Zeszyty Naukowe Wydziału
Elektroniki i Informatyki
Politechniki Koszalińskiej

ISSN:1897-7421
Nr 13, Listopad 2018
Str: 47-54

Grzegorz Górski
Marcin Nowacki
Zakład Systemów Multimedialnych i Sztucznej Inteligencji
Wydział Elektroniki i Informatyki
Politechnika Koszalińska

Analiza zagrożeń bezpieczeństwa dla współczesnych platform mobilnych

Słowa kluczowe: zaufany system informatyczny, urządzenia mobilne, analiza bezpieczeństwa

1. Wprowadzenie

Powszechna dostępność telefonii komórkowej istotnie zmieniła sposób funkcjonowania ludzi na całym świecie. O ile początkowo telefonów komórkowych używano główne do realizacji połączeń głosowych oraz wysyłania wiadomości tekstowych, to obecnie pełnią one rolę mobilnych komputerów. W telefonach przechowywane i przetwarzane są zarówno informacje biznesowe jak i prywatne w większości dostępnych postaci i formatów. Powszechny dostęp do informacji jest obecnie traktowany jako prawo jednostki gwarantowane przez państwo.

Nie byłoby to oczywiście możliwe bez nieustannego rozwoju technologicznego, tj. nowych procesów wytwarzania układów scalonych, nowych modeli coraz bardziej wydajnych procesorów oraz innowacyjnych narzędzi i technologii informatycznych wykorzystywanych do tworzenia rozmaitych usług w sieci Internet. Prowadzone prace badawcze dotyczą także zagadnień bezpieczeństwa danych przetwarzanych na urządzeniach mobilnych. Niestety w tej kwestii świadomość użytkowników telefonii komórkowej jest ciągle bardzo niska. W wielu przypadkach nie są oni świadomi, że korzystanie z publicznych sieci istotnie zwiększa ryzyko nieautoryzowanego dostępu do poufnych informacji zgromadzonych w telefonie.

2. Powszechne zagrożenia w systemach mobilnych

W artykule opisano wybrane grupy zagrożeń (klasy ataków), które w większości mogą być wykonane bez świadomości użytkownika, nawet w przypadku jeśli posiada on ponadprzeciętną wiedzę dotyczącą szeroko pojętej informatyki.

Do tych najbardziej popularnych należą:

- błędy w mobilnych systemach operacyjnych,
- korzystanie z sieci internetowej poprzez niezabezpieczone punkty dostępu Wi-Fi, m.in. w miejscach publicznych,
- instalowanie aplikacji mobilnych z niezaufanych źródeł,
- niedostateczna weryfikacja aplikacji przez tzw. „Sklepy aplikacji",
- brak świadomości użytkowników wobec zagrożeń, które mogą wystąpić w skutek niewłaściwego korzystania z urządzeń mobilnych.

Poza wymienionymi powyżej zagrożeniami, informacje zgromadzone na urządzeniach mobilnych - podobnie jak w przypadku komputerów osobistych – są podatne na znane rodzaje ataków takie jak: phishing (wyłudzenie informacji od użytkownika), backdoor (nieautoryzowane kanały dostępu do informacji), malware (modyfikacje kodu aplikacji lub podłączane złośliwego kodu do aplikacji użytkowych) oraz na ataki wykorzystujące komponenty sprzętowe telefonów komórkowych np. kamerę, czytnik linii papilarnych czy też skaner twarzy.

