Podpis cyfrowy i szyfrowanie z wykorzystaniem OpenSSL i GnuPG (GPG) (kod: LX-CRYPT)

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Opis i cel szkolenia

Certyfikaty trzeba wystawiać, odnawiać i sprawdzać, a pliki, kopie zapasowe i wiadomości – chronić i podpisywać. Na szkoleniu pracujemy z dwoma podstawowymi narzędziami do tych zadań: **OpenSSL** i **GnuPG (GPG)**. Zaczynamy od krótkiego wprowadzenia do kryptografii, a większość dnia spędzamy na ćwiczeniach: tworzymy klucze i certyfikaty, szyfrujemy i podpisujemy pliki, weryfikujemy podpisy i konfigurujemy bezpieczną pocztę.

Po tym dniu:

- zrozumiesz, czym różnią się szyfrowanie, skrót i podpis cyfrowy – i przed czym nie chronią,
- wygenerujesz klucz i żądanie certyfikatu (CSR), odczytasz certyfikat X.509 i przekonwertujesz go do potrzebnego formatu,
- sprawdzisz certyfikat serwera i rozpoznasz najczęstsze przyczyny błędów,
- zaszyfrujesz i podpiszesz plik w GPG oraz zweryfikujesz podpis pobranego oprogramowania,
- zadbasz o swoje klucze: kopia zapasowa, data ważności, unieważnienie, publikacja klucza publicznego,
- podpiszesz i zaszyfrujesz wiadomość e-mail w standardzie OpenPGP albo S/MIME.

Omawiamy też krótko kryptografię postkwantową: co się zmienia w OpenSSL i GnuPG i co warto zrobić już teraz. Asystentów AI używamy tam, gdzie realnie pomagają – przy objaśnianiu poleceń OpenSSL i komunikatów o błędach – zawsze ze sprawdzeniem wyniku.

Szkolenie przyda się administratorom systemów, inżynierom DevOps, programistom, specjalistom ds. bezpieczeństwa IT i wszystkim, którzy w pracy mają do czynienia z certyfikatami, kluczami albo poufną korespondencją.

Czas trwania

1 dzień

Program

1. Kryptografia w praktyce – najważniejsze pojęcia
   - kodowanie, szyfrowanie i funkcje skrótu – czym się różnią
   - szyfrowanie symetryczne i asymetryczne, klucz publiczny i prywatny
   - idea działania podpisu cyfrowego
   - granice użyteczności szyfrowania i podpisu cyfrowego
2. OpenSSL – klucze i skróty
   - generowanie kluczy, dobór algorytmu i długości klucza
   - obliczanie i sprawdzanie skrótów plików
   - praca z OpenSSL ze wsparciem AI: objaśnianie poleceń i komunikatów o błędach, weryfikacja wyniku
3. Certyfikaty X.509 i PKI
   - budowa certyfikatu, łańcuch zaufania, urzędy certyfikacji (CA)
   - żądanie certyfikatu (CSR) i nazwy alternatywne (SAN)
   - testowe CA i podpisywanie certyfikatów
   - formaty plików (PEM, DER, PKCS#12) i konwersje między nimi

   - sprawdzanie certyfikatu serwera TLS i najczęstsze błędy
   - klucze na kartach i tokenach sprzętowych (PKCS #11) – przegląd
4. GnuPG (GPG) – zarządzanie kluczami
   - tworzenie pary kluczy, podklucze, data ważności
   - eksport, import i kopia zapasowa kluczy
   - certyfikat unieważnienia i odwoływanie klucza
   - odcisk klucza, potwierdzanie tożsamości właściciela, sieć zaufania
   - publikowanie kluczy: serwery kluczy i inne metody
5. GnuPG (GPG) – szyfrowanie i podpis
   - szyfrowanie i odszyfrowywanie plików
   - podpis dołączony i odłączony, weryfikacja podpisu
   - sprawdzanie podpisów pobranego oprogramowania
   - aplikacje graficzne do zarządzania kluczami
6. Bezpieczna poczta elektroniczna
   - OpenPGP i S/MIME – różnice, kiedy który standard
   - podpisywanie i szyfrowanie wiadomości w Thunderbirdzie (wbudowana obsługa OpenPGP)
   - podpis i szyfrowanie wiadomości w Outlooku – omówienie możliwości
7. Kryptografia postkwantowa – co się zmienia
   - dlaczego dzisiejsze algorytmy asymetryczne będą wymagały następców
   - nowe algorytmy w OpenSSL i GnuPG – stan obecny
   - co warto zrobić już teraz

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Przeznaczenie i wymagania

Szkolenie jest przeznaczone przede wszystkim dla:

- administratorów systemów Linux i Windows, którzy obsługują certyfikaty i klucze,
- inżynierów DevOps i programistów, którzy konfigurują TLS albo podpisują pliki i wydania oprogramowania,
- specjalistów ds. bezpieczeństwa IT,
- osób, które chcą szyfrować i podpisywać pocztę oraz dokumenty i rozumieć, jak to działa.

Od uczestników oczekujemy:

- podstawowej umiejętności pracy w linii poleceń (Linux lub Windows) – większość ćwiczeń wykonujemy w terminalu,
- ogólnej orientacji w obsłudze klienta poczty elektronicznej (np. Outlook lub Thunderbird).

Wcześniejsza znajomość kryptografii nie jest potrzebna.

Certyfikaty

Uczestnicy szkolenia otrzymują imienne certyfikaty sygnowane przez ALX.

Lokalizacje

- Warszawa – ul. Jasna 14/16A
- Zdalnie – zajęcia realizowane poprzez platformę Zoom
- Kraków – ul. św. Filipa 23
- Warsaw (English) – Jasna 14/16A
- Online (English) – your home, office or wherever you want
- na życzenie dowolne miejsce w Polsce, lub UE (zajęcia prowadzone w języku angielskim)

Cena szkolenia

1190 PLN netto (VAT 23%)

W cenę szkoleń organizowanych w naszej siedzibie wliczone są:

— autorskie materiały szkoleniowe,
— indywidualne stanowisko komputerowe do pracy podczas zajęć,
— certyfikaty ukończenia szkolenia,
— drobny poczęstunek oraz ciepłe i zimne napoje,
— możliwość jednorazowego kontaktu z instruktorem (instruktorami) po szkoleniu i zadawania pytań dotyczących materiału szkolenia.

Cena szkolenia nie zawiera obiadów. Można je dokupić w cenie 35 zł netto za obiad.

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl