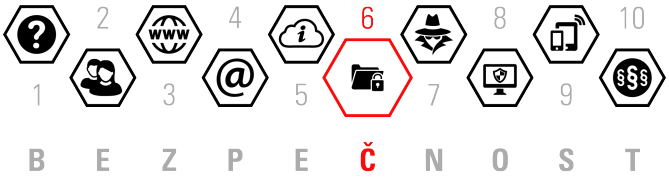
Školení IT bezpečnosti uživatelů sítě ZČU



Šifrování a elektronický podpis

Materiály vznikly v rámci projektu Fondu rozvoje CESNET na Západočeské univerzitě v Plzni. Školení má celkem 10 kapitol a veškeré texty, prezentace a další podrobnosti naleznete na stránce https://bezpecnost.zcu.cz.

CENTRUM INFORMATIZACE A VÝPOČETNÍ TECHNIKY ZÁPADOČESKÉ UNIVERZITY V PLZNI

cesnet fondrozvoje

Bezpečnostní desatero

1 Když nevíš, zeptáš se.

V případě podezření na kybernetický útok, když obdržím pochybný e-mail nebo se počítač chová divně, kontaktuji uživatelskou podporu a domluvím se na dalším postupu. Řídím se pokyny odborníků.

2 Budeš se autentizovat a autorizovat.

Počítač mě sám nepozná, proto mu musím svou identitu prokázat například znalostí hesla k uživatelskému účtu (autentizace). V aplikacích, programech a informačních systémech často nemám oprávnění ke všem činnostem. Proto po autentizaci následuje autorizace, která stanoví, co smím a co ne.

3 Dáš si pozor, kam heslo zadáváš.

Přihlašovací údaje vyplňuji pouze do webové stránky, která je šifrovaná, tedy její adresa začíná https:// nebo je na jejím začátku ikona zámku. Je důležité, aby adresa stránky byla uvedena přesně; i podvodné stránky mohou používat šifrování.

4 K příchozí poště budeš zdravě podezíravý(á).

Elektronická pošta je často zneužívána k rozesílání spamů, hoaxů, phishingových nebo hromadných zpráv. Dávám si pozor na podezřelé e-maily, zvláště na ty, které obsahují přílohu nebo odkazy na stránky. Příloha může obsahovat škodlivý kód a odkazovaná stránka může být podvodná.

5 Nebudeš věřit všemu, co se na Internetu píše.

Na Internetu může zveřejňovat informace každý, i autor neznalý nebo záměrně manipulující. Proto si věrohodnost získávaných informací vždy ověřuji. V pracovním prostředí musím zacházet s informacemi uváženě; ne všechny údaje jsou určeny všem.

6 Důvěrné informace budeš šifrovat.

Šifrování dat zajišťuje, že si informaci nemůže přečíst každý, kdo ji získá, ale jen ten, kdo zná navíc dešifrovací klíč. Elektronický podpis potvrzuje, že podepsaná osoba je autorem nebo že s obsahem souhlasí. Zároveň potvrzuje, že obsah elektronicky podepsaného dokumentu se po podepsání už nezměnil.

7 Na Internetu nejsi anonymní.

Prohlížením stránek i používáním služeb na Internetu po sobě zanechávám množství stop. Další stopy vznikají dobrovolným zveřejňováním informací o sobě, zejména na sociálních sítích. Všechny tyto činnosti moji anonymitu snižují a je dobrým zvykem chovat se tak, jako by mě mohl kdokoli identifikovat.

8 Budeš chránit své počítače a data zálohovat.

Nikdo nepovolaný by neměl používat cizí osobní věc, jakou je například počítač. Takové zařízení musím chránit zamykáním kanceláře a používáním zámku obrazovky. Dbám na aktuálnost jeho programového vybavení, případně svěřím správu zařízení odborníkům. Důležitá data pravidelně zálohuji.

9 Mobilní zařízení jsou také počítače.

Mobilní zařízení, dnes nejčastěji chytrý mobilní telefon, je malý počítač a chovám se k němu a datům v něm stejně jako v případě počítače. Navíc si musím uvědomovat rizika, která přináší možnost zařízení přenášet nebo ho mít stále u sebe.

