OWASP

Bezpieczeństwo aplikacji mobilnych

OWASP

Warszawa, 27 września 2011

Aleksander Ludynia

Plan prezentacji

- Platformy mobilne
- Ataki na platformy mobilne
- Projekt OWASP Mobile Security Project
- Podejście do testów bezpieczeństwa aplikacji mobilnych
- Źródła wiedzy

Platformy mobilne
Obecna sytuacja i prognozy

- Rynek aplikacji mobilnych rozwija się w imponującym tempie – jego przewidywana wartość w tym roku to 15 miliardów dolarów (*Gartner*)
- Przewidywana liczba pobrań aplikacji mobilnych w 2015 roku wyniesie 182 miliardy
- Najpopularniejsze platformy mobilne i ich udział w rynku (*IDC*)

System operacyjny	Udział w rynku 2011	Udział w rynku 2015
Android	38,9 %	43,8 %
BlackBerry OS	14,2 %	13,4 %
Symbian	20,6 %	0,1 %
iOS	18,2 %	16,9 %
Windows Phone	3,8 %	20,3 %
Inne	4,3 %	5,5 %

- Czynniki wpływające na popularność poszczególnych platform:
  - Liczba urządzeń mobilnych wykorzystujących dany system
  - Dostępność środowisk developerskich (SDK)
  - Sposób udostępniania aplikacji

Ataki na platformy mobilne

- Wraz ze wzrostem popularności platform mobilnych rośnie liczba związanych z nimi zagrożeń – często związanych z działaniem złośliwego oprogramowania
- W 2011 roku znanych już jest ponad 1200 rodzajów złośliwego oprogramowania na środowiska mobilne (*McAfee*)
- Głównym celem ataków w 2011 roku był system Android – około 70% wszystkich nowych zagrożeń dotyczy właśnie tego systemu (*McAfee*)
- Przykłady działania złośliwego oprogramowania:
  - Wysyłanie wiadomości SMS na numery premium
  - Nawiązywanie połączeń z numerami premium
  - Przekazywanie otrzymanych wiadomości SMS
  - Wysyłanie złośliwych wiadomości SMS na numery z książki kontaktów
  - Przekierowanie przeglądarki internetowej do stron phishingowych
  - Kopiowanie danych użytkownika telefonu
  - Instalacja złośliwego oprogramowania

Projekt OWASP Mobile Security Project (1/3)
Lista głównych zagrożeń – Top 10

1. Niezabezpieczone lub niepotrzebnie przechowywane dane po stronie klienta
2. Słabości w ochronie transmisji
3. Wyciek osobistych danych
4. Słabości w ochronie zasobów z wykorzystaniem silnych mechanizmów uwierzytelniających
5. Słabości w implementacji polityki autoryzacji
6. Wstrzyknięcie po stronie klienta
7. Ataki odmowy usługi po stronie klienta
8. Złośliwy kod strony trzeciej
9. Przepełnienie bufora po stronie klienta
10. Słabości we wdrożeniu mechanizmów kontrolnych po stronie serwera

Projekt OWASP Mobile Security Project (2/3)
Lista dodatkowych zagrożeń

- Naruszenie zasobów generujących koszty po stronie klienta
- Słabości w zarządzaniu otrzymanymi wiadomościami SMS
- Słabości w zarządzaniu wysłanymi wiadomościami SMS
- Złośliwe/fałszywe aplikacje pochodzące z zaufanego źródła
- Możliwość dostępu do danych innej aplikacji
- Przełączenie sieci w trakcie transakcji
- Słabości w ochronie wrażliwych danych przechowywanych w urządzeniu
- Słabości związane z obsługą niebezpiecznych funkcjonalności platformy mobilnej

Projekt OWASP Mobile Security Project (3/3)
Zasady bezpiecznego tworzenia aplikacji mobilnych

