

Bezpečnost počítačových sítí

sítí budeme rozumět soustavu několika výpočetních systémů, uživatelé přistupují k sítí prostřednictvím některého z těchto systémů

v této přednášce se budeme zabývat pouze bezpečnostní politikou, ne její implementací

zdroje bezpečnostních obtíží:

- Sdílení - potenciální přístup má velmi velké množství lidí, různé stroje mohou být řízeny různými ne nutně bezpečnými systémy
- Složitost - v síti se vyskytují nejrozličnější operační systémy komunikující spolu via spojovací mechanismus, který by měl zajišťovat ochranu, tento mechanismus však musí být dostatečně obecný, navíc síť jako celek nelze podrobit testování či dokonce certifikaci
- Neznámý perimeter - nikdy nevíme, kdo všechno je připojen, není jasné, jak se ostatní stroje chovají
- Množství zranitelných míst - je nutné uvěřit bezpečnostním mechanismům na všech strojích, mnohé části sítě leží mimo jakýkoliv dohled provozovatelů
- Neznámá cesta - většinou nelze ovlivnit, kudy budou data přenášena, tedy není k dispozici žádná informace, kdo s nimi může přijít do styku

Ochrana komunikace

principiálně je možné chránit komunikaci jakožto:

- proud dat – někdy nazýváno jako „stream enciphering“, tj. šifrování proudu dat, kdy se vytváří dojem, že komunikační kanál je spolehlivý z hlediska možného útoku
- jednotlivé zprávy – odpovídá dnes moderní volné vazbě systémů pomocí „messagingu“, šifrují se aplikační zprávy, nebo jejich relevantní části

proudové šifrování lze provádět mezi dvěma uzly sítě, nebo mezi dvěma aplikacemi běžícími na těchto uzlech

Šifrování na úrovni linky (Link Encryption)

data jsou šifrována těsně před vstupem do komunikačního media, dešifrována ihned po příchodu na druhý počítač

toto šifrování probíhá na úrovni fyzické případně linkové vrstvy referenčního modelu

výhodou je, že tento mechanismus je pro uživatele transparentní a může být i velmi rychlý, navíc je snadno připojitelný k stávajícím zařízením

je zcela nevhodný pokud nejsme schopni ovlivnit, kudy budou data přenášena

End-to-End šifrování

poskytuje kryptografickou ochranu po celou dobu přenosu

toto šifrování probíhá přibližně na úrovni aplikační nebo prezentační vrstvy referenčního modelu

toto šifrování však již nebývá transparentní a má-li být účinné, musí být vhodně zakomponováno do celého systému

další výhodou je, že není nutno šifrovat veškerou komunikaci, ale pouze citlivá data na rozdíl od šifrování linky je schopno zajistit autentizaci a integritu (end-to-end)

někdy jsou používány obě zmíněné metody zároveň - šifrování linky za účele běžné preventivní ochrany dat a End-to End šifrování k docílení skutečně kvalitní ochrany senzitivních dat

se zavedením šifrování souvisí nutnost existence mechanismu distribuce a správy nezbytných šifrovacích klíčů, potřebných centrálních autorit pro zajištění provozu systému kryptografické ochrany, vhodných kryptografických zařízení zajišťujících základní funkce kryptografické ochrany

Kontrola přístupu

v případě sítí přistupují k obvyklým problémům kontroly přístupu ještě následující okruhy

Ochrana komunikačních portů (Port protection)

před mechanismus autentizace uživatele lze předřadit ještě ochranu vlastního komunikačního portu

Automatické zpětné volání

metoda vhodná pro komutované (dial-up) spoje

Poté, co je navázáno spojení a uživatel se identifikuje, systém ukončí spojení, v interních tabulkách zjistí adresu (tfn. číslo) daného uživatele a pokusí se o navázání spojení na tuto adresu.

Tímto způsobem je zajištěno, že přístup je možný pouze z omezeného množství jiných uzlů (adres) a tedy výrazně omezena či alespoň zkomplikována možnost průniku 'zvenčí'.

Odstupňovaná přístupová práva

Přístup k senzitivním datům může být omezen na pouze některé uzly. Pokud i autorizovaný uživatel žádá o přístup z jiného uzlu, mohou jeho přístupová práva být výrazně omezena, nebo může být zcela odepřen přístup k datům.

