JOURNAL of COMPUTER SCIENCES INSTITUTE

JCSI 8 (2018) 220-225
Wysłane: 2017-12-27
Przyjęte: 2018-01-12

Zabezpieczenia systemowe oraz sprzętowe dostępne dla użytkowników na urządzeniach pracujących pod kontrolą systemu Android

Tomasz Borysiewicz*

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

Streszczenie: Producent systemu Android już od pierwszej wersji platformy stara się oferować użytkownikom sposoby na ochronę przechowywanych na urządzeniach danych cyfrowych. Rozwój możliwości systemu oraz nowe rozwiązania technologiczne pozwalają na wprowadzanie coraz bardziej innowacyjnych zabezpieczeń, które cechują się nie tylko większym poziomem bezpieczeństwa ale również większym komfortem w codziennym użytkowaniu. Artykuł przedstawia porównanie dostępnych rozwiązań, zarówno względem zapewnienia najlepszej ochrony, jak i pod względem wygody użytkowania. Zagadnienie komfortu wymagało przeprowadzenia badań, w celu zebrania informacji o najbardziej popularnych konfiguracjach wśród użytkowników. Analiza bezpieczeństwa blokad oraz otrzymane wyniki badań, pozwoliły zweryfikować, czy właściciele urządzeń pracujących pod kontrolą systemu Android odpowiednio zabezpieczają dane przechowywane w pamięci wewnętrznej swoich urządzeń.

Słowa kluczowe: Android, zabezpieczenia; blokady; bezpieczeństwo

*Autor do korespondencji

Adres e-mail: borysiewicztomasz@gmail.com

System and hardware security options available for users on devices running Android operating system

Tomasz Borysiewicz*

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

Abstract. Producer of Android operating system have been trying to offer ways to protect digital data on devices since 1st version of this platform. Development of possibilities of operating system and new technological solutions allows to launch more innovate protections, which are not only more secure, but also very comfortable in everyday usage. This article presents comparison of available solutions, both in terms of the best protection and convenience of usage. The topic of convenience of usage required research to collect information about the most popular configurations among users. The analysis of security level of available locks and obtained results allowed to verify whether owners of devices running Android operating system are properly securing digital data stored in internal memory of their devices.

Keywords: Android, security; locks; safety

*Corresponding author

E-mail address: borysiewicztomasz@gmail.com

1. Wprowadzenie

Android jest systemem mobilnym, który po raz pierwszy na rynku zadebiutował 5 listopada 2007 roku. W zaledwie trzy lata zdobył ponad 80% rynku [1] i od tego czasu nieprzerwanie utrzymuje dominującą pozycję [2]. W pierwszym kwartale 2010 roku, a więc w momencie zdobycia przewagi nad konkurencją, pod kontrolą tej platformy pracowało około 50 milionów urządzeń, a liczba ta nieustająco wzrasta [2]. Producent systemu stara się zaoferować użytkownikom wydajny system o ogromnych możliwościach, który jednocześnie będzie bezpieczny. W tym celu już w pierwszej jego wersji pojawiły się 3 formy zabezpieczania urządzeń przed niepowołanym dostępem. Był to kod PIN, hasło alfanumeryczne oraz wzór blokady. Każde z tych rozwiązań cechowało się różnym poziomem bezpieczeństwa oraz komfortem użytkowania. Niestety to te najmniej bezpieczne blokady były najgodniejsze w użyciu, a więc Google nie ustawało w pracach mających na celu stworzenie lepszych rozwiązań. Fragmentacja Androida, która uznawana jest za jego największą wadę, okazuje się ogromną zaletą w kwestii rozwoju platformy. Każdy z producentów urządzeń, których pracą zarządza system Android, oferuje swoje autorskie rozwiązania zabezpieczania systemu, zarówno sprzętowe jak i programowe. Google ma zatem ogromną grupę testową, która weryfikuje nowatorskie metody blokady, a najlepsze z rozwiązań wprowadzane są do oficjalnej wersji systemu. Dzięki takim działaniom system wyposażony został w obsługę czytników linii papilarnych oraz różne rodzaje akcji, które sprawiają, że korzystanie z urządzenia ze skonfigurowanymi blokadami staje się wygodniejsze, co wielu użytkowników skłania do korzystania z dostępnych blokad. Dodatkowo, rozwój platformy zaowocował pojawieniem się możliwości szyfrowania pamięci wewnętrznej urządzenia, a także pojawieniem się usług *Google Find My Device*, która pozwala zdalnie zarządzać urządzeniem oraz lokalizować je.

