JOURNAL of COMPUTER SCIENCES INSTITUTE

JCSI 6 (2018) 34-41
Wysłane: 2017-09-23
Przyjęte: 2017-09-27

Badanie zachowań użytkowników oraz metod autoryzacji w kontekście bezpieczeństwa urządzeń mobilnych

Piotr Król*, Damian Marek , Jakub Smołka
Politechnika Lubelska, Instytut Informatyki, Nadbystrzycka 36B, 20-618 Lublin, Polska

Streszczenie. W niniejszym artykule przedstawiono badania metod autoryzacji użytkowników mobilnych urządzeń wyposażonych w ekran dotykowy. Analizie poddano metody autoryzacji istniejące w systemie android, oraz nowe możliwości uwierzytelniania, zaproponowane przez autorów. Blokadę ekranu za pomocą PIN (ang. Personal Identification Number), oraz wzoru porównano z nowoopracowanymi przez autorów metodami. Analizowano czas wprowadzania klucza, liczbę pomyłek oraz liczbę kombinacji danej metody autoryzacji.

Słowa kluczowe: uwierzytelnianie użytkowników; blokada wzorem; blokada pinem; bezpieczeństwo systemu android; metody autoryzacji

*Autor do korespondencji.

Adresy e-mail: piotrekk6@gmail.com*, damian.marek@outlook.com, jakub.smolka@pollub.pl

Analysis of user behavior and authorization methods in context of mobile devices security

Piotr Król*, Damian Marek, Jakub Smołka
Institute of Computer Science, Lublin University of Technology, Nadbystrzycka 36B, 20-618 Lublin, Poland

Abstract. This article discusses authentication methods for users of mobile devices with touchscreens. The analysis concerns the authentication methods already existing in Android OS and new authorization methods proposed by the authors. Pattern and PIN (Personal Identification Number) lock were compared with two new authentication methods. The time required for entering the key, number of mistakes, number of possible combinations were analyzed.

Keywords: : user authentication; pattern lock; pin lock; android security; authorization methods

*Corresponding author.

E-mail addresses: piotrekk6@gmail.com*, damian.marek@outlook.com, jakub.smolka@pollub.pl

1. Wstęp

Początki telefonów komórkowych z Systemem Android miały miejsce w grudniu 2008 roku, gdy HTC zaprezentowało pierwsze urządzenie o przeznaczeniu komercyjnym [1]. Mowa o modelu G1 znanym również jako HTC Dream z preinstalowanym Androidem w wersji 1.0. Od tamtej pory w materii urządzeń mobilnych wiele się zmieniło. Zwykłe telefony komórkowe posiadające funkcję dzwonienia, pisania sms-ów oraz budzika zaczęły być wypierane przez urządzenia wielofunkcyjne, których głównym przeznaczeniem było korzystanie z Internetu.

Liczba użytkowników posiadających smartfony w ciągu ostatnich lat drastycznie wzrasta. W 2017 roku liczba ludzi korzystających z tych urządzeń szacowana jest na około 2, a 32 miliarda [2], z czego około 85% są to użytkownicy systemu Android [3]. Są to urządzenia, które przestały służyć już tylko i wyłącznie do dzwonienia czy pisania wiadomości tekstowych. Oprócz tych podstawowych rzeczy, smartfony są wykorzystywane do przeprowadzania płatności mobilnych, przechowywania haseł czy do zarządzania firmami. Oznacza to że wraz z popularyzacją mobilnych urządzeń wielofunkcyjnym stały się one miejscem gdzie przechowywane mogą być wrażliwe dane, których dostanie się w niepowołane ręce mogłoby mieć niepożądane skutki.

Standardowe metody blokady w systemie android, to płaszczyzna, gdzie niewiele się zmienia od dłuższego czasu. Istniejące rozwiązania są wszystkim znane, co oznacza że powstały sposoby ominięcia bądź wykradnięcia hasła użytkownika. Producenci smartfonów tacy jak LG, czy Samsung nierzadko wprowadzają autorskie sposoby blokady urządzeń, lecz nie są one dostępne dla użytkowników z czystym systemem Android.

Temat autoryzacji użytkowników w systemie opracowanym przez Google, jest powszechnie znany, lecz nowe bądź istniejące sposoby uwierzytelniania właścicieli urządzeń nie są rozwijane. Szerokie pole manewru, jakie pozostawili producenci mobilnych systemów operacyjnych skłoniło autorów do podjęcia powyższego tematu.

Poczucie bezpieczeństwa jest pożądane wśród użytkowników smartfonów, na których przechowywane są poufne dane, toteż w niniejszym artykule przeanalizowano najczęściej stosowane oraz nowe sposoby autentykacji opracowane przez autorów.

2. Przegląd literatury

Poniżej przedstawiono aktualny stan badań z zakresu zabezpieczeń urządzeń mobilnych. Dzięki pozycjom dostępnym w bazach naukowych takich jak Springer, ScienceDirect, BazTech, Scopus Przeanalizowano problem bezpieczeństwa przechowywanych informacji w urządzeniach mobilnych, oraz nowo zaproponowane rozwiązania w celu podniesienia poziomu bezpieczeństwa.

Pozycja [4] opisuje słabe punkty, które posiada zaimplementowana w systemie android blokada za pomocą wzoru. Opisuje ona ryzyko złamania blokady z wykorzystaniem smugi, jaką zostawia po sobie palec po wykonaniu wzoru blokady na ekranie. Artykuły [5, 6, 7] zawierają opis procesu tworzenia i badania nowych metod autoryzacji, które mogłyby podnieść poziom bezpieczeństwa użytkowników systemów mobilnych. Dodatkowo w pozycji [8] postarano się ulepszyć blokadę wzorem poprzez dodanie wskaźnika poziomu siły wzoru, co wpłynęło na to, że użytkownicy chętniej skłaniali się do tworzenia bezpieczniejszych wzorów.