10 Budeš dodržovat pravidla a ctít právo.

Na Internetu platí stejná legislativa jako v reálném světě, ale je rozšířená o některé další specifické právní normy. Mimo tuto státem vyžadovanou legislativu dodržuji také interní pravidla organizací nebo pravidla používání konkrétních služeb.

KAPITOLA 6

Šifrování a elektronický podpis

6.1 Úvod

Některé informace, které jsou uložené v počítačových systémech nebo jsou jimi posílány po síti, jsou citlivé a nikdo nepovolaný by neměl mít možnost si je přečíst a narušit tak základní prvek bezpečnosti – důvěrnost dat. Největší nebezpečí hrozí během přenosu počítačovou sítí nebo při krádeži zařízení obsahujícího data. Ke znečitelnění informací jsou proto používány různé způsoby šifrování. Dále by se v mnoha případech hodilo mít jistotu, kdo vlastně daná data vytvořil a odeslal. Analogicky k běžnému podpisu papírových dokumentů tak ve světě počítačů vznikl elektronický podpis.

6.2 Šifrování

Už od nepaměti existovala zejména v obchodních a vojenských kruzích potřeba zajistit, aby si důležitou zprávu mohl *přečíst pouze zamýšlený adresát a nikdo jiný*. Způsoby, jak takového znečitelnění pro nepovolané osoby dosáhnout, se vyvíjely od poměrně primitivních záměn písmen za jiné znaky až po dnešní poměrně sofistikované šifrovací algoritmy.

Příklad historické šifry

Caesarova šifra – římský císař používal pro znečitelnění komunikace se svými vojevůdci jednoduchý postup, kdy každé písmeno v abecedě nahradil písmenem o tři místa dále (např. $A \rightarrow D, B \rightarrow E, \ldots X \rightarrow A$).

Vlastní šifrování je přeměna srozumitelného textu (dat obecně) na nesrozumitelný určitým postupem, algoritmem. Opačný postup se nazývá dešifrování. V obou případech je postup (de)šifrování ovlivněn tajným parametrem, který se nazývá (de)šifrovací klíč. Pouze ten, kdo zná dešifrovací klíč, se může dostat k původní zprávě.

Šifra musí být odolná vůči pokusům o dešifrování bez znalosti klíče (prolomení). Kyberzločinci používají výkonné počítače a metody, ale pokud je šifra kvalitní, pak její prolomení trvá tak dlouho, že se nevyplatí to zkoušet.

Pokud je pro zašifrování i dešifrování zprávy použit stejný klíč, mluvíme o *symetrickém šifrování*. Tento typ šifrovacích funkcí je poměrně rychlý a pro běžné šifrovací funkce (např. AES) má většina současných počítačů vyhrazený speciální hardware, aby bylo možné rychle (de)šifrovat velké množství dat. Typicky jsou takto zašifrována datová úložiště (pevné disky, přenosná USB zařízení apod.), kdy příslušný klíč zná pouze majitel zařízení a v případě krádeže si útočník uložené informace přečíst nemůže. Pokud bychom zašifrovaná data chtěli někomu poslat, museli bychom si s druhou stranou klíč předem sdělit. Nevýhodou je, že každá komunikující dvojice musí mít

dohodnutý svůj klíč, takže třeba už pro 100 navzájem komunikujících lidí by bylo potřeba 4950 klíčů (výpočet viz níže), což není moc praktické.

Výpočet počtu párů šifrovacích klíčů

$nx\frac{(n-1)}{2}$, kde $n = 100$

$100x\frac{(100-1)}{2} = \frac{9900}{2} = 4950$

Odborníci na šifrování (kryptologové) naštěstí objevili i takzvané *asymetrické šifrování*, kdy algoritmus využívá speciálním postupem vytvořenou dvojici klíčů. S pomocí komplikovaného matematického aparátu je zajištěno, že data zašifrovaná jedním ze zmíněných klíčů lze dešifrovat pouze klíčem druhým. A také opačně. Každý, kdo chce komunikovat, si tedy vytvoří dvojici klíčů, jeden bude znát pouze on sám (proto se nazývá soukromý nebo privátní) a druhý poskytne ostatním (proto se nazývá veřejný). Komunikace mezi 100 lidmi tedy vyžaduje už jen 100 dvojic klíčů.

