Bezpieczne uwierzytelnianie biometryczne na przykładzie rozwiązania AXSionics Internet Passport

mgr inż. ROBERT POZNAŃSKI, mgr inż. KAROL SZACKI

Instytut Maszyn Matematycznych, Warszawa

W świecie, w którym kradzież tożsamości jest poważnym zagrożeniem, biometria staje się niezwykle istotną techniką bezpiecznego uwierzytelniania. W odróżnieniu od wszelkiego rodzaju kodów i haseł, cecha biometryczna jest ściśle i nierozerwalnie powiązana z daną osobą.

Wykorzystanie biometrii może stanowić pewne zagrożenie dla prywatności użytkownika. Ujawnienie danych biometrycznych osoby może skutkować różnego rodzaju nadużyciami. Z tego względu informacje te nigdy nie powinny być narażone na nieuprawnione modyfikacje lub kopiowanie. Ze względów bezpieczeństwa nie zaleca się też stosowania centralnych repozytoriów danych biometrycznych, gdyż przełamanie zabezpieczeń jednego systemu będzie miało konsekwencje dla wszystkich osób, których wzorce biometryczne były tam przechowywane.

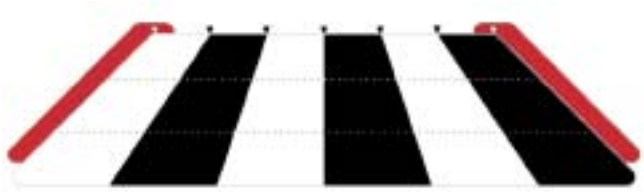
Na rynku pojawia się wiele nowych systemów uwierzytelniających. Szczególnie interesujące są te z potencjałem powszechnego wykorzystania w sieci Internet i posiadające jednocześnie możliwość uwierzytelniania biometrycznego chroniącego zarazem prywatność osób. Odznaczają się one przechowywaniem informacji wrażliwych oraz wykonywaniem operacji na tych danych bezpośrednio na urządzeniu będącym w posiadaniu użytkownika.

Jednym z takich rozwiązań jest AXSionics Authentication System. Pozwala on na uwierzytelnianie osób przy użyciu systemu zdecentralizowanego. Możliwe jest to dzięki obecności spersonalizowanego tokenu przypisanego do konkretnej osoby (Internet Passport).

Jak to działa

AXSionics Internet Passport (*rys. 1*) jest urządzeniem o rozmiarach zbliżonych do wymiarów powszechnie stosowanych kart elektronicznych. Wyposażony jest w monochromatyczny wyświetlacz OLED oraz czytnik linii papilarnych. Posiada także zestaw sześciu sensorów optycznych służących do odczytu danych wejściowych ze specjalnych animacji pokazywanych na ekranie komputera lub innego urządzenia wyposażonego w wyświetlacz graficzny.

Rys. 1. Urządzenie AXSionics Internet Passport
Fig. 1. AXSionics Internet Passport



Rys. 2. Wygląd animacji ekranowej wykorzystywanej w systemie AXSionics
Fig. 2. AXS-AS flickering bars

Odczyt danych kanałem optycznym następuje poprzez przyłożenie urządzenia na czas kilku sekund do ekranu w obszar, na którym wyświetlona zostaje animacja (*rys. 2*).

Główną funkcjonalnością paszportu internetowego AXSionics jest generowanie kodów jednorazowych. Mogą one znaleźć zastosowanie np. w bankowości elektronicznej, uwierzytelnianiu transakcji czy dostępie do systemów informatycznych.