Celem artykuł jest porównanie zaimplementowanych w systemie Android funkcji zabezpieczania systemu, których konfiguracja dostępna jest dla użytkowników. Porównanie ma na celu określenie zarówno poziomu bezpieczeństwa konkretnych rozwiązań, jak i wygodę korzystania z nich w życiu codziennym.

2. Potrzeba zabezpieczania urządzeń

Urządzenia pracujące pod kontrolą systemu Android towarzyszą użytkownikom w ich codziennym życiu. Telefony są narzędziem wykorzystywanym do komunikacji ze światem, a także zastępują wiele przedmiotów, z których korzystano przed rozwinięciem się technologii do obecnego stanu. W urządzeniu znajdują się aplikacje pozwalające zastąpić kalkulator, odtwarzacz muzyki, kalendarz, listę zadań, notatnik, budzik, mapę, nawigację, kartę bankową, a także programy pozwalające uzyskać dostęp do konta bankowego, wypożyczyć film, skorzystać z internetu, przesłać pliki, czy przeprowadzić rozmowy głosowe oraz video. Dodatkowo większość aplikacji pozwala synchronizację z serwerem, dzieci czemu wprowadzone treści na jednym z urządzeń dostępne są na pozostałych, powiązanych z tym samym kontem. Ogrom funkcjonalności oraz liczność aplikacji, które zapewniają do nich dostęp podnoszą także ryzyko wycieku, bądź przechwycenia wrażliwych danych. Potencjalny złodziej danych może uzyskać dostęp do bardzo wielu informacji o właścicielu urządzenia, takich jak historia lokalizacji, prywatne dokumenty czy notatki, zapamiętane hasła, dostępy do różnych kont (w tym bankowego), a także informacji, które nie wydają się być newralgiczne, między innymi upodobania muzyczne czy filmowe użytkownika. Wszystkie te dane w połączeniu tworzą skarbnicę wiedzy o właścicielu urządzenia, o jego danych personalnych, pracy, czy życiu codziennym, dlatego tak ważne jest jak najlepsze zabezpieczanie danych. Usługi, z których korzystają użytkownicy są na ogół bardzo dobrze zabezpieczone po stronie usługodawcy, jak również sam system Android stara się dostarczyć jak najlepsze mechanizmy zabezpieczania platformy. W przypadku ataków na serwery usługodawców użytkownik niestety nie ma żadnego wpływu na bezpieczeństwo swoich danych, jednak większość ataków na systemy mobilne skupia się na wykorzystaniu braku wiedzy użytkowników, bądź nieodpowiednim zarządzaniu blokadami w systemie. W tych kwestiach jednak użytkownik może zdobyć dodatkową wiedzę i wpłynąć na bezpieczeństwo swoich danych cyfrowych.

3. Dostepne zabezpieczenia

3.1. Rozwiązania wprowadzone przez producenta systemu Android

Najnowsze wersje platformy wciąż posiadają blokady, które obecne były w pierwszej kompilacji systemu, a więc kod PIN, hasło alfanumeryczne oraz wzór blokady. W kolejnych iteracjach pojawiła się obsługa czytnika linii papilarnych, szyfrowanie wewnętrznej pamięci urządzenia, kontrolowanie uprawnień aplikacji, a także usługę *Google Find My Device*. Dodatkowo wprowadzono opcje, które ułatwiają interakcję z systemem, na którym skonfigurowana zostały zabezpieczenia, a są to funkcje podwójnego stuknięcia, przesunięcia w celu odblokowania oraz podwójnego stuknięcia. Najnowszym tego typu rozwiązaniem jest zbiór inteligentnych blokad, w skład których wchodzą zaufane urządzenia, zaufane lokalizacje, zaufana twarz, zaufany głos oraz rozpoznawanie kontaktów z ciałem.

