UDC: 004.738.5:339 INFO M: str. 12-18

METODOLOŠKI PRISTUP PROCESU ZAŠTITE SISTEMA E-PLAĆANJA
E-PAYMENT SYSTEMS PROTECTION PROCESS - METHODOLOGICAL APPROACH

Marko Vulić, Marko Ranković, Vojkan Vasković

REZIME: Sve masovnija upotreba sistema plaćanja na Internetu dovela je do potrebe da se detaljno prouče postojeći sistemi napada i razrade tehnologije za njihovo sprečavanje. Sistematizacija tehnika napada, analiza primenjene tehnologije i njihovo grupisanje, potrebni su kako bi se razradile metodologije zaštite poslovanja. U radu su detaljno obrađene tehnologije napada koje su u literaturi poznate, ali su proučene i tehnike koje su se kao nove pojavile u proteklom periodu. Tehnike zloupotreba, odnosno prevara koje su posebno analizirane su: "Phishing", "Pharming", "Vishing" i "Phaxing". Analiza ovih metoda napada je rađena sa ciljem da se uoče nedostaci postojećih sistema plaćanja kako bi se u sledeću generaciju tehnologija plaćanja ugradili mehanizmi koji bi sprečili ovakve napade. Takođe su analizirane postojeće tehnike zaštite kako bi se sagledali propusti u njima. U cilju zaštite poslovanja preko Interneta razvijene su mnoge tehnike, a trenutno najperspektivniji od njih je 3D Secure (Three Domain Secure). Bazirajući se na 3-D Secure specifikaciji Visa, MasterCard i Japanski Kreditni Biro su razvili programe: Verified by Visa, MasterCard SecureCode i J/Secure. Rad treba da odgovori na pitanje koliko su postojeći sistemi pouzdani u sprečavanju zloupotreba sistema plaćanja preko Interneta.
KLJUČNE REČI: E-sistemi plaćanja, tehnike krađa na Internetu, VbV, MC SecureCode, J/Secure, metodologija rada VbV
ABSTRACT: The mass usage of the Internet payment systems resulted with need to research the most frequent fraud attacks and to make in-depth analysis of the technologies for fraud prevention. The systematization of the attack techniques, analysis of the technology and the classification of the technologies are needed to develop the methodologies for protection of e-payments processes. This paper deals with the fraud technologies, which are known to the literature, but also describes the new technologies. The fraud techniques, which are especially described are: "Phishing", "Pharming", "Vishing" and "Phaxing". The analysis of these fraud methods has been performed in order to determine the main weaknesses of the payment systems. This will enable the implementation of the security mechanisms into the new-generation payment systems to prevent attack like these. Also, the paper deals, on critical manner, with the existing techniques of protection. In order to protect the business, many techniques have been developed. The most respectable are protection techniques based on the 3-D Secure Specification. The most prominent programs are: Verified by Visa, MasterCard SecureCode and J/Secure, developed by Visa, MasterCard and JBC respectively. This paper should answer the question on how the existing systems are reliable in preventing fraud in the Internet payment systems.
KEY WORDS: E-payment systems, the Internet fraud techniques, VbV, MC SecureCode, J/Secure, VbV methodology

1. UVOD

Svakodnevni razvoj informacionih tehnologija i Interneta pruža sve više mogućnosti korisnicima koji trgovinu obavljaju na Web-u. Sa tim u vezi bitnu ulogu imaju e-sistemi plaćanja. E-sistemi plaćanja moraju biti pogodni za trgovinu na Web-u, lako prenosivi kroz mrežu, dovoljno jaki da spreče elektronske smetnje i troškovno isplativi za male vrednosti transakcija.

Kada se zna da ukupno u svetu ima preko 8.000 različitih sistema plaćanja preko Interneta jasno je da bi se oni analizirali moraju biti podeljeni u grupe po mehanizmima koje koriste.

Najčešće korišćeni e-sistemi plaćanja, podeljeni u grupe, prikazani su u sledećoj tabeli.

Analiziranjem sistema plaćanja datih u *tabeli 1* se jasno može zaključiti da je u domenu plaćanja došlo do konvergencije različitih tehnologija. Ono što posebno pada u oči je da su se kao posebno pogodne tehnologije izdvojile kartice, telefon (mobilni i fiksni) i P2P plaćanja. Karakteristika koja se takođe izdvaja je sve češće povezivanje i mobilnog telefona sa karticama, a preko njih sa bankom. Ovakvo povezivanje otvara nove probleme i rizike, posebno ako se zna da je komunikacija mobilnim telefonima nekriptovana.

2. Prevare na Internetu

Od kada je napravljena prva transakcija novcem preko Interneta bilo je onih koji su želeli da ga zloupotrebe zarad lične koristi. Postoji širok spektar prevara preko Interneta. Na *slici 1* dat je evolutivni prikaz tehnika krađa na Internetu, odnosno prevara, i potom za svaku od tih tehnika dati opisi načina funkcionisanja.