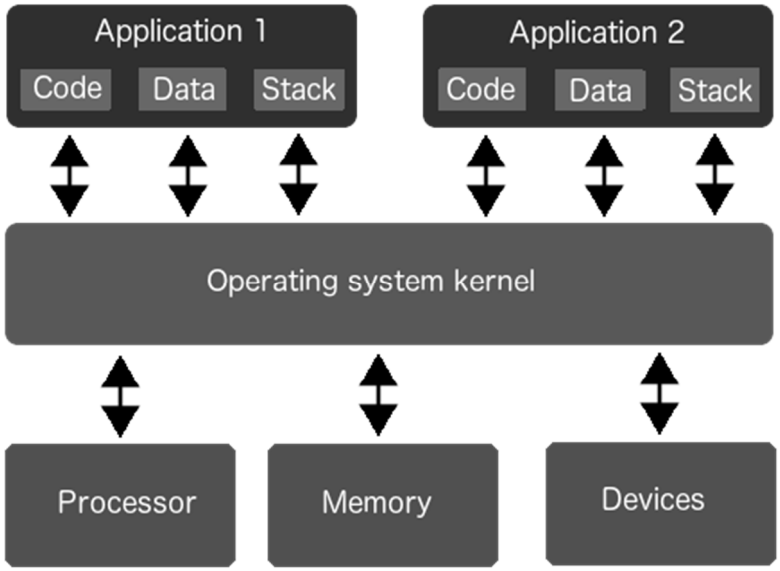
3. Zaufany system komputerowy

Celem każdej analizy zagrożeń jest wskazanie słabych ogniw systemów informatycznych, które mogą być wykorzystane do stworzenia nieautoryzowanego kanału dostępu do danych. Pierwotnym problemem jest określenie oczekiwań użytkowników, którzy chcą korzystać z urządzeń mobilnych przy jednoczesnym zapewnieniu akceptowalnego poziomu bezpieczeństwa, a zatem oczekują produktów, do których będą mieli zaufanie. Istnieje wiele definicji zaufanego system komputerowego. Jednakże każda z nich wskazuje, że jest to dany zestaw sprzętu i oprogramowania, na którym jego użytkownik może w pełni polegać oraz posiada nad nim całkowitą kontrolę.

Taka prosta definicja jest niezmiernie trudna do realizacji w tzw. otwartych platformach mobilnych, w których użytkownicy wymieniają się aplikacjami, przesyłają pomiędzy sobą informacje korzystając jednocześnie z publicznych, otwartych sieci pakietowych. Poniżej przedstawiono kilka klas ataków, które są możliwe do realizacji, a które pozostają poza kontrolą właściciela telefonu komórkowego.

3.1. Atak od środka

Większość współcześnie stosowanych systemów mobilnych jest zbudowanych w oparciu o architekturę z jądrem systemu operacyjnego (Rys. 1). Ten element systemu mobilnego pośredniczy w komunikacji pomiędzy zasobami sprzętowymi takimi jak: procesor, pamięć operacyjna, urządzenia zewnętrzne (wyświetlacz, kamera, żyroskop, mikrofon itp.) oraz aplikacjami (zarówno tymi zainstalowanymi przez użytkownika jak i dostarczonymi razem z systemem operacyjnym). Jądro systemowe posiada pełny dostęp do segmentu kodu, danych oraz stosu każdej działającej w systemie operacyjnym aplikacji.



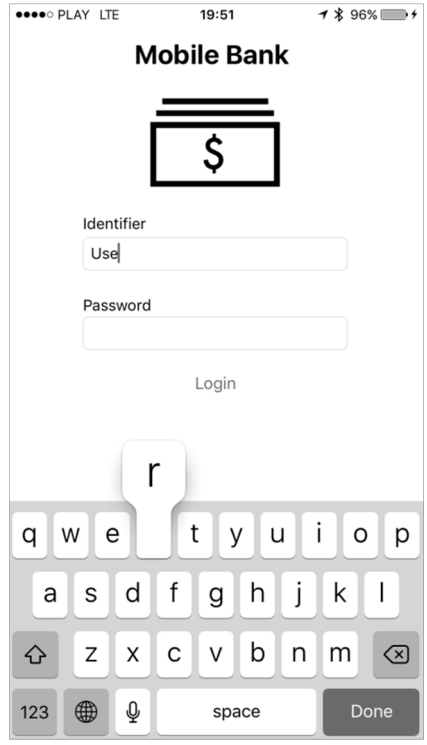
Rys. 1. Architektura systemu operacyjnego opartego na jądrze systemowym

Taka architektura systemu operacyjnego sprawia, że możliwe jest wykonanie tzw. „ataku od środka" (Man-Inside-Attack). Poniżej zaprezentowano przykładowy jego scenariusz.

