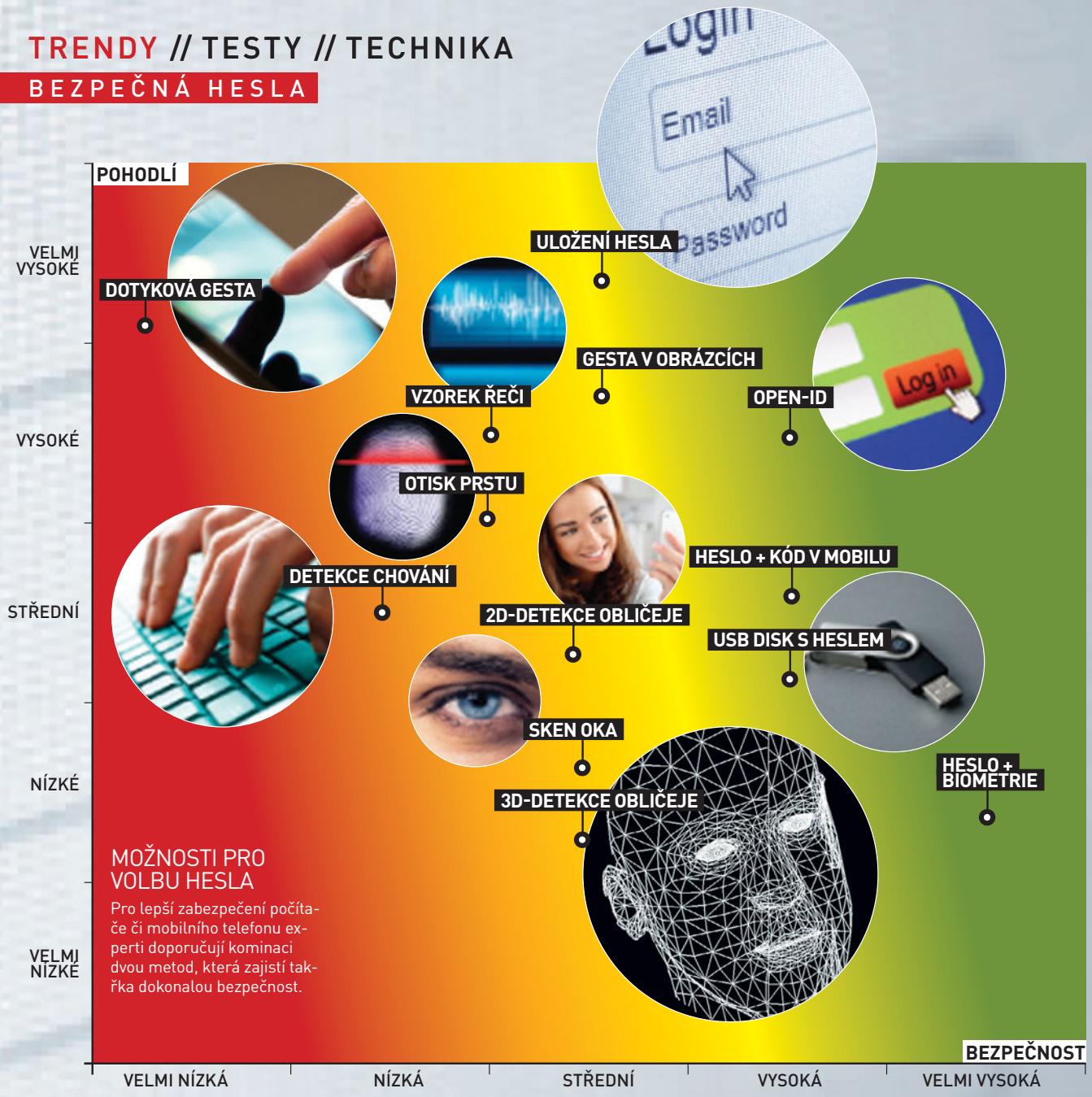


SBOHEM, hesla

Útoky hackerů a hardwarové a softwarové zranitelnosti představují hrozbu pro vaše internetové účty. Co tedy dělat? Uložit si heslo do bezpečí na USB disk, nebo jeho ochranu vzdát?

