Autentifikácia, heslá a digitálne podpisovanie

Marko Hölbl

Anotácia

Tento kurz predstavuje koncepciu autentifikácie a hesiel, ako aj základné princípy a technológie. Okrem toho je predstavená úloha digitálneho podpisovania v autentifikácii a jeho základné spôsoby aplikácie a technológie.

Ciele

Tento kurz poskytuje základné informácie o autentifikácii, jej prvkoch a autentifikácii založenej na heslách a o tom, ako adekvátne chrániť heslá na strane používateľa ale aj autentifikátora. Diskutuje sa o koncepciách správy hesiel, viacfaktorovej autentifikácii a autentifikácii bez hesla.
Okrem toho sú prezentované informácie o technickom pozadí digitálneho podpisovania vrátane hašovacích funkcií, kryptografie s verejným kľúčom a infraštruktúry verejného kľúča. Nakoniec je prezentované digitálne podpisovanie ako prostriedok autentifikácie.

Kľúčové slová

heslá, autentifikácia, digitálne podpisy, infraštruktúra verejných kľúčov, hašovacie funkcie

Dátum vytvorenia

06.01.2022

Časová dotácia

15 hodín

Jazyková verzia

slovensky

Licencia

ISBN

Literatúra

[1] Batten, L. M. (2013). Public key cryptography: applications and attacks, John Wiley & Sons.

[2] Boonkrong, S. (2021). Authentication and Access Control: Practical Cryptography Methods and Tools, Springer.

[3] Buchmann, J., et al. (2013). Introduction to public key infrastructures, Springer.

[4] Burnett, M. (2006). Perfect password: Selection, protection, authentication, Elsevier.

[5] Grassi, P. A., et al. (2017). "NIST special publication 800-63b: digital identity guidelines." National Institute of Standards and Technology (NIST).

[6] Grimes, R. A. (2020). Hacking Multifactor Authentication, John Wiley & Sons.

KAPITOLA 1

Úvod

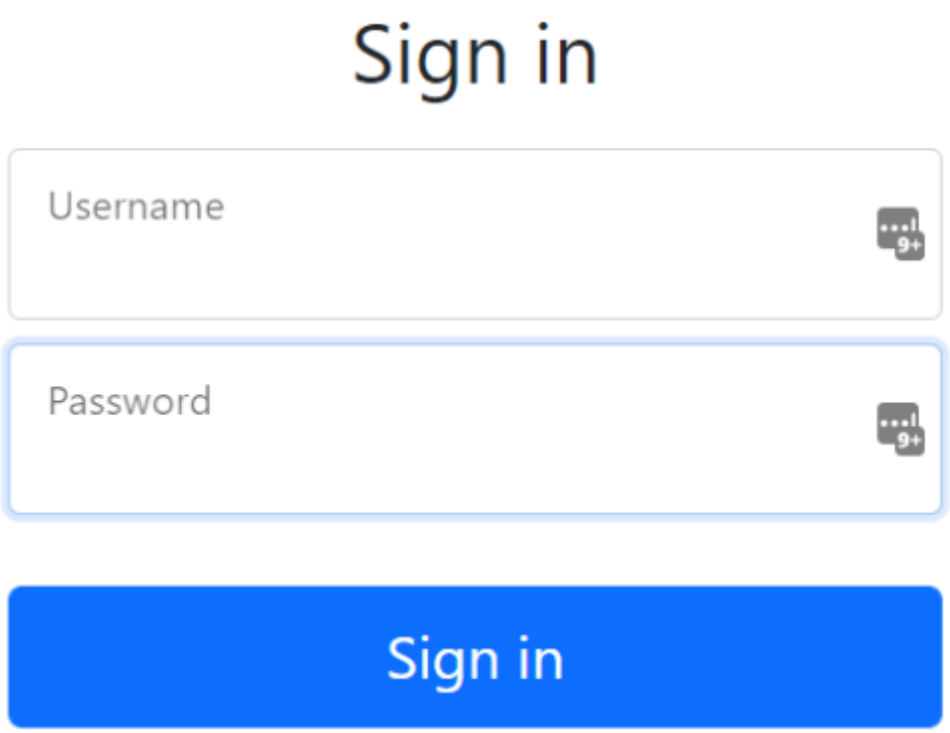
DEFINÍCIA

Autentifikácia je proces overovania identity niekoho alebo niečoho.

Vykonáva sa pomocou informácií poskytnutých subjektom, ktoré je potrebné skontrolovať. Proces autentifikácie v počítačových systémoch (súkromných a verejných) často vyžaduje, aby niekto, zvyčajne používateľ, použil na prihlásenie osobné údaje vydané systémom. Skutočnosť, že používateľ má heslo, má dokazovať, že je autentický. Najbežnejšou metódou overenia je kombinácia používateľského mena a hesla. Existujú však aj iné možnosti autentifikácie vrátane biometrie, čipových kariet, tokenov na jedno použitie atď.

Vo väčšine prípadov autentifikácia vyžaduje predloženie osobných údajov alebo aktíva na dokázanie tvrdenia, že ste tým, za koho sa vydávate. Aktíva alebo osobné údaje sú založené na množstve odlišných charakteristík, ktoré demonštrujú, čo poznáte, čo máte alebo čím ste.

- **Niečo, čo poznáte:** Môže to byť vaše mentálne vlastníctvo, napríklad heslo, ktoré pozná používateľ aj overovateľ. Ide o efektívne administratívne riešenie (vzhľadom na náklady). Je citlivé na výpadky pamäte a iné nedostatky, ako je napríklad bezpečné ukladanie súborov s heslami administrátorom systému. Používateľ môže použiť rovnaké heslo pre všetky systémové prihlásenia. Heslá, prístupové frázy a kódy **PIN** (***Personal Identification Numbers***) sú príkladmi takéhoto faktora (typu).

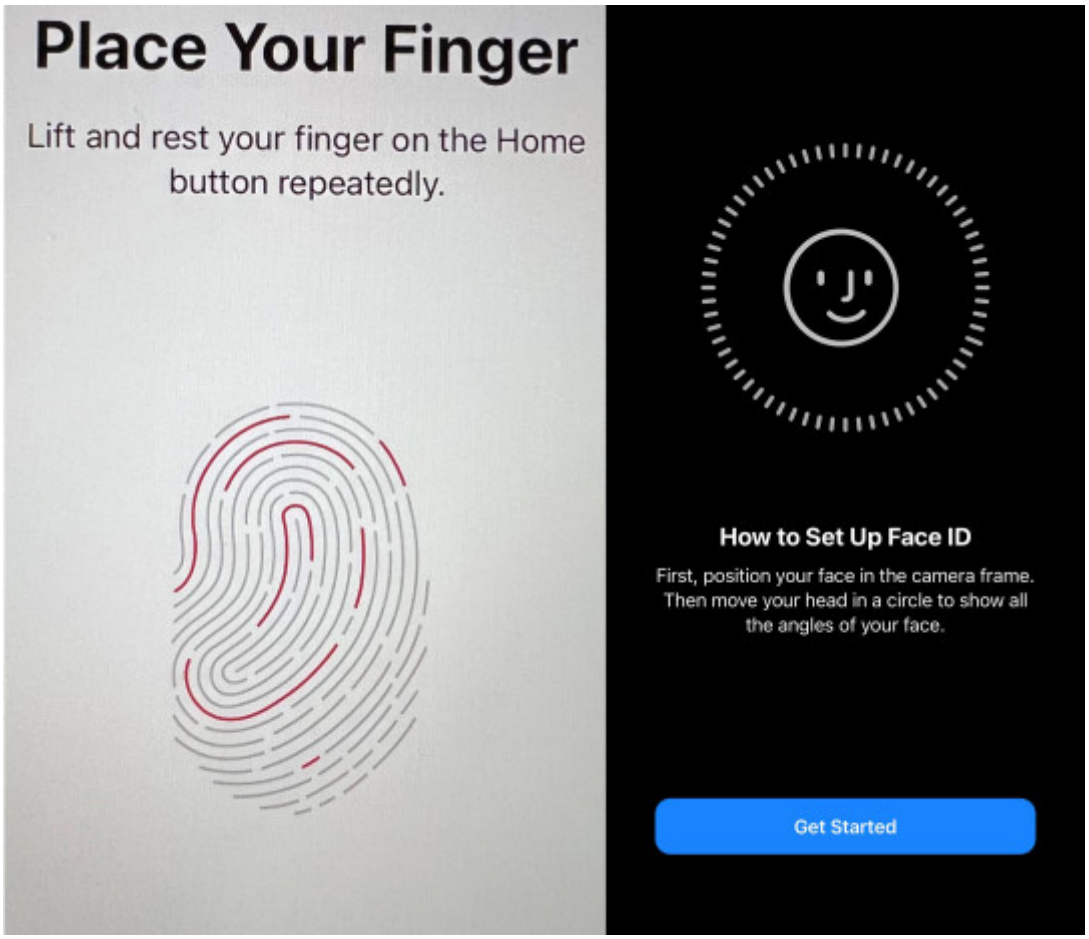


Obr. 1. Príklad prihlásenia používateľa pomocou používateľského mena a hesla

- **Niečo, čo máte:** Môže to byť akýkoľvek typ vydaného alebo získaného tokenu alebo štítku vlastnej identifikácie vrátane čipových kariet, hardvérových tokenov, mobilných telefónov a rôznych iných prostriedkov. Keďže je ťažké zneužiť jednotlivé fyzické identifikácie, táto forma je bezpečnejšia ako prvý prístup (niečo, čo poznáte). Napríklad stratiť čipovú kartu je ťažšie ako zapamätať si číslo karty.

Obr. 2. Príklady hardvérových tokenov pre typ autentifikácie „Niečo, čo máte“

- **Niečo, čím ste:** Ide o prirodzene získanú fyzickú vlastnosť, napríklad odtlačok prsta. Tento druh autentifikácie sa väčšinou označuje ako biometria. Hoci sa biometrické údaje používajú jednoducho, náklady na získanie biometrických čítačiek môžu predstavovať problém. Príklady tohto typu (faktora) sú odtlačky prstov, vzory sietnice, vzory DNA a rozpoznávanie tváre.



Obr. 3. Príklady biometrickej autentifikácie pomocou inteligentného telefónu

VÝHODY

Ak systém systematicky požaduje viaceré autentifikačné faktory, môže dosiahnuť robustnú bezpečnosť.

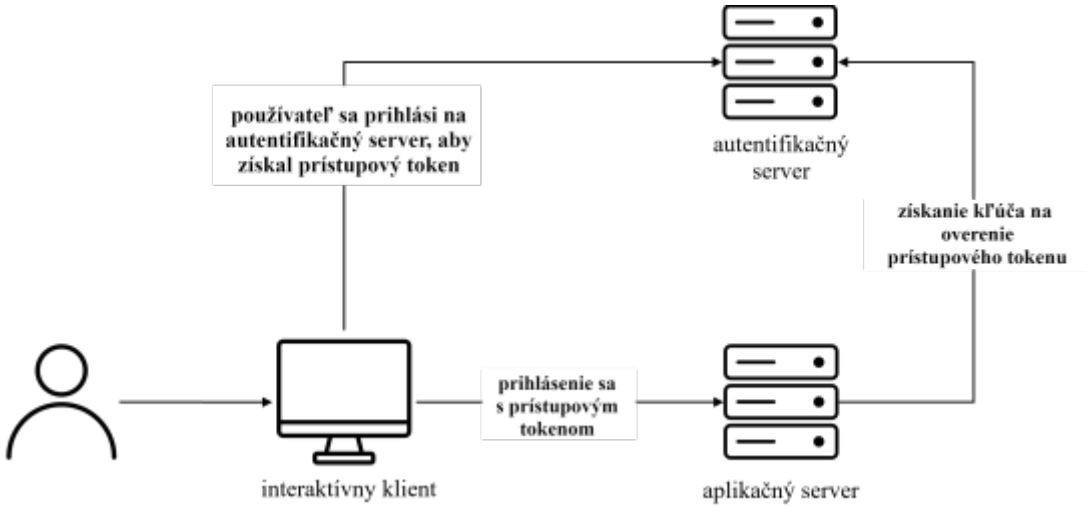
NEVÝHODY

Príliš častá autentifikácia však môže mať opačný efekt a ohroziť pohodlie používateľa.

Interaktivní prvek

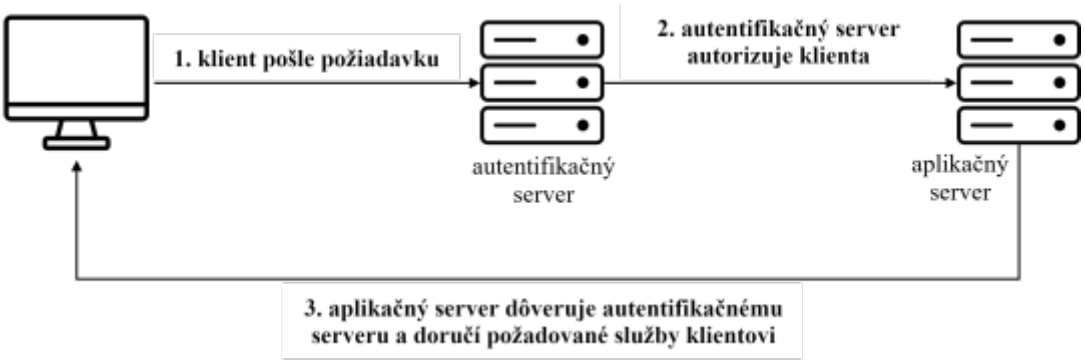
Iný spôsob, ako sa pozerať na autentifikáciu, je pomocou prostriedkov, ktoré využíva. Potom môže mať jednu z troch foriem:

- **Základná autentifikácia** zahŕňa server. Server uchováva používateľský súbor s heslami, používateľskými menami a niektorými ďalšími dôležitými overovacími údajmi. Toto je najrozšírenejší spôsob overovania používateľov. Má však niekoľko nedostatkov vrátane zabudnutia a nevhodného umiestnenia autentifikačných informácií (hesiel).



Obr. 4. Základná autentifikácia s použitím servera

- Autentifikácia založená na princípe **výzva/odpoveď** (challenge-response), pri ktorej server alebo iný autentifikačný systém vydá výzvu hostiteľovi požadujúcemu autentifikáciu a čaká na odpoveď. Príkladom tejto formy autentifikácie je použitie náhodného čísla (nonce) – ľubovoľné číslo alebo postupnosť bitov v čase, ktorá sa použije iba raz na overenie napr. prenesených údajov.
- **Centralizovaná autentifikácia** sa týka systému, v ktorom server autentifikuje, autorizuje a kontroluje používateľov siete. Tieto tri postupy sa vykonávajú v reakcii na aktivitu servera. Príkladom takejto autentifikácie je protokol Kerberos.



Obr. 5. Centralizovaná autentifikácia

Interaktivní prvek

KAPITOLA 2

Prvky a proces autentifikácie

Autentifikácia vyžaduje proces overovania, ktorý je založený na:

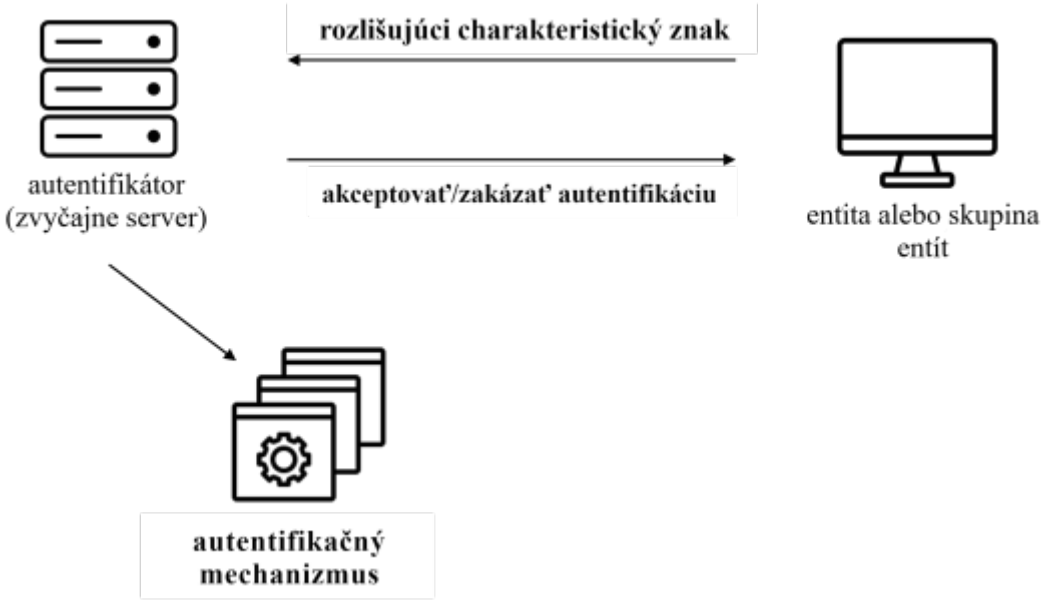
- entite alebo skupine entít hľadajúcich autentifikáciu;
- rozlišujúcom charakteristickom znaku overovanej entity (entít);
- autentifikátorovi (zvyčajne server);
- autentifikačnom mechanizme na overenie správnosti autentifikačných charakteristík;
- mechanizme riadenia prístupu na základe výsledku autentifikácie.

Prvým prvkom sú často jednotlivci, procesy alebo systémy, ktoré chcú získať prístup k systému. Ak konajú individuálne, musia byť pripravení preukázať autentifikátorovi dôkaz, že sú oprávnení využívať požadovaný systémový zdroj.

Druhým prvkom autentifikácie je charakteristický znak používateľa. Hovorili sme o nich predtým a sú rozdelené na niečo, čo poznáte, čo máte, a čím ste. Niektoré z týchto prvkov nemusia postačovať na úplnú autentifikáciu entity a preto na zlepšenie autentifikácie a poskytnutie silnejších záruk možno použiť kombináciu položiek z niekoľkých faktorov a dôveryhodnosti.

Funkciou autentifikátora je pozitívne a automaticky kontrolovať osobné údaje (doklady) entity a určiť, či má alebo nemá táto entita povolený prístup k požadovanému systémovému zdroju. Keď sa odošle požiadavka na autentifikáciu, autentifikátor vás vyzve na zadanie osobných údajov na dokončenie procesu autentifikácie. Potom autentifikátor zhromaždí údaje a odošle ich autentifikačného mechanizmu. Ako autentifikátor môže fungovať server určený používateľom, virtuálna privátna sieť (VPN), firewall, webový server, celopodnikový dedikovaný server, nezávislá autentifikačná služba alebo nejaký iný typ služby globálnej identity. Čokoľvek, čo sa používa ako autentifikátor, musí vykonať autentifikačnú procedúru, ktorá vedie k nejakému druhu výslednej hodnoty, ako je token, ktorý možno neskôr použiť na zistenie informácií o autorizovanom používateľovi.

