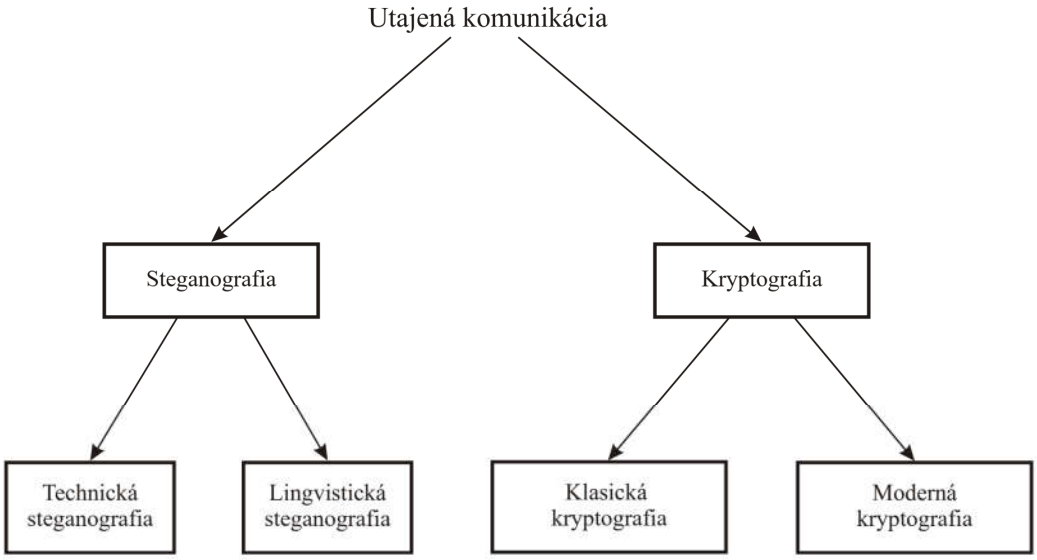
Počítačová bezpečnosť, úvod do problematiky, základné pojmy, princípy a súvislosti

Podklady k prednáškam a cvičeniam:
TUKE MOODLE (https://moodle.tuke.sk/moodle/) – prihlasovací kľúč **KEMTBPS**

Plán prednášok a doporučená literatúra:
https://data.kemt.fei.tuke.sk/Bezpecnost_v_pocitacovych_systemoch/_materialy/bps.pdf

Web stránka predmetu (len základné informácie a zaujímavé linky):
https://data.kemt.fei.tuke.sk/Bezpecnost_v_pocitacovych_systemoch/_web/

Primárny zdroj informácii k dnešnej prednáške:
[1] prof. Ing. Dušan Levický, CSc.
APLIKOVANÁ KRYPTOGRAFIA
od utajenia správ ku kybernetickej bezpečnosti
Elfa, Košice, 2018 (str.1-30)



Obr. 1.1 Metódy utajenej komunikácie

Kryptografia (Cryptography) nemá cieľ utajiť existenciu tajnej správy, resp. utajiť komunikáciu, jej cieľom je utajiť obsah správy metódami šifrovania

Šifrovanie (Enciphering, Encryption) je proces úpravy správy pred jej odoslaním s cieľom utajiť jej obsah. Zo zašifrovanej správy aj po jej zachytení nepovolanou osobou by sa nemal získať obsah vyslanej, resp. nezašifrovanej správy.

Konkrétny postup šifrovania sa označuje ako **šifrovací algoritmus**, resp. **šifra** (cipher).

Základnou teóriou kryptografie, ktorú sformuloval Auguste Kerckhoffs je, že bezpečnosť šifrovania nemožno založiť na utajení šifrovacieho algoritmu, ale výlučne na utajení kľúča. Takýto kľúč sa preto označuje ako tajný kľúč (secret key).

Poznámky:
Originál článku Augusta Kerckhoffa – pozri: https://www.petitcolas.net/kerckhoffs/index.html
Detailný životopis Augusta Kerckhoffa – pozri: https://eprint.iacr.org/2020/556.pdf

Klasická kryptografia (za koniec éry klasickej kryptografie sa považuje rok 1945) využívala klasické šifry a postupy, ktoré zahŕňajú:
• substitúciu
• transpozíciu.

