TEHNIKE I METODE NAPADA NA KOMUNIKACIONI KANAL PRI PRENOSU PODATAKA U MOBILNOJ TELEFONIJI

Mladen Veinović[1], Miroslav Ćajić[2], Bogdan Brkić[3]
[1]Univerzitet Singidunum, Beograd; mveinovic@singidunum.ac.rs
[2]O.Š. "Sveti Sava", Rogatica; miroslavcajic@gmail.com
[3]Fond za zaštitu životne sredine, Banja Luka; bogdan.brkic@gmail.com

Sažetak

U ovom radu analizirane su karakteristike komunikacionog kanala za prenos podataka mobilnih uređaja kao i bezbjednosni sistem koji se koristi. Predstavljen je nivo bezbjednosti koji se upotrebljava pri normalnom radu, kao i nivo bezbjednosti koji se preporučuje u mobilnim vezama u kojima postoji potreba za radom u zaštićenom komunikacionom kanalu. Metodološki su obrađeni tipovi kao i metode napada koji se mogu desiti u toku procesa komunikacije. Iznesene su preporuke za povećanje nivoa bezbjednosti i mjere za prevenciju u slučaju napada. Na osnovu dobijenih rezultata na kraju rada dat je zaključak.

Ključne riječi: *mobilni uređaj, komunikacioni kanal, napad, korisnik.*

Abstract

In this paper the characteristics of the communication channel for data transmission and mobile security system is analysed. The level of security that is used in normal work and level of security that is recommended in mobile connections in which there is a need to work in a protected communication channel is introduction. Types and methods of attack that could occur during the communication process is methodological processed.

Recommendations for increasing security and prevention measures in case of attack it is also gives. At the end of the paper's conclusion is based on the results.

Key words: *mobile device, communication channel, atack, mobile user.*

1. UVOD

Početak novog milenijuma u globalu može se povezati sa početkom ere pametnih, smart, telefona. Razvoja novog operativnog sistema za mobilne uređaje usloveljen je izlazkom na tržište nove serije određenog tipa telefona. Realizacijom novih operativnih sistema doprinosi poboljšanju funkcionalnosti i upravljivosti mobilnih telefona. Novi brojni mobilni uređaju kao što su BlackBerries, iPhones i uređaju pod Android operativnim sistemom naparavili su pravu revoluciju na tržištu telefona [1]–[8]. Masovnom upotrebom smart uređaja povećava se potreba uvođenja većeg nivoa zaštite integriteta informacija koje su pohranjene u ovim uređajima. Faktori koji utiču na bezbjednost ovih uređaja manje su izraženi u telefonima koji koriste neki od operativnih sistema. Više napada na bezbjednosni sistem kod smart telefona kao i veća učestalost napada dešava se prilikom prihvatanja preuzimanja i slanja podataka odobrenih od strane korisnika [9]. Međutim, činjenica je da mnoštvo napada nije čak ni primećeno niti registrovano od strane korisnika. Pored operativnih sistema kao što su Windovs Mobile i Simbian OS, mobilni svijet je tokom poslednjih nekoliko godina zabilježio i pojavu iPhone iOS i Linuks Android

operativnog sistema. Uprkos njihovom skorom startu, oba operativna sistema su već stekli veliki udio na tržištu mobilnih uređaja i predviđa se čak i veliko povećanje u budućnosti.

Tabela 1. Pregled upotrebe operativnih sistema za mobilne uređaje i pokazatelj ukupnog broja korisnika mobilne u odnosu na korisnike fiksne telefonije u Novembru 2011 godine.

