JOURNAL of COMPUTER SCIENCES INSTITUTE

JCSI 9 (2018) 302-307
Wysłane: 2018-06-22
Przyjęte: 2018-06-27

Ocena zabezpieczeń wybranej platformy mobilnej

Aleksandra Iwaniuk*

Politechnika Lubelska, Instytut Informatyki, Nadbystrzycka 36B, 20-618 Lublin, Polska

Streszczenie. Smartfony sukcesywnie zyskiwały na popularności, by w efekcie praktycznie zupełnie wyprzeć tradycyjne telefony. Stwarzają one wiele możliwości, jednak stają się też źródłem zagrożeń. W artykule poddano analizie zabezpieczenia systemu Android. Sprawdzono jakie zagrożenia czyhają na urządzenia mobilne a także jak system Android stara się przed nimi uchronić. Badaniem ankietowym sprawdzono, jak blokowane są ekrany telefonów a także jak często dokonywane są zmiany w blokadzie. Aby sprawdzić, czy blokadę ekranu można zdjąć przeprowadzono testy przy użyciu Google znajdź urządzenie, a także Dr. Fone. Przedstawiono zestawienie wyników a następnie wyciągnięto wnioski.

Słowa kluczowe: Android; bezpieczeństwo; testowanie zabezpieczeń

*Autor do korespondencji.

Adres e-mail: aleksandra.kowaluk3@gmail.com

Security assessment of the selected mobile platform

Aleksandra Iwaniuk*

Institute of Computer Science, Lublin University of Technology, Nadbystrzycka 36B, 20-618 Lublin, Poland

Abstract. Smartphones were gradually gaining popularity, so as to effectively replace traditional telephones. Devices creates many capabilities, but they can be a source of threats. In this article analyzed Android system security. Author checked what threats lurk for mobile devices and how the Android system tries to protect them. The questionnaire survey checked how the phone screens are blocked and how often changes are made to the blockade. To check if the screen lock can be removed, tests were performed using Google to find the device, as well as Fone. A summary of results was presented and conclusions were drawn.

Keywords: Android; security; security testing

*Corresponding author.

E-mail address: aleksandra.kowaluk3@gmail.com

1. Wstęp

Historia Androida rozpoczyna się w momencie założenia firmy Android Inc.,w październiku 2003 r. przez Andyego Rubina, Chrisa Whitea, Nicka Searsa i Richa Micera. W wyniku powstałych trudności w 2005 roku została wykupiona przez Google. W 2007 roku powstało konsorcjum OHA zrzeszające twórców oprogramowania i sprzętu. Dzięki systematycznemu rozwojowi systemów mobilnych Android w 2016 posiadał 64% udziałów w rynku [8].

W związku z dużą ilością użytkowników systemu Android doczekał się wielu wirusów i szkodliwych aplikacji. Zagrożenia te mogą mieć związek z użytkownikiem a także z lukami w zabezpieczeniach [1].

Niniejszy artykuł ma na celu omówienie zabezpieczeń, które chronią system Android, a także zagrożenia czyhające na urządzenia mobilne.

Przyjęto tezę: *Wbrew powszechnie akceptowanemu poglądowi dane użytkownika są bezpieczne.* Poddano również analizie świadomość użytkowników smartfonów a także wyniki odblokowania każdej z metod odblokowania ekranu, przeanalizowano czasy osiągnięte przez każdą z grup. Na tej podstawie wybrano najprostszą metodę. Sprawdzono też, czy jest możliwe zdjęcie blokady z ekranu smartfonu.

2. Rodzaje ataków

Z uwagi na objęcie pozycji lidera w rynku światowym, na urządzenia z systemem Android czyha wiele zagrożeń, działających na różnych założeniach.

2.1. Nieautoryzowany dostęp do danych

Urządzenia mobilne charakteryzuje to, że są praktycznie cały czas przy użytkowniku, stwarza to zagrożenie jego utraty. W momencie utraty urządzenia, jeśli brak skutecznej blokady ekranu może dojść do nieautoryzowanego dostępu do danych [3].