Substitúcia nahrádza každý symbol nezašifrovanej správy iným symbolom, ktorý zostáva na rovnakom mieste ako pôvodný symbol. Výber symbolov pre substitúciu určuje kľúč.

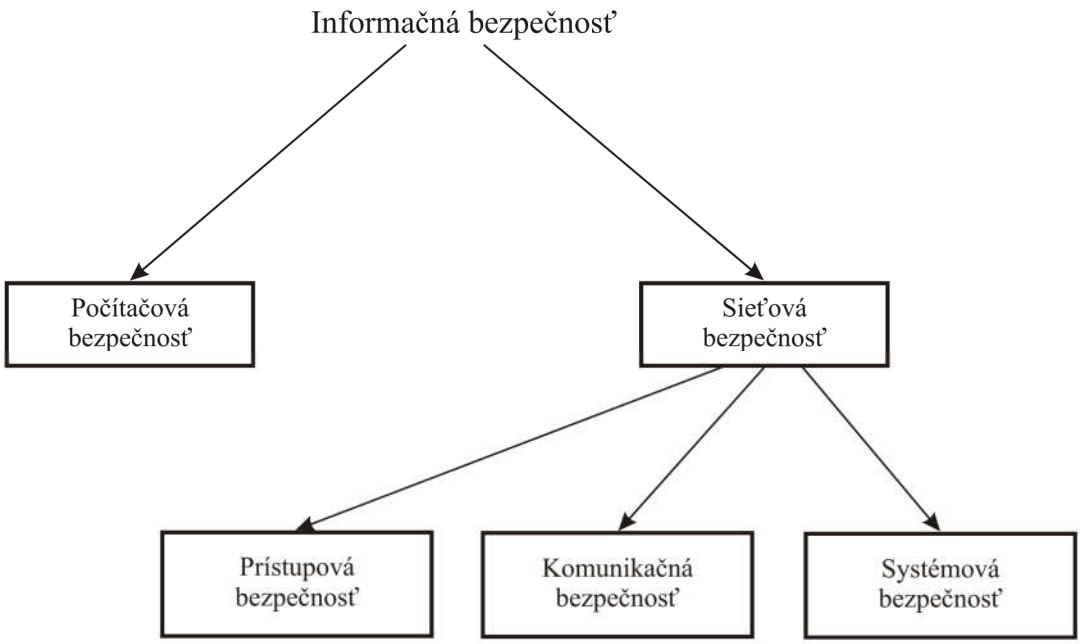
Transpozícia je preusporiadanie symbolov v nezašifrovanej správe, zvoleným spôsobom (napr. permutáciou), čím vzniká zašifrovaná správa.

Moderná kryptografia je spojená s rozvojom elektronickej formy komunikácie, kde zachytenie prenášanej správy je jednoducho technicky realizovateľné. Elektronická forma komunikácie prešla postupne od drôtovej komunikácie k bezdrôtovej, čo umožnilo prenosový kanál ľahko monitorovať a zachytiť vysielanú správu.

Modernú kryptografiu stimulovali najmä tieto skutočnosti:
• rozvoj teórie informácie a systematickej teórie komunikácie
• rozvoj výpočtovej techniky, ktorá prešla viacerým generáciami svojho vývoja
• vznik moderných komunikačných sietí s využitím počítačov.

Z hľadiska realizácie šifrovania a použitých kľúčov možno moderný kryptografiu rozdeliť na:
• kryptografiu **s tajným kľúčom** (secret key cryptography)
• kryptografiu s **verejným kľúčom** (public key cryptography).

Informačná bezpečnosť



Obr. 1.2 Komponenty informačnej bezpečnosti

Počítačová bezpečnosť rieši najmä otázky bezpečnej prevádzky a ochrany dát spracovávaných počítačmi, čo zahŕňa **dôvernosť** dát, **autentizáciu** a **autorizáciu** dát a **integritu** dát

