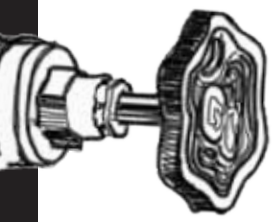
8/2016

FUNDACJA
bezpieczna
cyberprzestrzeń



zawór bezpieczeństwa 8/2016

3D w służbie policji

Amerykańska policja chce posłużyć się wydrukiem 3D palca zamordowanego mężczyzny, aby odblokować jego telefon komórkowy. Śledczy są przekonani, że urządzenie zawiera ważne informacje, które mogą pomóc rozwikłać sprawę zabójstwa.
W tym celu policjanci zwrócili się o pomoc do profesora z lokalnej uczelni specjalizującego się w biometrycznej identyfikacji tożsamości. Śledczy posiadają skan odcisku palca ofiary, gdyż mężczyzna figurował w policyjnej bazie. Na wykonany na podstawie skanu model 3D palca naniesione zostaną linie papilarne. Wydruk zostanie pokryty cienką warstwą metalu, aby czytnik w komórce uznał go za prawdziwy palec, odczytał dane i odblokował aparat. Eksperci ostrzegają jednak, że ten zabieg może nie wystarczyć, gdyż prawdopodobne jest, iż z racji tego, że telefon nie był od dawna odblokowywany, pojawi się żądanie dodatkowej weryfikacji, np. kodu.

A jeśli z odblokowaniem telefonu przy pomocy reprodukcji 3D pójdzie łatwo, to dla użytkowników jedyną ochroną przed nadużyciami będzie wyłączenie w urządzeniu biometrycznej weryfikacji. Ot, prywatność w małym palcu. [1]

Szpiegujące badge

Czy w pracy dużo rozmawiasz z ludźmi czy raczej masz naturę mruka? Ruszasz nerwowo nogą w sytuacjach stresowych? Tkwisz przez cały czas przy biurku czy masz w zwyczaju robić obchód po pokojach? Teraz podczas mierzenia Twojej służbowej efektywności żaden z tych detali nie umknie szefowi. Z pomocą pracodawcom przychodzi nowy produkt firmy Humanyze, skrojony wprost dla korporacyjnego świata. Chodzi o z pozoru zwykły badge, który w biurach noszą pracownicy. Z pozoru, bo dzięki wbudowanym czujnikom i mikrofonom gadżet ten ma funkcję śledzenia ruchu i nagrywania głosu. Pozwala to np. na monitorowanie nastrojów pracownika czy reakcji na sytuacje stresowe oraz generowanie odpowiednich statystyk, takich jak stopień produktywności, innowacji czy współpracy. Firma zaznacza, że wszystkie dane zbierane są za zgodą pracownika i zapowiada, że w przeciągu najbliższych 3-4 lat i tak każdy badge będzie miał takie czujniki. Wizja przerażająca? Na pocieszenie dodamy, że w ramach ochrony prywatności z monitoringu wyłączyć można np. strefę toalety czy kuchni.
Czy pracownik przyszłości tylko w takich rewirach będzie mógł być naprawdę sobą? [2]

FUNDACJA bezpieczna cyberprzestrzeń

Skąd 4-cyfrowy PIN?

Pierwsze bankomaty pojawiły się w 1967 roku i początkowo przywilej korzystania z nich mieli nieliczni. Dziś większość z nas korzysta z nich tak często, że numer PIN wstukujemy mechanicznie. Jeśli zgubisz kartę lub zostaniesz okradziony, Twój PIN jest jedyną tarczą ochronną. Czy kiedykolwiek zastanawiałeś się dlaczego jest on 4-cyfrowy? Czy pomysłodawcy bankomatów nie stać było na bardziej wyszukane zabezpieczenie?
Nie spodziewajcie się żadnego matematycznego wyjaśnienia. Historia jest prostsza niż się spodziewacie. Zamysłem twórcy bankomatów Johna Adriana Shepherd-Barrona było wprowadzenie 6-cyfrowego PINu. Jednak pierwsza osoba testująca jego nowy wynalazek – żona, nie sprostała wyzwaniu zapamiętania 6-cyfrowego hasła, utrzymując, że podobnie jak ona, większość użytkowników będzie w stanie zapamiętać maksymalnie 4 elementy. I w ten oto sposób nad kuchennym stołem zadecydowano, że 4 cyfry stały się światowym standardem.
W końcu podobno za każdym sukcesem mężczyzny stoi kobieta ;-). [3]