Pohľad na tento proces autentifikácie je znázornený na obrázku 6.



Obr. 6. Základný proces autentifikácie a jeho prvky

Metóda (systém) autentifikácie sa skladá z troch častí, ktoré spolupracujú, aby sa zabezpečili autentifikačné vlastnosti používateľa:

- vstup,
- transportný systém a
- overovateľ.

Interaktivní prvek

Vstupný komponent reprezentuje interakciu používateľa s mechanizmom autentifikácie. Ide napríklad o klávesnicu počítača, čítačku kariet, videokameru, telefón alebo porovnateľné zariadenie. Zachytené položky identifikujúce používateľa sa prenesú na miesto, kde budú skontrolované, analyzované a prijaté alebo odmietnuté. Aby sa však tieto produkty dostali na toto miesto, musia byť prepravené. Preto transportná sekcia systému má na starosti odovzdávanie údajov medzi vstupným komponentom a prvkom, ktorý dokáže overiť identitu osoby. Tieto informácie sa prenášajú cez sieť v moderných autentifikačných systémoch, kde ich dokážu zabezpečiť protokoly. Posledným komponentom autentifikačného systému je overenie, čo je mechanizmus kontroly prístupu.

Interaktivní prvek

2.1 Typy autentifikácie

Identifikovali sme tri faktory, ktoré sa využívajú pri autentifikácii používateľa. Poukázali sme tiež na to, že hoci sú tieto faktory dobré, v niektorých sú položky, ktoré trpia zraniteľnosťou. Tabuľka 1 ukazuje nedostatky každého z faktorov.

Tabuľka 1. Kategórie autentifikácie a ich nedostatky

Faktor	Príklady	Zraniteľnosti
niečo, čo poznáte	heslo, PIN	môže byť zabudnuté, uhádnuté, duplikované, jednoduché na získanie v prípade podvodu (napr. phishing)
niečo, čo máte	tokeny, čipové karty, jednorazové heslo poslané na číslo telefónu	môže byť stratené, ukradnuté, duplikované
niečo, čím ste	odtlačok prsta, tvár, dúhovka	nepopierateľný (nonrepudiable) - v prípade zneužitia ho nemožno zmeniť

NEVÝHODY

Spomenuli sme, že prvé dva faktory, „niečo, čo poznáte“ a „niečo, čo máte“, môžu spôsobiť problémy s autentifikátorom, pretože poskytnuté informácie môžu byť nepresné. Môže to byť nedôveryhodné. Takéto faktory sú vystavené mnohým známym problémom, vrátane možnosti straty, falšovania alebo ľahkej reprodukcie položiek. Vedomosti môžu byť tiež zabudnuté a znalosti a veci môžu byť zdieľané alebo ukradnuté.

Interaktivní prvek

2.1.1 Viacfaktorová autentifikácia

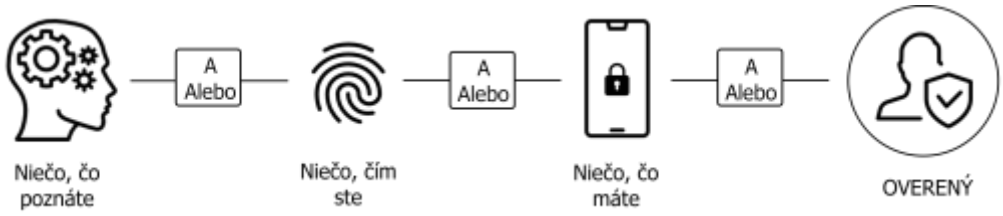
DEFINÍCIA

Viacfaktorová autentifikácia (MFA) využíva minimálne dva rôzne faktory (čo poznáte, čo máte a čím ste). Dvojfaktorová autentifikácia (2FA) je rovnaká, ale používajú sa presne dva faktory.

V súčasnosti, ak sa používa MFA, je to takmer vždy 2FA. Prvým faktorom je zvyčajne heslo alebo PIN (niečo, čo poznáte) a druhým zvyčajne banková karta, SMS alebo kód vygenerovaný aplikáciou (to, čo máte – t. j. vaše mobilné zariadenie). Ďalšou možnosťou je použitie odtlačkov prstov, skenov sietnice atď. Používa sa menej často, pretože je potrebný ďalší hardvér (vyššie náklady).

Viacfaktorová autentifikácia je dobrý spôsob, ako zmierniť riziko a znížiť pravdepodobnosť ohrozenia prihlasovacích údajov. Pozrime sa napríklad na kombináciu hesla a kódu aplikácie. Aj keď je napadnutá samotná stránka alebo je heslo získané odniekiaľ, útočník sa nemôže prihlásiť, pretože môže poskytnúť

príslušné používateľské meno a heslo, ale nemôže poskytnúť kód vygenerovaný na mobilnom zariadení. Ukradnuté heslo sa potom stane zbytočným (pokiaľ útočník neukradne aj mobilné zariadenie). Nejde o škálovateľný útok a pre väčšinu ľudí nepredstavuje vážnu hrozbu. Medzitým môžu správcovia systému stále detekovať neúspešné pokusy o prihlásenie a požiadať konkrétneho používateľa o zmenu hesla alebo všetkých používateľov, ak bol ich systém napadnutý a všetky heslá unikli.



Obr. 7. Viacfaktorová autentifikácia

KAPITOLA 3

Autentifikácia pomocou hesla

Technika overovania hesla je najbežnejším a najjednoduchším spôsobom autentifikácie v praxi. V mnohých systémoch je tento typ predvolený. Opätovne použiteľné heslá, jednorazové heslá (OTP), heslá na báze výzva/odpoveď a heslá s kombinovaným prístupom patria medzi príklady autentifikácie pomocou hesla.

Opätovne použiteľné heslá

Pri autentifikácii s opakovane použiteľným heslom existujú dve formy autentifikácie: autentifikácia používateľa a autentifikácia klienta.

- **Autentifikácia používateľa** je najrozšírenejším druhom overovania a väčšina používateľov ho pravdepodobne pozná. Spúšťa ho vždy používateľ, ktorý odošle serveru požiadavku na autentifikáciu a autorizáciu prístupu ku konkrétnemu systémovému zdroju. Keď server prijme požiadavku, vyzve používateľa na zadanie používateľského mena a hesla. Server ich po prijatí porovnáva s kópiami vo svojej databáze. Autorizácia sa poskytuje na základe zhody.
- **Autentifikácia klienta.** Používateľ zvyčajne požaduje autentifikáciu a následnú autorizáciu na prístup k systému alebo skupine systémových prostriedkov na serveri. Autentifikácia neudeľuje používateľovi prístup k žiadnemu systémovému zdroju, na ktorý nemá oprávnenie. Autentifikácia musí zabezpečiť autorizáciu používateľa, aby mohol používať zdroje v požadovanom rozsahu a nič viac. Autentifikácia klienta je názov pre tento druh autentifikácie. Stanovuje identity používateľov a umožňuje im kontrolovaný prístup k systémovým zdrojom.

Pretože tieto metódy autentifikácie sú najčastejšie používané, sú aj najviac zneužívané.

NEVÝHODY

Okrem toho sú tiež nespoľahlivé, pretože osobné údaje potrebné pri nich ľudia zabúdajú, zapisujú si, zdieľajú a čo je najdôležitejšie, dajú sa ľahko uhádnuť, pretože si ľudia vyberajú jednoduché heslá. A sú tiež náchylné na sledovanie a prelomenie. Navyše, slabé heslá (napr. krátke, s jednoduchou štruktúrou) sú zraniteľné voči dnešným super/silným počítačom, ktoré ich dokážu prelomiť hrubou silou t.j. vyčerpávajúcim hľadaním.

Jednorazové heslá

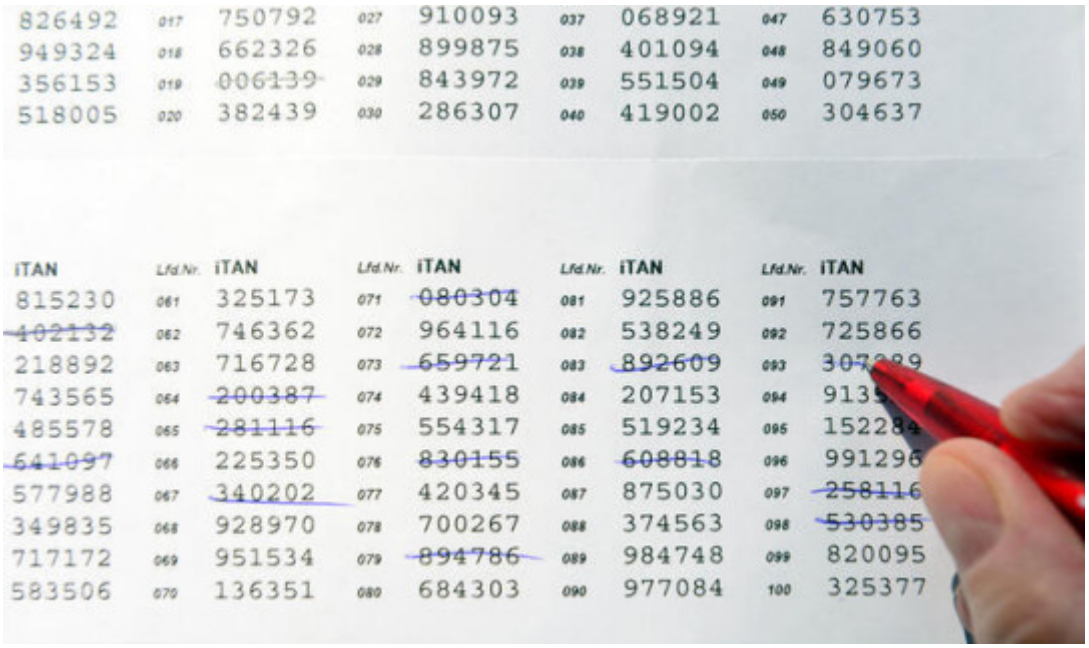
Autentifikácia relácie je iný názov pre autentifikáciu jednorazovým heslom. Na rozdiel od opätovne použiteľných hesiel, ktoré je možné použiť opakovane, sa jednorazové heslá použijú iba raz a potom sa zahodia.

VÝHODY

Pomocou silných generátorov náhodných čísel sú generované náhodným prístupom. Tým sa znižuje pravdepodobnosť, že budú uhádnuté. V mnohých prípadoch sú pred odoslaním zašifrované, aby sa obmedzila šanca na ich zachytenie.

Jednorazové heslá majú rôzne podoby. Medzi príklady patria S/Key a tokenové heslá. S/Key je systém na vytváranie jednorazových hesiel definovaný v RFC 1760.

Ďalším príkladom je takzvané číslo TAN používané v Nemecku v minulosti (obrázok 8). Hoci jednorazové heslá sú zvyčajne bezpečnejšie, majú množstvo nevýhod. Patria k nim problémy so synchronizáciou spôsobené časovým intervalom medzi časovou pečiatkou v hesle a systémovými hodinami. Keď sú tieto dva časy mimo fázy, heslo nemožno použiť.



Obr. 8. Čísla TAN ako príklad jednorazových hesiel (OTP)

Niektoré typy jednorazových hesiel (napr. SMS kódy a kódy generované aplikáciou) sa zvyčajne používajú ako druhý faktor pri použití 2FA.

Autentifikácia založená na princípe výzva/odpoveď

DEFINÍCIA

Pri metóde autentifikácie využívajúcej heslá a pracujúcej na princípe výzva/odpoveď je proces overovania založený na vzájomnej výmene (komunikácii), pri ktorej autentifikátor vyzýva používateľa, ktorý požaduje autentifikáciu. Aby bol používateľ overený, musí poskytnúť správnu odpoveď.

V závislosti od systému môže mať výzva mnoho rôznych podôb. Môže to byť základná požiadavka na heslo, číslo, súhrn alebo náhodné číslo (nonce). Jednotlivec, ktorý chce byť overený, musí odpovedať na

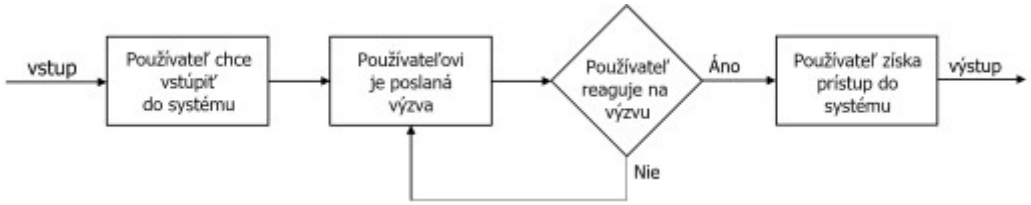
výzvu systému. V súčasnosti sa odpovede posielajú prostredníctvom jednosmernej funkcie a tokenu hesla, ktoré sú známe ako asynchrónne tokeny. Keď server dostane odpoveď od používateľa, vykoná dvojitú kontrolu hesla.

Najbežnejšia aplikácia autentifikácie založenej na princípe výzva/odpoveď je v distribuovaných systémoch. Napriek popularite, autentifikácia tohto typu čelí ťažkostiam. Nedostatkom je zapojenie používateľov a útoky typu pokus/omyl. Problém súvisiaci so zapojením používateľov je spojený so schopnosťou používateľa nájsť problém na stránkach (obrazovkách) s chaotickým obsahom. Používateľ potom musí rýchlo zadať odpoveď.

V závislosti od požadovanej úrovne zabezpečenia sa môže od používateľa vyžadovať, aby si spomenul na obšírnu odpoveď alebo môže byť nútený si ju zapísať. Potom ju musí používateľ prepísať a znovu zadať. Tak môžu vznikať chyby.

ZAUJÍMAVOSŤ

Niektorí výrobcovia sa pokúšali zbaviť používateľa bremena zapamätania si a zadávania dlhých reťazcov automatizáciou väčšiny potrebných krokov. Napr. vystrihnutím a prilepením výzvy a odpovede alebo nízkoúrovňovým automatizovaným procesom, ktorý zjednodušuje odpoveď používateľa na odpoveď typu áno/nie.



Obr. 9. Proces autentifikácie v systéme na báze výzva/odpoveď

Za zmienku tiež stojí, že odpovede na výzvy, ktoré vyžadujú heslá, môžu byť zneužité vo svojej najzákladnejšej forme, pretože heslá sa dajú relatívne ľahko získať. Heslá môžu byť potenciálne zachytené, ak sú odosielané v otvorenom formáte. Ak heslo nie je prenášané cez sieť v otvorenom formáte (t.j. je zašifrované), nepredstavuje bezpečnostné riziko.

Interaktivní prvek

3.1 Problémy so zabezpečením hesla

Pri kybernetických útokoch sú úniky údajov jedným z najrozšírenejších typov útokov a cieľov útočníka. Preto autentifikačné mechanizmy založené na heslách sú čoraz viac problematickejšie.

Jedinečnosť hesla je jednou z jeho najdôležitejších vlastností. Mnohé heslá sú však všetko, len nie práve toto. Najpopulárnejšie heslá a frázy používané ľuďmi na celom svete sú uvedené v tabuľke 2.

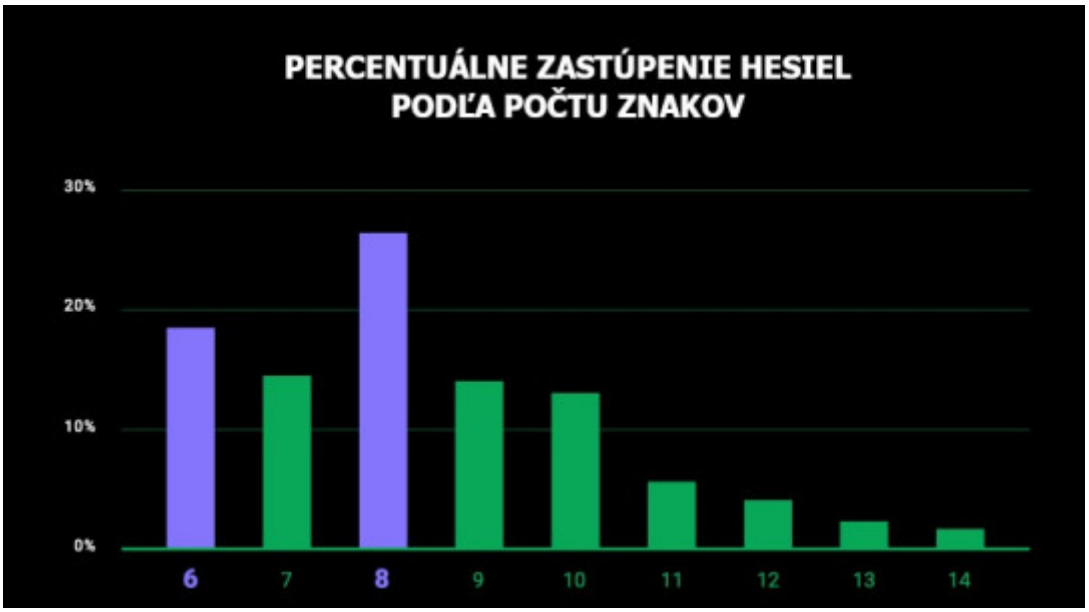
Tabuľka 2. 10 najčastejšie používaných hesiel, zdroj: cybernews.com

Heslá
123456
123456789
qwerty
password
12345
qwerty123
1q2w3e
12345678
111111
1234567890

NEVÝHODY

Okrem toho existujú ďalšie problémy týkajúce sa hesiel. Mnoho ľudí sa rozhodne prepojiť svoje webové stránky s niečím, čo si ľahko zapamätajú, aby vytvorili jednoduché, zapamätateľné kombinácie. To však neznamená, že heslo je jedinečné; opak je pravdou.

Vyšetrovanie skupinou Cybernews sa zameralo na približne 15 miliárd záznamov a zatriedilo ich do niekoľkých kategórií a fráz. Ich výsledky ukazujú, že problematické sú určité vlastnosti hesiel – údaje týkajúce sa používateľa. Okrem toho skúmali dĺžku hesiel z hľadiska počtu znakov, ktoré obsahovali. Bohužiaľ, väčšina použitých hesiel mala 8 znakov alebo menej.



Obr. 10. Štatistika dĺžok hesiel, zdroj: cybernews.com

Existujú efektívnejšie metódy na vytvorenie silného hesla. Pri použití slova „heat“ ako prvku hesla môže byť napríklad jednoduché heslo „letsgoheat“ (10 znakov), zatiaľ čo zložitejšie heslo môže byť „heatromearsenalhjamesp“ (22-znakové slovné spojenie). Ľudia tiež generujú bezpečné heslá pomocou mnemotechnických pomôcok, ktoré sú vhodnejšie. Sú často dlhé a obsahujú náhodné slová, medzi ktorými nie je žiadny logický vzťah. Pre človeka sú jednoduchšie zapamätateľné, ale pre algoritmus je ťažšie ich prelomiť.