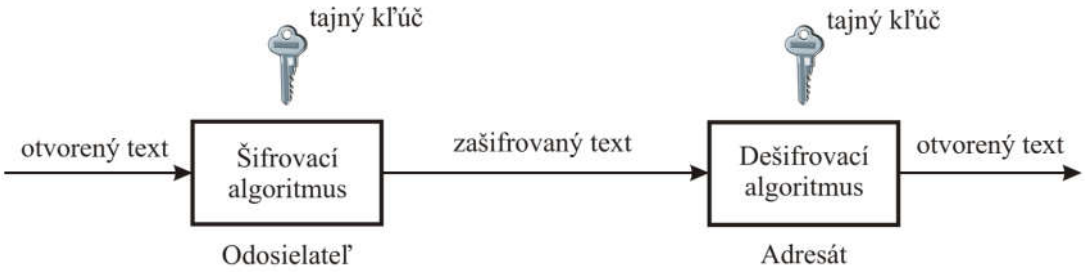
Komunikácia prostredníctvom moderných telekomunikačných sietí a pripojenie počítačov ako terminálov do týchto sietí podnietila riešenie bezpečnosti pripojených počítačov, ktorá sa označuje ako **sieťová bezpečnosť.**

Prístupová bezpečnosť rieši najmä otázky autentizácie používateľov a riadenie prístupu používateľov k systémovým prostriedkom a službám počítačovej, resp. telekomunikačnej siete.

Komunikačná bezpečnosť rieši najmä ochranu a bezpečnosť prenášaných dát na úrovni komunikačných protokolov.

Systémová bezpečnosť zahŕňa riešenie problémov, ktoré súvisia najmä s bezpečným oddelením komunikačných sietí s rôznym stupňom bezpečnosti, s bezpečnosťou interného prostredia (bezpečnosť operačného systému, bezpečnosť aplikácií) a s ochranou pred útokmi zlomyseľným softvérom (vírusy, červy).

Klasické kryptografické systémy



Obr. 2.1 Model konvenčného šifrovania

Otvorený text je správa, resp. dáta, ktoré predstavujú vstup kryptografického systému, resp. sú to vstupné dáta pre šifrovací algoritmus.

Šifrovací algoritmus je algoritmus, ktorý realizuje šifrovanie, t. j. transformáciu otvoreného textu na zašifrovaný text s využitím kryptografických techník, napr. substitúcie a permutácie.

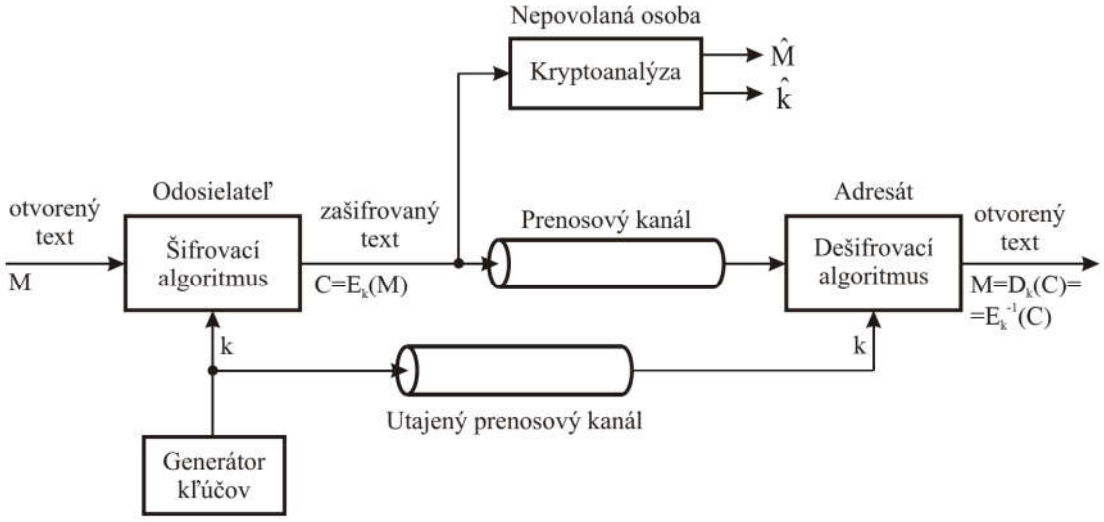
Tajný kľúč je tiež vstupom kryptografického systému a nezávisí od otvoreného textu. Tajný kľúč určuje konkrétny tvar transformácie otvoreného textu na zašifrovaný text.