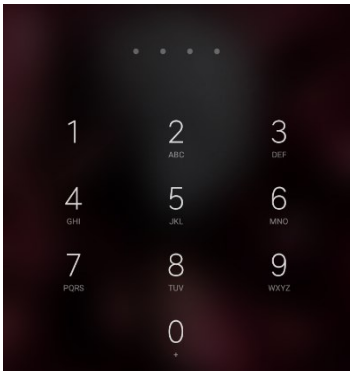
3. Metody autoryzacji w systemie Android

Popularyzacja urządzeń mobilnych z ekranem dotykowym otworzyła nowe możliwości blokady urządzeń kieszonkowych. Oprócz autoryzacji za pomocą hasła bądź kodu cyfrowego jak to było w przypadku tradycyjnych telefonów komórkowych, do smartfonów wkroczyły nieznane wcześniej nowe metody zabezpieczania ich przed niepowołanym użyciem.

Firma Google dostarcza użytkownikom swojego systemu operacyjnego możliwość zablokowania urządzenia przed użyciem przez osoby nieuprawnione na kilka sposobów. Najbardziej znanymi metodami są blokada wzorem, oraz blokada pinem. Sporą popularnością cieszy się również stosowana przez producentów blokada poprzez odcisk palca. Wymaga ona jednak posiadania specjalnego czytnika, który potrafi zeskanować linie papilarne. Rozwiązanie to zdaje się być dobrym zabezpieczeniem, gdyż nie da się w łatwy sposób podrobić odcisku palca. Rozwiązanie to jest również szybkie i można go używać bez patrzenia na ekran urządzenia mobilnego.

3.1. Blokada za pomocą PIN'u

Omawiany rodzaj blokady znany jest większości użytkowników. Ten rodzaj blokady w różnych formach znajduje zastosowanie w wielu obszarach takich jak: dostęp do konta bankowego, wejście do biura, czy dostęp do różnych aplikacji mobilnych.



Rys. 1. Ekran blokady za pomocą PIN'u

Jego działanie opiera się na kombinacji czterech cyfr (Rys. 1.), z których każda może występować dowolną ilość razy. Zmiana kolejności cyfr w PIN-ie również ma znaczenie więc funkcją opisującą liczbę możliwych kombinacji będą wariacje z powtórzeniami opisane wzorem (1)

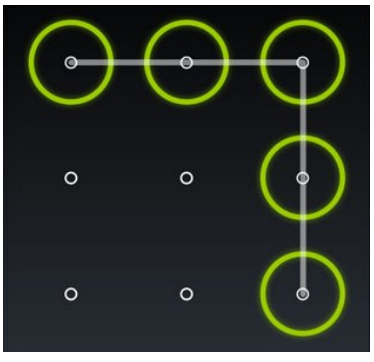
$$n^k \tag{1}$$

gdzie: n- wielkość zbioru cyfr ,k- liczba cyfr w pinie.

Zgodnie ze wzorem (1) dla systemu dziesiętnego liczba możliwych do utworzenia PIN-ów jest równa 10^k, czyli 10 000 dla najbardziej typowego cztero-cyfrowego PINu. Po zastosowaniu takiej metody zabezpieczenia użytkownika możliwe jest wykonanie pięciu prób odblokowania urządzenia. Po pięciu nieudanych próbach urządzenie zostaje zablokowane na 30 sekund bez możliwości odblokowania. Po upłynięciu tego czasu możliwe jest kolejne podejście do odblokowania, które w razie pomyłki skutkuje ponownym zamrożeniem urządzenia, lecz tym razem na 60 sekund. Kolejna nieudana próba zablokuje urządzenie na 4 minuty bez możliwości odblokowania i gdy następnym razem znów nie uda się poprawnie wprowadzić kodu PIN, niemożliwe będzie odblokowanie urządzenia za pomocą tego kodu. Jedynym sposobem na tak zablokowane urządzenie jest autoryzacja poprzez skrzynkę e-mail.

3.2. Blokada za pomocą wzoru

Metoda wykorzystująca wzór jest jednym z najpopularniejszych sposobów zabezpieczenia urządzenia przed niepowołanym dostępem. Popularność tej metody wynika głownie z faktu, że jest ona dostępna w systemie Android jako jeden z wbudowanych sposobów zabezpieczenia urządzenia. Spośród możliwości jakie oferuje mobilny system operacyjny firmy Google metoda wykorzystująca wzór sprawia wrażenie najbardziej skompilowanej do powtórzenia przez osoby niepowołane przy jednoczesnym zachowaniu intuicyjnego wyglądu i łatwości zapamiętania zdefiniowanego schematu. Główną zaletą przedstawionego rozwiązania jest możliwość zdefiniowania wzoru wedle uznania użytkownika.



Rys. 2. Ekran blokady za pomocą wzoru odblokowania

Działanie zabezpieczenia oparte jest o pozornie proste łączenie punktów wyświetlanych w formie siatki na ekranie (Rys 2.). Użytkownik wybiera jeden z punktów i rozpoczyna powtarzanie zdefiniowanej wcześniej kombinacji poprzez przeciągnięcie palcem przez wszystkie wymagane punkty. Podstawowym złożeniem przy tworzeniu i powtarzaniu

sekwencji odblokowywania jest fakt że każdy punkt może zostać wykorzystany tylko jeden raz.

Przykład z rys. 2 z siatką złożoną z 9 punktów przedstawia zdefiniowany wzór złożony z 5-ciu punktów. Minimalna liczba punktów użytych do zdefiniowania wzoru wynosi 4. Wartość ta jest narzucona przez twórców systemu Android, którzy stwierdzili, że sekwencja złożona z 3 punktów jest wyjątkowo nieskutecznym zabezpieczeniem. W takim rozwiązaniu maksymalna teoretyczna liczba kombinacji określona jest sumą permutacji (2):

$$\sum_{k=4}^{n} \frac{n!}{(n-k)!} \tag{2}$$

$$n - \text{liczba punktów siatki},$$
$$k - \text{liczba punktów użytych we wzorze}$$

