# Bezpieczeństwo Komputerowe - zadania i zagadnienia

Paulina Jędrzejewska, Bartosz Drzazga, Mikołaj Pietrek

## Semestr zimowy 2018/2019

### Zagadnienia (oprac. Paulina Jędrzejewska)

- timing-attack
- certyfikat, generowanie certyfikatu
- certificate pinning
- SSL, extended validation
- CRL
- OCSP
- HTTP Strict Transport Security (HSTS)
- RSA
- DSA
- kryptogram AES
- klucze Diffie-Hellmana
- szyfrowanie symetryczne
- szyfrowanie blokowe
- szyfr strumieniowy (salsa20, sosemanuk)
- szyfr AES
- chosen-plaintext attack
- replay attack
- security through obsecurity (przez zaciemnianie)
- hashe, funkcje hashujące
- macra
- SQL injection, XSS i XSRF
- memory hard functions
- przepełnienie bufora
- DNS
- PKI
- response spoofing, blind spoofing
- TLS
- SSH
- 2FA

### Pytania z list laboratoryjnych (oprac. Bartek Drzazga)

**Zadanie 1.** Czym jest certificate pinning? dlaczego się go stosuje?

*Rozwiązanie.* HTTPS zapewnia poufność, integralność oraz autentyczność komunikacji. Ten ostatni cel jest realizowany dzięki standardowi X.509. X.509 definiuje infrastrukturę klucza publicznego, umożliwiając tym samym potwierdzenie, czy host, z którym próbujemy się połączyć, jest istotnie tym, za którego się podaje. Potwierdzenie autentyczności hosta odbywa się przy użyciu szeregu certyfikatów. Na samej górze mamy certyfikat główny (root certificate). Ten certyfikat należy do głównego urzędu certyfikującego (root CA) i jest samopodpisany (self-signed). Główne urzędy certyfikujące mogą uprawniać inne podmioty do działania w ich imieniu poprzez wygenerowanie im certyfikatów pośrednich (intermediate certificate). Gdzie tkwi problem w tym modelu? Mianowicie główne oraz pośrednie centra certyfikacji nie mają wyszczególnionych konkretnych domen, do których mogą wystawiać certyfikaty.

Oznacza to, że każdy z tych podmiotów może wystawić zaufany certyfikat dla dowolnej domeny. Aby rozwiązać opisany powyżej problem, w przeglądarkach Chrome oraz Firefox zaczęto stosować przypinanie certyfikatów (certificate pinning). Ten mechanizm pozwala określić, które urzędy certyfikacji są uprawnione do wystawienia certyfikatu dla danej domeny. Na przykład Google może zdefiniować, że wszystkie certyfikaty dla ich domen muszą zostać podpisane przez urząd certyfikacji Google Internet Authority G2. Gdy ten warunek nie zostanie spełniony, przeglądarka wyświetli ostrzeżenie.

**Zadanie 2.** Czym jest Extended validation dla certyfikatów SSL?

*Rozwiązanie.* An Extended Validation SSL Certificate (also known as EV SSL for short) is the highest form of SSL Certificate on the market. During verification of an EV SSL Certificate, the owner of the website passes a thorough and globally standardized identity verification process (a set of vetting principles and policies ratified by the CA/Browser forum) to prove exclusive rights to use a domain, confirm its legal, operational and physical existence, and prove the entity has authorized the issuance of the certificate. This verified identity information is included within the certificate, with some pieces, including business name and country, presented directly in the browser window.

EV SSL to specjalny certyfikat, jak się wejdzie np. na https://www.google.com/ to przed adresem będzie wyświetlona tylko kłódka, ale jak się wejdzie np. na https://www.globalsign.com to obok kłódki widać dodatkowe informacje o właścicielu domeny (tutaj: "GMO GlobalSign, Inc. [US]") takie jak nazwa firmy i kraj. W szczegółach certyfikatu można zobaczyć że to rzeczywiście EV (swoją drogą w tym przypadku wystawiony przez tą samą firmę xD) Inne przykłady stron z EV to np. strony antyvirusów czy inne od bezpieczeństwa w necie: Symantec, Avast, Comodo...

**Zadanie 3.** Kto da się nabrać na taki atak (w kontekście zadania 3)?

*Rozwiązanie.* To zależy od tego jak dobrze przeprowadzony jest atak. Pewnie na bardziej wyrafinowane ataki dałby się nabrać nawet ktoś bardzo świadomy w kwestii bezpieczeństwa w internecie. Wymienię czynności które zmniejszają szansę na zostanie ofiarą takiego ataku tzn osoby które tak nie robią będą łatwiejszą ofiarą ataku)

1. korzystanie z antywirusa lub podobnego programu/rozszerzenie przeglądarki
2. nieotwieranie podejrzanych maili (np takich które nas nie interesują/nie spodziewaliśmy się ich otrzymać)
3. sprawdzenie adresu nadawcy przy otwieraniu wiadomości której się spodziewaliśmy
4. nie klikanie w linkii, np ręcznie wpisywać adres banku
5. sprawdzanie w internecie stron/serwisów w których zakładamy konto i podajemy wrażliwe dane np sprawdzać opinie o sklepie zanim się zarejestrujemy
6. przy każdym logowaniu sprawdzać czy w adresie jest „https” oraz ikona kłódki przed nim

TL;DR na taki atak da się nabrać przede wszystkim człowiek który klika co popadnie i przy tym nie czyta co klika oraz podaje swoje dane wszędzie tam gdzie jest o to proszony.

**Zadanie 4.** Czym są CRL, OCSP?

*Rozwiązanie.* Lista unieważnionych certyfikatów (lista CRL, ang. Certificate Revocation List) – lista certyfikatów unieważnionych przez organ certyfikujący z różnych powodów.

