Kryptografia i bezpieczeństwo

Laboratorium - lista nr 10, do 22 I

Zadanie 1 (20 pkt) Zmodyfikuj bibliotekę OpenSSL w taki sposób, aby wartości losowe generowane w procesie uzgadniania kluczy były zależne od danych przesyłanych tekstem jawnym (w szczególności preMasterSecret zależne od ClientHello; dla uzgadniania klucza RSA).

Napisz program, który wykorzystuje wiedzę o zmodyfikowanym procesie uzgadniania kluczy do dekodowania połączeń https. Program może np. odczytywać pliki w jednym z formatów, w którym zapisuje dane Wireshark.

Zadanie 2 (20 pkt) Zaimplementuj timing attack na swoją implementację RSA z listy 8. Więcej szczegółów było przedstawionych na wykładzie 9 I 2017. Można też sięgnąć po: [BB05, Koc96]. Przydatną funkcją umożliwiającą dokładny pomiar liczby cykli jest *rdtsc*.

Literatura

[BB05] David Brumley and Dan Boneh. Remote timing attacks are practical. *Computer Networks*, 48(5):701–716, 2005.

[Koc96] Paul C. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. pages 104–113. Springer, Berlin, Heidelberg, 1996.