Bezpečnost autentizace

Bezpečnostní politika hesel a vícefaktorová autentizace

Marie Kratochvílová

V tomto článku se dozvíte, co je vícefaktorová autentizace a zda a pro koho se ji vyplatí zavádět. V úvodu si ujasníme pojmy „autentizace“ a „autorizace“. Autentizace je proces, v rámci něhož je ověřována identita subjektu. Autorizace je proces, který uživateli povoluje určité akce. Autorizace rozhoduje o přidělování různých oprávnění uživatele na základě přístupových práv. Tento článek se bude zabývat metodami autentizace, nikoli autorizace.

Vícefaktorová autentizace je v dnešní době stále aktuálním tématem. Neustále roste počet sofistikovaných kybernetických útoků a množství hrozeb v informačním světě. Útočníci se stále častěji soustřeďují na běžné uživatele, kteří představují nejslabší článek bezpečnostního řetězce. Za typickou slabinu běžných uživatelů v autentizačním procesu se považuje problematika hesel. I když se na tento problém dlouhodobě upozorňuje, k výraznější nápravě nedochází. Stále se k nim přistupuje nezodpovědně. Uživatelé často volí krátká a pro ně dobře zapamatovatelná hesla, která mohou souviset s elementem z jejich osobního/soukromého života. Heslo může obsahovat slovo nebo frázi spojenou s křestním jménem, místem bydliště, oblíbeným zvířetem apod.

Základní druh přístupu k určitému chráněnému zdroji představuje autentizace se znalostí přístupového jména a hesla. A právě utajované heslo, které by si měl uživatel pamatovat, bývá pro některé z nich překážkou. Tento fakt vede k důvodu, že většina uživatelů volí snadno zapamatovatelná „slabá“ hesla, která mohou být snadno kompromitována.

Společnost SplashData [2], která vyvíjí software pro správu hesel, provedla analýzu nejčastěji používaných výrazů. Následující seznam definuje 10 nejhorších hesel pro rok 2015. V závorkách je zaznamenané jejich pořadí a změna od roku 2014:

1.	123456	(Beze změny)
2.	Password	(Beze změny)
3.	12345678	(↑ 1)
4.	qwerty	(↑ 1)
5.	12345	(↓ 2)
6.	123456789	(Beze změny)
7.	football	(↑ 3)
8.	1234	(↓ 1)
9.	1234567	(↑ 2)
10.	baseball	(↓ 2)

Už z toho je jasné, že krátká a snadno zapamatovatelná hesla nebudou pro útočníky těžkým oříškem k rozlousknutí. Je důležité tedy nalézt kompromis nejenom v jejich délce, v pravidelné obměně, ale nemělo by se spoléhat pouze na jediný způsob autentizace uživatele.

Bezpečnostní politika hesel

Útočníci se snaží získat přístup do systému z mnoha důvodů. Mezi ně obvykle patří vidina finančního zisku, špionáž, pomsta, informační válka nebo výzva. Mnohé z útoků jsou zaměřeny právě na prolomení hesel. Společnosti s nastavenou bezpečnostní politikou své uživatele zavazují k používání silných hesel, jejich pravidelné obměně i pravidlům o nakládání s nimi. V následujících odstavcích se podíváme na několik základních pravidel pro práci s hesly.

Důvěrnost

Každý uživatel nějakého systému by měl k heslům přistupovat jako k nejcitlivějším osobním údajům. Heslo by nemělo být sděleno žádné osobě, ani osobě, které důvěřujete, protože tato důvěra může lehce pominout.

Správná volba

Heslo by se mělo volit tak, aby neobsahovalo informace v souvislosti s vaší osobou. Vyberte takové, které nebude jednoduše odhalitelné osobě, která vás dobře zná. Pokud by heslo nebylo správně zvolené, možné riziko spočívá v jeho odhadnutí. Útočník zkusí jednoduše tipovat. Jak již bylo zmíněno dříve, uživatelé volí

taková hesla, která jsou pro ně dobře zapamatovatelná. Tedy taková, která jsou s nimi blízce spojená (např. rodné číslo, křestní jméno, jména dětí, partnerů a domácích mazlíčků).