Tichý modem (Silent Modem)

Po přijetí volání modem nezačne bezprostředně generovat nosnou, ale počká, až se druhá strana pokusí o negotiation.

Tím je přístup do jisté míry omezen pouze na uživatele, kteří vědí, že jde o linku vedoucí k počítači, metoda omezuje možnost náhodného nalezení tohoto portu.

Obdobou tichého modemu může být v případě IP protokolu služba, dostupná na daném stroji na jiném než obvyklém portu.

Řízení přístupu z vnějšího prostředí

- Firewally – filtry, aplikační brány
- Překlad adres
- Kontrola přenášených dat – antiviry, java, scripty,
- Omezení přístupu ke zdrojům / obsahu dat
- Prioritizace, qos
- IDS, IPS (intrusion detection/prevention system) – síťové, aplikační
- Demilitarizované zóny
- Content filtry

Parcelizace vnitřní sítě

- Oddělení kritických zdrojů, zónování
- Vydělení zvláštní sítě pro senzitivní informace
- Traffic shaping

Autentizace uzlů

Je třeba, aby existovaly mechanismy umožňující vzájemnou autentizaci jednotlivých uzlů, ne pouze uživatelů.

Autentizace v síti

Protože síťové prostředí zpravidla není považováno za bezpečné, je třeba využívat autentizační mechanismy odolné vůči odposlechu, resp. aktivním útokům

Často bývá žádoucí řešit *jednotné přihlášení (single sign on)*

- cookies

- tickety
- certifikáty, PKI
- čipové karty
- ...

S procesem integrace autentizačních mechanismů souvisí nutnost zavedení centrální správy uživatelů nebo alespoň synchronizace záznamů o uživateli

Aktivní útočník

v případě jednotlivých strojů může být útočníkem člověk, v prostředí sítí však již útočník může používat počítač a pokoušet se aktivně poškodovat systém ochrany dat

Playback starších zpráv

pokusy o znovupoužívání starších zachycených zpráv vhodnou metodou ochrany jsou časová razítka v kombinaci s šifrováním, různé tokeny s omezenou časovou platností, notarizace, nebo ofsetování zpráv.

Narušení služeb

velmi snadným způsobem útoku je přetěžování sítě nesmyslnými zprávami rovněž účinnou metodou je pokusit se pozměňovat routovací informace rovněž je možné zachycovat, nebo alespoň poškodovat zprávy zasílané určitému uživateli

proti mnohým útokům je možno se bránit vytvořením duplicitních linek, po kterých mohou být zprávy posílány, pokud je to možné, lze se omezit pouze na důvěryhodné uzly

Vkládání poškozených zpráv

útočník může vkládat poškozené zprávy, při jejichž zpracování může dojít ke zhroucení službu konajícího stroje, nebo k jeho nesprávné funkci

Řízení zátěže

útočník může zachycovat veškerou komunikaci a provádět rozbor, kdo s kým jak často komunikuje - jde o tzv. *analýzu zátěže* : z náhlých změn zátěže lze usuzovat na nadcházející výrazné události

vhodnou metodou ochrany je generování *vycpávací (pad) zátěže* v době, kdy nedochází ke skutečné komunikaci

Vycpávací zátěž

generovaná vycpávací zátěž může být prostředkem pro vytvoření skrytého kanálu administrátor tedy musí zajistit generování dalších vycpávacích zpráv doplňujících komunikaci mezi libovolnými dvěma uzly sítě

Kontrola routování

administrátor může aktivně zasahovat do procesu routování a náhodně měnit způsob routování některých zpráv, čímž se dosáhne větší náhodnosti do procesu přenosu zpráv a omezí možnost předchozích útoků

Další metody ochrany

administrátor může aktivními zásahy zvyšovat bezpečnost:

- náhodně zachycovat a mazat zprávy
- náhodně měnit adresáta zprávy na nejnižší úrovni
- pozdržovat doručení náhodně vybraných zpráv

Integrita dat

přenos zpráv je řízen přenosovými protokoly zajišťujícími integritu dat, pořadí doručených částí, detekci duplicit apod.