W przypadku siatki złożonej z 9 punków teoretyczna maksymalna liczba możliwych wzorów wynosi 985 824. Obliczenia dokonane według podanego wzoru pozwalają na określenie wszystkich możliwych połączeń punktów siatki wyświetlonej na ekranie. W celu obliczenia liczby dostępnych kombinacji w metodzie wzorcowej należy wykluczyć przypadki, w których użytkownik nie jest w stanie połączyć punktów. Przykładem takiej operacji jest próba połączenia punktów położonych w jednej linii, które nie sąsiadują ze sobą w taki sposób by pominąć punkt znajdujący się pomiędzy. Palec użytkownika i ekran telefonu są zbyt mało precyzyjnymi narzędziami wprowadzać sekwencje złożone z takich punktów i połączeń miedzy nimi. W konsekwencji należy wykluczyć część wzorców których użytkownik nie jest w stanie fizycznie wykonać. Wartości te zostały określone w pracy Marty Løge, która dokonała badań dotyczących m.in. liczby właściwych kombinacji uwzględniając tylko możliwe do powtórzenia sekwencje [9]. Zależność liczby możliwych wzorów w zależności od zastosowanej liczby punktów została przedstawiona w Tabeli 1.

Tabela 1. Zależność liczby możliwych wzorów od liczby wykorzystanych punktów siatki

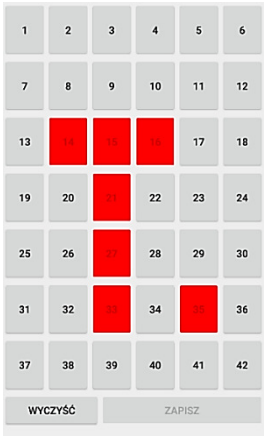
Liczba punktów	Liczba kombinacji
4	1624
5	7152
6	26016
7	72912
8	140707
9	140704

Przy zastosowaniu wzoru złożonego z 4 punktów na siatce 9 otrzymuje się 1624 kombinacji. Z zwiększenie liczby punktów we wzorze do 5 zwiększa liczbę możliwych kombinacji ponad czterokrotnie. Korzystając ze wzoru złożonego z maksymalnej liczby możliwych do użycia punktów uzyskuje się 9! możliwości, czyli 140704. Wykorzystanie wzoru złożonego z 8 punktów daje dokładnie taką samą liczbę kombinacji co w przypadku skorzystania z wzoru określonego na 9 punkach. Całkowita liczba możliwych do wykorzystania wzorów jest sumą możliwości dla poszczególnych ilości wykorzystywanych punktów i wynosi 389112. Po za siłą zabezpieczenia wynikającą z dużej liczby możliwych kombinacji autorzy zabezpieczyli się przed próbą złamania wzoru metodą siłową. Po 5-krotnym błędnie wprowadzonym wzorze zostaje zablokowana możliwość wprowadzania wzoru ponownie na czas 1 minuty. Po upływie czasu blokady, można spróbować wprowadzić wzór ponownie lecz po 5-tej nieudanej próbie urządzenie zostanie zablokowane na 5 minut. Trzecia podobna próba złamania wzoru skutkować będzie całkowitym zablokowaniem urządzenia a jedynym sposobem na odblokowanie będzie autentykacja za pomocą konta Google. W zależności od producenta i wersji systemu operacyjnego Android liczby dopuszczalnych prób mogą się nieznacznie różnić jednak zasada ograniczonego zaufania do osoby wprowadzającej wzór jest stosowana i nadmierne błędne wprowadzanie sekwencji skutkować będzie blokadą urządzenia na określony czas.

3.3. Proponowana blokada 1

Pierwszą metodą autoryzacji wykorzystującą ekran dotykowy opracowaną przez autorów jest blokada opracowana na potrzeby pracy badawczej. Głównym modułem systemu jest logika zawarta w części programistycznej, która odpowiada za zapisywanie wzorca odblokowującego oraz sprawdzenie czy jest on poprawny. Dodatkowo na potrzeby badań aplikacja wyposażona została w bazę danych, do której zapisywane są parametry konfiguracyjne oraz dane na temat samego procesu odblokowywania.

W tym rozwiązaniu użytkownik sam może zdecydować jak mocne będzie jego zabezpieczenie. Działanie tej formy upoważnienia właściciela korzysta z przycisków pojawiających się na ekranie w formie siatki (Rys. 3.). Użytkownik sam może zdecydować ile kolumn i wierszy będzie wykorzystywał. Możliwość ta pozwala osobie korzystającej z tej formy zabezpieczeń zdecydować jaki chce stosować poziom bezpieczeństwa. Minimalna liczba kolumn i wierszy została zdefiniowana odpowiednio na 3 kolumny oraz 4 wiersze. Ograniczenie to zostało nałożone z powodów bezpieczeństwa po to, aby użytkownik nie mógł ustawić kombinacji, którą możnaby odganąć w trzech próbach.



Rys. 3. Widok tworzenia blokady

Jak w każdej metodzie odblokowania na początku należy zdefiniować wzorzec. Użytkownik wybiera z jakiej siatki przycisków ma składać się ekran odblokowania. Następnie określa liczbę przycisków, których należy dotknąć aby odblokować urządzenie. Po tej czynności ukazuje się sam ekran odblokowania (Rysunek 3), na którym widoczna jest siatka przycisków a użytkownik wybiera te, które go interesują tym samym definiując wzorzec.

Ze względu na to, że rozmiar siatki przycisków oraz długość samego hasła blokady może być , liczba wszystkich możliwych do utworzenia haseł również będzie zmienna i będzie zależała od tych czynników. Liczba wariacji wszystkich możliwych haseł definiują wariacje bez powtórzeń opisane wzorem

$$\frac{(i*j)!}{[(i*j)-k]!} \tag{3}$$

gdzie i - ilość kolumn, j - ilość wierszy, k - długość hasła

Liczba kombinacji dla wszystkich konfiguracji hasła przedstawia Tabela 2.

