Bezpečnost

11. Informační bezpečnost 2

doc. Ing. Róbert Lórencz, CSc.

České vysoké učení technické v Praze
Fakulta informačních technologií
Katedra počítačových systémů

Příprava studijních programů Informatika pro novou fakultu ČVUT je spolufinancována Evropským sociálním fondem a rozpočtem Hlavního města Prahy v rámci Operačního programu Praha — adaptabilita (OPPA) projektem CZ.2.17/3.1.00/31952 – „Příprava a zavedení nových studijních programů Informatika na ČVUT v Praze“.
Praha & EU: Investujeme do vaší budoucnosti

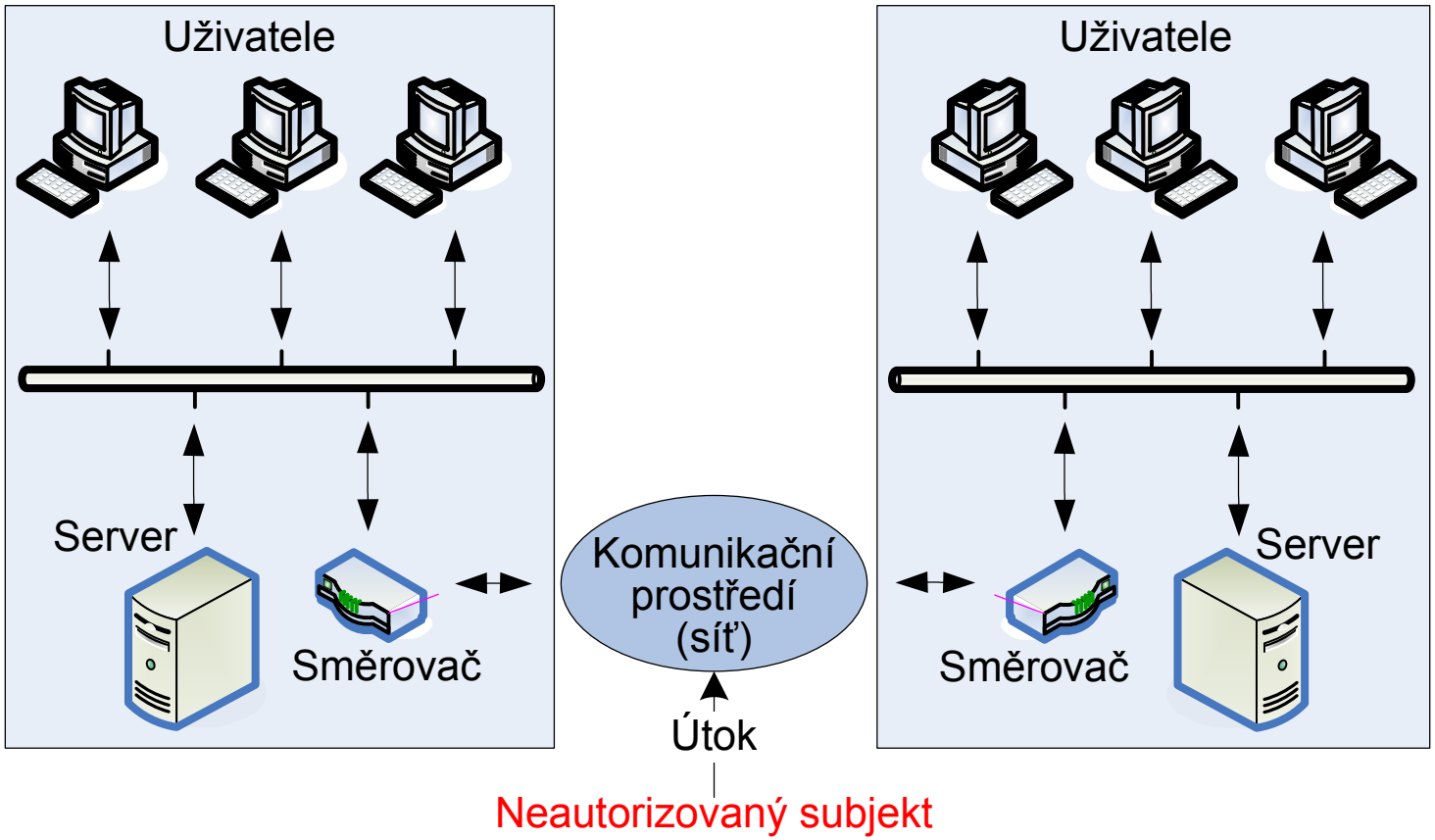
Obsah přednášky

- Síťová bezpečnost
- Komponenty síťové bezpečnosti
- Firewally
- Útočníci a systémy na jejich detekci
- Škodlivý software

Síťová bezpečnost

- Komunikační prostředí vytváří prostor pro potenciální útoky
- síťová bezpečnost (network security) řeší problémy bezpečnosti v sítích.

