich počet stále rastie.

Sféra elektronických platieb je veľmi široká a existuje niekoľko rôznych systémov, ktoré medzi sebou súperia o pozíciu lídra a snažia sa pritiahnuť obchodníkov na svoju stranu. Pokiaľ nebude jasne stanovené jedno bezpečné riešenie, ktoré bude dominovať celému trhu, budú tieto platobné modely ako sú šeky, kreditné karty, virtuálne peniaze existovať paralelne vedľa seba.

V súčastnosti by sme našli viacero typov systémov pre platby. V prostredí internetu sú najviac zaužívané systémy ako *3D Secure*, *cardPay* a iné proprietárne systémy. Výhodou dnešných mobilných telefónov a smartphonov je ten fakt, že ich operačné systémy sú schopné používať väčšinu z internetových platobných systémov. Využité môžu byť cez rôzne technológie, napríklad cez SIM Toolkit a samozrejme SMS, NFC, dátový tok, *Bluetooth* a dokonca aj cez hlas. Ďalším zaujímavým systémom je *Google Wallet* od spoločnosti Google. V poslednom rade pripomeniem mikroplatby, kde uvediem typický príklad - SMS lístok.

1.1.1 Všeobecné požiadavky a očakávania

Od elektronických platobných systémov sa predovšetkým očakáva vysoký stupeň zabezpečenia proti krádeži peňažných prostriedkov a podvodom rôzneho druhu, čo je už tradičným záujmom finančných inštitúcií, ktoré sa v tejto oblasti angažujú. A naviac je dôležitým požiadavkom tiež nízka cena vykonávajúcich operácií v týchto platobných systémoch.

Vývojári, ktorí navrhujú platobné systémy, musia brať do úvahy, že dobrý platobný systém je nezávislý na rôznych podporných systémoch (operačných, sieťovo komunikačných a pod.) rovnako ako na počte jeho užívateľov. Jednotlivé platobné transkacie sa musia vykonať kompletne, nie len z časti, a transkacie musia byť nezávislé na sebe. Vždy musí byť možné vrátiť sa do posledného konzistentného stavu v systéme.

Elektronické platobné systémy musia byť pre užívateľa zrozumiteľné a ľahko použiteľné.

1.1.2 Bezpečnostné požiadavky

Manipulácia s peniazmi, ak ide hlavne o manipuláciu pri ktorej nemáme fyzický kontakt a javí sa ako nespoľahlivá, je chúlostivá záležitosť. Preto musíme dorža ť určité bezpečnostné požiadavky na elektronické platobné systémy tak, aby všetky finančné a osobné informácie boli istené a neprišlo tak k odcudzeniu dôverných údajov.

Existujú scenáre - anonymné platby, kde obchodník nemá žiadne informácie o zákazníkovi a tak ho nie je možné žiadnym spôsobom identifikovať. Ale tu sa nám križujú naše záujmy. Na jednej strane ide o dôverné informácie, ale na druhej strane je potreba mať určitý druh potvrdenia platby, aby mal zákazník istotu, že jeho platba prebehla a neprišiel tak o čiastku. Systémy by mali umožňovať refundanciu platieb, ako sa napríklad v dnešnej dobe využíva v systémoch pri platení platobnými kartami, napríklad v bankových systémoch či v systémoch pre spätnú platbu financií zákazníkom, ktorí sa zúčastnili elektronickej aukcie.

1.1.3 Autorizácia, dôvernosť a integrita

Dôvernosť musí zabezpečiť, že neautorizované osoby nemôžu odposluchom komunikácie v sieti zistiť také informácie, akými sú príkazy, platby a účty zákazníka. Takáto vlastnosť sa zaisťuje pomocou kryptografie. Aby sme obmedzili výskyt krádeží a znížila sa tak celková cena spracovania platieb, preveruje sa identita zúčastnených strán autentizáciou. Obchodník si musí byť istý, že zákazník je legitímny užívateľ čísla účtu platnej platobnej karty. Zákazník musí mať možnosť identifikovať obchodníka, s ktorým môže bezpečne elektronicky obchodovať a musí si byť istý, že tento obchodník spolupracuje s finančnou organizáciou, ktorá akceptuje jeho platobnú kartu alebo údaje na platbu potrebné. Autentizácia sa implementuje digitálnymi podpismi a certifikátmi. Zákazník správami reprezentujúcimi platobné transakcie dáva najavo, čo objednáva, svoje personálne dáta a platobné inštrukcie. Obsah správ by sa behom prenosu nemal meniť. Vlastnosť integrity sa normálne implementuje digitálnymi podpismi.

Celistvý platobný systém tiež nedovoľuje, aby sa prevádzali peniaze od užívateľa, ktorý túto akciu neautorizoval. Umožňuje tiež odmietnuť prijatie platby bez súhlasu, aby zabránil podobným činnostiam, ako je napríklad podplácanie. Autorizácia tvorí u známych elektronických platobných systémov najdôležitejšiu zložku v platobnom systéme a môže byť konaná troma spôsobmi:

- *Autorizácia treťou stranou*: overujúcou stranou je typicky banka, ktorá buď zamietne alebo potvrdí transakciu použitím bezpečného vonkajšieho kanála (napr. pošta, telefón). Typické použitie je u objednávok po telefóne či maili, ďalej u platieb typu CNP. Ktokoľvek, kto pozná dáta z kreditnej karty, môže

vyvolať transakciu a zodpovedný užívateľ potom musí túto transakciu potvrdiť alebo naopak povedať, že ide o nepovolenú transakciu. Zvyčajne, ak užívateľ nepodá podnet proti danej transakcii do 90 dní, je automaticky schválená.

- *Heslom*: transakcia chránená heslom požaduje, aby každá správa od autorizovanej strany zahrňovala šifrovanú časť pre kontrolu. Táto časť je vypočítaná pomocou tajného kľúča, ktorý je známy iba autorizujúcej a overujúcej strane.

- *Digitálnym podpisom*: v tomto type autorizácie požaduje overujúca strana digitálny podpis autorizovanej strany. Digitálny podpis zaisťuje nepopierateľnosť pôvodnej správy, pretože iba majiteľ tajného podpisového kľúča sa môže podpísať pod túto správu (resp. podpísať sa môže každý, ale odpovedajúci digitálny podpis majiteľa môže vytvoriť iba ten istý majiteľ, pretože ten je jediný, ktorý ten tajný kľúč pozná).

1.1.4 Funkčné požiadavky

Platobné systémy by mali rozhodne spĺňať určité funkčné požiadavky[11]. V dnešnej dobe smerujeme k čo najväčšej jednoduchosti za predpokladu dodržania parametrov bezpečnosti a flexibility.

- *Flexibilita*: vypracovaný systém by určite nemal byť viazaný na jedno zariadenie. Čím viac prístrojov, ktoré sú schopné platobný systém použiť, tým lepšie. Takže uvažujeme, že platba platobným systémom by mala byť možná odvšadiaľ a z akéhokoľvek zariadenia.

- *Použiteľnosť*: platobný systém by mal byť jednoducho použiteľný. Povinnosť inštalovania softwéru odradzuje zákazníkov od toho, aby platobný systém používali, takže systém musí byť jednoducho implementovaný ako na strane zákazníka, tak na strane predajcu. Tak isto je dôležitá aj jednoduchosť systému, pretože zákazníci ju požadujú. Predajca zase na druhej strane požaduje čo najlacnejšiu implementáciu nového platobného systému za systém, ktorý práve používa.

- *Spoľahlivosť a dostupnosť*: ak počas transakcie dôjde k výpadku systému, systém musí zaistiť aby sa daná transakcia uviedla do pôvodného stavu a aby nedošlo k ujme. Čím vyššia dostupnosť a stálosť systému, tým viac spokojných zákazníkov a predajcov, pretože dôvera je dôležitá.

1.1.5 Univerzálnosť systému

Aby bola komunikácia medzi rôznymi systémami v širokom rozmedzí technologických podmienok, mala by byť kompatibilita platobných systémov založená na štandardoch a otvorených technológiách. Treba počítať s tým, že systém bude komunikovať aj so staršími systémami a mal by byť na to uspôsobený.

1.1.6 Platba kartami prostredníctvom internetu

Čo sa týka platieb kartami prostredníctvom internetu, najbežnejšie a najčastejšie sú platobné systémy, ktoré umožňujú použitie platobných kariet ktoré sú v správe bánk, resp. vydávateľa karty zákazníka.

Autentizácia prebieha takým spôsobom, že pre platbu treba zadať potrebné údaje (v prvom rade samotné číslo karty, pri niektorých platbách sa vyžaduje aj meno majiteľa karty, dátum expirácie karty a CVV2 kód), ktoré sa vzťahujú na konkrétnu platobnú kartu. Takže prioritou tohto systému musí byť ochrana osobných údajov, pretože pri odcudzení, či už formou odposlúchavania alebo zneužitím zo strany obchodníka by bolo možné použiť platobnú kartu aj bez vedomia majiteľa, a prišlo by k ujme.

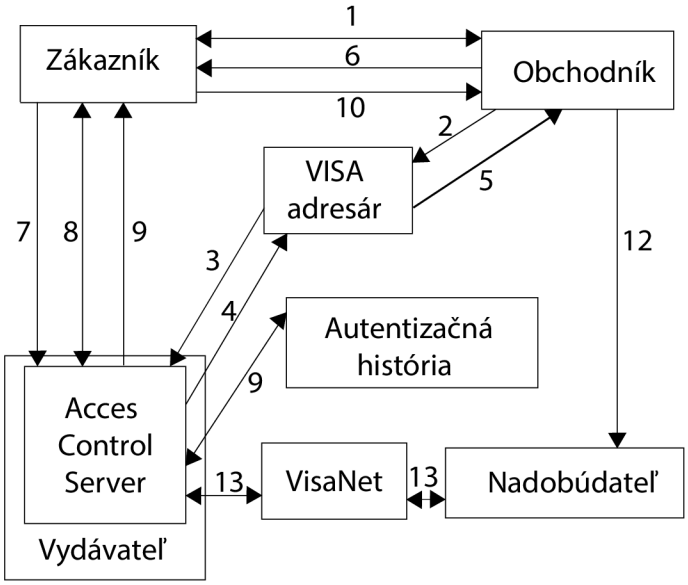
V minulosti viedli vtedajšie platobné systémy k tomu, aby boli vytvorené nové a bezpečnejšie architektúry, pretože vtedajšie systémy boli stavané takým spôsobom, že pri platbe bolo treba zadať požadované údaje, ktoré sa spracovávali priamo na servery obchodníka. Za priekopnícke systémy môžeme považovať *3D Secure* a *SET*.

1.1.7 Architektúra 3D Secure

Visa vyvinula troj-doménový zabezpečený protokol (*3D Secure*) k zvýšeniu bezpečnosti pri vykonávaní elektronických transakcií a snaží sa tak podporovať rast elektronickej komercie. Cieľom je priniesť konkurenčnú výhodu všetkým zúčastneným vďaka isteniu vydávajúcich bánk so schopnosťou autentizovať držiteľa platobných kariet pri on-line transakcii, a teda zníženia pravdepodobnosti podvodného užitia Visa karty a zlepšením transakčných výkonov.

VISA *3D Secure* protokol nasleduje centralizovaný autentizačný prístup, je založený na protokoloch TLS, HTTPS a XML. Vydávateľ karty je v komunikácii s držiteľom karty vďaka jeho prehliadača, kde sa zbierajú autentizačné detaily. Vydávateľ ich následne zvaliduje a pošle späť obchodníkovi ako autentizačnú odpoveď. Službu založenú na tomto protokole si už adaptovala spoločnosť pod menom MasterCard SecureCode a tak isto spoločnosťou JCB International pod menom J/Secure.

