UNAPREĐENJE SIGURNOSTI MOBILNOG BANKARSTVA I SPREČAVANJE PREVARA

IMPROVEMENT OF MOBILE BANKING SECURITY AND FRAUD PREVENTION

Slavoljub Milovanovic[1]

Rezime

Intenzivan razvoj informacionih tehnologija poslednjih decenija je stvorio okruženje u kome je globalno tržište postalo relevantno za odvijanje ekonomske konkurencije. Globalizacija trgovine, elektronskog i mobilnog bankarstva je u velikoj meri podstaknuta radikalnim inovacijama u informacionoj tehnologiji, kao i njenom konstantnom razvoju poslednjih godina. Evolucija informacionih tehnologija nastavlja razvoj zapanjujućom brzinom, pri čemu komunikaciona komponenta dobija sve više na značaju. Razvoj mobilnih tehnologija posebno je postao dinamičan tokom poslednjih nekoliko godina. Broj korisnika mobilnih i smart telefona konstantno raste. Mobilni operateri su povezani sa razvojem nove tehnologije koja se razvija brže nego ikada. Ekspanzija mobilnih mreža, rastuća stopa korišćenja mobilnih telefona i porast bankarskih usluga putem interneta su glavni razlozi za snažni rast mobilnog bankarstva.

Mobilno bankarstvo (m-bankarstvo) se posmatra kao sistem plaćanja preko mobilnih telefona i drugih mobilnih uredjaja, odnosno kao kanal koji koristi mobilnu telekomunikacionu mrežu u cilju pružanja bankarskih usluga potrošačima. Mobilno bankarstvo postaje sve značajniji element bankarske infrastrukture koja uključuje i druge komponente, kao što su bankomati, POS (Point-of-Sale) terminali i internet. Ovaj model bankarstva omogućava mobilna plaćanja, kontrolu stanja na računu, uzimanje zajmova i čitav niz drugih finansijskih usluga i transakcija. M-bankarstvo ima veliki značaj kako za razvijene zemlje, tako i za zemlje u razvoju. Brojna istraživanja pokazuju da u zemljama u razvoju, u proseku, na svakih 10.000 ljudi dolazi po jedna filijala banke i jedan bankomat. Ovaj nedostatak ili ograničen pristup bankarskim i finansijskim servisima ograničava rast i prosperitet za potošače i ekonomiju. Za ekonomiju zemlje, ograničavanje aktivnosti banaka na tradicionalne modele poslovanja može da uguši preduzetništvo, spreči razvoj i čak zaustavi ekonomski rast kroz isključivanje velikog broja potencijalnih bankarskih klijenata. Međutim, razvojem mobilnog bankarstva, potencijalni bankarski klijenti mogu da koriste različite finansijske usluge, uključujući mobilne transakcije i plaćanja, koristeći svoje mobilne telefone i bez potrebe da posete finansijsku instituciju. Imajući u vidu veliki prodor mobilnih servisa u mnogim zemljama, uključujući i zemlje u razvoju, m-bankarstvo predstavlja potencijalno važan način da se bankarski i finansijski servisi ponude ljudima kojima banke nisu dostupne.

Mobilno bankarstvo se razvija kroz veliki broj modela, koji su često mogu svrstati u dve kategorije ili se nalaze između dva ekstrema: model baziran na bankarskim institucijama i model baziran na nebankarskim institucijama. Ovi modeli imaju različite načine rada, posebno u pogledu odnosa sa krajnjim korisnicima i to u vezi sa uspostavljanjem računa, uzimanjem depozita i servisa za pozajmljivanje.

Obezbeđivanje sigurnosti transakcija u sistemima m-bankarstva i mobilnih plaćanja (m-plaćanja) ima više aspekata, koji se znatno preklapaju sa postojećim merama za obezbeđivanje sigurnosti elektronskih finansijskih transakcija. Iako ove odgovornosti nisu unikatne za m-bankarstvo, one su verovatno još važnije u mobilnom kontekstu, gde se mobilni telefoni mogu lako ukrasti ili izgubiti. Što

[1] Univerzitet u Nišu, Ekonomski fakultet, Trg Kralja Aleksandra 11, 18000, Niš

se tiče telekomunikacionih mreža, pretnje m-bankarstvu su iste kao i one drugim uslugama koje se pružaju preko mobilnih mreža. Takva bezbednosna pitanja obuhvataju:

- pokušaje da se onemogući ili ošteti mrežna infrastruktura, uključujući napade koji sprečavaju korišćenje usluge;
- pokušaje da se ograniči legitimni pristup korisnika mreži, kao na primer, putem bežične smetnje;
- neovlašćeni pristup mreži;
- presretanje, praćenje ili izmena transmisija.