2.2. Ataki na aplikacje

Aplikacje mogą zostać zaatakowane na dwa różne sposoby. Jeden z nich jest statyczny a drugi dynamiczny. Metoda statyczna polega na dokonaniu zmian w aplikacji, konkretnie w plikach dex lub apk. Metoda dynamiczna polega na dokonaniu zmian w trakcie działania aplikacji [4].

2.3. Programy szpiegujące

Programy szpiegujące są to aplikacje zbierające lub kradnące dane użytkownika. Najczęściej źródłem ataku na aplikacje jest adware (nękająca użytkownika reklama), po wejściu w link w tle odbywa się instalacja. Aplikacje te nie tylko naruszają bezpieczeństwo, ale mogą też udzielać dostępu innym aplikacjom a także zmniejszać zasoby urządzenia poprzez wysłanie danych do bazy [3].

2.4. Ataki phishingowe

Ataki phishingowe polegają na podszywaniu się pod zaufane lub nieszkodliwe firmy np. bank. Ataki te mają na celu pozyskanie od użytkownika wrażliwych danych np. hasła i PINu do konta bankowego. Może to osiągnąć na kilka sposobów: MMS z adresem URL do fałszywej strony banku, wysłanie adresu URL poprzez SMS a także atak poprzez połączenia głosowe [5].

2.5. Przelewanie

Przelewanie jest to atak pozwalający na uzyskanie od atakowanych środków pieniężnych a następnie przelanie środków na konto agresora. Może się to odbywać poprzez korzystanie z usług pay-per-use [6].

2.6. Ataki TOCTOU

Luka w zabezpieczeniach TOCTOU (Time of Check to Time of Use) istnieje w systemie Android głównie na zasadzie zmowy nazewnictwa. Uprawnienia są przechowywane w systemie jako ciąg znaków. Dlatego też dwa uprawnienia o takim samym łańcuchu są traktowane jako równoważne, nawet jeśli odnoszą się do niezwiązanych aplikacji. Aplikacja może tym sposobem uzyskać dostęp do zasobów, do których zasoby nie były jej przyznane [10].

2.7. Złośliwe aplikacje

Złośliwe aplikacje można pobrać wraz z aplikacją, którą użytkownik chce pobrać, lub poprzez odwiedzenie podejrzanych stron. Można wyróżnić wiele złośliwych aplikacji takich jak:

• Trojany – są to aplikacje mogące uzyskać kontrolę nad urządzeniem. Często wykazują użyteczne funkcjonalności, przy czym działania szkodliwe wykonywane są w tle. Można z ich pomocą uzyskać dostęp do wrażliwych danych a także zainstalować na urządzeniu inne szkodliwe aplikacje np. botnety.

• Botnety – określa się tym terminem grupę urządzeń zdalnie kontrolowanych i koordynowanych. Wykorzystuje on zaatakowane urządzenia np. do rozsyłania wiadomości SPAM.

• Rootkity – są to aplikacje uprawnione (w nieautoryzowany sposób) do osiągania bogatego zasobu uprawnień. Obecność aplikacji najczęściej jest maskowana przed użytkownikiem.

• Robaki – to samo-replikujące się szkodliwe aplikacje. Mogą one uzyskiwać dostęp do wrażliwych danych użytkownika [2].

3. Zabezpieczenia Androida

Wprowadzono liczne zabezpieczenia mające chronić użytkownika, jego dane i urządzenie.

3.1. Uprawnienia i selekcja uprawnień

Aby aplikacja działała poprawnie muszą jej nadane odpowiednie uprawnienia. Odbywa się to poprzez wpisanie odpowiednich uprawnień do pliku AndroidManifest.xml. Podstawowe aplikacje Android nie posiadają przypisanych domyślnie uprawnień, pozwalających na dostęp do zasobów. Przed instalacją aplikacji wyświetlana jest informacja o wszystkich wymaganych przez aplikację uprawnieniach [6].

Uprawnienia aplikacji podlegają separacji. System Android wymaga, aby każda aplikacja posiadała własny identyfikator użytkownika (UID) i identyfikator grupy (GID). Gwarantuje to, że aplikacje lub procesy nie mają uprawnień dostępu do innych aplikacji lub procesów.