CLAUDIO MÜLLER, PETR KRATOCHVÍL

Velmi oblíbená rada pro zabezpečení hesel pochází od vědce Clifforda Stolla: „Chovejte se ke svému heslu jako ke kartáčku na zuby: pečlivě ho vybírejte, nenechávejte ho nikde povalovat a měňte ho každých šest měsíců." Neodpustíme si ještě komentář k obecným tipům na téma bezpečnosti hesel – podle expertů mají přibližně stejný efekt jako výroky v čínských koláčcích štěstí. Pocit pohody z jejich lehce stravitelné moudrosti je vysoký, jejich skutečný ochranný efekt ale poměrně nízký. Obecné tipy pro hesla ke komplexnímu světu se stovkami oblíbených webů, internetových obchodů, aukčních serverů či bank jsou příliš zjednodušující.

Faktem je, že v praxi člověk nemůže mít všechna hesla doma jako zubní kartáčky. Obvykle je uživatelé ukládají v prohlížeči nebo na serverech samotných webových služeb. Ty jsou ale často pod palbou hackerů, a i když uživatel zachová maximální obezřetnost, stejně nemá jistotu, že se jeho heslo nedostane do jejich rukou. Své zkušenosti s tím mají například návštěvníci webů Sony, Yahoo, Gamigo, LinkedIn nebo naposledy i Evernote (viz vpravo). V některých případech zkrátka nezáleží, zda máte jako heslo 12345, nebo složitou kombinaci čísel, písmen a speciálních znaků. Ve světle těchto skutečností je ale nutné přiznat, že během několika posledních měsíců většina firem na ochraně dat svých zákazníků značně zapracovala a lze očekávat, že nejslabším článkem bude opět uživatel.

Základy pro bezpečné heslo

Bezpečnost na cizím serveru tedy neovlivníte, můžete ale alespoň ztížit práci hackerům a snížit riziko odhalení hesla hrubou silou. Prvním a základním tipem je nepoužívání existujících slov – a to i v případě, že nahradíte písmeno „i“ jedničkou a písmeno „e“ trojkou. Pokud hacker použije metodu slovníkového útoku, odhalí vaše heslo během několika málo minut. Bude-li vaše heslo kratší než šest znaků, pomocí útoku hrubou silou ho lze odhalit za méně než minutu. Jestliže si bezpečností svého hesla nejste jisti, podívejte se na web **www.howsecureismypassword.net**. Dalším důležitým tipem je nepoužívat stejné heslo na více serverech – pokud ho hacker odhalí, jsou v ohrožení všechny vaše účty.

Markus Jakobsson, vedoucí vědecký pracovník pro zabezpečení uživatelů u PayPalu, nám odhalil svou strategii pro používání hesel: vytvořte si silné hlavní heslo a pro konkrétní stránky k němu přidávejte dodatek. Hlavní heslo by mělo vypadat například takto: „HcPb84!“ (nepoužívejte žádné iniciály nebo data narození). K němu poté přidejte konkrétní znaky z webového serveru – například první dvě a poslední dvě písmena. Heslo na Facebook by tak mohlo vypadat například takto: „HcPb84!Faok“.

Obezřetní buďte také při volbě bezpečnostní otázky pro obnovení hesla, která je často součástí registrace na internetových stránkách. Typickou chybou je použití volby oblíbené barvy, která hádání hesla hackerům příliš neztěžuje. Využíváte-li velké množství internetových služeb, měli byste mít dobře zabezpečený e-mailový účet svázaný s těmito službami. Uvědomte si, že osoba, která kontroluje e-mailový účet, můžete také snadno změnit přihlašovací údaje na zvolené službě. Výsledkem pak může být situace, kdy hackeři zneužijí vaši identitu k nákupům v internetových obchodech nebo k nelegální činnosti například na sociálních sítích.

E-mail: Lepší ochrana ve hvězdách

Je zcela nepochopitelné, že celá řada e-mailových služeb neposkytuje dvě úrovně zabezpečení. Bezpečnostní experti upozorňují, že i přes rostoucí význam e-mailu (často jako zadní brány k důležitým službám) je jeho zabezpečení už několik desítek let na stále stejné úrovni – hackerům stačí získat heslo, a pak už jim nic nebrání v cestě. Dvoufaktorová autentizace (viz strana 32) je podporována jen u několika poskytovatelů. Tuto metodu znají například čeští uživatelé internetbankingu, kdy pro přihlášení ke svému účtu musí zadat nejen heslo, ale také kód, který obdrží prostřednictvím SMS.

