UDC: 004.78:336.717 INFO M: str. 46-52

ARHITEKTURA I OSNOVNE TEHNIKE ZAŠTITE SISTEMA ZA PLAĆANJE PREKO INTERNETA
ARCHITECTURE AND BASIC SECURITY TECHNIQUES FOR INTERNET PAYMENT SYSTEMS

Natasa Merker

REZIME: U ovom radu prikazana je arhitektura sistema za plaćanje u DinaCard sistemu i razrađene su neke od mogućih modifikacija te arhitekture kako bi se omogućila upotreba drugih platnih kartica kao što su VISA i MasterCard. Kao "parametar" na osnovu kojeg su analizirane modifikacije uzet je nivo aktivnosti Payment Gateway provajdera, koji raste sa migracijom sistema prema internacionalnim rešenjima. Takođe, u radu su opisane osnovne tehnike zaštite ovakvih sistema za online plaćanje.
KLJUČNE REČI: arhitektura platnih sistema, kartice za plaćanje, DinaCard, VISA, MasterCard, tehnike zaštite
ABSTRACT: This paper presents the arhitecture of the payment system in DinaCard system and elaborates possibly modifications of that arhitecture in order to enable the use of another payment card types as VISA and MasterCard. Analysis of modification is based on "parametar" which represents activity level of Payment Gateway Provider, which decrease with system migration to international solutions. This paper also, describes basic security techniques for such online payment systems.
KEY WORDS: payment systems arhitecture, payment cards, DinaCard, VISA, MasterCard, security techniques

1. UVOD

Sistemi za plaćanje generalno predstavljaju svaki sistem za procesiranje instrumenata za plaćanje i poravnanje dugova između učesnika u sistemu [1]. Termin platni sistem se danas često koristi za softverske sisteme i kompjuterske mreže finansijskih institucija. Prema tome, platni sistem se može preciznije definisati kao skup procedura i povezanih kompjuterskih mreža za poravnanje finansijskih transakcija na tržištu, i za transfer novčanih sredstava između finansijskih institucija [2]. Platni sistemi su danas sastavni deo modernog protoka novca.

Prvi sistemi za plaćanje nastali su sa potrebom za on-line plaćanjem kao odgovor na problem vazan za činjenicu da se novac ne može prenositi kroz mrežu. Kada je poslovni svet shvatio mogućnosti Interneta, počeo je masovni razvoj sistema za plaćanje, a jedno od prvih rešenja bile su kartice za plaćanje kao instrument plaćanja.

Danas je plaćanje platnom karticom jedno od najpopularnijih metoda plaćanja. Po dobijanju platne kartice, korisnik osniva račun sa bankom i može da kupuje. Plaćanje platnom karticom podrazumeva plaćanje na osnovu tog računa. Kada banka korisnika jednom autorizuje plaćanje za korisnika, trgovac dobija njihovu uplatu na bankovnom računu osnovanom u banci trgovca, koja je takođe povezana kao primalac. Neki od primera sistema za plaćanje su "Europay International", "MasterCard International" i "Visa International, a na domaćem tržištu DinaCard sistem.

U nastavku rada opisana je arhitektura DinaCard platnog sistema sa specifičnostima domaćeg rešenja, prema predviđenom toku plaćanja koji je objavljen u radu pod nazivom "Plaćanje na Internetu u DinaCard sistemu" [4].

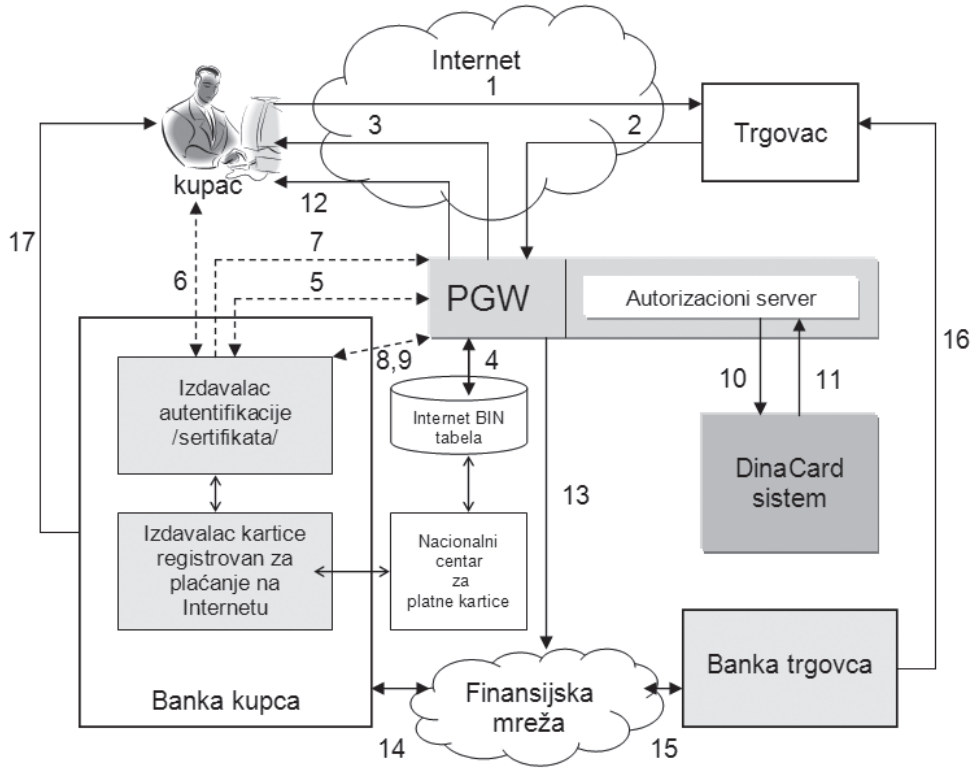
U radu su razrađene moguće modifikacije te arhitekture u cilju proširenja upotrebe na druge platne kartice VISA i MasterCard i sa stanovišta nivoa aktivnosti Payment Gateway provajdera, koja se menja sa migracijom arhitekture od specifičnog domaćeg rešenja prema internacionalnim rešenjima. Nivo aktivnosti PGW-a se može definisati kao ukupan broj obaveznih i opcionih operativnih pravila koje provajder mora da izvrši. Što je broj koraka operativnih pravila veći to je i nivo aktivnoati PGW-a veći. Na kraju rada navedene su osnovne i neophodne tehnike zaštite koje je potrebno primeniti kada je u pitanju bezbednost sistema za plaćanje na Internetu.

