ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2017
Seria: ORGANIZACJA I ZARZĄDZANIE z. 113 Nr kol. 1992

Dawid PIECHACZEK, Ireneusz J. JÓŹWIAK
Politechnika Wrocławska
Wydział Informatyki i Zarządzania
dawidpiechaczek.20@gmail.com, ireneusz.jozwiak@pwr.edu.pl

STRATEGIE ZAPEWNIANIA BEZPIECZEŃSTWA SYSTEMÓW MOBILNYCH

Streszczenie. Obecny postęp technologiczny oraz rozwijanie wielu nowych trendów w wytwarzaniu oprogramowania na smartfony powoduje, że coraz częściej poddawany wątpliwości jest aspekt bezpieczeństwa korzystania z systemów mobilnych. Istnieje szereg codziennych sytuacji, które zlekceważone mogą powodować wyciek bardzo wrażliwych danych lub ułatwienie przechwytywania ich przez przestępców. W artykule poddane dyskusji zostały różne podejścia ochrony danych użytkowników korzystających z urządzeń mobilnych.

Słowa kluczowe: bezpieczeństwo, systemy mobilne, aplikacje mobilne, oprogramowanie, strategia

STRATEGIES OF PROVIDING SECURITY IN MOBILE SYSTEMS

Abstract. Current technological progress and the evolution of a great number of new trends in software development for smartphones, causes a lot of doubts and questions about the security aspect of contemporary mobile systems. There are a lot of everyday situations, which, if underestimated, can put highly sensitive data in danger. The paper presents various strategies in providing security of data for mobile devices' users.

Keywords: security, mobile systems, mobile apps, software, strategy

1. Wprowadzenie

Urządzenia oparte na systemach mobilnych, to obecnie jedne z najbardziej powszechnych i ogólnodostępnych akcesoriów elektronicznych na rynku. W 2014 roku, w Polsce abonentami telefonii komórkowej było ponad 57 mln użytkowników według danych GUS [6].

Liczba ta przerasta już polską populację, prawodpodobnie z tego powodu, że dużo użytkowników posiada zarejestrowany więcej niż jeden numer telefonu. Ponadto jest wiele urządzeń, które posiadają systemy mobilne, ale ich główne przeznaczenie to rozrywka m.in. tablety i telewizory. Każde z wymienionych urządzeń posiada zazwyczaj więcej niż jedną aplikację. Dopiero po wstępnym oszacowaniu liczby potencjalnych użytkowników, można uzmysłowić sobie jak istotne jest zachowanie bezpieczeństwa danych, które są przetwarzane przez te aplikacje.

Odpowiednia kontrola oraz dbałość o bezpieczeństwo na wielu poziomach wymiany informacji może skutecznie utrudnić próby przejęcia danych przez napastnika lub pomóc zatuszować przynajmniej część z wrażliwych informacji.

2. Poziomy zapewniania bezpieczeństwa w systemach mobilnych

Zapewnienie bezpieczeństwa systemów mobilnych jest bardzo złożonym zagadnieniem, ponieważ zależy w dużej mierze od wielu osób - zaczynając od administratorów danych, poprzez programistów, kończąc na użytkownikach korzystających z urzadzeń oraz napastnikach, którzy mają na celu przechwycenie danych [4]. Wśród strategii dbania o bezpieczeństwo należy wyróżnić nastepujace poziomy ochrony danych [3]:

- bezpieczeństwo infrastruktury mobilnej,
- bezpieczeństwo aplikacji mobilnych,
- bezpieczeństwo urządzeń końcowych.

Na każdym z wymienionych poziomów zachowanie odpowiednich wzorców bezpieczeństwa jest kluczowe dla ochrony użytkowników systemów mobilnych. Warto skupić się na zagadnieniach dotyczących bezpieczeństwa przede wszystkim na platformie Android, ponieważ na niej istnieje całkowita dowolność ingerencji w system oraz możliwość łatwego korzystania z niezaufanych aplikacji, które mogą obniżać odporność systemu [3].