Ako prebieha nákup:



Obr. 1.1: Priebeh nákupu pomocou systému *3D Secure*

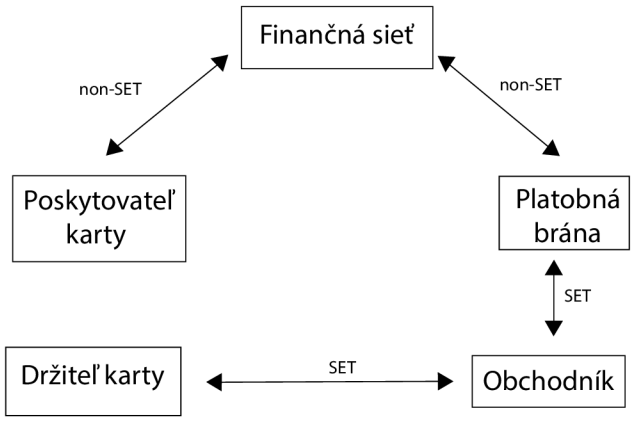
- 1. Ak si držitel VISA karty vybral obchodníka a tovar na jeho webe a rozhodol sa ho zaplatiť pomocou *3D Secure*, musí mu najprv poslať číslo svojej kreditnej karty.
- 2. Obchodníkov plug-in sa informuje o registračnom statuse zákazníka od VISA adresára.
- 3. Ak je číslo kreditnej karty v určitom kartovom rozsahu (definuje VISA), VISA adresár sa informuje o príslušnom ACS, či je číslo karty riadne registrované.
- 4. ACS odpovie adresáru VISA a pošle mu údaje o zákazníkovi.
- 5. VISA adresár prepošle túto odpoveď do obchodníkovho plug-inu.
- 6. Obchodníkov plug-in pošle požiadavok na autentizáciu platiča k ACS pomocou prehliadača zákazníka.
- 7. ACS obdrží požiadavku na autentizáciu.
- 8. ACS autentizuje nakupujúceho pomocou znalosti jeho hesla, potom formátuje autentizačnú odpoveď s príslušnými hodnotami a podpíše ju.
- 9. ACS vráti autentizačnú odpoveď obchodníkovmu plug-inu pomocou užívateľovho prehliadača. ACS pošle vybrané dáta na server autentizačnej histórie pre účely logovania.
- 10. Obchodníkov plug-in obdrží autentizačnú odpoveď.
- 11. Obchodníkov plug-in skontroluje podpis na tieto odpovede.

- 12. Obchodník pokračuje s autorizáciou k platbe u svojej banky.
- 13. Banka obchodníka (nadobúdateľ) autorizuje tento požiadavku banke zákazníka (vydávateľ) pomocou *VisaNetu*.

1.1.8 Architektúra SET

Ako ďalší príklad uvediem platobný systém, ktorý si získal veľkú popularitu, no pri rozšírení už nebol tak úspešný. SET tvorí otvorený štandard pre bezpečné platby platobnými kartami v prostredí internetu a popisuje kryptografické mechanizmy pre dosiahnutie potrebných bezpečnostných vlastností systému. Pri platbe sa v systéme vyskytujú traja účastníci: držiteľ karty, obchodník a platobná brána. Podstatné je, že obchodník nezískava prístup k platobným údajom pre bránu, platobná brána nezískava informácie o obsahu objednávky tovaru.

Rámec protokolu SET bol spočiatku značne obmedzený. Pôvodne bol zamýšlaný len ako platobný protokol. Špecifikačné dokumenty vyjasnili, že protokol môže byť rozširovaný ostatnými stranami pre on-line nakupovanie, zjednávanie ceny, výber platobnej metódy a ostatné funkcie elektronického obchodovania. SET príde na radu až po rozhodnutí zákazníka, čo si kúpi, za koľko a či si zákazník praje platiť kreditnou kartou.



Obr. 1.2: Priebeh platby kreditnou kartou podľa štandardu *SET*

Ako je vidieť z diagramu, SET nie je zamýšlaný ako univerzálny platobný protokol a je obmedzený na platobné karty alebo podobné aplikácie, kde účastníci prevezmú rolu zákazníka, obchodníka alebo poskytovateľa. Neposkytuje smerovanie financií od jedného jedinca k druhému, ale pre uskutočnenie platby sa spolieha na

existujúcu infraštruktúru kreditných kariet. Držiteľ karty uvidí uskutočnené SET transakcie na svojom výpise z účtu vedľa tradičných kartových platieb a poskytovateľ ich uvidí ako rozšírenie bežnej komunikácie medzi jeho obchodnými zákazníkmi.

Aj napriek veľkej popularite nedošlo pri systéme SET k jeho rozšíreniu. Na vine bola jeho prílišná zložitosť špecifikácie. Skutočnosť, že je SET popísaný v troch ťažkých zväzkoch predstavovala značné úsilie pre vytvorenie softwaru a jeho následné testovanie.

Druhou prekážkou pre nasadenie bola potreba hierarchie certifikačných autorít. Znova sa opakoval scenár použitia príliš zložitého softwaru.

1.1.9 Systémy pre mobilné platby

V dnešnej dobe existujú štyri mobilné platby[9]:

- SMS platby
- Direct Mobile Billing (priame platby mobilným telefónom)
- platby s užitím systému NFC
- klasické internetové platby zadané prostredníctvom prehliadača alebo aplikácie na mobilnom telefóne (s použitím platobnej karty alebo internetového platobného systému)

Až na posledný uvedený bod ide o spravidla jednoduché systémy, ktoré sa dajú spravovať jedným obchodníkom alebo jedným operátorom siete. Tieto systémy zvyčajne nespĺňajú bezpečnostné požiadavky, ktoré sú kladené na platobné systémy[8] a ich rozšírenie je tak často obmedzené iba na operácie s menšími čiastkami.

1.1.10 SMS platby

Za SMS platby považujeme také platby, ktoré zadáva zákazník prostredníctvom zaslania SMS správy (tiež USSD alebo MMS správ) na číslo, ktoré obsahuje prémiovú sadzbu poplatkov. Cena za tovar alebo službu je teda účtovaná prostredníctvom mobilného operátora.

Technológia SMS platieb je jednoduchá, ale stále vyžaduje inštaláciu klienstkej aplikácie alebo vyžaduje, aby si užívateľ pamätal presné textové znenie platobných príkazov. Veľkou nevýhodou tohto systému je jeho nízka bezpečnosť a pomalý a nespoľahlivý prenos správ.

1.1.11 Direct Mobile Billing

Direct Mobile Billing je platobná metóda, ktorá sa najviac používa na východe. Zákazník pri platbe v elektronickom obchode požiada o platbu systém, obdrží SMS

správu s jednorázovým heslom a ten zadá spolu s PIN kódom do formulára elektronického obchodu. Systém prevádzkuje mobilný operátor, takže časť s cekovej ceny je účtovaná týmto opeátorom.

1.1.12 Platby s použitím NFC systému

Systém NFC je používaný prevažne v maloobchodných predajoch a pre platby v oblasti dopravy. Tento systém obsahuje značný nedostatok štandardizácie a teda neexistujú vhodné infraštruktúry, konalo sa pomalšie rozširovanie technológie ako priemysel očakával. Väčšina systémov nevyžaduje autentizáciu pomocou PIN kódu. Služby sú účtované buď strhnutím z účtu za mobilný telefón, alebo sa riešia formou predplatenia.

1.1.13 Platobná aplikácia Mobito

Mobito je vcelku nová aplikácia od spoločnosti MOPET CZ, ktorá funguje na báze prepojenia s bankovým účtom. Zákazník má svoj bankový účet priamo zosynchronizovaný. Výhodou je, že sa transakcia vybavuje mimo telefón a teda aj mimo dosah teoretických zlodejov. Ďalšou výhodou aplikácie je, že zariaďuje aj prenos peňazí priamo z telefónu na telefón, takže používatelia nie sú nútení používať internetové portály bánk na prenos, resp. nemusia prísť fyzicky do banky a podpisovať doklady o transakcii. Výrobca si dal záležať na vysokej bezpečnosti. Systém *Mobito* má 7 základných prvkov zabezpečenia:

- peniaze nie sú v *Mobite* „fyzicky“ k dispozícii, sú bezpečne uložené na účtoch partnerských bánk
- *Mobito* je chránené osobným PIN kódom. Tento PIN kód sa používa aj na vstup do systému a aj na jednotlivé platby.
- každý účet *Mobita* je „zviazaný“ s konkrétnym mobilom a SIM kartou, kde bol účet aktivovaný, čo znamená, že aj keby niekto ukradol prihlasovacie údaje, z iného mobilu neuskutoční žiadnu platbu
- *Mobito* sa po určitej dobe nečinnosti automaticky odhlási
- len zákazník si k Mobitu prepája svoj zdroj peňazí, a len on má na *Mobito* portál, kde sú informácie o platbách a financiách, prístup
- *Mobito* komunikuje šifrovaným spôsobom a na to využíva sieťový protokol HTTPS
- dajú sa nastaviť maximálne limity pre platby

1.1.14 Internetové platobné systémy

Internetové platobné systémy, ako je napríklad *PayPal*, vznikli ako nezávislé riešenie nepohodlnej obsluhy a nedostatočnej bezpečnosti systémov pre platbu platobnými kartami pomocu internetu.

1.1.15 PayPal

PayPal je internetový platobný systém, patriaci pod spoločnosť *eBay*. Umožňuje prevody peňazí medzi účtami, ktoré sú identifikované e-mailovými adresami.

PayPal je možné prepojiť s jednou alebo viacerými platobnými kartami, ktoré majú povolené platby na internete. Pri potvrdení platobnej karty v systéme *PayPal* je potrebné zadať informácie o platobnej karte ako sú: typ karty, číslo karty, dátum expirácie, CVV2 kód. *PayPal* si následne z karty strhne malý poplatok, ktorý je pri prvej platbe vrátený ako bonus. Na výpise z účtu, ktorý je spojený s kartou, bude v podrobnostiach platby napísaný štvormiestny kód, ktorý je potrebný zadať do systému *PayPal*, aby prebehlo potvrdenie platobnej karty v systéme. Ak v systéme bude potvrdená karta, tak pri prevodoch cez *PayPal* sa čiastka stiahne z aktuálneho zostatku. V prípade, že na *PayPal* zostatku nebude požadovaná suma, spoločnosť ju stiahne z potvrdenej platobnej karty.

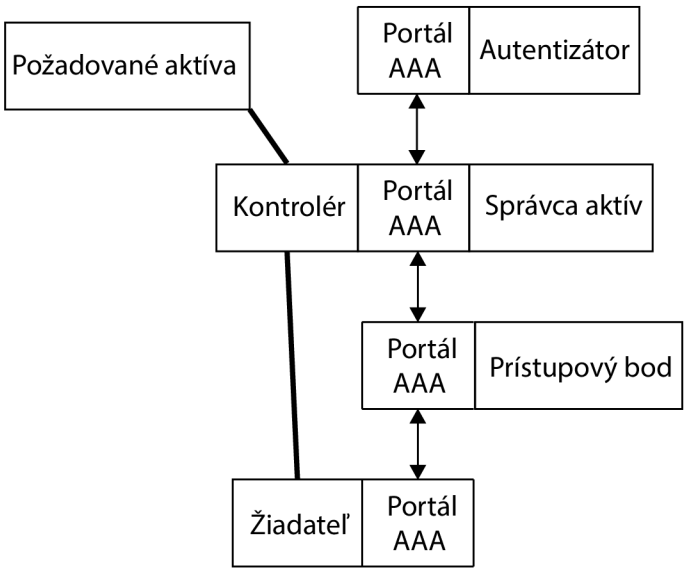
2 REALIZÁCIA PROTOKOLU ACP

V predošlej kapitole som rozpísal základnú problematiku elektronických platobných systémov a uviedol som konkrétne príklady. V tejto kapitole sa zameriam na systémy typu AAA a s tým súvisiaci rozbor a návrh samotného protokolu ACP.

2.1 Systémy typu AAA

V skupine doc. Burdy na Ústave telekomunikácií Vysokého učenia technického v Brne bol v posledných rokoch vyvíjaný mechanizmus univerzálneho rámca autentizácie a autorizácie (URA), ktorý umožňuje konštrukciu lubovoľne zložitých systémov typu AA/AAA.

Základnou motiváciou a dôvodom pre vytvorenie *univerzálneho rámca* je vznikajúca nutnosť zaistenia kompatibility a interoperability medzi systémami typu AAA.



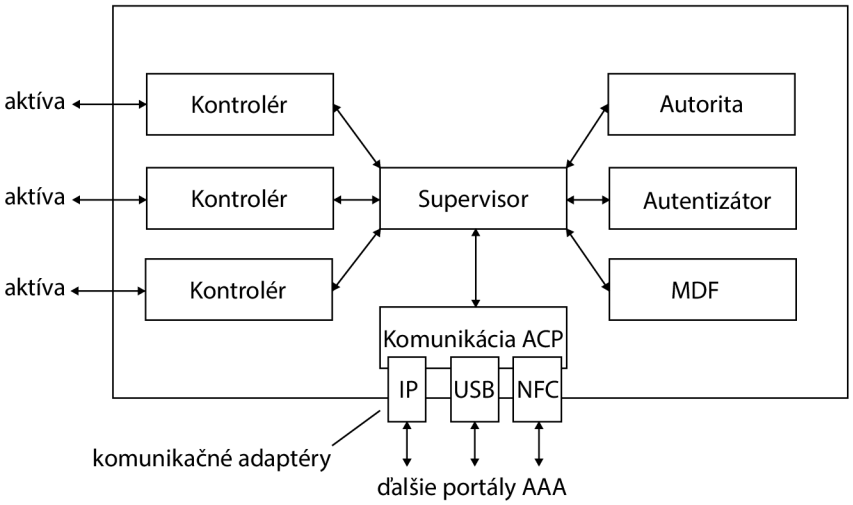
Obr. 2.1: Schéma komunikácie medzi portálmi AAA

V súčastnosti sa stretávame so systémami, ktoré sú založené na viacerých protokoloch a preto nie je zvyčajne ich vzájomná komunikácia možná. Tieto protokoly a systémy sú spravidla prispôsobené na riešenie konkrétnych situácií a tým sa stávajú limitovanými pri ich praktickom rozširovaní.

