- czym jest certificate pinning? dlaczego się go stosuje?

Już od dawna standardem w komunikacji pomiędzy aplikacją a serwerem jest nie tylko stosowanie protokołu TLS, ale także tzw. przypinanie certyfikatów, czyli zaszycie w kodzie aplikacji informacji o tym, jakie certyfikaty TLS może akceptować. Pozwala na lepszą ochronę internautów przed atakami z wykorzystaniem podrobionych (ale poprawnie podpisanych) certyfikatów

- czym jest Extended validation dla certyfikatów SSL?

Extended Validation Certificates (EV SSL, ang. certyfikaty rozszerzonej walidacji) – specjalny typ certyfikatu X.509, który wymaga obszerniejszego postępowania z wnioskiem podmiotu przez Urząd certyfikacji przed wydaniem. Charakteryzuje się zielonym paskiem adresu WWW w przeglądarce, który w widoczny sposób pokazuje nazwę twojej firmy.

- kto da się nabrać na taki atak (kontekście zadania 3)?

Osoba, która nie sprawdza pasku adresu, nieznająca standardów, czyli zapewne większość zwykłych użytkowników internetu.

- czym są CRL, OCSP?

CRL (ang. Certificate Revocation List) - lista certyfikatów unieważnionych przez organ certyfikujący z różnych powodów. Publikowana jest przez wystawcę certyfikatów (CA). Zawiera numery seryjne certyfikatów, które zostały unieważnione np. na skutek ujawnienia klucza prywatnego.

OCSP (ang. Online Certificate Status Protocol) - standard opisujący protokół komunikacyjny pomiędzy systemem informatycznym odbiorcy usług certyfikacyjnych a serwerem usługowym. Protokół ten określa format i strukturę zapytania (żądania) o status certyfikatu oraz format i strukturę odpowiedzi (tokenu), która zawiera wynik weryfikacji w postaci statusu: „poprawny”, „unieważniony”, „nieznany”. Korzystanie z zaufanej usługi OCSP jest praktyczniejszą i bardziej „bezpieczną” formą weryfikacji ważności certyfikatu niż przeszukiwanie list unieważnionych certyfikatów (CRL).

- co się stanie, gdy ktoś pozna klucz tajny serwera www?

Może się podszywać pod domenę serwera i użytkownik nie będzie widział nic nie porządku. W takiej sytuacji należy jak najszybciej powiadomić swój urząd certyfikacji.

- co się stanie, gdy ktoś pozna klucz tajny CA, który podpisywał certyfikat serwera www?

Będzie mógł tworzyć nowe certyfikaty, które będą całkowicie poprawne, jednakże nie będą one stworzone przez CA.

- co się stanie, gdy pewne CA wydaje certyfikaty w oparciu o słabe funkcje haszujące np. MD5?

Obniży to bezpieczeństwo certyfikacji, w przypadku MD5, częstym problemem były kolizje kryptograficzne.

- czym są downgrade attacks na TLS?

Forma ataku na system komputerowy lub protokół komunikacyjny, w wyniku którego następuje rezygnacja z bezpiecznego, wysokiej jakości trybu pracy (jak np. szyfrowane połączenie) na rzecz starego trybu o niższym poziomie bezpieczeństwa (tekst jawny), który jest dostępny dla zapewnienia kompatybilności wstecznej ze starszymi systemami. Luka ta, znaleziona w OpenSSL, pozwala atakującemu na ustanowienie starszej wersji TLS pomiędzy klientem a serwerem

- czym jest HTTP Strict Transport Security (HSTS)?

Jest to standard wprowadzający możliwość określenia w nagłówku wpisu "Strict-Transport-Security", który następnie zinterpretowany przez przeglądarkę sprawi, że wszystkie żądania do danej domeny zostaną przekierowane na protokół HTTPS, a jeśli takiej możliwości nie będzie (brak obsługi HTTPs), to przeglądarka powinna wyświetlić błąd i zablokować takowe żądanie, informując użytkownika o błędzie i ewentualnej próbie wykonania ataku MITM.