Politechnika Częstochowska

INTELIGENTNE SYSTEMY UWIERZYTELNIANIA

dr hab. inż. Mariusz Kubanek, prof. PCz
mariusz.kubanek@icis.pcz.pl
Katedra INFORMATYKI

POLITECHNIKA Politechnika Częstochowska

KI

Wykład 14
Metody wykrywania fałszerstw w systemach uwierzytelniania

Politechnika Częstochowska

WYKRYWANIE CZŁOWIECZEŃSTWA

- Jednym z głównych zabezpieczeń systemów biometrycznych jest wykrywanie człowieczeństwa, czyli weryfikacja, czy badany obiekt jest naprawdę człowiekiem.

- Większość systemów w wersji podstawowej analizuje tylko obraz i dają się one łatwo oszukać przez sztuczne (nie żywe) kopie cechy biometrycznej.

WYKRYWANIE CZŁOWIECZEŃSTWA

- Coraz częściej stosują one dodatkowe analizatory, które weryfikują cechy charakterystyczne dla żywej części ciała, np. zmienność wielkości źrenicy pod wpływem światła, temperaturę, pH, wilgotność.

WYKRYWANIE CZŁOWIECZEŃSTWA

- W przypadku czytników linii papilarnych rozróżnia się kilka rodzajów takich rozwiązań.

- Czytnik optyczny porównuje zapisane cyfrowo odciski palców, czytnik pojemnościowy mierzy pojemność kondensatora utworzonego z powierzchni palca i powierzchni sensora, a czytnik termiczny porównuje różnice temperatur pomiędzy punktami linii papilarnych.

POLI TECHNIKA Politechnika Częstochowska

WYKRYWANIE CZŁOWIECZEŃSTWA

[KI]

- Najpopularniejszymi czytnikami są optyczny oraz pojemnościowy. Niestety, tego typu czytniki nie są odporne na oszukiwanie za pomocą sztucznych odlewów odcisku, np. w żelu.

- Czytniki siatkówki oka wykorzystują kamery wysokiej rozdzielczości dodatkowo analizujące żywotność oka przez zmianę oświetlenia, które powoduje zmiany rozmiaru źrenicy.

PRÓBY OSZUSTWA - ODCISKI

- Proces oszukania systemu uwierzytelniania z wykorzystaniem odcisków palców dzieli się na dwa główne etapy: pobranie próbki odcisku palca ofiary oraz preparację sztucznego odcisku.

- W pierwszym etapie najistotniejsze jest znalezienie odpowiedniej jakości próbki, jaką zostawi osoba, pod którą chcemy się podszyć.

PRÓBY OSZUSTWA - ODCISKI

- Najlepiej w tym celu podłożyć ofierze szklane naczynie, płytę CD lub inny przedmiot o gładkiej strukturze, bez nadruków oraz wzorów.
- Następnie na odcisk należy nanieść pył, np. grafit, który spowoduje jego uwydatnienie.
- Innym dość dobrym sposobem jest naniesienie bardzo cienkiej warstwy cyjanoakrylu, który jest składnikiem klejów szybkoschnących i spowodowanie jej zaschnięcia.

Politechnika Częstochowska

PRÓBY OSZUSTWA - ODCISKI

- Wysychająca warstwa kleju spowoduje związanie się tłuszczu zawartego w odcisku z klejem.
- Następnie taki odcisk musi zostać sfotografowany w wysokiej rozdzielczości.
- Najlepsze efekty dają aparaty fotograficzne do zdjęć makro.

PRÓBY OSZUSTWA - ODCISKI

- Innymi metodami utworzenia odlewu odcisku jest użycie masy lateksowej lub ciastoliny, czyli masy podobnej do plasteliny.

- Każda z zaprezentowanych metod podrobienia odcisku palca jest bardzo prosta w realizacji i możliwa do wykonania w domu bez zastosowania specjalistycznego sprzętu.

Politechnika Częstochowska

PRÓBY OSZUSTWA - TWARZ

- W przypadku systemów rozpoznających twarz użytkownika najprostszym sposobem jest użycie zdjęcia ofiary.
- Metoda ta działa tylko, gdy twarz jest analizowana z jednej kamery.
- Jeśli chodzi o obraz z wielu kamer, metodą umożliwiającą oszukanie jest użycie maski bezpośrednio przylegającej do twarzy.