3. Strategie bezpieczeństwa na poziomie infrastruktury mobilnej

Infrastruktura mobilna jest kluczowa jeśli chodzi o interakcję systemu mobilnego z innymi systemami. Stale dochodzi do wymiany danych między nimi na odległość, przechowywania tych danych w pamięci oraz ich nieustannej synchronizacji. Dlatego na tym poziomie warto zadbać o odpowiednią jakość połączenia oraz stabilne miejsce przechowujące dane. Wybór połączenia między systemami bardzo często uzależniany jest od róznych czynników m.in. odległości. Obecnie bardzo popularnym rozwiązaniem jest korzystanie z

NFC (ang. *Near Field Communication*), korzystającego z RFID (ang. *Radio-Frequency Identification*), czyli technologii służacej do identyfikacji częstotliwości radiowej [3]. Jest to technologia krótkozasięgowa, bezprzewodowa, zapewniająca przesył danych na bardzo małe odległości, tj. do paru centymetrów. W wielu przypadkach wymaga wręcz stykania się urządzeń w celu wykonania akcji. NFC uznawany jest za bezpieczniejsze rozwiązanie od połączenia typu Bluetooth, głównie z powodu zasięgu jakim dysponuje – zmniejsza on prawdopodobieństwo przechwycenia danych. Początkowe standardy tej technologii służyły do przesyłania kontaktów oraz adresów URL (ang. *Uniform Resource Locator*). Obecnie NFC zyskało mocno na znaczeniu poprzez dokonywanie zbliżeniowych transakcji bezgotówkowych za pomocą tej technologii. Należy podejmować bardzo ostrożne strategie obchodząc się z narzędziami umożliwiającymi przepływ pieniędzy. Warto zwrócić uwagę, że pomimo tego, że połączenia są szyfrowane (zazwyczaj obowiązuje standard EMV – ten sam, który zabezpiecza karty płatnicze) i w momencie, gdy przestępca nie jest w stanie złamać klucza, to przesyłane informacje powinny pozostać bezpieczne. Jednakże transakcje zbliżeniowe pozbawione są dodatkowego zabezpieczenia w postaci kodu PIN, który jest używany przy standardowej płatności. Szczęśliwie większość banków wprowadza limity liczby operacji oraz ich wysokości, aby w razie utraty danych zapobiec niepożądanym transakcjom na wysokie kwoty. Wymiana danych z NFC przez takie limity staje się mniej atrakcyjna dla przestępców, a prawodpodobieństwo utraty pieniędzy jest na możliwie niższym poziomie od posiadania zwykłej gotówki w portfelu. Należy jednak nadal ostrożnie posługiwać się tą technologią, bo bardzo trudno stwierdzić, jakie dane mogą na karcie przechowywać banki, w których trzymane są nasze oszczędności. Konsekwencją tego nie musi być koniecznie utrata gotówki podczas ataku, ale zagrożenie dla danych użytkownika, które są odpowiedzialne za uwierzytelnianie transakcji. Dodatkowo udokumentowane są już ataki polegające na zarażeniu telefonu oprogramowaniem, które zamieniało NFC w terminal, który po zbliżeniu z portfelem był w stanie sczytywać dane z karty. Przed tym powinien chronić zakup portfela ekranowanego, który dzięki swojej strukturze i materiałom zapobiega sczytywaniu danych z kart zbliżeniowych.

Kolejną strategią używaną w łączności infrastruktury systemów mobilnych są sieci VPN (ang. *Virtual Private Network*). Zalecane jest korzystanie z nich w celu szyfrowania swojego połączenia, co pozwala na skuteczne ukrycie przesyłanych danych. Tego niestety nie jest w stanie zapewnić każde połączenie typu Wi-Fi [3]. Istnieje wiele niebezpiecznych sieci, które nie są dodatkowo zabezpieczone i mogą pozwolić na skuteczny atak lub obserwację ruchu sieciowego. Sposób szyfrowania VPN nazywany jest tunelowaniem i polega na wychwyceniu wszystkich wysyłanych przez użytkownika pakietów, szyfrowaniu ich, a następnie umieszczaniu w nowym pakiecie. Zaletą VPN jest to, że ukrywa ruch użytkownika przed innymi korzystającymi z sieci, co pozwala na większą swobodę korzystania z serwisów wykorzystujących wrażliwe dane m.in. konto pocztowe, czy bankowe. Najlepsze strategie bezpieczeństwa zdecydowanie powinny obejmować korzystanie z połączenia VPN, ponieważ

jest ono dostępne wszędzie, a zarazem zapewnia bezpieczeństwo na wyższym poziomie niż zwykłe połączenie z siecią Wi-Fi dostępną w miejscu publicznym.