Preto je úlohou *univerzálneho rámca* využiť celkom odlišný prístup a to taký, že vybavenie každého zariadenia v systéme bude kryptografický modul, ktorý obsahuje systém typu AAA, teda autoritu, kontrolér a autentizátor. Tento modul nazývame portál AAA.

Takým spôsobom príde k tomu, že prebehne aj samotná konfigurácia zariadenia a jeho portálu AAA. Tieto jednotlivé portály AAA sú schopné komunikovať práve protokolom ACP a predávať si vzájomne požiadavky na aktíva, typ autentizácie, vykonanie vlastnej autentizácie a prenos výsledkov autentizácie a autorizácie. A presne takýmto spôsobom môžme dosiahnuť jednotné riadenie prístupu ku všetkým aktivám siete.

Štruktúra portálu AAA (obr. 2.2) je modulárna: základnými prvkami sú koordinačný člen (supervisor), autorita, autentizátor a modul dokazovacích faktorov (MDF). Podľa miestnych aktív sú pripojené jednotlivé moduly kontrolérov aktív. Komunikačný protokol ACP je možno pomocou komunikačných adaptérov prispôsobiť rôznym technológiám nižších vrstiev dátových spojov a siete.



Obr. 2.2: Štruktúra portálu AAA

Pôvodná myšlienka systému bolo aplikovať ho na počítačovú sieť. Keďže systémy s potrebou bezpečnej autentizácie a autorizácie sa neorientujú iba v počítačovej oblasti, nie je dôvod aplikovať systém len v počítačovej oblasti. Systém je preto koncipovaný ako maximálne otvorený. Tomuto princípu sa podriaďuje aj samotný návrh protokolu ACP.

2.2 Základná definícia protokolu ACP

Protokol ACP je binárny protokol aplikačnej vrstvy pre jednotnú implementáciu rôznych metód riadenia prístupu k aktívom počítačových a mobilných zariadení, terminálov a všetkých ostatných prístrojov, ktoré by mali určitým spôsobom komunikovať s ostatnými zariadeniami. Protokol umožňuje dvojici zariadení v rámci transakcie zjednať požadované aktíva, zjednať autentizačnú metódu a následne ju

vykonať, doručiť prístupové parametre a vykonať účtovanie. Jednotlivé transakcie protokolu ACP možno rôznym spôsobom prepájať, čím sa dajú do riadenia prístupu zapojiť aj ďalšie zariadenia.

Jednotlivé sekvencie s práv súvisiace s riadením prístupu k jednému konkrétnemu aktívu sa nazývajú *transakcie*, portál žiadajúceho zariadenia sa nazýva *Žiadateľ (Supplicant)* a portál zariadenia so žiadanými aktívami sa nazýva *Poskytovateľ (Provider)*.

Žiadateľ a *Poskytovateľ* môžu v rámci transakcie komunikovať priamo alebo prostredníctvom iných portálov. Jednotlivé transakcie protokolu ACP možno rôznym spôsobom prepájať, čím sa dajú do riadenia prístupu zapojiť aj portály ďalších sieťových zariadení.

Samotný portál je zostavený z jadra a z voliteľných modulov. Správca sieťového zariadenia môže voľbou modulu nastaviť portál v súlade so svojimi potrebami čo sa týka prístupovej politiky a technických možností zariadenia. Moduly delíme na komunikačné, autentizačné a spravovacie. Komunikačný modul umožňuje komunikáciu medzi portálmi prostredníctvom vybraného prenosového spoja (napríklad spoja typu UDP, TLS, USB, EAPoL a pod.). Autentizačný modul umožňuje realizáciu vybranej autentizačnej metódy (napríklad EAP-MD, EAP-TLS a pod.). Spravovací modul (*Policy module*) umožňuje správcovi zariadenia definovať algoritmus riadenia prístupu k vybranému aktívu daného zariadenia (napríklad k dátumu na pevnom disku). Portál môže byť viac modulov rovnakého typu.

2.2.1 Typy ACP správy

Protokol ACP definuje šesť typov správ, ktoré sa nazývajú: *START*, *OFFER*, *SPECIFICATION*, *REQUEST*, *RESPONSE* a *FINISH*. Pomocou týchto správ sa uskutočňujú transakcie, čo sú vlastne výmeny správ medzi *Žiadateľom* a *Poskytovateľom*, ktorými sa zaisťuje riadenie prístupu *Žiadateľa* ku konkrétnemu aktívu *Poskytovateľa*.

Priebeh transakcie teda pozostáva z nasledujúcich fází:

- zahájenie transakcie (správa *START*)
- zjednanie parametrov transakcie (správy *OFFER* a *SPECIFICATION*)
- autentizácia (správy *REQUEST* a *RESPONSE*)
- ukončenie transakcie (správa *FINISH*)

Počas inicializácie medzi *Žiadateľom* a *Poskytovateľom* sa buduje vzájomné spojenie. V ďalšej fáze sa dohadujú parametre transakcie, zväčša ide o žiadané aktíva a typ autentizácie. Vo fáze autentizácie sa overuje identita *Žiadateľa* a poprípade aj identita *Poskytovateľa*. V poslednej fáze transakcie príde k prenosu už samotného aktíva alebo prístupových parametrov (napríklad schválenie či zamietnutie prístupu,

pridelená IP adresa a pod.). V tejto fáze sa tiež ruší vzájomné spojenie medzi *Žiadateľom* a *Poskytovateľom*.

Správu *START* odosiela vždy *Žiadateľ*. Na základe tejto správy sa buduje vzájomné spojenie medzi *Žiadateľom* a *Poskytovateľom*. Na základe potrebných údajov a údajov v správe *START* môže daný portál zistiť, ktorému ďalšiemu portálu a ktorým spojom má správu *START* predať. Takýmto spôsobom sa postupne vybuduje prenosová cesta medzi *Žiadateľom* a *Poskytovateľom*. S príchodom správy *START* každý zúčastnený portál danú transakciu zeregistruje a určí hodnotu pre spoj k ďalšiemu portálu. Všetky ostatné správy danej transakcie sú prenášané rovnakou cestou, ktorou bola prenášaná správa *START*.

Čo sa týka správy *OFFER*, je prvá z dvojice správ, kotré slúžia na zjednanie parametrov. Správu *OFFER* odosiela vždy *Poskytovateľ*, ktorý touto správou ponúka hodnotu nejakého parametra transakcie alebo sa na hodnotu daného parametra pýta.

Správa *SPECIFICATION* je druhou správou z dvojice správ fázi zjednávania parametrov. Odosiela ju vždy *Žiadateľ*, ako povinnú reakciu na správu typu *OFFER*. *Žiadateľ* v tejto správe zasiela hodnotu vybraného parametra transkacie, alebo sa na parameter pýta.

Fázu zjednávania parametrov transakcie tvorí výmena správ typu *OFFER* a *SPECIFICATION*. Týchto výmien dvojíc správ *OFFER-SPECIFICATION* môže nastať viac, pokiaľ sa hodnoty jednotlivých parametrov zjednávajú postupne. Fáza zjednania parametrov môže byť v transakcii vynechaná ak pripadá v úvahu jediná hodnota príslušných parametrov, alebo pokiaľ *Žiadateľ* uvedie korektné hodnoty parametra transakcie už v správe typu *START*.

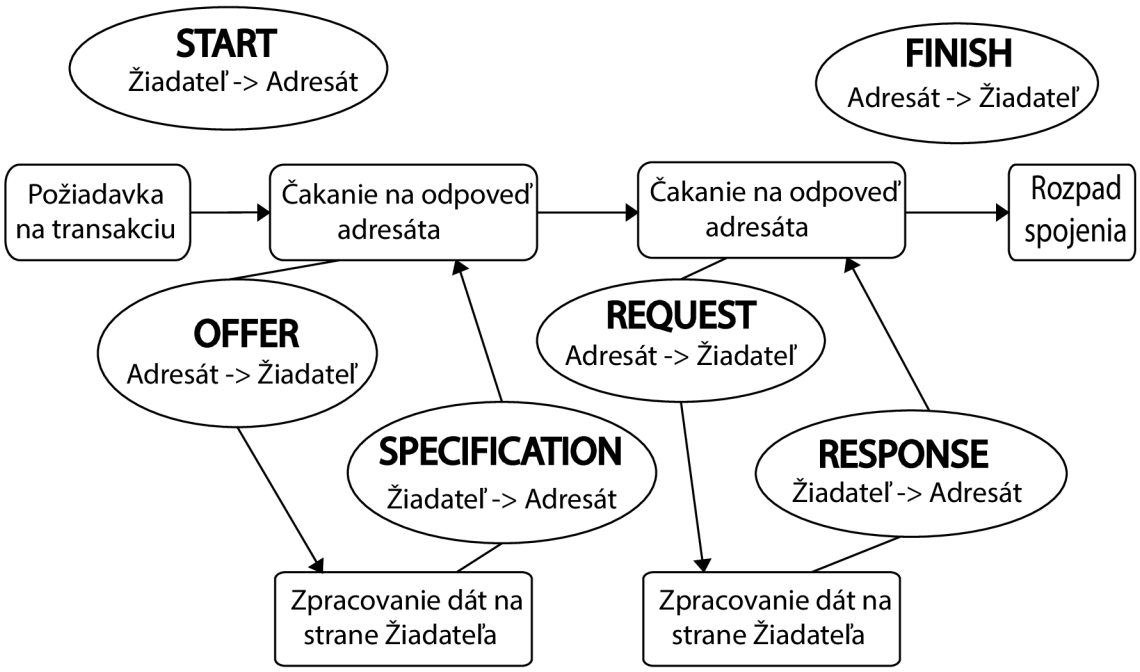
Správa typu *REQUEST* je prvá z dvojice správ slúžiacich pre autentizáciu. Odosiela ju vždy *Poskytovateľ*. Správa obsahuje dáta potrebné na vykonanie autentizácie.

Druhou z dvojice správ pre fázu autentizácie je správa typu *RESPONSE*. Odosiela ju vždy *Žiadateľ* ako povinnú reakciu na správu typu *REQUEST*. Podobne ako to je u správy typu *REQUEST*, aj táto správa obsahuje dáta potrebné na vykonanie autentizácie.

Takže fázu autentizácie tvoria správy typu *REQUEST* a *RESPONSE*. Podľa typu konajúcej autentizácie môže nastať k viacerým výmenám správ *REQUEST-RESPONSE*.

Správu *FINISH* odosiela vždy *Poskytovateľ*. Správa obsahuje buď samotné aktívum, alebo prístupové parametre (schválenie/zamietnutie prístupu, pridelená IP adresa a pod.). Správa typu *FINISH* ukončuje transakciu a ruší vzájomné spojenie medzi *Žiadateľom* a *Poskytovateľom*.

Obrázok 2.3 znázorňuje vyššie popísaný priebeh komunikácie za použitia správ protokolu ACP.



Obr. 2.3: Základná fáza komunikácie s použitím protokolu ACP

Protokol je dvojstranný. Zložitejšie transakcie sú riešené ako zreťazenie viacerých transakcií alebo sú riešené vložením transakcie, kedy jedna z komnunikujúcich strán získa potrebné dáta pre uskutočnenie požadovanej transakcie.

3 VYUŽITIE ACP PROTOKOLU V PLATOBNÝCH SYSTÉMOCH

3.1 Požadované vlastnosti scenára

Jednotlivé scenáre, ktoré som vypracoval, zhodnotím z hľadiska bezpečnosti, univerzality a dátovej náročnosti. Aby to bolo možné, nahliadnem do problematiky všetkých týchto parametrov.