3.2. Rozwiązania wprowadzone przez producentów urządzeń pracujących pod kontrolą systemu Android

Producenci urządzeń mobilnych często modyfikują platformę aby dodać firmowy akcent estetyczny lub umieścić w nim własne aplikacje. Zmiany niejednokrotnie dotyczą także rozszerzenia funkcjonalności systemu, w tym obsługi dodatkowych urządzeń wykorzystywanych do podniesienia bezpieczeństwa systemu oraz rozszerzeń podnoszących komfort korzystania z urządzenia. Do tego typu funkcjonalności należą inteligentne gesty, *moto actions*, *knock code* oraz skaner tęczówki.

4. Porównanie zabezpieczeń

4.1. Porównanie zabezpieczeń pod względem poziomu bezpieczeństwa

Najlepsza formą zabezpieczania danych w pamięci wewnętrznej urządzenia jest szyfrowanie. Pozwala to uniknąć przechwycenia danych w przypadku utraty telefonu, pod warunkiem, że był on wyłączony w momencie trafienia w niepowołane ręce, bądź posiadał skonfigurowane blokady ekranu.

Najlepsze z dostępnych rozwiązań to aktualnie czytnik linii papilarnych oraz skner tęczówki. Poziom bezpieczeństwa jak obu blokad jest bardzo zbliżony, dzięki analogicznemu sposobowi działania. Z odczytanego obrazu tworzony jest graf, na podstawie charakterystycznych punktów, takich jak zakończenia i rozgałęzienia linii papilarnych, czy specyficzne rozdzielenia tkanki tęczówki. Stworzony graf porównywany jest z tym, który utworzony został podczas konfiguracji blokady, a warunkiem na przyznanie dostępu do obsługi systemu jest zawieranie się nowopowstałego grafu w pierwowzorze [3][4]. Dzięki dużej unikalności badanych punktów wśród społeczeństwa, obydwie blokady wykazują się wysokim poziomem bezpieczeństwa, a więc powinny być pierwszym wyborem użytkowników, którzy cenią sobie bezpieczeństwo. Ogromnym atutem tych rozwiązań jest również brak możliwości ominięcia ich przez osoby postronne. Nawet jeżeli potencjalny złodziej próbowałby zaobserwować sposób na odblokowanie urządzenia, po jego przejęciu niemożliwe byłoby uzyskanie dostępu do systemu bez obecności uwierzytelnionej osoby. Niestety blokady te uzależnione są od urządzenia, a więc nie wszyscy użytkownicy mają możliwość skorzystania z nich. Na szczęście platforma Android oferuje wiele innych rozwiązań, które wykorzystane mogą być na telefonach o słabszej specyfikacji sprzętowej, a producenci niektórych urządzeń oferują również swoje autorskie rozwiązania, podobnie jak Samsung, który umieścił w swoich flagowych modelach skaner tęczówki oka.

Spośród podstawowych metod blokady, dostępnych już od pierwszej wersji systemu Android najbezpieczniejszą opcją będzie blokada hasłem. Rozwiązanie to pozwala na stworzenie skomplikowanego ciągu alfanumerycznego, który nie tylko trudno odgadnąć bądź złamać, ale również ciężko podejrzeć z pozycji osoby trzeciej podczas wprowadzana go na klawiaturze telefonu przez osobę uwierzytelnioną. O wiele prostsze jest to w przypadku blokady kodem PIN. Długość kodu może wynosić maksymalnie 8 znaków oraz musi się ona składać wyłącznie z cyfr. Brak możliwości zastosowania znaków specjalnych oraz liter, bardzo uszczupla dostępną pulę możliwych kombinacji. Rozwiązanie tego typu jest zatem o wiele łatwiej złamać, a uproszczona klawiatura