Do szyfrowania komunikacji w aplikacjach mobilnych najczęściej używanym protokołem jest HTTP (ang. *Hypertext Transfer Protocol*) ustanowiony w konwencji żądanie – odpowiedź. Zabezpieczenie tego protokołu opiera się zazwyczaj na dodaniu mechanizmu certyfikatu SSL. Wielu programistów wyznaje filozofię, że jeżeli używają protokułu HTTPS, to zapewniają już bezpieczną, zaszyfrowaną komunikację i to wszystko co mogli zrobić, aby uchronić użytkownika przed utratą danych. Niestety w tym momencie zapominają o możliwości przeprowadzenia bardzo powszechnego ataku znanym jako MiTM (ang. *Man in The Middle*), który może być przeprowadzony praktycznie z każdego miejsca [5]. Atak ten polega na dołączeniu się do sieci w taki sposób, aby urządzenie rozpoznawało inne urządzenie, np. router jako kolejny węzeł sieci. Taki skompromitowany węzeł ma jedynie za zadanie zaproponować dwa fałszywe certyfikaty, po jednym dla klienta i serwera. Wtedy urządzenie klienta nie rozpoznaje takiej sytuacji i użytkownik jest przekonany, że dane nadal są bezpiecznie wymieniane pomiedzy nim a serwerem. Komunikacja między źródłem, a celem nadal istnieje, niestety wszystkie informacje na dodanym węźle są rozszyfrowywane, pobierane i wysłane zaszyfrowne fałszywym certyfikatem. Rozwiązać ten probelm może bardzo prosta implementacja przypinania certyfikatów (ang. *certificate pinning*). Ten zabieg polega na ciągłej weryfikacji tego, czy przychodzący komunikat został na pewno zaszyfrowany przez serwer. Wtedy klient może komunikować się tylko z serwerami, których certyfikaty ma zapisane. Dzięki temu chronimy się przed ingerencją fałszywych węzłów w komunikację użytkownika z serwerem.

Obecnie bardzo dyskusyjną kwestią jest przechowywanie danych w chmurze. Rozwiązanie to zapewnia bezpieczeństwao danych rozumiane jako kopia, która pozwala przywrócić utracone dane w razie ich utraty. Dostęp do chmury jest zapewniony z każdego miejsca, w którym użytkownik ma dostęp do telefonu, dane można swobodnie zapisywać, edytować i usuwać. Dodatkowo chmura zapewnia bardzo dużą przestrzeń do przechowywania danych. Dużą wadą tego rozwiązania jest jednak to, że użytkownik nigdy nie może być pewny w jakim stopniu z tych danych korzysta oraz jak dobrze zabezpieczył dane użytkowników usługodawaca udostępniający taką chmurę [1]. Wydaje się jednak, że tak duży dostawca jak Microsoft, czy Google jest w stanie zapewnić dobry standard bezpieczeństwa swoim użytkownikom, a co za tym idzie przechowywanie swoich danych w chmurze powinno być coraz bardzej bezpieczne.

4. Strategie bezpieczeństwa na poziomie aplikacji mobilnych

Dbanie o bezpieczeństwo korzystania z aplikacji mobilnych zaczyna się już na etapie pobierania i instalacji oprogramowania. Aplikacje z systemem Android wymagają pozwoleń, aby dokonywać akcji narażonych na utratę danych [5]. Od wersji Androida 6.0 te pozwolenia są podzielone na pozwolenia niebezpieczne, które są udzielane za zgodą użytkownika (dynamicznie) oraz na normalne pozwolenia, które są umieszczane w pliku zwanym manifestem i nie wymagają zgody użytkownika w czasie działania aplikacji. O wszystkich wymaganych zezwoleniach użytkownik jest informowany przez aplikację już na etapie instalacji, dlatego przezorny użytkownik może zaniechać instalacji, jednocześnie chroniąc się przed niechcianym wyciekiem danych, jeśli uzna, że pozwolenie będzie wymagało zbyt poufnych informacji. Pozwolenia w systemach Android obejmują m.in. informacje o położeniu telefonu, zapis informacji do pamięci smartfona, korzystanie z Internetu oraz dostęp do ustawień telefonu. Aplikacje, które wymagają takich pozwoleń mogą po udzieleniu zgody bezkarnie pobierać lokalizację użytkownika (często używane dla celów marketingowych, np. pokazywanie reklam zależnie od zbliżającego się do danego obiektu użytkownika) [1] lub zapisywać istotne dane w pamięci telefonu (dane znajdujące się na dysku są stosunkowo łatwe do znalezienia i są często celem ataków). Dlatego najlepsza strategia dotycząca bezpieczeństwa korzystania z aplikacji mobilnych obejmuje uważne sterowanie pozwoleniami na telefonie. Nie powinno się instalować aplikacji wymagających zbyt wiele pozwoleń, względem tego, czego od aplikacji oczekuje użytkownik.

