WYŻSZA SZKOŁA HANDLOWA W RADOMIU

RADOM ACADEMY OF ECONOMICS

Wyższa Szkoła Handlowa w Radomiu

Podstawy kryptografii
Laboratorium 1

Radom 2020/2021

1. Cel zadania

Podstawowym celem zadania jest przetestować podstawowe techniki szyfrowania powszechnie użytkowanych technologii.

2. Potrzebne narzędzia.

- Wireshark
- XAMPP
- OpenSSL
- poczta elektroniczna (można wykorzystać własny, lokalny serwer pocztowy, np. MercuryMail)
- klucze PGP (np. https://www.openpgp.org/, https://pgpkeygen.com)
- opcjonalnie prosta strona z formularzem (https://www.w3schools.com/php/php_forms.asp)
- opcjonalnie system Linux Kali lub blackarch (https://blackarch.org, https://www.kali.org)

3. Informacje wstępne

W obecnych czasach bezpieczeństwo danych w każdej instytucji musi stać na najwyższym poziomie. Szczególnie narażone są wiadomości przesyłane pocztą elektroniczną. W dobie rozporządzeń RODO należy dbać, by wiadomość mogli odebrać jedynie adresaci. Ponadto warto mieć na uwadze wszelkiego rodzaju formularze logować i/lub kontaktu na stronach WWW. Również tutaj istnieje bowiem ryzyko, że poufną treść przechwyci osoba niepożądana.

Rozwiązaniem opisanych problemów będzie zastosowanie odpowiednich kluczy szyfrujących. Klucze PGP są od dawna stosowanym elementem szyfrującym. Ze względu na używanie asymetrycznej architektury szyfrowania możemy część publiczną dostarczyć każdemu (np. wstawiając klucz na stronie WWW czy wysłać takowy nieszyfrowaną pocztą). Z drugiej strony posiadamy własny klucz prywatny, dzięki któremu możemy odszyfrować wiadomość.

Z kolei w przypadku stron WWW od dłuższego czasu firmy i organizacje zajmujące się tworzeniem przeglądarek oraz wyszukiwarek internetowych forsują używanie przez wszystkie witryny kluczy uwierzytelniających witryny. Dzięki takiemu podejściu mamy użytkownik końcowy otrzyma odpowiedni komunikat od strony WWW, że użyty klucz nie pasuje do wpisanego adresu (phishing). Po drugie, klucze SSL szyfrują przesyłane dane na linii klient-serwer. Dzięki temu dane przesyłane przez sieć nie będą widoczne dla osoby nasłuchującej sieć.

4. Przebieg.

Laboratorium najlepiej wykonywać w parach. W pierwszej kolejności należy uruchomić program Wireshark i sprawdzić nim ruch na sieci, w szczególności ruch generowany przez sprzęt drugiej osoby z grupy. Szczególnie należy zwrócić uwagę na działanie stron WWW, które nie posiadają klucza SSL. W tym celu można stworzyć prostą stronę HTML+PHP (odnośnik w sekcji 2), uruchomić serwerze stron WWW (np. na narzędziu XAMPP bądź na jakimkolwiek serwerze WWW) i spróbować kilkukrotnie wysłać informacje przez formularz.

Następnie należy wystawić certyfikat dla strony i ponownie spróbować przesłać dane. Czy Wireshark był w stanie odczytać wartości przed wystawieniem certyfikatu? Co stało się po uruchomieniu strony z certyfikatem.

W drugiej części ćwiczenia należy przetestować wysyłanie wiadomości elektronicznej. Czy Wireshark jest w stanie przechwycić wiadomości pocztowe?

Następnie należy stworzyć i zastosować klucz PGP. Ponownie sprawdzić, czy można przechwycić wiadomość LUB czy można taką pocztę otworzyć, jeżeli wyślemy ją do kogoś innego (np. przez pomyłkę).

5. Zakończenie

Z przebiegu laboratorium należy sporządzić sprawozdanie. Powinno ono zawierać informacje o wykorzystanych technologiach, ich możliwościach oraz łatwości/trudności zastosowania. Ponadto należy zrobić rozeznanie jakie są mocne i słabe strony zaproponowanych technologii. Wskazane jest sporządzenie zrzutów ekranowych dokumentujących przebieg ćwiczenia. Wzór sprawozdania dostępny jest w plikach do pobrania na stronie WWW.