Typická konfigurace počítačových a telekomunikačních sítí

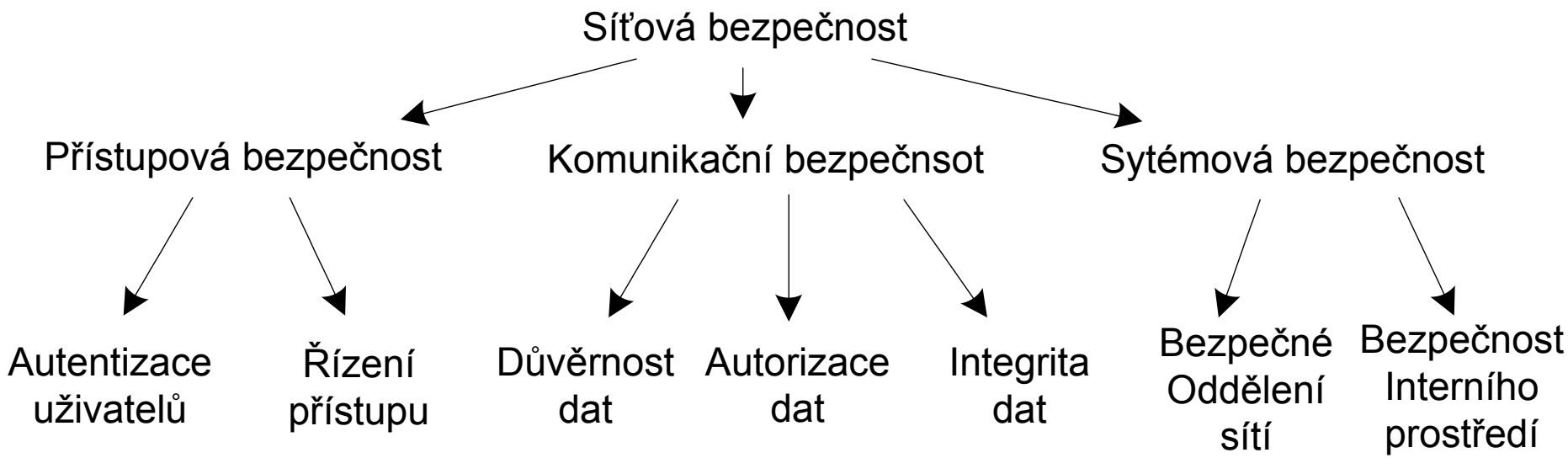


Komponenty síťové bezpečnosti (1)

Základní komponenty síťové bezpečnosti

- Přístupová bezpečnost
- Komunikační bezpečnost
- Systémová bezpečnost

Komponenty síťové bezpečnosti



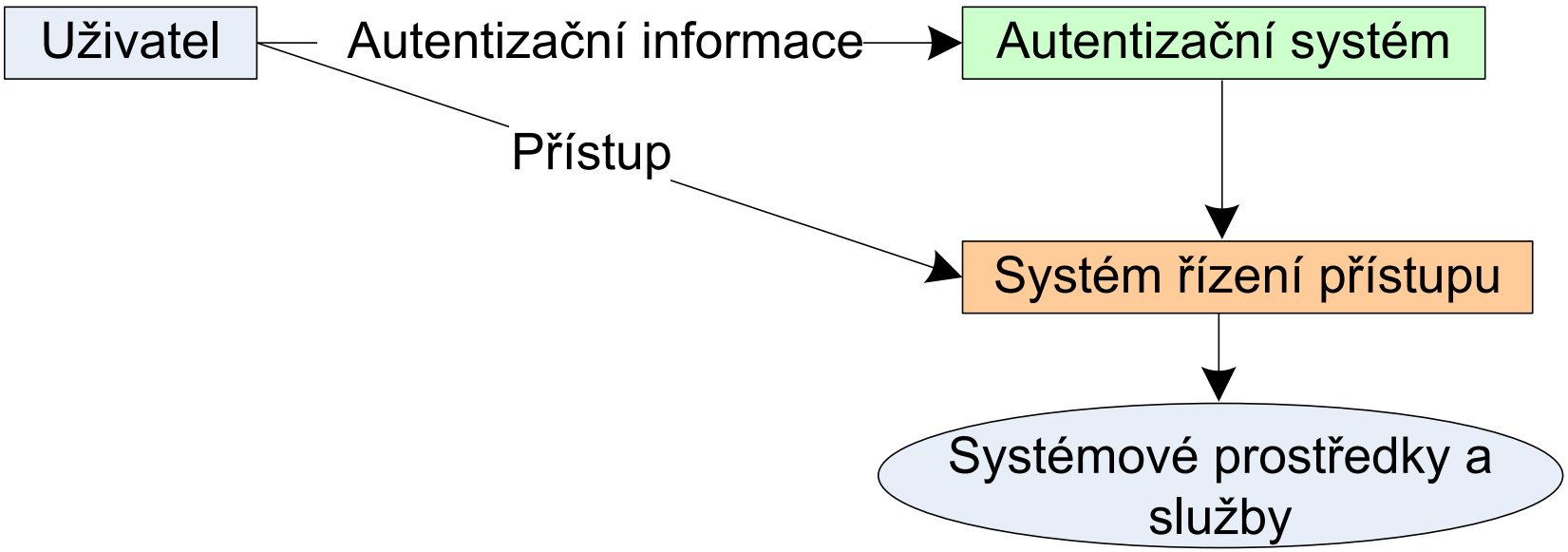
Komponenty síťové bezpečnosti (2)