Podstawą działania systemu, obok samego urządzenia, jest technologia animacji (*rys. 2*) wyświetlanych na witrynach internetowych. Użytkownik chcąc zalogować się do danej usługi podaje numer seryjny swojego paszportu internetowego oraz nazwę użytkownika. Na podstawie tych danych tworzona jest animacja, która pojawia się na ekranie komputera. Za generowanie animacji odpowiedzialna jest infrastruktura firmy AXSionics. Następnie, po przyłożeniu urządzenia do ekranu, dane zawarte w animacji zostają wczytane do jego pamięci. Aby rozszyfrować i wyświetlić komunikat użytkownik musi autoryzować się do swojego paszportu internetowego przeciągając palec przez czytnik linii papilarnych. Jeśli weryfikacja jest poprawna, na ekranie pojawia się kod jednorazowy, który należy przepisać jako hasło służące do logowania.

Łatwo zauważyć, że funkcjonalność paszportu internetowego AXSionics zbliżona jest do zastosowania jednorazowych kodów PIN powszechnie używanych w bankowości elektronicznej. Jednak tradycyjne kody jednorazowe przypisane są do jednej usługi. Jeśli posiadamy konta w różnych bankach lub korzystamy z innych usług wymagających bezpiecznego logowania otrzymamy do każdej z tych usług osobne listy kodów lub urządzenia służące do ich generowania tzw. tokeny. Rozwiązanie AXSionics Internet Passport integruje wszystkie te rozwiązania w jedno urządzenie dające dostęp do wielu usług on-line, oferowanych przez różne instytucje.

W przypadku zgubienia lub kradzieży listy kodów PIN jesteśmy narażeni na oszustwo i możliwość wykorzystania tych informacji bez naszej wiedzy. Dzięki wykorzystaniu biometrii nasz paszport internetowy jest zabezpieczony przed użyciem go przez niepowołane osoby.

Inną ciekawą możliwością zastosowania AXS Internet Passport jest przesyłanie wiadomości tekstowych. W animacji może być zakodowanych więcej informacji niż tylko kod jednorazowy. Istnieją witryny, które umożliwiają zaszyfrowanie krótkiego tekstu o długości około 160 znaków. Dodatkowym zabezpieczeniem jest przypisanie wiadomości do wybranego numeru seryjnego urządzenia, które będzie mogło ją odkodować. Adresat otrzymuje tylko plik graficzny przedstawiający animację. Po wczytaniu danych do urządzenia i uwierzytelnieniu, informacje zostaną wyświetlone na ekranie.

Połączenie obu funkcjonalności, generowania kodów oraz przesyłania wiadomości, może posłużyć do zabezpieczenia transakcji on-line. W przypadku dokonywania na przykład przelewu lub zakupów, w animacji poza samym kodem jednorazowym może zostać przesłany np. identyfikator transakcji, jej wartość czy inne informacje jednoznacznie ją identyfikujące.

Zabezpieczenie transakcji on-line oznacza, że wszystkie zagrożenia muszą być zminimalizowane do pewnego akceptowalnego poziomu. Jednocześnie powinna być zapewniona obsługa funkcjonalności, takich jak:

– wzajemne bezpieczne uwierzytelnianie użytkownika i operatora,
– ochrona prywatnych danych obu kontaktujących się stron,
– zachowanie anonimowości, w najlepszy możliwy sposób w zależności od charakteru transakcji,
– integralność i aktualność danych transakcyjnych,
– poufność danych transakcji,
– niezaprzeczalność.

Do tych wymagań możemy dodać jeszcze wymaganie łatwości obsługi (użyteczności), która oznacza ciągłą dostępność, ergonomię użytkowania i niskie koszty operacyjne. Warto w tym momencie zastanowić się jakie zagrożenia można napotkać w globalnej sieci.