Zašifrovaný text predstavuje výstup šifrovacieho algoritmu. Je jednoznačne určený otvoreným textom a tajným kľúčom. Pre daný otvorený text dva rôzne tajné kľúče produkujú dva rôzne zašifrované texty.

Dešifrovací algoritmus realizuje proces získania otvoreného textu z prijatého zašifrovaného textu s využitím rovnakého tajného kľúča, ktorý bol použitý pri šifrovaní.

Požiadavky na bezpečné symetrické šifrovanie možno formulovať takto:
• šifrovací algoritmus by mal byť taký, že znalosť tohto algoritmu a prístup k jednému alebo viacerým zašifrovaným textom by nemal umožniť dešifrovanie, t. j. získanie otvoreného textu, alebo získanie kľúča. Požiadavku možno sprísniť tak, že prístup k viacerým otvoreným textom a im zodpovedajúcim zašifrovaným textom by nemal umožniť dešifrovanie, resp. zistenie kľúča.

• odosielateľ aj adresát musia dostať bezpečným spôsobom rovnaký tajný kľúč a musia ho udržať v tajnosti. Ak nepovolaná osoba získa tajný kľúč a pozná šifrovací algoritmus, korešpondencia medzi odosielateľom a adresátom je čitateľná. Táto situácia sa označuje ako prelomenie kryptografického systému, resp. šifry (cipher breaking, cipher cracking).



Obr. 2.2 Model konvenčného kryptografického systému

Klasifikácia kryptografických systémov a šifier

1) Podľa **typu operácií** v kryptografickej transformácii:

Substitúcia nahrádza každý prvok otvoreného textu (bit, písmeno, skupinu bitov a písmen) iným prvkom otvoreného textu a tieto nové prvky ostávajú na mieste pôvodných prvkov. Adresát musí na získanie otvoreného textu použiť inverznú substitúciu.

Transpozícia je preusporiadanie prvkov otvoreného textu podľa určitého pravidla, napr. permutáciou. Adresát musí na získanie otvoreného textu použiť inverznú transpozíciu. V zjednodušenej podobe možno hovoriť o **substitučných** a **transpozičných šifrách**. Základnou požiadavkou na operácie pri šifrovaní je, aby sa pri ich aplikácii nestratila žiadna informácia, t. j. **musia byť invertibilné**.

2) Podľa **počtu a typov kľúčov** možno kryptografické systémy rozdeliť na:

Kryptografické systémy s tajným kľúčom používajú rovnaký kľúč na šifrovanie aj dešifrovanie a označujú sa tiež ako symetrické, resp. konvenčné kryptografické systémy. Bezpečnosť týchto systémov spočíva v utajení kľúča, ktorý si musia odosielateľ aj adresát vymeniť pred samotnou komunikáciou, čo predstavuje určitú nevýhodu z hľadiska pohotovosti komunikácie.

Kryptografické systémy s verejným kľúčom používajú iný kľúč na šifrovanie a iný kľúč na dešifrovanie , teda platí

$$C = E_{k_1}\left(M\right) \tag{2.3}$$

$$M = D_{k_2}\left(C\right) = D_{k_2}\left(E_{k_1}\left(M\right)\right) \tag{2.4}$$

Šifrovací kľúč k_1 je tzv. **verejný kľúč**, dešifrovací kľúč k_2 je **súkromný kľúč** a je známy len adresátovi.

Kryptografické systémy **s verejným kľúčom** sa tiež označujú ako **nesymetrické kryptografické systémy** a ich bezpečnosť je založená na **matematickej zložitosti** určenia súkromného kľúča zo známeho verejného kľúča.

3) Podľa **spôsobu spracovania** otvoreného textu šifrovacie algoritmy môžu využívať dva základné
režimy a to:

Blokový režim je základom **blokových šifier** (block ciphers), ktoré spracovávajú otvorený text po skupinách prvkov. Výstupom je blok zašifrovaného textu, ktorý má obvykle rovnakú veľkosť ako blok otvoreného textu.

Prúdový režim je základom **prúdových šifier** (stream ciphers), ktoré spracovávajú otvorený text priebežne po jednotlivých prvkoch. Každému prvku otvoreného textu teda zodpovedá jeden prvok zašifrovaného textu.