Przeciętny użytkownik smartfona nie jest świadom wielu niebezpieczeństw czyhających przy codziennym użytkowaniu swojego urządzenia. Wiele z takich problemów wydaje się być trywialnych, ale warto zwrócić uwagę jak proste strategie mogą pomóc w ochronie danych użytkowników. Powszechnym problemem jest tworzenie zrzutów ekranu. Użytkownik może zachować widok znajdujący się na ekranie i zapisać w pamięci telefonu. Niestety często dzieje się tak, że użytkownik nie jest świadom, że zapisuje na zrzucie bardzo istotne informacje, których nie dostrzegł w momencie zapisu. Bardzo mała liczba osób jest świadoma, że zrzuty ekanu są robione nie tylko w momencie, gdy żąda tego użytkownik. Najbardziej powszechnym momentem, kiedy najczęściej widok naszego ekranu jest zapisywany bez naszej wiedzy to chwila odesłania aplikacji w tzw. tło. Osoba korzystająca z telefonu może używać zarazem większej liczby aplikacji, ale w danym momencie używania jednej, drugą najprawdopodobniej wysłał w stan oczekiwania, nazywanym pracą w tle. Wtedy większość telefonów posiada skrót pokazujący jakie aplikacje działają w tle, a ich zawartość jest obrazowana właśnie zrzutami ekranu, które są zapisane w pamięci telefonu. Dlatego istotną strategię przyjęły aplikacje bankowe, które są najbardziej narażone na tego typu wycieki. Poprzez proste zabiegi na poziomie kodu można utajnić aplikację tak, aby nie była widoczna w kontenerze zawierającym aplikacje w tle, lub w ogóle można zabronić

wykonywanie takiej aplikacji zrzutów tzw. screeshotów. Takie zachowanie upewnia ludzi rozwijajacych dany produkt, że użytkownik nie dokona jakiegoś niespodziewanego zapisu wrażliwych danych takich jak hasła, numery identyfikujące klienta czy numery karty.

Kolejnym bardzo prostym zagadnieniem w tematyce bezpieczeństwa, a zarazem często pomijanym jest korzystanie z klawiatury w telefonie. Aplikacja najczęściej musi przetworzyć wszystkie wyrazy wpisywane przez użytkownika, w tym ważne hasła, numery, czy dane logowania. Często klawiatury w smartfonach w celu ułatwienia życia użytkownikom proponuje możliwość zapisywania wcześniej wpisanych wyrazów np. adresu e-mail, danych wpisywanych w formularzach itd. Jednak nie wszystko co ułatwia życie jest bezpieczne, a to najlepszy przykład. Ostatnim głośnym przypadkiem była klawiatura, zapamiętująca adresy e-mail ludzi, którzy korzystali z monitora – informatora jednej z sieci kin. Dowolna osoba korzystająca z niego mogła swobodnie sczytać wrażliwe dane, ponieważ aplikacja podpowiadała kolejne słowa na podstawie już wpisanych. Na szczęście tutaj również istnieją mechanizmy, które zapobiegają zapisywaniu takich danych przez klawiaturę. Najłatwiejszym sposobem ochrony użytkownika przez programistę jest dbałość o nadawanie odpowiednich typów dla pól, w których można wpisywać tekst – w Androidzie kontrolki te noszą nazwy EditText. Można w nich wyspecyfikować typ wpisywanych danych, np. liczba lub e-mail, co pozwoli zrozumieć systemowi, że dana kontrolka wymaga specjalnego traktowania. Wszystkie hasła powinny być strzeżone za pomocą typu „password”. Pozwala on na utajnienie treści pisanego tekstu oraz zapobiega zapamiętywaniu pisanego tekstu na klawiaturze i nie będzie on wyświetlany w podpowiedziach. Dodatkowo odpowiedni typ wygasza możliwość kopiowania tesktu z kontrolki, ponieważ trzymanie poufnych danych w schowku telefonu jest również bardzo niebezpiecznym zjawiskiem, którego powinno się unikać.