Zagrożenia komunikacji elektronicznej

Potencjalnym słabym punktem narażonym na atak jest sama infrastruktura Internetu. Każda bramka, czy inny przekaźnik danych może być wykorzystany do podsłuchania lub posłużyć do ingerencji w przesyłane informacje. Jeżeli komunikacja pomiędzy serwerem a urządzeniem końcowym zabezpieczona jest poprzez połączenie SSL/TLS, ryzyko tego rodzaju ataku staje się marginalne. Istnieje jednak niebezpieczeństwo, że atakujący zmieni konfigurację lokalnej infrastruktury sieciowej, tak aby akceptowano fałszywe certyfikaty SSL. Może to skutkować tym, że niczego nieświadomy użytkownik połączy się z serwerem cyberprzestępcy. W takim przypadku atakujący staje się oszustem, który kieruje cały ruch sieciowy przez swoją maszynę i poprzez takie działanie może się podszyć pod osobę, którą zaatakował. Tego typu zachowanie nazywane jest atakiem *Man-in-the-Middle* (MitM).

Najbardziej narażone na atak jest urządzenie, przy pomocy którego użytkownik łączy się z Internetem. Komputery osobiste są zwykle niedostatecznie zabezpieczone przeciw najnowszemu złośliwemu oprogramowaniu. Dodatkowo ludzie są często podatni na *phishing*. Atakujący przy pomocy fałszywych wiadomości, podobnych w wyglądzie np. do e-maili wysyłanych przez banki, nakłania użytkownika do instalacji złośliwego oprogramowania. Takie działanie pozwala napastnikowi na monitorowanie komputera użytkownika, a nawet na wprowadzanie modyfikacji w oprogramowaniu bez jego wiedzy. Tego typu ataki są zwykle nazywane atakami *Man-in-the-Browser* (MitB).

Kradzieże tożsamości oraz ataki polegające na przechwytywaniu sesji połączeniowej (MitM, MitB) to najczęstsze typy ataków na użytkownika i jego komputer. Mogą być stosowane z powodzeniem w przypadku słabego zabezpieczenia systemu uwierzytelnienia użytkownika do usług oferowanych on-line.

Aby ochronić informacje przesyłane poprzez sieć Internet należy położyć szczególny nacisk na metody autoryzacji i uwierzytelniania. To one są punktem wyjściowym do nawiązania bezpiecznego połączenia pomiędzy dwiema stronami wymieniającymi się danymi. Firma AXSionics zaprezentowała system AXS Authentication System wspomagający te mechanizmy. Daje on możliwość wzajemnego uwierzytelniania oraz weryfikacji autentyczności.

Główną ideą rozwiązania jest zastąpienie wrażliwych na ataki części kanału komunikacyjnego bezpośrednim połączeniem z bezpiecznej strefy do dedykowanego terminala będącego w posiadaniu użytkownika. W systemie AXS-AS takie bezpieczne połączenie jest realizowane przez wykorzystanie stosunkowo prostego urządzenia Internet Passport, które nie jest zintegrowane z lokalnym systemem komputerowym i nie jest narażone na atak.