3.2 Útoky na heslá

Heslá môžu byť napadnuté rôznymi spôsobmi a vo všeobecnosti možno útoky klasifikovať takto:

- Neelektronické útoky nevyžadujú technické znalosti na prelomenie hesla. Príklady takýchto útokov zahŕňajú sledovanie potenciálnej obete (shoulder surfing), sociálne inžinierstvo a prehrabávanie sa v odpadkoch obete (dumpster diving).
- Útoky elektronického typu vyžadujú technické znalosti. Príklady takýchto útokov zahŕňajú slovníkové útoky, útoky hrubou silou a útoky pomocou dúhových tabuliek.

3.2.1 Neelektronické útoky

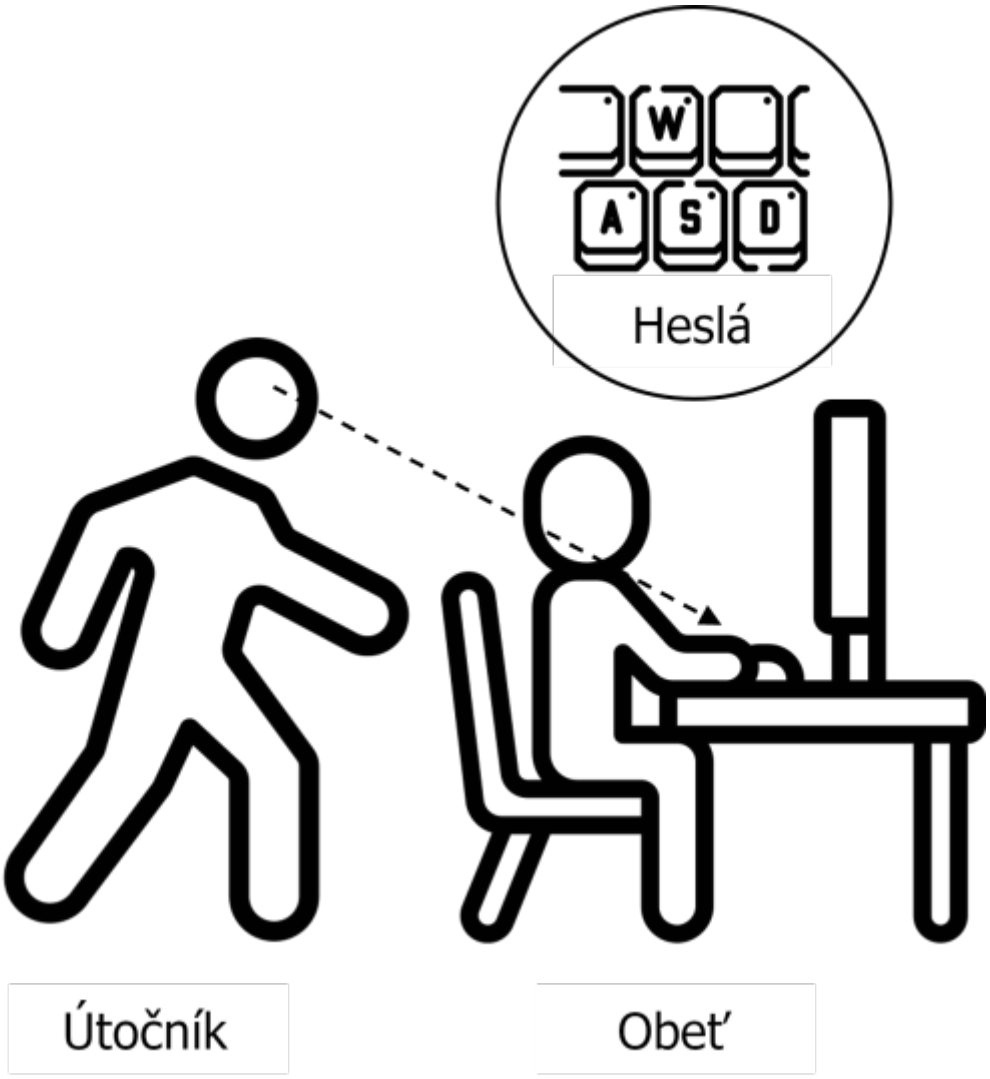
DEFINÍCIA

Sociálne inžinierstvo je typ útoku, pri ktorom sa útočník snaží využiť prirodzenú tendenciu ľudí dôverovať komukoľvek. Využitím tejto dôvery útočník rýchlo získa osobné údaje obete a neskôr ich použije na získanie prístupu k jeho/jej účtu.

Útoky typu phishing, pharming a whaling sú len niektoré príklady. Upozorňujeme, že niektoré z nich vyžadujú určité technické zručnosti (napr. phishing).

Obr. 11. Proces phishingového útoku

Pri útoku založenom na sledovaní obete stojí útočník za vami a sleduje, ako zadávate svoje prihlasovacie údaje, ktoré následne použije na prístup k vášmu účtu.



Obr. 12. Príklad útoku založenom na sledovaní obete

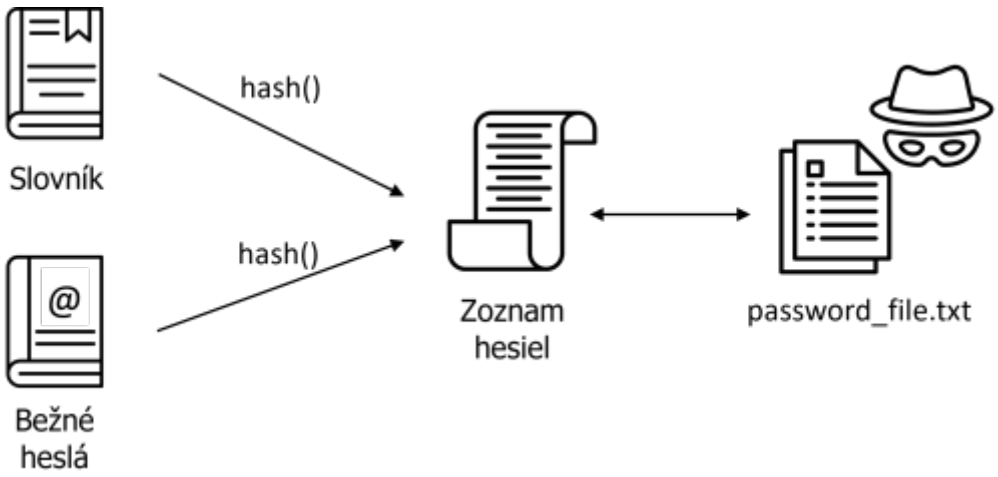
Pri útoku typu prehrabávanie odpadkov útočník objaví niečo cenné vo vašom odpade, ako je vaše heslo alebo PIN k vašej kreditnej karte.

3.2.2 Elektronické útoky

DEFINÍCIA

Slovníkový útok je útok, pri ktorom sa útočník pokúša dostať do systému chráneného heslom použitím každého slova zo slovníka ako typu hesla pre tento systém.

Zahŕňa testovanie všetkých reťazcov v zozname, ktorý bol vopred usporiadaný. Historicky sa pri takýchto útokoch používali slová zo slovníka (odtiaľ názov slovníkový útok).



Obr. 13. Ako funguje slovníkový útok

Slovníkový útok skúša iba možnosti, ktoré sú považované za najpravdepodobnejšie na úspech. Mnoho ľudí má tendenciu vyberať si krátke heslá, ktoré sú obyčajnými slovami alebo bežnými heslami, prípadne varianty získané napríklad pridaním číslice alebo interpunkčného znaku. Preto sú slovníkové útoky často úspešné.

Keďže dostupné zoznamy (slovníky) pokrývajú väčšinu typických stratégií vytvárania hesiel, je ťažké odolať slovníkovým útokom nástrojov, ktoré generujú vzory na prelomenie hesla. Bezpečnejším spôsobom je použiť nástroj na správu hesiel alebo manuálnu metódu na vytvorenie veľkého hesla (15 alebo viac písmen) alebo viacslovného hesla náhodným spôsobom.

Útoky hrubou silou

DEFINÍCIA

Zjednodušene povedané, útok hrubou silou je prístup k prelomeniu hesla, pri ktorom útočník skúša čo najviac potenciálnych kombinácií hesiel pomocou súboru parametrov.

Webová stránka môže napríklad stanoviť obmedzenie, ktoré vyžaduje, aby heslo malo dĺžku 8 až 16 znakov. Nástroj na prelomenie hesiel by mohol začať s 00000000 v najzákladnejšom tvare. Potom môže skúšať 00000001, 00000010, 00000100 a tak ďalej, kým nevyčerpá všetky mysliteľné kombinácie znakov.

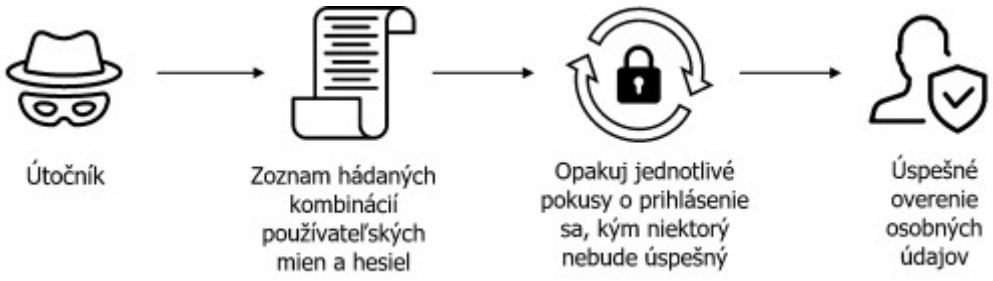
Heslá teda môžu obsahovať znaky:

- malá (anglická) abeceda (26 možností),
- veľká (anglická) abeceda (26 možností),
- číslice (10 možností od 0 do 9),
- interpunkčné znamienka alebo iné špeciálne znaky (33 možností).

Vzhľadom na toto všetko si môžete vypočítať konečný počet možných hesiel pre 8 znakové heslo: 3 025 989 069 143 040, teda približne 3 kvadrilióny, pričom každé z nich je samostatný pokus.

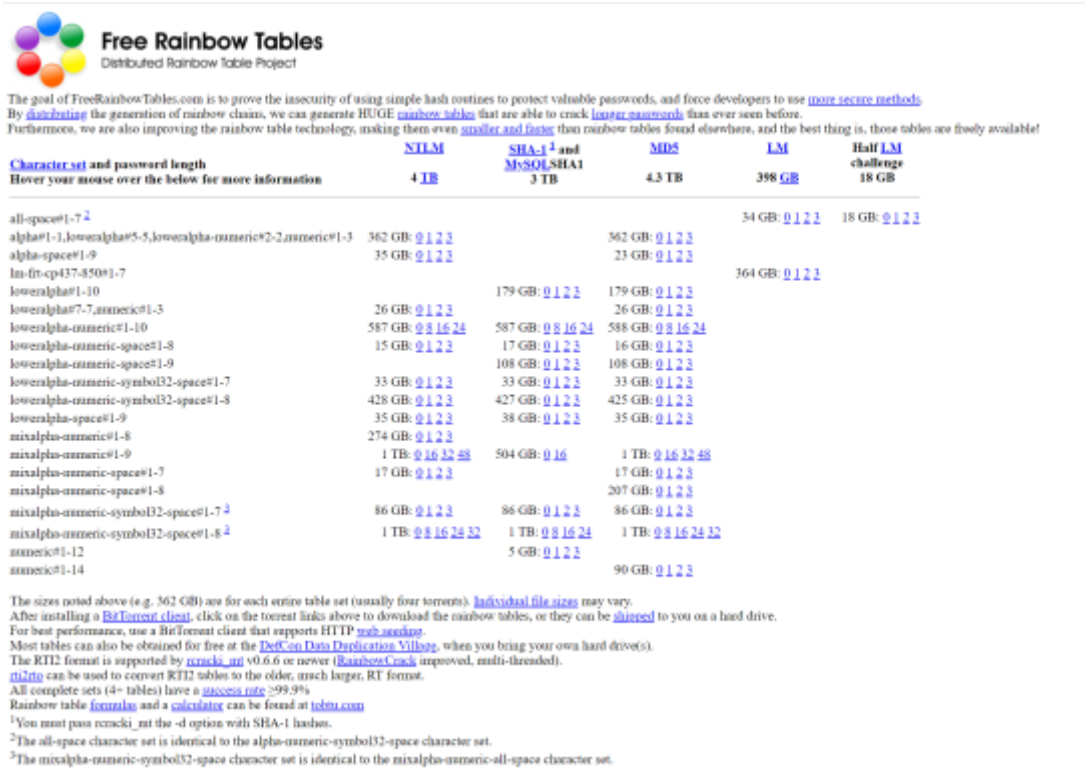
Možno si myslíte, že niekto vytvorí program, ktorý prejde na webovú stránku, zadá vaše používateľské meno a heslo, stlačí tlačidlo prihlásenia a pokúsi sa uhádnuť vaše heslo. Potom proces zopakuje ešte tri kvadrilióny krát. To však nie je tento prípad. Ak webovej stránke trvá načítanie stránky 2 sekundy, ide o 2 sekundy čakania na každý pokus o získanie prístupu s „nesprávnym heslom“. Inými slovami, ak webová stránka nezablokuje prihlásenie po určitom množstve podozrivých pokusov, môže to trvať až 9 kvadriliónov sekúnd alebo 287,9 milióna rokov. V skutočnosti sa takýto útok vykonáva pomocou uniknutých používateľských mien a hesiel. Tie unikli v dôsledku krádeže údajov (čo sa stáva častejšie, než si myslíte). Heslo je teda možné odhaliť jedným z dvoch spôsobov:

- Vaše heslo nie je hašované a je uložené ako obyčajný text v extrémne nezabezpečenom prostredí. Od čitateľa sa nebude vyžadovať nič viac ako skopírovanie a vloženie hesla. Ak je vaše heslo napríklad heslo1, každý, kto si prečíta obsah uniknutých údajov, uvidí heslo1. V tomto prípade je útok hrubou silou zbytočný, pretože webová stránka už odovzdala vaše informácie na striebornom podnose.
- Vaše heslo je hašované a teda nie je uložené ako obyčajný text a je prenášané v bezpečnejšom prostredí. Ak webová lokalita zahašuje vaše heslo pomocou hašovacej funkcie SHA-256, napríklad heslo1 sa zobrazí ako 0b14d501a594442a01c6859541bcb3e8164d183d32937b851835442f69d5c94e.



Obr. 14. Útok hrubou silou na heslá

Útoky pomocou dúhových tabuliek sú špeciálnym typom útoku hrubou silou na prelomenie hesla. Je určený na prelomenie hesiel uložených pomocou hashov. Pretože dúhové tabuľky sú vopred vypočítaným zoznamom hashov slovníkových výrazov alebo predtým prelomených hesiel a sú uložené v databáze priamo pomocou hashov, existuje kompromis medzi časom prelomenia a požadovanou veľkosťou pamäte. Generovanie dúhovej tabuľky môže trvať dlho, ale stačí to urobiť raz. Môžete vyhľadať hodnoty hashov hesiel a po dokončení rýchlo získať príslušné heslo. Aby ste mohli získať predstavu o veľkosti týchto databáz, niektoré dúhové tabuľky môžu mať veľkosť 7–9 TB.



Free Rainbow Tables
Distributed Rainbow Table Project

The goal of FreeRainbowTables.com is to prove the insecurity of using simple hash routines to protect valuable passwords, and force developers to use more secure methods.
By distributing the generation of rainbow chains, we can generate HUGE rainbow tables that are able to crack longer passwords than ever seen before.
Furthermore, we are also improving the rainbow table technology, making them even smaller and faster than rainbow tables found elsewhere, and the best thing is, those tables are freely available!

Character set and password length Hover your mouse over the below for more information	NTLM 4 TB	SHA-1 [1] and MySQL SHA1 3 TB	MD5 4.3 TB	LM 398 GB	Half LM challenge 18 GB
all-space#1-7 [2]				34 GB: 0 1 2 3	18 GB: 0 1 2 3
alpha#1-1,loweralpha#5-5,loweralpha-numeric#2-2,numeric#1-3	362 GB: 0 1 2 3		362 GB: 0 1 2 3		
alpha-space#1-9	35 GB: 0 1 2 3		23 GB: 0 1 2 3		
lm-frt-cp437-850#1-7				364 GB: 0 1 2 3	
loweralpha#1-10		179 GB: 0 1 2 3	179 GB: 0 1 2 3		
loweralpha#7-7,numeric#1-3	26 GB: 0 1 2 3		26 GB: 0 1 2 3		
loweralpha-numeric#1-10	587 GB: 0 8 16 24	587 GB: 0 8 16 24	588 GB: 0 8 16 24		
loweralpha-numeric-space#1-8	15 GB: 0 1 2 3	17 GB: 0 1 2 3	16 GB: 0 1 2 3		
loweralpha-numeric-space#1-9		108 GB: 0 1 2 3	108 GB: 0 1 2 3		
loweralpha-numeric-symbol32-space#1-7	33 GB: 0 1 2 3	33 GB: 0 1 2 3	33 GB: 0 1 2 3		
loweralpha-numeric-symbol32-space#1-8	428 GB: 0 1 2 3	427 GB: 0 1 2 3	425 GB: 0 1 2 3		
loweralpha-space#1-9	35 GB: 0 1 2 3	38 GB: 0 1 2 3	35 GB: 0 1 2 3		
mixalpha-numeric#1-8	274 GB: 0 1 2 3				
mixalpha-numeric#1-9	1 TB: 0 16 32 48	504 GB: 0 16	1 TB: 0 16 32 48		
mixalpha-numeric-space#1-7	17 GB: 0 1 2 3		17 GB: 0 1 2 3		
mixalpha-numeric-space#1-8			207 GB: 0 1 2 3		
mixalpha-numeric-symbol32-space#1-7 [3]	86 GB: 0 1 2 3	86 GB: 0 1 2 3	86 GB: 0 1 2 3		
mixalpha-numeric-symbol32-space#1-8 [3]	1 TB: 0 8 16 24 32	1 TB: 0 8 16 24	1 TB: 0 8 16 24 32		
numeric#1-12		5 GB: 0 1 2 3			
numeric#1-14			90 GB: 0 1 2 3		

The sizes noted above (e.g. 362 GB) are for each entire table set (usually four torrents). Individual file sizes may vary.
After installing a BitTorrent client, click on the torrent links above to download the rainbow tables, or they can be shipped to you on a hard drive.
For best performance, use a BitTorrent client that supports HTTP web seeding.
Most tables can also be obtained for free at the DefCon Data Duplication Village, when you bring your own hard drive(s).
The RTI2 format is supported by rcracki_mt v0.6.6 or newer (RainbowCrack improved, multi-threaded).
rti2rto can be used to convert RTI2 tables to the older, much larger, RT format.
All complete sets (4+ tables) have a success rate ≥99.9%
Rainbow table formulas and a calculator can be found at tobtu.com
[1] You must pass rcracki_mt the -d option with SHA-1 hashes.
[2] The all-space character set is identical to the alpha-numeric-symbol32-space character set.
[3] The mixalpha-numeric-symbol32-space character set is identical to the mixalpha-numeric-all-space character set.