wprowadzania kodu, sprawia że obserwacja właściwej kombinacji z pozycji osoby trzeciej jest również o wiele prostsza. Najmniej bezpiecznym rozwiązaniem jest natomiast wzór blokady, zwany popularnie wężykiem. Polega on na wprowadzeniu przez użytkownika na ekranie urządzenia linii przechodzącej przez odpowiednie punkty, konkretnej kolejności, bez możliwości wykorzystania punktów więcej niż jeden raz. Pomimo wygody tego rozwiązania, ilość możliwych kombinacji jest dość ograniczona, a obserwacja poprawnego wzoru jest o wiele łatwiejsza niż w przypadku wyżej opisywanych rozwiązań. Co więcej, po wprowadzeniu wzoru blokady, na urządzeniu pozostają charakterystyczne wzory pozostawione przez palec użytkownika, dzięki czemu odgadnięcie właściwej kombinacji niejednokrotnie okazuje się naprawdę proste. Rozwiązaniem dość podobnym do kodu PIN jest blokada wprowadzona przez firmę LG, nazwana *knock code*. Podczas korzystania z tej metody zabezpieczenia, użytkownik ma do dyspozycji cztery części ekranu, a odpowiednia kombinacja stuknięć w poszczególne ćwiartki powala uzyskać dostęp do systemu[5]. Ilość możliwych kombinacji jest bardzo niewielka, ponieważ tego typu blokadę można by rozważyć jako czteroznakowy kod PIN, których składać się może tylko z cyfr w zakresie 1-4. Złamanie takiego kodu jest stosunkowo proste, a sposób wprowadzania sekwencji stuknięć jest łatwy do zaobserwowania, a więc blokada ta powinna być ostatnim wyborem wśród użytkowników ceniących sobie bezpieczeństwo danych.

Dodatkowymi rozwiązaniami, które wprowadzone zostały przez producentów urządzeń pracujących pod kontrolą systemu Android, są inteligentne gesty, inteligentne blokady oraz *moto actions*. Wprawdzie głównym celem wprowadzenia tych rozwiązań było podniesienie komfortu korzystania z telefonu, jednak w wielu sytuacjach podnoszą one bezpieczeństwo danych w pamięci wewnętrznej urządzenia. Inteligentne gesty oraz *moto actions* pozwalają wywoływać przydatne funkcjonalności systemu (takie jak aparat czy latarka) bez potrzeby odblokowywania urządzenia, dzięki czemu użytkownik korzystający z łatwych do zaobserwowania metod blokady dostępu, może spokojnie skorzystać z niektórych funkcji systemu, bez ryzyka, że w tłocznym miejscu ktoś podejrzy wymagany kod lub wzór blokady. Rozwiązanie inteligentnych blokad oferuje możliwość całkowitego wyłączenia blokady w określonych sytuacjach, bądź pominięcie wprowadzania hasła przy spełnieniu określonych warunków. Zabezpieczenia mogą zostać wyłączone w określonych lokalizacjach, podczas korzystania z określonych urządzeń bluetooth w zasięgu telefonu, bądź w momencie, kiedy użytkownik przemieszcza się z urządzeniem, natomiast brak potrzeby wprowadzania hasła zaistnieje kiedy przednia kamera urządzenia rozpozna twarz właściciela, bądź mikrofon zarejestruje odpowiednią frazę, wypowiedzianą głosem uwierzytelnionej osoby. Korzyści używania tych rozwiązań są analogiczne jak w przypadku inteligentnych gestów oraz *moto actions*, jednak nie wszystkie charakteryzują się taką samą odpornością na próby złamania. Rozpoznawanie głosu, lokalizacji oraz urządzeń jest wystarczająco bezpieczne aby korzystać z tych rozwiązań na co dzień, pamiętając jednak by nie pozostawiać zaufanego urządzenia wraz z telefonem bez nadzoru oraz nie dodawać zbyt wielu zaufanych lokalizacji, szczególnie takich, które są miejscami publicznymi. Rozpoznawanie twarzy jest podatne na próby oszustwa zdjęciem uwierzytelnionej osoby, a wykrywanie kontaktu z ciałem może pozwolić uzyskać złodziejowi pełen dostęp do systemu, jeżeli napastnik wyciągnie go z torebki czy kieszeni właściciela, ponieważ blokada uruchomiła by się dopiero wtedy, kiedy urządzenie przestałoby być w ruchu, a więc korzystanie z tych rozwiązań nie jest bezpieczne.