Kryptoanalýza

Snaha o získanie otvoreného textu, resp. kľúča sa tiež označuje ako **lúštenie** (attack). Získanie kľúča iným spôsobom ako kryptoanalýzou sa nazýva **kompromitácia kľúča**.

Lúštenie v konvenčných kryptografických systémoch možno principiálne realizovať dvoma spôsobmi:
• kryptoanalýzou
• metódou totálnych skúšok (brute force attack).

Tab. 2.1 Klasifikácia spôsobov lúštenia v kryptoanalýze

Spôsob lúštenia (Attack)	**Informácie dostupné pre kryptoanalýzu**
Lúštenie so znalosťou zašifrovaného textu (Ciphertext-only attack)	• Šifrovací algoritmus • Zašifrovaný text
Lúštenie so znalosťou otvoreného textu (Know-plaintext attack)	• Šifrovací algoritmus • Zašifrovaný text • Jeden, resp. viacej párov otvoreného a zašifrovaného textu generovaných neznámym kľúčom
Lúštenie so znalosťou vybraných otvorených textov (Chosen-plaintext attack)	• Šifrovací algoritmus • Zašifrovaný text • Otvorený text vybraný kryptoanalytikom a zodpovedajúci zašifrovaný text generovaný neznámym kľúčom
Lúštenie so znalosťou vybraných zašifrovaných textov (Chosen-ciphertext attack)	• Šifrovací algoritmus • Zašifrovaný text • Zašifrovaný text s určitým významom vybraný kryptoanalytikom a zodpovedajúci dešifrovaný otvorený text
Lúštenie so znalosťou vybraných textov (Chosen text attack)	• Šifrovací algoritmus • Zašifrovaný test • Otvorený text vybraný kryptoanalytikom a zodpovedajúci zašifrovaný text generovaný neznámym kľúčom • Zašifrovaný text s určitým významom vybraný kryptoanalytikom a zodpovedajúci dešifrovaný otvorený text

Metóda totálnych skúšok (brute-force attack) sa zakladá na systematickom overovaní všetkých možných kľúčov na dešifrovanie zašifrovaného textu, až sa získa zrozumiteľná podoba otvoreného textu. Aby bolo lúštenie úspešné je potrebné v priemere vyskúšať polovicu z celkového počtu možných kľúčov.

Tab. 2.2 Priemerná doba trvania totálnej skúšky pri rôznych dĺžkach kľúčov a rôznej rýchlosti dešifrovania

Dĺžka kľúča [bit]	Celkový počet kľúčov	Doba trvania totálnej skúšky pri 1 dešifrovaní/μs	Doba trvania totálnej skúšky pri 10^6 dešifrovaní/μs
32	$2^{32}=4.3\times10^{9}$	2^{31}μs=35.8 minút	2.15 milisekúnd
56	$2^{56}=7.2\times10^{16}$	2^{55}μs=1142 rokov	10.01 hodín
128	$2^{128}=3.4\times10^{38}$	2^{127}μs=5.4×10^{24} rokov	5.4×10^{18} rokov
168	$2^{168}=3.7\times10^{50}$	2^{167}μs=5.9×10^{36} rokov	5.9×10^{30} rokov

Poznámka: vek vesmíru sa odhaduje (https://sk.wikipedia.org/wiki/Vek_vesm%C3%ADru) len na cca **4.5*10^17 sekúnd**… „☺

Bezpečnosť kryptografických algoritmov

Bezpečnosť kryptografických algoritmov je schopnosť odolať ich rozlúšteniu (prelomeniu). Z pohľadu stupňa bezpečnosti možno rozdeliť kryptografické algoritmy na:

• absolútne bezpečné (unconditionally secure)
• výpočtovo bezpečné (computationaly secure).

Absolútne bezpečný kryptografický algoritmus sa vyznačuje tým, že kryptoanalytik nebude schopný získať otvorený text ani vtedy, keď má k dispozícii neobmedzené množstvo zašifrovaného textu a neobmedzenú výpočtovú kapacitu. Toto hľadisko splňuje iba algoritmus s **jednorazovým kľúčom (one–time pad)**.