Politechnika Częstochowska

PRÓBY OSZUSTWA - TĘCZÓWKA

KI

- Systemy opierające się na tęczówce oka dają się oszukać przez wydruk zdjęcia oka w dużej rozdzielczości.
- Dość skuteczną próbą zabezpieczenia się przed oszustwem jest zmiana oświetlenia i analiza zmiany wielkości źrenicy oka.

POLITECHNIKA Politechnika Częstochowska

PRÓBY OSZUSTWA - GŁOS

[KI]

- W przypadku systemów z analizą głosu stosuje się zwykle nagrania wypowiedzi ofiary.
- Słabo zabezpieczony system bez problemu potwierdzi weryfikację, pomimo iż głos wydobywany jest z nagrania.
- Zabezpieczeniem przed tego typu rozwiązaniami jest konieczność podania różnych sekwencji słów przez użytkownika.

PRÓBY OSZUSTWA - GŁOS

- Czasem dobrym podejściem jest analiza treści hasła znanego wyłącznie użytkownikowi.
- Niestety w obecnych czasach bardzo łatwo jest podsłuchać drugą osobę.
- Istnieją również systemy, w których wykorzystuje się próbę wykrycia szumu charakterystycznego dla odtwarzanego dźwięku, jednak to rozwiązanie może powodować nieprawidłowe działanie w niektórych środowiskach eksploatacji.

METODY ZABEZPIECZEŃ

- Najnowocześniejsze systemy wykorzystują wielomodułowe systemy biometryczne i bardzo często analizują dodatkowo rozkład żył w palcu.
- Jest to metoda dość nowa, która nawet samodzielnie daje bardzo dobre wyniki.
- Integracja takiego systemu z czytnikiem odcisków palców znacznie skraca czas analizy, gdyż system ten służy potwierdzeniu tożsamości, która została określona przez strukturę odcisku palca.

METODY ZABEZPIECZEŃ

- Nowością są również analizatory dynamicznego podpisu.
- Parametry dynamiczne, nie są możliwe do zarejestrowania podczas składania tradycyjnego podpisu.
- Szansa na podrobienie go jest zatem bliska zeru, a bezpieczeństwo jest znacznie większe.

METODY ZABEZPIECZEŃ

- Dokładność i różnorodność mierzonych parametrów sprawia, że z pozoru podobnie wyglądające odręczne podpisy biometryczne zostaną rozpoznane przez program jako zupełnie różne.

- Identyfikacja osoby podpisującej staje się więc znacznie prostsza, przebiega ona również elektronicznie, inaczej niż w przypadku sygnatur na papierze, gdy konieczna jest pomoc grafologa.

METODY ZABEZPIECZEŃ

- Bezpośrednie powiązanie podpisu biometrycznego z wybranym dokumentem prowadzone jest w taki sposób, aby wszelkie późniejsze próby modyfikacji dokumentu były możliwe do wykrycia.

- Wspomniana funkcja jest koniecznym warunkiem bezpieczeństwa, bez niej niemożliwe byłoby udowodnienie, że postać umowy lub innego dokumentu jest identyczna z tą, która istniała podczas składania sygnatury.

BEZPIECZEŃSTWO SYSTEMU

- Tworząc systemy uwierzytelniania należy wziąć pod uwagę przede wszystkim bezpieczeństwo takiego systemu.

- Słabo zabezpieczone systemy nie zachęcą społeczeństwa do korzystania z tego typu rozwiązań, pomimo wielu zalet, jakie dostarczają systemy biometryczne w porównaniu do tradycyjnych metod weryfikacji tożsamości.

Politechnika Częstochowska

Projekt finansowany w ramach programu Ministra Nauki i Szkolnictwa Wyższego pod nazwą „Regionalna Inicjatywa Doskonałości" w latach 2019 - 2023 nr projektu 020/RID/2018/19 kwota finansowania 12 000 000 PLN

Politechnika Częstochowska

KI

Dziękuję za uwagę

dr hab. inż. Mariusz Kubanek, prof. PCz
mariusz.kubanek@icis.pcz.pl
Katedra INFORMATYKI