2. ARHITEKTURA SISTEMA PLAĆANJA UPOTREBOM DINACARD

Prema arhitekturi sistema plaćanja na Internetu upotrebom DINA kartice sa slike 1, Payment Gateway provajder ima veoma zahtevnu ulogu, što je jedna od osnovnih razlika u odnosu na većinu internacionalnih sistema platnih kartica. Payment Gateway provajder (PGW) je učesnik sistema, čija je jedna od osnovnih delatnosti online plaćanje. Na taj način se postiže rasterećenje ostalih učesnika u sistemu, a PGW je zamišljen kao model informacionog preduzeća, čiji je dalji razvoj baziran na većem broju aktivnosti u elektronskom okruženju [10].

Putanje od 1 do 17 sa slike 1 određuju relacije između učesnika i imaju sledeće značenje:

1. korisnik inicira plaćanje karticom na sajtu trgovca
2. sajt trgovca redirektuje korisnika na PGW
3. korisnik unosi podatke sa kartice kojom plaća
4. PGW proverava Internet BIN tabelu
5. PGW redirektuje korisnika na sajt izdavaoca za autentifikaciju
6. izdavalac autentifikuje korisnika i pamti ishod
7. izdavalac redirektuje korisnika na PGW
8. PGW proverava ishod autentifikacije kod izdavaoca
9. izdavalac šalje odgovor PGW o ishodu autentifikacije



Slika 1. – *Arhitektura sistema za plaćanje preko Interneta korišćenjem DINA kartice*

10. PGW generiše autorizacioni zahtev ka DinaCard sistemu
11. PGW dobija autorizacioni odgovor
12. PGW obaveštava korisnika o ishodu transakcije
13. PGW pokreće finansijsku transakciju i transakcija ulazi u mrežu za plaćanje
14. banka kupca plaća banci trgovca
15. banka trgovca prihvata plaćanje
16. banka trgovca obaveštava trgovca
17. banka kupca obaveštava kupca

Nacionalni Centar za platne kartice distribuira svim Payment Gateway provajderima tabelu registrovanih izdavalaca kartica za plaćanje na Internetu na teritoriji Republike Srbije, takozvanu Internet BIN tabelu, i serverske SSL sertifikate izdavalaca. Na osnovu toga, Payment Gateway provajder obavlja funkcije provere neophodnosti autentifikacije i vrši njeno iniciranje korišćenjem podataka iz Internet BIN tabele. Pored toga Payment Gateway provajder je u obavezi da proveri verodostojnost serverskog SSL sertifikata izdavaoca.

Korisnik na sajtu trgovca bira željene proizvode, zaključuje kupovinu, unosi potrebne podatke o adresi za dostavljanje kupljene robe i inicira plaćanje karticom. Sajt trgovca, zatim redirektuje korisnika na sajt Payment Gateway provajdera, gde korisnik popunjava formular unošenjem podataka o kartici kojom se plaća.

Na osnovu BIN-a banke iz unetog PAN-a provajder proverava u svojoj Internet BIN tabeli da li je izdavalac kartice registrovan za plaćanje na Internetu. U slučaju da izdavalac kartice nije registrovan Payment Gateway provajder odbija transakciju i o tome obaveštava korisnika. Ukoliko je izdavalac kartice registrovan za online plaćanje, Payment Gateway provajder proverava u Internet BIN tabeli da li je za taj BIN obavezna autentifikacija korisnika.

Ukoliko je autentifikacija korisnika obavezna Payment Gateway provajder redirektuje korisnika na sajt izdavaoca za autentifikaciju. Isprekidane linije sa slike 1 se odnose na dodatnu autentifikaciju korisnika, koja se odvija u dve faze.

Prva faza autentifikacije odvija se između korisnika i izdavaoca kartice. Izdavalac kartice može po svom izboru da odredi način autentifikacije korisnika, pošto o tome obavesti i dobije dozvolu od Nacionalnog Centra za platne kartice. Nezavisnost procesa autentifikacije između korisnika i izdavaoca od ostatka sistema daje mogućnost izdavaocima da koriste najsavremenija rešenja za autentifikaciju, kao što su tokeni, čip kartice ili biometrijske metode. Izdavaoci kartica treba da praktikuju višefaktornu autentifikaciju, što podrazumeva kombinovanje više različitih metoda u cilju povećanja bezbednosti.