Sa *slike 1* se jasno vidi da su vremenom metodologije napada napredovale u skladu sa tehnologijom koja je primenjivana. Svakako da su i korisnici postajali sve više edukovani sa boljim alatima za zaštitu, a i svi ostali učesnici su postali svesni da Internet poslovanja treba zaštititi. Takođe treba primetiti da su tehnološki napadi sve manje značajni, a da su se napadi preselili u domene socijalnog inženjeringa. Čitava ideja socijalnog inženjeringa sastoji se u tome da se dođe do podataka (broj kartice, PIN, lozinka, ...) preko kojih bi se obavila nelegalna transakcija i opljačkao naivni korisnik.

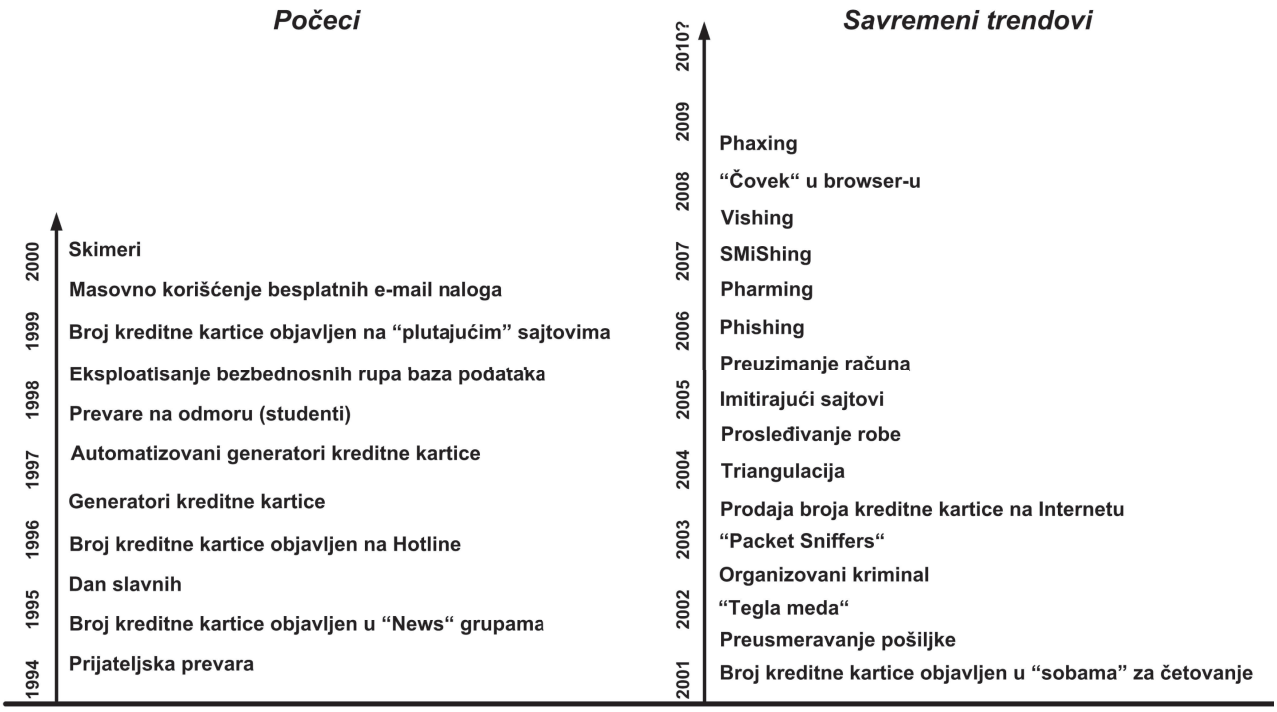
Tehnike krađa na Internetu (prikazane na *slici 1*) i način na koji funkcionišu:

1. *Prijateljska prevara*

Kada potrošač obavlja kupovinu sa Web sajta, a zatim ne prihvati transakciju po prijemu stanja na kreditnoj kartici.

Tabela 1. – *E-sistemi plaćanja*

Sistemi elektronskog novca	CyberCash, NetCash, Ecash, Edram, InternetCash, Mondex, WebMoney, PayByCash, cashU, Ukash, Boleto Bancário, Pago Fácil, Moneybookers, VirtualPayCash, Yandex Money
Electronic Bill Presentment and Payment (EBPP)	BillView, Bill Pay Rout, Striata
E-sistemi plaćanja putem kartica	Hartland, MyPaylinQ, UDPay, INOCard, eNETS, Nochex, Visa, MasterCard, JCB, American Express, Laser, Carte Bleue, SOLO, CartaSi
E-sistemi za mikroplaćanja	Daopey, qPass, eCoin, NetCard, Netpay, Wallie-card, MOLPoints, CLICK2PAY, T-Mobile Micropayment Service
Peer-to-Peer (P2P) sistemi plaćanja	AllCharge, PayPal, Neteller. icWallet
E-sistemi plaćanja preko banke	SWIFT, Fedwire, CHIPS, CertaPay, iDEAL, Giropay, ING Home' Pay, Nordea, POLi, Sofortüberweisung.de, Przelewy24
E-sistemi plaćanja preko računa	BizPay, BidPay, CheckFree, Netbill, Paytrust, INSTADEBIT
E-sistemi plaćanja putem mobilnog i fiksnog telefona	ePoint, LUUP, Movilpago, NTT DoCoMo, Mobipay, Pay@Once, GiSMo, Sonera Mobile Pay, Metax, Paybox, Paiment CB sur mobile, w1pay, Paymo, Pay by Phone, mChek, ICICI Bank iMobile, Rabo Mobile, Citi Mobile, Hal M-Payments, Mobile EMV Chip Debit/Credit, Visa, MasterCard, American Express, PayPal, BPAY, Mobi-karta, domaći sistemi plaćanja putem mobilnih telefona
E-sistemi plaćanja Savezne vlade i pošte	PAID, Pay.gov
E-sistemi plaćanja u zlatu	Pecunix, i-Gold, Digi Gold, E-gold, e-Bullion
Biometrijski sistemi plaćanja	Pay By Touch, OKI
E-sistemi plaćanja putem vaučera	VoucherDigital, QVoucher