Ověření vlastníka klíče

Chceme-li někomu poslat šifrovanou zprávu, musíme ji zašifrovat jeho veřejným klíčem (dešifrovat ji totiž může jen *vlastník příslušného privátního klíče*). Bylo by ale nesprávné použít špatný veřejný klíč, takže by si zprávu náš zamýšlený komunikační partner přečíst nemohl, ale naopak by si ji mohl přečíst úplně někdo jiný. V případě šifrovaného e-mailu je obvyklým komunikačním partnerem živá osoba, ale můžeme komunikovat i s počítači, například s webovými stránkami.

Proto je třeba si být jistý, kdo k danému veřejnému klíči vlastní odpovídající privátní klíč. Jednou z možností je osobní návštěva a následné ověření. Ale lidí i webových serverů je na takovéto řešení příliš mnoho, takže se používá pouze omezeně. Běžným způsobem je spolehnout se na někoho důvěryhodného, kdo toto ověření provede za nás – na tzv. CA, certifikační autoritu. Prakticky to funguje tak, že si buď osoba pro sebe, nebo provozovatel webu pro web vytvoří dvojici klíčů, následně pak svůj veřejný klíč a své identifikační údaje pošle certifikační autoritě, která si vše prověří a tato fakta zapíše do tzv. *certifikátu*. Každý, kdo dané certifikační autoritě důvěřuje, má na základě vydaného certifikátu jistotu, komu patří daný veřejný klíč.

Šifrovaná komunikace

V dnešní době už je šifrování komunikace považováno za běžný standard a provádí ho prakticky každý uživatel Internetu, aniž by o tom věděl (stačí navštívit zabezpečenou stránku, jejíž URL začíná **https://** (viz kapitola Bezpečné používání webu). Kromě webů se s ní běžně potkáte také u vzdáleného přístupu k počítači přes tzv. vzdálenou plochu (**RDP**) nebo pomocí vzdálené příkazové řádky (**SSH**). Šifrování je možné používat i v elektronické poště a odesílané zprávy zašifrovat tak, aby je mohl přečíst pouze adresát (resp. vlastník privátního klíče k veřejnému, kterým šifrujeme).

Vlastní proces šifrování provádějí námi používané aplikace – webové prohlížeče, terminálové nebo e-mailoví klienti apod. Stejně tak jsou schopny uchovávat náš privátní klíč a související certifikát a současně ověřit platnost certifikátu druhé strany. Uživatel je o šifrování buď pouze informován (například prohlížeč zámečkem ukazuje, že šifruje), nebo aktivně sám rozhoduje, zda odesílanou zprávu chce zašifrovat (například v e-mailovém klientovi).

Kdy je vhodné šifrovat komunikaci?

Paranoici by řekli, že vždy. Realisté zastávají názor, že šifrování je nezbytné v případech, kdy je informace určena pouze jednomu příjemci nebo omezené skupině a ostatní se ji nemají dozvědět.

Šifrovaná datová úložiště

Šifrování je často aplikováno také na data, která se nikam neposílají a jen jsou uložena v počítači, externím disku apod. Cílem je zajistit důvěrnost uložených dat i v případech, že vypnuté zařízení nebo externí disk někdo získá do své moci – zašifrovaná data si totiž dotyčný nepřečte.

Naše uložená data se vyplatí tedy šifrovat všude tam, kde hrozí nebezpečí krádeže hardware, na kterém se data nacházejí – notebooky brané na služební cesty, USB flash disky nošené v kapsách apod. Současné nástroje pro šifrovaní umožňují také šifrovat pouze část zařízení, takže lze rozdělit data na důležitá šifrovaná (interní dokumenty, plány, licenční klíče apod.) a na nešifrovaná, ostatní data (stažené hudební klipy, e-knihy apod.)