Heslo by nemělo tvořit slovo nebo frázi

Ideální je kombinace náhodných velkých a malých písmen, čísel a speciálních znaků. Pokud zvolíte jako heslo slovo „password“, je jasné, že jej útočník prolomí celkem rychle. Nicméně v kombinaci velkých a malých písmen, čísel a speciálních znaků – heslo ve tvaru například „p@$sW0r5!“ – by jeho prolomení bylo obtížné. Typickou technikou prolomení hesla v tomto případě může být tzv. slovníkový útok. Jedná se o metodu odhalování hesel, kdy útočník zkouší všechna pravděpodobná hesla z připraveného seznamu nejčastěji používaných hesel – tzv. slovníku.

Minimální délka hesla alespoň 8 znaků

Obecně ale platí, čím delší heslo je, tím hůře ho lze prolomit. Čas potřebný k jeho prolomení roste exponenciálně s rostoucí délkou hesla. Proto se doporučuje používat alespoň 8 znaků. Pokud je heslo příliš krátké, hrozí riziko útoku hrubou silou (angl. Brute Force Attack). Útok se provádí tak, že útočník na svém počítači použije skript, který generuje hesla (nebo šifry) z možných kombinací písmen, čísel a jiných znaků. Skript zasílá průběžně dotazy na server či počítač oběti a zkouší různé kombinace. Útok hrubou silou se často kombinuje se slovníkovým útokem. Obranou proti útoku hrubou silou je právě zmiňovaná délka hesla doporučovaná v kombinaci s velkými a malými písmeny, číslicemi a nealfanumerickými znaky. Další jednoduchou ochranou je časový zámek, který po určitém počtu neúspěšných pokusů vynutí časovou prodlevu (obvykle 20 sekund až 1 minutu), po které je možné v zadávání pokračovat. Útok hrubou silou tedy potřebuje dlouhé časové období na zkoušení kombinací a bývá brzy odhalen.

Obměna / Správa hesel

- Hesla by se neměla nikomu sdělovat a ani zaznamenávat na štítek papíru.
- Hesla by se měla pravidelně obměňovat. Někteří odborníci doporučují obměnu ideálně 1/14 dní nebo 1/3 měsíce. V bezpečnostních politikách firem se však častěji setkáváme s obdobím jednou za půl roku nebo jedenkrát ročně.
- Pro každý účel je doporučováno používat jiné heslo. Není vhodné používat stejné heslo pro přístup např. k soukromé e-mailové schránce a do firemní sítě. Toto pravidlo bývá nejvíce porušované, a přitom pro obranu je přímo zásadní. Pokud budete používat různá hesla, útočník nemusí automaticky získat přístup ke všemu.

MFA neboli vícefaktorová autentizace

K lepšímu zabezpečení přichází na pomoc vícefaktorová autentizace (z angl. Multi Factor Authentication, zkráceně MFA). Jedná se o metodu ochrany přístupu k určitému prostředku (zdroji), jako je například informační systém nebo web.

Do oblasti vícefaktorové autentizace spadá nejznámější dvoufaktorová autentizace. U dvoufaktorové autentizace hraje každý uživatel roli toho, kdo „něco ví“ (např. přístupové jméno a heslo) a „něco vlastní“ (např. generátor jednorázového hesla). Účinná autentizace uživatele je například prostřednictvím tokenů a biometrik. Navíc v kombinaci spolu s heslem posouvá úroveň zabezpečení na mnohem vyšší úroveň. Ale vše má své meze, i zde se vše odvíjí od finančních možností daného subjektu. Cílem vícefaktorové autentizace je zlepšit proces ověřování identity daného uživatele a snížit pravděpodobnost kybernetického útoku. Vícefaktorová autentizace kombinuje zabezpečení ve třech autentizačních faktorech:

1. **Znalostní faktor** zahrnuje něco, co uživatel zná. Jedná se například o heslo nebo PIN ke kreditní kartě, popř. mobilnímu telefonu.
2. **Faktor vlastnictví** představuje něco, co má uživatel ve svém vlastnictví. Jedná se například o mobilní telefon, platební karty, HW tokeny, ale i o osobní doklady (např. řidičský či občanský průkaz), které ho identifikují.
3. **Biometrický faktor** je činitel, který představuje uživatele samotného, jinak řečeno, kým uživatel sám je. Za typickou biometrickou identifikaci uživatele lze považovat otisk prstu, sken oční sítnice, hlasový vzorek či rozpoznání obličeje.

Tyto tři faktory dobře charakterizuje obr. 1, na kterém je Vennův diagram, jehož průnikem je vícefaktorová autentizace.

Výhoda a hlavní síla MFA spočívá v její bezpečnosti. Aby útočník zjistil citlivá data nebo přístup ke chráněnému zdroji, musel by disponovat přístupem ke všem zmiňovaným faktorům, kterými se uživatel ověřuje. Tímto způsobem zabráníme útočníkovi v tom, aby převzal kontrolu nad chráněným zdrojem

Obr. 1: Vennův diagram

v případě, že by obešel jeden vyžadovaný autentizační mechanismus.

Vícefaktorová autentizace v praxi

V praxi se setkáme nejčastěji s použitím kombinace faktoru znalosti a vlastnictví. Jako příklad můžeme uvést transakci platební kartou, kde uživatel musí něco mít, tj. debetní karta, a něco znát, tj. PIN kód. Nejrozšířenějším druhým faktorem je faktor vlastnictví, kdy má uživatel v držení vlastní zařízení (například mobilní telefon), které dokáže získat jednorázové heslo s omezenou časovou platností. S tímto případem se můžeme setkat u bank, kde se pro přístup k internetovému účtu musí uživatel přihlásit prostřednictvím jména nebo čísla účtu a hesla. Následně je mu na mobilní telefon zaslaná SMS s jednorázově vygenerovaným heslem, které obsahuje obvykle 6–8 číslic. Základní výhoda těchto hesel zasílaných pomocí SMS spočívá v jejich jednoduchosti. Uživatel jednoduše dostane SMS zprávu a opíše kód. Hlavní nevýhodou tohoto přístupu jsou náklady na straně provozovatele, tedy banky. Případně na straně klienta, pokud na něj provozovatel tyto náklady přenáší.

Vícefaktorová autentizace je v bankovní sféře standardem minimálně 10 let. Dnes se začíná uplatňovat také v oblasti služeb (sociální sítě, elektronická pošta), které obsahují citlivá data a vyžadují ochranu proti nechtěné ztrátě důvěrnosti. Zde se zavádí například používání autentizačních softwarových (SW) tokenů. SW token má podobu aplikace, která pracuje v mobilním telefonu a je spárována s autentizačním serverem a generuje náhodné klíče, kterým daný autentizační protějšek rozumí. SW tokeny řeší některé nevýhody HW tokenů, jako jsou pořizovací cena, distribuce zařízení nebo riziko man-in-the-middle útoku. Použití SW nebo HW tokenů nalezneme převážně v korporátní sféře.

Biometrická autentizace

Problém, který s sebou nese neochotu uživatelů zapamatovat si složitá „bezpečná“ hesla, částečně řeší biometrická autentizace, která se specializuje na **fyziologické a na behaviorální vlastnosti** člověka. Využívá jedinečných tělesných nebo behaviorálních znaků pro identifikaci osoby. Fyziologické vlastnosti se vztahují k tvaru těla a mohou zahrnovat otisk prstů nebo rozpoznání obličeje. Behaviorální vlastnosti se zaměřují na chování člověka a mohou zahrnovat rozpoznání hlasu, dynamiku podpisu nebo psaní na klávesnici.

