Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 4.633
DOI: https://doi.org/10.24867/33BE31Petric

METODE OTKLJUČAVANJA MOBILNIH TELEFONA

METHODS FOR UNLOCKING MOBILE PHONES

Jelena Petrić, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *Ovaj rad se bavi forenzičkim metodama otključavanja ekrana Android i iOS uređaja, uz analizu savremenih bezbednosnih mehanizama i izazova koje oni postavljaju. Analizirani su operativni sistemi i bezbednosne arhitekture pametnih telefona, kao i postojeći pristupi zaobilaženja biometrijske autentifikacije, lozinki i šablonske zaštite uz primenu forenzičkih alata. Posebna pažnja je posvećena praktičnom testiranju otpornosti biometrijskih sistema i istraživanju karakterističnih obrazaca za zaključavanje, uz osvrt na etičke i pravne aspekte prikupljanja dokaza.*

Ključne reči: *digitalna forenzika, mobilni uređaji, zaštitni mehanizmi, metode otključavanja*

Abstract – *This paper deals with forensic methods for unlocking the screens of Android and iOS devices, along with an analysis of modern security mechanisms and the challenges they pose. Smartphone operating systems and security architectures were analyzed, as well as existing approaches to bypassing biometric authentication, passwords, and pattern protection using forensic tools. Special attention is paid to practical testing of the resilience of biometric systems and research of characteristic locking patterns, with a focus on the ethical and legal aspects of evidence collection.*

Keywords: *digital forensics, mobile devices, protection mechanisms, unlocking methods*

1. UVOD

Otključavanje ekrana predstavlja bitan korak u procesu prikupljanja dokaza tokom forenzičke istrage, jer ovaj čin omogućava direktan pristup podacima u njihovom originalnom i neizmenjenom obliku. Uspešnim otključavanjem izbegava se upotreba rizičnih i potencijalno destruktivnih metoda zaobilaženja zaštite, koje mogu ugroziti integritet ili pravnu prihvatljivost dokaza.

Zadatak ovog rada je da istraži forenzičke metode koje se koriste za otključavanje ekrana pametnih telefona i da putem izvedenih zaključaka demonstrira postojeće metode na odabranim uređajima. Rad je isključivo edukativnog karaktera i nema za cilj podsticanje ili promociju zloupotrebe stečenih znanja, već prvenstveno unapređenje razumevanja metoda otključavanja mobilnih uređaja u kontekstu digitalne forenzike.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Stevan Gostojić, red. prof.

2. FORENZIKA MOBILNIH UREĐAJA

Forenzika mobilnih uređaja predstavlja specifičnu granu digitalne forenzike, usmerenu na prikupljanje i analizu podataka pohranjenih na mobilnim uređajima ili prenošenih putem celularne mreže [1].

2.1. Izazovi forenzike mobilnih uređaja

Brza evolucija mobilnih tehnologija i kratak ciklus razvoja proizvoda doveli su do velikih razlika u hardveru, softveru i strukturama čuvanja podataka između različitih proizvođača i verzija operativnih sistema mobilnih uređaja. Ova raznovrsnost, u kombinaciji sa sve naprednijim bezbednosnim mehanizmima stvara ozbiljne izazove prilikom prikupljanja dokaza u forenzičkim istragama.

2.2. Proces forenzičke istrage

Forenzička istraga je proces koji obuhvata identifikaciju, prikupljanje, čuvanje, pregled, analizu i prezentaciju dokaza korišćenjem pravno i naučno prihvaćenih metoda i alata.

2.3. Forenzički alati

U situacijama kada je telefon zaključan obično je neophodna upotreba specijalizovanih tehnika ili alata za zaobilaženje zaštitnih slojeva kako bi se na bezbedan i legalan način došlo do traženih informacija. Forenzički alati su softverske i hardverske tehnologije koje se koriste u istrazi kao pomoćna sredstva prilikom pristupa, obrade i ekstrakcije podataka sa različitih uređaja.

2.3. Jailbreaking i rooting

Najčešće korišćeni postupci za sticanje najvišeg nivoa privilegija nad mobilnim operativnim sistemima uključuju procese root-ovanja na Android platformama i jailbreak-a na iOS uređajima. Primena ovih metoda nosi velike rizike po integritet digitalnih dokaza i zahteva pažljivo izvođenje i strogo poštovanje forenzičkih principa.