Tabela 2. Liczba kombinacji hasła w zależności od długości hasła oraz kolumn i wierszy przycisków

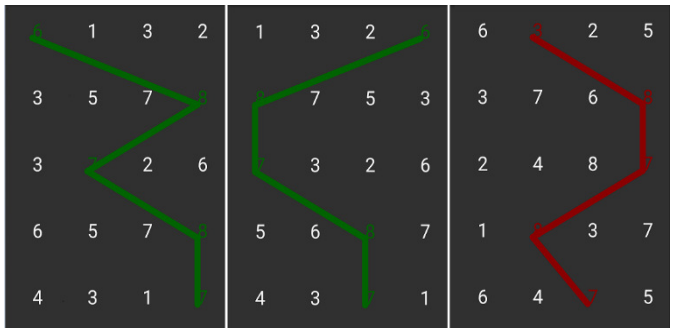
	Długość hasła				
Siatka	**4**	**5**	**6**	**7**	**8**
3x4	11880	95040	665280	3991680	19958400
3x5	32760	360360	3603600	32432400	259459200
3x6	73440	1028160	13366080	160392960	1764322560
3x7	143640	2441880	39070080	586051200	8204716800
4x4	43680	524160	5765760	57657600	518918400
4x5	116280	1860480	27907200	390700800	5079110400
4x6	255024	5100480	96909120	1744364160	29654190720
4x7	491400	11793600	271252800	5967561600	125318793600
4x4	116280	1860480	27907200	390700800	5079110400
5x5	303600	6375600	127512000	2422728000	43609104000
5x6	657720	17100720	427518000	10260432000	235989936000
5x7	1256640	38955840	1168675200	33891580800	948964262400
6x4	255024	5100480	96909120	1744364160	29654190720
6x5	657720	17100720	427518000	10260432000	235989936000
6x6	1413720	45239040	1402410240	42072307200	1220096908800
6x7	2686320	102080160	3776965920	135970773120	4758977059200

3.4. Proponowana blokada 2

Druga metoda opracowana przez autorów jest połączeniem metody wykorzystującej wzór z PIN-em. Na potrzeby badan została opracowana implementacja nowatorskiego podejścia do wprowadzania kodu cyfrowego. Ideą tego rozwiązania jest wprowadzenie kolejnych cyfr PIN-u poprzez odnalezienie i wskazanie ich na ekranie urządzenia.

Rozwiązanie to zakłada, że w etapie tworzenia zabezpieczenia użytkownik wprowadza kod cyfrowy złożony z 5 cyfr a następnie zapisuje go jako bazowy kod PIN.

Odblokowanie odbywa się przy pomocy gestu przeciągnięcia palcem po ekranie w sposób podobny do wzoru odblokowania (Rys. 4.). Podczas próby odblokowania użytkownik wybiera jedną z czterech cyfr wyświetlonych w pierwszej linii. Po wybraniu punktu z uznaną za właściwą cyfrę przechodzi do wybrania kolejnej cyfry PIN-u spośród wyświetlonych w linii drugiej. Liczba wyświetlanych linii jest równa liczbie cyfr zadeklarowanego PIN-u. Pojawiające się na ekranie liczby w danej linii zawierają cyfry spośród których tylko jedna będzie właściwa, pozostałe natomiast są liczbami losowymi z przedziału 0-9 z wykluczeniem wartości właściwej. Istotną cechą w wyświetlanej linii jest fakt, że za każdym razem przy odblokowaniu cyfry są tasowane co sprawia, że ślad wykonywanego gestu za każdym razem będzie inny co ogranicza złamanie wzoru poprzez podejrzenie przez osoby postronne. Poniżej zaprezentowano grafiki



Rys. 4. Wprowadzanie kodu odblokowania przy pomocy nowego rozwiązania

przedstawiające 3 próby wprowadzenia wzoru z czego jedna okazuje się być niewłaściwa (Rys.4).

Wykorzystanie PIN-u o długości większej lub równej 5 umożliwi uzyskanie kombinacji określonych wzorem (4)

$$n^k \tag{4}$$

gdzie: n- wielkość zbioru możliwych cyfr ,k-liczba cyfr w PINie.

Natomiast wprowadzanie PIN-u przy pomocy metody wykorzystującej wzór uniemożliwi osobie niepowołanej jednoznaczne określenie szyfru. Dodatkowym zabezpieczeniem jest losowanie miejsca w linii, w którym pojawiać się będzie właściwa cyfra PIN-u co w rezultacie sprawi ze wskazywany na ekranie wzór nie będzie powtarzany oraz nie będzie możliwe powtórzenie zapamiętanego przez osobę niepowołaną wzoru.

Pojawienie się właściwej liczby na określonej pozycji jest określone prawdopodobieństwem wynoszącym 0,25.

W przypadku kiedy wzór ma długość 5 prawdopodobieństwo pojawienia się takiej samej kombinacji wynosi:

$$(1/4)^5 = 0.0009765625 \qquad (5)$$

4. Metoda Badań

4.1. Przedmiot badań

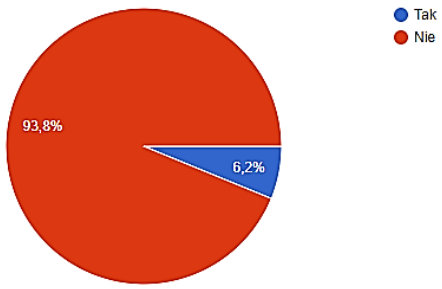
Przedmiotem badań są 2 aplikacje imitujące ekran blokady urządzenia z systemem Android. Dodatkowo aplikacje te w celu porównania badanych parametrów implementują funkcjonalności blokowania ekranu znane użytkownikom z system Android. Wspomniane aplikacje zbierają informacje na temat własności takie jak liczba pomyłek przy wprowadzaniu wzorca, czas wprowadzania wzorca, liczba możliwych kombinacji. Wykonanie aplikacji przez autorów zostało przy wykorzystaniu różnych technologii, tudzież języka programowania, lecz parametry podczas badania są mierzone według tych samych wyznaczników.

4.2. Grupa badawcza

Badania pozwalające na ocenę skuteczności i użyteczności metod autoryzacji użytkowników zostały przeprowadzone na grupie potencjalnych odbiorców tego typu rozwiązań.

