SVĚTCHYTŘE.CZ

NA **SVĚTCHYTŘE.CZ** NAJDETE AKTUÁLNÍ INFORMACE O TECHNOLOGIÍCH, KTERÉ VÁM USNADŇUJÍ ŽIVOT A ŠETŘÍ PENÍZE.
VYDÁNÍ PRO VÝZKUM ZNALOSTÍ O BIOMETRIÍCH

Tomáš Doseděl

Biometrie není jen otisk prstu.

Dávejte pozor, komu své údaje poskytnete

Česko již několik let vydává výhradně biometrické cestovní pasy, řada mobilů umožňuje odemykání pomocí otisku prstu nebo fotky obličeje a do práce se spousta z nás dostává přiložením palce na umatlanou čtečku otisku prstů. Biometrie je všude kolem nás, jen málokdo však ví, co všechno umožňuje a na co je dobré si dávat pozor.

Jedním ze zásadních problémů, které řeší vývojáři počítačů, mobilních telefonů i nejrůznějších informačních systémů, je takzvaná autentizace neboli ověření totožnosti. Jakým způsobem zjistíte, že za klávesnicí sedí skutečně ten, kdo tam sedět má? Existují tři obecně platné metody, které známe i z běžného života. Člověk prokazující svou totožnost může něco tajného znát (například heslo), něco unikátního vlastnit (třeba čipovou kartu) nebo něčím nenapodobitelným být.

Právě poslední zmíněnou kategorii řeší vědní oblast nazvaná biometrická autentizace. Biometrie jako taková se totiž zabývá měřením vlastností člověka; pokud jsou tyto vlastnosti jedinečné, dají se použít k prokázání totožnosti.

Barva očí nestačí

Ve starých občanských průkazech bývala uvedena barva očí a barva vlasů. Na základě černobílé fotky obličeje a těchto údajů dokázal úředník nebo policista ověřit s dostatečnou mírou jistoty, že předkladatel občanského průkazu o své totožnosti nelže.

Tyto tělesné vlastnosti ale nejsou příliš unikátní, modrookých blonďáků nebo hnědookých brunetek pobíhá po světě několik stovek milionů. A jak plyne čas od vytvoření fotky, stává se tato metoda stále méně spolehlivou. Aby biometrická autentizace fungovala, musí být použita taková tělesná vlastnost, kterou má každý člověk odlišnou. A když už ji nemá odlišnou úplně každý, tak by šance, že na základě této vlastnosti dva lidi zaměníme, měla být přiměřeně nízká.

Jako první se všem vybaví otisk prstu, který odedávna využívají kriminalisté k identifikaci pachatelů. Existuje ale celá řada dalších vlastností, kterými se od sebe vzájemně lišíme. Běžně se v bankách používá rukopis, zejména klasický podpis. Stále se také využívá již zmíněná fotografie, která přeci jen napoví víc než jen barva očí a vlasů. Další možností je identifikace skrze krevní řečiště v oční sítnici nebo jiné části těla, barevnost oční duhovky, kód DNA nebo třeba způsob chůze. Některé z uvedených vlastností jsou unikátní více, jiné méně. Některé lze relativně snadno napodobit; třeba o věrohodnosti rodičovského podpisu v žákovské knížce by mohly zábavné historky vyprávět celé generace učitelů.

V praxi záleží také na tom, jak snadno se daná tělesná vlastnost měří. Sejmout někomu otisk prstu zvládne dnes každý lepší mobil a trvá to jen zlomek sekundy. Na druhou stranu udělat analýzu DNA vyžaduje solidně vybavenou laboratoř.

V reálném světě se asi nejčastěji používá biometrická autentizace pomocí otisku prstu, protože jeho načtení je rychlé a neinvazivní. Pro případy, kdy nepotřebujete stoprocentní spolehlivost, dobře poslouží i rozpoznávání obličeje. To se běžně využívá k vyhledávání důležitých osob na letišti nebo sportovních utkáních. Automatický systém upozorní na podezřelou osobu a živá ostraha pak ověří, jestli je dotyčný skutečně hledaný výtržník nebo terorista. Na automatickém rozpoznávání obličejů je mimochodem založen také čínský systém kontroly obyvatelstva.