pro účely ochrany dat nedostačující - tyto informace jsou v plaintextu bez potřebné detekce modifikací

různé zabezpečovací kódy je snadné replikovat

vhodnější je použití kryptografických kontrolních součtů - zde je vhodné do každého šifrovaného bloku zprávy přidat jeho pořadové číslo, aby útočník nemohl provádět záměny pořadí

notarizace zpráv - každou posílanou zprávu je možné nechat ověřit centrální autoritou

Lokální síť

jsou v mnohém specifické - jejich uživatelé často jsou lidé pracující ve společném oboru, bývají laici v oblasti počítačů, povětšinou si mezi sebou do značné míry důvěřují

problémy nastávají při vzájemném propojování těchto sítí

lokální síť má většinou jednotnou topologii, dle které lze modifikovat použité ochranné mechanismy

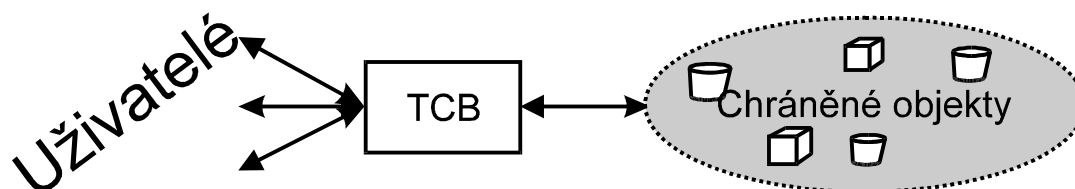
vzhledem k tomu, že lokální síť bývá umístěna uvnitř jedné budovy, či dokonce pouze její části, lze uplatnit různé metody fyzické ochrany

lokální síť rovněž mívá administrátora, který může efektivně vynucovat dodržování stanovené bezpečnostní politiky ve všech uzlech

zvýšená míra důvěry však vede ke snížení obranyschopnosti v případě náhlého útoku či zvýšení jeho hrozby

Víceúrovňová bezpečnost

rovněž v počítačových sítích mohou pracovat uživatelé s různým stupněm prověření, síť obsahuje data různých stupňů utajení
nejčastěji se používá nějaká modifikace military security modelu
operační systémy, navrhované pro vysokou bezpečnost bývají rozděleny na moduly, na jejichž bezpečnost nejsou kladeny nároky, které přistupují k chráněným objektům prostřednictvím spolehlivých modulů, jež tvoří *spolehlivou výpočetní bázi (TCB)*

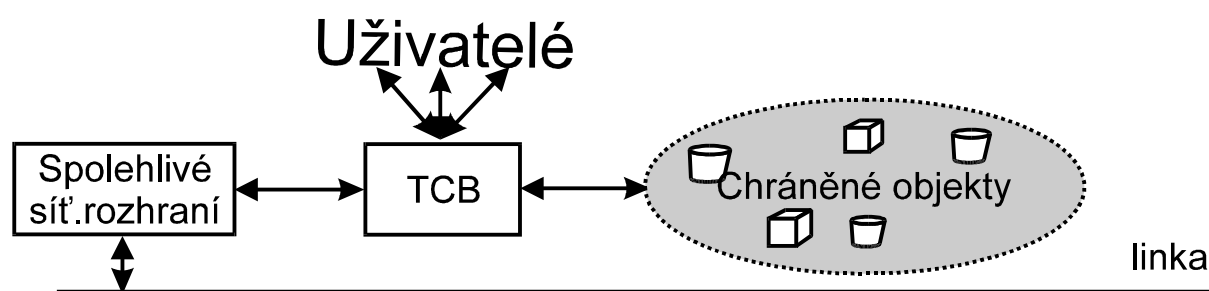


obdobně pro síť:

Spolehlivé síťové rozhraní (trusted network interface)

každý uzel sítě musí být "opatrný" vůči ostatním uzlům, měl by zajistit, že spojení naváže pouze s dalším uzlem, který má spolehlivé síťové rozhraní
funkce spolehlivého síťového rozhraní:

1. zajištění bezpečnosti vlastního uzlu - před útoky zvenčí
2. veškerá výstupní data musí být označena příslušnou bezpečnostní klasifikací
3. před uvolněním dat je provedena verifikace oprávněnosti žadatele a jeho autentizace
4. ověření konzistence došlých dat
5. nesmí docházet k míchání dat různého stupně utajení, nebo samovolnému předávání informací ostatním uzlům
6. bezpečnost dat nesmí záviset na bezpečnosti linky