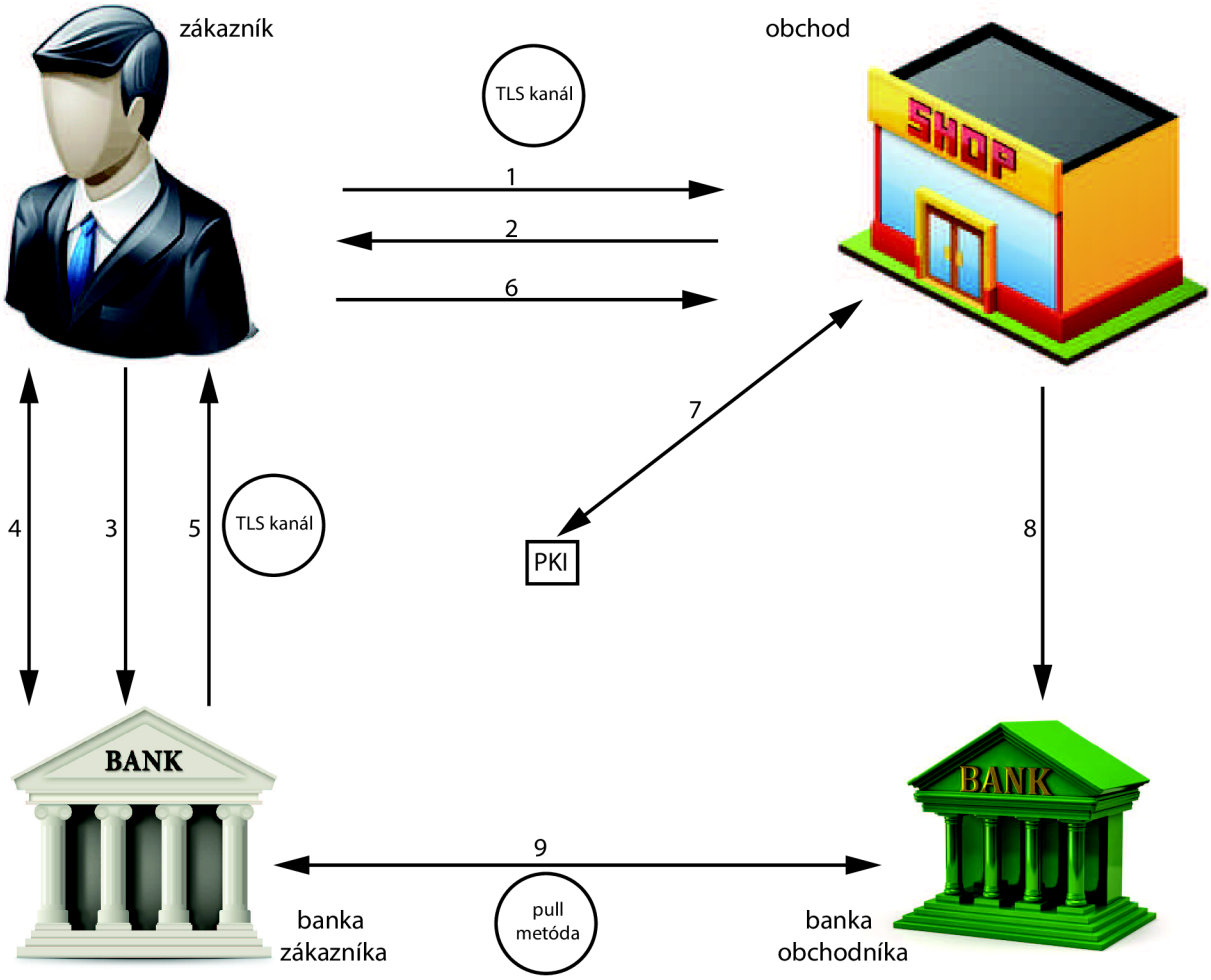
3.1.1 Štandardná platba online

Aby sme mohli bližšie nahliadnuť do problematiky užitia ACP protokolu v platobnom systéme, mali by sme najprv poznať, ako prebieha platobný systém bez použitia ACP protokolu. Tento scenár vychádza z dnešných stávajúcich riešení.

1. v prvom bode dôjde k samostatnej objednávke, pri ktorej sú udané informácie a podmienky transakcie
2. obchodník vystaví formu elektronických peňazí pre zákazníka
3. zákazník udáva požiadavok svojej banke - o aký účet sa jedná, výška čiastky a pod.
4. priebeh samotnej autentizácie
5. banka zasiela podrobnú formu elektronických peňazí - účet, čiastka, adresa banky
6. forma elektronických peňazí spolu s podrobnosťami sa predávajú obchodníkovi
7. obchodník následne overuje, či sa jedná o legitímny požiadavok
8. obchodník komunikuje so svojou bankou, pričom prichádza k realizácii služby
9. nasleduje vyrovnanie medzi bankami

Formu elektronických peňazí môžeme považovať za súbor informácií udávajúci o aký účet zákazníka sa jedná, výšku čiastky trankakcie a identifikátor samotnej platby.

Výraz metóda pull označuje takú platbu, pri ktorej sa účtuje priamo z účtu zákazníka na účet priamo obchodníkovi. Sú aj iné metódy, napríklad metóda push je taký postup, kedy banka zaplatí za zákazníka transakciu, a následne si účtuje financie od zákazníka.



Obr. 3.1: Štandardná platba online

3.1.2 Bezpečnosť

Dôvernosť správ prenášaných protokolom ACP môže byť zaistená externe alebo interne. Externá ochrana spočíva v použití zabezpečených spojov či šifrovaných spojov - kanál TLS. Interná ochrana špočíva v kryptografickom zabezpečení jednotlivých správ. Pri komunikácii prípade uvažujeme, kto je nútený poskytnúť svoje dôverné informácie druhej strane, poprípade či sa zaobíde transakcia bez výmeny týchto údajov.

Externá ochrana

Protokol TLS (Transport Layer Security) a jeho predchodca SSL (Secure Sockets Layer) sú kryptografické protokoly poskytujúce možnosť zabezpečenej komunikácie v sieti Internet (služby ako WWW, elektronická pošta...) a dalšie dátove prenosy. Medzi TLS a SSL protkolom sú menšie rozdiely, ale v zásade sú rovnaké.[12]

Protokol TLS teda umožňuje aplikáciám komunikovať po sieti spôsobom, ktorý zabraňuje odposlúchavaniu či falšovaniu správ.

TLS zahrňuje tri základné fázy:

- dohodu účastníkov na podporovaných algoritmoch
- výmenu kľúčov založenú na šifrovaní s verejným kľúčom a autentizáciu z certifikátov
- šifrovanie prevádzky symetrickou šifrou

Prenos TLS tunelom je potreba zahrnúť primárne tam, kde prichádza k prenosu dôverných informácií, ktorých odcudzenie by mohlo viesť k porušeniu súkromia či k možnosti ohrozenia majetku. Z praktického hľadiska uvažujeme samotný prenos formy elektronických peňazí, kde sú uvedené dôverné informácie ako číslo účtu, identifikácia, podpis banky a iné dôverné informácie.

Interná ochrana

Interná ochrana spočíva v autonómnom kryptografickom zabezpečení správ protokolu ACP. Toto zabezpečenie je založené na kryptografických primitívoch z povinnej sady protokolu TLS:

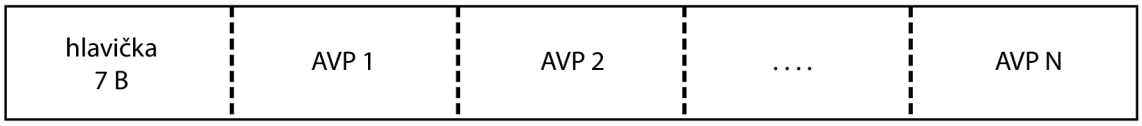
- INIT (SAVP): obsahuje inicializačný vektor
- PMS (SAVP): obsahuje premaster secret, vo vhodnom kontexte môže obsahovať kľúč šifry AES
- CERT (LAVP): obsahuje certifikát podľa štandrardu X.509
- AES (LAVP): obsahuje dáta, ktoré sú šifrované šifrou AES v režime CBC pomocou kľúča dĺžky 128 b
- ENC (CAVP): obsahuje AVP INIT následované AVP AES. INIT obsahuje inicializačný vektor potrebný k dešifrovaniu dát z AVP AES.
- HMAC (SAVP): obsahuje autentizačný kód reťazca všetkých AVP, ktoré sa v danom MAC nachádzajú pred ním, určuje sa pomocou funkcie SHA1
- MAC (CAVP): obsahuje reťazec AVP, ktorý je nasledovaný koncovým AVP typu HMAC, ktorý obsahuje autentizačný kód reťazca AVP
- RSA (LAVP): obsahuje reťazec AVP, ktorý je zašifrovaný šifrou RSA
- PSS (LAVP): obsahuje digitálny podpis reťazca všetkých AVP, ktoré sa v danom SIG nachádzajú pred ním

3.1.3 Dátová náročnosť

Pri riešení dátovej náročnosti uvažujeme protokol ACP podľa jeho štruktúry. V jednotlivých scenároch je používaný protokol ACP na prenos elektronickej formy peňazí, autentizácie, overenie a prenos samotných dát, pričom každá z týchto správ

má svoju štruktúru a veľkosť, ktorá sa odzrkadlí na konečnom dátovom prenose a tým aj časovej náročnosti prenosu.

Štruktúru ACP správy zobrazuje obrázok 3.2:



Obr. 3.2: Štruktúra ACP správy

Správa pozostáva z hlavičky (header), ktorej veľkosť je 7 bajtov a z N AVP (Attribute-Value Pairs), kde N = 0, 1, 2, ...
Správa, kde N má hodnotu 0, sa nazýva prázdna správa.

Sú definované tri následujúce formáty AVP:

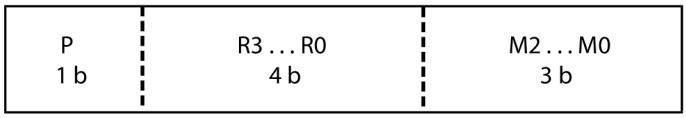
- Krátke (short) AVP (SAVP): obsahuje jediný typ dát o dĺžke kratšej než je $< 2^8$ bajtov. Tento formát je určený pre prenos krátkych blokov dát a pre použitie v zariadeniach s obmedzenými možnosťami. Hodnota Typ týchto AVP je v rozsahu hodnôt 0-127.
- Dlhé (long) AVP (LAVP): obsahuje jediný typ dát o dĺžke kratšej ako $< 2^{16}$ bajtov. Tento formát je určený pre prenos dlhších blokov dát. Hodnota Typ týchto AVP je v rozsahu hodnôt 128-191.
- Kontajnerové (container) AVP (CAVP): obsahuje jedno či viacej AVP ľubovolného typu. CAVP môže obsahovať rôzné SAVP, LAVP a CAVP v rôznych kombináciách. Celková dĺžka všetkých zoskupených AVP musí byť kratšia než $< 2^{16}$ bajtov. Tento formát AVP je určený pre zoskupovanie viacerých AVP do jednej AVP. Kritériom zoskupenia môže byť spoločný typ AVP, spoločný autentizačný kód skupiny a pod. Hodnota Typ týcho AVP je v rozsahu 192-255.

Hlavička ACP správy pozostáva z polí *CODE*, *IDENTIFIER* a *LENGTH*. Pole *CODE* (1 bajt) udáva typ správy a signalizuje, že ide o správu protokolu ACP. Táto signalizácia umožňuje spoluprácu protokolu EAP (Extensible Authentication Protocol) a ACP v jednom spoločnom spoji.

Obr. 3.3: Štruktúra ACP hlavičky

Význam jednotlivých bitov v poli *CODE* je následujúci:

- Bit P: tento bit odlišuje správu protokolu ACP od správy protokolu EAP a musí mať hodnotu 1
- Bity R3...R0: sú rezervné bity, ktorých hodnota (ak je rezervný bit) musí byť 0
- Bity M2...M0: bity určujúce typ správy - M0 udáva smer prenosu správy. Správy zahŕňujúce M0 = 0 sú správy v smere Žiadateľ -> Poskytovateľ. Správy s M0 = 1 naopak, v smere Poskytovateľ -> Žiadateľ.



Obr. 3.4: Štruktúra pola CODE

Pole *IDENTIFIER* (3 bajty) obsahuje unikátny identifikátor, ktorým sa v danom spoji rozlišujú správy určitej transakcie od správ ostatných transakcií. Hodnotu tohto pola pre každú transakciu určuje portál, ktorý v danom spoji vyšle prvú správu tejto transakcie, čiže správu *START*.

Pole *LENGTH* (3 bajty) uvádza celkovú dĺžku správy spolu s hlavičkou v bajtoch. Ak nejaký portál príjme správu s nesprávnou dĺžkou, tak musí transakciu zrušiť a to tak, že vymaže všetky prevádzkové informácie súvisiace s danou transakciou. Zrušenie transakcie vo všetkých ostatných portáloch nastane vypršaním časového limitu. Poskytovateľ môže transakciu zrušiť tiež zaslaním prázdnej správy *FINISH*.

Samotné dáta sú prenášané v dátovej štruktúre AVP, ktorá je zobrazená na obrázku 3.5:

Obr. 3.5: Štruktúra AVP

- Pole Typ (1 bajt): definuje význam dát v poli Hodnota
- Pole Dĺžka (x bajtov): definuje dĺžku pola Hodnota v bajtoch
- Pole Hodnota ($< 256^x$ bajtov): obsahuje samotné dáta

Ak Žiadateľ alebo Poskytovateľ príjme AVP takého typu, ktorý nedokáže spracovať, tak musí transakciu zrušiť.