Kod servisa i modela mobilnog bankarstva, korisnici će očekivati bar isti nivo bezbednosti koji postoji i kod *online* bankarstva preko njihovih računara. Da bi se podstaklo uvođenje mobilnog bankarstva moraju se rešiti kako realni problemi (na pr., prisluškivanje, ubacivanje virusa i modifikacija podataka), tako i problemi „percepcije" (na pr., kako bezbednost ili nedostatak bezbednosti utiče na brend finansijske institucije). Prema tome, mobilno bankarstvo treba da odgovori sledećim zahtevima:

- **Prenos podataka mora biti siguran.** U ovom slučaju termin „siguran" se odnosi uglavnom na koncept poverljivosti i stoga zahteva šifrovanje veze između mobilnog uređaja i banke.
- **Pristup aplikaciji i podacima mora biti kontrolisan.** Pre nego što korisnici dobiju bilo kakvu osetljivu informaciju koja se odnosi na njihov bankovni račun, mora da se izvrši određeni nivo verifikacije. Idealno, kombinacija nekoliko faktora autentifikacije i mogućnost da se ospori korisnik u slučaju (potencijalne) povrede bezbednosti treba da budu deo procedure.
- **Mora se obezbediti integritet podataka.** Svaki kritični podatak koji je uskladišten na mobilnom uređaju mora biti zaštićen od neovlašćene modifikacije. Potrebno je rešiti i pitanje moguće greške, oštećenja ili brisanja važnih podataka.
- **Gubitak uređaja mora da ima ograničeni značaj.** Servis mobilnog banakrstva mora da bude tako dizajniran da gubitak telefona korisnika nema veliki značaj. Na primer, servis može da pruža funkciju daljinskog zaključavanja koja je sadržana u softveru klijenta i koja sprečava da se sa izgubljenog telefona pristupa klijentovom bankovnom računu. Ova funkcija pomaže da korisnici budu mirniji i da se lakše odlučuju da koriste usluge mobilnog bankarstva.

Pošto i servisi m-bankarstva i telekomunikacione mreže nastavljaju da se razvijaju, biće novih prilika za pretnje bezbednosti m-bankarstva, ali i za nove tehnike za ublažavanje takvih pretnji. Na primer, dok se većina transakcija m-bankarstva i m-plaćanja u zemljama u razvoju odvija uz korišćenje osnovne telefonske opreme, moćniji (*3G* i *4G*) telefoni omogućavaju složeniju bezbednosnu funkcionalnost. Međutim, uvođenje dodatne složenosti i na telefonu i u bankarskim programima može, takođe stvoriti dodatne mogućnosti za zlonamerne napade (hakovanje) ili za bezbednosne propuste.

Sprečavanje prevara je krajnja odgovornost provajdera usluga m-bankarstva, bez obzira koji se model m-bankarstva upotrebljava. Odgovornost za nadzor i sprovođenje mera protiv prevara zavisi od pravnog i regulatornog okvira i modela m-bankarstva koji se koristi, i može spadati u nadležnost agencija koje se brinu za sprovođenje zakona, regulatora finansijskog sektora ili telekomunikacionog regulatora, ili neke kombinacije tih agencija. Prevare u m-bankarstvu mogu imati više oblika, ali se generalno mogu kategorisati u četiri grupe: (1) pranje novca; (2) prevara korisnika od strane posrednika ili drugih korisnika; (3) prevara servisa ili sistema od strane posrednika; ili (4) prevara posrednika od strane pojedinaca/korisnika

Telekomunikacioni operateri i proizvođači i prodavci tehnologija su mnogo uložili u tehnologiju zaštite i odgovarajuće procese, da bi minimizirali bezbednosna pitanja mobilnih mreža, i takve tehnologije se mogu primeniti i na usluge m-bankarstva. Ovaj rad upravo razmatra tehnologije i mere zaštite koje se koriste u mobilnom bankarstvu, sa posebnim osvrtom na sprečavanje prevara.

Ključne reči: mobilno bankarstvo, sigurnost, sigurnost mobilnih mreža, sigurnost mobilnih aplikacija, sprečavanje prevara

Summary

The intensive development of information technology in the last decades has created a context in which global market has become a relevant environment for the economic competition. Globalization of the commerce, the electronic and mobile business are greatly encouraged by radical innovations in information technology as well as its permanent development in last years. The

evolution of informational technologies continues in the same dynamic manner and their communication component becomes more and more significant. The field of mobile technologies was particularly dynamic during the past few years. The number of mobile phone users has grown permanently. Mobile operators are involved in launching new technologies which are developing faster than ever. The degree of expansion of the mobile phone networks, fast penetration rate of mobile devices and the emerging use of banking services via the fixed Internet are the main reasons for a strong anticipated growth of mobile banking.