Pozitivní přístup k bezpečnosti vašeho e-mailového účtu má nově i Google – u něj se funkce jmenuje „Ověření ve dvou krocích“

17 % **VŠECH UŽIVATELŮ POUŽÍVÁ JAKO HESLO EXISTUJÍCÍ SLOVA NEBO JMÉNA.**

NEJVĚTŠÍ HACKY HESEL

Sony Playstation Network (77 milionů účtů):
Matka všech hacků hesel ohrozila všechny majitele síťových PS účtů v dubnu 2011. Útočníci kromě hesel získali přístup i k číslům kreditních karet zákazníků. V důsledku útoku odpojila společnost Sony službu od sítě a ta zůstala mimo provoz po dobu 24 dní.

Evernote (50 milionů účtů):
Služba pro ukládání dat a poznámek odhalila hackerský útok v březnu letošního roku. Při útoku bylo odcizeno 50 milionů datových záznamů (uživatelská jména, e-mailové adresy, zašifrovaná hesla).

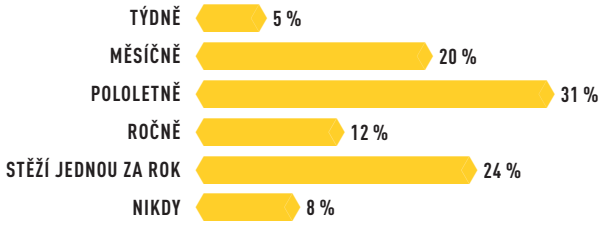
Gamigo (8 240 000 účtů):
Německý provozovatel on-line her Gamigo (Jagged Alliance, Ufo) byl hacknut v únoru 2012. Hesla a e-mailové adresy se objevily na webu v červenci a staly se tak největší zveřejněnou sbírkou takovýchto dat.

LinkedIn (6,5 milionů účtů):
Síť profesionálů byla hacknuta v červnu 2012, hesla byla zveřejněna na ruském webovém fóru.

Yahoo (450 000 účtů):
Ukradená hesla služby Yahoo Voices, zveřejněná v červenci 2012, byla uložena nešifrovaná, hackeři je tedy mohli přímo používat.

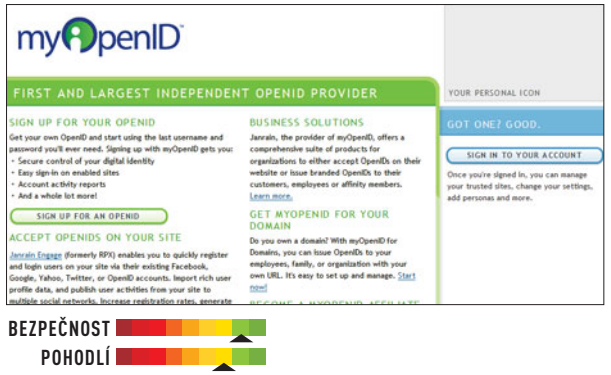
Twitter (250 000 účtů):
V únoru, krátce poté, co došlo k útoku čínských hackerů na známé internetové služby ze Spojených států amerických, jako je Facebook, Twitter, Apple nebo New York Times, se na webu vynořilo 250 000 datových záznamů z účtů na Twitteru.

FREKVENCE, S NÍŽ UŽIVATELÉ MĚNÍ SVÁ HESLA



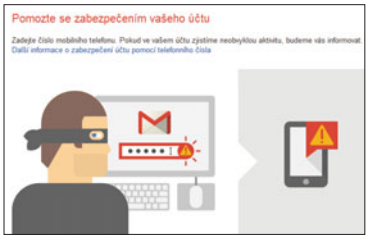
OPENID

Při využívání OpenID se nepřihlašujete pomocí uživatelského jména a hesla, ale pouze prostřednictvím svého OpenID. Tuto technologii bohužel příliš mnoho webů nepodporuje.