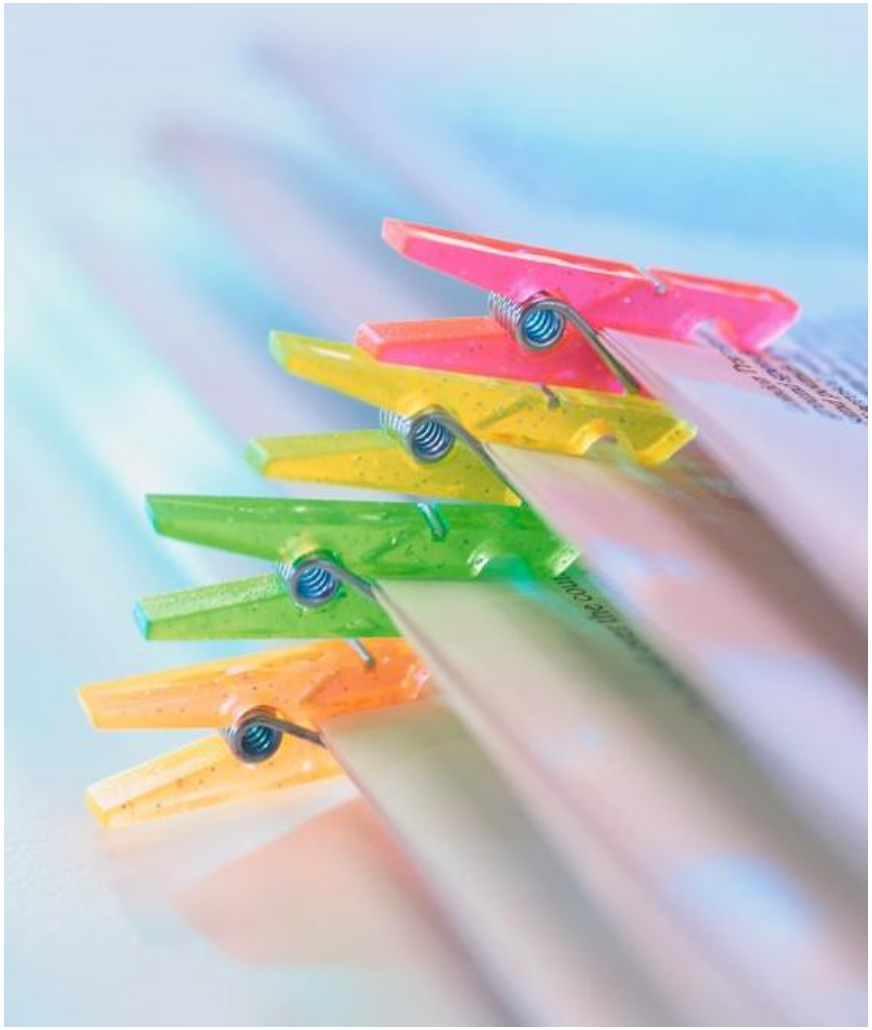
1. Identyfikacja i ochrona wrażliwych danych przechowywanych na urządzeniu mobilnym
2. Zapewnienie bezpieczeństwa danych uwierzytelniających w urządzeniu mobilnym
3. Zapewnienie bezpieczeństwa transmisji danych
4. Poprawne wdrożenie uwierzytelniania, autoryzacji oraz zarządzania sesją
5. Zapewnienie bezpieczeństwa udostępnianych usług oraz serwerów
6. Zapewnienie bezpieczeństwa danych wymienianych ze stronami trzecimi
7. Określenie zasad gromadzenia, przechowywania i przetwarzania danych użytkowników
8. Ochrona przed nieautoryzowanym dostępem do zasobów generujących koszty
9. Zapewnienie bezpieczeństwa procesu dystrybucji oprogramowania
10. Identyfikacja i weryfikacja błędów wynikających z interpretacji przez aplikację wprowadzonego kodu

Podejście do testów bezpieczeństwa aplikacji mobilnych

- Testy uruchomionej aplikacji
  - Urządzenie mobilne
  - Emulator + proxy
- Przegląd bezpieczeństwa usług udostępnianych po stronie serwera aplikacji
- Analiza kodu źródłowego aplikacji
  - Przegląd kodu dostarczonego przez developera
  - Dekompilacja aplikacji

Źródła wiedzy

- Projekt OWASP Mobile Security - https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
- Foundstone Mobile Applications Security Testing http://www.mcafee.com/in/resources/white-papers/foundstone/wp-mobile-app-security-testing.pdf
- US-CERT Cyber Threats to Mobile Devices http://www.us-cert.gov/reading_room/TIP10-105-01.pdf
- Mobile Application Security - McGraw-Hill Osborne Media - ISBN-10: 0071633561
- Portal Android Developers - http://developer.android.com/
- iOS Developer Library http://developer.apple.com/library/ios/navigation
- Windows Phone 7 Developer Guide http://msdn.microsoft.com/en-us/library/gg490765.aspx



Pytania?

Aleksander Ludynia
Konsultant, Ernst & Young
e-mail: aleksander.ludynia@pl.ey.com
Tel.: +48 12 424 3213
Fax: +48 22 557 7001