V praxi sa bezpečnosť kryptografických algoritmov preto obvykle posudzuje podľa toho, koľko úsilia je potrebné vynaložiť na jeho prelomenie. Z praktického hľadiska by mal kryptografický algoritmus splniť jednu, resp. obe nasledujúce podmienky:

• **náklady** potrebné na prelomenie šifrovacieho algoritmu sú vyššie než hodnota zašifrovaných dát
• **doba** potrebná na prelomenie algoritmu je väčšia než doba, počas ktorej sa musia zašifrované dáta utajovať.

Uvedené aspekty zohľadňujú tzv. **praktickú bezpečnosť** kryptografických algoritmov, ktoré možno charakterizovať ako výpočtovo bezpečné.

Výpočtovo bezpečný kryptografický algoritmus sa považuje za silný, ak nemôže byť prelomený použitím súčasných, resp. v blízkej budúcnosti dostupných prostriedkov na lúštenie.

Substitučná šifra nahradzuje každý znak otvoreného textu iným znakom zašifrovaného textu. Na získanie otvoreného textu musí adresát použiť inverznú substitúciu.

V klasickej kryptografii sú známe štyri typy substitučných šifier. Sú to:
• monoalfabetické šifry
• homofónne šifry
• polygramové šifry
• polyalfabetické šifry.

Ako príklad uvedieme len monoalfabetické šifry, podrobnejšie informácie k ďalším typom sú v [1]. **Monoalfabetické šifry** (Monoalphabetic ciphers) realizujú jednoduchú substitúciu každého písmena otvoreného textu *p*, iným písmenom, ktoré je v abecede otvoreného textu A_{pt} posunuté o konštantný počet miest.

Ak uvažujeme, že abeceda otvoreného textu A_{pt} pozostáva z N znakov, potom pre monoalfabetickú šifru platí, že každý znak zašifrovaného textu C možno vyjadriť v tvare:

$$C = E(p) = (p + k) \bmod N \tag{2.5}$$

kde k je posun a operácia mod N je operácia modulo N. Dešifrovací algoritmus možno vyjadriť v tvare:

$$p = D(C) = (C - k) \bmod N \tag{2.6}$$

Cézarova šifra bola historicky prvou známou monoalfabetickou šifrou, pre ktorú je k=3.

Vernamova substitučná šifra(2) navrhnutá v r. 1917 používa kľúč s dĺžkou rovnajúcou sa dĺžke otvoreného textu. Kľúč je štatisticky nezávislý od otvoreného textu. Šifrovací systém na báze Vernamovej substitučnej šifry pracuje s binárnymi údajmi a šifrovanie možno vyjadriť v tvare

$$c_i = p_i \oplus k_i$$

kde c_i – i-tý binárny znak zašifrovaného textu

k_i – i-tý binárny znak kľúča

p_i – i-tý binárny znak otvoreného textu

$\oplus$ – operácia XOR (Exclusive OR)

Dešifrovanie možno zapísať v tvare

$$p_i = c_i \oplus k_i$$

Vernam navrhol generovať kľúče v slučke, teda s dlhou ale konečnou periódou, čo síce sťažuje kryptoanalýzu šifry, ale uvedenú šifru možno prelomiť.

Šifra s jednorazovým slovníkom, resp. kľúčom (One–time pad) bola navrhnutá Josephom Mauborgneom a je zdokonalením Vernamovej šifry. Používa náhodný kľúč s dĺžkou rovnajúcou sa dĺžke otvoreného textu bez opakovania. Jednorazový slovník predstavuje systém na zabezpečenie jednorazového použitia kľúča, ktorý sa po použití zničí. Rovnaký slovník s kľúčom má odosielateľ aj adresát. V pôvodnej forme sa jednalo o jednorazové diaľnopisné dierne pásky.

Uvedený systém generuje zašifrovaný text, ktorý neobsahuje žiadnu informáciu o otvorenom texte a teda je absolútne dokonalý, resp. nemožno ho pri splnení uvedených podmienok prelomiť.

Transpozičné šifry (transposition ciphers) sú založené na transpozícii písmen otvoreného textu, ktorej výsledkom je ich preusporiadanie. Cieľom transpozície je difúzia informačného obsahu správy po celej dĺžke zašifrovaného textu, čo sťažuje jeho kryptoanalýzu. Transpozícia sa snaží likvidovať systematické štruktúry otvoreného textu pretože mení usporiadanie jeho písmen.