Aby umożliwić separację każda z aplikacji działa w dedykowanym Sandboxie. Sandboxingowi przyświeca zasada, aby żadna aplikacja nie miała możliwości nadpisania i zmian w kodzie innych aplikacji [9].

3.2. Podpis aplikacji

Wszystkie paczki z aplikacjami instalowanymi na urządzeniach muszą posiadać stosowny certyfikat. Dzięki temu użytkownik może stwierdzić autentyczność aplikacji. Pomaga to ustalić prawdziwy związek między użytkownikiem a twórcą. Nie istnieje jednak żaden urząd przyznający certyfikaty. Są więc one generowane przez twórców oprogramowania. Oznacza to, że użytkownik musi się wykazać zaufaniem do twórcy oprogramowania [7].

3.3. Pochodzenie aplikacji

Aby rozpocząć dystrybucję aplikacji za pośrednictwem Google Play Store programista musi założyć konto o odpowiednich uprawnieniach i uiścić opłatę w wysokości 25$. Przed przesłaniem do Google Play aplikacja musi zostać cyfrowo podpisana. Podpisu może oczywiście dokonać twórca oprogramowania [11].

3.4. Ochrona danych

Każda aplikacja działa w odseparowanej części systemu Android. Izolacją systemów od siebie steruje jądro Linux systemu. Dodatkowo mechanizm bezpieczeństwa jest oparty o system uprawnień a także procesów, jakie każda aplikacja może wykonać. Aplikacje są identyfikowane po kluczu aplikacji. Dostęp do danych jest nadawany w czasie rzeczywistym. Bezpieczeństwo danych opiera się głównie na mechanizmie podpisu aplikacji. System, jak i aplikacje potrzebują podpisu do prawidłowego funkcjonowania [8].

3.5. Statyczna i dynamiczna analiza aplikacji

Dwoma podstawowymi praktykami jest statyczna i dynamiczna analiza aplikacji, mająca na celu wykrycie ataku. Analiza statyczna wykorzystuje dekompilację, odszyfrowanie, dopasowywanie wzorców, a także analizę wywołań systemowych. W trakcie analizy program nie jest wykonywany. Podstawową praktyką analizy jest filtrowanie binarne, w celu wykrycia złośliwego kodu, wykorzystując przy tym sygnatury programów.

Inną metodą wykrywania wirusów, jest dynamiczna analiza. Obejmuje ona uruchamianie systemu w kontrolowanym środowisku i obserwację jego zachowania. Zawarta w tym jest obserwacja wymiany plików, połączenia sieciowego, zachodzących procesów itp. Podstawowym sposobem na dynamiczne sprawdzenie oprogramowania jest sandboxing. Sandbox może być definiowany jako środowisko, w którym wykonywany jest proces [10].

4. Metoda badań ankietowych

Badanie ankietowe przeprowadzono w celu zbadania świadomości użytkowników smartfonów o zabezpieczeniach i bezpieczeństwie urządzeń mobilnych. Jednym z założeń, było sprawdzenie, jak użytkownicy blokują swoje urządzenia, czy dokonują zmian w sposobie blokady a także ustalenie najbardziej przyjaznej metody blokowania ekranu.

Zastosowano urządzenia: Xiaomi Redmi 3S Pro, Sony Xperia S a także tablet Sony Xperia Z3. Każde z urządzeń cechuje inna wielkość wyświetlacza, miało to na celu zbadanie, czy wielkość ekranu ma wpływ na wynik odblokowania ekranu.

Na każdym z urządzeń dokonano następujących testów:

- Odblokowanie urządzenia kodem PIN o długości 4 znaków.
- Odblokowanie urządzenia kodem PIN o długości 8 znaków.
- Odblokowanie urządzenia hasłem o długości 4 znaków.
- Odblokowanie urządzenia hasłem o długości 8 znaków.
- Odblokowanie urządzenia wzorem o długości 4 znaków.
- Odblokowanie urządzenia wzorem o długości 8 znaków.

