Wojciech Ciemski

CYBERSECURITY

w pytaniach i odpowiedziach

Helion

Redaktor prowadzący: Szymon Szwajger

Projekt okładki: Studio Gravite / Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki
Grafika na okładce została wykorzystana za zgodą Shutterstock.com.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *https://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://helion.pl/user/opinie/cybwpy
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-283-9924-2

Printed in Poland.

Spis treści

Kryptografia

Jakie informacje znajdują się w certyfikacie SSL?

Certyfikat SSL jest małym plikiem danych, który cyfrowo wiąże klucz kryptograficzny i służy do poświadczenia wiarygodności domeny oraz jej właściciela. Umożliwia dzięki temu ustanowienie bezpiecznego połączenia między przeglądarką a serwerem internetowym.

Certyfikat **SSL** zawiera dane strony, dla której został wydany:

- nazwa domeny,
- okres ważności certyfikatu,
- szczegóły dotyczące urzędu certyfikacji (CA),
- klucz publiczny i wersja SSL/TLS,
- algorytm klucza publicznego,
- algorytm podpisu certyfikatu.

MD5 czy SHA-256 — co jest lepsze i dlaczego?

SHA-2 (ang. *Secure Hash Algorithm*) — zestaw kryptograficznych funkcji skrótu (SHA-224, SHA-256, SHA-384, SHA-512), zaprojektowany przez National Security Agency (NSA) i opublikowany w 2001 roku przez National Institute of Standards and Technology (NIST) jako federalny standard przetwarzania informacji rządu Stanów Zjednoczonych. SHA-1, SHA-256, SHA-384 i SHA-512 to iteracyjne, jednokierunkowe funkcje skrótu, które mogą przetwarzać komunikat o maksymalnej długości od 2^{64} do 2^{128} bitów w celu uzyskania od 160- do 512-bitowej skróconej reprezentacji, zwanej skrótem wiadomości.

MD5 (ang. *Message Digest*) to wszechobecny algorytm haszujący, który został opracowany przez Rona Rivesta i jest obecnie wykorzystywany w wielu aplikacjach internetowych. Algorytm MD5 przyjmuje na wejściu komunikat o dowolnej długości i generuje jako wyjście

128-bitowy „odcisk palca" lub „skrót wiadomości" komunikatu wejściowego. Skrót MD5 jest zwykle wyrażany jako 32-cyfrowa liczba szesnastkowa i uważa się, że jest uszkodzony kryptograficznie i może mieć kolizje. Przez kolizję rozumiemy fakt, że różne komunikaty wejściowe mogą mieć taką samą funkcję skrótu.

Podobnie jak MD5, SHA jest również szeroko stosowany w aplikacjach, takich jak SSH, SSL, S-MIME (ang. *Secure/Multipurpose Mail Extension*) i IPsec.

Algorytm SHA jest nieco wolniejszy niż MD5, ale większa długość skrótu sprawia, że jest on bardziej zabezpieczony przed atakami inwersyjnymi i kolizją siłową.

Jakie znasz metody szyfrowania?

Wyróżnia się dwie metody szyfrowania danych: symetryczną oraz asymetryczną.

Szyfrowanie symetryczne — szyfrowanie, w którym klucz szyfrowania danych jest taki sam jak klucz do ich deszyfrowania. Odbiorca i nadawca muszą przed przekazaniem poufnych zaszyfrowanych informacji ustalić, jak będzie wyglądać tajny klucz oraz jakim bezpiecznym kanałem go sobie dostarczą. Metodą symetryczną szyfrowania jest m.in. kod Cezara, AES, One-Time i 3DES.

Szyfrowanie asymetryczne — szyfrowanie z użyciem klucza jawnego/publicznego i prywatnego. Klucz do szyfrowania jest inny od klucza do deszyfrowania. Klucz publiczny jest powszechnie znany. Każdy jego posiadacz może za jego pomocą zaszyfrować dowolne dane. Natomiast jedynie posiadacz klucza prywatnego może odszyfrować otrzymane szyfrogramy. Analogicznie: posiadacz klucza prywatnego może używać go do szyfrowania danych, pozwalając w ten sposób każdemu posiadaczowi odpowiadającego mu klucza publicznego odszyfrować je. Metodą asymetryczną szyfrowania jest m.in. RSA.

Kiedy mamy do czynienia z kolizją w kontekście kryptografii?

Ze względu na to, że liczba wyników funkcji skrótu jest skończona, może się okazać, że dla dwóch zupełnie różnych wartości wejściowych otrzymamy taką samą wartość skrótu. Taką sytuację nazywamy **kolizją**.

Kiedy stosuje się szyfr blokowy, a kiedy szyfr strumieniowy?

Szyfr blokowy i **szyfr strumieniowy** to metody używane do konwersji zwykłego tekstu bezpośrednio na tekst szyfru. Należą do rodziny symetrycznych szyfrów kluczy.

