8. Identyfikacja - uwierzytelnianie strony

Uwierzytelnienie strony (ang. entity authentication) nazywa się też identyfikacją (ang. identification).

8.1 Metoda haseł

Strona pragnąca uzyskać dostęp do zasobów systemu ang. prover podaje systemowi weryfikującemu ang. verifier parę: (nazwa użytkownika, hasło).

Metoda haseł nie należy do najbezpieczniejszych ale stanowi prawie zawsze pierwszą linię obrony systemu. Wszystkie systemy operacyjne wykorzystują tę metodę.

Hasło jest to ciąg znaków wprowadzany przez użytkownika i sprawdzany przez system weryfikujący. Jeśli hasło podane przez użytkownika jest identyczne z pamiętanym przez komputer hasłem, które zostało przypisane temu użytkownikowi, to zostaje on uwierzytelniony uzyskując dostęp do zasobów systemu.

Hasło nigdy nie jest pamiętane w systemie weryfikującym postaci jawnej. Z reguły pamiętana jest odpowiednia tablica wartości funkcji skrótu dla haseł używanych w systemie. Praktycznie nie można z niej odtworzyć haseł.

Metoda haseł jest nazywana również słabym uwierzytelnianiem (ang. weak authentication)

8.2 Metoda pytanie-odpowiedź (metoda chalenge-reponse)

Metoda pytanie-odpowiedź to inaczej metoda chalenge–response. Zakładamy, że prover posiada specjalne urządzenie zwane tokenem, które potrafi generować odpowiedź na przesłane pytanie. Pytanie jest wygenerowaną przez verifier'a liczbą losową. Zadaniem provera jest podanie prawidłowej odpowiedzi na pytanie. Z reguły verifierowi dla akceptacji provera wystarczy jedna prawidłowa odpowiedź ale procedurę pytanie-odpowiedź można powtarzać wielokrotnie uzyskując większe prawdopodobieństwo poprawnej identyfikacji.

8.3. Protokoły uwierzytelniania z wiedzą zerową

Protokoły uwierzytelniania z wiedzą zerową (ang. ZK protocols) wykorzystują koncepcję tzw. dowodów z wiedzą zerową.

Najprostszym przykładem dowodu z wiedzą zerową jest tzw. „jaskinia wiedzy zerowej". W tym bardzo prostym modelu prover dowodzi tego, że posiada klucz do wewnętrznych drzwi jaskini odpowiadając na ciąg pytań verifiera.

Protokół identyfikacji (uwierzytelniania strony) Fiata – Shamira.

Protokół identyfikacji (uwierzytelniania strony) Fiata – Shamira jest klasycznym protokołem wykorzystującym koncepcję dowodu z wiedzą zerową.

Wprowadzimy następujące oznaczenia:

Strona A jest „proverem", dowodzi swojej tożsamości.

Strona B jest „verifierem", sprawdza tożsamość strony A.

Zaufana trzecia strona T wybiera dużą liczbę bezkwadratową $n = pq$ (p i q są dużymi różnymi liczbami pierwszymi) i ogłasza publicznie n utrzymując w tajemnicy p i q.

Każdy z prover'ów wybiera swoją liczbę $s \in <1, n-1>$ względnie pierwszą z n i ogłasza $v = s^2 \pmod n$ jako swój klucz publiczny.

Protokół ma $t \in N$ wykonań. W każdym wykonaniu mamy 3 następujące przebiegi (3 przesłania).

1. Prover A losuje liczbę $r \in Z_n$, $r \neq 0,1$ i przesyła $x = r^2 \pmod n$ do B.

2 Verifier B wybiera losowo $e \in \{0,1\}$ tak, by prawdopodobieństwo wyboru 0 było równe ½ i 1 też ½ i przesyła e do A.

3. Prover A oblicza $y = rs^e \pmod n$ i wysyła y do B.

Teraz B podejmuje decyzję oblicza wstępnie kwadrat $y^2 \pmod n$.
Jeśli verifier B wysłał do A w drugi kroku $e = 0$, to powinno być $y^2 = r^2 = x$.
Jeśli $y^2 = x$, to jest tak jak powinno być.
Jeśli $y^2 \neq x$, to „prover" jest oszustem.

Jeśli verifier B wysłał do A w drugi kroku $e = 1$, to powinno być $y^2 = r^2 \cdot s^2 (\mathrm{mod}\, n) = x \cdot v (\mathrm{mod}\, n)$. B oblicza iloczyn $x \cdot v (\mathrm{mod}\, n)$.

Jeśli $y^2 = x \cdot v (\mathrm{mod}\, n)$, to jest tak jak powinno być.

Jeśli $y^2 \neq x \cdot v (\mathrm{mod}\, n)$, to „prover" jest oszustem.

Istota rzeczy w protokole identyfikacji Fiata – Shamira.

Zauważmy, że jeśli prover A nie zna tajemnicy s, jest oszustem to może odpowiedzieć prawidłowo tylko na co najwyżej jedno z pytań zadanych przez verifiera B. Już podając x w pierwszym kroku musi się zdecydować, czy postępuje tak:

1.losuje r, oblicza r^2 i wysyła $x = r^2$ do B. Wtedy na pewno odpowie prawidłowo na pytanie odpowiadające $e = 0$ ale odpowie źle na pytanie odpowiadające $e = 1$.

Czy postępuje tak:

2.losuje r, oblicza r^2 i wysyła $x = r^2 / v$ do B. Wtedy na pewno odpowie prawidłowo na pytanie odpowiadające $e = 1$ ale odpowie źle na pytanie odpowiadające $e = 0$.

Tak więc oszust „obstawia orła albo reszkę", ale „rzut monetą" zależy od „verifiera". Jeśli rzut nie wypadnie po myśli oszusta tzn. zgodnie z tym co obstawił, to zostanie zdemaskowany.

Prawdopodobieństwo, że oszustowi uda się przejść przez $t \in N$ realizacji protokołu Fiata-Shamira jest więc równe $\left(\frac{1}{2}\right)^t$. Jest to jednocześnie prawdopodobieństwo błędnego zadziałania protokołu.

.

Literatura

[1] A. Menezes, P. Oorschot, S. Vanstone; Handbook of Applled Cryptography; CRC Press Inc., 1997. (treść jest na stronie: http://cacr.math.uwaterloo.ca/hac)

[2] J.Stokłosa, T.Bilski,T.Pankowski; Bezpieczeństwo danych w systemach informatycznych; PWN, Warszawa 2001.

[3] M.Kutyłowski, W.Strothmann; Kryptografia, teoria i praktyka zabezpieczania systemów komputerowych; Oficyna Wydawnicza Read Me, Warszawa 2001.

[4] B.Schneier; Kryptografia dla praktyków; WNT, 2002.