DVOUFAKTOROVÁ AUTENTIZACE

Vyšší úrovně bezpečí dosáhnou pouze ti, kdo používají dvě cesty pro zadání hesla. Nejčastější je zadání číselného kódu, který můžete obdržet prostřednictvím SMS nebo aplikace v telefonu.

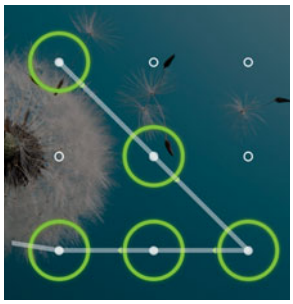


POSKYTOVATEL	METODA
SLUŽBY GOOGLE	Prostřednictvím SMS nebo autentizační aplikace
MICROSOFT	Prostřednictvím SMS, aplikace, nebo alternativního e-mailu
PAYPAL	Pomocí generátoru kódu nebo SMS
FACEBOOK	Prostřednictvím SMS nebo aplikace
DROPBOX	Prostřednictvím SMS nebo autentizační aplikace Googlu
LASTPASS	Prostřednictvím autentizační aplikace Googlu
YAHOO	Prostřednictvím SMS nebo bezpečnostní otázky
WORDPRESS	Prostřednictvím autentizační aplikace Googlu
APPLE ID, ICLOUD	Prostřednictvím SMS (ale pouze v USA a Velké Británii)

BEZPEČNOST
POHODLÍ

SWIPE

Swipe gesta jsou jednoduchá, a proto i nebezpečná. Navíc hrozí riziko, že na displeji za dobrých světelných podmínek lze vidět stopy prstů. Pak si člověk musí jen vyzkoušet směr gesta, a zařízení se odemkne.



BEZPEČNOST
POHODLÍ

HESLO NA USB KLÍČI

Ochrana systému Windows pomocí hesla na USB klíči je jednoduchá. Člověk se musí jen ujistit, že tuto malou a důležitou věc neztratí.

BEZPEČNOST
POHODLÍ

OBRÁZKOVÉ HESLO VE WINDOWS 8

Zopakovat tři různá gesta na jednom snímku je pro útočníky obtížné a pro uživatele na dotykovém zařízení je to mnohem jednodušší než napsání složitého hesla.

a jste na ni upozorněni při vstupu do svého profilu. V rámci nastavení účtu ji poté najdete v sekci »Zabezpečení | Ověření ve dvou krocích | Nastavení«. Pak už stačí sledovat pokyny průvodce, a během chvíle je váš e-mailový účet o něco bezpečnější.

U dvoufaktorového zabezpečení je ale nutné zmínit nižší uživatelský komfort: musíte u sebe vždy mít mobilní telefon a v případě změny čísla nezapomenout změnit nastavení i v rámci služby. Pohodlnějším řešením může být specializovaná aplikace pro ukládání hesel: například program LastPass, který najdete na **lastpass.com**. LastPass ukládá vaše přihlašovací údaje na chráněné on-line úložiště s 256bitovým šifrováním a „master" heslem. Pro použití stačí buď doplněk do prohlížeče, nebo aplikace (pro mobilní zařízení), a přihlášení k libovolnému webu je dětskou hračkou. Pokud chcete, LastPass automaticky vyplní všechna požadovaná políčka ve formulářích, což má dvě výhody: nemusíte si pamatovat už žádná data a trojské koně s keyloggery mají smůlu. I zde je ale obrovské riziko v případě odhalení hlavního hesla (na počítači nebo na serveru poskytovatele služeb) – v tom případě budou hackeři znát všechny vaše přihlašovací údaje.

Podobnou taktiku využívá i technologie OpenID. V rámci ní získáte osobní identifikaci, kterou lze použít pro přihlášení i na jiných webech. OpenID můžete v současnosti získat například založením účtu u Googlu, Yahoo nebo Flickru. U nás je propagátorem OpenID především Seznam, celkový počet webů, na které se takto můžete přihlásit, ale není příliš velký.