Dodatkowo wymagana jest odpowiednia strategia ochrony aplikacji już po wydaniu jej dla użytku publicznego. Zawartość każdej aplikacji może zostać odkryta przy użyciu odpowiedniego dekompilatora, co pozwala zajrzeć napastnikowi w kod źródłowy aplikacji. Dlatego bezwzględnie należy unikać sytuacji, w których istotne informacje są zapisywane bezpośrednio w programie m.in. poufne dane, klucze czy tokeny pozwalające łączyć się z serwerami. Posiadając część tych danych napastnik może nie tylko zaatakować aplikację mobilną, ale również uzyskać dane do części serwerowej aplikacji. Dodatkowym zabezpieczeniem jest używanie narzędzi szyfrujących kod lub zmniejszające jego czytelność [1]. Android zapewnia w swoich aplikacjach wbudowane narzędzie ProGuard, które pomaga zaciemniać odczyt kodu programu. Ponadto zalecane jest szyfrowanie programu przy pomocy klucza, generowanego przy pomocy dobrego algorytmu szyfującego np. AES lub RSA, który powinien być trzymany w KeyStore, który umożliwia bezpieczne przechowywanie danych dla każdej aplikacji osobno. Codziennością powinno być używanie funkcji skrótu do przechowywania wrażliwych danych użytkownika wpisywanych przez niego w aplikacji.

5. Strategie bezpieczeństwa na poziomie urządzeń końcowych

Ostatnim poziomem dbania o bezpieczeństwo są same urządzenia i zarządzanie nimi w taki sposób, aby nie były narażane na ataki. Na pewno jednym z niebezpieczeństw jest sprzedaż telefonu innej osobie. Należy przed taką transakcją dokonać procedury całkowitego wyczyszczenia pamięci telefonu lub przywrócenia jej do ustawień fabrycznych. Jakiekolwiek ręczne usuwanie danych może pozostawić wiele pominiętych plików, które zawierają istotne informacje o użytkowniku. Nawet usunięcie wszystkich utworzonych przez właściciela plików nie jest gwarantem, że zostały usunięte również pliki aplikacji (część źle zaprogramowanych aplikacji nie usuwa wszystkich plików powiązanych z nią), które również przechowują cenną zawartość.

Kolejnym niezwykle ważnym apektem ochrony swojego urządzenia jest dbałość o stałe aktualizacje. Jedna sprawa to aktualizacja aplikacji, z których korzysta użytkownik – na pewno nowsza wersja stara się eliminować błędy wersji poprzednich. Przede wszystkim jednak należy pamiętać o aktualizacji całego systemu, w szczególności korzystając z platformy Android [3]. Niestety smartfony z tym systemem są dużo bardziej podatne na ataki i różne luki w bezpieczeństwie, dlatego każda nowa aktualizacja ma na celu eliminację takich dziur i poprawę wydajności urządzenia. Dodatkowo należy pamiętać, że produkty z Androidem, które nie są flagowymi produktami wielkich producentów zazwyczaj dosyć szybko tracą wsparcie, tzn. brak jest dostępnych aktualizacji na te urządzenia, co automatycznie skazuje je na duże niebezpieczeństwo – każdy użytkownik powienien być tego świadomy.

Dosyć trywialnym zagadniem jest dbałość o odpowiednie blokowanie dostępu do telefonu. Jednak wiele ludzi kierujących się wygodą (często liczy się szybkość dostępu do urządzenia) rezygnuje z tego rodzaju zabezpieczenia, a to duży błąd. Mamy całą gamę dostępnych rozwiązań będacych rodzajem blokady na telefony. Zaczynając od standardowego PINu (jego długość nie musi być 4 znakowa, coraz częściej spotykane są dłuższe wersje tego kodu), znaki rysowane przez użytkownika na ekranie, hasła, ale ostatnio również coraz częściej są to zabezpieczenia wykorzystujące unikalność ludzką – linie papilarne, rozpoznawanie twarzy oraz tęczówki oka [6]. O ile trudno podejmować dyskusję z bezpieczeństwem tych ostatnich metod, to standardy używania haseł są dobrze znane. Obecnie najlepszą strategią jest wymaganie zróżnicowanego tekstu, posiadającego duże i małe litery, cyfry oraz znaki specjalne. Jest to absolutne minimum, które mimo wszystko powinno zapewnić bezpieczeństwo urządzenia.