Jak funguje biometrická autentizace? Aby se uživatel mohl začít autentizovat, musí nejprve projít procesem tzv. **enrolmentu** (zaznamenání vzorku zvolené charakteristiky). Tento vzorek je uložen jako údaj v databázi pro pozdější účely ověření. Pakliže se uživatel identifikuje, jeho předložená charakteristika se porovná s údaji uloženými v databázi. Shodují-li se, uživateli je udělen přístup do systému / k chráněným datům.

Výhoda biometrické autentizace není pouze v tom, že si uživatel nemusí pamatovat složitá a několikamístná hesla, ale i ve skutečnosti, že biometrické znaky uživatele zůstávají během života neměnné a nelze je zapomenout. Jinými slovy nejsou v podstatě na uživatele kladeny žádné mentální požadavky.

Nutno dodat, že se musí brát v úvahu i možnost ztráty hlasu nebo prstu. V případě, že uživatel přijde o prst nebo ztratí hlas, poskytuje většina autentizačních metod alternativní způsob ověření. Do nevýhod biometriky lze zařadit složitost a náročnost na pořízení technických a finančních prostředků pro snímání, různou chybovost přijetí (nesprávné ztotožnění uživatele se vzorkem jiného uživatele) a odmítnutí (nespárování uživatele s jeho vlastním vzorkem) identifikace osoby. Biometrické charakteristiky jsou citlivá data, a mohou tak obsahovat informace o osobě uživatele. Použití biometrických systémů představuje určitou ztrátu anonymity [8], neboť pár identit v běžných systémech může být jednoduše svázáno s jedním uživatelem.

Nejrozšířenějšími implementacemi stále zůstávají **dynamické biometrické podpisy** (DBP), které jako první v ČR zavedli mobilní operátoři. V bankovní sféře je v České republice první zavedla MONETA Money Bank, následována dalšími bankami. Tatra Banka zavedla biometrické podpisy jako první na Slovensku, kdy v létě r. 2013 začala ověřovat své klienty na Call centru pomocí jejich hlasu. Biometrické podpisy používá i Air Bank a Česká spořitelna, která mimo jiné pracuje na zavedení hlasové biometrie na klientské lince, kterou plánují spustit ještě v letošním roce.

Dynamické podpisy při vyhodnocování využívají statických charakteristik, jako jsou velikost a sklon písma, poměr mezi nimi nebo obloučky, které mají vliv na výslednou podobu podpisu. Dále se sleduje a zaznamenává rychlost a počet tahů, přítlak v určité fázi podpisu nebo délka trvání, které jsou pro každého člověka jiné. Výhody biometrických podpisů spočívají v tom, že jsou časově a administrativně méně náročné.

V poslední době banky dávají přednost skenům otisků prstů před zabezpečením účtu klientů hesly. Soudobá podoba skenů otisků prstů je v jednoduchém nástroji např. pro uzamknutí mobilního telefonu nebo pro potvrzení bankovní transakce z mobilního telefonu. Potvrzení takové transakce funguje tak, že uživatel načte transakci pomocí QR kódu nebo pomocí aplikace a autorizuje ji svým otiskem prstu. Začínají se používat skeny pro rozpoznávání obličeje nebo jiné biometrické druhy k ověření identity uživatele.

Biometrie se stále zdokonaluje díky různým firmám a institucím z jejich finanční podpory výzkumu a vývoje. Jisté je i to, že biometrie pomalu nahrazuje klasická hesla.