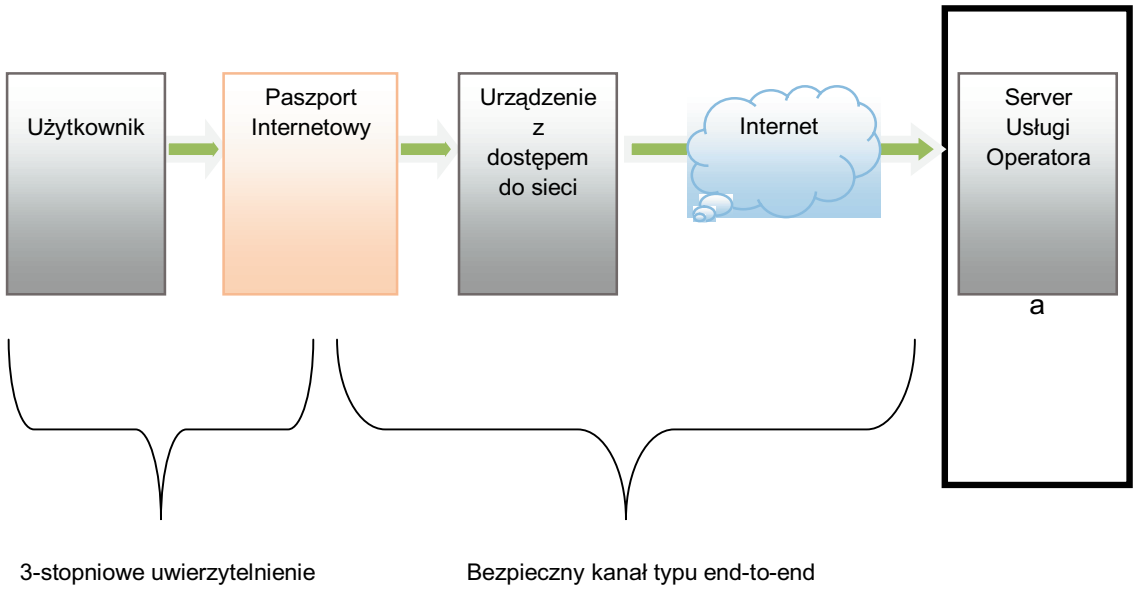
Bezpieczny dostępu do wielu usług

Rozwiązanie z użyciem AXS Internet Passport wprowadza możliwość uwierzytelnienia na trzech poziomach (*rys. 3*). Pierwszym jest coś co się posiada, czyli właśnie Paszport Internetowy. Na drugim poziomie użytkownik musi zaprezentować coś co może wiedzieć tylko on, np. hasło albo kod PIN, czyli kod jednorazowy odczytany z animacji i wyświetlony na ekranie urządzenia. Trzeci poziom uwierzytelnienia polega na sprawdzeniu unikalnej cechy użytkownika weryfikującej dostęp do kodu jednorazowego czy cechy biometrycznej. Część ta jest realizowana poprzez technologię skanowania linii papilarnych.

Całkowita siła zabezpieczeń jest wypadkową zastosowania powyższych składowych. W przypadku Internet Passport możliwe jest wykorzystanie wszystkich trzech poziomów na raz, co daje najwyższy poziom bezpieczeństwa. Nawet w przypadku zgubienia urządzenia, dzięki wykorzystaniu biometrii, osoby trzecie nie będą mogły z niego skorzystać.

Dane biometryczne od początku użytkowania urządzenia są pod wyłączną kontrolą użytkownika. Żadne informacje nie są nigdy przechowywane w centralnej bazie danych tylko bezpośrednio w urządzeniu.

Każdy paszport Internetowy AXSionics może zarządzać wieloma tożsamościami w pełni niezależnymi od siebie. Interfejs zarządzania bezpieczeństwem bazuje na prostym w implementacji modelu realizowanym w technologii WebService. To sprawia, że rozwiązanie oferowane przez AXSionics zapewnia wysoki stopień skalowalności w dwóch kierunkach – zarówno w ilości użytkowników końcowych jak i ilości dostawców usług. Dodatkowo nie jest potrzebna instalacja żadnego dodatkowego oprogramowania lub sprzętu. Klawiatura i monitor są jedynie urządzeniami wejścia/wyjścia, które są obecne wszędzie gdzie odbywa się interakcja użytkownika z komputerem osobistym. Do wyświetlenia animacji może



Rys. 3. Architektura AXS-AS Fig. 3. AXS-AS architecture

być użyty zarówno monitor komputerowy jak i ekran telefonu komórkowego. Nie ma zatem potrzeby inwestowania w dodatkową infrastrukturę.

Wzrost bezpieczeństwa, ale nie bez wad

W związku z coraz większym znaczeniem roli Internetu, a co za tym idzie, zwiększającą się skalą przestępstw w sieci, społeczność E-biznesu jest zmuszona do znajdowania coraz to nowszych i skuteczniejszych rozwiązań. Niezbędne jest zapewnienie bezpiecznej komunikacji pomiędzy operatorami usług, a użytkownikami. Nadal jednak nie ma jednomyślności co do sposobu, który miałby sprostać temu wyzwaniu. Istnieje natomiast przekonanie, że do bezpiecznej komunikacji potrzebny jest pewien rodzaj dedykowanej infrastruktury.