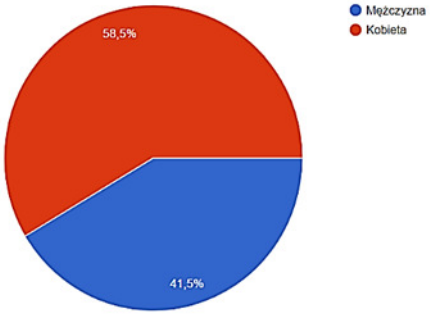
Pierwszą grupę stanowią anonimowi użytkownicy którzy za pomocą ankiety internetowej udzielili informacji na temat obecnego stanu znajomości tematyki związanej z autoryzacją dostępu do ich urządzeń.

Do ankiety przystąpiło 85 osób które odpowiedziały na 10 kluczowych pytań z zakresu wykorzystania metod blokady ekranu. Na pytania związane ścisłe z tematyką pracy odpowiadali tylko ci ankietowani, którzy zadeklarowali używanie urządzenia wyposażonego w ekran dotykowy z systemem Android. Zdecydowana większość, wynosząca 97,5% odpowiedziała twierdząco na pytanie czy zależy im aby urządzenie, z którego korzystają było zabezpieczone przed niepowołanym dostępem (Rys. 5).

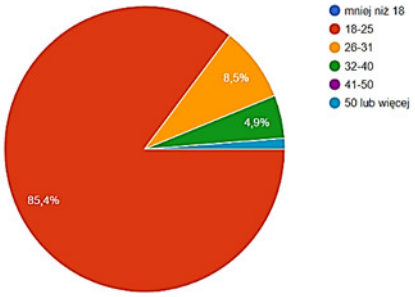


Rys. 5. Podział odpowiedzi użytkowników na pytanie o przywiązywanie uwagi do bezpieczeństwa posiadanego urządzenia

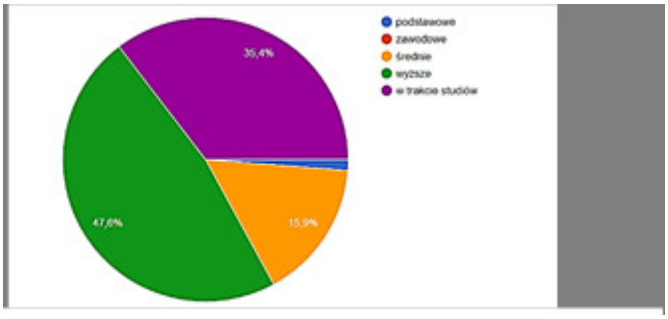
Spośród ankietowanych 58,5% stanowiły kobiety a 41,4% mężczyźni w wieku od 18 do 40 lat (Rys.6). Najliczniejszą grupę stanowiły osoby pomiędzy 18 a 25 rokiem życia, która liczyła 85,4 % całości (Rys. 7).



Rys. 6. Procentowy udział mężczyzn i kobiet w przeprowadzonej ankiecie



Rys. 7. Podział procentowy respondentów ze względu na wiek



Rys. 8. Procentowy udział ankietowanych ze względu na deklarowane wykształcenia

Osoby biorące udział w ankiecie deklarowały w 47,6%, że są osobami o wykształceniu wyższym a 35,4% w trakcie studiów. 15,9% to osoby które w pytaniu o wykształcenie zaznaczyły wartość „Średnie” (Rys 8).

Drugą grupę stanowiło 21 użytkowników, którzy przetestowali zaimplementowane przez autorów rozwiązania i poprzez użycie konkretnych metod, dostarczyli danych na podstawie których dokonywana była dalsza analiza problemu.

4.3. Proces gromadzenia danych

Badania, na których opierali się autorzy, przy sprawdzeniu efektywności metod zabezpieczania urządzeń mobilnych zostały wykonane w dwojaki sposób. Podział procesu pozyskiwania danych uwzględniał kontekst informacji i był uwarunkowany sposobem komunikacji z użytkownikami.

W pierwszej kolejności została przeprowadzona ankieta za pośrednictwem popularnej platformy Google Forms. Ankieta miała na celu dostarczenie informacji dotyczących świadomości użytkowników na temat problematyki autoryzacji dostępu i sposobów zabezpieczania prywatnych

urządzeń mobilnych, na których przechowują cenne oraz często prywatne dane. Postawione użytkownikom pytania dotyczyły m.in. faktu posiadania danych o charakterze poufnym oraz czy użytkownicy używają metod autoryzacji dostępu. Ponadto ankietowani zostali zapytani czy uważają, że domyślne sposoby autoryzacji są dostatecznie bezpieczne oraz czy znają i pokusiliby się o stosowanie takich rozwiązań.

Drugim sposobem na pozyskanie danych na potrzeby badań było udostępnienie użytkownikom urządzeń z wdrożonymi mechanizmami zabezpieczającymi oraz poproszenie ich o użycie zaprezentowanych metod autoryzacji. Badanie to miało na celu pozyskanie danych dotyczących jakości mechanizmów, na które wpływały m.in czas odblokowywania, liczba pomyłek na określoną liczbę prób. Czas odblokowania podany w sekundach, jest parametrem, którego pomiar zaczyna się przy wybraniu pierwszego elementu/liczby hasła, a pomiar kończy się po wybraniu ostatniego elementu. Kolejny badany parametr czyli liczba pomyłek, jest wartością, która mówi ile razy dany użytkownik pomylił się podczas autoryzacji.

5. Analiza wyników

5.1. Aplikacja

W tabeli 3 zestawiono maksymalne ilości kombinacji haseł, jakie można utworzyć w porównywanych metodach autoryzacji systemu Android.