Jedan od primera je višestruka autentifikacija kombinacijom lozinke, PIN-a i čip kartice što predstavlja tipično multifaktorno rešenje autentifikacije gde se kombinuje "nešto što korisnik zna" i "nešto što korisnik ima". Na primer, lozinka i token uređaj kao što je čip kartica. Na taj način, u slučaju da korisnik izgubi čip karticu, ona ne može biti upotrebljena bez poznavanja lozinke i PIN-a. Mere zaštite koje treba primeniti pri autentifikaciji putem lozinke obuhvataju ograničenje vremenskog opsega kada korisnik može da se uloguje u sistem kao i ograničenje broja pokušaja unosa korisničkog imena i lozinke. Kada sistem registruje pokušaje napadača, treba predvideti automatsko slanje e-mail-a ili sms-a administratoru. Čip kartica je elektronski uređaj veličine platne kartice sa ugrađenim mikroprocesorom i memorijom koja se koristi za identifikaciju korisnika i nalazi se u vlasništvu autorizovanog korisnika. Informacije o korisniku, digitalni sertifikat i ključevi za kriptovanje su sigirno smeštani u kartici. Prema

opisanoj arhitekturi za plaćanje na Internetu, prva faza autentifikacije se odvija između kupca i izdavaoca kartice. Na sajtu izdavaoca kupac unosi lozinku i PIN. Zatim se od njega traži odgovarajući sertifikat. Kupac tada unosi čip karticu u čitač čip kartice. Čitač razmenjuje podatke sa autentifikacionim serverom izdavaoca koji poseduje verodostojan serverski SSL sertifikat. Po završetku autentifikacije izdavalac redirektuje korisnika na sajt Payment Gateway provajdera koji ponovo proverava ishod autentifikacije, na osnovu baze podataka o autentifikaciji izdavaoca.

Kao drugi primer može se navesti višestruka autentifikacija kombinacijom lozinke i otiska prsta, pri čemu se kombinuje "nešto što korisnik zna" kao što je lozinka i "nešto što korisnik jeste" kao što je otisak prsta. Autentifikacija otiskom prsta nudi moćniju i sigurnu autentifikaciju identiteta korisnika u poređenju sa ostalim metodama. Međutim ova metoda još uvek spada u jako skupe metode, što se svakako može navesti kao mana, naročito ako se govori o online plaćanju kod nas. Međutim, rešenja zasnovana na biomertiji podrazumevaju i kriptovanje biometrijskih podataka, odnosno otiska prsta, što dodatno povećava sigurnost. U skladu sa opisanom arhitekturom za online plaćanje, autentifikacija između korisnika i izdavaoca kartice započinje na sajtu izdavaoca kada korisnik unosi svoju lozinku. Zatim se od njega traži podatak otiska prsta. Korisnik tada skenira otisak prsta preko posebnog digitalnog skenera za otisak prsta. Kriptovani otisak prsta se šalje ka autentifikacionom serveru izdavaoca. Po izvršenoj transmisiji podataka, sledi odgovor o konačnoj identifikaciji korisnika. Dalji korak je redirekcija korisnika sa sajta izdavaoca na sajt Payment Gateway provajdera koji ponovo proverava ishod autentifikacije kod izdavaoca, na već opisan način.

Druga faza autentifikacije je provera ishoda autentifikacije između provajdera i izdavaoca.

Dodatna autentifikacija korisnika prilikom online plaćanja je opcija na strani izdavaoca kartice. Proces dodatne autentifikacije ne zavisi od trgovca i svi Payment Gateway provajderi su u obavezi da podrže ovu funkcionalnost. Realizacija autentifikacije na strani izdavaoca kartice garantuje da će svaka online transakcija platnom karticom tog izdavaoca biti autentifikovana. To je još jedna razlika u odnosu na druge internacionalne platne sisteme gde funkcija autentifikacije zavisi i od realizacije na strani trgovca.

Proces autentifikacije korisnika prilikom plaćanja na Internetu započinje na strani Payment Gateway provajdera. Kada dobije podatke od korisnika o platnoj kartici kojom se vrši plaćanje, Payment Gateway provajder na osnovu Internet BIN tabele proverava da li je izdavalac kartice registrovan za online plaćanje i da li postoji mogućnost autentifikacije korisnika. Ukoliko su oba uslova zadovoljena, Payment Gateway provajder redirektuje korisnika na sajt izdavaoca kartice, pri čemu se proces autentifikacije odvija direktno između korisnika i izdavaoca. Po završenoj autentifikaciji izdavalac redirektuje korisnika na sajt Payment Gateway provajdera.

Podatke o ishodu autentifikacije, izdavalac kartice za online plaćanje pamti u svojoj bazi podataka. Na osnovu toga, Payment Gateway provajder proverava ishod autentifikacije kod izdavaoca. Prema dobijenoj informaciji o ishodu autentifikacije Payment Gateway provajder odbija transakciju ili je pokreće. Kada je finansijska transakcija odobrena ona dalje ulazi u mrežu za plaćanje.

Format i nazivi ulaznih parametara Payment Gateway provajdera i odgovora izdavaoca platnih kartica su precizno definisani Tehničkom specifikacijom DinaCard sistema. Payment Gateway provajder je u obavezi da proveri verodostojnost serverskog SSL sertifikata izdavaoca. U slučaju neuspešne provere sertifikata izdavaoca kartica, Payment Gateway provajder odbija transakciju. Izdavalac je tada u obavezi da tu transakciju u svojoj bazi podataka označi kao završenu i u slučaju dobijanja zahteva za proveru već završene autentifikacije pošalje odgovor da je autentifikacija neuspešna. Na taj način se dodatno povećava sigurnost autentifikacije.