3.1.4 Refundácia platieb

K samotnej platbe príde až po úspešnej výmene všetkých správ potrebných na uskutočnenie transakcie. To znamená, že až keď sa spojenie ukončí správou *FINISH* po úspešnej komunikácii (zjednané aktíva, vykonaná autentizačná metóda a autentizácia, doručené parametre), vykoná sa účtovanie (odrátanie čiastky z účtu zákazníka, prirátanie čiastky na účet obchodníka - medzibankové vyrovnanie). Ak sa stratí počas komunikácie správa, po vypršaní časovaču sa vyhodnotí transakcia za neúspešnú. Tak isto pri duplicite správy je trasnakcia označená za neúspešnú, končí sa komunikácia. Tým sa predíde k prípadnej neúspešnej transkacii.

Stabilita komunikácie

Dôležitým parametrom pri vytváraní platobných scenárov s použitím prokolu ACP je myšlienka zabezpečenia všetkých transkakcií takým spôsobom, aby nedošlo k strate informácií a aby priebeh a vyrozumenie platieb bol jasný a tým aj zrozumiteľný.

Protokol ACP umožňuje Žiadateľovi a Poskytovateľovi zjednať požadované aktíva, autentizačné motódy, vykonať samotnú autentizáciu, doručiť prístupové parametre a vykonať účtovanie. Každý jeden portál zahrnutý v komunikácii nesmie vyslať dalšiu správu skôr, kým nepríjme správu od druhej strany. Prípadnú segmentáciu správ a ochranu proti chybám zaisťuje príslušný komunikačný modul portálu.

Komunikáciu v protokole ACP riadi Poskytovateľ. Žiadateľ môže v správe *START* uviesť požadované aktívum, ponúknuť variantu protokolu a pod., lenže Poskytovateľ môže tieto údaje ignorovať a dotázať sa na ne až v priebehu dalšej komunikácie. Portál môže byť nastavený tak, aby reagoval iba na správy *START* s požadovanými vlastnosťami.

Stratu niektorej správy alebo prenosovú chybu majú riešiť komunikačné moduly portálu a protokol ACP preto prípadné prenosové chyby interpretuje ako potenciónálne útoky. Ak portál neobdrží do danej doby správnu odpoveď na svoju správu alebo naopak, obdrží túto správu viackrát po sebe, tak sa transakcia ruší. Pre časovú kontrolu je po prijatí správy *START* spustený časovač, ktorý sa resetuje po prijatí každej následujúcej správy. Ak časový interval uplynie, daná transakcia je zrušená a portál nebude reagovať na žiadne správy, ktoré príjme od tohto momentu týkajúcich sa tejto transakcie. Poskytovateľ môže transakciu zrušiť aj poslaním prázdnej správy *FINISH*.

Ak by došlo k incidentu, kde zákazník alebo obchodník duplicitne pošle šek, príde správa ACP protokolu (s rovnakou identifikáciou transakcie) dvakrát, tým sa transkacia preruší a je zhodnotená ako neúspešná.

3.2 Scenáre užitia ACP v platobnom systéme

Pri implementácii protokolu ACP do platobných systémov by sme mohli naraziť na pár prekážok. Ide hlavne o spôsob komunikácie zo strany Používateľa, pričom by musel mať nainštalovaný špeciálny software umožňujúci prevádzku ACP protokolu (môže sa jednať napríklad o AAA systémy spomenuté v kap. 2). Je nutné riešiť otázku, či je naozaj potrebné nútiť zákazníka, aby si pre uskutočnenie transakcie bol povinný nainštalovať software či riešil potrebu certifikátov.

Univerzalita ACP v platobnom systéme

Protokol ACP používa k riadeniu prístupu AC portály. Tieto portály sú súčasťou sieťového zariadenia, ktoré riadi prístup ostatných zariadení k atívam daného zariadenia alebo vyjednáva prístup k atívam iných zariadení.

V praxi to znamená, že ak chceme, aby koncové zariadenia mali možnosť komunikovať prostredníctvom ACP protokolu, je nutné, aby mali implementovaný (buď hardwarovo alebo softwarovo) portál, prostredníctvom ktorého budú môcť komunikovať.

Ak chceme docieliť to, že zákazník si nebude musieť inštalovať software (či implementovať hardware) na to, aby mohol vykonávať transakcie pomocou protokolu ACP, je tu možnosť návrhu protokolu ACP v programovacom jazyku JavaScript, ktorý umožní, aby dané funkcie portálu boli vykonávané „mimo“ zákazníkovej kompetencie pomocou technológií Ajax preposielané cez HTTP/HTTPS komunikáciu.

Ajax (Asynchronous JavaScript + XML) je súhrnné označenie pre technológie vývoja interaktívnych webových aplikácií, ktoré umožňujú meniť obsah stránok bez potreby ich kompletného znovunačítania zo serveru.

Týmto docielime to, že zákazník si nie je povinný nainštalovať žiadny software (túto problematiku rieši za neho server, s ktorým komunikuje).

Samozrejme, naskýta sa tu otázka zabezpečenia takéhoto prenosu. Pri prenose informácií takýmto spôsobom sú zabezpečené všetky komunikačné kanály. Celkový prenos informácií je zabezpečený synchrónnou (vyžaduje certifikát) alebo asynchrónnou šifrou (systém hesla slúžiaceho na autentifikáciu). Tým pádom prípadné podsunutie paketu je zistené nesprávným podpisom podsunutého paketu.

V prípade šifrovania synchrónnou šifrou je potrebné, aby zákazník mal certifikát, ktorý slúži na overenie strán (neslúži na samotné šifrovanie dát). Šifrovanie samotných dát zaisťuje protokol. Mohlo by sa jednať napríklad o protokol EAP-TLS.

V prípade šifrovania asynchrónnou šifrou je potrebné, aby zákazník mal heslo (ktoré má k dispozícii aj server v hashovanej podobe), ktoré slúži na overenie zákazníka. Toto heslo sa už pri inicializácii komunikácie zahashuje (napríklad šifrou

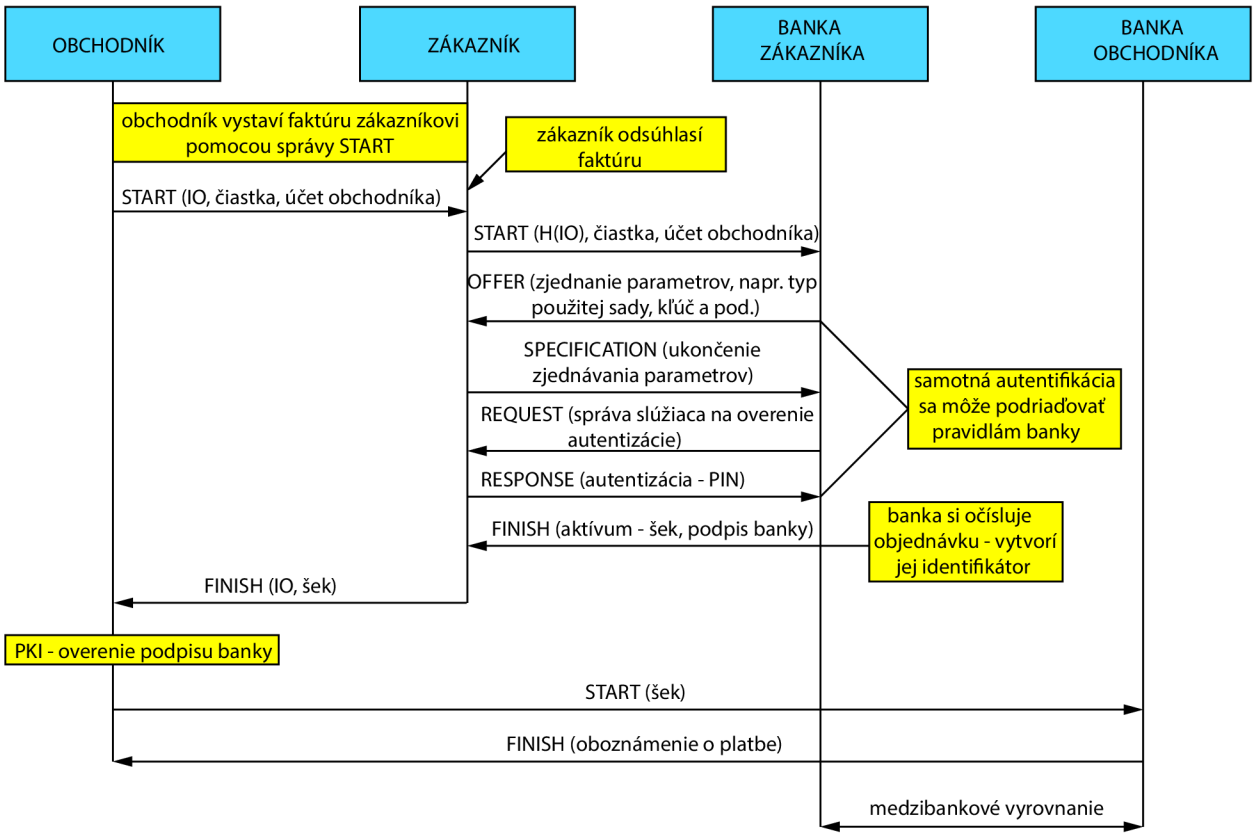
HMAC) a server, ktorý príjme zahashované heslo si hash tohto hesla porovná so svojim hashom hesla zákazníka.

Takéto riešenie by mohlo byť základom implementácie ACP protokolu v budúcnosti do platobných systémov (na koncových zariadeniach podporujúcich prehliadače) bez nutnosti inštalovania softwaru.

Pri počiatku návrhu budem prizerať na typ ochrany, nakoľko je to podľa mňa základ pri postupe navhrhovania.

3.2.1 Scenár s internou ochranou

Môj prvý návrh bude obsahovať zabezpečenie internou ochranou.



Obr. 3.6: Platba s použitím internej ochrany

Pri vyhotovovaní platby príde k vystaveniu faktúry zaužívaným komunikačným kanálom, a vo forme správy *START* pošle faktúru, pretože požadované parametre sa dajú uviesť už v tejto správe. Zákazník teda obdrží faktúru, a po jej odsúhlasení ju predá svojej banke znova v správe *START*, ktorá obsahuje zahashovanú ifentifikáciu objednávky - H(IO), čiastku platby a účet obchodníka. Zahashovaná identifikácia

objednávky neskôr slúži na overenie, či sa jedná práve o túto platbu. Tým sa započne nová výmena správ protokolu ACP.

Vyššie je uvedená sada protokolu TLS, ktorá sa využíva na internú ochranu. Každá banka podľa čiastky transakcie a dalších podmienok si stanoví spôsob autentizácie. Spravidla sa ale jedná o autentizáciu za pomoci šifrovania RSA. Tento spôsob autentizácie obsahuje aj protokol ACP, takže sa dá uvažovať o možnom použití aj pri autorizovaní v samotnej banke.

Výmena správ *OFFER* a *SPECIFICATION* slúži na zjednanie parametrov pre následujúcu komunikáciu a použitie sád protokolu. Výmena správ *REQUEST* a *RESPONSE* slúži na preposlaní zašifrovaných verejných a súkromných kľúčov a použitý šifier na uzrejmenie autentizácie či autorizácie. Po úspešnom vykonaní autentizácie (do procesu autentizácie je zahrnutý PIN - Personal identification number ktorý zaistí autentizáciu medzi bankou a zákazníkom) je súčasťou správy *FINISH* k dispozícii vystavený šek od banky spolu s podpisom banky ktorá ho vystavila a daná transakcia je uložená do databázy transakcií (v tomto prípade bude mať transakcia status „pending“ (čiže jedná sa o prebiehajúcu transakciu), po záverečnom medzibankovom vyrovnaní nadobudne status „successful“ a pri prípadnom zlyhaní transakcie status „failed“ (jedná sa o ilustračný príklad, ale banka si určite vedie podobným spôsobom záznamy o platbách aby jednak mali doklad o platbe a aby bolo možné spätne uskutočniť platbu - platba obchodník -> zákazník). Podpis banky neskôr slúži na overenie platnosti šeku zo strany obchodníka po obdržaní tohto šeku.

Zákazník po obdržaní šeku od svojej banky prída k šeku identifikáciu objednávky aby obchodník vedel, o ktorú transakciu sa jedná, toto všetko pošle vo forme správy *FINISH*.

Krok, pri ktorom si obchodník overuje pomocou podpisu banky, či sa jedná o legitímnu transkaciu je teoreticky možné vynechať, nakoľko je toto overenie uskutočnené samotnou bankou obchodníka pred vyrovnávaním transakcie.

Pomocou správy *START* zasiela obchodník šek svojej banke, ktorá vykoná potrebné opatrenia, aby si overila, či sa jedná o legitímnu platbu a či bude platba vykonaná v poriadku. Po kladnom overení posiela v správe *FINISH* oboznámenie obchodníkovi, že platba prebehla (resp. prebehne) úspešne.

V poslednom kroku príde k vyrovnaniu medzi bankami.