Worldwide smartphone operating system (OS) market share in 2009-2015, according to Gartner

OS (listed alphabetically)	2009 market share	2010 market share	2011 market share	2015 market Share
Android	3.9%	22.7%	38.5%	48.8%
BlackBerry	19.9%	16.0%	13.4%	11.1%
iOS	14.4%	15.7%	19.4%	17.2%
Symbian	46.9%	37.6%	19.2%	0.1%
Windows Phone/Mobile	8.7%	4.2%	5.6%	19.5%
Others	6.1%	3.8%	3.9%	3.3%
Total smartphones sold	172 million	297 million	468 million	631 million

Source: Gartner (April 2011)

Smartphone OS market share and compound annual growth rate 2011-2015, according to IDC

2011 market share	2015 market Share	2011-2015 CAGR
39.5%	45.4%	23.8%
14.9%	13.7%	17.1%
15.7%	15.3%	18.8%
20.9%	0.2%	-65.0%
5.5%	20.9%	67.1%
3.5%	4.6%	28.0%
450 million	N/A	19.6%

Source: IDC (March 2011) via: mobiThinking

Key Global Telecom Indicators for the World Telecommunication Service Sector in 2011 (all figures are estimates)

	Global	Developed nations	Developing nations	Africa	Arab States	Asia & Pacific	CIS	Europe	The Americas
Mobile cellular subscriptions (millions)	5,981	1,461	4,520	433	349	2,897	399	741	969
Per 100 people	86.7%	117.8%	78.8%	53.0%	96.7%	73.9%	143.0%	119.5%	103.3%
Fixed telephone lines (millions)	1,159	494	665	12	35	511	74	242	268
Per 100 people	16.6%	39.8%	11.6%	1.4%	9.7%	13.0%	26.3%	39.1%	28.5%
Active mobile broadband subscriptions (millions)	1,186	701	484	31	48	421	42	336	286
Per 100 people	17.0%	56.5%	8.5%	3.8%	13.3%	10.7%	14.9%	54.1%	30.5%
Fixed broadband subscriptions (millions)	591	319	272	1	8	243	27	160	145
per 100 people	8.5%	25.7%	4.8%	0.2%	2.2%	6.2%	9.6%	25.8%	15.5%

Source: International Telecommunication Union (November 2011) via: mobiThinking

2. VRSTE TEHNIKA

Predstavljeni napadi podrazumijevaju primjenu izabrane tehnike koja se odnosi na narušavanje bezbjednosti framework-a mobilnog uređaja. Naš cilj je da objasnimo neke od tehnika koje se mogu koristiti od strane napadača. Navadene prijetnje su klasifikovane po svojoj pripadnosti, onosno, orjentaciji a dijelimo ih na četiri klase. U ovom radu će biti obrađene: hardverske, tipske nezavisne, i korisničke [10]:

- Hardverski orjentisane tehnike pripadaju dijelu bezbjednosti mobilnih uređaja sa aspekta šireg stanovišta. Ove vrste napada su pogodne za kršenje osobine integriteta podataka jer se izvršavaju prepravkom već ugrađenog hardvera.
- U tipski nezavisne tehnike spadaju prisluškivanje etera preko WiFi mreže i curenje podataka kroz proizvođačev „back door“. Napadač uz pomoć odgovarajuće opreme prisluškuje komunikacioni kanal između dva korisnika, detektuje pojedinačne slabosti, ubacuje se u kanal i vraća nekorektne podatke.
- Korisnički orjentisane tehnike koriste slabosti koji nisu tehničke prirode. Mnogi maliciozni programi za mobilne uređaje koriste sigurnosne propuste koji nisu tehničke, odnosno, programske prirode. Svojim pokretanjem izvršavaju niz korisničkih neovlaštenih procesa. Zbog svoje prirode zaobilaze sigurnosne mehanizme čime povećavaju nivo ranjivosti operativnog sistema [5].

3.1 Hardverski orjentisane tehnike

Ovu vrstu tehnike smo podijelili na napade prilikom presretanja komunikacije u smart uređajima kao i na klasične napade koji se dešavaju.