Tabela 3. Ilość kombinacji w zależności od rodzaju blokady

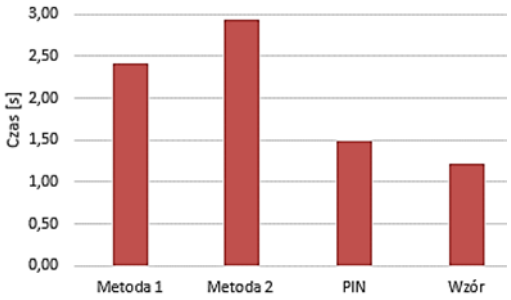
Rodzaj blokady	Maksymalna ilość Kombinacji
PIN	10000
Wzór	140704
Metoda 2	100000
Metoda 1	4758977059200

Największą liczbę kombinacji dostarczyć może nowo opracowana Metoda 1, gdzie przy konfiguracji siatki przycisków 6x7 oraz haśle o długości 8-miu liczb, można utworzyć ponad 4,7 biliona różnych haseł. Jest to wartość znacznie przewyższająca konkurencyjne rozwiązania. Im wyższa jest ta wartość, tym trudniej daną blokadę złamać, gdyż zmniejsza się prawdopodobieństwo odgadnięcia hasła, co jest jak najbardziej pożądanym zjawiskiem. Drugim pod tym względem rozwiązaniem jest blokada za pomocą wzoru, czyli sposób, który można znaleźć domyślnie zaimplementowany w systemie Android. Liczba kombinacji wzoru, jaki można utworzyć wynosi ponad 140tys. Niewiele gorszym rozwiązaniem pod względem ilości kombinacji hasła okazała się Blokada 2 opracowana przez autorów. Liczba różnych haseł jakich możliwe jest utworzenie wynosi 100tys. Najsłabszą metodą okazała się blokada przy pomocy cztero-cyfrowego kodu PIN. Dostarczyć ona może tylko 10 tys. różnych haseł, co powoduje, że w porównaniu do trzech pozostałych blokad staje się rozwiązaniem, które potencjalnie najłatwiej jest złamać, próbując wprowadzić jak najwięcej kombinacji.

Kolejnym analizowanym aspektem jest czas autoryzacji (Rys. 9, Tabela 4), czyli wprowadzanie wcześniej zdefiniowanego hasła bądź wzoru odblokowania. Jest to aspekt ważny, gdyż rozwiązania, które wymagają długiego czasu wprowadzania wzorca, mogłyby męczyć użytkowników i pomimo zapewnienia dobrego poziomu zabezpieczenia mogłyby sprawić, że użytkownik zrezygnowałby z ich używania na rzecz słabszych metod autoryzacji.

Tabela 4. Średni czas trwania autoryzacji użytkownika w zależności od blokady

Rodzaj blokady	Średni czas autoryzacji [s]
Metoda 1	2,42
Metoda 2	2,94
PIN	1,49
Wzór	1,21



Rys. 9. Średnia długość trwania autoryzacji dla poszczególnych metod

Odnotowano, że średni czas autoryzacji, jest najkrótszy w przypadku blokady wzorem. Czas ten wynosi 1,21s. Jest to najlepszy wynik spośród badanych narzędzi. Niewiele gorsza okazuje się blokada PIN, gdyż średni czas wprowadzania hasła wynosił prawie 1,5s. Gorzej wypadły nowo opracowane przez autorów rozwiązania. Średnie czasy wynosiły odpowiednio 2,42s (metoda 1), oraz 2,94s (metoda 2). Można zauważyć, że blokada PIN oraz wzór, wypadły lepiej niż pozostałe, lecz warto wspomnieć, że są to blokady, które większość użytkowników zna, posiada w swoim urządzeniu, bądź najprawdopodobniej kiedyś ich używało. Mogło to wpłynąć na to, że osoba testująca nie musiała na nowo poznawać danego mechanizmu działania, co skróciło czas autoryzacji. W przypadku rozwiązań opracowanych w celach naukowych, użytkownicy musieli poznać nowe mechanizmy autoryzacji oraz je zrozumieć, tak by potem pomyślnie stworzyć blokadę i przejść proces uwierzytelnienia. Z uwagi na ten fakt, czas potrzebny na odblokowanie mógł się wydłużyć. Warto dodać, że różnica między najwolniejszą metodą, a najszybszą to zaledwie 1,73s, co nie powinno mieć negatywnego wpływu na odczucia użytkowników.

Tabela 5. Ilość pomyłek w zależności od blokady

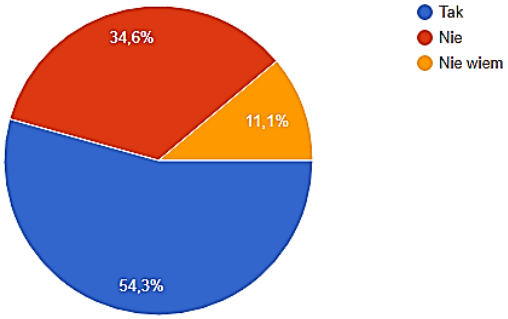
Rodzaj blokady	Liczba pomyłek
Metoda 1	2
Metoda 2	2
PIN	2
Wzór	1

Tabela 5 przedstawia ile osób popełniło błąd, w każdej testowanej metodzie podczas procesu uwierzytelniania. W trzech metodach czyli: metoda 1, metoda 2 oraz blokada PIN, dwóch użytkowników popełniło 2 błędy, natomiast tylko jeden użytkownik popełnił błąd przy użyciu blokady PIN. Analiza liczby popełnionych błędów może doprowadzić do wskazania rozwiązania, którego wzorzec może być trudny do zapamiętania. Dane zebrane podczas tego testu nie różnią

się od siebie drastycznie. W przypadku wszystkich testowanych metod autoryzacji wyniki były podobne, dlatego można stwierdzić, że pod względem trudności zapamiętania wzorca, badane rozwiązania są takie same.

5.2. Ankieta

Przeprowadzone badanie w formie anonimowej ankiety umożliwiło poznanie oczekiwań i świadomości użytkowników w zakresie skuteczności używanych przez ankietowanych rozwiązań. Spośród wszystkich ankietowanych niemal każdy uczestnik stwierdził że zależy mu na bezpieczeństwie danych, które przechowuje na swoim urządzeniu. Wyjątkami okazały się dwie osoby które na to pytanie odpowiedziały negatywnie.