Haker umieszcza w urządzeniu mobilnym „złośliwą" aplikację lub skrypt, którego zadaniem jest uzyskanie kontroli nad jądrem systemowym. Takie działanie może zostać wykonane, np. poprzez atak typu phishing lub poprzez backdoor. W momencie, gdy taka kontrola zostanie uzyskana, możliwe jest przeprowadzanie analizy przesyłanych danych pomiędzy jądrem a aplikacją mobilną. Przeprowadzenie tego ataku jest zadaniem, które wymaga od hakera znajomości struktury warstwy jądra systemu operacyjnego będącego celem ataku. Istnieją również inne sposoby ataków, które mogą być przeprowadzone w prostszy sposób.

3.2. Atak wykonany przez inną aplikację

We współczesnych systemach mobilnych podjęto próbę wzajemnej separacji uruchamianych aplikacji. Do tego celu wykorzystywane jest rozwiązanie typu „sandbox", w którym każdy program posiada swoje środowisko uruchomieniowe. Utrudnia to także zablokowanie systemu poprzez wykorzystanie wszystkich zasobów przez jedną wadliwie działającą aplikację. Celem twórców takiego rozwiązania było zablokowanie bezpośredniego dostępu do danych pomiędzy aplikacjami. Projektanci systemów operacyjnych nie wyeliminowali wszystkich metod nieautoryzowanego dostępu do zasobów współdzielonych przez poszczególne programy. Taki atak może być wykonany, np. poprzez nagrywanie ekranu urządzenia. W sklepach aplikacji mobilnych dostępne są aplikacje, które umożliwiają użytkownikowi rejestrację interakcji użytkownika z inną aplikacją. Aplikacje nagrywające posiadają swój interfejs użytkownika, który jest widoczny w trakcie ich działania. To powoduje, że użytkownik posiada nad taką aplikacją „kontrolę", ale nie może być w pełni pewny, czy ekran jego urządzenia nie jest szpiegowany.



Rys. 2. Ekran autoryzacji na stronie internetowej banku

Skoro jednak istnieje mechanizm dostępu jednej aplikacji do zasobów, które powinny być wyłącznie używane przez drugą aplikację, to możliwe jest stworzenie takiego rodzaju aplikacji o podobnym działaniu, która nie będzie prezentowała jakiegokolwiek interfejsu użytkownika oraz będzie nagrywała ekran w sposób niewidoczny. Złośliwa aplikacja może być uruchomiona w tle jako proces o nazwie, np. „Aktualizacja systemowa". W tej sytuacji użytkownik nie jest w stanie wykryć zagrożenia. Skutki takiego rodzaju ataku mogą być bardzo poważne, np. uzyskanie poufnych identyfikatorów dostępu użytkownika podczas jego logowania do bankowości elektronicznej. Klawiatura używana w urządzeniach mobilnych jest widoczna na ekranie, więc aplikacja nagrywająca ekran może w łatwy sposób śledzić sekwencję wybieranych w niej znaków (Rys. 2).

3.3. Atak z wykorzystaniem warstwy sprzętowej

Większość używanych systemów mobilnych zakłada, że najważniejszym atrybutem informacji jest jej dostępność. Użytkownicy wybierają telefony z coraz większymi zasobami pamięci, aby wszystkie istotne informacje były dostępne na każde żądanie. Potencjalny dostęp do takich informacji przez producentów urządzeń mobilnych staje się coraz większą przewagą konkurencyjną umożliwiającą lepszy dobór produktów pod upodobania klientów, skuteczne dostarczanie reklam pozycjonowanych prywatnymi danymi użytkownika. Nieautoryzowany dostęp do takich informacji może być realizowany przez nieudokumentowane funkcjonalności mobilnych systemów operacyjnych. Pośrednio mogą to zauważyć także dociekliwi użytkownicy korzystając z najbardziej popularnych wyszukiwarek, których wyniki są bardziej spersonalizowane w przypadku, gdy wyszukujący używa zarówno przeglądarki jak i systemu operacyjnego dostarczanego przez producenta usługi wyszukującej. W 2018 roku zostały opublikowane prace przedstawiające realne możliwości przeprowadzenia ataku z wykorzystaniem warstwy sprzętowej. Potencjalnie także producenci układów scalonych mogą mieć dostęp do danych przetwarzanych na urządzeniach mobilnych.