Základná klasifikácia útokov
Informačná a sieťová bezpečnosť (http://techpedia.fel.cvut.cz/sk/home/blocks**) –** (https://techpedia.fel.cvut.cz/project/modules/improvet/download/C2SK/Informacna_a_sietova_bezpecnost.pdf)

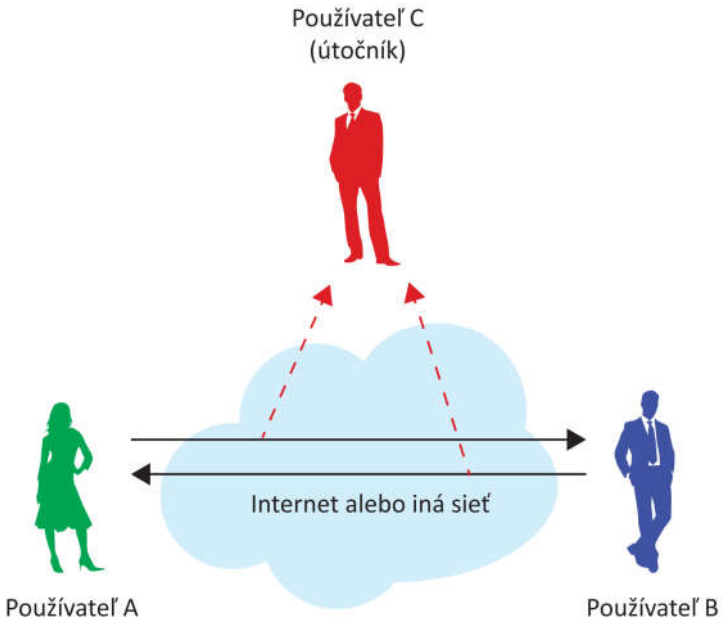
Bezpečnostné útoky môžu byť rozdelené do dvoch hlavných kategórií:
• pasívne útoky,
• aktívne útoky.

Pasívne útoky sa pokúšajú zistiť alebo využiť informáciu zo systému bez ovplyvňovania systémových prostriedkov. Pasívny útok je taký, pri ktorom útočník iba monitoruje komunikačný kanál. Pasívny útočník len ohrozuje dôvernosť dát. Povaha pasívnych útokov je založená na odpočúvaní alebo monitorovaní prenosu. Cieľom útočníka je získanie informácie, ktorá je prenášaná.

S obsahom správ a analýzou prevádzky súvisia dva typy pasívnych útokov:

• **Odpočúvanie.** Vo všeobecnosti väčšina sieťovej komunikácie prebieha v nezabezpečenom formáte (tzv. „otvorený text“), ktorý umožňuje útočníkovi, ktorý získal prístup k prostriedkom siete „načúvať“ alebo interpretovať (čítať) dáta vymieňané prostredníctvom siete. Schopnosť odpočúvajúceho monitorovať sieť je vo všeobecnosti najväčší bezpečnostný problém s ktorým je konfrontovaný administrátor v podniku. Bez využitia silných šifrovacích techník založených na kryptografii môžu byť dáta čítané inými osobami počas ich prenosu sieťou.

• **Analýza** prevádzky (traffic analysis)**.** Zodpovedá procesu odpočúvania a analýzy správ s cieľom odvodiť informáciu zo vzorov prenášaných dát. Môže byť realizovaná dokonca aj v prípade, že správy sú šifrované a nemôžu byť útočníkom dešifrované. Všeobecne platí, že čím väčší počet správ je možné sledovať alebo zachytiť a uložiť, tým viac informácií môže byť z prevádzky odvodených.



Model pasívneho útoku

Aktívne útoky sa pokúšajú modifikovať systémové prostriedky alebo ovplyvniť ich činnosť. Pri tomto type útoku sa útočník snaží vymazať, pridať, alebo nejakým iným spôsobom pozmeniť prenos informácie kanálom. Aktívny útočník ohrozuje integritu dát a autentizáciu ako aj dôvernosť.