Obr. 15. Veľkosti dúhových tabuliek z freerainbowtables.com

Interaktivní prvek

Interaktivní prvek

3.2.3 Nástroje na odhaľovanie hesiel

Nástroje na odhaľovanie (prelomenie) hesiel sa v dnešnej dobe stávajú čoraz obľúbenejšími, a preto si niektoré z nich prejdeme. Nástroje na prelomenie hesiel sa väčšinou používajú na testovanie sily hesla alebo na spustenie nepriateľského útoku. Existuje množstvo online a offline nástrojov určených len na prelomenie hesiel. Rozhrania vzdialeného prihlasovania sa, ako sú služby SSH a RDP, sú terčom online útokov. Na druhej strane k offline útokom dochádza po úniku súborov. Potom sú heslá okamžite odhalené.

Niektoré z dostupných nástrojov sú Hashcat, John the Ripper alebo THC Hydra.

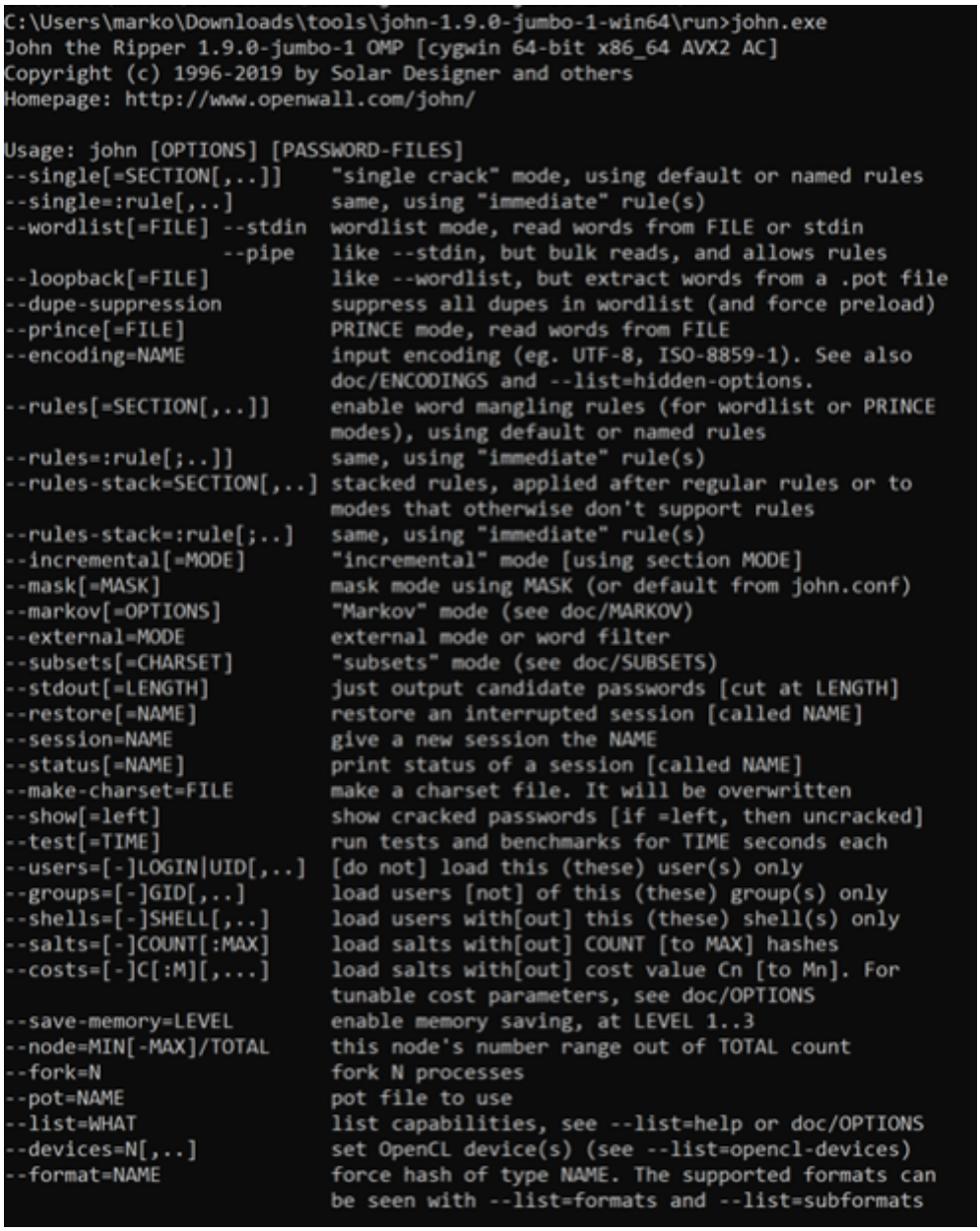
Hashcat je multiplatformový program na obnovu hesla, ktorý pracuje s GPU aj CPU. Hashcat bol vytvorený v roku 2009 (distribuovaný pod licenciou MIT) a je uznávaný kvôli podpore širokej škály hašovacích algoritmov, ako sú LM Hash, NT Hash, MD4, MDS a mnoho ďalších. Keď bol vyvinutý tento program, podporoval štyri rôzne druhy útokov:

- Slovníkové útoky: viac ako 14 miliónov hesiel, počnúc najpopulárnejším a končiac najmenej bežným. Uhádne heslo, zahašuje ho a porovná hash s heslom, ktoré sa pokúša prelomiť.
- Kombinované útoky: podobné slovníkovým útokom, ale namiesto používania dvojslovných zoznamov ako slovníky vytvára nový zoznam slov, kde každé slovo je spojené s každým iným slovom.
- Útoky založené na maskách: ak napríklad viete, že heslo vášho účtu má 9 znakov a končí číslicou, viete, že na uhádnutie hesla bude potrebné vyskúšať $52*10^9$ kombinácií, čo bude trvať približne 4 roky. Ak však viete, že heslo začína veľkým písmenom a končí číslicou, čas sa skráti na polovicu.
- Útoky založené na pravidlách: Hashcat môže určiť, aký druh hesla sa má vyskúšať na základe toho, ako si vaša obeť vytvára heslo.
- Útoky hrubou silou: vyskúša všetky možnosti, kým nenájde niečo (čo zvyčajne bude trvať dlho, pretože bude skúšať všetky možné kombinácie).

John the Ripper vydaný pod licenciou GNU **GPL** (***General Public License***) v roku 1996 je offline nástroj (s otvoreným kódom) na zabezpečenie, overenie a obnovu hesiel, ktorý podporuje stovky typov hašov a šifier. Je k dispozícii pre rôzne platformy, čo vám umožňuje použiť rovnaký nástroj na ktorejkoľvek z nich. Ako už bolo uvedené, tento nástroj podporuje rôzne typy hašov.

Pri spustení na rôznych platformách sa tieto typy hašov môžu líšiť. Tento nástroj má mnoho režimov prelamovania (hesiel), ako napríklad:

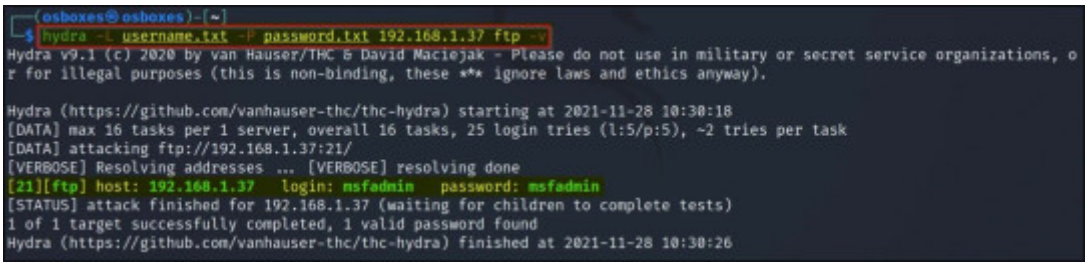
- Režim zoznamu slov (slovníkový útok): V tomto režime zadáte textový súbor so zoznamom slov, ktorý by mal byť v ideálnom prípade usporiadaný a slová sa porovnávajú s heslom, ktoré sa pokúšate prelomiť. Je možné aplikovať rôzne pravidlá.
- Single Crack: Toto je prvý režim, s ktorým sa začína odhaľovanie hesiel. V skutočnosti sa úspešne odhalené heslo porovnáva so všetkými načítanými heslami (v systéme), aby sa overilo, či niektorí používatelia nemajú rovnaké heslo, čo urýchli proces.
- Inkrementálny režim: najvýkonnejší lámací režim, ktorý vyskúša všetky mysliteľné kombinácie, no nezastaví sa kvôli veľkému počtu možných kombinácií.
- Externý režim: sú to funkcie napísané v jazyku C, ktoré sú vytvorené nástrojom pri spustení a výsledný program sa použije na vygenerovanie kandidátov na heslá.



Obr. 16. John the Ripper v akcii

THC Hydra, navrhnutý Van Hauserom v roku 2001, je online crackovací program, ktorý ukazuje, aké jednoduché je získať neoprávnený prístup k vzdialenému stroju. Tento nástroj podporuje rôzne protokoly vrátane FTP, HTTP, HTTPS, MySQL, Postgress, atď. a rôzne platformy vrátane UNIX, MacOS, Windows a mobilných zariadení. Tento nástroj môže vykonať paralelný slovníkový útok, útok hrubou silou alebo hybridný útok, paralelný útok na mnohé servery a ďalšie. THC Hydra je uznávaná ako rýchla a účinná, ale závisí to od protokolu.

Hlavný rozdiel medzi týmto nástrojom a nástrojom John the Ripper je v tom, že THC Hydra je online nástroj na prelomenie hesiel, zatiaľ čo John the Ripper je offline nástroj.



Obr. 17. THC Hydra v akcii

Interaktivní prvek

KAPITOLA 4

Rôzne aspekty zabezpečenia heslom

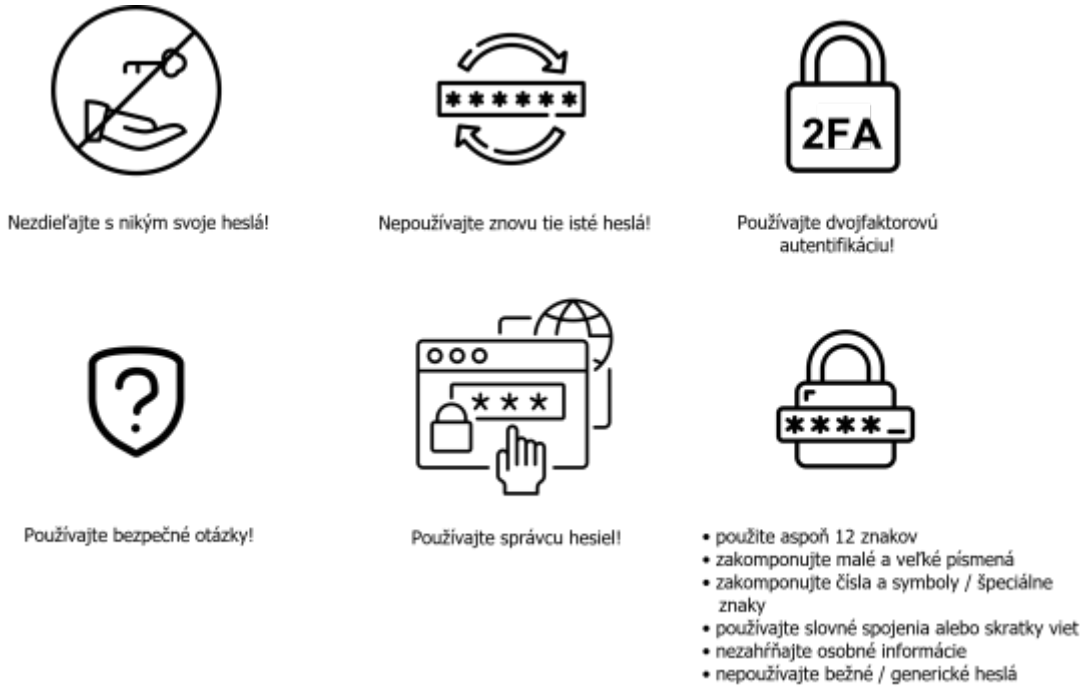
V tejto kapitole sa budeme zaoberať rôznymi aspektmi zabezpečenia hesiel, ktoré možno rozdeliť na aspekty:

- spojené s používateľom,
- spojené so serverom.

Tieto aspekty zahŕňajú pokyny pre bezpečné heslá, 2-faktorovú autentifikáciu, primerané ukladanie hesiel na strane servera atď.

4.1 Pokyny pre bezpečné heslo a osvedčené postupy

Heslá sú prevládajúcou metódou autentifikácie, pretože sú pre vývojárov najjednoduchšie na implementáciu a pre používateľov najjednoduchšie na pochopenie a používanie. Niektoré koncepčné nedostatky sú však spojené s používaním hesiel (napr. zle zvolené, ľahko uhádnuteľné atď.). Národný inštitút pre štandardy a technológie (NIST) v USA pravidelne aktualizuje svoje odporúčania na vytváranie a správu hesiel. V jednom z nedávnych odporúčaní zabezpečenia hesiel navrhli, aby sa používatelia zamerali viac na dĺžku hesla ako na zložitosť (kombinácie špeciálnych znakov, číslic, malých alebo veľkých písmen), pretože zložité heslá sú ťažko zapamätateľné. V dôsledku toho majú používatelia tendenciu dosahovať zložitosť predvídateľnými spôsobmi (napr. pridaním čísla 1 na koniec hesla). Jedným zo spôsobov, ako dosiahnuť dĺžku, sú nezmyselné slovné spojenia, v ktorých sú slová v poradí, ktoré nemá žiadny význam. Z rovnakého dôvodu už NIST neodporúča prísne pravidlá zloženia znakov pri vytváraní hesla. Odporúčajú však pravidelne porovnávať heslá (alebo aspoň akékoľvek nové heslá) so zoznamom napadnutých hesiel, aby ste identifikovali už odhalené a slabé heslá. Odporúčaná minimálna dĺžka hesla je 12 znakov. Zatiaľ čo v minulosti sa odporúčali pravidelné zmeny hesiel, už to tak nie je, pretože je menej pravdepodobné, že si používatelia po zmenách zapamätajú svoje heslá a namiesto toho začnú používať rovnaké heslá s malými úpravami.



Obr. 18. Najlepšie postupy pri používaní hesiel

Pre bezpečné, vlastnoručne vytvorené heslo je potrebné vziať do úvahy nasledujúce požiadavky:

- použite aspoň 12 znakov,
- zakomponujte malé a veľké písmená,
- zakomponujte čísla a symboly / špeciálne znaky,

- používajte slovné spojenia alebo skratky viet,
- nezahŕňajte osobné informácie,
- nepoužívajte bežné / generické heslá.

Majte na pamäti, že heslo NESMIE obsahovať osobné informácie, ako je dátum narodenia, meno domáceho maznáčika, vaše meno alebo e-mailová adresa.

Aj keď môžete použiť technické opatrenia, aby ste sa uistili, že používatelia si vyberajú silné heslá, nie je možné kontrolovať, čo používatelia s týmito heslami robia. Môžu si ich napísať na papier vedľa svojho počítača, zdieľať ho s inými ľuďmi alebo ich použiť na iné účty. To druhé je obzvlášť nebezpečné, pretože používanie rovnakého hesla na viacerých účtoch ohrozí všetky z nich, ak dôjde k nabúraniu niektorej zo služieb používajúcich rovnaké heslá. To znamená, že ak na prístup do knižnice a e-mailového účtu používate rovnaké heslo a niekto prelomí zabezpečenie knižnice (čo by malo byť oveľa jednoduchšie ako servery veľkého poskytovateľa e-mailových služieb – napr. Google) a ukradne heslo, môžu tieto informácie použiť na získanie prístupu k vášmu e-mailovému účtu. Vzdelávanie používateľov je jediným skutočným riešením, ako takýmto zlým praktikám predchádzať. Používatelia by preto mali byť poučení, ako si majú vytvárať silné heslá, aby ich nepísali na žiadnych dostupných miestach a aby nikdy nepoužívali rovnaké heslo.

Existujú aj ďalšie osvedčené postupy, pokiaľ ide o ochranu hesiel na strane používateľa:

- Používajte rôzne heslá pre rôzne scenáre
- Používajte slovné spojenia
- Používajte správcu hesiel
- Používajte dvojfaktorovú autentifikácia (2FA)

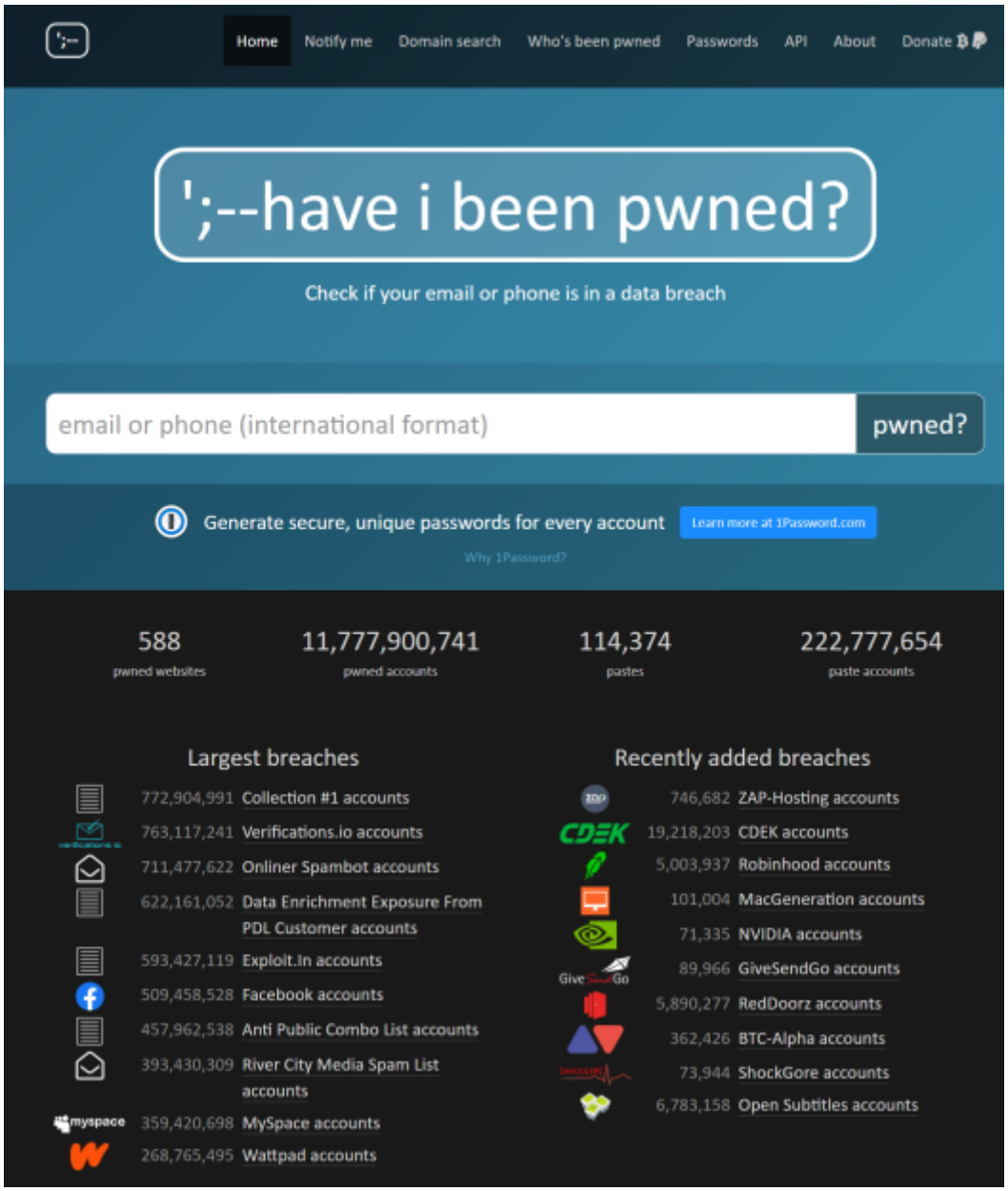
Aj keď sa to môže zdať nevinné, používanie rovnakého hesla na mnohých webových stránkach je nebezpečné. Kompromitácia osobných údajov na webových stránkach spotrebiteľov je čoraz rozšírenejšia. Ak sú vaše informácie odcudzené zo stránky sociálnych médií a vy používate rovnaké heslo vo svojej aplikácii online bankovníctva a na niekoľkých stránkach online nakupovania, útočník získa voľnú kontrolu nad všetkými týmito stránkami. Existuje softvér a aplikácie, ktoré vás môžu skutočne upozorniť, keď sa vaše heslá stali súčasťou porušenia ochrany údajov. Ak vaše informácie unikli, môže vás na to upozorniť napríklad Správca hesiel od Google.