Z hľadiska univerzality je veľkou výhodou, že zákazník nie je nútený inštalovať software alebo certifikáty (ak sa jedná o platbu online, software je súčasťou webovej stránky, a ak by sa jednalo o platbu platobnou kartou, tento systém musí byť implementovaný pri použití samotnej karty na platobný terminál, takže zákazník je v oboch prípadoch mimo riešenia kompatibility).

Prenos potrebných informácií je zobrazený v tabulke 3.1(modrá farba značí správy prenášané medzi obchodníkom a zákazníkom, žltá farba značí správy me-

dzi zákazníkom a jeho bankou, zelená farba značí prenos medzi obchodníkom a jeho bankou).

Tab. 3.1: Prenesené informácie v scenári s internou ochranou

START	IO	čiastka		účet ob.		
START	AVP NAME _SUP	čiastka		účet ob.	H(IO)	
OFFER	AVP typ aut.					
SPECIFY	AVP spec.					
REQUEST	SAVP LAM					
RESPONSE	dáta k aut.					
FINISH	AVP RESULT	čiastka	adr. banky z.	2 x účet	H(IO)	podpis banky z.
FINISH	AVP RESULT	čiastka	adr. banky z.	2 x účet	H(IO)	podpis banky z.
START	AVP NAME_SUP	čiastka	adr. banky z.	2 x účet	H(IO)	
FINISH	AVP RESULT					

Každá správa protokolu ACP má hlavičku, ktorá slúži na identifikáciu o akú správu ide (typ správy, identifikácia komunikácie a pod.). Veľkosť hlavičky je 56 b a je statická. AVP správy (obsiahnuté v ACP správach) majú okrem dát a entít, ktoré sú potrebné k prenosu aj polia potrebné k určeniu typu tejto AVP správy a dĺžky (ktorá slúži k overeniu či správa prišla celá a nedošlo k výpadku pri prenose). Typ AVP je statická (8 b) a dĺžka závisí od veľkosti dát v poli Hodnota. Pohybuje sa od 8 do 16 b (vo väčšice prípadov je pole Dĺžka 8 b, pretože veľkosť prenášaných dát v poli Hodnota neprekročí veľkosť 256 b, až na zahashovanú IO, ktorá má statickú veľkosť 512 b).

Identifikácia objednávky (IO) obsahuje unikátne číslo (pre každú transkaciu iné) a má hodnotu short INT (16 b). Slúži na to, aby boli jednotlivé transakcie od seba odlíšitelné. Čiastka má hodnotu positive long INT (32 b + špecifikáciu meny 3 x CHAR = 24 b, dokopy teda 56 b) a vyjadruje čiastku danej transakcie. Účet entity je 14 miestne číslo (spolu aj s kódom banky), takže jeho veľkosť je statická (48 b). AVP s názvom NAME SUP slúži k identifikácii žiadateľa. Hodnota pola Hodnota je v tomto prípade Text (jeden znak = 8 b). Hashovaná identifikácia objednávky má statickú veľkosť (512 b). Dôvodom je skutočnosť, že nech číslo akejkoľvek dĺžky pridáme na vstup algoritmu, dostaneme vždy rovnako veľký údaj. AVP obsiahnuté v správe *OFFER* oznamuje, o aký typ autentizácie sa bude jednať (správa je poslaná od Poskytovateľa, čo znamená že podmienky si bude určovať banka na základe čiastky a cieľa transakcie). Typ dát v poli Hodnota bude STRING (veľkosť by sa mala pohybovať okolo cca 8-16 b podľa typu zjednávaných parametrov). Žiadateľ následne odošle v správe *SPECIFICATION* obsiahnutú AVP správu, ktorá je odozvou na

zjednávané parametre autentizácie. Táto správa má rovnakú veľkosť, nakoľko je potvrdzujúcou k predošlej správe. Samozrejme, pri komunikácii môže prísť k viacerým výmenám správ *OFFER* a *SPECIFICATION* (záleží na dohodnutí najlepšej možnej varianty alebo „jedinej“ možnej varianty). Správa *REQUEST* obsahuje SAVP názvu LAM (lokálna autentizačná metóda). Dôvodom je skutočnosť, že autentizácia prebieha podla banky (autentizačnú metódu určuje Poskytovateľ - banka). Typ Hodnota má dátový typ STRING (hodnota sa pohybuje od 8-16 b). Ako povinná odpoveď od Žiadateľa je správa *RESPONSE*, ktorá obsahuje dáta potrebné k autentizácii (hodnota STRING, veľkosť podľa typu autetizácie). Súčastou správy *FINISH* je AVP s názvom RESULT a uvádza výsledok transakcie. Hodnota 0 reprezentuje stav, že prístup je povolený a hodnota 2 znamená, že prístup je zamietnutý (jeho veľkosť je teda 8 b). Ďalšími súčasťami správy *FINISH* je čiastka (56 b), adresa banky (STRING = počet znakov adresy x 8 b), účet obchodníka a účet zákazníka (2 x 48 b = 96 b), hashovaná IO (512 b) a podpis banky zákazníka. Táto správa spolu s výsledkom od banky zákazníka ide ďalej od zákazníka k obchodníkovi. Obchodník po obdržaní správy od zákazníka pošle správu *START* svojej banke, kde je cez správu AVP s názvom NAME SUP autorizovaný. Súčasťou správy je čiastka (56 b), adresa banky (STRING), 2 x účet (96 b) a zahashovanú identifikáciu objednávky (512 b). Banka overí, či sa jedná o legitímny požiadavok. Ak je všetko v poriadku (identifikácia objednávky je unikátna, banka zákazníka vie o transakcii a pod.), banka obchodníka pošle správu *FINISH* s AVP s názvom RESULT, kde uvádza výsledok transakcie. Následne dôjde ku konečnému vyrovnaniu bánk.

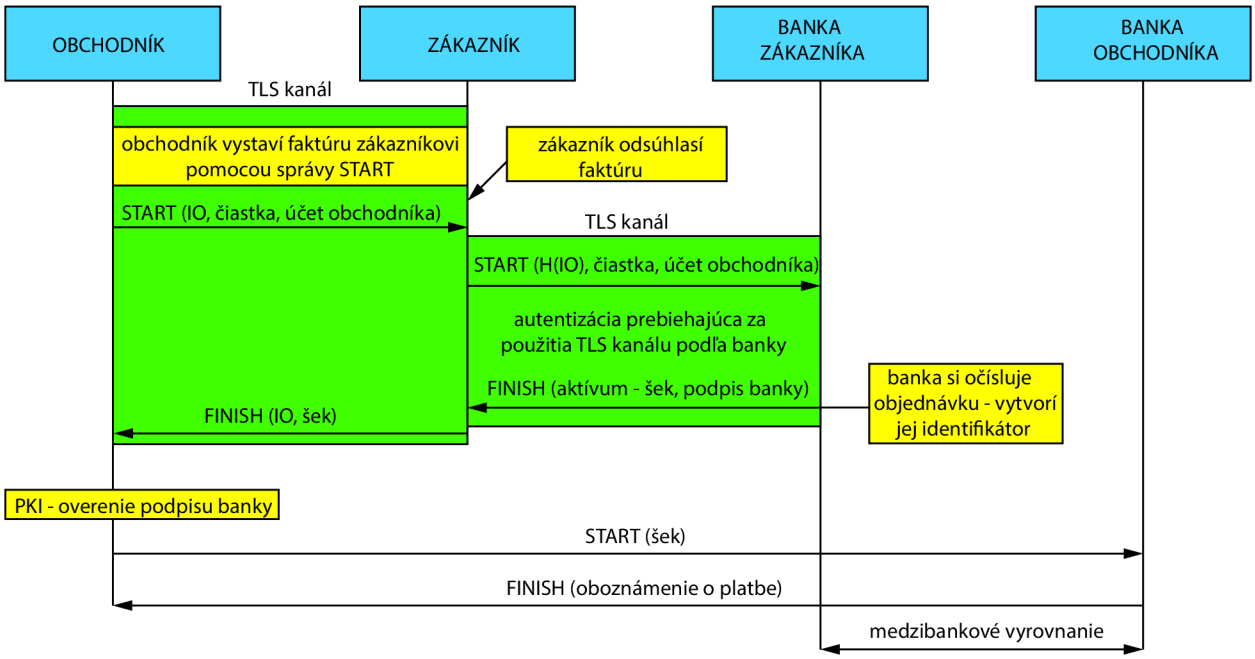
Po zrátaní veľkostí (doplnil som pomyselnú adresu banky, podpis banky, typ autentizácie a pod.) som sa dopracoval k celkovej veľkosti prenosu 4000-5000 bitov (0.00047 - 0.00059 MB). Táto veľkosť je veľmi malá v porovnaní s dnešnými prenosovými rýchlosťami. Pre zaujímavosť by sme si nahliadnuť na situáciu, kde by bol celkový prenos najdlhší. Teoreticky sa jedná o prenos GPRS (mobilnou dátovou) službou. Najpoužívanejšími kódovými schémami sú dnes kódovanie CS - 1 (8 kbit/ s) a CS - 2 (12 kbit/ s). Pri najväčšej prenosovej rýchlosti GPRS trvá naviazanie TCP spojenia (ping) až 600 - 700 ms [13]. To by mohlo znamenať, že by sa celkový prenos mohol dostať až na 1 sekundu (v najhorších prípadoch).

3.2.2 Scenár s externou ochranou

Transakcie protokolu ACP môžu prebiehať v redukovanej podobe. Žiadateľ udáva potrebné parametre už v správe *START*, takže nie je nutné aby došlo v výmene správ *OFFER* a *SPECIFICATION*. V prípade, že Žiadateľ aj Poskytovateľ sú koncovými uzlami zabezpečeného kanálu (v tomto prípade TLS kanálu), tak je možné vypustiť výmenu správ *REQUEST* a *RESPONSE*. Dôvodom je skutočnosť, že au-

tentičnosť strán je daná zabezpečeným kanálom. Typicky je autorizovaný len server (to znamená že jeho identita je zaručená), zatiaľ čo klient ostáva neautorizovaný. To znamená, že koncový užívateľ, či už jednotlivec alebo aplikácia, si môže byť istý s kým komunikuje. Ďalšia úroveň zabezpečenia, v ktorej obe komunikujúce strany si môžu byť isté s kým komunikujú, je známa ako obojstranná autorizácia. Obojstranná autorizácia vyžaduje infraštruktúru verejného kľúča (PKI).

V tomto prípade sa dá transakcia ACP redukovať iba na výmenu správ *START* a *FINISH*.



Obr. 3.7: Platba s použitím externej ochrany

Na počiatku transakcie sa vybuduje TLS kanál medzi obchodníkom a zákazníkom. Následné obchodník vystaví faktúru pre zákazníka, ktorá je súčasťou správy *START*.

V tomto bode sa tvorí TLS kanál medzi zákazníkom a bankou zákazníka, vykoná sa autorizácia. Zákazník po autorizácii posiela faktúru, ktorú obdržal od obchodníka, predáva ju svojej banke v správe *START* podobne, ako ju obchodník predal predtým zákazníkovi. Banka vystaví šek, a spolu so svojím podpisom ho predá ako aktívum v správe *FINISH* naspäť zákazníkovi.

Zákazník, ktorý disponuje šekom vystaveným od svojej banky, posiela tento šek spolu s podpisom svojej banky ako aktívum v správe *FINISH*, ktorá stále spadá pod komunikáciu v prvom TLS kanáli.

Obchodník má teraz šek, ktorý bol vystavený bankou zákazníka. Podobne ako v scenári s internou ochranou, je krok overenia podpisu banky zákazníka nepovinný,

nakoľko dochádza k overeniu medzi bankami pri vzájomnou vyrovnaní.

Obchodník predá šek svojej banke v správe *START*. Akonáhle banka obchodníka vie, že sa jedná o legitímnu platbu, oboznámi obchodníka správou *FINISH*, ktorá zároveň ukončí komunikáciu.

V poslednom kroku dôjde k vzájomnému vyrovnaniu medzi bankami.

Z hľadiska univerzality za znova jedná o scenár, ktorý žiadnym spôsobom nenúti zákazníka, aby si inštaloval prídavný software alebo certifikát (technológie Ajax). Týmto môžeme považovať oba scenáre za uspokojivo univerzálne.

Na rozdiel od prvého scenára, kde bezpečnosť rieši samotný protokol ACP, v tomto prípade je bezpečnosť riešená kanálom TLS.