Główna różnica między szyfrem blokowym a szyfrem strumieniowym polega na tym, że ten pierwszy szyfruje i odszyfrowuje blok tekstu naraz. Z kolei szyfr strumieniowy szyfruje i odszyfrowuje tekst, przyjmując jeden bajt tekstu naraz.

Jakiej minimalnej długości powinno być hasło użytkownika?

Hasła powinny się składać z co najmniej ośmiu znaków oraz być złożone z małych i wielkich liter, cyfr lub znaków specjalnych. Należy oczywiście pamiętać, że jest to minimalna polityka haseł. Im dłuższe hasło, tym lepsze. Warto też zwrócić uwagę na czas, po jakim należy zmieniać hasła. Obecnie trendem jest ustanawianie dłuższych haseł (przynajmniej dwunastoznakowych) i okresu zmiany przynajmniej raz na 3 – 6 miesięcy.

Jaka jest różnica pomiędzy haszowaniem a szyfrowaniem?

Haszowanie to wyliczanie przy użyciu funkcji skrótu (algorytmu takiego jak na przykład MD5 czy SHA) unikalnego ciągu znaków o stałej długości dla dowolnego tekstu. Istotną cechą haszowania jest fakt, że jest to proces nieodwracalny.

Szyfrowanie to proces zamiany tekstu jawnego, zrozumiałego dla człowieka (ang. *cleartext*, *plaintext*), w szyfrogram (ang. *cryptogram*, *ciphertext*), czyli postać otrzymaną za pomocą serii przekształceń i podstawień, której nie da się odczytać ani odszyfrować bez znajomości klucza szyfrującego.

Po co stosujemy funkcje skrótu?

Funkcja skrótu (funkcja mieszająca lub funkcja haszująca) to funkcja przyporządkowująca dowolnie dużej liczbie krótką wartość o stałym rozmiarze, tzw. skrót nieodwracalny.

W informatyce funkcje skrótu pozwalają na ustalenie krótkich i łatwych do weryfikacji sygnatur dla dowolnie dużych zbiorów danych. Sygnatury mogą chronić przed przypadkowymi lub celowo wprowadzonymi modyfikacjami danych (sumy kontrolne), a także mają zastosowanie przy optymalizacji dostępu do struktur danych w programach komputerowych (tablice mieszające).

Co zapewnia kod HMAC?

HMAC (ang. *Keyed-Hash Message Authentication Code*, *Hash-based Message Authentication Code*) — kod **MAC** z wmieszanym kluczem tajnym, zapewniający zarówno ochronę integralności, jak i autentyczności danych.

Czy jest jakaś różnica pomiędzy SSL a TLS?

Najważniejszą różnicą pomiędzy SSL a TLS jest to, że **TLS** jest bezpieczniejszy. Wynika to z faktu, że TLS jest po prostu wyższą wersją **SSL**, z której to TLS wyewoluował. W istocie TLS 1.0 to SSL 3.1.

Zmiana nazewnictwa wynika z tego, że za stworzeniem SSL w 1994 roku stoi Netscape, który nie miał wkładu w wersję TLS z 1999 roku. Autorzy chcieli więc odciąć się od skojarzeń z Netscape.

Obecnie zamawiając czy instalując certyfikat SSL, tak naprawdę mamy do czynienia z certyfikatem TLS. Nazwa „certyfikaty SSL" pozostała w użyciu, ponieważ była już rozpowszechniona i szeroko stosowana.

Jaka jest przewaga kryptografii krzywych eliptycznych nad RSA?

Kryptografia krzywych eliptycznych (ang. *Elliptic Curve Cryptography*, ECC) wykorzystuje matematyczne właściwości krzywych eliptycznych do tworzenia systemów kryptograficznych z kluczem publicznym. Mniejsze rozmiary kluczy ECDSA (ang. *Elliptic Curve Digital Signature Algorithm*) oznaczają, że można osiągnąć silniejsze szyfrowanie przy mniejszej mocy obliczeniowej i przepustowości sieci niż w przypadku RSA. Jest to szczególnie korzystne w kontekście urządzeń mobilnych i internetu rzeczy (IoT) o niskiej mocy, które stają się coraz bardziej wszechobecne.

Do czego można użyć klucza publicznego?

Klucz publiczny używany w szyfrowaniu asymetrycznym (z użyciem pary kluczy publicznego i prywatnego) służy do szyfrowania informacji. Klucz publiczny jest powszechnie dostępny, jednak zaszyfrowane nim informacje może odczytać jedynie posiadacz **klucza prywatnego**. Możemy go wykorzystać do bezpiecznej komunikacji i do bezpiecznego połączenia z serwerem, na przykład przy użyciu SSH.

Jak zdefiniować salting i do czego jest on używany?