Završni koraci u online plaćaju, prema opisanoj arhitekturi sistema plaćanja, odvijaju se između banke kupca i banke trgovca. Banka kupca plaća banci trgovca koja prihvata plaćanje. Po završetku plaćanja, banka kupca obaveštava kupca da je plaćanje izvršeno, dok banka trgovca obaveštava trgovca da je plaćanje završeno.

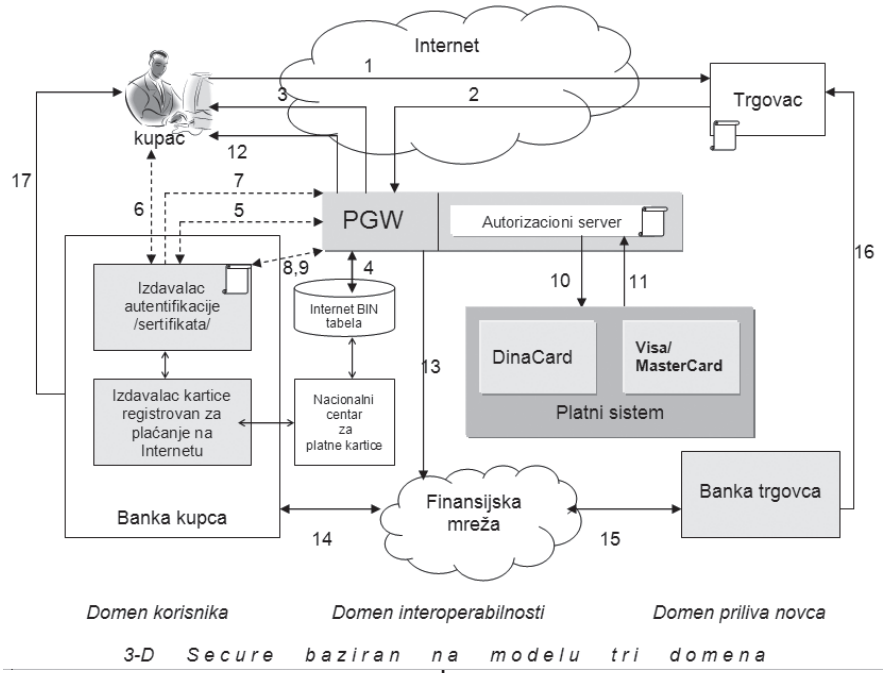
Dalji razvoj opisanog sistema za online plaćanje, pored mogućih novih servisa za korisnike potrebno je usmeriti ka unapređenju sistema zaštite, uvođenjem dodatnih mehanizama zaštite učesnika plaćanja na Internetu, u skladu sa postojećim rešenjima i trendovima u svetu. Pored toga, prikazanu arhitekturu je moguće modifikovati i obogatiti softverskim paketima da bi se postigla 3-D Secure zaštita, i na taj način omogućilo korišćenje drugih vrsta platnih kartica.

3. ARHITEKTURA SISTEMA ZA PLAĆANJE DRUGIM TIPOVIMA KARTICA

Modifikovana arhitektura sistema za on-line plaćanje sa slike 1 prilagođena je implementaciji 3-D Secure zaštite i prikazana je na slici 2. Putanje sa šeme na slici 2 od 1-16 u principu imaju isto značenje kao i putanje na slici 1. Glavna razlika između dve arhitekture je u proširenosti platnog sistema i dodatnim ulogama na strani izdavaoca kartice i Payment Gateway provajdera dok trgovac i dalje ostaje rastrećen. Proširenje platnog sistema, bazirano na upotrebi dodatnih softvera, otvara mogućnost za upotrebu VISA i MasterCard kartica.

Kada je reč o zaštiti baziranoj na tri domena, bilo da se radi o tipu *Verified by VISA*, odnosno *MasterCard SecureCode*, zahteva se postojanje dodatnog softvera na strani sajta trgovaca i na strani izdavaoca koji vrši autorizaciju transakcija, prema postojećem standardu. Trgovcima se najčešće nudi softverski modul za funkcionalnost 3-D Secure zaštite, koji treba da ugrade u postojeći sajt, ili veći softverski paket za plaćanje na Internetu sa raznim servisima. Izdavaoci kartica za plaćanje na Internetu pored obimnih softverskih zahteva za realizaciju 3-D Secure zaštite, moraju proći i zahtevan proces sertifikacije. 3-D Secure zaštita povećava poverenje korisnika u kupovinu online jer so oni, izdavalac kartice i trgovac deo jednog tima koji ima za cilj da ostvari bezbednu online trgovinu.

Modifikovana arhitektura za plaćanje upotrebom drugih vrsta platnih kartica, kao što su VISA i MasterCard kartice, se razlikuje od opisanog standarda, jer je predviđeno da softverski modul za funkcionalnost 3-D Secure zaštite, bude ugrađen u sajt Payment Gateway provajdera. Na taj način trgovac i dalje ostaje rasterećen, dok je uloga i nivo aktivnosti Payment Gateway provajdera još veća u odnosu na opisanu arhitekturu plaćanja sa slike 1.