Slika 1. – *Evolucija prevara na Internetu [1][4][8]*

2. ***Broj kreditne kartice objavljen u "News" grupama***

Sistem koristi veoma uspešan mehanizam za distribuciju poruka koje prevaranti koriste kako bi prekinuli dostavljanje broja kartice od potrošača.

3. ***Dan slavnih***

Prevaranti pretenduju da budu, da rade za ili budu u vezi sa poznatom ličnošću sa ciljem da izmame informacije od potrošača.

4. ***Broj kreditne kartice objavljen na Hotline***

Ukradene kartice često su u upotrebi još par sati od trenutka prijave krađe do njene blokade, prevaranti su se organizovali da koriste što je brže moguće podatke sa kartice do kojih su došli.

5. ***Generatori kreditne kartice***

Prevarant jednostavno generiše novi broj kreditne kartice, i ubaci ga u Web formular za e-trgovinu.

6. ***Automatizovani generatori kreditne kartice***

Sofisticiran oblik generatora kreditne kartice gde program automatski snabdeva brojevima kreditne kartice.

7. ***Prevare na odmoru (studenti)***

Prevaranti pažljivo biraju vreme da izvrše prestup kada je trgovac prezauzet.

8. ***Eksploatisanje bezbednosnih rupa baza podataka***

Mnogi "rani" Web sajtovi i alati koji su korišćeni za kreiranje sajtova e-trgovine su bili loše napisani i nisu proveravali dovoljno dobro ulazne podatke. Ovo je omogućilo hakerima da pažljivo postave oblikovane podatke u polja za unos podataka tako da izgleda da je aplikativni server zapravo pokrenuo SQL komandu.

9. ***Broj kreditne kartice objavljen na "plutajućim" sajtovima***

"Plutajući sajtovi" su Web sajtovi koji su oteti. Kada je Web server izložen opasnosti od strane hakera, on može instalirati svoj sopstveni Web sadržaj (obično je u pitanju pornografija, piratske kopije softvera, muzika, ali takođe može obuhvatiti i ukradene podatke kartice).

10. ***Masovno korišćenje besplatnih e-mail naloga***

Odsustvo validacije korisnika i postojanje anonimnosti korisnika e-mail naloga omogućava prevarantima u slučaju da budu otkriveni, jednostavno kreiraju drugu adresu.

11. ***Skimeri***

Skimeri su ručni uređaji za skeniranje magnetne trake na kartici.

12. ***Broj kreditne kartice objavljen u "sobama" za četovanje***

Račun kreditne kartice može biti zloupotrebljen od strane nekoliko prevaranata bilo da je kartica fizički ukradena ili presretnuta na mreži.

13. ***Preusmeravanje pošiljke***

Iako podaci vlasnika kartice mogu biti kompletni i adresa verifikovana, prevaranti su u stanju da zatraže od kurira prijem robe na drugom mestu ili presretnu isporuku.

14. ***"Tegla meda"***

Mamac za potrošače - obično ovi sajtovi nude korisnicima "besplatnu probnu verziju", ali samo ako se izvrši pretplata (najčešći primer su sajtovi pornografskog sadržaja).

15. ***Organizovani kriminal***

Organizovane kriminalne bande sada su usmerene na Internet. Omogućeno im je efikasno korišćenje podataka sa ukradenih kreditnih kartica.

16. ***"Packet Sniffers"***

"Packet Sniffers" su legitimne mreže i alati za upravljanje bezbednošću. Međutim oni mogu biti podrivani za dobijanje podataka finansijskih transakcija.

17. ***Prodaja broja kreditne kartice na Internetu***

Neki hakeri ne žele da rizikuju i budu uhvaćeni u varanju brojevima kreditnih kartica, i prodaju ih prevarantima. Direktna nepovezanost prevaranata i žrtve otežava praćenje kriminala.

18. ***Triangulacija***

Prevarant lažno deluje kao legitimni posrednik između potrošača i trgovca. Prevarant reklamira i prodaje artikal (npr. na eBay-u), prima uplate za to i "ispunjava" nalog za korišćenje ukradene kreditne kartice. Ovo je metod prevare koji efikasno generiše novac za prevaranta.

19. ***Prosleđivanje robe***

Špediterske kompanije pružaju usluge dalje isporuke robe, i favorizovane su od strane prevaranata.