Vážení čtenáři,

od roku 2017 na serveru SvetChytre.cz píšeme o chytrých domovech, městech, dopravě i výrobě. Píšeme o chytrém Česku i o tom, co přinese umělá inteligence.

Do tištěné ukázky, kterou právě držíte v rukou, jsme vybrali to nejzajímavější. Každý den vydáváme nové články o digitálních technologiích. Texty o aktuálních trendech, rozhovory s inspirativními lidmi i komentáře těch, kdo vidí pod povrch.

Přesvědčte se sami na **SvetChytre.cz**

Příjemné čtení přeje
Ivo Minařík
šéfredaktor

Nevěřte špionům

Naopak v akčních filmech se asi nejčastěji setkáme s ověřením pomocí skenu oka, přičemž není vždy jasné, jestli jde o sken duhovky, nebo krevního řečiště na sítnici. Velmi často se pak ve filmech stá-

SvětChytře.cz na sociálních sítích:

facebook.com /svetchytre/

twitter.com /SvetChytre

linkedin.com /company/svet-chytre

SvetChytre.cz /rss/s/homepage

vá, že padouch vydloubne někomu oko, s jehož pomocí pak obalamutí i ten nejdokonalejší systém. A pokud k tomu nevyužije vydloubnuté oko, stáhne (nejlépe přes několik družic a za využití zelenočerného operačního systému, samozřejmě jediným příkazem) ze systému všechny otisky prstů, které pak vytiskne na 3D tiskárně a použije ke vstupu do banky nebo bytu amerického prezidenta.

Ve skutečném světě by žádný z těchto scénářů nefungoval. Biometrické systémy téměř nikdy neuchovávají kompletní otisk prstu. Je to pro ně zbytečné, úplně stačí, když si zapamatují několik charakteristických znaků otisku, tedy bodů a linií, podle kterých pak člověka dobře identifikují. Totéž platí pro skeny oka nebo jakékoliv jiné biometrické informace. Vytáhnout ze systému váš prst a vyrobit jeho kopii je tudíž nemožné.

Kopii lze samozřejmě vyrobit z vašeho skutečného prstu. Doba pokročilých skenerů a 3D tiskáren je dávno tady a stačí vás pod vhodnou záminkou (například zdravotní vyšetření nebo výroba prstenů na míru) přesvědčit, abyste svou ruku poskytli k nekalým účelům. Skutečně dobrý biometrický systém se ale vytisknutou kopií nedá ošálit, stejně jako nepřijme vydloubnuté lidské oko.

Základním krokem, který se při biometrické autentizaci provádí, je totiž takzvaný test živosti. Při snímání otisku prstu se měří teplota nebo elektrický odpor. Při skenování oka se zase posuzuje, nakolik je posmrtně zakalené, při ověřování podle obličeje se posoudí, zda je předložený obličej trojrozměrný a nejedná se pouze o fotku.

Právě kvůli těmto technikám by filmový špion ve skutečném světě příliš neuspěl, tedy za předpokladu, že výrobce čtečky na test živosti nezapomněl. I to se ale, zejména u velmi levných čteček, občas stává.

Máme se biometrie bát?

Své biometrické charakteristiky kolem sebe trousíme v podstatě neustále. Pokaždé, když se člověk něčeho dotkne, zanechá na místě otisk prstu (a často i vzorek DNA). Každý pohled do kamery v supermarketu znamená, že někdo získal digitální kopii vašeho obličeje. Vánoční pohledy zasílané rodině obsahují vzorek vašeho rukopisu. Propadat paranoie a začít chodit v masce a rukavicích ale samozřejmě nemá vůbec smysl.

Obezřetní buďte raději v případech, kdy někdo vaše biometrické údaje sbírá přiznaně. Ať už se jedná o státní úřad, který chce váš otisk prstu kvůli vydání pasu či víza, o soukromou firmu vyžadující váš vzorový podpis k ověření převzetí balíku, nebo o mobilní telefon, který se odemkne, když položíte prst na to správné místo.

V těchto případech totiž můžete aspoň částečně ovlivnit, co se s vašimi biometrickými údaji stane, a v některých případech dokonce odmítnout jejich poskytnutí. Někdy dokážete posoudit, nakolik je čtečka daného údaje kvalitní, případně si o ní vyhledat nějaké informace na internetu. Stejně tak je vaše svobodné rozhodnutí, jestli dané instituci věříte natolik, abyste jí poskytli své tělesné údaje, případně jestli v budoucnu svůj souhlas raději neodvoláte.