Slika 2. – *Modifikovana arhitektura sistema za plaćanje preko Interneta korišćenjem drugih vrsta platnih kartica*

Internet BIN tabela treba da bude proširena i da sadrži dodatne spiskove registrovanih izavalaca drugih kartica za online plaćanje na teritoriji Republike Srbije. Za ažuriranje Internet BIN tabele zadužena je banka, izdavalac kartice za online plaćanje, koja poseduje dozvolu za izdavanje VISA i MasterCard kartica za plaćanje na Internetu u Republici Srbiji i Nacionalni Centar za platne kartice. Banka izdavalac VISA i MasterCard kartica šalje podatke sa tabelom registrovanih korisnika VISA i MasterCard kartica za online plaćanje u Republici Srbiji Nacionalnom Centru za platne kartice. Podaci se distribuiraju svim Payment Gateway provajderima zajedno sa tabelom registrovanih izdavalaca kartica za plaćanje na Internetu i serverskim SSL sertifikatima izdavalaca. Na taj način Payment Gateway provajderi koriste proširenu Internet BIN tabelu u slučaju upotrebe kartica za online plaćanje. Pored toga, platni sistem je proširen sa DinaCard sistema, tako da podržava i ostale platne sisteme, kao što su Visa i MasterCard.

Slično kao u prethodnom rešenju, Payment Gateway provajder proverava spisak registrovanih korisnika za online plaćanje. Ako je korisnik registrovan za plaćanje, Payment Gateway provajder redirektuje korisnika na sajt izdavaoca kartice. U ovom slučaju izdavalac kartice ima odgovarajući softver za podršku 3-D Secure zaštitu i odgovarajući sertifikat. Realizacija autentifikacije se vrši na strani izdavaoca, tako da je i u ovoj funkciji trgovac rasterećen. Autentifikacija koja se odvija direktno između korisnika i izdavaoca kartice pruža mogućnost korišćenja savremenih metoda kao što je predloženo.

Alternativna arhitektura sistema modifikovanom predlogu arhitekture za plaćanje na Internetu, sa slike 2 zasniva se na integraciji programa Verified by VISA ili MasterCard SecureCode za kupovinu na Internetu, na postojeći e-komerc sistem trgovca i predstavlja sledeći korak migracije arhitekture ka internacionalnim rešenjima. Pri tome VISA i MasterCard sertifikuju glavne učesnike u sistemu: izdavaoca kartice, trgovca i Payment Gateway provajdera. U ovom slučaju dolazi do izražaja promenjena uloga trgovca u odnosu na prethodno opisana rešenja. Glavna razlika je u tome što ovde trgovac zahteva autorizaciju od PGW-a, linija 11 sa slike 3, dok u prethodnim rešenjima taj zahtev nije bio predviđen. VISA i MasterCard modul koji se nalaze kako na slici 2 tako i na slici 3 ukazuju na postojanje odgovarajućih sertifikata, kao i na mogućnost jednostavne modifikacije u okviru datih šema u okviru datih potreba. Na ovaj način bi se procesirale kartice izdate od banaka sa teritorije Republike Srbije. Kako je ovim rešenjem trgovac u obavezi da bude učlanjen i poseduje odgovarajuće sertifikate da bi mogao da koristi usluge Verified by VISA ili MasterCard SecureCode, postoji mogućnost upotrebe kartica izdatih u inostranstvu tako što bi trgovac redirektovao korisnika na sajt servisa Verified by VISA ili MasterCard SecureCode, pri čemu se autentifikacija korisnika obavlja između izdavaoca kartice i trgovca.

Vlasnici kartice su takođe u obavezi da registruju kartice kod svojih izdavalaca kartica na njihovom sajtu, da bi mogli da dobiju usluge servisa Verified by VISA. Prema alternativnoj arhitekturi sistema sa slike 3 ulogu servisa Verified by Visa kada je u pitanju provera spiska registrovanih korisnika, obavlja Payment Gateway provajder. Payment Gateway provajder to radi na već opisan način, koristeći proširenu Internet BIN tabelu. Kada izdavalac kartice registruje korisnika za plaćanje na Internetu, podaci se automatski prosleđuju bazi podataka Nacionalnog centra za platne kartice, koji takođe automatski prosleđuje podatke u proširenu Internet BIN tabelu.

MasterCard SecureCode takođe zahteva da bude inkorporiran u sajt trgovca, tako da se sve transakcije obavljaju prolaskom autentikacije kroz MasterCard Universal Autentication Field, što opet prema alternativnoj arhitekturi sa slike 3 obavlja Payment Gateway provajder.

Putanje od 1 do 19 sa slike 3 imaju sledeće značenje:

1. korisnik inicira plaćanje na sajtu trgovca unošenjem VISA ili MasterCard broja i klikne na dugme za kupovinu.
2. sistem na sajtu trgovca proverava da li se uneti VISA ili MasterCardSecureCode nalazi na spisku registrovanih korisnika i redirektuje korisnika na PGW koji ima ulogu servisa za proveru
3. korisnik unosi lični pasvord na sajtu PGW
4. PGW proverava proširenu Internet BIN tabelu
5. PGW redirektuje korisnika na sajt izdavaoca za autentifikaciju
6. izdavalac autentifikuje korisnika i pamti ishod
7. izdavalac redirektuje korisnika na PGW
8. PGW proverava ishod autentifikacije kod izdavaoca
9. izdavalac šalje odgovor PGW o ishodu autentifikacije
10. PGW šalje poruku trgovcu o statusu autentifikacije
11. trgovac traži autorizaciju od PGW
12. PGW generiše autorizacioni zahtev ka platnom sistemu
13. PGW dobija autorizacioni odgovor
14. PGW obaveštava korisnika o ishodu transakcije
15. PGW pokreće finansijsku transakciju i transakcija ulazi u mrežu za plaćanje
16. banka kupca plaća banci trgovca
17. banka trgovca prihvata plaćanje
18. banka trgovca obaveštava trgovca
19. banka kupca obaveštava kupca

Rešenje sa slike 3 povećava poverenje korisnika u kupovinu online jer su oni, izdavalac kartice, Payment Gateway provajder i trgovac deo jednog tima koji ima za cilj da ostvari bezbednu online trgovinu. Na osnovu dobijene informacije o ishodu autentifikacije PGW odbija transakciju ili je pokreće. Kada je finansijska transakcija odobrena ona dalje ulazi u mrežu za plaćanje, kao u rešenju sa slike 1.