Niewspomniane powyżej rozwiązania, takie jak podwójne stuknięcie czy przesunięcie ekranu w celu odblokowania, bez skonfigurowanych dodatkowych blokad, w żaden sposób nie zabezpieczają systemu przed dostępem niepowołanych osób. Korzystanie z nich nie wpływa zatem w żaden sposób na bezpieczeństwo danych na urządzeniu, zatem używanie tylko tych rozwiązań jest całkowicie niebezpieczne.

Poza metodami blokowania urządzenia, producent systemu Android wprowadził również funkcjonalność o nazwie *Google Find My Device*. Dostępne w ramach tej usługi opcje, pozwalają odnaleźć zagubione, bądź skradzione urządzenia poprzez wyświetlenie ich aktualnej pozycji geograficznej na mapie, zdalnie wywołać na urządzeniu dźwięk w celu zlokalizowania go w bliskim otoczeniu użytkownika, zablokować urządzenie, tak aby możliwe było skorzystanie z niego tylko po wprowadzeniu hasła do konta Google, a także zdalnie wyczyścić pamięć urządzenia. Usługa zdecydowanie podnosi bezpieczeństwo danych na urządzeniu, pozwalając zdalnie zablokować do nich dostęp lub usunąć je, a korzystanie z tego rozwiązania nie wymaga żadnej konfiguracji ze strony użytkownika.

W szóstej wersji platformy Android o nazwie Marshmallow, producent systemu wprowadził możliwość kontrolowania uprawnień aplikacji [6]. W celu wykonania danej operacji użytkownik musi zezwolić aplikacji na skorzystanie z danych zasobów systemu, bądź podzespołów urządzenia. Rozwiązanie to posiada pewne wady, jak na przykład zbyt szerokie grupowanie uprawnień, przez co użytkownik może nie wiedzieć, czy program chce jedynie odczytać informacje z danego zasobu czy też je nadpisać. Pomimo tego, jest to przyznanie właścicielowi urządzenia pewnego rodzaju kontroli nad aplikacjami, dzięki któremu może zablokować niektóre, niepożądane operacje, co niewątpliwie wpływa bardzo pozytywnie na bezpieczeństwo danych w pamięci wewnętrznej urządzenia.

Użytkownicy tabletów pracujących pod kontrolą systemu Android mają do wyboru te same metody blokowania urządzenia, co użytkownicy telefonów, za wyłączeniem rozwiązań wprowadzanych przez producentów urządzeń, a zatem inteligentnych gestów, skanera tęczówki oka, *knock code* oraz *moto actions*. Dostępne blokady działają w taki sam sposób jak na telefonach, a więc kolejność ich wyboru ze względu na poziom bezpieczeństwa, również będzie taka sama.

Właściciele inteligentnych zegarków mają możliwość skonfigurowania jedynie najprostszych metod blokady, a zatem hasła, kodu PIN oraz wzoru blokady. Stosowanie zabezpieczeń na inteligentnych zegarkach jest bardzo ważne, ponieważ kolejne aktualizacje systemu wprowadzają coraz więcej możliwości systemu, przez co narażone mogą być dane oraz finanse użytkownika [7]. Zasada działania dostępnych

blokad różni się nieco w porównaniu do telefonów oraz tabletów, ponieważ zabezpieczenie uruchamiane jest jedynie wtedy, kiedy urządzenie znajduje się w stanie spoczynku, a jeżeli użytkownik ma je cały czas przy sobie, blokada pozostaje wyłączona. Jednak sam proces odblokowywania urządzenia oraz możliwości konfiguracji kombinacji autoryzacyjnych są niezmienne, a więc hierarchia dostępnych rozwiązań, ze względu na poziom bezpieczeństwa, będzie analogiczna jak przy wyżej opisywanych urządzeniach.