3. OPERATIVNI SISTEMI MOBILNIH TELEFONA

Zbog brojnih mehanizama zaštite koje implementiraju savremene mobilne platforme, alati i metode koji su efikasni na jednom sistemu često nisu primenljivi na drugom zbog specifičnosti arhitekture i nivoa otvorenosti platforme.

3.1. Tipovi operativnih sistema

Tehnike za zaobilaženje zaključanog ekrana često uključuju složene procedure koje zavise od hardvera i verzije operativnog sistema. Prema statistici [2] za mesec avgust 2025. godine, trenutno tržištem mobilnih telefona dominiraju dva operativna sistema, Android i iOS.

3.2. Zaštitni mehanizmi

Zaštitni mehanizmi mobilnih telefona obuhvataju skup mera i tehnologija dizajniranih da zaštite uređaj i privatnost korisnika od krađe i drugih oblika zloupotrebe.

3.2.0. Mehanizmi zaključavanja ekrana

Mehanizmi poput PIN-a, lozinke, šablona i biometrijske autentifikacije se razlikuju po kompleksnosti i nivou bezbednosti koji mogu da pruže korisniku u zaštiti podataka.

3.2.1. Zaštita naloga i enkripcija

Enkripcija podrazumeva pretvaranje svih podataka na telefonu u nečitljiv format, koji se može dešifrovati jedino putem odgovarajućeg kriptografskog ključa. Na starijim modelima implementirana je full disk encryption (FDE), dok se na novijim modelima koristi file-based encryption (FBE).

3.2.2. Izolacija aplikacija

Sandbox predstavlja izolovano okruženje u kome aplikacije mogu nesmetano da obavljaju svoje funkcije, ali bez direktne interakcije sa drugim aplikacijama ili kritičnim komponentama sistema.

3.3. iOS

Za razliku od otvorenijih platformi, iOS sistem ograničava pristup resursima, čime se umanjuje mogućnost neautorizovanog pristupa podacima. Postupak za otključavanje ovih uređaja zahteva upotrebu naprednih forenzičkih alata i tehnika, kao i detaljno poznavanje arhitekture sistema. U pojedinim slučajevima, posebno kod novijih modela, saradnja sa proizvođačem može biti neophodna kako bi se osigurala forenzički prihvatljiva i tehnički izvodljiva obrada digitalnih dokaza.

3.3.0. Arhitektura

Arhitektura je zasnovana na višeslojnom modelu koji obuhvata četiri osnovna sloja: Cocoa Touch, Media, Core Service i Core OS.

3.3.1. Bezbednost sistema

Apple je razvio bezbednosni model koji objedinjuje hardverske i softverske komponente u cilju zaštite korisničkih podataka i očuvanja integriteta operativnog sistema. Ovaj nivo zaštite predstavlja značajan izazov u forenzičkim istragama, posebno kada je uređaj zaključan i nije jailbreak-ovan jer onemogućava pristup kritičnim sistemskim podacima i aplikacijama bez odgovarajućih autorizacija.

3.3.1.0. Sigurnosno pokretanje procesa

Potpisivanje koda je proces digitalnog potpisivanja izvršnih fajlova ili softvera kako bi se verifikovala autentičnost i integritet programa u cilju sprečavanja instalacije neproverenih aplikacija.

3.3.1.1. Bezbedna enklava

Bezbedna enklava predstavlja izolovano okruženje unutar iOS uređaja, koje funkcioniše nezavisno od glavnog procesora i poseduje sopstevni memorijski kontroler i kriptografske funkcije. Njen dizajn se zasniva na principu separacije privilegija.

3.3.1.2. Zaštita podataka

Apple primenjuje enkripciju celog diska, kojom šifruje kompletan sadržaj uređaja, uključujući sistemske i korisničke podatke. Operativni sistem definiše dva ključna stanja: before first unlock (BFU) i after first unlock (AFU). Ključnu ulogu u sigurnosti igra jedinstveni UID ključ, ugrađen u bezbednu enklavu.

3.4. Android

Zbog otvorene prirode Android platforme, uređaji mogu biti podložni zloupotrebama, naročito ukoliko ne dobijaju redovna bezbednosna aužuriranja. U takvim slučajevima, zlonamerne aplikacije mogu iskoristiti poznate ranjivosti, kompromitovati izolovano oktuženje i steknuti neovlašćene privilegije, što dovodi do ugrožavanja sigurnosti sistema.

3.4.0. Arhitektura

U osnovi arhitekture se nalazi Linux kernel, koji predstavlja temelj čitavog sistema. Iznad njege nalaze se Hardware Abstraction Layer, Android Runtime i Application Framework.