Salting to proces dodawania unikalnych losowych ciągów znaków do haseł w bazie danych lub każdego hasła przed zaszyfrowaniem hasła. Ma to na celu zmianę skrótu i zwiększenie bezpieczeństwa haseł. Ciąg znaków dodawany do hasła nazywa się solą. Sól można dodać przed lub za hasłem.

Sól nie jest upubliczniana i jest znana tylko lokalnie.

Do czego służą sól i pieprz w kontekście haszowania haseł?

Sól (ang. *salt*) — dane losowe dodawane do hasła podczas obliczania funkcji skrótu przechowywanej w systemach informatycznych. Celem soli jest ochrona systemowej bazy haseł przed atakami słownikowymi. Jako że sól jest przechowywana jawnie, nie ma ona znaczenia w przypadku ataków brute force.

Pieprz (ang. *pepper*) to statyczna, tajna wartość przechowywana oddzielnie od bazy danych (zawierającej hasze). Zwykle kodowana na twardo w kodzie źródłowym aplikacji. Chroni hasła przed atakami typu brute force.

Co oznacza utajnianie z wyprzedzeniem?

Utajnianie z wyprzedzeniem (ang. *Perfect Forward Secrecy*, PFS; zwane także *forward secrecy*, FS) odnosi się do systemu szyfrowania, który często i automatycznie zmienia klucze używane do szyfrowania oraz deszyfrowania informacji. Ten ciągły proces zapewnia, że nawet jeśli najnowszy klucz zostanie skompromitowany, ujawniona zostanie jedynie minimalna ilość poufnych danych.

Czym różni się zaufany certyfikat SSL od niezaufanego? Po co nam zaufane główne urzędy certyfikacji?

Podstawowe różnice między tymi certyfikatami to:

- **weryfikacja praw własności domeny** — ma ona miejsce dla certyfikatów komercyjnych, co zwiększa bezpieczeństwo usługi;
- **gwarancja** — jest to kwota pieniężna, jaką wypłaca jednostka certyfikująca w sytuacji, kiedy dojdzie do złamania klucza certyfikatu;
- **dodatkowa weryfikacja** — w przypadku certyfikatów OV i EV ma miejsce dodatkowa weryfikacja w postaci przesłania odpowiednich dokumentów do jednostki certyfikującej przed wystawieniem SSL, co zwiększa wiarygodność;
- **cena**;
- **czas** — certyfikaty komercyjne wystawiane są najczęściej na rok, po tym okresie należy ponownie aktywować usługę.

Urząd certyfikacji (ang. *Certificate Authority*, CA) — podmiot, który wystawia certyfikaty cyfrowe. Certyfikat potwierdza własność klucza publicznego poprzez wskazanie podmiotu certyfikatu. Pozwala to innym powołującym się stronom polegać na podpisach lub zapewnieniach złożonych przez klucz prywatny odpowiadający kluczowi publicznemu. W tym modelu relacji zaufania CA jest zaufaną stroną trzecią.


PROGRAM
PARTNERSKI
GRUPY HELION
1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ
Zmień swoją stronę WWW w działający bankomat!
Dowiedz się więcej i dołącz już dzisiaj!
http://program-partnerski.helion.pl
GRUPA
Helion

CYBERSECURITY
w pytaniach i odpowiedziach

Co o cyberbezpieczeństwie każdy wiedzieć powinien

W świecie, w którym większość naszych mniej lub bardziej wrażliwych danych przechowywana jest w sieci, cyberbezpieczeństwo powinno być tematem numer jeden. Niestety, na ogół nie jest, bo... Po prostu nie chce się nam myśleć o zastosowaniu odpowiednich zabezpieczeń. Stają się one dla nas kluczowe dopiero, kiedy ktoś się cyberwłamie i realnie skradnie coś, co było dla nas istotne: hasło do poczty e-mail, pieniądze z konta w banku, zdjęcia, które wolelibyśmy zachować dla siebie, itd. Tyle że wtedy jest już za późno.

Ta książka powstała po to, by jej czytelnik zdążył wyprzedzić zagrożenie. Stanowi wprowadzenie do zagadnienia cyberbezpieczeństwa. Podzielona na kilka kluczowych części (systemy operacyjne, sieci komputerowe, aplikacje webowe, kryptografia, wreszcie cyberbezpieczeństwo jako takie), pozwala zapoznać się z najważniejszymi zagrożeniami i ze sposobami zabezpieczeń. Przybliża terminologię związaną z tematem i stanowi świetny punkt wyjścia do dalszego zgłębiania jego wybranych aspektów.

Cyberniebezpieczeństwo czyha.
Czy jesteś na nie przygotowany?

Helion

helion.pl

HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej! ▶

ISBN 978-83-283-9924-2

9 788328 399242

Cena: 39,90 zł