Kodowanie i bezpieczeństwo

Laboratorium - lista nr 8, 22 XII

Zadanie 1 (10 pkt) Zaimplementuj przedstawiony na wykładzie *timing attack* [1] na program z poprzedniej listy.

Aby zredukować poziom "szumu" możesz uruchamiać i mierzyć czas wykonania operacji lokalnie. Do dokładnego pomiaru czasu możesz wykorzystać funkcję rdtsc bądź rdtscp [2].

Zadanie 2 (10 pkt) (2 pkt) Zmodyfikuj działanie serwisu z listy 4. Wygeneruj dla serwera certyfikat SSL dla domeny: www.mojWspanialyBank.com (ale może to być adres, który był wykorzystywany na liście 3). (8 pkt) (TLS Client Authentication) Wygeneruj certyfikat użytkownika, który będzie można zainstalować w przeglądarce. Skonfiguruj serwer www w ten sposób, aby zezwalał na połączenie jedynie użytkownikom, którzy przedstawią odpowiedni certyfikat.

Literatura

[1] Paul C Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In *Annual International Cryptology Conference*, pages 104–113. Springer, 1996.

[2] Gabriel Paoloni. How to benchmark code execution times on intel® ia-32 and ia-64 instruction set architectures. `https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/ia-32-ia-64-benchmark-code-execution-paper.pdf`, 2010.