Atak określany terminem Meltdown polega na pokonaniu zabezpieczeń pomiędzy systemem operacyjnym a działającymi w nim aplikacjami. Dzięki temu program posiada możliwość uzyskania dostępu do pamięci procesora, a tym samym do danych zapisanych w innych programach oraz systemie operacyjnym. Tego typu podatność jest luką sprzętową, która dotyczy najbardziej popularnych procesorów z rodziny Intel, AMD oraz ARM, a zatem może być zrealizowana na każdym urządzeniu bez względu na system operacyjny. Producenci systemów operacyjnych przygotowali stosowne aktualizacje oprogramowania, które chronią przed tym zagrożeniem, lecz ich zainstalowanie ma zauważalny wpływ na wydajność działania systemu.

Spectre to kolejny rodzaj ataku wykorzystujący warstwę sprzętową, który wynikiem jest przełamanie zabezpieczeń pomiędzy środowiskami uruchomienio-

wymi aplikacji. Umożliwia on uruchomienie w systemie operacyjnym procesu posiadającego uprawnienia zwykłego użytkownika, który w sposób nieautoryzowany uzyskuje dostęp do segmentu kodu, danych lub stosu innych procesów działających w systemie. W tym ataku użyto powszechnie stosowanego w procesorach mechanizmu przewidującego instrukcje warunkowe oraz rozgałęzienia programów w celu przyśpieszenia realizacji kolejnych instrukcji. W przeciwieństwie do ataku Meltdown, Spectre jest nieusuwalny poprzez modyfikację oprogramowania systemowego. Jedynym rozwiązaniem jest wymiana procesora na nową generację, co w przypadku urządzenia mobilnego jest trudne lub nawet niemożliwe do realizacji, gdyż producenci nie oferują możliwości tego typu modyfikacji urządzeń mobilnych.

4. Urządzenie mobilne jako system zaufany

Zaliczenie urządzenia mobilnego do kategorii zaufanych systemów komputerowych wymagałoby spełnienia warunków podanych definicji systemu zaufanego. Przedstawione powyżej klasy ataków, które są reprezentatywne dla konkretnych luk bezpieczeństwa opisywanych w literaturze dowodzą, że współczesne systemy mobilne nie mogą być traktowane jako systemy zaufane.

Problematyka bezpieczeństwa informacji przetwarzanych przez urządzenia mobilne jest istotnym tematem badań zmierzających do stworzenia rozwiązań, które umożliwią zaklasyfikowanie urządzeń mobilnych do grupy systemów zaufanych.

Jednym z potencjalnych rozwiązań może być użycie zewnętrznej karty mikroprocesorowej (smart card), wyposażonej w pamięć do przechowywania danych oraz mikroprocesor kryptograficzny do ich przetwarzania. Karta za pośrednictwem zewnętrznego czytnika kart może być podłączona do urządzenia mobilnego za pomocą specjalnego złącza (USB) lub przy użyciu technologii bezprzewodowej (NFC). Na karcie może być przechowywany sekret np. klucz prywatny wykorzystany m.in. w procesie autoryzacji w systemie bankowym lub systemach opieki medycznej. Karty mikroprocesorowe wyposażone w koprocesor kryptograficzny wraz z chronioną przestrzenią pamięci uniemożliwiają bezpośredni dostęp do przechowywanego sekretu. Próba takiego dostępu wiązałaby się ze zniszczeniem struktury układu i nieodwracalną utratą sekretu. Możliwe jest natomiast wykonywanie operacji przez koprocesor kryptograficzny z użyciem sekretu i przesłanie wyników do urządzenia mobilnego. Standardowe czytniki danych nie są jednak wyposażone w klawiatury dedykowane niezbędne do wpisania kodu PIN niezbędnego do autoryzacji operacji wykonywanej przez kartę mikroprocesorową. Użycie klawiatury ekranowej z urządzenia mobilnego, czyni jednak rozwiązanie podatnym na atak polegający na przechwyceniu kodu PIN i wykonaniu operacji bez wiedzy właściciela karty, jeśli tylko karta z czytnikiem ma

zestawiony kanał komunikacyjny z urządzeniem mobilnym. Jest to modyfikacja powszechnie znanego ataku na bankomaty.