Otrzymane wyniki poddano analizie w oparciu o wyniki uczestników badania. Na tej podstawie przeprowadzono stosowne analizy.

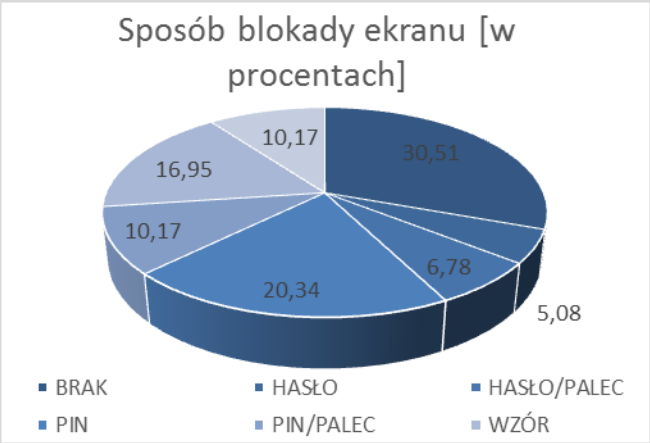
Badanie ankietowe przeprowadzono na grupie 66 osób. Badane osoby były w wieku 18-65 lat. Podzielono je na grupy wiekowe: do 20 lat, 20-30 lat, 30-40 lat, 40-50 lat, a także 50+. Podział miał na celu ułatwienie analizy danych. Badane osoby mieszkają zarówno w mieście jak i na wsi, nie dokonano jednak podziału ze względu na wielkość miasta (np. ze względu na liczbę mieszkańców). Osoby biorące udział w badaniu w większości nie były osobami związanymi z branżą IT.

5. Analiza badań ankietowych

Przeprowadzono analizę danych demograficznych, na ich podstawie zauważono, że większość wśród badanych stanowili mieszkańcy miast, wśród płci dominowali mężczyźni natomiast ze względu na wiek przeważały osoby w wieku 30-40 lat.

Rys. 1. Użycie smartfonu wśród ogółu ankietowanych.

Ankietowanych zapytano o użycie smartfonów (Rys. 1). Można zauważyć, że większość badanych (89,39%) na co dzień używa smartfonów. Nie stosowano podziału na system operacyjny stosowanego urządzenia. Jest to zbieżne z danymi na temat udziału w rynku telefonów [12]. Sprawdzono, jaki sposób blokady jest stosowany przez ankietowanych (Rys.2).



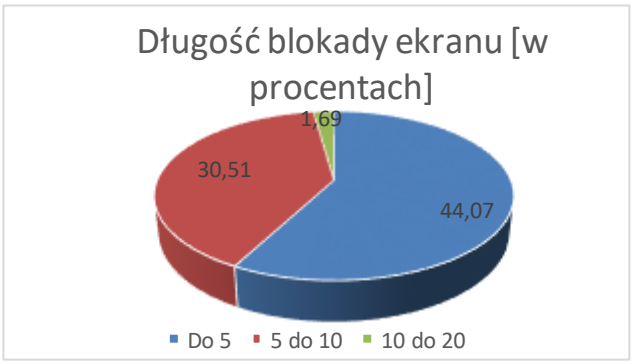
Rys. 2. Sposób blokady ekranu.

Przeanalizowano również deklarowany przez użytkowników sposób blokady ekranu. Niestety większość, bo 30,51% ogółu nie stosuje żadnej blokady ekranu (przeciągnięcie). Wśród powszechnie dostępnych metod blokady ekranu największą popularnością cieszył się kod PIN, na drugim miejscu wzór, najmniejszą zaś hasło. Można również zauważyć sporą popularność danych biometrycznych takich jak odcisk palca. Muszą one jednak być wspierane przez inną blokadę ekranu jak np. kod PIN.