Biometrika je vnímána pozitivně

Globální platební technologická společnost Visa Inc., provedla na přelomu dubna a května 2016 průzkum o biometrických platbách [4] v 7 evropských státech, kterého se zúčastnilo 14 236 respondentů. Průzkum ukázal, že 73 % dotázaných respondentů považuje za bezpečný způsob ověření identity dvoufaktorovou autentizaci platby s využitím biometrických prvků. Jinými slovy, čím dál více lidí vnímá biometriku jako důvěryhodnou formu autentifikace. Nejoblíbenější bezpečnou metodou biometrické autentifikace je sken otisku prstů (volí ji 81% dotázaných), po ní následují snímání oční duhovky a rozpoznávání hlasu. Z průzkumu rovněž vyplývá, že od roku 2014 výrazně vzrostla důvěra spotřebitelů v biometrii (téměř o pětinu).

Prolomení dvoufaktorové autentizace

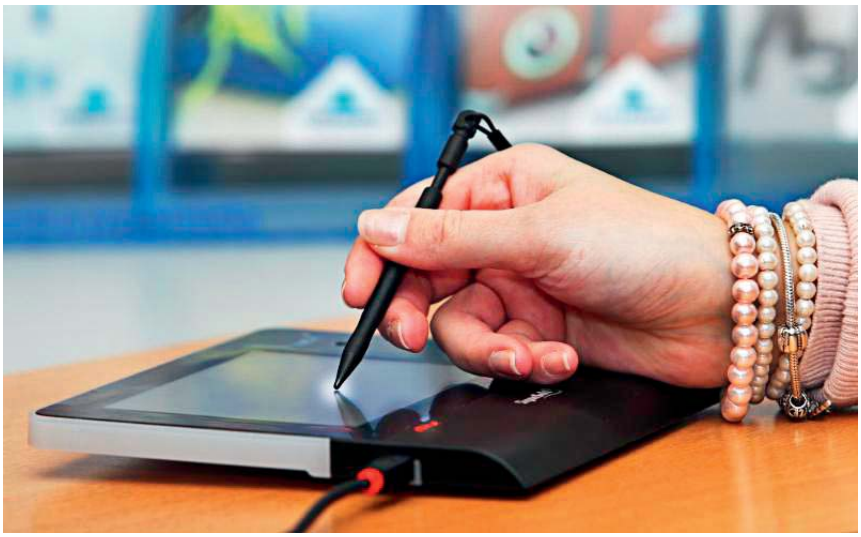
Na reálném příkladu z praxe si ukážeme, že ani technika dvoufaktorové autentizace neřeší všechny způsoby útoků. Následující případ prolomení autentizace v elektronickém bankovnictví se v praxi skutečně přihodil klientovi jedné nejmenované banky. Klientovi zavolala osoba vydávající se za zaměstnance banky s podezřením na zneužití klientovy platební karty. K tomu,

aby ověřila jeho identitu, jej vyzve k nadiktování zaslané autorizační SMS. Klient požadovanou informaci nadiktoval a osoba na druhém konci telefonu mu poděkovala a rozloučila se s ujištěním, že je vše v pořádku. Následně si tento útočník „převedl" finanční sumu v řádu tisíců Kč. Co se stalo? Útočník si nejprve skrze podvrženou phishingovou stránku zjistil přihlašovací údaje oběti, poté zneužil důvěry klienta v banku a získal nadiktovanou autorizační SMS. Ta nebyla použita pro ověření identity klienta, ale posloužila ke změně telefonního čísla pro zasílání autorizačních SMS. Z takto kompromitovaného bankovního účtu mohl útočník provádět finanční transakce.

Výše zmíněný příklad je spíše výjimkou. Mnohem častěji se setkáváme s krádežemi a zneužitím identity, které jsou poměrně jednoduché a lze je úspěšně provést pomocí metody phishingu. Phishing je většinou založen na zasílaných falešných e-mailech, které se mnohdy tváří jako důležité zprávy z banky a stejně tak mohou obsahovat odkaz na podvrženou přihlašovací stránku do internetové bankovnictví. Po kliknutí na daný odkaz je klient přesměrován na danou stránku a v dobré víře zadá své přístupové údaje. Tyto údaje si útočník uloží pro pozdější zneužití, a aby uživatel nic nepoznal, současně ho s nimi přihlásí do pravé bankovní aplikace.