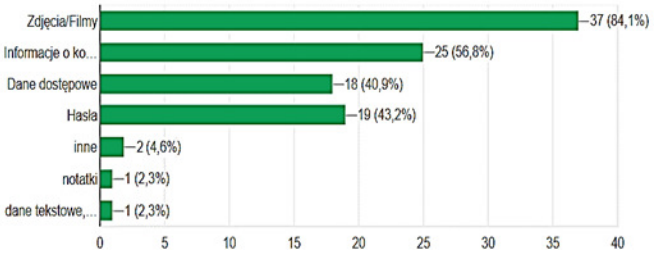
Rys. 10. Podział ankietowanych ze względu na świadomość posiadania danych poufnych na urządzeniach mobilnych

Istotną kwestią, która w ankiecie została poruszona, było pytanie do użytkowników na temat tego czy na swoich urządzeniach posiadają dane uznawane jako wrażliwe lub poufne. Spośród wszystkich odpowiedzi 54,3% użytkowników wykorzystuje swoje urządzenia do przechowywania takich informacji. 34,6% ankietowanych deklaruje, że nie posiada tego typu danych lub nie traktuje ich w taki sposób natomiast 11,1% respondentów nie było w stanie opowiedzieć zarówno twierdząco jak i przecząco na zadane pytanie (Rys.10).

Ankietowani zostali również zapytani o typy danych jakie przechowują. Dane te zostały zestawione na Rys. 11. Najpopularniejszą grupę stanowią prywatne zdjęcia i nagrania wideo. 84,1% ankietowanych udzieliło takiej odpowiedzi. Ponad połowa zapytanych osób przechowuje w swoich urządzeniach informacje teleadresowe i stanowi 56,8% całej grupy ankietowanych. Niewątpliwie istotną grupą danych jakie użytkownicy urządzeń przechowują są hasła i inne dane dostępowe do kont. Wyniki ankiety dla wyżej wymienionych grup wynoszą kolejno 43,2% dla haseł i 40,9% dla innych danych dostępowych. Sumując te wyniki otrzymujemy grupę która stanowi blisko 85% osób deklarujących posiadanie tego typu danych spośród wszystkich ankietowanych.

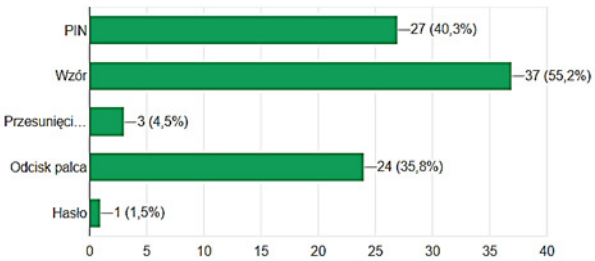
Wynik ten, w zestawieniu z najpopularniejszą grupą jaka stanowią multimedia, ukazuje jak poważną sprawą jest autoryzacja dostępu urządzeń mobilnych

Najrzadziej ankietowani wykorzystują smartfony do przechowywania poufnych notatek i dokumentów tekstowych (2,3%) oraz danych innej kategorii (4,6%).



Rys. 11. Najczęściej przechowywane na urządzeniach typy danych

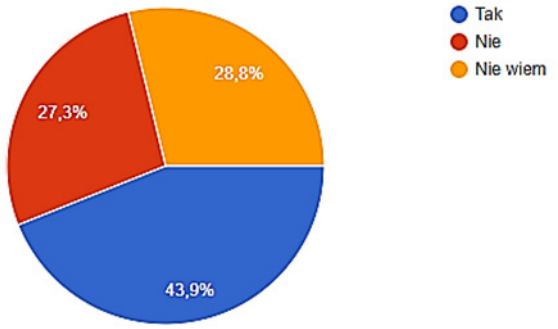
Kluczowym pytaniem przeprowadzonej ankiety było pytanie o to czy ankietowani w ogóle korzystają z jakiegokolwiek mechanizmu blokady ekranu. Jak się okazuje, pomimo świadomości zagrożeń i konsekwencji wynikających z nieautoryzowanego dostępu zaledwie 82,7% ankietowanych włączyło w swoim urządzeniu mechanizmy zabezpieczające. Widać zatem, że mimo deklaracji respondentów o tym, że zależy im na bezpieczeństwie urządzeń istnieją osoby, które nie podjęły kroków w tym kierunku i nie zabezpieczyły się przed niepowołanym dostępem. Na podstawie informacji uzyskanych od osób które zabezpieczyły swoje urządzania dostrzegamy, że najpopularniejszym sposobem blokady niepowołanego dostępu jest wzór odblokowania. Metoda polegająca na wprowadzeniu identycznej kombinacji połączenia punktów na ekranie jest stosowana przez 55,2% ankietowanych. Kolejnym bardzo popularnym sposobem okazuje się tradycyjny PIN, który stosowany jest przez 40,3% osób. 35,8% respondentów jako zabezpieczenie swoich urządzeń wykorzystuje metodę sprawdzania odcisku palca. Wynik ten jest uzależniony od liczby urządzeń wyposażonych w odpowiedni sensor pozwalający na sprawdzenie zgodności linii papilarnych. Najrzadziej wykorzystywanym sposobem jest odblokowanie za pomocą hasła złożonego ze znaków alfanumerycznych i jest wykorzystywany przez ok. 1,5% zapytanych osób (Rys. 12).



Rys.12. Popularność stosowanych mechanizmów zabezpieczających

Ankietowane osoby zostały również poproszone o odpowiedź na pytanie czy istniejące i znane im metody autoryzacji dostępu są skuteczne i wystarczające by zabezpieczyć urządzenie. Spośród zapytanych osób 43,9% są przekonane iż istniejące i wykorzystywane rozwiązania są bezpieczne i skutecznie uniemożliwiają dostęp do urządzenia i znajdujących się na nim danych osobom postronnym. Trochę więcej niż ćwierć osób (28,8%) nie jest w stanie określić czy i w jakim stopniu istniejące na rynku rozwiązania są skuteczne. Grupa ta nie odpowiedziała na pytanie się ani twierdząco ani przecząco. Pozostali, stanowiący 27,3% czyli nieco mniej niż niezdecydowani, są przekonani iż stosowane metody autoryzacji dostępu są zbyt

słabe i nie gwarantują satysfakcjonującego ich poziomu bezpieczeństwa.