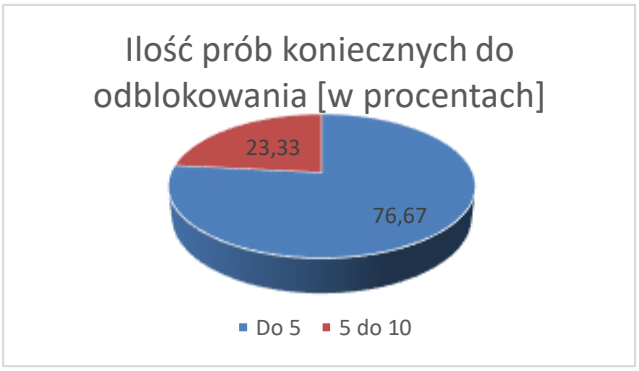
Innym istotnym elementem zabezpieczeń urządzeń mobilnych jest długość blokady ekranu (Rys.3).

Najbardziej popularną długością blokady ekranu jest blokada do 5 znaków. Mniejszą popularnością cieszyły się kody 5-10 znakowe. Najmniejszą grupę stanowiły blokady 10-20 znakowe. Ankietowanych zapytano, czy każda próba odblokowania urządzenia kończy się sukcesem. Ankietowanych którzy przyznali że nie zawsze udaje im się

odblokować urządzenie zapytano ile prób najczęściej potrzebują do odblokowania urządzenia (Rys. 4).

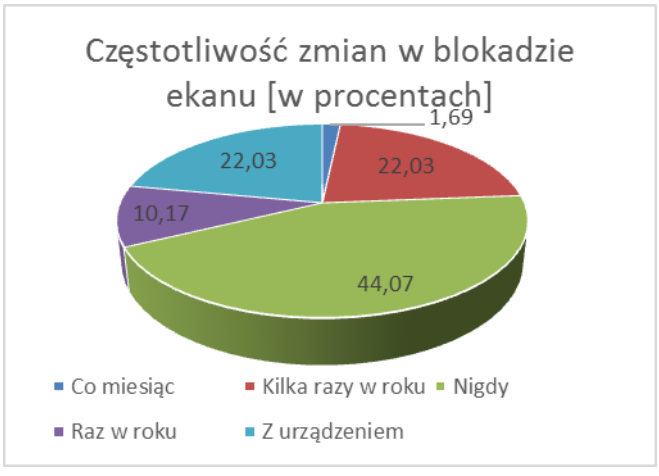


Rys. 3. Długość blokady ekranu.



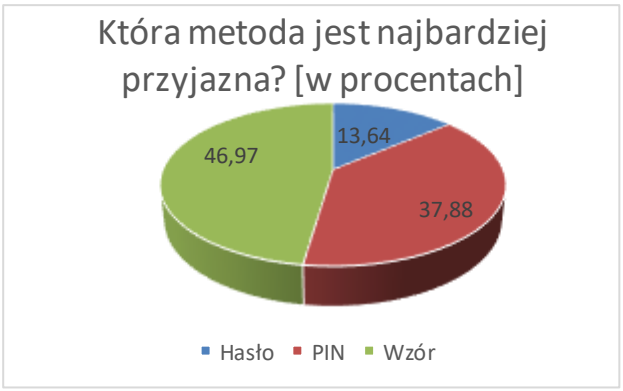
Rys. 4. Liczba prób potrzebnych do skutecznego oblokowania urządzenia.

Najczęściej ankietowani, którzy wymagali wielu prób najczęściej potrzebowali do 5 prób aby odblokować urządzenie. Mniejszą grupę stanowiły osoby potrzebujące 5 do 10 prób odblokowania. Nie wykazano w trakcie badania zapotrzebowania na większą liczę prób. Kolejnym pytaniem zadanym ankietowanym była częstotliwość zmian w blokadzie ekranu. Wliczano w to zmianę w obrębie sposobu np. zmiana z „1234" na „1235", jak również zmiany sposobu blokady np. z kodu PIN na wzór.



Rys. 5. Częstotliwość zmian w blokadzie ekranu.

