Bezpieczeństwo oprogramowania

Paweł Krawczyk
kravietz@aba.krakow.pl

Skutki

Skutki wykorzystania błędów w oprogramowaniu, mające wpływ na bezpieczeństwo całego systemu.

- Otrzymanie nadmiernych przywilejów
- Uzyskanie zastrzeżonej informacji
- Modyfikacja zastrzeżonej informacji
- Zablokowanie usługi (*denial of service*)

ABA

Przyczyny

- Zbytnie zaufanie do danych wejściowych
  SQL injection
- Zakładanie, że kod jest wykonywany w sposób niepodzielny
  race conditions
- Przyznawanie zbyt dużych praw
  katalogi a+w, *czytanie* /etc/shadow *przez serwer* XFree86
- Nieprzewidywanie sytuacji awaryjnych
- Niezrozumienie istoty problemu
  szyfrowanie haseł w aplikacji IBM
- Czas życia informacji
  odzyskiwanie poufnych informacji z pliku core

Przykład SQL injection

Dziura obecna w aplikacjach dostępnych przez WWW i korzystających z SQL–owych baz danych. Zakładana postać zapytania z formularza:

SELECT * FROM keywords WHERE keyword 'costam';

Zapytanie nie przewidziane przez autorów:

SELECT * FROM keywords WHERE keyword 'costam';
DROP TABLE keywords;';

Rezultat — skasowanie tabeli *keywords*.

Przykład szyfrowania haseł w IBM

Zapobieganie

- Na etapie projektowania — zasada maksymalnej nieufności do danych zewnętrznych
- Weryfikacja poprawności danych wejściowych oraz struktur wewnętrznych
- Określenie dopuszczalnych postaci danych wejściowych
- Unikanie błędnych założeń
- Sprawdzanie kodów powrotu i obsługa sytuacji awaryjnych
- Zasada najmniejszych przywilejów
- Bezpieczne wartości domyślne, wyłączanie niepotrzebnych usług
- Usuwanie poufnych danych po ich użyciu

ABA

Wykrywanie

- Weryfikacja projektu
- Weryfikacja implementacji — audyt kodu
- Testowanie w nieprzyjaznym środowisku

Wzór: metodologia pracy *NSA*.

Dodatkowe zabezpieczenia

Półśrodki, jednak pomagają zapobiegać nieznanym atakom.

- Perl tainting
- Blokada wykonywalnego stosu (*Linux, Solaris*)
  http://www.openwall.com/linux/, http://pageexec.virtualave.net/
- Sprawdzanie zakresów odwołań (*bounds checking*)
  StackGuard http://immunix.org/
- Przechwytywanie niebezpiecznych funkcji
  LibSafe http://www.bell-labs.com/org/11356/libsafe.html
- Narzędzia wspomagające audyt kodu
  ITS4, SLINT, LCLint

Atak na OpenPGP

- Umożliwia odzyskanie części klucza prywatnego, nawet zabezpieczonego hasłem (*passphrase*)
- Dotyczy wyłącznie części klucza służącej do podpisywania
- Polega na zmuszeniu aplikacji do prowadzenia obliczeń na zmodyfikowanym kluczu
- Wymaga dostępu do zaszyfrowanego klucza
- Ciekawy, ale o małym znaczeniu praktycznym

Atak na OpenPGP

1. Modyfikacja wybranych bajtów klucza prywatnego
   - publicznych parametrów w przypadku DSA
   - fragmentu zaszyfrowanego klucza RSA
2. Oczekiwanie na uruchomienie aplikacji przez użytkownika
3. Użytkownik generując podpis podaje hasło
4. Aplikacja rozszyfrowuje klucz prywatny
5. Aplikacja używa zmodyfikowanego klucza do wygenerowania podpisu
6. Przechwycony podpis służy do obliczenia wartości klucza

ABA

http://ipsec.pl/