3.4.1. Bezbednost sistema

Bezbednosna arhitektura u velikoj meri se oslanja na Trusted Execution Environment ili Secure Element okruženja. Savremene verzije Android-a podržavaju ugrađenu enkripciju podataka za razliku od ranijih verzija koje često nisu imale podrazumevano omogućeno šifrovanje diska, niti su posedovale druge naprednije bezbednosne mere zaštite.

3.4.1.0. Šifrovanje diska

FBE deli skladišni prostor uređaja na dva odvojena kriptografska prostora: Credential Encrypted i Device Encrypted prostor.

3.4.1.1. Trusted Execution Environment

Trusted Execution Environment predstavlja izolovano hardevrsko okruženje dizajnirano za bezbedno čuvanje i obradu osetljivih podataka, kao što su korisničke lozinke, kriptografski ključevi i biometrijske informacije. Kriptografski ključevi nikada ne napuštaju ovaj prostor u nešifrovanom obliku.

3.4.1.2. Sigurnosni moduli

Samsung Knox predstavlja sveoubuhvatan bezbednosni okvir integrisan u određene Android uređaje, koji obezbeđuje zaštitu od hardverskog do aplikacionog sloja sistema. U kontekstu otključavanja ekrana ima bitnu ulogu u zaštiti biometrijskih i autentifikacionih podataka, koji se čuvaju u izolovanim okruženjima kao što su Knox Vault i TrustZone.

3.5. Prikupljanje dokaza

Tipovi metoda koje se koriste u istragama su ručna ekstrakcija, logička ekstrakcija i fizička ekstrakcija, prikupljanje iz oblaka i prikupljanje iz celularne mreže. Svaka od ovih metoda ima svoje prednosti i ograničenja, a izbor odgovarajuće tehnike uslovljen je nivoom pristupa samom uređaju kao i tipom informacija koji je od interesa za istragu.

3.5.0. Forenzičke metode akvizicije podataka

Metoda ručnog prikupljanja je izvodljiva jedino ako je uređaj funkcionalan i otključan. Logičko prikupljanje ne zahteva dublju intervenciju sa hardverom ili operativnim sistemom uređaja, ali je najčešće ograničena ukoliko nije moguće dobiti autorizaciju za pristup. Fizička ekstrakcija je najbolji izbor kada je potreban potpun pristup svim podacima ali je za njeno izvođenje potrebna visoka ekspertiza.

3.5.0.0. JTAG i Chip-off

Tehnike fizičke ekstrakcije poput JTAG i Chip-off mogu se koristiti i za pokušaj zaobilaženja zaključanog ekrana. JTAG se koristi za ekstrahovanje slike memorije, uključujući i fajlove koji sadrže podatke o PIN-u, šablonu ili enkripcionim ključevima

3.5.0.1. Android Debug Bridge

Android Debug Bridge (ADB) je alat koji omogućava komunikaciju između računara i mobilnog uređaja putem USB-a i pod specijalnim uslovima, može da se korsti za otključavanje ekrana starijih Android modela kada šifra i šablon nisu poznati.

3.5.1. Evolucija zaštitnih mehanizama

Evolucija zaštitnih mehanizama na mobilnim uređajima značajno je ograničila forenzičke mogućnosti za prikupljanje dokaza i tradicionalni pristupi postaju sve manje efikasni u situacijama kada je uređaj zaključan i ne postoji mogućnost saradnje sa korisnikom.

4. METODE OTKLJUČAVANJA TELEFONA

U ovom odeljku razmatrane su različite metode otključavanja telefona koji koriste biometrijsku autentifikaciju, šablon ili lozinku. Primeri uspešnih slučajeva otključavanja, opisani u ovom delu rada, preuzeti su iz stručne literature i naučnih radova.

4.1. Spoofing metode i biometrijska autentifikacija

Spoofing napad je napad tokom koga se lažira identitet odnosno biometrijski parametar korisnika kako bi se prevario sistem i dobio pristup uređaju. U cilju sprečavananja ovih napada, savremeni operativni sistemi se oslanjaju na različite tehnike detekcije živosti.

4.1.0. Vrste senzora za prepoznavanje otiska prsta

Postoje tri vrste senzora koji se ugrađuju u mobilne uređaje i to su: optički, kapacitativni i ultrazvučni. Svaki od ovih senzora ima različit stepen otpornosti na prepoznavanje replika.