Niebezpieczne są również takie zjawiska jak jailbreaking i rootowanie [2]. Pierwszy termin określa czynność, która polega na celowym zrzuceniu ograniczeń z systemu, aby móc dokonywać na nim operacji, które były skutecznie ograniczane przez poprzednią dystrybucję. Częściej to zjawisko występuje jednak na telefonach z systemem iOS, gdy użytkownicy po

prostu chcą korzystać swobodniej z produktów tego systemu lub gdy chcą zainstalować inny system. Rootowanie z kolei jest zjawiskiem najczęściej obserwowanym na Androidzie, kiedy użytkownik nadaje sobie uprawnienia administratora, czyli root'a [3]. Takie sposoby wydają się dla wielu użytkowników korzystne, ponieważ zrzucają pewnego rodzaju ograniczenia, ale najczęściej łączą się one z utratą gwarancji na dane urządzenie oraz sporym niebezpieczeństwem związanym z tym, że dostęp do aplikacji jest nieograniczony. Osoba nieświadoma tego co robi może przyczynić się do zaprzestania poprawnego działania systemu. Ponadto brak podjęcia działań, które zablokują pootwierane przez mechanizm rootingu drogi dostępu do smartfona może spowodować, że bezpieczeństwo zostanie trwale naruszone przez atakującego [5].

6. Podsumowanie

Przy programowaniu aplikacji mobilnych oraz korzystaniu z urządzeń mobilnych istotne jest ograniczenie niebezpieczeństwa do minimum. Nigdy nie będzie możliwości pełnej ochrony swoich danych, ale każde nawet najmniejsze zabezpieczenie może być kluczowe w walce z potencjalnymi atakami. Poruszane w tym artykule strategie mogą wydawać się trywialne, ponieważ część zachowań jest ogólnie znana i respektowana, przede wszystkim w środowisku informatyków oraz młodzieży. Jednak ciągle istnieje duża grupa osób, szczególnie ludzi starszych oraz mniej zaznajomionych z nowymi technologiami, która nie jest świadoma, że takimi prostymi sposobami można przynajmniej w małym stopniu utrudnić potencjalnemu intruzowi uzyskać nasze dane lub pieniądze – co najczęściej jest przykrą konsekwencją braku przestrzegania podstawowych zasad bezpieczeństwa. Dodatkowo, ten artykuł ma na celu uświadamiać programistów (nie zawsze tych poczatkujących), że wszystko co jest przez nich oprogramowane, wymaga dobrego szyfrowania – od obiektów i haseł użytkowników w bazie danych, po elementy zawarte w kodzie, m.in. tokeny dostępu do serwisów [1]. Zaproponowane strategie powinny poprawić bezpieczeństwo naszych danych, co w obecnych czasach jest bardzo cenną wartością.

Bibliografia

1. Czajka R., Lipszyc J.: Poradnik bezpieczeństwa mobilnego. Fundacja Nowoczesna Polska, Warszawa 2014.
2. Dickson F.: Hardening Android: Building Security into the Core of Mobile Devices, [in:] Secure Networking, vol. 2 No. 4. Frost & Sullivan, San Antonio 2014.

3. Drake J., Fora P., Lanier Z., Mulliner C., Ridley S., Wicherski G.: Android. Podręcznik Hackera. Helion, Gliwice 2015.
4. Dziedzinowe Bazy Wiedzy GUS, http://swaid.stat.gov.pl/TransportLacznosc_dashboards/Raporty_predefiniowane/RAP_DBD_TRANS_19.aspx [dostęp 24.08.2017]
5. Elenkov N.: Android Security Internals. No Starch Press Inc., San Francisco 2015.
6. Rostański M., Borczyk W., Buchwald P., Duda J., Mączka K., Świtała P.: Projektowanie, zastosowania i rozwój aplikacji mobilnych. Wyższa Szkoła Biznesu w Dąbrowie Górniczej, Dąbrowa Górnicza 2015, s. 83-98.