Zauważyć można, że większość użytkowników nigdy nie dokonuje zmian w blokadzie ekranu. Uwzgledniono w tym wykresie zarówno osoby które stosują jedną z metod blokady ekranu a także osoby nie blokujące telefonu. Najpopularniejszą opcją wśród dokonujących zmian były zmiany wraz ze zmianą urządzenia a także zmiana kilka razy w roku. Zapytano uczestników ankiety o opinię na temat metody najbardziej przyjaznej użytkownikowi (Rys. 6).



Rys. 6. Opinia ankietowanych na temat najwygodniejszej metody blokowania ekranu.

Według ankietowanych metodą najbardziej przystępną użytkownikom jest wzór, najmniej zaś hasło. Opinia ta wyrażona została zarówno przez osoby stosujące na co dzień smartfony jak i użytkowników tradycyjnych urządzeń.

6. Metoda badań nad zdjęciem blokady

Przeprowadzono również badanie fizycznego urządzenia. Poddano analizie tablet Sony Xperia Z3 a także smartfon Xiaomi Redmi 3S Pro. Sukcesem metody będzie zdjęcie blokady bez utraty danych. Sprawdzone zostanie, czy konieczne jest tzw. Rebootowanie systemu, czy uda się to osiągnąć inną metodą. Przeanalizowanych zostanie kilka metod i oceniona zostanie ich skuteczność.

Ocenie zostanie poddana metoda:

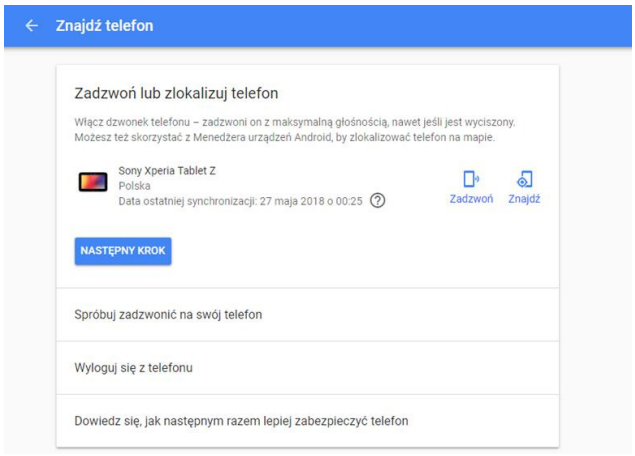
- Google znajdź urządzenie,
- Dr fone.

7. Badania nad zdjęciem blokady ekranu

7.1. Google znajdź urządzenie

Jest to opcja dostarczana przez Google, dzięki której można namierzyć swoje urządzenie, można też je zablokować a także wyczyścić zawartość pamięci. Wystarczy tylko aby urządzenie było włączone, użytkownik musi być zalogowany na koncie Google, musi mieć włączone Wi-fi lub transmisję danych. Można za pomocą tego narzędzia zmienić blokadę ekranu na nową.

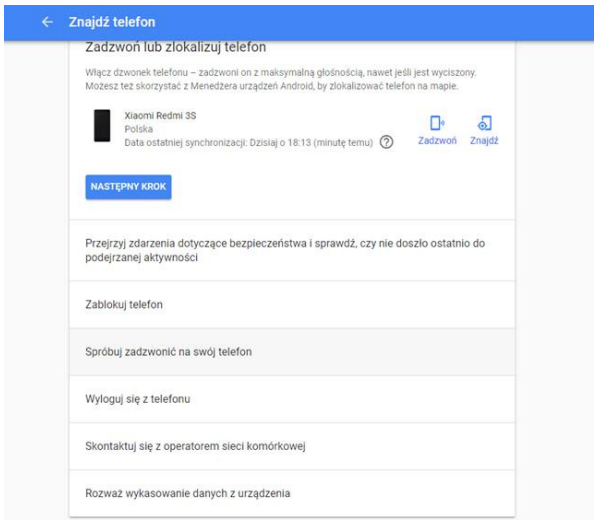
W przypadku tabletu Sony nie było możliwe dokonanie zmiany hasła, z uwagi na brak stosownej opcji w menu narzędzia (Rys. 7).



Rys. 7. Menu główne narzędzia znajdź urządzenie tabletu Sony.