4.1.0.0. Metode kloniranja otisaka prstiju

Istraživači i forenzički stručnjaci pokazali su da je moguće izraditi veštačke otiske prstiju korišćenjem materijala kao što su silikon, lateks ili čak glina.

4.1.1. Tehnologija skeniranja lica

Postoje dve vrste skenera za prepoznavanje lica koji koriste mobilni uređaji i to su 2D i 3D skeneri. Najpoznatiji primer je Apple Face ID koji koristi 3D tehnologiju skeniranja.

4.1.1.0. Metode replikacije facijalnih karakteristika

Spoofing napad nad ovim mehanizmom se može izvesti upotrebom fotografija visoke rezolucije, videa ili čak izradom kvalitetnih 3D maski.

4.1.2. Tehnologija skeniranja mrežnjače

Skeniranje mrežnjače koristi infracrvenu kameru za skeniranje jedinstvenog obrasca šarenice oka korisnika. Ova autentifikacija se pokazala manje praktična u poređenju sa drugim oblicima autentifikacije zbog čega je i slabo zastupljena kod komercijalnih telefona.

4.2. Brute-force metode oktljučavanja ekrana

PIN-ovi, lozinke i obrasci mogu biti podložni napadima grubom silom koji se svode na sistematsko nagađanje i isprobavanje svih mogućih kombinacija unosa. Sprovođenje ove tehnike je skoro nemoguće na modernim uređajima zbog mehanizama koji definišu dozvoljen broj pokušaja i korišćenje vremenskog intervala za kašnjenje između pogrešnih unosa.

4.2.0. Alati za automatizaciju procesa pogađanja

Kako bi se proces ručnog unosa kredencijala optimizovao i kako bi se izbegle bezbednosne prepreke, u forenzičkim istragama se koriste alati poput IP Box 3, Atiny85 i GrayKey-a.

4.3. Zaobilaženje zaključanog ekrana Android uređaja 5.1 i starijih verzija

U ovom odeljku su opisane metode zaobilaženja zaključanog ekrana koje se oslanjaju na iskorišćavanje slabosti u korisničkom interfejsu starijih modela.

4.3.0. Postupak “rušenja“ ekrana

Ovaj napad zahteva fizički pristup uređaju i uključuje unos dugog niza znakova u polje za lozinku putem funkcije hitnog poziva, što dovodi do rušenja interfejsa i omogućava pristup bez unosa ispravne lozinke.

4.3.1. Forgot pattern/password opcija

Na uređajima sa operativnim sistemom Android verzije 4.4, funkcija forgot password/pattern omogućavala je korisniku da resetuje šablon za otključavanje pomoću validnog email naloga.

4.4. Otključavanje mobilnih uređaja preko Cloud naloga

Ovaj metod je koristan jer omogućava otključavanje mobilnih uređaja direktno sa cloud naloga korisnika.

4.5. Metode socijalnog inženjeringa

Ova tehnika se ne oslanja na hardverske ili softverske alate, već na manipulaciju ljudima kako bi se dobio pristup osetljivim informacijama. Zastupljeni oblici ovog napada su phishing, vishing, pretexting.

4.5.0. Shoulder surfing

Shoulder surfing je tehnika koja podrazumeva direktno ili inderektno posmatranje korisnika dok unosi svoje podatke za autentifikaciju kao što su pin kod, šifra ili obrazac.

5. DEMONSTRACIJA I DISKUSIJA

U ovom odeljku su demonstrirane odabrane metode otključavanja ekrana na testnim uređajima.

5.1. Izrada silikonskog otiska prsta

Proces kreiranja lažnog otiska se odvijao u nekoliko iteracija, tokom kojih je izveden zaključak da je najkvalitetnija replika u ovom eksperimentu dobijena upotrebom silikona RTV i parafin voska. Na slici 1. prikazan je krajnji rezultat replikacije koja iako verna originalu, nije uspela da prevari sistem koji koristi kapacitativni senzor.

Slika 1. *Otisak prsta od silikona*

Zagrejan vosak je prvo izliven u plitku metalnu posudu i posle izvesnog vremena kada je podloga postala dovoljno tvrda, na njoj se mogao utisnuti šablon pravog otiska. Zatim je dodat tanak sloj jestivog skroba i silikona. Nakon što se smesa stvrdnula, posuda je ubačena u ključalu vodu kako bi se materijali prirodno razdvojili usled razlike u temperaturi topljenja silikona i voska.