Interaktivní prvek

Ďalšou dobrou praxou je použiť viac ako jedno slovo. Prístupová fráza (passphrase) je sekvencia slov, ktorá vyzerá ako veta, ale nemala by mať žiadny význam. Vaša prístupová fráza by nemala obsahovať ľahko získané osobné informácie, rovnako ako heslo. Môžete dokonca použiť generátory na vytvorenie náhodného reťazca slov pre používateľa.

Interaktivní prvek

Nakoniec je možné použiť rôzne online služby na kontrolu, či nebolo prelomené vaše heslo. Jednou z najznámejších služieb tohto typu je web haveibeenpwned.com. Existujú však rôzne iné webové služby, ako je táto.



Obr. 19. Webové služby typu „';--have I been pwned?“

4.2 Správcovia hesiel

Okrem dvojfaktorovej autentifikácie je použitie správcu hesiel dobrým spôsobom, ako udržať heslá v bezpečí. Táto možnosť funguje takmer univerzálne, zlepšuje bezpečnosť vašich hesiel a robí postup prihlasovania pohodlnejším.

Na druhej strane dobrí správcovia hesiel šifrujú vaše údaje dôkladne. Aj keď útočník získa prístup k súboru s údajmi, musí ho pred extrahovaním akýchkoľvek užitočných informácií najskôr dekódovať. Vo väčšine prípadov je to veľmi ťažké a nestojí to za námahu. V porovnaní s alternatívou pravidelné používanie správcu hesiel zaisťuje, že máte vždy k dispozícii zoznam účtov, ktorý je možné podľa potreby aktualizovať.

Útočníci sú odrádzaní, keď sa ukladajú údaje lokálne a nie v cloude. Získanie údajov jednej osoby alebo rodiny si vyžaduje značné úsilie. Pomocou dobrých správcov hesiel si môžete vybrať, kde budú uložené vaše heslá.

Mnoho ľudí má na to vlastné systémy a majú tendenciu zdieľať veci spoločne, rovnako ako bežné heslá. Tieto taktiky sú medzi útočníkmi dobre známe. Tieto znalosti boli integrované do crackovacích algoritmov a v dôsledku toho môžu byť takéto systémy viac škodlivé ako prospešné. Predpokladajme, že váš systém je vynikajúci. Aj tak je tu stále riziko. Keď útoky na iné systémy/služby odhalia vaše heslo, zvyšuje sa pravdepodobnosť napadnutia vášho systému. Akonáhle je váš systém prelomený, útočník ho môže použiť na uhádnutie vašich prihlasovacích údajov na iných webových stránkach. Nakoniec, používanie vášho systému namiesto správcu hesiel je v skutočnosti menej výhodné.

Dlhé prístupové frázy (slovné spojenia) sú často vhodnejšie ako heslá. Mnohé webové stránky ich však nepodporujú (obmedzenia týkajúce sa znakov a ich počtu). Okrem toho, hoci sú ľahšie zapamätateľné ako heslá, nerieši problém ľudí, ktorí používajú rovnaké heslo na rôznych stránkach alebo sa spoliehajú na systém.

Ako hlavné heslo pre správcu hesiel, ktorý je kľúčom na odomknutie všetkých údajov o hesle, sa však odporúča použiť prístupovú frázu. To vám umožní ľahko si vybrať a zapamätať si extrémne dlhé hlavné heslo.

Ak uvažujete o ukladaní hesiel v prehliadači, existuje niekoľko dôvodov, prečo je toto riešenie zlé. Prehliadače neberú zabezpečenie heslom tak vážne, ako by mali, pretože na prístup nevyžadujú hlavné heslo. Všetko, čo musíte urobiť, je byť prihlásený do počítača. Pri používaní iných počítačov, ako sú vaše, je táto metóda nepohodlná. Heslá prehliadača sú účinné iba v prehliadači. V súčasnosti to nie je praktická možnosť, pretože vaše heslo sa často vyžaduje pre webové aj mobilné aplikácie.

Správcovia hesiel poskytujú možnosť ukladať viac než len jednoduché heslá, čo je celkom užitočné. Na uloženie a vyplnenie prihlasovacích údajov (ako sú kreditné karty), môžete použiť správcu hesiel, čo je možné vykonať aj pomocou prehliadačov. V správcovi hesiel si môžete ponechať aj ďalšie citlivé informácie, ako sú licencie, identity, čísla bankových účtov atď.

Považujte teda správcu hesiel za digitálny trezor, ktorý môžete nosiť so sebou.

VÝHODY

Okrem toho správcovia hesiel ponúkajú aj ďalšie výhody súvisiace s používaním:

- Je integrovaný s oblasťami, kde potrebujete používať heslá, je rýchle a jednoduché vytvárať, aktualizovať a vypĺňať heslá.
- Je kompatibilný s mnohými platformami a heslá sú synchronizované.
- Funguje dobre v širokom spektre okolností a prevedení a zvyčajne sa dobre udržiava.
- Bezpečnosť berie vážne a vynakladá úsilie (silné end-to-end šifrovanie), aby zabezpečil, že dáta budú v bezpečí, aj keď dôjde k narušeniu.

Aby bol správca hesiel efektívny, musíte si zapamätať niekoľko kľúčových bodov:

- Mal by sa používať na všetkých vašich webových stránkach. Všade. Výnimky len zvyšujú zraniteľnosť a zložitosť systému (menšia pravdepodobnosť úspešnej obrany).
- Pre každú stránku vytvorte jedinečné heslo. Ak máte možnosť, urobte ich čo najdlhšie. Mali by ste použiť minimálne 20 až 30 znakov. Čím je heslo dlhšie, tým ťažšie je prelomiť ho (v skutočnosti exponenciálne ťažšie). Keďže správca hesiel ich väčšinu času vyplní za vás, nebudete ich musieť zadávať.
- Nie každá webová lokalita plne podporuje správcov hesiel a heslá je potrebné pred vložením do prihlasovacieho formulára občas skopírovať do schránky. Nie je to veľmi bezpečné, pretože by to mohlo viesť k odhaleniu vášho hesla rôznymi spôsobmi. Po krátkom čase väčšina správcov hesiel automaticky odstráni údaje o heslách zo schránky.
- Niektoré služby naďalej kladú absurdné požiadavky na heslá, ako napríklad heslá s dĺžkou aspoň 12 znakov. Tu sa hodia správcovia hesiel, pretože takéto heslá generujú náhodne, čo je asi najbezpečnejšie riešenie, aké sa dá vzhľadom na obmedzenia získať.
- Majte svoje hlavné heslo čo najdlhšie a používajte heslo, ktoré je ťažké uhádnuť. Je tiež dobré pravidelne meniť svoje hlavné heslo, aby ste znížili riziko jeho úniku alebo zachytenia nástrojom typu keylogger.
- Ak si chcete vymieňať heslá, požiadajte druhú osobu, aby si vytvorila svoj vlastný trezor a s použitím funkcie zdieľania poskytovanou správcom hesiel môžete navzájom zdieľať svoje heslá.

Príklady niektorých populárnych správcov hesiel sú:

- LastPass
- Dashlane
- LogMeOnce
- 1Password

- Keeper
- KeePass

Niektorí z nich prichádzajú zadarmo; za niektoré musíte zaplatiť. A niektoré sú síce zadarmo, no za pokročilé funkcie si musíte zaplatiť.

Interaktivní prvek

4.3 Dvojfaktorová autentifikácia (2FA)

DEFINÍCIA

2FA je ďalšia vrstva ochrany, ktorá overuje, že každý, kto sa pokúša o prístup k online účtu, je tým, za koho sa vydáva.

Používateľ musí najprv zadať svoje používateľské meno a heslo. Potom bude požiadaný, aby predložil ďalšie informácie skôr, ako získa prístup.

Výber peňazí z bankomatu je dobrým príkladom dvojfaktorovej autentifikácie. Transakciu je možné uskutočniť len so správnou kombináciou bankovej karty (niečo, čo máte) a PINu (osobné identifikačné číslo; niečo, čo poznáte).

Väčšina webových stránok ponúka možnosť overenia prostredníctvom SMS. Pre 2FA sa však čoraz viac presadzujú mobilné zariadenia.

VÝHODY

Výhody sú zrejmé:

- Pretože využíva mobilné zariadenia, ktoré máte (zvyčajne) stále pri sebe, nie sú potrebné žiadne ďalšie tokeny.
- Dynamicky generované prístupové kódy sú bezpečnejšie na používanie ako pevné (statické) prihlasovacie informácie, pretože sa neustále menia.

NEVÝHODY

Existujú však aj nevýhody:

- Nepohodlie – vždy, keď sa vyžaduje overenie, používatelia musia mať nabitý mobilný telefón a musia byť v dosahu mobilnej siete. Prístup je často nemožný bez záložných plánov, keď telefón nedokáže zobraziť správy, napríklad ak je poškodený alebo sa vypne kvôli aktualizácii alebo z dôvodu extrémnych teplôt (napr. v zime). Je možné, že textové správy neprídu okamžite, čo spôsobí ďalšie oneskorenia v autentifikačnom procese v dôsledku kopírovania/prilepovania alebo manuálneho vkladania.

Upozorňujeme, že SMS správy nie sú také bezpečné, ako by ste očakávali. Prenosy SMS správ na mobilné telefóny sú neisté a náchylné na odpočúvanie. V dôsledku toho môžu tretie strany ukradnúť a použiť token. Mobilný telefón 2FA sa často obchádza počas obnovy účtu. Moderné inteligentné telefóny sa používajú na kontrolu e-mailov a prijímanie textových správ. Vo väčšine prípadov ste na svoj e-mail vždy prihlásený. Keďže telefón môže dostať druhý faktor, v prípade straty alebo krádeže telefónu môžu byť napadnuté všetky účty, pre ktoré je e-mail kľúčom. Výsledkom je, že inteligentné telefóny spájajú tieto dve kritériá do jedného. Ak dôjde k odcudzeniu telefónu používateľa, zločinec môže získať prístup k účtom používateľa. Hackeri môžu získať prístup k mobilným telefónnym sieťam klonovaním

SIM kariet. Ak zariadenie nepodporuje SMS, dvojfaktorová autentifikácia prostredníctvom hlasového hovoru je reálnou možnosťou prakticky pre každého.

Mobilná aplikácia Authy

Predpokladajme, že máte inteligentný telefón alebo iné mobilné zariadenie. V takom prípade môžete získať svoj dvojfaktorový autentifikačný kód bez použitia SMS alebo hlasových hovorov stiahnutím a inštaláciou jednej z mnohých obľúbených aplikácií na dvojfaktorovú autentifikáciu priamo do vášho zariadenia. Toto je oveľa bezpečnejší spôsob prihlásenia pomocou dvojfaktorovej autentifikácie. Aplikácie ako Authy a Google Authenticator vytvárajú **TOTP** (***Time-based One-Time Passcode***) priamo v aplikácii.

VÝHODY

Aj keby sa útočníkovi podarilo presvedčiť vášho poskytovateľa mobilných služieb, aby zmenil SIM kartu, stále nebude mať prístup k vašim overovacím kódom. Informácie potrebné na vytvorenie týchto kódov sú uložené vo vašom skutočnom zariadení a nie na karte SIM.

Po nainštalovaní Authy do telefónu budete chcieť nastaviť svoje prvé účty s 2FA. To sa vykonáva naskenovaním QR kódu (poskytnutého webom, na ktorom si chcete zabezpečiť účet) pomocou aplikácie. Po zachytení počiatočného kódu a ochrane prvého účtu pravdepodobne začnete chrániť ďalšie účty.

Obr. 20. Skenovanie QR kódu v mobilnej aplikácii Authy

Teraz si musíte vybrať medzi uchovávaním všetkých svojich tokenov 2FA na jednom zariadení a ich zálohovaním do cloudu.

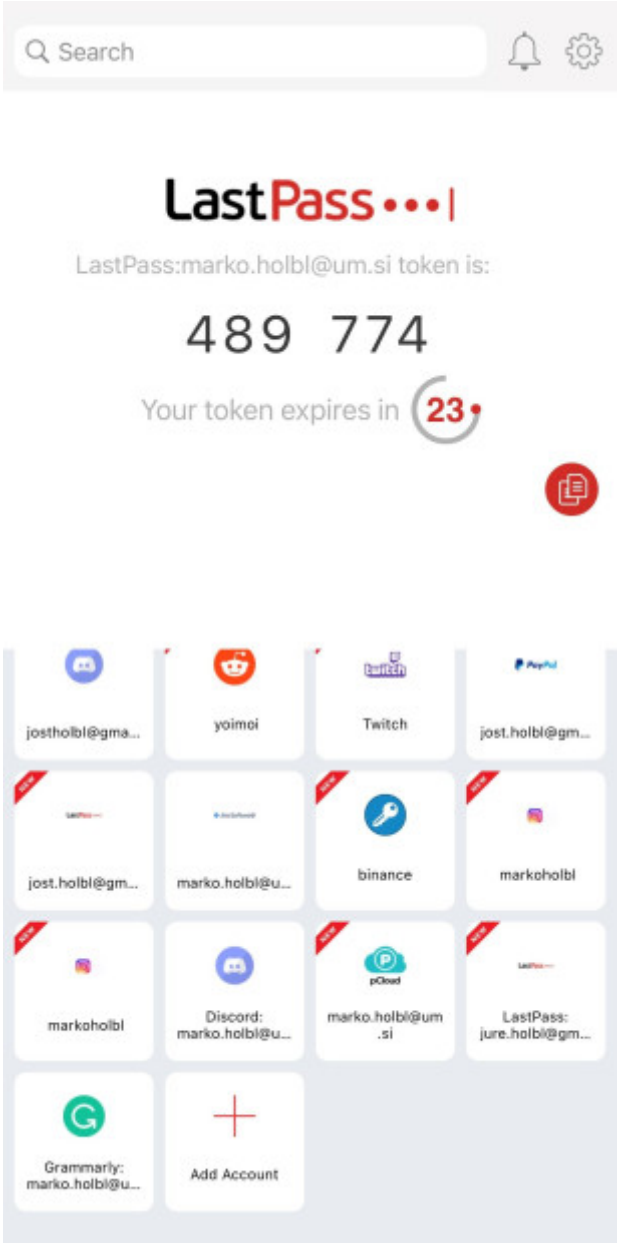
NEVÝHODY

Ak použijete prvú možnosť a potom zariadenie stratíte, aktualizujete/modernizujete alebo vám ukradnú vaše zariadenie, budete musieť presvedčiť každú službu, kde ste si aktivovali 2FA, aby ju vypli. Potom, keď zmeníte telefón, budete sa musieť vrátiť do svojho účtu a manuálne znova povoliť 2FA pre každú službu.

VÝHODY

To je dôvod, prečo vám Authy umožňuje zálohovať vaše 2FA tokeny na bezpečné cloudové úložisko, ku ktorému máte prístup iba vy, takže svoje účty môžete kedykoľvek obnoviť, ak stratíte, bolo vám ukradnuté alebo vymeníte zastarané zariadenie.

Žiadame vás, aby ste si pri zálohovaní tokenov 2FA do cloudu nastavili záložné heslo, ktoré sa použije na šifrovanie vašich údajov a ich synchronizáciu s cloudovou službou. Vaše údaje sú na cloudovej platforme mimoriadne bezpečné, pretože vaše heslo sa nikdy fyzicky neukladá – je však dôležité, aby ste si ho zapamätali.



Obr. 21. Používanie mobilnej aplikácie Authy

Potom sa dôrazne odporúča nainštalovať Authy na iné zariadenie. Aplikácia automaticky synchronizuje tokeny s každým zariadením, na ktorom máte nainštalovanú aplikáciu Authy, ak ste ich synchronizovali s cloudom Authy. Ak máte iba jedno mobilné zariadenie, môžete si stiahnuť aj aplikáciu Authy Desktop

nezávislú od prehliadača.

Interaktivní prvek

4.4 Aspekty bezpečného ukladania hesiel (na strane servera)

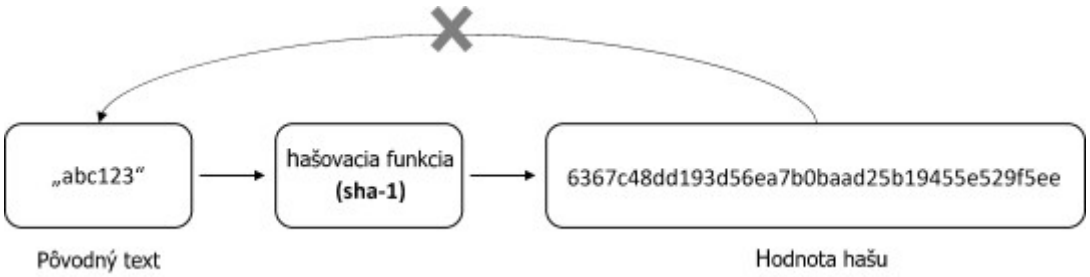
Heslá musia byť dostatočne chránené na strane autentifikátora (zvyčajne servera). Denne je hlásených veľa únikov údajov, preto sa nemožno spoliehať na bezpečnosť systémov autentifikátora. Heslá teda nemôžu byť uložené ako obyčajný text (v otvorenom formáte) a mali by byť uložené chráneným spôsobom. Najprv však stručne predstavíme niektoré pojmy potrebné na pochopenie bezpečného ukladania hesiel.