Sprawdzono tą metodę również na urządzeniu Xiaomi (Rys. 8).

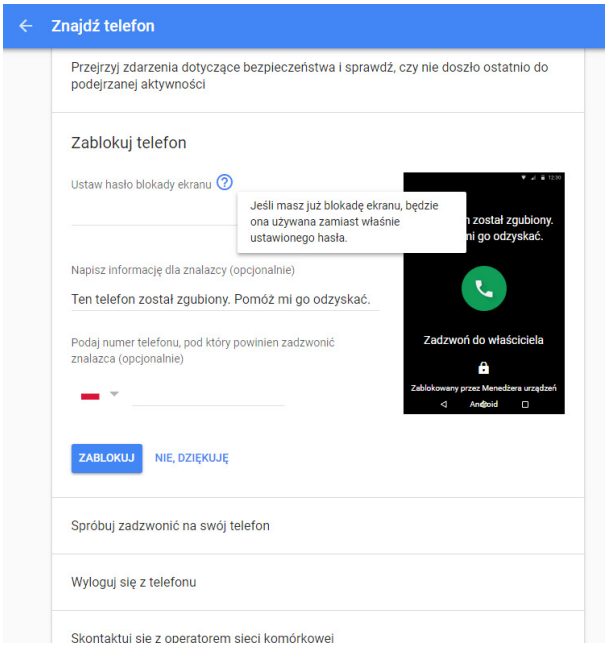
Aby metoda zadziała urządzenie musi być połączone z siecią Wifi lub transferem mobilnym, a także być zalogowanym na koncie Google. W ten sposób po zalogowaniu na Google znajdź urządzenie uzyskuje się dostęp do m.in. lokalizacji urządzenia. Innymi funkcjonalnościami oferowanymi przez Google jest odtworzenie zdalne dzwonka, umieszczenie na ekranie informacji, jak skontaktować się z właścicielem, zablokowanie urządzenia lub jego wyczyszczenie.



Rys. 8. Menu główne narzędzia znajdź urządzenie smartfonu Xiaomi.

W przypadku tego urządzenia opcje wszystkie były dostępne (Rys. 9), wobec czego można było przeprowadzić testy.

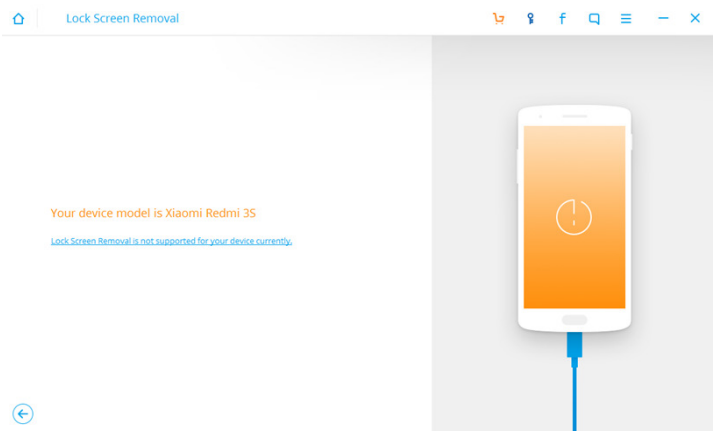
Po wybraniu stosownych opcji „Zablokuj telefon" uzyskuje się kilka opcji, jedną z nich jest interesująca z punktu widzenia testów „Ustaw hasło blokady ekranu". Należy w tym miejscu ustawić nowe hasło odblokowania i odblokować nim urządzenie.



Rys. 9. Opcje zmiany blokady ekranu.

7.2. Dr fone

Dr Fone to program komputerowy oferujący wiele opcji, jedną z nich jest zdjęcie blokady ekranu zdalnie. Do przeprowadzenia próby konieczne jest urządzenie mobilne i komputer z zainstalowanym programem połączonych kablem USB. Aplikacja po wyborze interesującej opcji program łączy się z urządzeniem mobilnym. Niestety w obu przypadkach urządzenie nie jest wspierane przez program (Rys. 10).