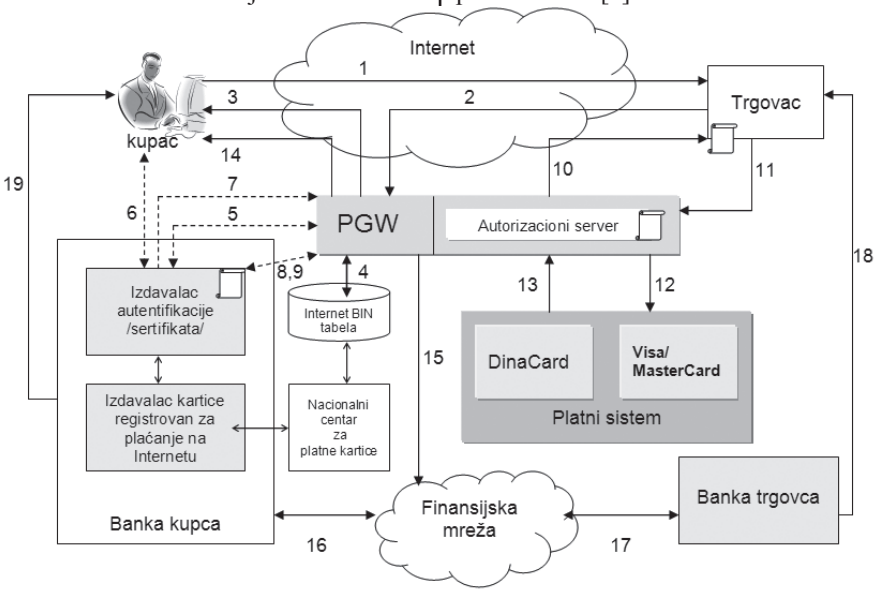
"Parametar" koji bi odgovarao nivou aktivnosti PGW-a menja se od slike 1 do slike 3 raste zajedno sa migracijom arhitekture sistema za plaćanje, od specifičnog domaćeg rešanja DinaCard sistem ka sistemima sličnijim internacionalnim rešenjima, zasnovanim na 3D Secure zaštiti. U sve tri prikazane arhitekture, zadržana je ideja da PGW proverava da li je dodatna autentifikacija potrebna, a zatim je inicira i proverava. Dalja modifikacija arhitekture opisanih sistema mogla bi da ide u smeru porasta "parametra" nivoa aktivnosti PGW-a, pri čemu bi se njegovoj opisanoj delatnosti dodao servis za proveru spiska registrovanih korisnika, kao što je na primer servis Verified by VISA.

Drugom varijantom rešenja najveći deo aktivnosti bi se prebacio na trgovca, što se idejno približava već postojećim svetskim standardima. Kao što je već opisano, intemplementacija 3D Secure zaštite tipa Verified by Visa ili MasterCard SecureCode uključila bi dodatne softvere na strani sajta trgovca i na strani izdavaoca koji vrši autorizaciju transakcija. Kao i u opisanim rešenjima trgovci bi koristili softverski modul za funkcionalnost 3D Secure zaštite, koji treba da ugrade u postojeći sajt, ili softverski paket za online plaćanje sa raznim servisima. Izdavaoci kartica bi takođe morali da ispune softwerske zahteve za realizaciju 3D Secure zaštite. Svi učesnici u sistemu bi morali da poseduju zahtevane sertifikate.

4. TEHNIKE ZAŠTITE U SISTEMIMA ZA PLAĆANJE PREKO INTERNETA

Kada se govori o tehnikama zaštite sistema za plaćanje na Internetu, pre svega, potrebno je napomenuti da svi članovi u sistemu, izdavalac kartice, provajder i trgovac treba da budu korektno usklađeni, da bi se uklonila opasnost od kompromitovanja podataka sa kartice. Pored toga, pojava individualnih brendova kartica, nikako ne sme da dovede do neadekvatne podrške što može dovesti do opoziva privilegija kartičnog servisa.

Prema postojećem standardu za sigurnost sistema za online plaćanje PCI SSC- *Payment Card Industry Data security Standard*, neophodno je da predviđene tehnike zaštite zadovolje šest glavnih kategorija sa dvanaest osnovnih zahteva prikazanih u tabeli 1, sa ciljem eliminisanja mogućnosti prevare upotrebom platne kartice [3].



3-D Secure baziran na modelu tri domena

Slika 3. – *Alternativna arhitektura sistema modifikovanog predloga arhitekture za plaćanje preko Internta korišćenjem VISA i MasterCard kartica*

KATEGORIJE		ZAHTEVI	
1	izgradnja i održavanje sigurne mreže	1	instalacija i održavanje firewall konfiguracije za zaštitu podataka
		2	ne koristiti default za sistem i drugih parametara bezbednosti na strani trgovca
2	zaštita podataka sa kartice	3	zaštita sakupljenih podataka
		4	kriptovanje transmitovanih podataka sa kartice i osetljivih informacija kroz javnu mrežu
3	upranljanje programom za izdržavanje ranjivosti sistema	5	upotreba regularno update-ovanog antivirus softwera
		6	razvoj i održavanje sistema i aplikacija za bezbednost
4	implemantacija strogih mera kontrole pristupa	7	ograničen pristup podacima prema tome ko treba da zna određene poslovne podatke
		8	dodeliti jedinstvan ID svakoj osobi koja pristupa sa kompjutera
		9	ograničiti fizički pristup podacima o koricima kartica
5	regularni monitoring i testiranje svih mreža	10	snimanje i monitoring svih pristupa mrenžnim resursima i podacima o kicimc kartica
		11	regularno testiranje sistema bezbednosti i procesa
6	održavanje politike za informacionu bezbednost	12	održavanje politike koja je usmerena na informacionu bezbednost