5. Podsumowanie

Zaprezentowana w artykule analiza bezpieczeństwa współczesnych aplikacji mobilnych pokazała, że istnieją podatności, które są bardzo trudne lub niemożliwe do wyeliminowania za pomocą elementów wbudowanych w telefon komórkowy zarówno w odniesieniu do dodatkowego sprzętu jak i oprogramowania (mechanizmów zaimplementowanych w mobilnym systemie operacyjnym). Zawarta w pracy definicja systemu zaufanego stawia wysokie wymagania, które potencjalnie mogłyby spełnić rozwiązania z niezależnym urządzeniem (komponentem sprzętowym) realizującym procesy autoryzacji i kodowania danych.

Bibliografia

1. Syed Farhan Alam Zaidi, Munam Ali Shah, Muhammad Kamran, Qaisar Javaid, Sijing Zhang „*A Survey on Security for Smartphone Device*", International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4 (2016).
2. Murat Yesilyurt, Yildiray Yalman, „*Security Threats on Mobile Devices and their Effects: Estimations for the Future",* International Journal of Security and Its Applications Vol. 10, No. 2 (2016).
3. N. Asokan, Jan-Erik Ekberg, Kari Kostiainen, Anand Rajan, Carlos Rozas, Ahmad-Reza Sadeghi, Steffen Schulz, and Christian Wachsmann, „*Mobile Trusted Computing*", Proceedings of the IEEE | Vol. 102, No. 8 (2014).
4. Jalaluddin Khan, Haider Abbas, Jalal Al-Muhtadi, „*Survey on Mobile User's Data Privacy Threats and Defense Mechanisms*", Procedia Computer Science 56 (2015).
5. H Wonjong Kim, Seungchul Kim, Younghwan Bae, Sungik Jun, Youngsoo Park, and Hanjin Cho, "*A Platform-Based SoC Design of a 32-Bit Smart Card*", ETRI Journal, Volume 25, Number 6 (2003).
6. M, Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh,, J. Horn, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, M.Hamburg: „*Meltdown: Reading Kernel Memory from User Space*" https://meltdownattack.com/
7. „Spectre and Meltdown processor flaws threaten billions of computers and mobile devices", Computer Fraud & Security Vol. 2018, Issue 1, Elsevier
8. G. Górski, „*Token programowy dla urządzeń mobilnych wspierający silne uwierzytelnianie użytkowników z wykorzystaniem infrastruktury klucza publicznego*", Przegląd Telekomunikacyjny 8-9/2013, str. 1231-1236, 2013

9. G. Górski, „*Algorytm weryfikacji haseł wykorzystujący badanie integralności danych*”, Przegląd Telekomunikacyjny 8-9/2012, str. 842-848, 2012
10. G. Gorski, „*System płatności mobilnych wykorzystujący biometryczną identyfikację użytkowników oraz infrastrukturę klucza publicznego*”, - Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne –No. 8-9/2015 – str, 1489-1495, 2015

Streszczenie

W artykule zostały opisane wybrane grupy zagrożeń (klasy ataków) dla współczesnych systemów mobilnych, które w większości mogą być wykonane bez wiedzy użytkownika. Poszczególne podatności sklasyfikowano w trzech grupach jako zagrożenia pochodzące od innych aplikacji działających na urządzeniu mobilnym, wynikające z niedoskonałości lub ukrytych funkcjonalności systemu operacyjnego oraz ataków z wykorzystaniem warstwy sprzętowej telefonu. Wprowadzono także definicję oraz wymagania jakie stawiane są dla systemu zaufanego. Obecny poziom zabezpieczeń w konfrontacji z zaprezentowanymi podatnościami uniemożliwia w obecnym stanie zaklasyfikowanie systemów mobilnych do grupy systemów zaufanych.

Abstract

The article describes selected groups of attacks for modern mobile systems which can mostly be executed without the user awareness. The particular vulnerabilities have been classified into 3 groups as threats from other applications executed in a mobile device resulting from defects or the other hidden functionalities present in the operating system and the attacks executed by using the hardware layer. A definition and requirements for a trusted system have been introduced. The current level of security in confrontation with the presented vulnerabilities does not allow in the current state to classify the mobile systems into the group of trusted systems.

Keywords: Trusted computer system, mobile devices, security analysis