W przeciwieństwie do pozostałych urządzeń pracujących pod kontrolą systemu Android, właściciele telewizorów, których pracą również zarządza ta platforma, nie posiadają żadnej możliwości zabezpieczenia swoich danych cyfrowych. Co więcej Android pracujący na telewizorach jest jedyną wersją tego systemu, która nie wspiera usługi *Google Find My Device*, zatem użytkownicy powinni zwracać szczególną uwagę na to, aby nie przechowywać na tego typu urządzeniach wrażliwych informacji, prywatnych zdjęć, czy informacji wymaganych do płatności elektronicznych.

4.2. Prównanie zabezpieczeń pod względem komfortu użytkowania

W celu zweryfikowania jakie metody zabezpieczeń najchętniej wybierają użytkownicy przeprowadzone zostały trzytygodniowe badania na pięćdziesięcioosobowej grupie chętnych. Badani zostali dobrani tak, aby podczas testów mieli możliwość skorzystania urządzeń pochodzących od różnych wytwórców. Dzięki temu możliwe było wypróbowanie przez nich wszystkich metod zabezpieczania systemu. Uczestnicy zostali dobrani również pod względem zainteresowań i pochodzenia, aby badania przedstawiały globalne zachowanie użytkowników, którzy niekoniecznie interesują się tematem bezpieczeństwa oraz technologii. Po zakończonym okresie badań, uczestnicy poproszeni zostali o wypełnienie ankiety, której wyniki przedstawia wykres (Wykres 1). Poniższy test zawiera analizę otrzymanych wyników.

Jedynym rozwiązaniem, z którego korzystało 100% badanych jest szyfrowanie pamięci urządzenia. Rozwiązanie to jest dla użytkownika całkowicie niezauważalne, a więc w żaden sposób nie utrudnia codziennej pracy z urządzeniem, będąc jednocześnie bardzo dobrą ochroną danych przechowywanych w pamięci urządzenia.

Wśród blokad dostępu do systemu, zdecydowaną przewagę zyskał czytnik linii papilarnych, który aż 76% użytkowników skonfigurowało jako swoją główną metodę zabezpieczania urządzenia przed niepowołanym dostępem. Niewątpliwie jest to sukces producenta systemu Android, ponieważ jedna z najlepszych blokad oferowanych w platformie jest jednocześnie wystarczająco wygodna, aby użytkownicy chętnie korzystali z niej na co dzień. Druga pod względem bezpieczeństwa metoda blokady, zaproponowana przez firmę Samsung nie uzyskała już tak dobrego wyniku. Zaledwie 8% badanych zdecydowało się na skonfigurowanie skanera tęczówki oka jako główną metodę uwierzytelniania w systemie. Jednak jako alternatywna metoda, uzyskany wynik był o wiele lepszy, bo wynosił aż 62%. Prostsze metody blokady, takie jak *knock code*, kod PIN, hasło oraz wzór odblokowania nie zyskały zainteresowania użytkowników jako główna metoda blokady. Urządzenia badanych wyposażone były w wygodniejsze rozwiązania, a więc wybór użytkowników wydaje się być oczywisty.

Rys. 1. Procentowy wykaz wykorzystywania poszczególnych blokad wśród grupy badanych użytkowników

Najbezpieczniejsze z tych rozwiązań, a więc blokada hasłem okazała się niestety na tyle uciążliwa, że żaden z uczestników badania nie zdecydował się skonfigurować jej nawet jako

zabezpieczenie alternatywne. Jako dodatkową blokadę użytkownicy najchętniej wybierali wzór blokady, który wybrało aż 74% badanych. Mimo dużej podatności tego rozwiązania na obserwację wprowadzanej kombinacji z pozycji osoby trzeciej, jest to stosunkowo bezpieczna blokada jako zabezpieczenie dodatkowe. Użytkownik wprowadza wzór tylko w nielicznych sytuacjach, kiedy zawiodły inne możliwości uwierzytelnienia dostępu, a więc ciężko jest podejrzeć poprawną sekwencję. Potencjalny złodziej musiałby zatem spróbować złamać tę blokadę, co nie byłoby proste, ponieważ możliwych jest ponad 400 000 różnych kombinacji połączenia punktów [8].