Tabela 1. – *Zahtevi tehnika zaštite po kriterijumima, prema standardu PCI SSC*

	Instalacija i održavanje Firewall konfiguracije za zaštitu podataka			
	Firewall	Tehnologije	Autentifkacione šeme	Zahtev standarda PCI SSC
IZGRADNJA I ODŽAVANJE SIGURNE MREŽE	– ruteri – host kompjuteri – "proxy" serveri	– HTTP – SSL – TLS – SSH – VPN – IP/ IP maskiranje (REC 1918 sa port adresom PAT ili NAT)	**- RADIUS** – SecureID – PKI	RADIUS+VPN
	Default za sistem lozinke i parametre bezbednosti na strani trgovca ne treba koristiti			
	– Firewall – VPN – SNMP-Simple network management protocol – Kriptovanje svih administrativnih pristupa: SSH,VPN,SSL/TLS			

Tabela 2. – *Pregled osnovnih tehnika zaštite koje se primenjuju za izgradnju i održavanje sigurne mreže*

Podaci o korisniku kartice broj računa PAN *Primary Acount Number*, ime korisnika, kod servisa i datum važenja moraju biti zaštićeni ako se čuvaju zajedno sa PAN-om. Zaštita mora biti ostvarena prema generalnim zahtevima standarda za zaštitu okruženja korisnika kartice. Takođe osetljivi podaci za autentifikaciju moraju biti zaštićeni, i ne smeju se sačuvati nakon autentifikacije. Ovi zahtevi bezbednosti treba da se odnose na sve komponente sistema: komponenete mreže, servere ili aplikacije koje su povezane sa okruženjem korisnika kartice. Adekvatna segmentacija mreže, koja izoluje sisteme za čuvanje, procesiranje i slanje podataka korisnika kartice, smanjuje domet okruženja korisnika kartice. Komponente mreže uključuju firewall-ove, svičeve, rutere, bežične tačke pristupa, mrežne uređaje i druge uređaje za ostvarenje bezbednosti. Tipovi servera uključuju web, baze podataka, autentifikaciju, mail, proxy, *network time protokol* (NTP) i *domain name server* (DNS). Aplikacije obuhvataju sve korisničke i prodajne aplikacije, uključujući interne i eksterne Internet aplikacije.

Standard signosti podaka PCI SSC podrazumeva kriptovaje podataka u prenosu, kotrolu pristupa, uništavanje podataka i slušanje. Standard ja dizajniran prema potrebama sigurnosti trgovaca. Podaci se kriptuju na POS sistemima od trenutka prihvatanja kartice preko procesiranja podataka i brisanja.

Standard treba da zadovolje kako trgovci tako i servis provajderi koji skladište, procesiraju ili prosleđuju podatke sa kartice. Na taj način se ostvaruje potrebni minimum kada su u pitanju mere bezbednosti. Standard prvenstveno pruža zaštitu podataka vlasnika kartica.

Zaštita računarskih mreža je kompleksan zadatak i zahteva pažljivo istraživanje, planiranje i implementaciju, sa ciljem da se postigne "razumna predostrožnost" i bezbednost poverljivih i privatnih elektronskih informacija [6]. Zaštita podataka obuhvata tri osnovne oblasti, koje se odnose na različite delove zaštite računarskih sistema. Efikasan plan zaštite mora da sadrži procenu rizika, odgovarajući strategiju i metode za svaku pojedinačnu oblast, što obuhvata fizičke mere zaštite, operativne mere zaštite, upravljanje i politiku bezbednosti [7]. Kada je reč o zaštiti računarskih sistema, svaki učesnik u prikazanoj arhitekturi, korisnik, trgovac, banka i PGW moraju se posmatrati kao celina, uz evidentiranje svih problema koji imaju uticaj na zaštitu. Radi postizanja bolje efikasnosti celog sistema, neophodno je pažljivo planiranje, izvršavanje i monitoring svakog učesnika u sistemu [9]. Snažno upravljanje bezbednošću celog sistema treba da bude usmereno dobrim poznavanjem tehnologija i aktuelnih spornih pitanja [8].

U tabelama koje slede prikazan je pregled najvažnijih tehnika zaštite u sistemima za plaćanje na Internetu. Tabele su grupisane prema najbitnijim zahtevima koje je neophodno ispuniti u obezbeđenju sistema za online plaćanje:

1. zgradnja i održavanje sigurne mreže, tabela 2
2. zaštita podataka korisnika kartica, tabela 3
3. kontrola pristupa, tabela 4

ZAKLJUČAK:

Internacionalna rešenja za plaćanje na Internetu podrazumevaju proveru autentifikacije korisnika u okviru svojih servisa, kao što je to servis Verified by Visa ili MasterCard Universal Autentication Field. Kod internacionalnih rešenja provera neophodnosti dodatne autentifikacije vrši se na strani trgovca pomoću dodatnog softverskog modula, tako da se ceo proces autentifikacije obavlja između korisnika trgovca i izdavaoca, što znatno usložnjava mere zaštite na strani izdavaoca.

