Bezpieczeństwo komputerowe

Laboratorium - lista nr 10, 14 I

Zadanie 1 (10 pkt) Napisz aplikację (skrypt) przechwytującą nieszyfrowane sesje www (wykorzystaj np. Wireshark). Program ma (1) nasłuchiwać ruch sieciowy, (2) wynajdywać identyfikatory sesji (dla predefiniowanych stron), a następnie (po wybraniu) (3) zmieniać odpowiednie wpisy w ciasteczkach Twojej ulubionej przeglądarki tak, aby można było się podszyć pod podsłuchaną sesję.

Wykorzystaj np. programy tcpdump i aircrack (dla sieci zabezpieczonych WEP/WPA).

Zadanie 2 (5 pkt) Na przykładzie programu z zadania 6.1 pokaż jak można obejść uwierzytelnianie poprzez przepełnienie bufora.

W razie konieczności zmodyfikuj kod programu, aby to było możliwe.

Zadanie 3 (10 pkt) Zmodyfikuj binarkę programu z zadania 6.1 w ten sposób, aby nie trzeba było wpisywać hasła.

Zadanie 4 (10 pkt) Zmodyfikuj działanie programu z zadania 6.1 w ten sposób, aby hasło do klucza było przechowywane w "keystorze".

Zadanie 5 (20 pkt) Zmodyfikuj działanie programu z zadania 6.1 w ten sposób, aby nawet uprzywilejowany[1] atakujący nie mógł uzyskać dostępu do klucza wykorzystywanego do podpisywania.

Wykorzystaj technologię Intel SGX. Możesz skorzystać z symulatora OpenSGX (`https://github.com/sslab-gatech/opensgx`) bądź z SDK SGX (w trybie simulation mode: `https://github.com/surentharbe/Intel_SGX/tree/master/Simulation_Code`).

Zadanie 6 (10 pkt) Przygotuj politykę bezpieczeństwa dla (do wyboru): produktu, który realizujesz na programowaniu zespołowym (możecie przygotować wspólny dokument w dwie osoby); dla legitymacji studenckiej (pamiętać należy o warstwie wizualnej i elektronicznej).

[1] Rozwiązanie z zadania 4 nie chroni przed atakującym, który może "podejrzeć" pamięć procesu.