4.4.1 Ukladanie hašovaných hesiel

DEFINÍCIA

Kryptografická hašovacia funkcia preberá vstup (alebo správu) a vracia alfanumerický reťazec s pevnou dĺžkou.

Reťazec je známy ako hodnota hašu (hash), digitálny odtlačok prsta, odtlačok správy, súhrn (digest) alebo kontrolný súčet.



Obr. 22. Ako funguje hašovanie

Obrázok 22 znázorňuje proces hašovania. Začneme slovom „abc123“ a pomocou hašovacej funkcie SHA-1 získame alfanumerický výstup s pevnou veľkosťou, ktorý nazývame haš alebo hodnota hašu. Pomocou tejto hodnoty hašu nebudeme môcť obnoviť náš pôvodný vstupný text. Nemôžeme previesť hodnotu hašu naspäť, aby sme dostali pôvodný obsah, pretože hašovacie funkcie sú jednosmerné a teda nevratné. Ak ten istý materiál prechádza cez rovnakú hašovaciu funkciu, výsledok výstupu (hašu) by mal byť rovnaký. Takže namiesto ukladania hesla v obyčajnom texte ho môžeme hašovať pomocou hašovacej funkcie a uložiť hodnotu hašu.

meno použív.	heslo
john	abc123
sam	abc123
alice	xyz456

→

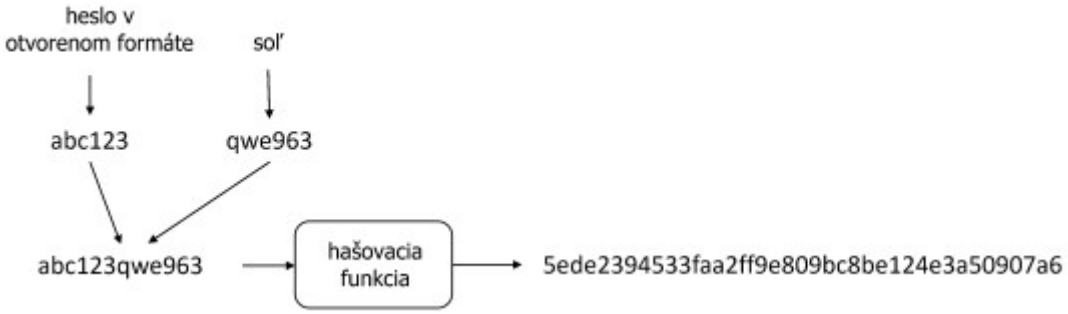
meno použív.	vypočítaný haš hesla
john	6367c48dd193d56ea7b0baad25b19455e529f5ee
sam	6367c48dd193d56ea7b0baad25b19455e529f5ee
alice	0772dbe339a885eb2ed73c1fe842d2ef6e9003a3

Obr. 23. Ochrana uložených hesiel pomocou hašovania

Keď sa používateľ pokúsi prihlásiť do systému, hašovacia funkcia sa použije na hašovanie hesla používateľa a následne jeho porovnanie s hodnotou hašu, ktorá je uložená v tabuľke. Používateľovi môžeme umožniť prihlásiť sa do systému, ak sú obe hodnoty hašu rovnaké. Na obrázku 23 majú John a Sam rovnaké heslo „abc123“ a hodnoty ich hašov sú po použití hašovacieho algoritmu rovnaké. Zvážte prípad, keď má John prístup k databáze a vidí haš hesla. Potom John môže vidieť, že hodnota hašu jeho hesla je rovnaká ako hodnota hašu hesla Sama. Výsledkom je, že John bude môcť použiť osobné údaje Sama na prihlásenie sa do systému. Aby sme sa tomu vyhli, môžeme použiť techniku nazývanú solenie.

4.4.2 Hašovanie so soľou

Naším cieľom je pomocou hašovania so soľou (náhodným reťazcom) urobiť hodnotu hašu hesla jedinečnou. Systém teda generuje náhodnú postupnosť znakov nazývanú soľ. Keď používateľ zadá heslo vo formáte obyčajného textu, pripojí sa k nemu vytvorená náhodná postupnosť znakov. Potom sa pomocou hašovacej funkcie extrahuje hodnota hašu z vloženého textu (solené hašovanie). V tomto prípade musí byť hodnota soli každého používateľa uložená.



Obr. 24. Proces soleného hašovania

Aj keď majú John a Sam rovnaké heslo, hodnoty ich hašov sú odlišné (pozri obrázok 25).

Interaktívní prvek

Počas procesu prihlásenia systém získa z databázy príslušnú hodnotu soli používateľa, pripojí ju k vstupnému heslu, aplikuje hašovaciu funkciu a porovná výslednú hodnotu hašu s hodnotou hašu zaznamenanou v tabuľke. Používateľ je úspešne overený (autentifikovaný), ak sa obe hodnoty hašov zhodujú.

meno_použ.	solená_hodnota	solené_hašované_heslo
john	qwe963	5ede2394533faa2ff9e809bc8be124e3a50907a6
sam	hjk521	6367c48dd193d56ea7b0baad25b19455e529f5ee
alice	asd753	0772dbe339a885eb2ed73c1fe842d2ef6e9003a3

Obr. 25. Príklad tabuľky uchovávajúcej solené a hašované heslá

Minimálna ochrana uložených hesiel by mala zahŕňať hašovanie a používanie solí. Okrem toho NIST navrhuje:

- uzamknúť systém pred používateľom, ak príliš veľakrát použije nesprávne heslo (napr. po troch neúspešných pokusoch to používateľ môže skúsiť až o jednu minútu),
- povoliť emotikony, znaky ASCII a Unicode v heslách
- a povoliť funkcie kopírovania a vkladania (copy/paste) do polí pre heslá, aby bolo používanie správcov hesiel a viacfaktorová autentifikácia pohodlnejšia.

Interaktivní prvek

KAPITOLA 5

Autentifikácia bez hesla

Vzhľadom na všetky problémy a slabé stránky hesiel nie je myšlienka autentifikácie bez hesiel nová. Ako už názov napovedá, autentifikácia bez hesla umožňuje používateľovi prihlásiť sa alebo získať prístup bez zadania hesla alebo zodpovedania bezpečnostných otázok. Autentifikácia bez hesla znižuje potrebu nebezpečných hesiel a ich administráciu a zároveň zlepšuje bezpečnosť používateľských účtov znížením ich zraniteľnosti voči útokom. Existujú rôzne mechanizmy autentifikácie bez hesla, ako sú bezdotykové karty/odznaky (proximity cards/badges), fyzické tokeny, zariadenia/kľúče USB, magické odkazy (magic links), biometrické rozpoznávanie, mobilné aplikácie atď. Väčšina týchto techník sa bežne používa pri viacfaktorovej autentifikácii na zvýšenie bezpečnosti. Niektoré z týchto riešení však možno použiť ako systém overovania prvého faktora (typu).

Prvky autentifikácie bez hesla sa zvyčajne delia do dvoch kategórií:

- Príkladmi **prvkov vlastníctva** sú inteligentné telefóny, tokeny OTP, čipové karty alebo hardvérové tokeny („niečo, čo používateľ má“).
- Príkladmi **základných (vrodených) faktorov** sú odtlačky prstov, skeny sietnice, rozpoznávanie tváre alebo hlasu a iné biometrické identifikátory („niečo, čím používateľ je“).

Autentifikácia bez hesla sa často zamieňa s viacfaktorovou autentifikáciou (MFA), pretože obe používajú rôzne autentifikačné faktory. Zatiaľ čo sa však MFA používa ako ďalšia vrstva zabezpečenia popri autentifikácii založenej na hesle, autentifikácia bez hesla nevyžaduje zapamätané tajomstvo a zvyčajne používa iba jeden vysoko bezpečný faktor na autentifikáciu identity, vďaka čomu je pre používateľov rýchlejšia a jednoduchšia.

Heslá sa ťažko pamätajú a požiadavky sú čoraz zložitejšie. Rôzne stránky môžu mať rôzne pravidlá hesiel, takže heslo vygenerované pre jednu stránku nemusí fungovať na inej. Zapamätať si heslo vygenerované pre modernú rozšírenú politiku hesiel je často náročné.

Podobne ako pri **FIDO** (***Fast Identity Online***) aj tu vstupujú do hry rôzne štandardy. Hoci autentifikácia bez hesla a technológia FIDO existujú už nejaký čas, online služby a poskytovatelia identity ich ešte len musia nasadiť vo väčšom meradle. Autentifikácia bez hesla sa stane budúcnosťou autentifikácie vďaka začleneniu biometrických možností do väčšiny moderných mobilných zariadení a notebookov.

VÝHODY

Autentifikácia bez hesla vylepšuje pohodlie koncového používateľa tým, že odstraňuje trápenie sa s heslom. Používateľ už nemusí vytvárať dlhšie a bezpečnejšie heslo a môže získať jednotný prístup ku všetkým programom jednoduchým pripojením k USB zariadeniu alebo naskenovaním

odtlačku prsta.

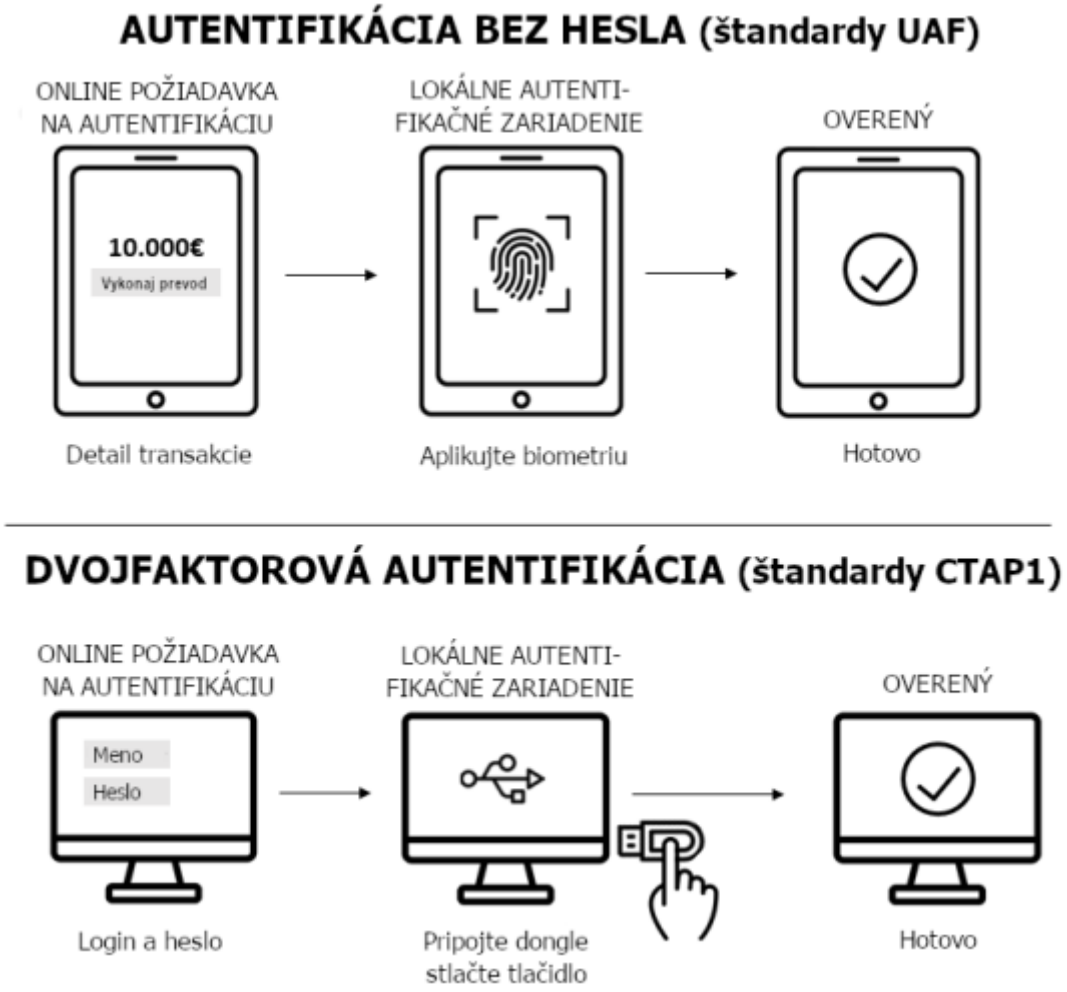
5.1.1 FIDO (Fast Identity Online)

FIDO je súbor otvorených autentifikačných protokolov vytvorených alianciou FIDO Alliance na odstránenie hesiel. Na implementáciu bezpečnej autentifikácie používajú protokoly FIDO základné kryptografické algoritmy s verejným kľúčom. Súkromné kľúče nikdy neopustia bezpečnostné zariadenie a všetky konverzácie budú šifrované.

Obr. 26. Príklad autentifikácie založenej na FIDO

Aliancia FIDO vydala tri súbory noriem:

- **UAF** (***Universal Authentication Framework***): Funkcia autentifikácie bez hesla je súčasťou protokolu FIDO UAF. Používatelia, ktorí používajú tento protokol, by mali podpísať výzvu poskytnutú serverom FIDO pomocou jedného alebo viacerých bezpečnostných faktorov dostupných v ich bezpečnostnom/digitálnom zariadení.
- **U2F** (***Universal Second Factor***): Funkciu dvojfaktorovej autentifikácie poskytuje protokol FIDO U2F. Na zistenie totožnosti musia používatelia poskytnúť dva dôkazy (faktory). Toto bolo premenované na CTAP1 so spustením protokolu FIDO2.
- FIDO2: Najnovší súbor špecifikácií aliancie FIDO je známy ako FIDO2.



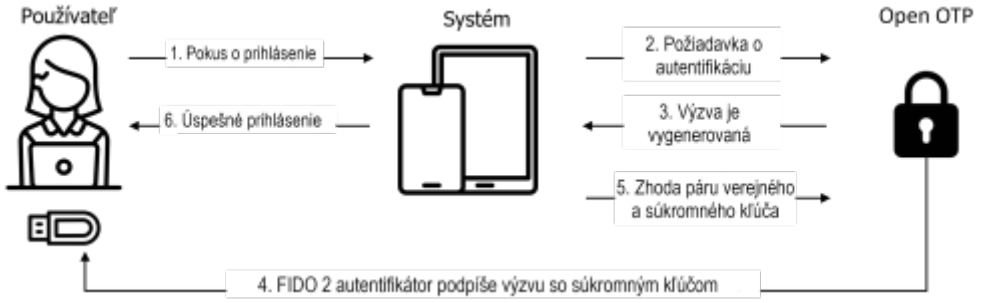
Obr. 27. Štandardy UAF a U2F (CTAP1) pre autentifikáciu bez hesla

5.1.2 FIDO2 a WebAuthn

Špecifikácia FIDO2 pozostáva z:

- štandardu W3C WebAuthn (Web Authentication) a
- protokolu FIDO **CTAP2** (***Client to Authenticator Protocol 2***).

FIDO2 umožňuje používateľom používať bežné zariadenia na jednoduchú autentifikáciu k internetovým službám v mobilnom aj desktopovom kontexte. WebAuthn je štandardné online API pre autentifikáciu FIDO, ktoré je začlenené do platforiem a prehliadačov. CTAP2 je verzia CTAP, ktorá používateľom umožňuje používať externé a vstavané autentifikátory na poskytovanie bezheslovej, dvojfaktorovej alebo viacfaktorovej autentifikácie. WebAuthn API je nástroj na vytváranie a správu poverení verejného kľúča. Prehľad metódy autentifikácie FIDO2 je znázornený na obrázku 28.



Obr. 28. Spôsob autentifikácie podľa FIDO2

Interaktivní prvek

KAPITOLA 6

Úvod do digitálneho podpisovania

DEFINÍCIA

Matematický systém na kontrolu platnosti digitálnych správ alebo dokumentov je známy ako digitálny podpis.

Skutočný digitálny podpis dáva príjemcovi dobrý dôvod domnievať sa, že správu vytvoril známy odosielateľ (autenticita) a že nebola pozmenená pri prenose, ak sú splnené predpoklady (integrita).

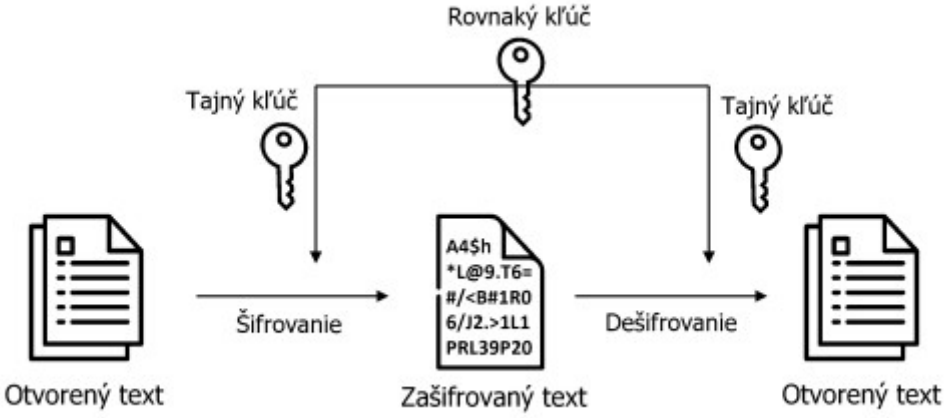
Hlavné ciele, ktoré sa digitálny podpis snaží dosiahnuť, sú:

- **Autenticita**: Digitálne podpisy sú viazané na konkrétneho používateľa prostredníctvom jeho súkromného kľúča. Vďaka tomu je možné určiť, kto vlastní súkromný kľúč použitý na podpísanie pôvodných údajov/správ (napr. dokumentu, e-mailu alebo súboru). Ďalšie informácie o súkromných a verejných kľúčoch nájdete nižšie.
- **Integrita**: V digitálnych podpisoch sa používa technika hašovania, aby sa zabezpečilo, že so správou nebude manipulované. Viac o hašovaní nájdete nižšie.

Digitálne podpisy sú teda jedným zo spôsobov, ako autentifikovať entitu. Najprv si treba objasniť niektoré pojmy, kým sa ukáže, ako sa dá digitálny podpis použiť pri autentifikácii.

6.1 Kryptografia s verejným kľúčom

Aby sme pochopili digitálne podpisy, musíme najprv vysvetliť asymetrickú kryptografiu, často označovanú ako kryptografia s verejným kľúčom. Na rozdiel od klasického (symetrického) šifrovania, ktoré používa na šifrovanie iba jeden kľúč, asymetrické šifrovanie využíva pár kľúčov. Šifrovanie je proces kódovania informácií, ako je znázornené na obrázku 29.