20. ***Imitirajući sajtovi***

Lažni Web sajtovi dizajnirani da zbune žrtvu. Mogu biti imitacija legitimnog sajta (npr. ***ebav.com***), ili potpun ali lažan e-trgovinski sajt koji postoji isključivo da bi prikupio brojeve kartica.

21. ***Preuzimanje računa***

Otmica računa presretanjem ili obaranjem sesije. Može se postići i "Phishing"-om ili IRC (Internet Relay Chat) virus metodom.

22. ***"Phishing"***

Mrežna krađa identiteta. Pošiljalac navodi žrtvu da kao odgovor na e-mail unese svoje korisničko ime (username) i šifru (password) za pristup sajtu. Omiljena meta su sajtovi koju pružaju finansijske usluge ili aukcijski sajtovi (eBay).

23. ***"Pharming"***

Reč je o "presretanju". Koncept prevare je da korisnika "na putu" do Web sajta čiju je on-line adresu uneo u browser na računaru, presretne klonirani sajt na koji sa punim poverenjem korisnik unosi svoje podatke. "Provalnici" obično napadaju bazu kartica, odnosno pre će napasti on-line prodavnicu koja radi sa određenom bankom, a ne samu banku.

24. ***"SMiShing" (SMs phISHING)***

SMS pecanje. Tekstualna poruka biva poslata na mobilni telefon pojedinca u pokušaju da se otkriju lične informacije, na taj način što prispela poruka usmerava korisnika da pozove određeni broj telefona ili da poseti Web sajt za potvrdu ličnih podataka.

25. ***"Vishing"***

Korišćenje telefonskog sistema za pristup ličnim i finansijskim informacijama korisnika. Napad se nekada kombinuje sa e-mailom u kome "banka" obaveštava korisnika o grešci u vezi sa on-line nalogom. Zatim se zahteva da se korisnik javi na određeni broj telefona naveden u e-mailu, prati uputstva automata i unese broj kartice ili računa kako bi se proverili nastali problemi.

26. ***"Čovek" u browseru***

Presretanje toka podataka od korisnika ka on-line nalogu. Trojanac "ugrađen" u korisnikov browser može biti programiran da se aktivira prilikom pristupa određenim sajtovima na mreži od strane korisnika, kao što su Web stranice banaka.

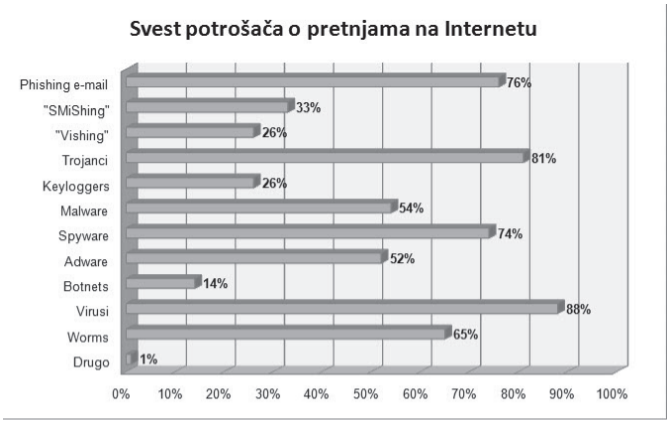
27. ***"Phaxing"***

Kriminalci se predstavljaju kao banka ili određena kompanija, i šalju poruke putem faksa. U faksu dostavljaju URL adresu i traže od žrtve da ih kontaktira preko nje na Internetu.

Zaštitu od ovakvih napada je teško organizovati. Značajan segment populacije korisnika Interneta predstavljaju ljudi koji malo znaju o problemima zaštite ili pripadaju grupi koja se povodi za rečenicom: "Neće to baš meni da se desi", a njima se po pravilu najčešće dešava. Ovo je poznato i napadačima tako da

uvek postoji deo populacije koji će biti izložen (uvek kad uđete u autobus gradskog saobraćaja možete biti odžepareni). Jedino rešenje za ovaj problem je edukovanje korisnika, jer ako oni sami sebe ne štite niko ih ne može zaštititi.

Drugi deo zaštitnih mehanizama je u tehnološkim strogo formalizovanim metodologijama koje neće dopustiti korisniku da svojim nemarom ili neznanjem bude pokraden. Ovo se pre svega odnosi na tehnološka rešenja smart kartica i korišćenje PKI infrastrukture za autentifikaciju i autorizaciju korisnika i transakcija.



Slika 2. – *Svest potrošača o pretnjama na Internetu [6]*

Slika 3. – *Evolucija Phishing napada [7]*

Sa grafikona prikazanog na *slici 2* uočava se da svesnost potrošača o mogućim napadima na Internetu tokom on-line trgovine i plaćanja, nije u dovoljnoj meri razvijena u poređenju sa postojećim vrstama napada prikazanim na *slici 1*. Pre svega se misli na napade koji su zabeleženi u skorijem periodu, gde osim u anketi pomenutih "Phishinga" (u vezi sa kojim su građani očigledno najviše upoznati), "SMiShinga" i "Vishinga", ne bi trebalo zanemariti "Pharming", "Čovek" u browseru i "Phaxing". Kada je reč o "Phishingu", primetno je da se broj ove vrste napada iz godine u godinu drastično povećavao.