FIRMY CHYTŘE

Jan Čambora

Kyberbezpečnost v práci Češi neřeší.

K počítači pustí i cizího člověka

Série testů IT společnosti Servodata odhalila, že mezi největší slabiny kybernetické bezpečnosti českých firem patří sami zaměstnanci. Více než polovina z nich do svého počítače bez obav zapojí neznámý flash disk ponechaný na stole. Falešné IT specialisty vyslané do firmy pod smyšlenou záminkou dokonce ke svým souborům pustil každý. Sedm z deseti zaměstnanců se zase nechalo zmást phishingem.

Společnost Servodata prováděla loni a letos testy kybernetické bezpečnosti mezi svými klienty. Jejich účelem bylo zjistit, jak pracovníci dodržují běžná uživatelská opatření IT bezpečnosti. Experti společnosti proto provedli sérii phishingových útoků s cílem fiktivně vylákat ze zaměstnanců citlivé údaje nebo infiltrovat software do systému klienta. V 70 % byly fingované útoky úspěšné. „Vyzkoušeli jsme i baiting, což znamená kladení návnad. Těmi byly flash disky rozmístěné po stolech v kancelářích. V šedesáti procentech případů je pracovníci zapojili do svých počítačů, přestože nevěděli, odkud jsou nebo co na nich je. Mohly přitom obsahovat potenciálně škodlivý software," uvádí Miroslav Kvapil, generální ředitel společnosti Servodata.

Nejlepších výsledků ale dosahovali falešní IT specialisté, kteří se pokoušeli projít přes recepci a od zaměstnanců následně získat přístup do jejich pracovních počítačů. Stačilo, aby pracovníkům řekli, že je za nimi posílá jejich nadřízený.

Pokračování článku zde

STÁT CHYTŘE

Rani Tolimat

Máme se bát Číny?

Aneb moderní technika může být i nepřítel

Jak se žije v zemi, kde je pod kontrolou každý váš pohyb, ale také každá navštívená webová stránka i sebemenší bankovní transakce? A jak se na tomto stavu podílejí špičkové technologické firmy, jejichž produkty běžně používáme?

Ještě nedávno jsme si mysleli, že moderní technologie osvobozují, že jsou s totalitou podobně neslučitelné jako hospodářská prosperita. Jenže především čínská realita posledních let nás z téhle iluze vyléčila – dnes už víme, že i diktatura může být ekonomickou a dokonce i technologickou velmocí a že kvalitní technika ve špatných rukou slouží k utužení autoritářské moci. Teď je na nás, abychom se s tím nějak vyrovnali a přitom si udrželi své hodnoty i přesto, že to nemusí být nejsnazší a nejlevnější cesta.

Tato myšlenka se jako refrén táhla konferencí nazvanou Beyond Huawei (Nejen Huawei) s podtitulem Jak si Evropa zvyká na čínskou technologii a jaké to má důsledky, kterou v Akademii věd ČR uspořádal sinologický think-tank Sinopsis. Čínský vývoj posledních sedmdesáti let shrnul ředitel Sinopsis Martin Hála: „Komunistická historie země má v zásadě tři hlavní fáze. První byla éra Mao Ce-tunga – megalomanského samovládce, který naštěstí neměl dost technických prostředků k tomu, aby své vize uskutečnil ve velkém.

Pokračování článku zde

SvětChytře ≡ ISSN 2570-8627 ≡ **Šéfredaktor:** Ivo Minařík, sefredaktor@svetchytre.cz ≡ **Vydavatel:** SocialBooster, s.r.o. – IČO 04123417
inzerce: inzerce@svetchytre.cz ≡ **Tiskové zprávy a náměty zasílejte na:** tz@svetchytre.cz
facebook.com/SvetChytre ≡ twitter.com/SvetChytre ≡ linkedin.com/company/svet-chytre ≡ Copyright © 2018 SocialBooster
sazba, zlom: Ivona Krátká, **www.kratkagrafika.cz** – grafické práce, stavební tiskoviny ≡ Vydáno v Praze dne 20. 8. 2020
Projekt Průzkum a edukace občanů České republiky v oblasti biometrie je podpořen grantem Technologické agentury ČR / ÉTA č. TL02000134

Za podpory T