3.1.1. Presretanje komunikacije

Komunikacija između mobilnog uređaja i Smart kartice nije šifrovana, pa ne postoji opasnost prilikom man-in-the-middle (MITM) napada na ovu komunikaciju pošto ne postoji specifičan interfejs za ovu vrstu komunikacije. Međutim, danas postoji proizvod pod nazivom TurboSIM [12] koji se uspješno primenjuje prilikom napada na pametne kartice MITM metodom. TurboSIM je mali čip koji presreće komunikaciju između pametne kartice i mobilnog uređaj. Ugrađuje se priključenjem, odnosno, uklanjanjem malog dijela plastičnog okvira SmartCard-a. Uz korišćenje TurboSIM moguće je uspješno ukloniti zaključavanje SIM iPhone uređaju [18]. Kao hardverski interfejs TurboSIM moguće je koristiti za obje postavke isti je, odnosno, za 2G SIM karticu (Subscriber Identity Module) i za 3G UICCs (Universal Integrated Circuit Card). Nedavno je započet projekat pod nazivom Osmocom SIMtrace koji je takođe u stanju da uđe u trag komunikacije između SIM kartice i mobilnog aparata [12].

3.1.2. Napadi na uređaje

Hardverski orjentisane tehnike koje se odnose na klasično napadanje uređaja mogu da sadrže ili da ne sadrže tragove napada. JTAG (Joint Test Action Group) su napadi koji sadrže tragove napada dok forenzički analizirani napadi ne sadrže tragove napada na uređaj. JTAG napadi predstavljaju standard za testiranje i debagovanje hardvera mobilnog uređaja. Iako ovakav način otklanjanja grešaka nije više neophodan u mobilnim uređajima koji se danas prodaju krajnjim korisnicima, JTAG funkcionalnost ponekad još uvek dobrodošla. Pomenuta funkcionalnost omogućava provjeru uređaja na dubokom nivou, što dovodi do stanja eksploatisanja mogućih slabih tačaka. Ova slabost može biti „implemetirana“ od strane proizvođača mobilnog uređaja [13]. Neka istraživanja pokazuju da ova vrsta napada obuhvata i podatke i lične razgovore koji se poverljive poslovne prirode [14], [15].

3.2. Tipski nezavisne tehnike

Tipski nezavisne tehnike za cilj imaju direktno napadanje sistema zaštite mobilnih uređaja korisnika. Ovi napadi ne mogu biti iskorišćeni širenje za malvera. Izuzetak može biti bežični proces uparivanja, koji pod uticajem zlonamernih programa primorava mobilni uređaj za povezivanje sa lažnom pristupnom tačkom ili baznom stanicom. Za razliku od fiksnih, GSM sistemi koriste radio talase za povezivanje različitih korisnika u komunikaciji. Tačnije, mobilni telefon sa baznom stanicom se povezuje preko šifrovanog kanala. Sa bezbjednosne tačke gledišta, ovdje imamo nekoliko pitanja koja treba razmotriti. GSM specifikacija podržava nekoliko bezbjednosnih mehanizama koji služe da bi se sprečili potencijalni napadi. U ovom dijelu ćemo govoriti o A3 algoritmu koji se koristi za autentifikaciju, A8 algoritamu koji se upotrebljava za distribuciju ključeva , vrstama A5 algoritama (A5 / 1, A5 / 2, i A5 / 3) koji se koriste za šifrovanje kao i o "algoritmu" A5 / 0 koji radi bez bez enkripcije.

Da bi korisnik koristio mobilni telefon, sistem mora dokazati da ima pristup proizvođački ispravnoj SIM kartici. U tu svrhu se koristi simetrična kriptografija. Asimetrična kriptografija se takođe može upotrijebiti ali je prije 25 godina kada su protokoli dizajnirani bila suviše „teška“ za tu upotrebu jer je čak dodatno optetrećivala kapacitet baterije samog uređaja tako da se u ovom slučaju danas još uvijek koristi simetrična kriptografija. Dakle, sva rješenja u nastavku ovog rada zasnivaju se na upotrebi simetrični kriptografskih rješenja. Ukratko, tajna riječ *s* se dobija randomiziranim nizom zajedno sa slučajnom vrijednost *r*. Dobijena vrijednost predstavlja novi privremeni string za potvrđivanje autentičnosti: *a* = A3 (s, r). Kad bazna stanica potvrdi autentičnost mobilnog korisnika šalje mu novi novi zajednički ključ *k*: = A8 (s, r). Dobijena