Mobile banking (m-banking) is viewed as a payment system through mobile telephones and the other mobile devices, apropos as a channel using mobile telecommunication network with aim of providing banking services to consumers. Mobile banking becoming more and more important element of banking infrastructure that includes the other elements, such as Automated Teller Machines (ATM), Point-of-Sale terminals and internet. This model of banking enables mobile payments (m-payments), management of account balance, taking loans and wide range of the other financial services and transactions. M-banking is of the great importance for developed as well as for developing countries. Researches indicates that within developing countries, on average, one bank branch and one ATM exists for every 10,000 people. This lack of, or limited access to, banking and financial services constrains growth and prosperity for consumers and the economy. For a country's economy, limiting banking activity to traditional approaches can constrein entrepreneurship, retard development and economic growth through exclusion of large numbers of potential banking customers. However, for those "unbanked" individuals, access to a variety of financial services is now accessible through their mobile devices. Individuals can engage in a variety of financial services, including mobile transactions and payments, by using their mobile devices and without having to visit a financial institution. Given the large penetration of mobile services in many countries, including in developing countries, m-banking offers a potentially important way to bring banking and financial services to the "unbanked."

There are a variety of m-banking models, which have often been described as falling into two primary categories or on a continuum between two extremes: a bank-based model and a branchless or non-bank-based model. These models each have distinct means of operating, especially with respect to the relationship with the end customer in terms of establishing accounts, deposit taking, and lending services.

Ensuring transaction security in m-banking and m-payment systems has multiple aspects, overlapping considerably with existing measures to ensure security in electronic financial transactions. While these responsibilities are not unique to m-banking, they are even more relevant in a mobile context, where mobile devices can be easily misplaced or stolen. With respect to telecommunications networks, the threats to m-banking are the same that apply to any other services delivered over the mobile network. Such security issues include:

- attempts to disable or damage the network infrastructure, including denial of service attacks;
- attempts to limit legitimate users' access to the network, such as through wireless interference;
- unauthorized access to the network; and
- interception, monitoring or alteration of transmissions.

Users will expect at least the same level of security that is available in online banking via their PC. Both the real problem (e.g. eavesdropping, injection and modification) and the „perception" issue (e.g. how security – or lack thereof – affects the financial institutions' brand) must be addressed in order to encourage adoption of mobile banking. Therefore mobile banking should meet following requirements:

- **Data transmission must be secure**. In this case, the term secure addresses mainly concept of confidentiality and therefore requires encryption of the connection between mobile device and the bank.
- **Application and data access must be controlled**. Before users receive any sensitive information related to their bank accounts, a certain degree of verification must be completed. Ideally, the combination of several authentication factors and the possibility to challenge the user in case of a (potential) security breach should be part of the procedure.
- **Data integrity must be provided**. Any critical data stored on the mobile device must be protected against unauthorized modification. The issue of possible corruption and deletion error of sensitive information must be addressed.
- **Loss of device must have limited impact**. The mobile banking service should be designed so that there is limited impact when customers lose their devices. For example, the service could support a remote-locking feature embedded in the software client that prevents a lost phone from accessing the customers' account. Such features also encourage customers to try mobile banking.

As both m-banking services and telecommunications networks continue to evolve, there will be new opportunities for both threats to m-banking security and techniques to mitigate such threats. For example, while most m-banking and m-payment transactions in developing countries are conducting using relatively basic handsets, more powerful (3G or 4G) handsets enable more complex security functionality. However, the introduction of additional complexity in both the handset and the banking application can also create additional opportunities for malicious attacks (hacking) or for security failures.

Fraud prevention is ultimately the responsibility of the m-banking service provider, regardless of the m-banking model employed. Responsibility for oversight and enforcement of anti-fraud measures depend on the legal and regulatory framework and the m-banking model employed, and may fall under the jurisdiction of agencies including law enforcement, the financial sector regulator or the telecommunications regulator, or some combination of those agencies. Fraud can take many forms, but can be generally categorized into four cases: (1) money laundering; (2) defrauding of customers by agents or other consumers; (3) agents defrauding the service or system; or (4) individuals/consumers defrauding agents.

Telecommunications operators and technology vendors have invested heavily in technologies and processes to minimize security issues on mobile networks, and such technologies can be applied to m-banking services as well. This paper just considers technologies and measures which are used in mobile banking with special attention to fraud prevention.

Keywords: mobile banking, security, security of mobile networks, security of mobile applications, fraud prevention