Selfie-weryfikacja

Skoro o PINie mowa to okazuje się, że coraz więcej użytkowników jest znudzonych tą formą autoryzacji transakcji i liczy na coś nowego. Około 84% badanych przez firmę Mastercard przyznało, że zdarzyło im się zapomnieć hasła, a 54% uważa, że na pewno istnieje jakaś alternatywa w stosunku do tradycyjnego PINu. Na ich oczekiwania firma zareagowała szybko, wprowadzając od przyszłego roku na polski rynek nową aplikację do autoryzacji płatności „Identity Check".
Teraz zapamiętywanie i każdorazowe wstukiwania PINu już nie będzie potrzebne. Idąc z duchem czasu nowa aplikacja wykorzystuje technologię rozpoznawania twarzy – do autoryzacji płatności wystarczy więc... zrobić sobie selfie!

Co na to amatorzy wrzucania swoich „słitfoci" na portale społecznościowe? Wielu twierdzi, że gotówka w portfelu zawsze najbezpieczniejsza. [4]

2040 bez prądu?

Zgodnie z prognozami amerykańskiej organizacji Stowarzyszenie Przemysłu Półprzewodnikowego (Semiconductor Industry Association - SIA) do 2040 komputery będą zużywać więcej energii niż jesteśmy w stanie wyprodukować. Według najnowszego raportu „oszalałym na punkcie komputerów społeczeństwom zabraknie prądu do 2040 roku". Firmy będą musiały zmierzyć się z wyzwaniem innego projektowania urządzeń elektronicznych i wymyślenia nowego sposobu ich zasilania. Nowe technologie muszą być wydajniejsze niż te, którymi dysponujemy obecnie – twierdzi SIA. A skoro ryzyko jest tak poważne, to może warto połączyć przyjemne z pożytecznym? Jak wiadomo praca przy komputerze związana jest ze szkodliwym siedzącym trybem życia. Może pora na urządzenia zasilane wysiłkiem ludzkich mięśni? Na przykład, komputer działający tylko wtedy, gdy użytkownik wprawia w ruch pedały rowerowe? [5]

FUNDACJA bezpieczna cyberprzestrzeń

Nie schowasz się za pikselami

Eksperci twierdzą, że pikselizacja, zamazywanie czy kodowanie elementów JPEG już nie chroni skutecznie wizerunku na zdjęciach. Ich zdaniem można „przeszkolić sztuczną inteligencję, aby z sukcesem identyfikowała twarze i rozpoznawała obiekty, nawet gdy zdjęcia są chronione przy użyciu różnych technik maskowania". Wyniki wahają się od 50 do 95 procent w zależności od typu maskowania. W procesie szkolenia, który musi obejmować dostęp do wyraźnych zdjęć, sieci neuronowe uczą się wykorzystywać korelacje między ukrytą i widoczną informacją. Po takim treningu są w stanie identyfikować zamaskowane twarze szybciej niż ludzie. Cały proces jest bowiem skomputeryzowany i zautomatyzowany, więc idzie sprawniej, zarówno w dzień, jak i w nocy. Spod maskowania wydobyć można również tekst lub pismo odręczne, oczywiście pod warunkiem, że maszyna ma dostęp do bazy danych, na której może się szkolić.

Czy to oznacza, że Google Maps z gdzieniegdzie pustymi miejscami, plamami i zamazanymi polami nie będzie już miało przed nami żadnych tajemnic? [6]

[1] http://tinyurl.com/h8do975
[2] http://tinyurl.com/hben5zj
[3] http://tinyurl.com/gpfljtu
[4] http://tinyurl.com/gpm9egl
[5] http://tinyurl.com/z8fcter
[6] http://tinyurl.com/hpax58q

Kolejne numery biuletynu „Zawór Bezpieczeństwa" można również śledzić na serwisie społecznościowym LinkedIn

Fundacja Bezpieczna Cyberprzestrzeń zaangażowana jest w wiele inicjatyw, konferencji, szkoleń i projektów dotyczących tematyki bezpieczeństwa teleinformatycznego. Celem Fundacji jest działanie na rzecz bezpieczeństwa cyberprzestrzeni, w tym na rzecz poprawy bezpieczeństwa w sieci Internet.

www: https://cybsecurity.org
Twitter: @cybsecurity_org
Facebook: https://www.facebook.com/FundacjaBezpiecznaCyberprzestrzen

Redakcja: Adrianna Maj, Agnieszka Wrzesień-Gandolfo