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”. Wydanie zaświadczenia ze statusem „poprawny”

oznacza, że certyfikat jest wystawiony przez jeden z podmiotów, których certyfikaty objęte są usługą OCSP oraz że podmiot ten na moment udzielania odpowiedzi skutecznie nie unieważnił sprawdzanego certyfikatu.

Korzystanie z zaufanej usługi OCSP jest praktyczniejszą i bardziej „bezpieczną" formą weryfikacji ważności certyfikatu niż przeszukiwanie list unieważnionych certyfikatów (CRL).

**Zadanie 5.** Co się stanie, gdy ktoś pozna klucz tajny serwera www?

*Rozwiązanie.* If the private key for the digital certificates has been exposed, it means an attacker could perform a man-in-the-middle attack and read the traffic.

Leaked secret keys allows the attacker to decrypt any past and future traffic to the protected services and to impersonate the service at will.

Klucze takie niezbędne są do utworzenia szyfrowanego połączenia, a poznanie ich umożliwia rozszyfrowanie całej komunikacji. Narażone także są dane dostępowe użytkowników oraz inne dane znajdujące się po stronie serwera. Atakujący ma możliwość podsłuchiwania komunikacji, podszywania się pod usługi i użytkowników oraz kradzieży danych.

**Zadanie 6.** Co się stanie, gdy ktoś pozna klucz tajny CA, który podpisywał certyfikat serwera www?

*Rozwiązanie.* Będzie można wygenerować fejkowy certyfikat i móc podszywać się pod ten konkretny serwer www. Następne pytanie jest podobne. Różnica jest taka, że w tym chodzi ściśle o serwisy WWW.

**Zadanie 7.** Co się stanie, gdy ktoś pozna klucz tajny jakiegoś CA?

*Rozwiązanie.* Actually, if you had a CA's private key, you could make real, but illegitimate, certificates. There would be nothing fake about them, except that they wouldn't be made by the CA.

Podobnie jak w zadaniu poprzednim, lecz tym razem chodzi o wszystkie scenariusze gdzie używane są certyfikaty, np. WiFi zabezpieczone przez WPA2-Enterprise czy przy ściąganiu aktualizacji dystrybucji Linuksa z mirrorów/repozytoriów.

**Zadanie 8.** Co się stanie, gdy pewne CA wydaje certyfikaty w oparciu o słabe funkcje haszujące np. MD5?

*Rozwiązanie.* Z powodu znanych ataków kryptoanalitycznych funkcja MD5 zdecydowanie nie powinna być używana w zastosowaniach wymagających odporności na kolizje, na przykład w podpisie cyfrowym.

Some CAs used the MD5 algorithm to compute the digital signatures for certificates. MD5 has been known for some time to be weak against collision attacks, but running a CA is a pretty complex operation, so the entities behind them are slow to change.

Researchers attacked the MD5 algorithm using 200 PlayStation 3 systems and were able to construct a bogus Certificate Authority that looks like a known trusted CA. What this means is that these guys could generate a certificate for www.amazon.com which, when presented to your browser, would be accepted as the real thing. The digital signature on the fake certificate is listed as coming from a supposedly reputable CA, so your browser happily accepts it, reassuringly showing you the little padlock icon.

TL;DR: Z powodu kolizji fejkowy certifikat może być uznany za prawdziwy.

**Zadanie 9.** Czym są downgrade attacks na TLS?

*Rozwiązanie.* Atak typu downgrade (aktualizacja wsteczna) – 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. Jest to jeden z najpowszechniejszych ataków typu downgrade.

All modern browsers support SSLv3 up to TLSv1.2, but will use the highest version supported by a server. A middleman cannot directly modify any packets sent in the handshake, but a middleman can intercept and drop certain packets. By tricking the browser into thinking that the server does not support a given version of SSL/TLS, an attacker can downgrade the negotiated version. Let's see how this is done.

Protocol downgrade attacks rely on the assumption that an error or termination of the connection means the connection failed due to a SSL/TLS failure. Additionally, in order to be compatible with previous versions of SSL/TLS, a client may attempt multiple connections until a successful connection is made. Therefore, by repeating the protocol downgrade, a middleman can convince the client to negotiate SSLv3 with the server.

**Zadanie 10.** Czym jest HTTP Strict Transport Security (HSTS)?

*Rozwiązanie.* HTTP Strict Transport Security (HSTS) – mechanizm bezpieczeństwa sieci, który chroni strony przed atakami takimi, jak wymuszone zmniejszenie poziomu protokołu oraz przechwytywanie sesji. Dzięki niemu do serwerów można połączyć się tylko za pomocą przeglądarek, korzystających z bezpiecznych połączeń HTTPS, natomiast nigdy nie dopuszcza on połączeń na bazie niezabezpieczonego protokołu HTTP. O stosowaniu polityki HSTS serwer informuje użytkownika za pomocą pola znajdującego się w nagłówku odpowiedzi HTTP o nazwie „Strict-Transport-Security". Polityka HSTS określa czas, w którym użytkownik może być połączony z serwerem tylko poprzez bezpieczne połączenie.

Działa on tak, że jeżeli przeglądarka zobaczy, że witryna wysyła ten nagłówek, to przez czas określony w nagłówku cała komunikacja będzie się odbywać po HTTPS. Jest to działanie na poziomie przeglądarki, więc jeżeli użytkownik z niewiedzy lub przez roztargnienie będzie próbował połączyć się z wersją HTTP, to przeglądarka automatycznie podmieni jego zapytanie na HTTPS oraz zmieni wszystkie występujące na stronie linki na HTTPS.