Mora se priznati da je inovativnost i inventivnost napadača na zavidnom nivou. Ako se zna da se gotovo svakodnevno pojavljuju nove tehnologije napada ili prevara, mora se priznati da je teško sve to pratiti, adekvatno upozoravati i edukovati korisnike. Poseban problem je to što se ove metodologije brzo pojavljuju na Internetu u obliku objašnjenja pa to dalje služi za obuku drugima, ali i kao ideja za nove nadogradnje.

3. KLJUČNI ELEMENTI U ZAŠTITI PLAĆANJA PREKO INTERNETA

Tabela 2: Tehnologije zaštite plaćanja na Internetu [1]

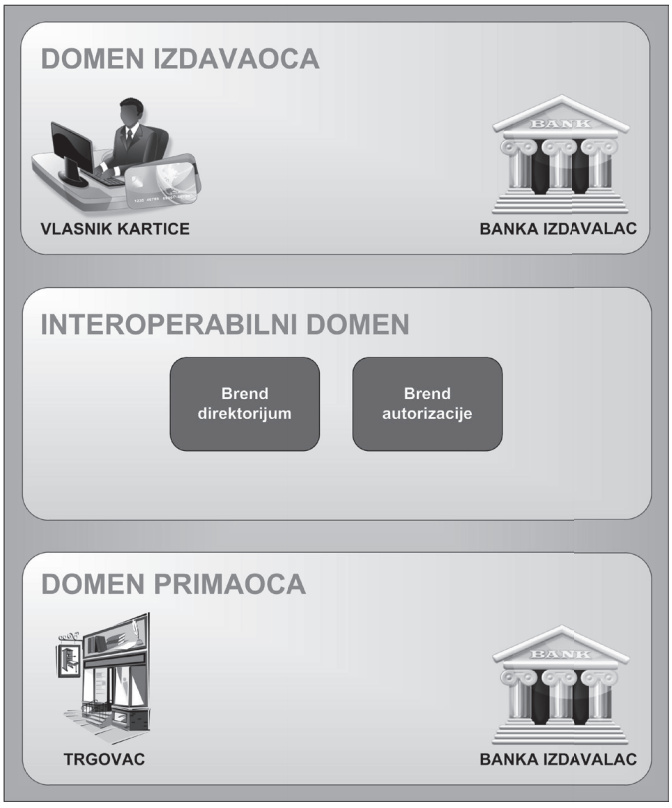
Autentifikacija kupca je najnovija alatka danas dostupna trgovcima u elektronskom poslovanju. Autentifikacija kupca omogućava trgovcu elektronski ekvivalent potpisane priznanice. Visa 3-D Secure inicijativa omogućava Internet trgovcima da učestvuju u autentifikaciji kupaca. MasterCard i Japanski Kreditni Biro (JCB) takođe imaju 3-D Secure (*3-D Secure™ je Visa trademark*) programe: MasterCard SecureCode i J/Secure. Sva tri programa rade na potpuno isti način, rade validaciju korisnika koji kupuje na Web sajtu trgovca. [3]

3.1 *Visa program Verified by Visa*

Verified by Visa (VbV) je program autentifikacije baziran na 3-D Secure Specifikaciji. Sa ciljem eksploatacije široko prihvaćene Secure Socket Layer (SSL) enkripcije, kao Internet tehnologije koja se koristi da se zaštite informacije o platnoj kartici za vreme prenosa preko Interneta, 3-D Secure koristi autentifikaciju korisnika kartice da verifikuje strane uključene u transakciju. [2]

Program VbV je struktuiran kroz tri domena:

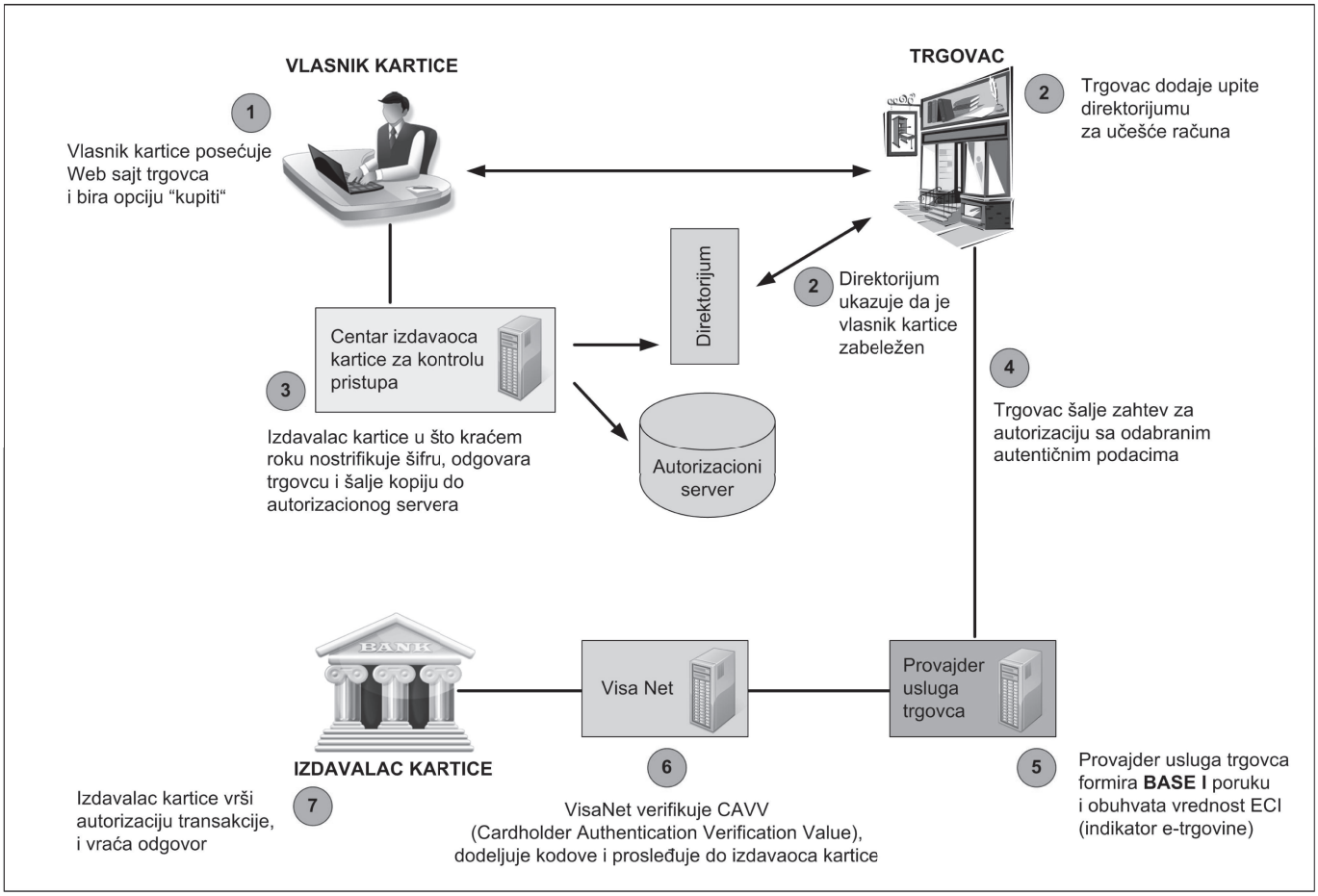
1) Domen izdavaoca;
2) Domen primaoca;
3) Interoperabilni domen.



Slika 4. – *3D Secure [5]*

Učesnici u VbV su:

- **Izdavalac** – finansijska institucija koja izdaje Visa karticu klijentima;



Slika 5. – *Verified by Visa proces transakcija [11]*

- **Vlasnik kartice** – vlasnik računa Visa platne kartice;
- **Primalac** – finansijska institucija koja potpisuje ugovor sa trgovcem za prihvatanje Visa platnih kartica;

Slika 6. – *Prednosti Verified by Visa [9]*

- **Trgovac** – nudi trgovačke ili servise na Web sajtu, i prihvata uplate od korisnika Visa kartica koji kupuju preko Interneta;
- **VisaNet** – sistem i usluge, uključujući Visa Integrisan Platni Sistem i BASE II.

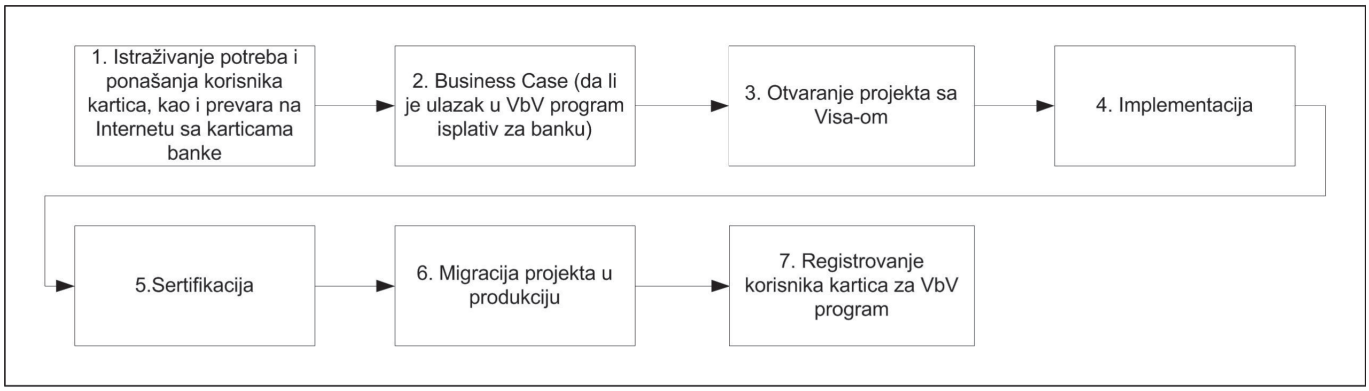
3.2 *MasterCard program MasterCard SecureCode*

MasterCard SecureCode (MC SecureCode) funkcioniše na istom principu kao i VbV program. Koristeći 3-D Secure specifikaciju MC SecureCode program omogućava svojim korisnicima autentifikaciju transakcije prilikom kupovine preko Interneta, i na taj način značajno umanjuje mogućnosti prevare.