Prenos potrebných informácií je zobrazený v tabulke 3.2(modrá farba znamená výmenu správ medzi obchodníkom a zákazníkom, žltá medzi zákazníkom a bankou zákazníka a zelená medzi obchodníkom a jeho bankou):

Tab. 3.2: Prenesené informácie v scenári s externou ochranou

START	IO	čiastka		účet ob.		
START	AVP NAME _SUP	čiastka		účet ob.	H(IO)	
FINISH	AVP RESULT	čiastka	adr. banky z.	2 x účet	H(IO)	podpis banky z.
FINISH	AVP RESULT	čiastka	adr. banky z.	2 x účet	H(IO)	podpis banky z.
START	AVP NAME_SUP	čiastka	adr. banky z.	2 x účet	H(IO)	
FINISH	AVP RESULT					

Pri vzniku komunikácie je vytvorený kanál TLS medzi obchodníkom a zákazníkom. Obchodník v správe *START* zasiela zákazníkovi faktúru (identifikácia objednávky = 16 b, čiastka = 56 b a účet obchodníka = 48 b). Ak zákazník odsúhlasí faktúru, naviaže sa kontakt zákazníka s jeho bankou, vytvorí sa medzi nimi kanál TLS a zákazník predáva v správe *START* AVP s názvom NAME SUP (8 x počet CHAR b, identifikácia zákazníka k banke), H(IO) = 512 b, čiastku = 56 b a účet obchodníka = 48 b. Banka pridá šeku (AVP RESULT = 8 b, čiastka = 56 b, adresa banky = 8 b x počet znakov, účet zákazníka aj obchodníka = 96 b, H(IO) = 512 b, a podpis banky) identifikátor, čím si uloží prebiehajúcu transakciu do databázy a správou *FINISH* ho pošle zákazníkovi. Zákazník preposiela šek obchodníkovi, ktorý si môže (a nemusí) overiť podpis banky. Obchodník kontaktuje svoju banku, posiela správu *START* (AVP NAME SUP = 8 b x počet znakov, čiastka = 56 b, adresa banky (8 b x počet znakov), oba účty = 96 b a H(IO) = 512 b. Obchodníkova banka po overení či sa jedná o legitímny požiadavok zasiela správu *FISNIH*, ktorá obsahuje vyrozumenie v AVP RESULT (8 b). Ak sa jedná o legitímnu transakciu, nasleduje medzibankové vyrovnanie.

Po zrátaní veľkostí (doplnil som pomyselnú adresu banky, podpis banky a pod.) som sa dopracoval k celkovej veľkosti prenosu 3200 - 3500 bitov (0.00038 - 0.00041 MB). Samozrejme, do výsledného času celkového priebehu komunikácie musím zarátať aj tvorbu TLS kanálov. Vo výsledku sa jedná o „zanedbateľné“ číslo a do celkového časového priebehu nemá znamenitý vplyv. Podobne ako pri scenári s internou ochranou, celkový prenos prebehne za veľmi krátky časový úsek (vzhľadom na veľmi malú veľkosť všetkých prenesených informácií).

3.2.3 Scenár bezpečnosti

Či za použitia externej alebo internej ochrany, celkový prenos je v konečnom dôsledku šifrovaný takým spôsobom, aby znemožnil odcudzenie majetku a dôverných informácií, ale aj podsunutie cudzích informácií, ktoré by kompromitovali danú transakciu.

Riešenie šifrovania privátnym a verejným kľúčom je celkom spoľahlivé, v tomto systéme dochádza k šifrovaniu a dešifrovaniu kľúčmi, z ktorých privátny je chránený, takže je zaistené to, aby v prípade, že sa niekto dostane do komunikácii medzi stranami, ukradnuté informácie budú pre útočníka nepoužiteľné, nakoľko sú chránené daným kľúčom.

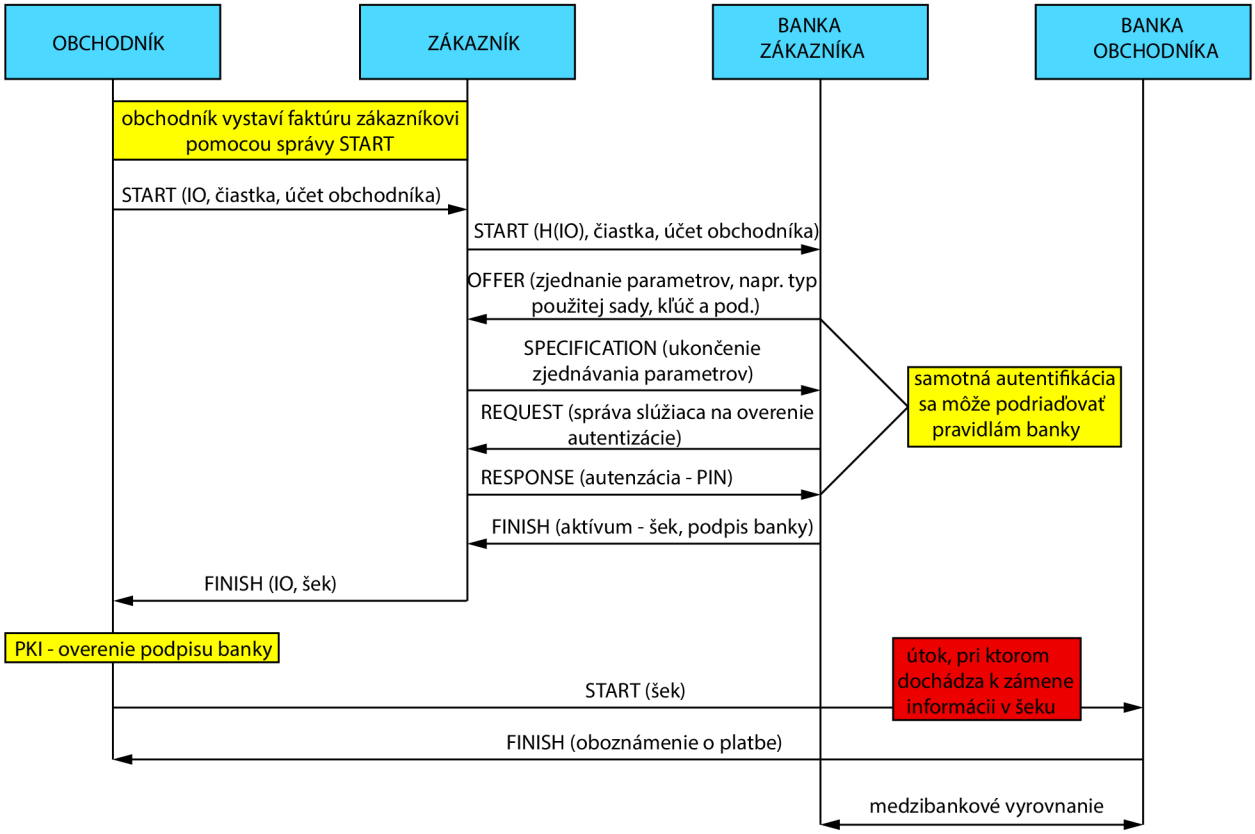
Kedže je použitá šifrovaná komunikácia v protokole ACP, a v kanáli TLS, ostávajú komunikačné spoje (v oboch scenároch), ktoré by sa mohli zdať na prvý pohľad nezabezpečené. Takýto príklad je zakreslený na obrázku 3.8.

V tomto prípade útočník napadne komunikáciu v bode, kde dochádza k predaniu šeku, ktorý je zašifrovaný podpisom. Šek nesie informácie, o akú objednávku sa jedná (IO), o účet obchodníka a o výšku čiastky transakcie.

V šeku je textová podoba všetkých týchto údajov (IO, účet obchodníka, výška čiastky transkacie) a tak isto rovnaké informácie znova, ale chránené podpisom.

Útočník, ktorý chce, aby sa transkacia vyúčtovala na jeho účet, zamení údaj v šeku a to tým spôsobom, že zamení informácie v textovej podobe tak, že mu budú vyhovovať - prvotný údaj o čísle účtu obchodníka zamení za svoj účet, aby peniaze boli vyplatené na jeho konto (môže prípadne zameniť výšku čiastky, tým dostane väčší obnos financií). Útočník je schopný zameniť informácie chránené podpisom, lenže po jeho dešifrovaní nebude schopný údaje naspäť zašifrovať do podoby, v ktorej boli predtým, pretože nemá prístup ku privátnemu kľúču banky.

Obchodníkova banka obdrží šek, ktorý bol napadnutý, no v tomto bode to ešte netuší. Dôjde k samotnému dešifrovaniu podpisu verejným kľúčom, a k porovnaniu textovej časti šeku s dešifrovanou časťou. Tu si banka obchodníka uvedomí, že došlo k nezhode, pošle prázdnu správu *FINISH* a tým je transakcia zrušená.



Obr. 3.8: Ukážka útoku pri platbe

MITMA útok

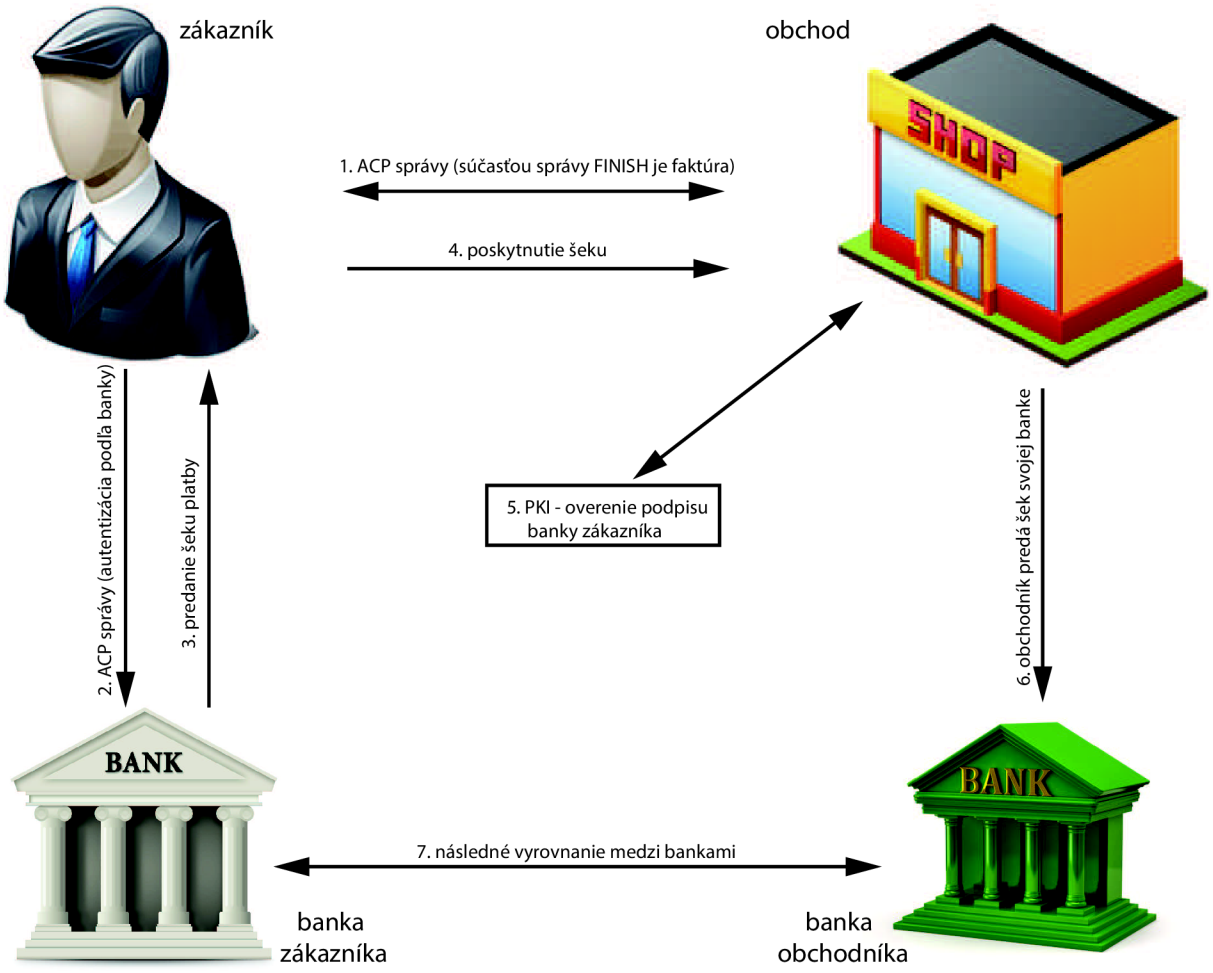
MITMA (Man in the middle attack - človek uprostred) patrí medzi najznámejšie problémy pri riešení bezpečnosti v informatike. Jeho podstatou je snaha útočníka odposlúchavať komunikáciu medzi účastníkmi tak, že sa stane aktívnym prostredníkom. Dôležitý je fakt, že útočník nie je nutený sa fyzicky nachádzať medzi účastníkmi komunikácie, pretože sieťovú prevádzu možno jednoducho presmerovať.