ZAŠTITA PODATAKA	**Zaštita sačuvanih podataka korisnika kartica**	
	Kriptovanje-primarna metoda	Kompenzaciona kontrola
	– nečitljiv prikaz primarnog broja računa: ▪ jaka jednosmerna hash funkcija ▪ odsecanje ▪ indeks tokeni – generacija jakih ključeva, sigurna distribucija ključeva, sigurno čuvanje ključeva, periodično menjanje ključeva, uništavanje starih ključeva, prevencija od neautorizovane zamene ključeva, opiziv starih i nevazećih ključeva.	– dodatna segmentacija na mrežnom nivou – restrikcija pristupa podacima korisnika kartice ili bazama podataka – ograničen logički pristup bazama podataka – kontrola logičkog pristupa bazama podataka nezavisno od Active Directory ili Lightweight Directory Access Protocol (LDAP) – zaštititi/detektovati moguće napade na aplikaciju ili baze podataka (SQL injection)
	Kriptovanje transmitovanih podataka sa kartice i osetljivih informacija kroz javnu mrežu	
	Javna mreža	Bežični prenos
	– SSL – TLS – IPSEC.	– WiFi zaštićeni pristup – WPA ili WPA2 tehnologije – IPSEC VPN ili SSL/TLS – 104-bitni ključ za kriptovanje – 24 bitni nivo inicijalizacije – Kontrolu pristupa je potrebno bazirati na MAC adresi
	Antivirus softveri ili programi	**Razvijanje i održavanje sigurnih sistema i aplikacija**

Tabela 3. – *Pregled osnovnih tehnika zaštite podataka*

KONTROLA PRISTUPA	**Ograničen pristup podacima**		
	autorizacija - osetljivim podacima mogu da pristupe samo autorizovane osobe		
	Jedinstven ID za svaku osobu koja pristupa sa kompjutera		
	Autentifikacija		
	korisnika		zaposlenih/administratora
	višestruka autentifikacija, dvo-faktorna, tro-faktorna		dvo-faktorna autentifikacija za udaljen pristup mreži
	Metode autentifikacije: – password – token uređaj ▪ SecureID ▪ Sertifikate ▪ javni ključ – biometrija	– pasvord/otisak prsta – pasvord/PIN/čip kartica	Tehnologije: – RADIUS – TACACS sa tokenima – VPN (baziran na SSL/TLS ili IPSEC) sa individualnim sertifikatima.
	Ograničen fizički pristup podacima o korisnicima kartica		
	•brave •alarmi •detektori •čuvari •kamere		

Tabela 4. – *Pregled osnovnih tehnika zaštite za kontrolu pristupa*

Specifičnost domaćeg rešenja opisanog u radu za plaćanje na Internetu u DinaCard sistemu u odnosu na internacionalna rešenja je u izrazito zahtevnoj ulozi Payment Gateway provajdera, koji obavlja proveru neophodnosti autentifikacije, vrši njeno iniciranje a zatim ponovo proverava ishod autentifikacije kod izdavaoca što dodatno povećava bezbednost celog sistema. Opisana modifikacija prikazane arhitekture sistema za online plaćanje predstavlja migraciju sa specifično domaćeg rešenja ka internacionalnim rešenjima što se ogleda u porastu "parametra" koji odgovara nivou aktivnosti PGW. Na taj način se otvara mogućnost razvoja provajdera u elektronsko preduzeće u elektronskom okruženju, što može biti veoma značajno u domaćim uslovima. Iako se sama arhitektura sistema na taj način dodatno komplikuje, bezbednost sistema raste, jer pored sertifikovanih učesnika, dodatnu kontrolu autentifikacije obavlja provajder.

Tehnike zaštite za sisteme online plaćanja bazirane su na standardu koji treba da zadovolje svi učesnici sistema, kako trgovci tako i servis provajderi. U radu je naveden pregled osnovnih tehnika zaštite sistema za plaćanje na Internetu. Dalji razvoj opisanih sistema može da ide u smeru uvođenja novih servisa za korisnike i daljem unapređenju zaštite korisnika, posebno sa stanovišta bezbedne autentifikacije.

LITERATURA:

[1] www.gbc.t-online.hu
[2] en.wikipedia.org
[3] visaeurope.com
[4] Aleksandar M. Lagator, Milan I. Vidović, Zoran B. Sofilj, Sandra M. Hadži-Ristić, "Plaćanje na Internetu u DinaCard sistemu", VII međunarodna konferencija E-trgovina, Srbija, Palić, 18-20.april, 2007
[5] Nataša Merker, "Platna infrastruktura i bezbednost e-komerc sistema", magistarski rad, 2007
[6] Nataša Ćurčić, Dr Dejan Simić, "Tehnologije zaštite računarskih mreža na mrežnom nivou", časopis za informacione tehnologije i multimedijalne sisteme, Info M, 2004
[7] Mike Pastore, Emmett Dulaney, Security+, 2007
[8] Jill Slay, Andy Koronios, "IT Securitu and Risk Managament", 2006
[9] Yi-chen lan, Bhuvan Unhelkar, "Global enterprise Transitions: Managing the Process", 2005
[10] Andrew S.Targowski, "Electronic Enterprise: Strategy and Architecture", 2003

Natasa Merker, diplpmirani fizicar i specijalista za elektronsko poslovanje,"Politehnika" škola za nove tehnologije, Novi Beograd
Oblast profesionalnog interesovanja: elektronsko poslovanje