

chcesz zmniejszyć koszty...

...i zwiększyć sprzedaż ?

potrzebujesz

evolve™



Klucze USB - dwustopniowa identyfikacja z evolve™

W wersji 3.1 evolve™, obok wielu innych ważnych ulepszeń, wprowadzono też zasadniczą zmianę sposobu logowania się użytkowników do systemu.

Wcześniej logowanie następowało za pomocą zwykłych nazwy użytkownika i hasła – zwykle kombinacji imienia i alfanumerycznego hasła, zaszyfrowanych i przekazanych do systemu w celu identyfikacji.

To podejście ma jednak wiele wad, między innymi nieuchronny konflikt między potrzebami użytkowników, którzy chcą łatwych do zapamiętania haseł, a wymogami bezpieczeństwa, które wymagają haseł bardziej skomplikowanych.

Po prostu, 'frank' to hasło które o wiele łatwiej zapamiętać niż 'nL991&4Ssa4', chociaż to drugie zapewnia o wiele lepszą ochronę przed włamaniem do systemu.

Problem nie ogranicza się jednak do samego wyboru hasła; takie podejście ma o wiele więcej wad.

Na przykład, większość z nas prędzej czy później zapisze gdzieś swoje hasło i login. Niestety, całkiem prawdopodobne jest, że ktoś natrafi na tę informację. Co więcej, w erze rosnącej liczby używanych na co dzień haseł łatwiej jest zawsze korzystać z tego samego...

Pomimo faktu, że dane w evolve™ są zaszyfrowane (więc nie da się przechwycić nazwy użytkownika i hasła), zawsze istnieje możliwość, że takie 'uniwersalne' hasło będzie wykradzione gdzieś indziej.

Podstawowym problemem jest to, że użycie nazwy użytkownika i hasła nie daje gwarancji, że osoba zalogowana za pomocą konkretnych danych jest naprawdę osobą, do której są one przypisane. Zaś w przypadku poufnych danych personalnych i handlowych, bezpieczeństwo i ograniczony dostęp są niezwykle istotne.

Rozwiązanie – dwustopniowa identyfikacja, „masz coś i pamiętasz coś”

Na szczęście, opisane powyżej przypadki nie zdarzają się często i zwykle problemem z identyfikacją polega na tym, którego hasła i loginu używamy w którym miejscu...

Dzięki użyciu klucza sprzętowego, możemy nie tylko pozbyć się tych wszystkich problemów, lecz również zwiększyć nasze bezpieczeństwo online.

Jak to działa

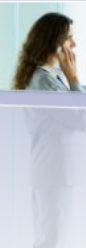
Sam klucz sprzętowy to urządzenie USB, kompatybilne nawet ze starszą wersją portu z czasów Windows 95. Mogą mieć różny kształt, ale te używane w evolve™ wyglądają tak:

chcesz zmniejszyć koszty...

...i zwiększyć sprzedaż?

potrzebujesz

evolve™



Token USB Aladdin R2

rozmiar 16x47 mm

Są bardzo podobne do popularnych dysków USB (tzw. pendrive), używanych do przenoszenia danych.

Jednak podobieństwo jest tylko zewnętrzne.

Zamiast układu, który umożliwia przenoszenie danych (jak w pendrivie), klucz sprzętowy zawiera układ w którym znajduje się unikalny podpis cyfrowy (bardzo długi łańcuch cyfr i liter) – który w żaden sposób nie może być zmieniony, eksportowany ani skopiowany.

Ten 'prywatny' podpis jest wygenerowany w momencie, w którym powstaje klucz i jest powiązany z pasującym tylko do niego podpisem 'publicznym'.

Ważne jest to, że klucza 'prywatnego' nie można określić na podstawie 'publicznego'. Nie pomoże nawet najbardziej skomplikowana matematyka. podobnie, klucza 'publicznego' nie da się określić na podstawie 'prywatnego' (nawet gdyby udało się odczytać go z układu scalonego).

Najważniejsze jest jednak to, że te dwa klucze są ze sobą powiązane. Coś, co jest 'podpisane' za pomocą danego klucza prywatnego można zweryfikować tylko za pomocą pasującego do niego, unikalnego klucza publicznego.

Podobnie, jeśli ktoś chce sprawdzić kim jest użytkownik (tak jak my w evolve™), może sprawdzić, czy jego klucz prywatny pasuje do publicznego (co nie wymaga ujawnienia klucza prywatnego). Tylko odpowiedni klucz prywatny poda właściwą odpowiedź na elektroniczne pytanie.