Jedným z najefektívnejších riešení obrany proti tomuto útoku je implementovať do autentizácie vzájomne vymenený kľúč (PIN kód, elektronický podpis a pod.), ktorý poznajú len účastníci (v tomto prípade zákazník a banka zákazníka) komunikácie. Kedže útočník nemá prístup ku kľúču (pretože kľúč sa nenachádza v digitálnej forme na sieti), pri prípadnom podvrhnutí jednej z informácií by pri autentifikácii prišlo k tomu, že by podvrhnuté informácie neobsahovali kontrolu kľúčom, a tým pádom by bol útočník odhalený. Môže sa jednať o ochranu PIN kódom tým spôsobom, že pri hashovaní faktúry, šeku či akejkoľvek informácie je pred informáciu doplnený tento kód, ktorý musí byť po dešifrovaní rovnaký s kódom, ktorý má druhý účastník (banka) k dispozícii.

3.2.4 Scenár s plnou ACP komunikáciou

Sú prípady, kedy je potrebné, aby už prvotná komunikácia medzi zákazníkom a obchodníkom bola autorizovaná. Jedná sa o také platby, kedy je v záujme samotného obchodníka, aby daná platba bola pridelená správnemu zákazníkovi, a nie komukoľvek (pretože obchodníkovi je v podstate jedno, kto za tovar zaplatí, hlavne ak sa bude jednať o právoplatnú platbu medzi bankami a obchodník obdrží za daný tovar či službu zaplatené). Môže sa jednať napríklad o uplatnenie zľavy formou odrátania DPH, kedy obchodník odráta (resp. nenavýši) DPH ku konečnej cene firme, ktorá je v obchodnom registry a tým pádom má na to právo. Samozrejme že dnes existujú spôsoby, ako dochádza k samotnému overeniu, či sa jedná o legitímneho zákazníka, ale ako bude vidieť v tomto scenári, je možné to vyriešiť aj pomocou protokolu ACP.

V tomto scenári dochádza k plnej výmene všetkých ACP správ už pri zadávaní požiadavku na transakciu.



Obr. 3.9: Scenár s použitím plnej ACP komunikácie

Keď príde k tomu, že zákazník bude chcieť zaplatiť za tovar či službu, je mu vystavená faktúra, ktorú musí za daný tovar či službu uhradiť. Pri predávaní samotnej faktúry dôjde medzi zákazníkom a obchodníkom k prenosu všetkých ACP správ, pričom nastane základné budovanie cesty pre túto transakciu, zjednajú sa parametre autentizácie, vykoná sa autentizácia a po úspešnej komunikácii sa v spáve *FINISH* pošle samotná faktúra (v reále to skôr znamená preukázanie občianským preukazom alebo prihlásením do portálu s menom a heslom, aby sa „zaistila“ identita zákazníka).

Zákazník, ktorý v tomto momente disponuje faktúrou, komunikuje so svojou bankou. Pri tomto procese dôjde znova k prenosu všetkých ACP správ. Faktúra sa posiela už v správe *START*. Kedže každá banka vyžaduje podľa výšky čiastky a podmienok transkacie svoju autorizáciu, tak sa autorizácia pomocou ACP správ podriaďuje týmto podmienkam.

Banka teda obdrží faktúru, vystaví šek, ktorý má svoje identifikačné údaje a v konečnej správe *FINISH* ju poskytne zákazníkovi.

Zákazník predá šek obchodníkovi, ktorý si jeho platnosť overí. Po kladnom overení je zrejmé, že sa jedná o legitímnu transakciu a preto obchodník predá tento šek svojej banke.

Keď obchodníkova banka obdrží šek, kontaktuje banku zákazníka a dochádza k vzájomnému vyrovnaniu. Týmto celá transakcia prebehla úspešne.

Z hľadiska univerzality je veľkou nevýhodou, že zákazník je nútený inštalovať potrebný software, ktorý umožní prvotnú komunikáciu pomocou ACP protokolu. Toto môžeme považovať za vysokú prekážku pri samotnej implementácii.

Jedná sa skôr o experimetnálny scenár, ktorý by mohol v budúcnosti zaistiť autentifikáciu bez použitia osobných dokladov (občiansky preukaz) a prihlasovacích údajov (ktoré sú v dnešnej dobe ľahko napadnuteľné) voči obchodníkovi. Jedným z možných riešení je generovanie unikátneho certifikátu pre každého užívateľa. V tomto prípade používateľ nie je nútený inštalovať si software, len umiesniť daný certifikát do svojho koncového zariadenia, cez ktoré transakciu vykonáva. Ak by táto autentifikácia bola doplnená heslom, jednalo by sa o relatívne veľmi spoľahlivú metódu.

4 ZÁVER

Bakalárska práca sa zaoberá problémami zabezpečenia prevádzky platobných systémov s použitím protokolu ACP.

Systém, s ktorým som pracoval je navrhnutý tak, aby bol schopný prevádzky na rozličných hardwarových platformách, čo plne vyhovuje rozmanitostiam prvkov užívaných v platobných systémoch.

Po naštudovaní systému platieb a protokolu ACP som navrhol scenáre, do ktorých som tento protokol implementoval a následne som tieto scenáre zhodnotil z hľadiska bezpečnosti, univerzality a dátovej náročnosti. Vychádzal som zo stávajúcich riešení platobných systémov. Pri návrhu som dbal hlavne na bezpečnosť jednotlivých scenárov tak, aby sa dali prehlásiť za bezpečné. Snažil som sa brať do úvahy všetky možné spôsoby napadnutia útočníkom a následne domyslieť scenár tak, aby sa týmto potenciálnym útokom dalo zabrániť. Scenáre som rozdelil na základe bezpečnosti, a to na scenár s internou ochranou a scenár s externou ochranou. Obidva scenáre umožňujú implementáciu protokolu ACP bez nutnosti inštalovania softwaru (v prípade použitia technológií Ajax), čím sa dajú považovať za univerzálne. Pri obidvoch scenároch som dopodrobna opísal priebeh komunikácie a následne vypočítal veľkosť všetkých informácií, ktoré sa prenesú. Kedže sa hodnoty prenesených informácií pohybovali v rozmedzí od 3200 do 5000 bitov v závislosti od scenára, môžeme usúdiť, že samotný prenos informácií potrebuje veľmi malý časový úsek v závislosti na rýchlosti prenosu (v normálnej prevádzke nebude účastník schopný zaregistrovať odozvu).

Kedže dnes ešte nie je vymyslený spôsob autentifikácie pri platbách, kde je nutné, aby obchodník poznal pravú identitu zákazníka (a prípadne aj naopak), navrhol som scenár, ktorý by mohol byť v budúcnosti použitý pri vytváraní univerzálneho scenára, v ktorom sa zákazník nepreukazuje fyzicky dokladom a ani sa neprihlasuje na webovú stránku ako používateľ.

LITERATÚRA

[1] BURDA, K.; STRAŠIL, I.; PELKA, T.; STANČÍK, P. *Access Control Protocol (ACP); Access Control Protocol (ACP). RFC draft.* Dostupné z URL: <http://tools.ietf.org/html/draft-kaaps-acp-01>.

[2] HASELSTEINER, E.; BREITFUSS, K. *Security in Near Field Communication (NFC).* [online]. 2006. Dostupné z URL: <http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf

[3] BURDA, K. *AAA systémy a protokoly. Elektrorevue - Internetový časopis* 2009. ISSN: 1213-1539. Dostupné z URL: <http://www.elektrorevue.cz/cz/clanky/informacni-techologie/0/aaa-systemy-a-protokoly/>.

[4] BURDA, K. *Univerzální rámec pro řízení přístupu v počítačových sítích. Elektrorevue - Internetový časopis* 2011. ISSN: 1213-1539. Dostupné z URL: <http://www.elektrorevue.cz/cz/clanky/komunikacni-technologie/0/univerzalni-ramec-pro-rizeni-pristupu-v-pocitacovych-sitich/>.

[5] GUADAMUZ, A. *PayPal: The Legal Status of P2P Payment Systems.* 2004. Dostupné z URL: <http://hdl.handle.net/1842/2262>.

[6] DIERKS, T., Allen, C. *The TLS Protocol Version 1.0* [Internet Draft]. Internet Engineering Task Force, Fremont, 1999. Dostupné z URL: <http://www.ietf.org/rfc/rfc2246.txt>.

[7] *MeT White Paper on Mobile Transactions, Mobile Electronic Transaction.* Január 2003. www.mobiletransaction.org

[8] KARNOUSKOS, V. *The European Perspective on Mobile Payments . In: IEEE Symposium on Trends in Com munications Proceedings* [online]. 2004. Dostupné z URL: <http://sites.google.com/site/karnouskos/files/2004_SYMPOTIC.pdf>.

[9] KARNOUSKOS, STAMATIS. *Mobile payment: A journey through existing procedures and standardization initiatives. In: IEEE Communications surveys and tutorials: A journey through existing procedures and standardization initiatives.* 2004. Dostupné z URL: <http://www.alice-dsl.net/netspace/files/2004_COMSOC-SURVEYS.pdf>.

[10] PIJÁK, M. *Elektronické platební systémy* 2003. Dostupné z URL: <http://www.fi.muni.cz/usr/staudek/vyuka/security/e_payment/index.html#2-4-4>.

[11] JARUPUNPHOL, P., MITCHELL, C. J.P. *Measuring 3-D Secure and 3D SET against e-commerce end-user requirements. In: Proceedings of the 8th Collaborative electronic commerce technology and research conference.* Jún 2003. Dostupné z URL: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.65.6613&rep=rep1&type=pdf>.

[12] *Wikipedia: Transport Layer Security* 2013. Dostupné z URL: <http://en.wikipedia.org/wiki/Transport_Layer_Security>.

[13] GsmServer Team *GPRS: Briefly about GPRS technology.* 2013. Dostupné z URL: <http://gsmserver.com/articles/gprs.php>.

[14] KRAWCZYK, H., BALLARE, M., CANETTI, R. *HMAC: Keyed-Hashing for Message Authentication* [RFC 2104] Internet Engineering Task Force, Fremont, February. 1997. 11 s. [cit. 12. 12. 2012]. Dostupné z URL: <http://www.ietf.org/rfc/rfc2104.txt>.

[15] MURDOCH, S.J. a ANDERSON R.. Verified by VISA and MasterCard SecureCode: or, How Not to Design Authentication. In: *Financial Cryptography and Data Security.* Tenerife, Spain: University of La Laguna, 2010. Dostupné z URL: <http://www.cl.cam.ac.uk/~rja14/Papers/fc10vbvsecurecode.pdf>.

[16] LEŽÁK, P. *Testovací implementace protokolu ACP*: diplomová práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2012. 67 s. Vedoucí práce byl doc. Ing. Karel Burda, CSc.

[17] HANEWINKEL, H. RSA Public Key Encryption Demo. [online]. 2005 Dostupné z URL: <http://www.hanewin.net/encrypt/rsa/rsa-test.htm>.

[18] PATIDAR a JAIN. *Performance Measurements of RSA Algorithm on Web Browsers* [online]. Mandsaur Institute of Technology, Mandsaur, c2009. Dostupné z URL: <http://mewaruniversity.academia.edu/NileshJain/Papers/504242/Performance_Analysis_of_RSA_on_Webbrowsers_using_Java_Script>.

ZOZNAM SYMBOLOV, VELIČÍN A SKRATIEK

NFC Near Field Communication: krátkodosahové, vysokofrekvenčné, bezdotykové spojenie, umožňujúce výmenu dát medzi zariadeniami do vzdialenosti okolo 10 cm

POS miesto predaja (POS) je miesto, kde nastanú transakcie výmenou za tovar alebo služby

CNP typ služby, ktorá slúži na vykonávanie platieb za tovar alebo služby objednané na základe poštovej alebo telefonickej objednávky alebo objednávky prostredníctvom internetu

ACS Acces Control Server - v protokoli *3D Secure* je na vydávateľskej strane (banka)

SET štandardný aplikačný protokol určený pre zabezpečenie transakcií platobnými kartami

AAA systém poskytujúci funkcie autentizácie, autorizácie a účtovania

ACP Access Control Protocol: protokol riadenia prístupu

AVP Attribute-Value Pair: jedna zo základných reprezentácií dát v počítačových systémov a aplikáciách

TLS Transport Layer Security: protokol slúžiaci na šifrovanie dát, nástupca SSL

SSL Secure Socket Layer: protokol postavený nad transportnou vrstvou zaisťujúci bezpečnosť komunikácie po internete

AVP Attribute-Value Pair: dátová štruktúra správ ACP

PKI Public Key Infrastructure: v krytptografii označenie infraštruktúry správy a distribúcie verejných kľúčov z asymetrickej kryptografie

SAVP Short AVP: krátka verzia AVP

LAVP Long AVP: dlhá verzia AVP

CAVP Container AVP: AVP obsahujúca radu iných AVP

PIN Personal Identification Number: tajné číselné heslo zdieľané medzi systémom a používateľom slúžiace na autentizáciu

GPRS General Packet Radio Service: univerzálna paketová rádiová služba - mobilná dátová služba prístupná pre používateľov GSM mobilných telefónov

MITMA Man In The Middle Attack: jeden z najznámejších problémov pri riešení bezpečnosti v informatike