Rys. 10. Efekt działania Dr. Fone

Oznaczać to może nieskuteczność metody. Nie można z jej pomocą zdjąć blokady z powodu braku wsparcia przez aplikację.

8. Wnioski

Na podstawie badań przeprowadzonych na 66 osobach zauważono, że większość osób współcześnie używa smartfonów. Niestety większość z nich nie stosuje skutecznej ochrony swojego urządzenia a także danych na nim

zgromadzonych. Wśród osób stosujących skuteczniejszą ochronę urządzenia najpopularniejszą blokadą urządzenia był kod PIN, najmniej popularną było hasło. Można zauważyć spore zainteresowanie danymi biometrycznymi takimi jak odcisk palca. Użytkowników smartfonów zapytano o długość hasła, w większości hasła miały do 5 znaków długości, najczęściej jest to zbyt mało, aby niemożliwe było obejście blokady atakiem brutal force. Duża część użytkowników zadeklarowała konieczność wykonania do 5 prób, aby skutecznie odblokować urządzenie. Najczęściej mimo wiedzy o wpływie zmian w blokadzie ekranu, użytkownicy zmian tych nie dokonują wcale lub dokonują ich wraz ze zmianą urządzenia. Zapytani o najbardziej przyjazną użytkownikowi metodę blokady ekranu wskazano najczęściej wzór, najmniej zwolenników uzyskało hasło.

Na postawie analizy źródeł można wywnioskować, że na urządzenia z systemem Android stworzono wiele rodzajów ataków i zagrożeń, system Android opracował wiele sposób ochrony przez zagrożeniami, zdarza się jednak że zabezpieczenia zawodzą. Często w kontekście bezpieczeństwa najsłabszym z ogniw jest użytkownik nie przykuwający należytej uwagi do bezpieczeństwa urządzenia i danych na nim zgromadzonych.

Przeprowadzone badania z użyciem urządzeń mobilnych można zauważyć, że zdjęcie lub obejście blokady ekranu nie jest łatwym zadaniem i nie zawsze okazuje się skuteczne. Jednym ze sposobów zabezpieczenia przed obejściem blokady jest zachowanie wyłączonego Debugowania przez USB, uchroni to urządzenie przed spora grupą metod korzystających z połączenia USB. Odnosząc się do postawionej tezy można zauważyć, że przy należytej uwadze i prawidłowym nawykom użytkowników dane przechowywane na urządzeniach mobilnych są bezpieczne. W przypadku braku świadomości lub lekceważenia bezpieczeństwa, dane te nie mają zagwarantowanego bezpieczeństwa.

Literatura

[1] Drake J.J. Fora P.O. Lanier Z. Mulliner C. Pidley S. A. Wicherski G., Android Podręcznik Hackera, Helion, 2015.

[2] Bing H., Analysis and Research of System Seciurity Based on Android, Fifth International Conference on Intelligent Computation Technology and Automation, 2012

[3] Mu J. Cui A. Rao J., Android Mobile Security – Threats and Protection, International Conference on Computer, Network and Communication Engineering, 2013.

[4] Wu X. Li X, Hack Android Application and Defence, 3rd International Conference on Computer Science and Network Technology, 2013.

[5] Weidman G., Bezpieczny system w praktyce. Wyższa szkoła hackingu i testy penetracyjne, Helion, 2015.

[6] Rashidi B. Fung C., A Survey of Android Security Threats and Defenses, ResearchGate, 2015.

[7] Fang Z. Han W. Li Y., Permission based Android security: Issues and countermeasures, Research Collection School Of Information Systems, 2014.

[8] Delac G. Silic M. Krolo J., Emerging Security Threats for Mobile Platforms, Faculty of Electrical Engineering and Computing.

[9] Gunasekera S., Android Apps Security, Apress, 2012.

[10] Holla S. Katti M.M., Android based mobile application development and its serciurity, Inernational Journal of Computer Trends and Technology, 2012.

[11] Liebergeld S. Lange M., Android Security, Pitfalls, Lessons Learned and BYOD, 2013.

[12] https://www.spidersweb.pl/2018/02/android-ios-udzialy-rynkowe.html