Bezpečná komunikace

vlastní síť včetně příslušných řídicích modulů není uvažována
bezpečnou komunikaci zajišťují samy komunikující procesy ve spolupráci s operačním systémem
jsou dodržována pravidla Bell-LaPadula bezpečnostního modelu
pokud chceme zavést potvrzování zpráv, je nutné, aby na každém uzlu běžel pro každou bezpečnostní úroveň komunikační server - posílá-li proces zprávu procesu vyšší úrovně na jiném uzlu, zašle ji tamnějšímu kom. serveru své úrovně, od kterého obdrží potvrzení a který ji předá
posílání zpráv procesům nižší úrovně probíhá prostřednictvím spolehlivé centrální autority - *network manažera*, který zkoumá, zda nedochází k únikům klasifikovaných informací

Bezpečné síťové spojení

spolehlivá síťová rozhraní rozdělíme na moduly se vstupními a výstupními sokety
pokud u daného modulu můžeme dokázat, že jeho výstupy závisí pouze na některých vstupech - *multilevel modul* - může mít výstupní sokety různých úrovní citlivosti

jinak má modul výstupy odpovídající nejvyšší citlivosti vstupu

opět budeme dbát na zachování pravidel Bell-LaPadula modelu, tzn. výstup modulu může být připojen pouze na vstup jiného s nejméně stejným stupněm citlivosti
každý proces prohlásíme rovněž za modul se specifickým stupněm citlivosti
takto lze definovat povolená spojení v rámci celé sítě

Bezpečnost komunikace

bezpečnost je do určité míry závislá na použitém přenosovém mediu
útok proti komunikačním linkám může být *pasivní* (pouze odposlech), nebo *aktivní* (vkládání dalších informací do komunikace)

Kabely

častým útokem je tzv. *napíchnutí* (wiretaping)

proti tomuto způsobu útoku jsou obzvláště bezbranné metalické vodiče, je však možné monitorovat i optické kabely

obecně lze mezi metalickými kabely považovat za bezpečnější kabely koaxiální
vyrábí se celá řada kabelů s omezeným vyzařováním případně s detekcí napíchnutí
k napíchnutí jsou náchylnější pevné linky (leased lines), obecně je útok pravděpodobnější u některého z konců linky

Mikrovlny

svazek není možno zcela přesně měrovat, navíc se mírně rozbíhá
komunikace může být zachycena kdekoli mezi vysílačem a přijímačem, nebo v
prostoru za přijímačem
obdobné nedostatky z hlediska možnosti aktivního útoku

Satelitní přenos

poznamenejme, že ta samá technologie je používána k **šíření** TV signálu

Celulární radio

nebezpečí útoku je velké, vlastní zejména pasivní útok je snadno proveditelný

Analogové sítě

většina těchto sítí původně navržena pro přenos hlasu,
častým problémem autentizace, sítě většinou neposkytují informace o zdroji
přenášené informace
problém lze řešit zejména použitím kryptografie v zařízeních tvořících rozhraní
těchto sítí a počítače, dosud však neexistuje dostatek standardů

X.25

veřejné datové sítě již poskytují prostředky pro autentizaci entit, umožňují
vytváření uzavřených logických podsítí celé sítě
vlastní komunikační linky bývají spolehlivější
lze rovněž provádět end-to-end šifrování přenášených dat, bohužel již ne šifrování
záhlaví zpráv, tedy je možná analýza zatížení
nebezpečí představují připojení via trojici protokolů X.3, X.28, X.29 - po
analogových linkách - zde nelze spoléhat na autentizaci
obecným problémem potom je propustnost těchto sítí

ISDN

poskytuje celou řadu identifikačních služeb počínajíc identifikací volajícího či
volaného účastníka a končíc možnostmi omezit nebo zcela vyloučit spojení z (jiných
než) určitých směrů
daleko propracovanější vytváření logických podsítí

Pevné linky

výhodou je, že linku používá pouze nájemce, je jisté spojení
na druhou stranu okruh vede stále stejnou cestou, je snadněji k nalezení a
následnému odposlechu

X.400 - message handling

protokol poskytuje kompletní škálu bezpečnostních funkcí - autentizace původu zpráv, důkazy přijetí, security labeling, utajení toku dat a spojení, autentizace entit, bezpečnost přenášené informace, zajištění integrity a neopakovatelnosti