Obr. 29. Symetrické šifrovanie

Predstavte si, že chcete niekomu poslať zašifrovanú správu pomocou klasického šifrovania. V tomto scenári sa obe strany musia dohodnúť na jedinom kľúči. Nemôžete si ho navzájom prenášať, pretože potom ho môže niekto vidieť a bude môcť vidieť všetky vaše správy.

DEFINÍCIA

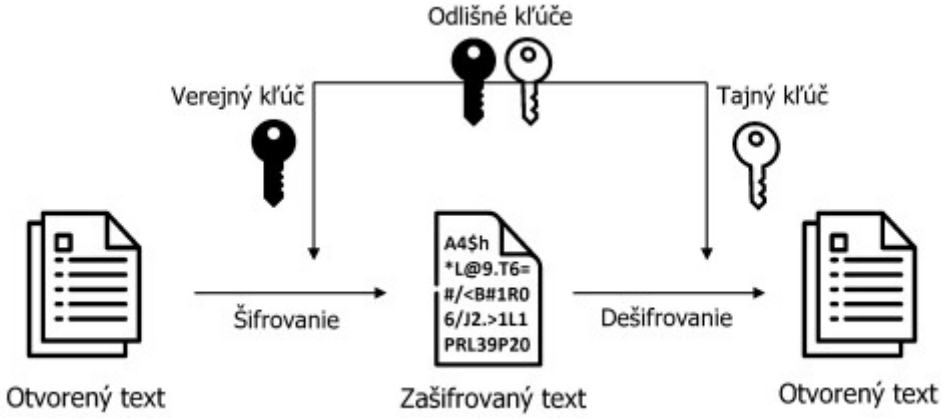
Na druhej strane, asymetrické šifrovanie využíva pár kľúčov, verejný a súkromný kľúč, ktoré k sebe matematicky patria. Iba prepojený súkromný kľúč môže dešifrovať to, čo je zašifrované verejným kľúčom.

Ak teraz niekto chce, aby mu iní posielali zašifrované správy, jednoducho zverejní svoj verejný kľúč, aby ho každý videl. Potom jednoducho použije svoj súkromný kľúč na dešifrovanie správ zašifrovaných jeho verejným kľúčom, keďže správy zašifrované jeho verejným kľúčom je možné dešifrovať iba jeho súkromným kľúčom. Je to užitočné, pretože sa netreba obávať zdieľania verejného kľúča bezpečným spôsobom.

Stručne povedané, pre bezpečnú komunikáciu dvoch strán pomocou asymetrického šifrovania je proces nasledujúci:

- Verejné kľúče si vymieňajú obe strany.
- Osoba 1 zašifruje správu, ktorú chce odoslať, pomocou verejného kľúča osoby 2 a odošle ju osobe 2.
- Osoba 2 dešifruje správu pomocou svojho súkromného kľúča.

Tento proces je znázornený na obrázku 30.



Obr. 30. Proces asymetrického šifrovania (na základe verejného kľúča)

DEFINÍCIA

Digitálne podpisy fungujú tak, že čokoľvek podpíšu (zašifrujú) súkromným kľúčom, sa potom overí verejným kľúčom, ktorý je s ním spojený. Takže jednotlivé kľúče z daného páru kľúčov sa používajú opačne.

Dôvodom je, že podpisovateľ je jedinou osobou s prístupom k súkromnému kľúču použitému na podpis. Preto si môžete byť istí, že to podpísala táto osoba. Každý môže použiť verejný kľúč na overenie (t. j. na úspešné dešifrovanie správy), že vlastník verejného kľúča správu vytvoril.

Interaktivní prvek

6.2 Proces digitálneho podpisovania

Ako už bolo spomenuté pri digitálnom podpisovaní, používa sa pár kľúčov, ktorý pozostáva z verejného a súkromného kľúča. Páry kryptografických kľúčov sa používajú na šifrovanie (uzamykanie) a dešifrovanie (odomykanie) zdrojových údajov rovnakým spôsobom, ako sa fyzické kľúče používajú na zamykanie a odomykanie. Súkromné kľúče sa uchovávajú v bezpečí a tajnosti, pretože ak sa niekto dozvie súkromný kľúč inej osoby, môže podpísať zdrojové údaje ako táto osoba. Na druhej strane sa predpokladá, že verejné kľúče budú zdieľané so všetkými. Údaje zašifrované súkromným kľúčom možno dešifrovať iba verejným kľúčom, čím sa odkryjú pôvodné údaje.

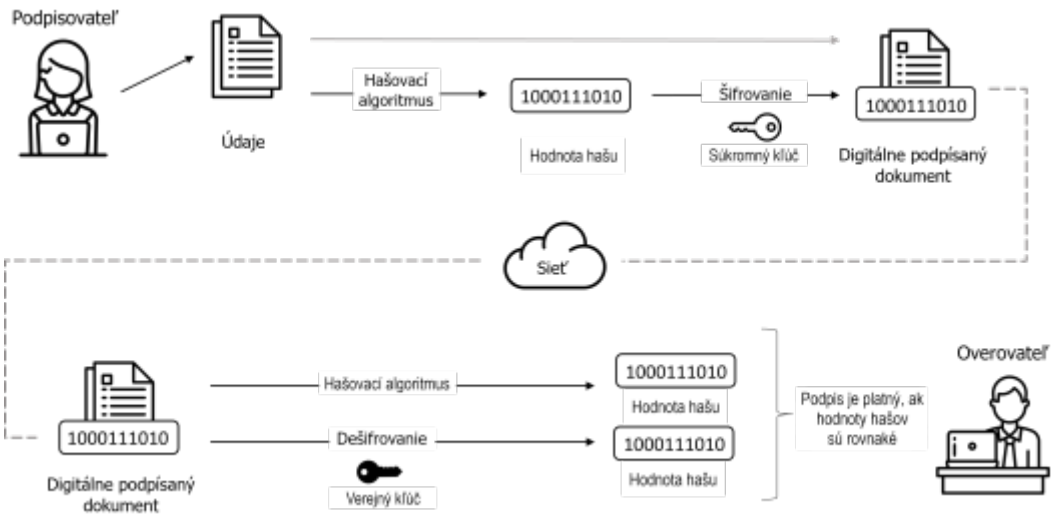
DEFINÍCIA

Proces digitálneho podpisovania zahŕňa asymetrickú kryptografiu a hašovacie funkcie.

Tieto dva stavebné bloky sa kombinujú a tvoria skutočný proces podpisovania takto

1. Pomocou metódy hašovania odosielateľ vypočíta haš zdrojového obsahu, ktorý chce doručiť.
2. Odosielateľ zašifruje vypočítaný haš svojim súkromným kľúčom, aby vytvoril digitálny podpis.
3. Potom môžete obsah a digitálny podpis odoslať príjemcovi.
4. Po prijatí správ príjemcom použije príjemca verejne dostupný verejný kľúč odosielateľa na dešifrovanie zašifrovaného digitálneho podpisu odosielateľa. V prípade úspechu sa potvrdí identita odosielateľa ako vlastníka súkromného kľúča použitého na šifrovanie súboru.
5. Príjemca potom získa pôvodný obsah z prijatej správy a vygeneruje haš tohto obsahu.
6. Ak sa vypočítaný haš príjemcu zhoduje s odosielateľom vloženým hašom, obsah je overený ako identický s tým, čo odoslal odosielateľ. Ak sa hodnoty hašov nezhodujú, obsah bol sfalšovaný, a preto podpis nie je platný.

Grafické znázornenie procesu je na obrázku 31.



Obr. 31. Schematické znázornenie vytvorenia a overenia digitálneho podpisu

Keďže verejný kľúč odosielateľa je verejne dostupný, každý môže dešifrovať zašifrovaný obsah, ktorý odosielateľ odosiela. Výsledkom je, že táto metóda šifrovania overuje iba integritu, nie dôvernosť.

Niekto by sa mohol opýtať, prečo generujeme hodnotu hašu údajov pred ich podpísaním. Jednoducho preto, že podpis je oveľa menší a proces vytvárania a overovania digitálneho podpisu je rýchlejší, keďže sa porovnávajú iba hodnoty hašov a nie celé dáta/dokument. Všimnite si, že to funguje, pretože hašovacie algoritmy vždy vytvárajú hodnotu nastavenej dĺžky.

VÝHODY

Ako ste možno uhádli, digitálne podpisy poskytujú niekoľko výhod, vrátane nasledujúcich:

- zvyšujú bezpečnosť a dôveru, pretože sa nedajú spätne analyzovať alebo sfalšovať;
- poskytujú záruku, že autor podpisu nemôže neskôr poprieť svoje autorstvo (non-repudiation);
- zabezpečujú integritu prenášaných údajov.

NEVÝHODY

Digitálne podpisy však majú aj nevýhody, ako napríklad:

- skutočnosť, že neexistuje spôsob, ako odvolať podpisy (dôveru zdrojovým údajom) po ich distribúcii, čím sa rozhodnutia stanú nezvratnými;
- používanie verejných kľúčov znemožňuje utajenie. Každý, kto má verejný kľúč, môže overiť podpis.

Interaktivní prvek

Interaktivní prvek

KAPITOLA 7

Infraštruktúra verejného kľúča

Už sme sa dozvedeli o koncepcii digitálneho podpisovania a kryptografie s verejným kľúčom. Ako sa ukazuje, na správne fungovanie celého konceptu v reálnom živote potrebujeme niečo viac. Potrebujeme niečo, čo sa nazýva infraštruktúra verejného kľúča (PKI).

DEFINÍCIA

PKI je súbor technológií, procesov a entít, ktoré umožňujú bezpečnú komunikáciu cez nezabezpečené verejné siete.

Napríklad PKI je to, čo pridáva S k HTTPS, a ak si prezeráte tento obsah vo webovom prehliadači, pravdepodobne ho používate, aby ste sa uistili, že pochádza z dôveryhodného zdroja. PKI umožňuje regulovaný prístup k systémom a zdrojom, ochranu údajov a zodpovednosť za transakcie stanovením identity jednotlivcov, zariadení a služieb.

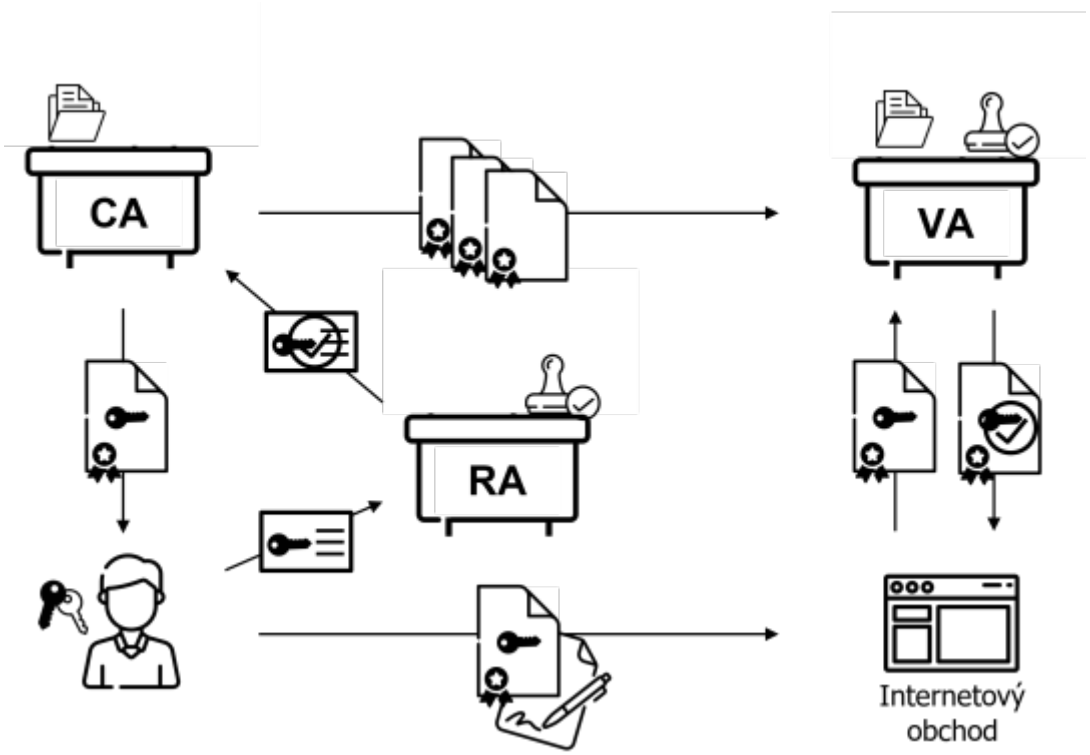
PKI sa využíva v rôznych aplikáciách vrátane zabezpečenia komunikácie na Internete vecí (IoT) a podpisovania digitálnych dokumentov. PKI, ktorá je založená na asymetrickej kryptografii, sa bežne používa na nastavenie bezpečnej elektronickej komunikácie, ako je online nakupovanie, bankovníctvo a e-maily, komunikácia medzi používateľmi a webovými stránkami, ku ktorým sa pripájajú pomocou protokolu HTTPS. PKI umožňuje silnú autentifikáciu, šifrovanie údajov a digitálne podpisy pre ľudí, služby a objekty poskytovaním digitálnych identít. Tieto bezpečnostné metódy poskytujú bezpečný prístup k fyzickým a digitálnym zdrojom, zabezpečenú komunikáciu medzi ľuďmi, službami a vecami a digitálne podpisovanie dokumentov, transakcií alebo iných údajov.

7.1 Komponenty infraštruktúry verejného kľúča

PKI sa skladá z nasledujúcich komponentov:

- certifikačná autorita (CA),
- registračná autorita (RA),
- validačná autorita (VA),
- digitálne certifikáty.

A, samozrejme, kryptografia s verejným kľúčom (PKC).



Obr. 32. Komponenty infraštruktúry verejného kľúča (PKI)

Certifikačná autorita

DEFINÍCIA

Certifikačná autorita je spoločnosť, ktorá vytvára a distribuuje digitálne certifikáty.

Digitálny certifikát overuje, že menovaný subjekt certifikátu vlastní verejný kľúč. Ostatné (spoliehajúce sa strany) môžu dôverovať podpisom a tvrdeniam o súkromnom kľúči, ktorý sa zhoduje s certifikovaným verejným kľúčom. CA slúži ako dôveryhodná tretia strana, ktorej dôveruje subjekt certifikátu (vlastník) ako aj strana, ktorá sa na certifikát spolieha.

Podpisovanie certifikátov používaných v HTTPS (protokole bezpečného surfovania) je jedným z najbežnejších spôsobov použitia certifikačných autorít. Ďalšou populárnou aplikáciou je pre národné

vlády vydávanie preukazov totožnosti, ktoré možno použiť na digitálne podpisovanie alebo elektronickú verejnú správu.

Registračná autorita

DEFINÍCIA

V infraštruktúrach verejných kľúčov vykonáva registračná autorita (RA) funkciu registrácie certifikátov. Má na starosti prijímanie žiadostí o vydanie certifikátov od jednotlivcov, serverov, vecí a iných aplikácií, či už ide o počiatočnú registráciu alebo obnovenie. Tieto žiadosti overuje registračná autorita a postúpi ich certifikačnej autorite (CA).

Aj pri riadení životného cyklu certifikátov sa zúčastňuje registračná autorita. Zvážte prípad odvolania. RA zahŕňa obchodnú logiku na prijímanie žiadostí vrátane metód na overenie pôvodu žiadateľa a strany, ktorá by mala mať certifikát.

Z dôvodov dostupnosti a bezpečnosti je registračná autorita zvyčajne oddelená od certifikačnej autority. K RA je možné pristupovať cez používateľsky prívetivé GUI alebo pomocou API a štandardných protokolov, ktoré sa ľahko integrujú.

Validačná autorita

Certifikáty PKI sú overované validačným úradom (autoritou). Prístup k **zoznamom zrušených certifikátov** (CRL), protokol **OCSP** (***Online Certificate Status Protocol***) a sťahovanie **reťazcov certifikátov CA** sú príkladmi služieb overovania certifikátov. Pretože certifikáty je možné vydávať a odvolávať, je dôležité overiť pravosť certifikátu skôr, ako mu začnete dôverovať. Úlohou validačného orgánu je vyriešiť tento problém.

Vydávajúca certifikačná autorita je zodpovedná za poskytovanie aktualizácií stavu certifikátu validačnej autorite podľa zavedenej politiky. Pri používaní zoznamu CRL (CA) sa spoliehate na to, že každá pripojená certifikačná autorita vydá zoznam zrušených digitálnych certifikátov.

Digitálny certifikát

Digitálny certifikát je typ elektronickej identifikácie pre jednotlivé subjekty alebo organizácie, podobne ako ID. Obsahuje informácie, ako je identifikácia, sériové číslo a doba platnosti. V informáciách vidíme aj digitálny podpis certifikačnej autority, ktorý zabezpečuje pravosť certifikátu a verejný kľúč držiteľa certifikátu. Napríklad PKI umožňuje autentifikované spojenia a v kombinácii s inými kryptografickými prístupmi tiež zabezpečuje spojenia medzi dvoma komunikujúcimi strojmi, pretože identity dvoch strán možno potvrdiť pomocou digitálnych certifikátov. Takmer všetky v súčasnosti vydávané certifikáty zodpovedajú štandardu X.509.

Existujú certifikáty rôznych typov:

- **Certifikáty na podpisovanie kódu**: Kód bol overený ako kód pochádzajúci od vývojárov a nebol upravený, vďaka čomu je softvér dôveryhodný. Používa sa na podpisovanie verzií softvéru a overovanie softvéru od predajcu alebo vývojára, aby sa potvrdilo, že je legitímny.

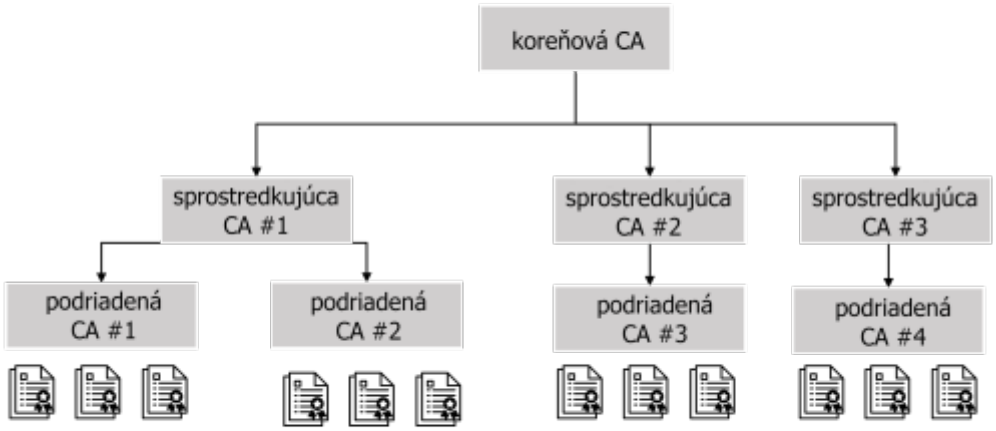
- **E-mailové certifikáty**: Protokol S/MIME možno použiť na ochranu a overenie e-mailov, čo umožňuje odosielateľovi určiť autorstvo a zabrániť neoprávnenej manipulácii.
- **Certifikáty na podpisovanie dokumentov**: Na podpisovanie dokumentov by sa mali používať programy Adobe, Microsoft a ďalšie softvérové programy, aby sa zaistilo, že budú nezmenené a dôveryhodné. Tento typ certifikátov sa takmer vždy používa, keď na dokumente vidíte digitálny podpis.
- **Certifikáty TLS (HTTPS)**: Používajú sa na zabezpečené spojenia HTTPS.