Rys. 13. Procentowy rozkład zadowolenia z poziomu bezpieczeństwa zapewnianego przez standardowe mechanizmy autoryzacji

Zdecydowana większość użytkowników nie korzysta z popularnych i niestandardowych metod autoryzacji. Zapytani w ankiecie w 93,8% oznajmili, że nie używają metod które nie są preinstalowane w samym systemie operacyjnym. Zaledwie 6,2% ankietowanych zaznajomiło się z tematem i użyło mniej popularnych mechanizmów, które mogą okazać się nie lada zaskoczeniem dla osób niepowołanych. Ostatnim elementem ankiety były wolne sugestie ankietowanych dotyczące metod i możliwości jakie mogły by w przyszłości skutecznie służyć za mechanizmy zabezpieczające urządzenia. Wśród odpowiedzi najczęściej pojawiały się metody skanowania tęczówki oka oraz walidacja modelu głosu użytkownika. Ponadto ankietowani wymieniali ujęty w zestawieniu odczyt odcisku palca. Dużą uwagę ankietowanych przykuwała autoryzacja wieloetapowa wykorzystująca różne kanały komunikacyjne m.in. wiadomości SMS, email. Najbardziej wybiegającymi w przyszłość sugestiami były sposoby analizy DNA

6. Wnioski

Na podstawie badań przeprowadzonych pośród 21 osób zaobserwowano, że proces autoryzacji nowo opracowanych metod trwa w większości przypadków dłużej niż dla metod już stosowanych w systemie Android. Jest to m.in. spowodowane tym, że użytkownicy mieli styczność z takimi sposobami zabezpieczeń po raz pierwszy i po dłuższym czasie użytkowania ten czas mógłby ulec skróceniu. Biorąc pod uwagę liczbę kombinacji hasła najgorzej wypada blokada PIN, co oznacza że zapewnia najniższy poziom odporności na złamanie metodą sprawdzenia wszystkich kombinacji hasła zwaną Brute Force [10]. Najlepsza pod tym względem jest proponowana metoda 1, gdyż przy najbardziej złożonym haśle i największej siatce wzorca, zapewnia największą liczbę kombinacji. Druga po metodzie 1 jest blokada wzorem, która dostarcza o przeszło 40tys więcej kombinacji niż metoda 2. Poddając analizie liczbę błędów popełnianych przez testujących, wszystkie rozwiązania wypadają podobnie. Rozwinięcie badań w postaci przebadania dużo większej grupy, mogłoby dostarczyć dane, których analiza pomogłaby stwierdzić jakiś różnice pomiędzy badanymi rozwiązaniami.

Przeprowadzona ankieta dostarcza informacji dotyczących zachowania, przyzwyczajeń oraz oczekiwań użytkowników urządzeń mobilnych. Z badania jednoznacznie wynika, że respondenci chcą chronić swoje urządzenia przy pomocy skutecznych mechanizmów jednak niejednokrotnie brakuje im poczucia iż wykorzystywane obecnie metody są nadal bezpieczne. Spośród wykorzystywanych predefiniowanych mechanizmów w systemie Android najbardziej doceniany przez użytkowników jest „wzór odblokowania" stosowany przez ponad połowę ankietowanych. Zestawienie wykorzystywanych mechanizmów i ich procentowy udział w stosowaniu ukazuje, że blokada przy pomocy odcisku palca staje się coraz częściej wykorzystywanym sposobem. Walidacja odcisku palca zapewnia duże poczucie bezpieczeństwa o czym może świadczyć fakt wskazywania tego rozwiązania w wolnych sugestiach od ankietowanych. Najczęściej przechowywanymi materiałami są dane multimedialne często o charakterze poufnym i istotnym znaczeniu sentymentalnym dla użytkowników, a także dane wykorzystywane w codziennych czynnościach związanych z bankowością, biznesem i komunikacją. Tego rodzaju dane wymagają szczególnej ochrony, którą mechanizmy autoryzacji powinny zapewniać.

Wyniki ankiety ukazują, że blisko 29% niepewność ankietowanych oraz 27% przekonanie o braku skuteczności popularnych sposobów autoryzacji dostępu wskazuje obszar, w którym istnieje potrzeba rozwijania oprogramowania i ulepszania urządzeń w celu zapewnienia jak najbardziej bezpiecznego i odpornego na ataki mechanizmu blokady urządzenia przed niepowołanym dostępem. Sprostanie wymaganiom użytkowników w tym obszarze stanowi niewątpliwie wyzwanie dla producentów zarówno oprogramowania jak i urządzeń a także okazuje się świetnym obszarem badań, których rezultatem mogą być nowe przełomowe koncepcje jak i udoskonalone wersje znanych metod zabezpieczania urządzeń.

Literatura

[1] First Android Phone http://www.spinfold.com/first-android-phone/ [30.05.2017]

[2] Number of smartphone users worldwide from 2014 to 2020 (in billions, https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ [26.05.2017]

[3] Global market share held by smartphone operating systems from 2009 to 2016, https://www.statista.com/statistics/263453/ global-market-share-held-by-smartphone-operating-systems// [26.05.2017]

[4] Taekyoung Kwon, Sarang Na, TinyLock: Affordable defense against smudge attacks on smartphone pattern lock systems, Graduate School of Information, Yonsei University, Seoul 120-749, Republic of Korea, 2013.

[5] J. Angulo, E. Wästlund, P. Gullberg, D. Kling, D. Tavemark, S.Fischer-Hübner, Understanding the user experience of secure mobile online transactions in realistic contexts of use, 2012.

[6] Kwang Il Shin ,Ji Soo Park, Jae Yong Lee, Jong Hyuk Park, Design and Implementation of Improved Authentication System for Android Smartphone Users, 2012.

[7] Hsin-Yi Chiang, Sonia Chiasson, Improving user authentication on mobile devices: A Touchscreen Graphical Password, 2013.

[8] Chen Sun, Yang Wang, Jun Zheng, Dissecting pattern unlock: The effect of pattern strength meter on pattern selection, 2014.

[9] Marte Dybevik Løge, Tell Me Who You Are and I Will Tell You Your Unlock Pattern, 2015.

[10] M. Bond, P. Zielinski Decimalisation table attacks for PIN cracking, 2013