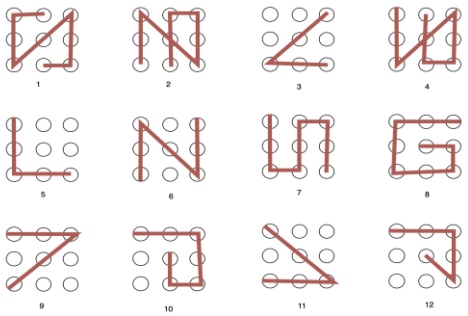
5.2. Otključavanje fotografijom lica

Testni uređaj Redmi 7A sa Android verzijom 9 koji koristi 2D tehnologiju skeniranja lica, uspešno je otključan sa slikom korisnika. Slika je bila visokog kvaliteta i lice je jasno prikazano na fotografiji.

Rezultati studije [3] pokazali su veliki potencijal upotrebe veštačke inteligencije i slika dostupnih na društvenim mrežama korisnika kako bi se izradio virtuelni avatar koji može da prevari sisteme sa naprednijim tehnologijama skeniranja.

5.3. Rekonstrukcija šablona

Sprovedena anketa imala je za cilj da prikupi testni skup šablona zaključavanja ekrana kako bi se uočile i uporedile karakteristike najčešćih odgovora. Na slici 2. je prikazan deo rezultata.



Slika 2. Deo rezultata ankete

Od 42 uzorka, 11 figura je bilo jedinstveno nad datim skupom što dovodi do zaključka da je četvrtina ispitanika koristila šablon koji se nije našao kao zaštita ekrana ni na jednom uređaju ostalih korisnika. Trend koji je primećen kod ovih podataka jeste da u približno 80% slučajeva korisnici su izabrali početak crteža da bude u levom gornjem uglu i da su oblici L i N bili učestal izbor.

5.4. Otključavanje preko ADB-a

Otključavanje ekrana Redmi 7A, ili bilo kog drugog uređaja, preko ADB-a nije uvek izvodljivo jer zavisi od više preduslova koji moraju biti ispunjeni pre nego što dođe do zaključavanja. Na telefonu je potrebno omogućiti režim za programere i uspostaviti komunikaciju radne stanice i testnog uređaja putem verifikacije računara prilikom povezivanja. Zatim ako je ovo ispunjeno, potrebno je izvršiti set komandi za brisanje određenog fajla koji bi omogućio pristup telefonu bez unosa lozinke. Ovaj postupak je bio učinkovit na starijim verzijama Android-a ali usled napredne zaštite sistema uvedene od verzije 9 i kasnije, ovaj metod se pokazao neučinkovit na testnom uređaju.

3. ZAKLJUČAK

Rad ukazuje da nema univerzalnog rešenja za otključavanje mobilnih uređaja. Umesto toga, potrebno je proceniti svaki slučaj ponaosob, uz izbor metode koja balansira između efikasnosti, očuvanja dokaza, tehničkih mogućnosti i pravne validnosti.

Predlozi za dalja istraživanja se odnose na primenu saznanja i tehnologija iz oblasti mašinskog učenja i veštačke inteligencije u predikciji biometrijskih šablona i obrazaca korisničkog ponašanja, kao i u optimizaciji napada grubom silom. Može se izdvojiti i orijentacija ka razvoju naprednih softverskih alata za analizu ranjivosti u operativnim sistemima, uključujući istraživanje procesa Secure Boot-a i USB protokola, uz potencijalnu primenu mašinskog učenja za automatizovano otkrivanje slabosti.

7. LITERATURA

[1] Prof. dr Stevan Gostojić, Fakultet tehničkih nauka, Novi Sad, predmet Digitalna forenzika, Uvod u digitalnu forenziku (predavanja 2023, lekcija 1)

[2] Mobile operating systems popularity statistics, https://gs.statcounter.com/os-market share/mobile/worldwide (pristupljeno u septembru 2025.)

[3] Yi Xu, True Price, Jan-Michael Frahm, Fabian Monrose. Virtual U: Defeating Face Liveness Detection by Building Virtual Models from Your Public Photos, USENIX Security Symposium 2016.

Kratka biografija:

Jelena Petrić rođena je u Novom Sadu 2000. Diplomirala je na Fakultetu tehničkih nauka 2023. godine. Master rad na Fakultetu tehničkih nauka iz oblasti Elektrotehnike i računarstva odbranila je 2025. godine

kontakt: jelena.petric@uns.ac.rs