Jak można zauważyć tendencja prowadzi do unifikacji rozwiązań i integracji ich w jedno urządzenie. Jednak niezależnie od wszystkich technologii, które mogą zaistnieć w przyszłości, efektywne rozwiązania potrzebne są już dzisiaj. Powinno być to rozwiązanie działające w oparciu o obecną infrastrukturę IT, ponadto będące stosunkowo wygodne w użyciu, oraz zapewniające ochronę prywatności a także niewygórowane koszta. Zaprezentowany system AXSionics Internet Passport wydaje się spełniać pokładane w nim nadzieje. Trzeba również zaznaczyć, że paszporty internetowe są dopiero na poziome adoptowania przez społeczności użytkowników Internetu.

Model systemu AXSionics w zdecentralizowany sposób łączy osobę fizyczną z jej cyfrowym odpowiednikiem tożsamości, tokenem, przechowującym informacje takie jak np. dane biometryczne. Paszport internetowy sam w sobie jest potwierdzeniem tożsamość jego posiadacza. Służy przede wszystkim do generowania kodów jednorazowych oraz do przesyłania bezpiecznych wiadomości. Może współpracować z wieloma witrynami i usługami, bez potrzeby rozbudowy infrastruktury i oprogramowania. System AXSionicsa pokazuje, że możliwa jest pełna ochrona prywatności oraz danych biometrycznych, niezależnie od tego z jakiej maszyny podczas uwierzytelniania korzystamy. AXSionics pozwala także w łatwy sposób wykorzystać zalety standardu OpenID. W szybki i łatwy sposób pozwala właścicielowi paszportu internetowego potwierdzić swoją tożsamość 3-stopniowym poziomem uwierzytelnienia na każdym komputerze i dla wszystkich usług, które akceptują OpenID.

Rozwiązanie Internet Passport nie jest wolne od wad. Oparcie się na biometrii niesie za sobą pewne implikacje. W przypadku urazu dłoni czy samych palców traci się dostęp do usług i urządzenie jest wtedy bezużyteczne. Powszechnie znanym faktem jest także nieczytelność linii papilarnych u pewnego odsetka populacji. Kłopotliwą czynnością może też być przyłożenie paszportu internetowego do ekranu. Trzeba to zrobić w odpowiednim miejscu i przytrzymać nieruchomo na czas potrzebny do odczytania danych z animacji. Wykonanie tych czynności wymaga pewnej wprawy i precyzji co może stanowić kłopot w przypadku starszych użytkowników systemu.

Istotnym zagrożeniem może być także kwestia stabilności działania serwerów firmy AXSionics, które odpowiadają za generowanie animacji. W przypadku awarii bądź ataku na nie operacja logowania do jakiejkolwiek witryny korzystającej z paszportu internetowego stanie się niemożliwe.

Ponieważ liczba usług wykorzystujących AXS Internet Passport będzie stopniowo rosła, wraz z nią zwiększać się będzie potencjał i możliwości zastosowania urządzenia. Jednak nawet już teraz jest to ciekawa propozycja dla instytucji traktujących priorytetowo bezpieczeństwo danych. Dodatkowym atutem jest uniezależnienie działania od dodatkowego oprogramowania czy sprzętu. Powoduje to, że ciekawym obszarem użycia może być dyplomacja, lub dostęp do danych w firmach, których pracownicy często podróżują. Jednak głównym środowiskiem, które może najwięcej skorzystać na takim urządzeniu, jest bankowość elektroniczna i wszelkie inne usługi finansowe zarządzane przez Internet. Są to jedne z najbardziej narażonych na ataki pól, dlatego wprowadzenie dodatkowych mechanizmów uwierzytelniania i ochrony mogłoby przyczynić się do dalszego upowszechnienia tego typu usług.