Za bezpečností rizika lze považovat:

- Predikovatelnost znalostních faktorů (viz slabá hesla).
- Lidský faktor – příkladem je situace, kdy si zaměstnanec určité firmy napíše heslo nebo PIN kód na kus papíru.
- Ztráta nebo krádež samotného faktoru – např. mobilního telefonu, platební karty, tokenu. V souvislosti s online službami, kde se uplatňují SW tokeny, ztráta faktoru, jako je mobilní telefon, může znamenat i odepření přístupu k uživatelskému účtu.
- Možnost Man-in-the-Middle útoku [5] – jedná se o snahu útočníka odposlechnout komunikaci mezi účastníky tak, že se stane aktivním prostředníkem. Například když útočník vstoupí do komunikace mezi SW tokenem a autentizačním protějškem a odposlechne zaslaný kód.
- Možnost útoku Man-in-the-Browser [6] – tento typ útoku je zaměřen na finanční instituce. Jedná se o útok, kdy útočník nainstaluje do počítače oběti trojského koně, který je schopen modifikovat webové transakce uživatele v reálném čase.



Ilustrační foto: Využití signpadu pro biometrický podpis, zdroj: Modrá pyramida

Způsobem, kterým lze při použití vícefaktorové autentizace řídit riziko kybernetického útoku, je **adaptivní autentizace**, která je založena na *risk-based vícefaktorové autentizaci*. Adaptivní autentizace zároveň slouží k maximalizaci uživatelského komfortu omezením použití více faktorů pouze na nezbytné minimum v závislosti na aktuální úrovni rizika. **Risk-based vícefaktorová autentizace** znamená, že síla a způsob ověřování uživatele se určí až v okamžiku, kdy se připojí k internetovému bankovnictví. Pokud by se uživatel přihlásil normálně ze svého počítače se standardní IP adresou, postačila by autentizace jménem a heslem. V situaci, kdy systém určí jakoukoliv anomálii v uživatelově připojení, označí se toto připojení za rizikové a uživatel je následně požádán o dodatečnou autentizaci, například se mu zašle autorizační SMS kód.

Obrana v internetovém bankovnictví je poměrně složitá, protože vyžaduje odbornou znalost různých forem útoků, schopnost na ně reagovat a zavčas je eliminovat, ale i chránit klienty před jejich možnými dopady. Proto je vhodné mimo jiné zavádět specializované služby (monitoring, auditing, end-point protection, network security...), které se na danou problematiku zaměřují.

Závěrem

Vícefaktorová autentizace výrazně zvyšuje zabezpečení přístupu ke chráněnému zdroji, ale neřeší všechny formy útoků, jako je například phishing a social engineering obecně. Je třeba se zamyslet a zvážit, kdy má smysl investovat do vícefaktorové autentizace na základě citlivosti dat zpracovávaných systémem i firmou. ■

Zdroje:

1. WIKIPEDIA. *en.wikipedia.org* [online]. [cit. 11. 9. 2016].
2. MORGAN. *Announcing Our Worst Passwords of 2015* [online]. [cit. 11. 9. 2016].
3. RAK, Roman, Václav MATYÁŠ, Zdeněk ŘÍHA a kolektiv. *Biometrie a identita člověka – ve forenzních a komerčních aplikacích.* Praha: Grada Publishing, a. s., 2008. 664 s. Profesionál. ISBN 978-80-247-2365-5.
4. VISA. *Evropané důvěřují v zavádění biometrických plateb nejvíce bankám* [online]. [cit. 21. 9. 2016].
5. DUPAUL, Neil. *Man in the Middle (MITM) Attack* [online]. [cit. 11. 9. 2016].
6. OWASP. *Man in the Browser attack* [online]. [cit. 29. 9. 2016].

Marie Kratochvílová

Autorka článku je expertkou na informační bezpečnost ze společnosti AEC.