Smartphone: Ochrana pohybem prstu

Kromě webových služeb a počítače by měla být stejně dobře chráněna i vaše mobilní zařízení. Často totiž obsahují detailní i citlivé informace z vašeho digitálního života a jejich ochrana je obvykle absurdně slabá. Nedávno jste se například mohli v rubrice Bezpečnost dočíst o bezpečnostní mezeře, která umožnila snadno obejít ochranu nejlepších telefonů (například Samsungu Galaxy S III) pomocí funkce tísňového volání na displeji uzamčené obrazovky. Zde vám bohužel mnoho rad nenabídneme, protože lepší způsoby ochrany (například biometrické postupy) jsou prozatím většinou ve stavu vývoje či beta-verzí.

Ve většině mobilních zařízení tak v současnosti můžete nastavit kromě ochrany karty SIM PIN kódem pouze blokovací kód nebo gesto pohybu přes mřížku s devíti body. V této situaci je navíc paradoxem, že v rámci analýzy bezpečnostní firmy Symantec týkající se odcizených smartphonů bylo zjištěno, že 40 procent těchto zařízení bylo zabezpečeno kódem [1234]. I když má zloděj telefonu jen tři pokusy na zadání hesla, takovýto kód lze poměrně rychle odhalit. Stejně málo bezpečné je využití výše zmíněných gest pohybu, protože je zloděj může odhalit pomocí otisků prstů na displeji. Ve srovnání s Apple a Googlem je Microsoft v oblasti ochrany mobilních zařízení již o krok napřed. Například v systému Windows 8 lze použít obrazové heslo, které je stejně bezpečné jako komplexní heslo zadávané z klávesnice. V rámci této ochrany na obrázku vyznačíte gesto – například bod, kruh nebo přímku mezi dvěma obrazovými prvky.

Tip: Nepoužívejte bodová gesta, ale pouze čáry a kruhy. Jsou bezpečnější, neboť obsahují jak pozici, tak směr. Dále nedoporučujeme používat předvídatelná gesta, jako kruh kolem obličeje.

Naše tipy a triky vám rozhodně nezaručí, že se vaše hesla nedostanou do rukou hackerů, minimálně však sníží pravděpodobnost útoku na ně. Po prvním neúspěchu si stejně jako v reálném životě útočníci raději vyberou jednodušší cíl.

PETR.KRATOCHVIL@CHIP.CZ

PLACENÁ INZERCE

BEZPEČNÁ HESLA

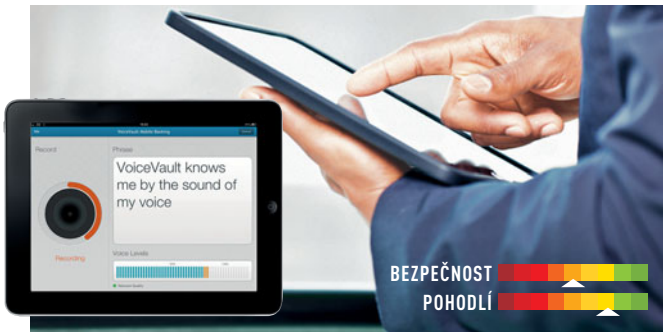
Přihlašování pohledem

Oční skenery už delší dobu najdete například na letištích a zabezpečených pracovištích. Dokážou identifikovat osoby pomocí rozpoznání kapilár v sítnici nebo struktury duhovky. Tato identifikace je v optimálních podmínkách téměř bezchybná, ale špatný odraz světla, nebo dokonce poškození oka může zabránit identifikaci. Navíc by mohl být skener duhovky přechytračen pomocí fotografie oka. A kvalitní skener, který pracuje většinou s infračervenou technologií, není bohužel vhodný pro použití v mobilních zařízeních – kromě aplikace EyeVerify, pro kterou jsou dostatečné již integrované fotoaparáty od dvou megapixelů. Tato aplikace fotografuje oči a majitele později identifikuje pomocí žilek v očních bulvách. Výhodou je, že pro odemknutí telefonu pomocí aplikace se musí shodovat pouze jeden ze čtyř sledovaných znaků (levé a pravé části oční duhovky na obou očích). V případě zranění oka tak můžete odemknout a zavolat si lékaře. Aby bylo možné rozlišit fotografii od skutečného člověka, software náhodně mění osvětlení a ostření a kontroluje reakce oka. EyeVerify by se měl na trhu objevit v létě 2013.