Glavni cilj MC SecureCode-a je povećanje sigurnosti transakcija u okruženju elektronskog poslovanja. Kao i VbV program, dizajniran je da poveća poverenje i korisnika kartice i trgovca prilikom Internet kupovine, i da redukuje broj reklamacija i žalbi i aktivnosti prevara vezanih, u ovom slučaju, za korišćenje MasterCard platnih kartica.

3.3 *Program J/Secure Japanskog Kreditnog Biroa*

Kao jedan od veoma poznatih brendova kreditnih kartica Japanski Kreditni Biro (JCB) je, prateći trendove renomiranih međunarodnih kartičnih organizacija, uveo program zaštite korisnika kartica i Internet trgovaca koji učestvuju u trgovini



Slika 7. – *Metodologija implementacije programa VbV*

preko Interneta pod nazivom J/Secure. J/Secure program je pokrenut 2004. godine. [10]

J/Secure funkcioniše na istim principima kao VbV i MC SecureCode. Zasniva se na 3-D Specifikaciji, i koraci registracije i korišćenja su potpuno isti kao i kod pomenutih programa Visa-e i MasterCard-a. Prilikom kupovine preko Interneta pred korisnikom platne kartice se pojavljuje pop-up prozor u koji on unosi svoju šifru. Vrši se autentifikacija identiteta korisnika kartice, a transakcija se, nakon uspešne autentifikacije identiteta, šalje dalje na autorizaciju.

4. METODOLOGIJA IMPLEMENTACIJE VERIFIED BY VISA ZA BANKU IZDAVAOCA

Metodologija implementacije programa VbV za banku izdavaoca prikazana je na slici ispod.

(1) ***Istraživanje potreba i ponašanja korisnika kartica, kao i prevara na Internetu sa karticama banke***

Banka pokreće istraživanje potreba i ponašanja korisnika kartica, da utvrdi koliko korisnika koristi karticu za kupovinu preko Interneta, koji je broj CNP transakcija, koji je promet po transakciji i ukupan promet ostvaren ovim vidom kupovine. Takođe, potrebno je da Banka utvrdi, da ukoliko postoji značajan broj CNP transakcija, koje su najčešće prevare prilikom kupovine preko Interneta, i da li ulazak u program VbV može doneti zadovoljavajuće rezultate:

- smanjenje broja prevara;
- povećanje broja transakcija;
- povećanje prometa;
- povećanje poverenja korisnika kartica u kupovinu preko Interneta.

(2) ***Business Case (da li je ulazak u VbV program isplativ za banku)***

Imajući u vidu da proces sertifikacije za VbV program zahteva značajna finansijska sredstva, i shodno sa prethodnim istraživanjem, Banka mora da napravi Business Case i da zaključi da li je ulazak u program isplativ. Business Case mora posebno da bude fokusiran na sledeće elemente:

- troškovi ulaska u VbV program;
- potencijalna dobit;
- nefinansijska dobit (pozicioniranje na tržištu).

(3) ***Otvaranje projekta sa Visa-om***

Nakon odluke o ulasku u program VbV, potrebno je pokrenuti projekat sa kartičnom organizacijom (Visa). Koraci projekta su sledeći:

1) iniciranje projekta;
2) ICO kreira plan projekta i budžet;
3) banka prihvata plan i budžet;
4) popunjavanje dokumentacije.

(4) ***Implementacija***

Nakon popunjavanja dokumentacije, a na osnovu parametara koji su navedeni, Banka i ICO započinju proces implementacije. Implementacija obuhvata kreiranje testnog okruženja, parametarizaciju (opšti i posebni parametri, a na osnovu zahteva Banke).

(5) ***Sertifikacija***

Po završetku implementacije, ICO određuje datum prenosa projekta u testno okruženje, i po završetku te aktivnosti, startuje proces sertifikacije. Sertifikacija predstavlja testiranje u testnom okruženju, koje simulira produkciono okruženje. Po završenoj sertifikaciji, ICO obavlja validaciju rezultata i ako je pozitivna, zakazuje migraciju projekta u produkciju.

(6) ***Migracija projekta u produkciju***

Nakon uspešne sertifikacije, projekat se, u određeno vreme, prebacuje u produkciju. Nakon migracije, Banka je sertifikovani 3-D Secure Izdavalac.

(7) ***Registrovanje korisnika kartica za VbV program***

Korisnici kartica izdatih od strane sertifikovanog VbV, MC SecureCode i J/Secure izdavaoca, mogu se registrovati na sajtovima tih programa i učestvovati u istom.

5. ZAKLJUČAK

Koliko god se sistemi plaćanja razvijali u smislu pružanja mogućnosti i usluga klijentima, odnosno korisnicima istih, u tolikoj meri su i rasprostranjenije krađe na Internetu. Ne misli se da su sistemi plaćanja nepouzdani za bezbednost korisnika, već da sistemi zaštite nisu u dovoljnoj meri primenjeni i razvi-

jeni u njihovom okviru. Jedan od načina da se otklone njihovi nedostaci, i steknu preduslovi za prevazilaženje napada na Internetu je u metodološkom pristupu sistema za zaštitu.