Obr. 33. Príklad digitálneho certifikátu v systéme Microsoft Windows

Interaktivní prvek

7.2 Hierarchická štruktúra infraštruktúry verejného kľúča

V PKI je bežná hierarchia certifikačných autorít, ktoré podpisujú a vydávajú digitálne certifikáty alebo osobné údaje. Podriadené (lokálne) CA majú právomoc podpisovať digitálne certifikáty pre zariadenia od každej CA. Koncové zariadenia (v spodnej časti hierarchie) oznamujú digitálne certifikáty, ktoré sú povolené lokálnymi certifikačnými autoritami nad nimi, ktoré ich vygenerovali a podpísali. Tie sa niekedy označujú ako certifikácie zariadení. Lokálne CA, ktoré vytvárajú certifikáty zariadení, majú svoj vlastný certifikát, ktorý je autorizovaný digitálnym podpisom CA nad nimi (nadriadenej CA) atď. PKI nakoniec dosiahne koreň, ktorý slúži ako základ pre túto konkrétnu doménu ekosystému PKI.



Obr. 34. Príklad hierarchie PKI

Môžeme povoliť špecifické úrovne odvolania alebo odmietnutia prístupu v prípade úniku alebo kompromitácie súkromného kľúča v ekosystéme nasadením hierarchií do ekosystémov PKI.

Každý môže odvolať certifikát u akéhokoľvek prvku PKI, od zariadenia až po CA na najvyššej (koreňovej) úrovni, v závislosti od povahy narušenia bezpečnosti. Toto zrušenie certifikátu však zruší čokoľvek aj pod týmto prvkom v hierarchii.

Okrem toho to ukazuje, prečo sú implementácie PKI organizované v stromových hierarchiách. Tento dizajn umožňuje vlastníkovi ekosystému vykonávať selektívnu kontrolu poškodenia v prípade prelomenia/narušenia. To je dôvod, prečo vydávanie certifikátov zariadení z koreňovej CA nie je dobrý nápad, pretože to obmedzuje flexibilitu. Ak sa v tomto prípade niečo pokazí, možno budeme musieť

zneplatniť a odvolať celý PKI a všetky nasadené zariadenia v teréne. Výsledkom je, že certifikáty zariadení prakticky vždy vydávajú podriadené CA pod koreňovou certifikačnou autoritou.

7.3 Životný cyklus digitálneho certifikátu

Životný cyklus digitálneho certifikátu začína jeho vytvorením a možno ho stručne vysvetliť takto:

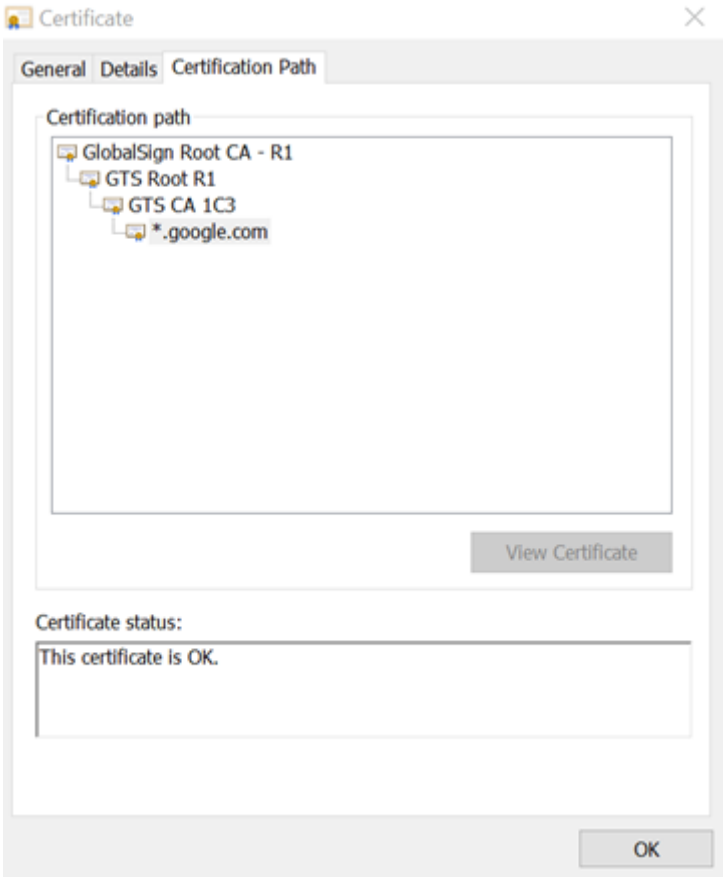
- **Registrácia certifikátu**: Certifikačná autorita (CA) dostane žiadosť o certifikát od nejakej entity (subjektu). Za entitu možno považovať osobu, zariadenie alebo dokonca niekoľko riadkov kódu.
- **Vydanie certifikátu**: RA musí overiť totožnosť žiadateľa, čo sa zvyčajne vykonáva prostredníctvom osobných údajov alebo spoliehaním sa na totožnosť inej RA, ktorá už žiadateľa overila.
- **Overenie certifikátu**: Server sa spája s CA zakaždým, keď sa certifikát použije na autentifikáciu, aby sa uistil, že je stále platný a či nevypršala platnosť alebo nebol odvolaný.
- **Zrušenie certifikátu**: Pri prvom vydaní certifikátov je uvedený dátum vypršania platnosti. Keď tento dátum uplynie, certifikačná autorita zaradí certifikát do zoznamu zrušených certifikátov (CRL), čo je forma čiernej listiny, ktorá hovorí serveru, aby nedôveroval určitým certifikátom.
- **Obnova certifikátu**: CA môže byť nakonfigurovaná tak, aby automaticky obnovovala certifikáty, keď nastane dátum vypršania platnosti, aj keď zvyčajne vyžaduje opätovné overenie identity.

Interaktivní prvek

Certifikačné autority a reťazec dôvery

Pojem "reťazec dôvery" sa odvoláva na vzťah medzi digitálnym certifikátom a dôveryhodnou CA. Aby bol certifikát dôveryhodný, musí byť vysledovateľný späť až k dôveryhodnému koreňu, ktorým bol vydaný, čo znamená, že všetky certifikáty v reťazci – server, sprostredkovateľ a koreň – musia byť dôveryhodné.

Na obrázku 35 môžeme vidieť, že pre server google.com je GTS-CA 1C3 CA nižšej úrovne. GTS-Root R1 je CA strednej úrovne. R1 je koreňová CA pre GlobalSign. Pri tejto metóde je možné vytvoriť reťazec dôvery.



Obr. 35. Príklad reťazca dôvery

Reťazec dôvery má 3 časti:

- **Koreňový certifikát** je digitálny certifikát, ktorý patrí certifikačnej autorite, ktorá ho vydala. Väčšina prehliadačov ho má napríklad predinštalovaný a je uložený v „dôveryhodnom úložisku“. Certifikačné autority pozorne sledujú koreňové certifikáty. Napríklad GlobalSign Root CA-R1 je koreňová CA.
- **Sprostredkovacie (intermediate) certifikáty** sú ako konáre na strome a koreňový certifikát je ako kmeň stromu. Slúžia ako prepojenie medzi chránenými koreňovými certifikátmi a verejne vydanými serverovými certifikátmi. Vždy bude existovať aspoň jeden sprostredkovací certifikát v reťazci, ale môže ich byť viac.
- **Certifikát servera** je ten, ktorý bol udelený určitej doméne (v tomto prípade www.google.com).

7.4 Autentifikácia pomocou PKI a PKC

V digitálnom svete je infraštruktúra verejného kľúča (PKI) systémom na autentifikáciu ľudí a zariadení. Jedna alebo viac dôveryhodných strán digitálne podpisuje dokumenty, ktoré overujú, že konkrétny kryptografický kľúč patrí konkrétnemu používateľovi alebo zariadeniu. Kľúč potom možno použiť ako identitu používateľa v digitálnych sieťach.

Digitálne certifikáty je možné použiť aj v 2FA alebo pri autentifikácii bez hesla.

Keď sa používateľ pokúsi overiť svoju identitu na serveri, server vytvorí náhodné údaje a odošle ich používateľovi. Používateľ potom zašifruje údaje pomocou svojho súkromného kľúča a vráti ich späť na server. Server dešifruje údaje pomocou verejného kľúča digitálneho certifikátu používateľa a ak sa dešifrované údaje zhodujú s prijatými údajmi, server vie, že používateľ je tým, za koho sa vydáva. Toto je základný proces používania PKI+PKC na účely autentifikácie.

KAPITOLA 8

Test

Najbezpečnejší spôsob ukladania hesiel je:

- ◯ šifrovanie
- ◯ hašovanie
- ◯ otvorený text
- ◯ solené hašovanie

Čo je cieľom autentifikácie?

- ☐ overiť identitu niekoho
- ☐ identifikovať niekoho
- ☐ skontrolovať, k čomu môže niekto pristupovať
- ☐ je podstatnou časťou kyberbezpečnosti

Solenie hesiel sťažuje útočníkovi útok, pretože slovníkový útok je špecifický pre:

- ◯ každého používateľa
- ◯ každého útočníka
- ◯ každé zariadenie
- ◯ každé heslo

Aké sú najbežnejšie metódy overovania?

- ☐ používateľské meno a heslo
- ☐ sken tváre

- ☐ email a heslo
- ☐ RSA SecureID

Aká je najvýraznejšia zraniteľnosť autentifikácie založenej na vlastnosti „niečo, čím si“?

- ◯ je nepopierateľná
- ◯ to niečo môže byť stratené
- ◯ to niečo, môže byť zabudnuté
- ◯ to niečo môže byť ukradnuté

Aké sú hlavné kategórie autentifikácie?

- ☐ to, ako vyzeráte
- ☐ niečo, čo poznáte
- ☐ niečo, čím ste
- ☐ niečo, čo máte

Čo je to viacfaktorová autentifikácia?

- ◯ Autentifikácia, ktorá používa aspoň dva rôzne faktory pre autentifikáciu.
- ◯ Autentifikácia, ktorá používa presne dva rôzne faktory pre autentifikáciu.
- ◯ Autentifikácia, ktorá používa presne jeden faktor pre autentifikáciu.
- ◯ Je rovnaká ako dvojfaktorová autentifikácia (2FA).

Príklady overenia pomocou princípu „čo máte“ zahŕňajú:

- ☐ inteligentný telefón
- ☐ heslo
- ☐ odtlačok prsta
- ☐ čipová karta

Základný proces autentifikácie zahŕňa:

- ☐ server
- ☐ autentifikačné údaje
- ☐ používateľ
- ☐ kľúčové slovo

Komu sa v metóde autentifikácie založenej na výzve/odpovedi posiela výzva?

- ◯ používateľovi
- ◯ serveru
- ◯ programu
- ◯ autentifikátorovi

Aké dlhé by mali byť heslá podľa aktuálnych pokynov a osvedčených postupov?

- ◯ 6 znakov
- ◯ 4 znaky
- ◯ 7 znakov
- ◯ aspoň 12 znakov

Časti metódy autentifikácie sú:

- ☐ vstup
- ☐ overovateľ
- ☐ počítač
- ☐ prenosový systém

Ktoré prvky (faktory) možno použiť na dvojfaktorovú autentifikáciu?

- ☐ správa SMS
- ☐ identifikačný token
- ☐ aplikácia na inteligentnom telefóne
- ☐ používateľské meno

Čo robia hašovacie funkcie?

- ◯ vytvárajú hashtag
- ◯ vypočítavajú jedinečný identifikátor údajov
- ◯ vytvárajú heslá
- ◯ ochraňujú autentifikáciu

Súčasné priemyselné štandardy pre bezpečné ukladanie hesiel zahŕňajú:

- ☐ šifrovanie
- ☐ hašovanie
- ☐ ukladanie v otvorenom formáte
- ☐ solené hašovanie

Aký je štandard pre autentifikáciu bez hesla?

- ◯ FIDO2
- ◯ FIBA
- ◯ UFI
- ◯ UPA

Aký druh útokov sťažuje technika solenia hesla?

- ☐ slovníkové útoky
- ☐ útoky hrubou silou

- ☐ útoky na server
- ☐ útoky na mobilné zariadenia

V akom poradí proces digitálneho podpisovania používa kľúče?

- ◯ súkromný kľúč odosielateľa a verejný kľúč príjemcu
- ◯ súkromný kľúč odosielateľa a verejný kľúč odosielateľa
- ◯ súkromný kľúč príjemcu a verejný kľúč príjemcu
- ◯ verejný kľúč odosielateľa a súkromný kľúč príjemcu

Ak sa na účely šifrovania používa kryptografia verejného kľúča, ktorý kľúč sa používa na šifrovanie údajov?

- ◯ verejný kľúč príjemcu
- ◯ verejný kľúč odosielateľa
- ◯ súkromný kľúč príjemcu
- ◯ súkromný kľúč odosielateľa

Aké sú slabé miesta autentifikačnej techniky založenej na „niečom, čo poznáte“?

- ☐ to niečo môže byť zabudnuté
- ☐ to niečo môže byť stratené
- ☐ to niečo môže byť duplikované
- ☐ to niečo môže byť zakázané

Aké sú slabé miesta autentifikačnej techniky založenej na „niečom, čo máte“?

- ☐ to niečo môže byť zabudnuté
- ☐ to niečo môže byť stratené
- ☐ to niečo môže byť duplikované

☐ to niečo môže byť zakázané

Aká je postupnosť kľúčov používaných v asymetrickom šifrovaní?

◯ súkromný kľúč odosielateľa a verejný kľúč príjemcu

◯ súkromný kľúč odosielateľa a verejný kľúč odosielateľa

◯ súkromný kľúč príjemcu a verejný kľúč príjemcu

◯ verejný kľúč odosielateľa a súkromný kľúč príjemcu

Aká je správna postupnosť krokov v procese digitálneho podpisovania?

◯ hašovanie, podpísanie a poslanie

◯ podpísanie, hašovanie a poslanie

◯ šifrovanie, hašovanie a poslanie

◯ hašovanie, kódovanie a poslanie

Aké sú príklady autentifikácie pomocou hesla?

☐ jednorazové heslá

☐ opätovne použiteľné heslá

☐ štruktúrované heslá

☐ osobné údaje

Aké sú komponenty PKI (infraštruktúry verejného kľúča)?

◯ CA, MA, LA, digitálny podpis

◯ CA, RA, PA, digitálny podpis

◯ CA, RA, PKC, digitálny certifikát

◯ CA, RA, PKC, digitálny podpis

Čo patrí medzi neelektronické útoky na heslá?

- ☐ sledovanie potenciálnej obete
- ☐ sociálne inžinierstvo
- ☐ slovníkový útok
- ☐ útok hrubou silou

Čo je hlavnou úlohou certifikačnej autority (CA)?

- ◯ vydávanie certifikátov
- ◯ vydávanie digitálnych podpisov
- ◯ kontrola digitálnych podpisov
- ◯ overovanie identity jednotlivcov

Čo patrí medzi elektronické útoky na heslá?

- ☐ phishing
- ☐ sociálne inžinierstvo
- ☐ slovníkový útok
- ☐ útok hrubou silou

Ktoré z nasledujúcich nástrojov sú nástroje na prelomenie hesiel?

- ☐ John the cracker
- ☐ John the Ripper
- ☐ Hydra
- ☐ Hybrid

Ako sa implementuje PKI?

- ◯ ako stromová štruktúra
- ◯ ako klient/server systém
- ◯ hardvérovo
- ◯ sekvenčne

Ako možno použiť digitálne certifikáty na autentifikáciu?

- ◯ slúžia ako hlavný autentifikačný faktor
- ◯ slúžia na symetrické šifrovanie obsahu autentifikácie
- ◯ nedajú sa použiť
- ◯ na podpisovanie dokumentov

Čo by heslá nemali obsahovať?

- ☐ odlišné typy znakov
- ☐ slová spojené s vašou osobou
- ☐ dátumy narodenia
- ☐ špeciálne znaky

Aké funkcie zvyčajne obsahuje správca hesiel?

- ☐ automatické dopĺňanie
- ☐ generovanie hesiel
- ☐ hodnotenie kvality hesiel
- ☐ odmietanie hesiel

Aké sú nevýhody 2FA?

- ☐ nepohodlie
- ☐ vyššia bezpečnosť

- ☐ obavy o súkromie
- ☐ silnejšia autentifikácia

Aké sú hlavné ciele digitálnych podpisov?

- ☐ poskytnutie autentifikácie
- ☐ poskytnutie integrity
- ☐ poskytnutie dôveryhodnosti
- ☐ poskytnutie autorizácie

Aké kľúče sa používajú pri asymetrickom šifrovaní?

- ☐ verejný kľúč
- ☐ tajný kľúč
- ☐ prihlasovací kľúč
- ☐ súkromný kľúč

Aké stavebné bloky sú zahrnuté v procese digitálneho podpisovania?

- ☐ hašovacie funkcie
- ☐ symetrické šifrovacie algoritmy
- ☐ algoritmy na výmenu kľúčov
- ☐ asymetrické šifrovacie algoritmy

Aká je správna postupnosť krokov v procese overovania digitálneho podpisu?

- ☐ získať haš z podpisu, získať haš z údajov, porovnať ich navzájom
- ☐ získať haš z údajov, získať haš z podpisu, porovnať ich navzájom
- ☐ porovnanie hašov, následne získanie hašu z údajov a získanie hašu z podpisu
- ☐ porovnanie hašov, následne získanie hašu z podpisu a potom získanie hašu z údajov

Ktoré komponenty patria medzi komponenty PKI (infraštruktúry verejného kľúča)?

- ☐ certifikačná autorita (CA)
- ☐ prevádzková autorita (PA)
- ☐ digitálny podpis
- ☐ digitálny certifikát

Aké sú typické súčasti digitálnych certifikátov?

- ☐ doba platnosti
- ☐ vydavateľ
- ☐ veľkosť
- ☐ digitálny podpis

Aké sú hlavné časti reťazca dôvery v PKI?

- ☐ koreňový certifikát
- ☐ sprostredkovací certifikát
- ☐ digitálny podpis
- ☐ administratívny certifikát