Na korzystanie z rozwiązań, które w żaden sposób nie podnoszą bezpieczeństwa danych przechowywanych na urządzeniu, zdecydowało się łącznie jedynie 4% badanych, którzy skonfigurowali przesunięcie w celu odblokowania, bądź podwójne stuknięcie, jako główne metody blokady. Tak mały odsetek badanych spowodowany był najprawdopodobniej zbyt dużym ryzykiem przypadkowego odblokowania urządzenia w kieszeni czy torebce. Podwójne stuknięcie w ekran było jednak chętnie wybieraną alternatywną metodą blokady. Aż 52% badanych korzystało z tego rozwiązania w celu wybudzenia urządzenia ze stanu czuwania.

Z możliwości kontrolowania uprawnień aplikacji korzystało jedynie 8% badanych. Najprawdopodobniej użytkownicy nie posiadają odpowiedniej wiedzy, które uprawnienia są aplikacjom niezbędne do poprawnego działania i przyznają im wszystkie żądane dostępy. Z kolei wyłączenie raz przyznanych uprawnień jest „schowane" w systemie, a więc sposób obsługi dostępów nie jest wystarczająco przejrzysty dla użytkowników, aby zdecydowali się na rozważne kontrolowanie uprawnień.

Rozwiązania wprowadzone przed producentów urządzeń w celu podniesienia komfortu wykonywania prostych akcji na telefonie, bez potrzeby odblokowywania go, a więc *moto actions* oraz inteligentne gesty, nie były często wybieranymi rozwiązaniami wśród użytkowników. Łącznie, z obu blokad korzystało zaledwie 20% użytkowników. Opcje oferowane przez inteligentne gesty były wybierane przez użytkowników zdecydowanie częściej. Ponad 50% badanych korzystało z zaufanych lokalizacji, 46% skonfigurowało zaufane urządzenia, a 28% używało rozpoznawania kontaktu z ciałem w celu czasowej dezaktywacji zabezpieczenia systemu. Dodatkowo, jako alternatywne metody odblokowania urządzenia, użytkownicy wykorzystywali zaufany głos (52%) oraz rozpoznawanie twarzy (56%).

Usługa *Google Find My Device* okazała się chętnie wykorzystywanym rozwiązaniem wśród badanych. Aż 86% z nich zadeklarowało aktywne korzystanie z usługi podczas przeprowadzonych badań. Podobnie jak szyfrowanie pamięci urządzenia, korzystanie z tej usługi jest dla użytkownika całkowicie niezauważalne i w żaden sposób nie wpływa na komfort korzystania z urządzenia. Zaawansowane opcje zdalnej ochrony danych zachęciły jednak badanych do korzystania z tej usługi, w celu odszukania swoich urządzeń, bądź zabezpieczenia danych na telefonach.

Przeprowadzone badania dotyczyły korzystania z telefonów, jednak uzyskane wyniki można odnieść również do właścicieli tabletów, które pracują pod kontrolą systemu Android, ponieważ wszystkie dostępne zabezpieczenia działają w ten sam sposób, a więc wybór użytkowników również były taki sam. Na podstawie otrzymanych wyników można jednoznacznie stwierdzić, że użytkownicy nie są obojętni na bezpieczeństwo swoich danych, jednak przedkładają wygodę ponad ochronę danych. Z całą pewnością można zatem stwierdzić, że odsetek użytkowników korzystających z blokady ekranu na inteligentnych zegarkach byłby naprawdę niewielki, a właściciele telewizorów, których pracą zarządza platforma Android nie zdecydowaliby się na skorzystanie z jakichkolwiek blokad, nawet, jeżeli byłyby one dostępne.