Sa druge strane uočljivo je da su napadi uglavnom u domenima socijalnog inženjeringa i da tu tehnološka rešenja malo ili ni malo ne mogu da spreče krađe. Možete imati najbolju bravu na stanu, ali ako ostavite ključ ispod otirača ispred vaših vrata, pljačku nećete sprečiti. Tako je i na Internetu, najbolja zaštita se lako kompromituje ako korisnik sam oda svoje lozinke i PIN-ove. Ključ zaštite mora biti u tehnologiji kombinovanoj sa edukovanjem korisnika, njegovom informisanju i strogo formalizovanim procedurama koje zahtevaju autentifikaciju i autorizaciju.

U radu su analizirane metodologije napada i tehnologije zaštite metodom Verified by Visa. Pomenuta metodologija započinje utvrđivanjem potreba korisnika i najčešćih prevara na mreži, kao i isplativosti samog projekta za banku. Sledeći korak je ulazak u program sa Visa-om, te se nakon toga implementaciom, sertifikaciom i migraciom projekta u produkciju dolazi do poslednjeg dela, odnosno registracije korisnika za korišćenje Verified by Visa programa. Na ovakav način pristupajući implementaciji bilo kog od e-sistema plaćanja mogućnost za Internet krađama, tj. prevarama, se svodi na minimum.

Bitno je da korisnici sistema, odnosno klijenti na Internetu, budu upoznati sa aktuelnim i najčešćim prevarama kao i načinima zaštite svojih podataka od istih. U prilog ovome su u radu dati i statistički podaci o svesnosti, tj. upoznatosti potrošača sa mogućim Internet prevarama, iz čega se zaključuje da njihova informisanost o aktuelnim opasnostima na mreži nije u dovoljnoj meri razvijena.

LITERATURA

[1] Karen Williams, "The Evolution of Online Fraud: Staying ahead of the curve", eFunds, <http://www.efunds.com>
[2] 3-D Secure Member Implementation Guide, Cemea Region, Issuer and Acquirer, Visa, 2002.
[3] Click with Confidence - VbV, Visa Cemea, 2004.
[4] "Phishing, phaxing, vishing and other identity threats: The evolution of online fraud", White paper, Sophos, April 2007.
[5] "ProxyPay Issuer 3-D Secure Solutions - Card Payment Authentication and Enrolment", Clear2Pay, 2009.
[6] "RSA 2010 Global Online Consumer Security Survey", White paper, RSA, 2009.
[7] RSA AFCC phishing statistics
[8] "Special Online Fraud Report: What to Expect in 2010", White paper, RSA, 2010.
[9] Verified by Visa (VbV)-Merchant Implementation Guide, Version 2.0, Visa Cemea, 2005.
[10] http://www.jcb-global.com/english/solution/ec.html
[11] http://www.peonline.ca/main.php/en/page/What_is_Verified_by_VISA/

Marko Vulić, BSc
MSc student, Univerzitet u Beogradu, Fakultet organizacionih nauka, Beograd
Kontakt: *marko313@msn.com*
Oblasti profesionalnog interesovanja: elektronsko poslovanje, bankarstvo na Internetu, Internet tehnologije, mobilno računarstvo.

Marko Ranković, PhD, EuroPlanet d.o.o, Beograd
Kontakt: *mrankovic@euronetworldwide.com*
Oblasti profesionalnog interesovanja: upravljanje projektima u oblasti finansijskih servisa i usluga, procesiranje elektronskih finansijskih transakcija

Vojkan Vasković, PhD ,
Univerzitet u Beogradu, Tehnički fakultet Bor
Kontakt: *vaskovic@bvcom.net*
Oblasti profesionalnog interesovanja: elektronsko poslovanje (e-commerce, e-banking, sistemi plaćanja), Internet tehnologije i njihova primena, mobilne tehnologije, e-goverment.

UPUTSTVO ZA PRIPREMU RADA

1. Tekst pripremiti kao Word dokument, A4, u kodnom rasporedu 1250 latinica ili 1251 ćirilica, na srpskom jeziku, bez slika. Preporučen obim – oko 10 strana, single prored, font 11.
2. Naslov, abstakt (100-250 reči) i ključne reči (3-10) dati na srpskom i engleskom jeziku.
3. Jedino formatiranje teksta je normal, bold, italic i bolditalic, VELIKA i mala slova (tekst se naknadno prelama).
4. Mesta gde treba ubaciti slike, naglasiti u tekstu (Slika1...)
5. Slike pripremiti odvojeno, VAN teksta, imenovati ih kao u tekstu, radi identifikacije, u sledećim formatima: rasterske slike: jpg, tif, psd, u rezoluciji 300 dpi 1:1 (fotografije, ekranski prikazi i sl.), vektorske slike – cdr, ai, fh,eps (šeme i grafikoni).
6. Autor(i) treba da obavezno priloži svoju fotografiju (jpg oko 50 Kb), navede instituciju u kojoj radi, kontakt i 2-4 oblasti kojima se bavi.
7. Maksimalni broj autora po jednom radu je 5.

Redakcija časopisa Info M