Aktívne útoky zahŕňajú určitú formu modifikácie dátového toku alebo vytvorenie falošného toku a je ich možné rozdeliť do šiestich kategórií:

• **Predstieranie identity (masquerade).** Je to typ útoku, pri ktorom útočník predstiera, že je autorizovaným užívateľom systému s cieľom získať prístup do systému alebo získať väčšie privilégia než na ktoré má autorizáciu.

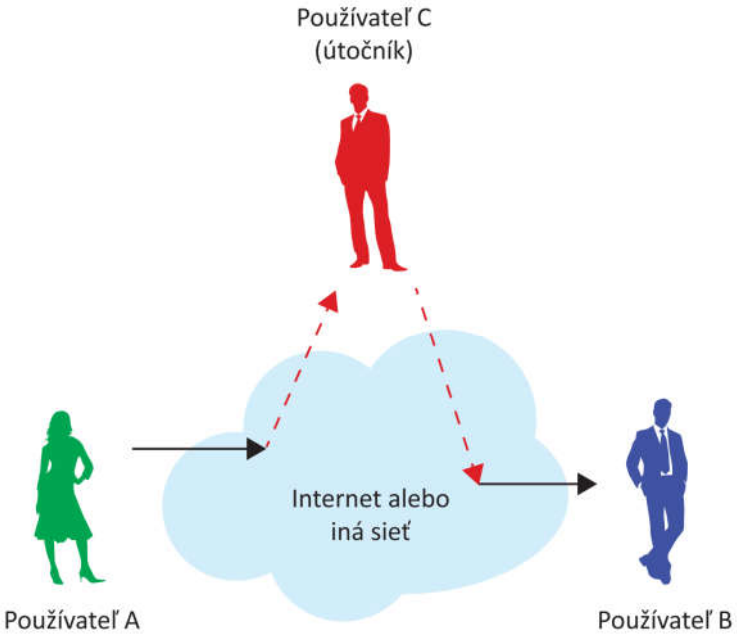
• **Opakovanie.** Pri tomto type útoku je platný dátový prenos úmyselne alebo podvodne opakovaný alebo oneskorený. Toto je dosiahnuté buď pôvodcom správy alebo útočníkom, ktorý zachytil dáta a opäť preposlal, eventuálne ako časť útoku s predstieraním identity.

• **Modifikácia správ**. Útočník odstráni správu zo sieťovej komunikácie, pozmení ju a opätovne vloží do komunikačného kanála.

• **Útok zo stredu** *(MitM - Man in the Middle attack*). Pri tomto type útokov narušiteľ preruší komunikáciu medzi dvomi stranami, zvyčajne koncovým užívateľom a web stránkou. Útočník môže využiť získanú informáciu na krádež identity alebo iný typ podvodu.

• **Odmietnutie služby** *(DoS- Denial of Service)* a *distribuované odmietnutie služby (DDoS - Distributed Denial of Service) útoky*. DoS útok je incident počas ktorého je používateľovi alebo organizácii odoprená služba alebo prostriedok, ktoré by za normálnych okolností boli k dispozícii. Pri distribuovanom odmietnutí služby útočí veľký počet kompromitovaných systémov (niekedy nazývaných botnet) na jeden cieľ.

• **Pokročilé trvalé ohrozenie** *(APT - Advanced Persistent Threat)*. Je sieťový útok počas ktorého neautorizovaná osoba získa prístup do siete a ostáva dlhodobo neodhalená. Zámerom APT útoku je tajne získať dáta a nie spôsobiť škodu sieti alebo organizácii. APT útoky sú smerované na organizácie v sektoroch kde sa pracuje s cennými informáciami ako sú národná obrana, priemysel a finančný sektor.



Aktívny útok s pozmenením správy

Základné stavebné bloky (kryptografické primitíva) moderných kryptografických systémov

- symetrické šifry (symmetric ciphers)
- nesymetrické šifry (asymmetric ciphers)
- hašovacie funkcie (hash functions)
- generátory náhodných čísel (random number generators)

Uvedené kryptografické stavebné bloky tvoria základ v súčasnosti využívaných kryptografických algoritmov a protokolov (digitálne podpisy, výmena kľúčov, autetizácia správ, ...) a preto budú v ďalších prednáškach a cvičeniach opísané základné princípy využívané na ich realizáciu.