aut. Sylwia Gliwa 24.01.2019

BIOMETRIA BEHAWIORALNA WKRACZA DO BANKOWOŚCI [TEST TECHNOLOGII]

Innowacyjny system biometrii behawioralnej wkroczył do branży bankowej jako rozwiązanie do wykrywania nieuprawnionych przelewów bankowych. Rozwiązanie testowane jest obecnie pośród klientów mBanku. Test nowej technologii specjalnie dla CyberDefence24.pl przeprowadził jej twórca, Mateusz Chrobok, Prezes i Założyciel, Digital Fingerprints.

SG: Biometria behawioralna wykorzystana w technologii właśnie wdrażanej w mBanku, często mylona jest z klasyczną biometrią. Jaka jest podstawowa różnica pomiędzy nimi?

MCh: Biometria klasyczna związana jest z cechami fizycznymi, na przykład skanami odcisków palców, tęczówki czy rozpoznawaniem twarzy. Ponieważ związana jest z nasza fizycznością często jest trudna do zmiany. Przykładem ataku na biometrię fizyczną jest historia byłej Pani Minister Obrony Niemiec, Ursuli Von Der Leyen. Na podstawie zdjęcia jej dłoni badaczom udało się stworzyć odciski palców, które umożliwiły odblokowanie jej telefonu.

Biometria behawioralna jest związana z naszym zachowaniem. To zaś w swej naturze jest zmienne w czasie. Nie jest ona tak wrażliwa jak biometria cech fizycznych z perspektywy ochrony danych. Olbrzymią zaletą jest ciągłość działania biometrii behawioralnej - chroni jeszcze przed momentem zalogowania do systemu i działa aż do momentu wylogowania. W przypadku biometrii klasycznej mogłoby to wymagać ciągłego trzymania palca na czytniku linii papilarnych.

Test pokazał, jak zachowuje się rozwiązanie przy zmianie sposobu korzystania z komputera, czyli przy zmianie sposobu pisania na klawiaturze. Jakie jest prawdopodobieństwo, że dwie lub więcej osób korzysta w podobny sposób z komputera?

Każde uwierzytelnianie za pomocą biometrii charakteryzuje się pewnymi błędami związanymi z jakością sensorów i zastosowanych metod. Dla odcisków palców najczęściej mówi się o unikalności w stosunku 1 do 50 000. Oznacza to, że statystycznie co pięćdziesięciotysięczna osoba może być w stanie odblokować za pomocą swojego odcisku palca nasz telefon. Korzystanie z komputera to dostarczanie dużej ilości danych, które mogą być wykorzystane jako dane pomiarowe.

W związku z tym odpowiedź na pytanie związane z prawdopodobieństwem, że dwie lub więcej osób korzysta z komputera w podobny sposób zależy od interfejsu danej usługi i ilości interakcji. Jest także związana z ilością korzystających użytkowników i ich charakterystyką interakcji. Jakość rozpoznawania jest związana z ilością danych wykorzystaną w procesie uczenia maszynowego. Im więcej danych - tym wyższa jakość - tym mniejszy błąd rozpoznawania.

Czym charakteryzują się ataki: Man-In-The-Middle, Man-In-The-Browser attack

Man-In-The-Middle attack - Atak, w którym pomiędzy użytkownikiem a docelową usługą znajduje

się cyberprzestępca. W takim wypadku jest on w stanie zazwyczaj przechwytywać ruch sieciowy, podsłuchiwać go i modyfikować. Takim klasycznym przykładem jest korzystanie z otwartych sieci wifi na lotnisku. **Man-In-The-Browser attack** - Podobnie jak MITM, jednak atakujący ma pełną kontrolę nad zachowaniem przeglądarki i wysyłanym przez nią ruchem. **Session Hijacking attack** - Podczas trwania sesji zazwyczaj ciasteczka i unikalne numery sesji są wykorzystywane przy wysyłaniu zapytań w celu weryfikacji tożsamości. W sytuacji, gdy cyberprzestępca taką sesję przechwyci, może podszyć się pod właściciela danego zasobu, przykładowo konta bankowego lub mailowego.

W każdym z trzech opisanych przypadków biometria behawioralna ma możliwości wykrycia anomalii i dzięki temu jako dodatkowy składnik uwierzytelniania -powstrzymania cyberprzestępców.

Czytaj też: Linie papilarne na celowniku hakerów. Klawiatura sposobem na sprawdzenie tożsamości użytkownika?