vrijednost *k* sada se koristi za šifrovanje komunikacije između bazne stanice i mobilnog telefona. Primjena tipski nezavisne tehnike mogu biti ostvarena zbog loše projektovanih korisničkih servisa, odnosno, zbog postojanja back door-a. To se posebno odnosi na SMS i MMS servise pomoću kojih može da se primi određena zlonamjerna instrukcija. Upotreba UMTS (Universal Mobile Telecommunications System) tehnologije u velikoj mjeri prevazilazi dosadašnju GSM tehnologiju u pogledu korisničke bezbjednosti [13].

3.3. Korisnički orjentisane tehnike

Određena istraživanja su izvršena iz oblasti poznavanja procjene bezbednosti za prosečnog korisnika mobilnog uređaja. Zanimljiv je rezultat dvojice istraživača Whitten and Tygar [13] koji su došli do zaključka da obični korisnici ne mogu da koriste mehanizme bezbednosti ispravno! Iako je bilo nekoliko pokušaja da se učini jednostavan bezbjednosni interfejs za korisnike, čak i veoma jednostavan Windows security klizač sa samo četiri moguće pozicije nije bio u potpunosti razumljiv, čime ovi korisnici nisu stekli status IT stručnjaka [15].
Stoga, moramo da se zapitamo koja je svrha ovim brojnim bezbjednosnim mehanizmima ukoliko prosječan korisnik ne razumije njihovu ulogu. Čak i ako on uspije da razumije funkciju jednog specifičnog mehanizama, da li će još jedan mehanizam biti teško shvatljiv za njega? Osobe koje rade u bezbjednosti ne žele da postignu pogrešan cilj, ali više integrisanog bezbjednosnog obruča u korisniku može povećati želju za istraživanjem ovih barijera [15].

4. VRSTE METODA

Pored nabrojanih vrsta tehnika važno je nabrojati i metode napada koji se mogu izvršiti. U suštini napadač određenom tehnikom ispituje ranjivost žrtve koju napada dok metoda napada zavisi od granica moći samog napadača. Preciznije rečeno, razlikujemo dva tipa metoda. To su metode pasivnog napadača, odnosno onog koji ne mijenja integritet podatka i metode aktivnog napadača koji mijenja integritet presretnute poruke. Očigledno je da je druga metoda snažnija od prve i da je manje vjerovatno da će proći neopaženo za razliku od prve koja ne mijenja strukturu podataka. Ipak, obje metode imaju sledeće ciljeve:

- Prisluškivanje: pasivni napadač pokušava da presretne razgovor između korisnika mobilnog telefona i bazne stanice, odnosno, između tačke A i tačke B.
- Dostupnost napada: jedan od mogućih primera je aktivni napadač koji blokira signal mobilnog telefona ili bazne stanice.
- Privatnost napada: pasivni napadač može koristiti ID smart uređaj prilikom pronalaska njegovog vlasnika. Ovaj napad može biti efikasniji korišćenjem aktivnog tipa napada.
- Napadi imitiranja: u ovom slučaju postoje dva identična uređaja gdje jedan telefon imitira drugi. Jedan mobilni telefon se predstavlja kao drugi čime izbjegava finansijske troškove, odnosno, koristi usluge na lažan način.

5. ZAKLJUČAK

Iz svega gore navedenog i iz našeg ličnog iskustva u ovom radu došli smo do sledećih zaključka:

- Stvaranje troškova je tema koja će biti još važnija u budućnosti. Kako se povećava broj usluga koje se odnose na mobilne uređaje, pretpostavljamo da će usluge koje nemaju zagarantovan nivo bezbjednosti biti čak besplatne.
- Mrežno okruženje će vjerovatno ostati nepromenjeno. Imajući u vidu zapažanja u poslednjih nekoliko godina, došli smo do zaključka da postoji sklonost ka povećanju potrebe daljinskog upravljanja kao i daljinskom ažuriranja firmwera uređaja.
- Značaj skupa bežičnih veza će vjerovatno biti smanjena. Iz ugla ekonomske perspektive, komunikacioni troškovi će se smanjiti, jer veći propusni opseg postaje sve dostupni u mobilnim mrežama. Sa finansijske strane, troškovi upotrebe kriptografskih algoritama na uređajima će se takođe smanjiti jer četvrta generacija mobilnih mreža (4G) je dizajnirana za visoki propusni opseg i nisku latenciju podataka u saobraćaju. Dakle, ima veći propusni opseg, nižu latenciju, što znači da se brži prenos podataka može koristiti za nova sigurnosna rešenja.
- Ograničeni resursi uređaja će se verovatno smanjiti, što će dovesti do više procesorske snage i više količine memorije. Ipak, baterija uređaja će izgleda ostati najveći limitirajući faktor u mobilnim uređajima u bliskoj budućnosti.
- Sa nivoa bezbjednosti nesvjesni korisnik može postati nešto više obazriviji prilikom upotrebe uređaja koji sa nivoa bezbjednosti zahtijeva široku pažnju. Ova činjenica može biti povezana sa vrstom operativnog sistema koji se koristi.
- Heterogenost u uređajima, operativnim sistemima i aplikacija, kada se govori o mobilnim uređajima, je osobina bezbednosti kaja je već u prošlosti. Takođe, teško je predvidjeti da li će pojava monopola u svijetu mobilne telefonije biti slična kao i u svijetu desktop računara.

Činjenica je da su mobilni telefoni brzo prevazišli razliku u odnosu na obične računare, u smislu procesorske snage, tehnologije izrade i raznovrsnosti operativnih sistema. Međutim, određena ograničenja mobilnih u odnosu na desktop uređaje će ostati na snazi i u budućnosti. Postoji mnogo dokaza da smo zaista na početku doba napada na smart telefone. U svakom slučaju, područje istraživanja iz oblasti mobilne bezbjednost će biti interesantno za godine koje dolaze.

LITERATURA

[1.]N. Leavitt, "Malicious Code Moves to Mobile Devices," IEEE Computer, vol. 33, no. 12, 2000.

[2.] S. N. Foley and R. Dumigan, "Are Handheld Viruses a Significant Threat?" Commun. ACM, vol. 44, no. 1, 2001.

[3.] D. Dagon et al., "Mobile Phones as Computing Devices: The Viruses are Coming!" IEEE Pervasive Computing, vol. 3, no. 4, 2004.

[4.] N. Leavitt, "Mobile Phones: The Next Frontier for Hackers?" IEEE Computer, vol. 38, no. 4, 2005.

[5.] M. Hypponen, "State of Cell Phone Malware in 2007," 2007,http://www.usenix.org/events/sec07/tech/hypponen.pdf.

[6.] J. Kleinberg, "The Wireless Epidemic," Nature, vol. 449, no. 20, Sep. 2007.

[7.] G. Lawton, "Is It Finally Time to Worry about Mobile Malware?" IEEE Computer, vol. 41, no. 5, 2008.

[8.] J. Oberheide and F. Jahanian, "When Mobile is Harder Than Fixed (and Vice Versa): Demystifying Security Challenges in Mobile Environments," in Workshop on Mobile Computing Systems and Applications (HotMobile), February 2010.

[9.]M. Kotadia, "Major Smartphone Worm 'by 2007'," Jun.

[10.] http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats

[11.] OsmocomBB project, "SIMtrace," http://bb.osmocom.org/ trac/wiki/SIMtrace.

[12.] OMTP Limited, "Advanced Trusted Environment – OMTP TR1," May 2008.

[13.] University of Glamorgan, "Disk Study 2008-2009," May 2009,

[14.] http://isrg.weblog.glam.ac.uk/2009/5/7/disk-study-2008-2009.

[15.] F. C. Freiling et al., "Reconstructing people's lives: A case study in teaching forensic computing," in Conference on ITIncidents Management & IT-Forensics - IMF, 2008.