3D analýza tváře

Poprvé na operačním systému Android 4.0 se objevila aplikace schopná odemknout smartphone díky rozpoznání obličeje. Funkce Face Unlock je spolehlivá, někdy ale vyžaduje řadu pokusů. Zpočátku bylo možné přelstít Face Unlock pomocí fotografie, nyní je potřeba mrkat, aby uživatel dokázal, že je opravdu člověk. Uživatelé PC mohou pro rozpoznávání obličejů použít software Blink (najdete ho na **www.luxand.com/blink**). Tento program používá 2D rozpoznání obličeje, při kterém ověřuje asi 80 vlastností (například vzdálenost mezi očima, šířku nosu...), a na základě těchto hodnot vytváří odpovídající vzor.

Vzhledem k tomu, že 2D rozpoznávání není ani bezchybné, ani příliš odolné proti neoprávněnému zásahu, trendem je technologie 3D skenování obličeje, která je také méně závislá na dostatku světla. Tato technologie například i díky analýze povrchu kůže umožňuje dokonce rozlišení mezi identickými dvojčaty. Tuto technologii už v současné době využívá armáda a některé bezpečnostní složky, lze ji ale najít v i aplikaci FaceR MobileID od firmy Animetrics.



Hlasový kód pro internetbanking

Jednou z nejoblíbenějších metod zabezpečení v akčních filmech je rozpoznání hlasu. Bohužel v praxi je při každodenním použití obtížné rozpoznat hlasy kvůli ruchu pozadí. Takzvaná hlasová analýza četnosti a algoritmy rozpoznávání ale již dlouho spolehlivě fungují v klidném prostředí, proto vědci intenzivně pracují na zlepšení potlačení šumu. Pokud budou ve své aktivitě úspěšní, bude tato funkce zajímavá pro bankovní transakce se smartphonem. První pokusy v této oblasti už podnikl poskytovatel finančních služeb GFT. Uživatel nejprve obdržel čtyřmístný číselný kód, který bylo nutné pro vytvoření řečového vzoru třikrát zopakovat do telefonu při registraci. Při každé operaci s penězi poté uživatel přijme automatický hovor, v rámci něhož musí tento kód zopakovat. Podle bezpečnostních expertů z firmy GFT má prototyp v současné době přesnost kolem 85 procent. Jakmile se ještě zlepší, hodlají produkt nabídnout na trhu.

Podobné řešení předložila v březnu i firma VoiceVault. To ale umožňuje pro kontrolu hlasu využít komplexní fráze, nebo dokonce celé věty v jakémkoli jazyce, což ještě dále zvyšuje spolehlivost zabezpečení.

Skenování otisku prstu

Skenery otisků prstů najdete na noteboocích, klávesnicích nebo externích USB zařízeních už celou řadu let. Očekává se, že skener otisku prstu může mít Phone5 i na domovském tlačítku. Zajímavým projektem je myIDkey, v rámci kterého je USB flash disk zajištěn otiskem prstů, a na disk jsou ukládána hesla, dokumenty nebo obrázky v zašifrované verzi. K počítači lze disk připojit jak přes USB, tak i přes Bluetooth. Nástroj dokáže vytvořit bezpečné heslo pro zvolenou aplikaci, a dokonce po určeném počtu chybných pokusů umí odstranit uložená data. Na trhu bude myIDkey k dispozici od srpna, přibližně za 100 amerických dolarů.

BEZPEČNOST
POHODLÍ

Vzorec chování

Jen málokdo ví, že interakce uživatele se zařízením vytváří jedinečný vzor. Pro jeho rozpoznávání vyvinula software švédská firma BehavioSec. V rámci jeho kontroly lze využít nejen správnost hesla nebo gesta, ale i to, jak jsou tyto údaje zadány. Mezi analyzované faktory patří například rychlost psaní a jeho kadence, případně zrychlení myši a frekvence klikání. V případě dotykového displeje software rozpozná tlak a úhel gest. Tato metoda patří k nejjednodušším způsobům, jak zajistit další úroveň zabezpečení.

BEZPEČNOST
POHODLÍ