6.3 Elektronický podpis

U všech dokumentů je poměrně často vhodné mít jistotu, kdo je vytvořil. Na papírové dokumenty můžeme dát své razítko, pečeť nebo podpis, čímž dáváme najevo, že jsme dokument vytvořili nebo alespoň jeho obsah potvrzujeme (když nám jej například připravila sekretářka).

U všech elektronických dat (například zpráv elektronické pošty), můžeme naštěstí využít výše popsaný aparát používaný při šifrování. Využijeme ale opačné vlastnosti, tj. že data zašifrovaná naším privátním klíčem lze dešifrovat pouze naším veřejným klíčem. Z podepisovaných dat spočítáme jejich otisk (hash) a ten zašifrujeme naším privátním klíčem (který máme pouze my). Máme tedy originální dokument a jeho zašifrovaný otisk, přidáme ještě certifikát obsahující náš veřejný klíč a tento balíček můžeme odeslat adresátovi.

Adresát (respektive jeho aplikace) si pak z certifikátu ověří, komu patří veřejný klíč. Tento klíč použije k dešifrování otisku a výsledek porovná s vypočítaným otiskem zaslaného dokumentu. Pokud jsou otisky shodné, je jasné, že dokument elektronicky podepsala osoba, která je v certifikátu zapsaná jako majitel veřejného klíče. Současně je také zřejmé, že dokument nebyl cestou změněn (jinak by otisky nebyly shodné).

Co to je hash/otisk

Hash, neboli otisk, je hashovací funkcí získaný jedinečný shluk čísel a písmen, které odpovídají původnímu dokumentu. Pokud se původní dokument i drobně změní, otisk se změní zásadně. Hashovací funkce je jednosměrná funkce, čili z otisku nelze zpět obnovit původní dokument.

Co to je certifikát?

Certifikát je vlastně také elektronický dokument a je elektronicky podepsán certifikační autoritou. A aby bylo možné ověřit platnost podpisu, musíme mít další certifikát, který ověřuje, že daný klíč patří uvedené certifikační autoritě. Ten je opět elektronicky podepsán… a aby nedocházelo k nekonečnému řetězení, mají aplikace v sobě zapsány tzv. kořenové certifikáty důvěryhodných certifikačních autorit a umí ověřit platnost jimi podepsaných certifikátů.

6.4 Shrnutí

V dnešním Internetu nelze spoléhat na to, že data posílaná po síti si nikdo nepřečte nebo je nebude chtít změnit. Proto je důležité přenášená data šifrovat – tak je zajištěno, že se k nim nedostane nikdo nepovolaný. Pro snazší distribuci šifrovacích a dešifrovacích klíčů je používáno asymetrické šifrování a pro ověření vlastnictví privátních klíčů existují certifikační autority, které vlastnictví potvrzují vydáváním certifikátů. Ve výsledku je díky současným aplikacím snadné poslat konkrétnímu člověku zprávu nebo komunikovat s konkrétní webovou stránkou šifrovaně a také dešifrovat nám zaslanou zprávu nebo dešifrovat obdržená data z webové stránky. Šifrování by mělo být používáno všude tam, kde jsou zasílaná data určená pouze omezené skupině adresátů.

Pomocí šifrování lze chránit před neoprávněným čtením také uložená data, což se hodí zejména v případech, kdy hrozí krádež daného zařízení a nechceme zloději umožnit číst naše důvěrná data. V tomto scénáři se používá symetrické šifrování, protože šifrovací i dešifrovací klíč je stejný

a zná jej pouze majitel zařízení. Data uložená v pracovních noteboocích nebo nahraná na přenosná média (USB flash disky, externí disky apod.) by měla být šifrována. Dalším problémem Internetu je jistota autorství zaslaných zpráv, protože kyberpodvodníci se rádi vydávají za někoho jiného (například v elektronické poště). Pro ověření autorství existuje elektronický podpis, který je založen na stejném základu jako šifrování. Příslušné aplikace (typicky klienti elektronické pošty) umožňují odchozí zprávy podepisovat a ověřovat přítomnost i platnost elektronického podpisu u zpráv příchozích.

Šifrování i elektronický podpis by měly být samozřejmostí pro každého uživatele Internetu, který pracuje s daty, u nichž je třeba zajistit důvěrnost.