5. Wnioski

Na podstawie wyników otrzymanych badań można zauważyć, że użytkownicy pomimo braku obojętności na bezpieczeństwo danych, wybierają jednak takie rozwiązania i blokady, które są jak najbardziej komfortowe w codziennym użytkowaniu i ułatwiają pracę z urządzeniem. Porównanie zabezpieczeń pod względem bezpieczeństwa blokad, w zestawieniu z odpowiedziami użytkowników na temat przeprowadzonych badań, ukazują że użytkownicy przedkładają wygodę ponad bezpieczeństwo danych przechowywanych w pamięci wewnętrznej urządzeń pracujących pod kontrolą systemu Android. Przyczyny takiego zachowania mogą być różne. Może być to brak wiedzy użytkowników o istniejących zagrożeniach, brak świadomości na temat istnienia niektórych blokad, jak również chęć wygodnej pracy z urządzeniem, pomimo świadomości narażania plików na ataki i wycieki. Niewątpliwie dałoby się ustalić konfigurację, która zapewniłaby odpowiednią ochronę, nie utrudniając jednocześnie pracy z urządzeniem. Problemem jednak byłoby zachęcenie właścicieli urządzeń do korzystania z takiego zestawu blokad, ponieważ musieliby zrezygnować z niektórych wygód, do których przyzwyczaili się przez lata korzystania z systemu Android. Co więcej, wielu z nich należałoby zainteresować tematem bezpieczeństwa oraz możliwości wykorzystania przechwyconych danych, aby mieć pewność, że w przypadku pojawienia się kolejnych metod blokady urządzenia, zweryfikują oni poziom jej bezpieczeństwa i rozważą korzystanie z niej. Producent systemu rozumie istniejące problemy i stara się dostarczać coraz lepsze rozwiązania, które są nie tylko coraz bardziej bezpieczne ale także coraz wygodniejsze w codziennej pracy z urządzeniem. Jak łatwo można zauważyć to na przykładzie czytnika linii papilarnych, z powodzeniem udaje się wprowadzać takie rozwiązania do codziennego użytku, jednak dzieje się to stosunkowo powoli. Ogromna grupa docelowa oraz mnogość wytwórców urządzeń sprawia, że niejednokrotnie te najlepsze rozwiązania trafiają do wielu użytkowników z dużym opóźnieniem, na przykład z powodu dużych kosztów wytworzenia urządzeń wspierających daną blokadę.

Google niewątpliwie stara się dostarczać jak najlepiej zabezpieczony system, nieustannie wprowadzając do systemu poprawki bezpieczeństwa. Rynek mobilny rozwija się jednak bardzo szybko i nawet tak ogromna firma nie jest w stanie zapewnić rozwiązań spełniających oczekiwania wszystkich użytkowników. Należy więc starać się uświadamiać

właścicieli urządzeń pracujących pod kontrolą systemu Android do korzystania z dostępnych zabezpieczeń oraz przekonywać ich do poświęcania części komfortu codziennej pracy z urządzeniem, w celu zapewnienia bezpieczeństwa swoim danym cyfrowym, a przez to i samym sobie.

Literatura

[1] 3 Android Data Showing "Why Android is the New King of Technology?", SOURCE DIGIT, http://sourcedigit.com/1913-smartphone-os-global-market-share-data-2014 [11.04.2016]

[2] Smartphone OS Market Share, 2017 Q1, IDC, http://www.idc.com/prodserv/smartphone-os-market-share.jsp, [02.01.2016]

[3] Poznajmy technologię: Jak działa czytnik linii papilarnych?, LenovoZone, https://lenovozone.pl/porady/poznajmy-technologie-jak-dziala-czytnik-linii-papilarnych [17.06.2017]

[4] T. Nick, Here is how the iris scanner on the Galaxy Note 7 works, phoneArena.pl, https://www.phonearena.com/news/Here-is-how-the-Galaxy-Note-7-iris-scanner-works_id82854 [15.08.2017]

[5] J. Stępień, Knock Code przełomowa metoda budzenia smartphona, www.shemag.pl/trend/knock-code-przelomowa-metoda-budzenia-smartphona [30.08.2017]

[6] Control your app permissions on Android 6.0 and up, Google Play Help, https://support.google.com/googleplay/answer/6270602 [15.08.2017]

[7] P. Lamkin, Android Wear 2.0: Ultimate guide to the major smartwatch update, WAREABLE, https://www.wareable.com/android-wear/android-wear-update-everything-you-need-to-know-2735 [16.09.2017]

[8] U. Malhotra, How many combinations of locking pattern are possible for a Samsung 3*3 locking grid?, Quora, https://www.quora.com/How-many-combinations-of-locking-pattern-are-possible-for-a-Samsung-3*3-locking-grid [03.10.2017]