Ochrona klucza

Dostęp do samego klucza sprzętowego (zwykle nazywane są one *tokenami*) jest chroniony prostym hasłem. Kiedy klucz jest podłączony do komputera, prosi on użytkownika o podanie hasła. Wyjęcie klucza z gniazda powoduje automatyczne wylogowanie.

Ta 'dwustopniowa' identyfikacja – coś, co użytkownik ma (klucz sprzętowy) i coś, co wie (jego własne hasło) to bardzo bezpieczny sposób na zapewnienie, że jest on właśnie tą osobą, która ma prawo dostępu do ważnych danych, sposób używany w wielu miejscach od kont bankowych (karta do bankomatu) po systemy obronne.

chcesz zmniejszyć koszty...

...i zwiększyć sprzedaż ?

potrzebujesz

evolve™



Świetną rzeczą jest to, że hasło nie musi wcale być skomplikowane ('franek' w zupełności wystarczy), ponieważ właściwie ma ono tylko zapobiegać możliwości użycia klucza sprzętowego przez kogoś innego.

Jeśli hasło zostanie błędnie wprowadzone 3 razy z rzędu, klucz zostaje elektronicznie zamknięty i nie może być użyty przez nikogo – tylko jego ponowne sformatowanie i wygenerowanie nowego podpisu sprawi, że będzie znowu działał.

W razie zgubienia tokena, możemy usunąć z systemu związany z nim klucz publiczny i wydać użytkownikowi nowy klucz.

Inne sposoby wykorzystania

Chociaż my używamy kluczy sprzętowych do identyfikacji użytkowników, można je wykorzystać do wielu innych rzeczy w których zaletą jest system podpisu publicznego/prywatnego i dostęp poprzez pojedyncze hasło. Są to na przykład:

- logowanie do sieci Windows – zamiast nazwy użytkownika / hasła przy wczytywaniu profilu
- ochrona komputerów typu laptop – do identyfikacji i szyfrowania danych
- podpisywanie e-maili – elektroniczne podpisywanie i/lub szyfrowanie komunikacji przez e-mail
- szyfrowanie – plików, folderów lub całych napędów, co zapewnia dostęp do nich tylko posiadaczom określonych kluczy
- dostęp do sieci VPN – bezpieczny, szyfrowany dostęp do wewnętrznych sieci

Chociaż w większości z tych przypadków potrzebne jest dodatkowe oprogramowanie, wszystkie opierają się na tej samej zasadzie. **Jeśli interesuje Cię którekolwiek z powyższych sposobów wykorzystania systemu klucza prywatnego/publicznego, skontaktuj się z nami.**

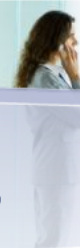
Inne fakty o kluczach i ich wykorzystaniu w evolve™

- Jeśli z jakiegoś powodu Twój komputer nie ma portu USB (lub jest on niedostępny, np. wszystkie są zajęte) łatwo można zaopatrzyć się w odpowiedni kabelek.
- Zgubione klucze sprzętowe mogą być odzyskane w ciągu jednej nocy – wysyłamy je kurierem. Awaryjny login do systemu będzie dostępny do czasu, kiedy użytkownik otrzyma swój nowy klucz. Za zagubiony klucz pobrana będzie opłata, pokrywająca koszt jego produkcji i przesyłki.
- Odłączenie klucza powoduje automatyczne wylogowanie użytkownika. Każde zalogowania i wylogowanie jest zapisywane (można wykorzystać je do kontroli

chcesz zmniejszyć koszty...

...i zwiększyć sprzedaż ?

potrzebujesz **evolve**™



czasu pracy).

Inne fakty

- Klucze nie potrzebują baterii – zasilane są bezpośrednio przez port USB.
- Są wodoodporne, ich obudowa zrobiona jest z materiału o dużej wytrzymałości
- Będą dobrze pasowały do Twoich kluczy – ważą ok. 5 gramów (tyle, co dwa spinacze biurowe)
- Podpis cyfrowy składa się z numeru o długości 120 bitów – czyli z 2^{120} albo 1.329.227.995.784.915.872.903.807.060.280.344.576 możliwych kombinacji.

Warstwa szyfrująca składa się ze 128 bitów – czyli 2^{128} albo 340.282.366.920.938.463.463.374.607.431.768.211.456 możliwych kombinacji.

Przy bieżących możliwościach techniki, zajęłoby więcej czasu niż pozostało go do końca wszechświata by wypróbować wszystkie kombinacje (źródło: *Thawte Security*).