Přístupová bezpečnost

Ověřuje identitu uživatelů žádajících o přístup k IS nebo síti.

Autentizace uživatelů: cílem je ověření identity a následné rozhodnutí o přístupu k systémovým prostředkům a službám. Toto vykoná systém řízení přístupu určující současně rozsah a pravomoci přístupů.

Autentizace uživatelů a řízení přístupu



Komponenty síťové bezpečnosti (3)

Autentizace uživatelů je složena z následujících 3 fází:

1. Registrace platného uživatele - přiřazení autentizační informace uživateli (také registrační fáze).
2. Získání autentizační informace od uživatele - informace potvrzující totožnost uživatele předepsaným způsobem.
3. Povolení/zamítnutí přístupu k sys. prostředkům a službám.

Autentizační informace splňuje:

- jednoduchost generování nebo zapamatování uživatelem,
- jednoduchost utajení,
- lehká manipulace.

Generování autentizační informace může být založeno:

1. prokazatelné znalosti něčeho (something to know),
2. prokazatelné vlastnictví něčeho (something to have),
3. důkaz biometrickými parametry (something to be).

Komponenty síťové bezpečnosti (4)

Autentizační informace na bázi znalosti:

- Nejčastěji má formu hesla, osobního identifikačního čísla (PIN), nebo jiné posloupnosti znaků.
- Nevýhoda jsou nároky na zapamatování a nutnost ji měnit v pravidelných intervalech.
- Musí být dostatečně složitá.

Autentizační informace na bázi vlastnictví:

- Vlastnictví speciálního technického prostředku - čipová karta, mag. karta, USB token atd.
- Elektronicky generuje autentizační informaci pomocí snímacího zařízení nebo připojení do systému přes stand. rozhraní.
- Nevýhoda - nesmí dojít ke ztrátě.

Komponenty síťové bezpečnosti (5)

Autentizační informace na bázi důkazu biometrickými parametry:

- Informace získaná o některé tělesné charakteristice uživatele - otisk prstu, dlaně, oční duhovky, řeči, atd.
- Problém: Je osoba živá? Je spolehlivost autentizace dostatečná?

Důležitá je otázka útoku v procesu autentizace. Mezi typické útoky na autentizační informaci můžeme zařadit:

- Útok odposlechem a opakováním – útočník odposlouchává proces autentizace a získané informace využívá později na autentizaci.
- Útok ze středu – útočník je zprostředkovatelem komunikace mezi komunikujícími subjekty.
- Útok na hesla – útok na verifikační tabulku hesel, haš kódů hesel v centrální databázi. Není tedy realizovaný v procesu komunikace.
- Útok na integritu – využívá nedokonalost výměny autentizační informace – protokolu. Protokol ne vždy řeší všechny situace $\Rightarrow$ lze jej modifikovat.

Komponenty síťové bezpečnosti (6)

Komunikační bezpečnost

Řeší otázky ochrany přenášených dat komunikačním prostředím. Základními typy ohrožení jsou odposlech přenosu a narušení integrity přenášených dat. Ochrana je použití mechanizmů zabezpečení důvěrnosti dat a mechanizmů autorizace nebo integrity dat.

Bezpečný přenos dat komunikačním prostředím je realizován na bázi komunikačních protokolů (jsou navrhovány pro konkrétní vrstvu síťového modelu). Z aplikačního hlediska můžeme kom. protokoly rozdělit do skupin:

- Realizace vzdáleného přístupu.
- Přenos souborů.
- Přenos HTML souborů.
- Elektronická pošta.
- Přenos paketů přes IP síť.
- Přenos souborů přes bezdrátové sítě.

Komponenty síťové bezpečnosti (7)

Vzdálený přístup: SSH je zabezpečená verze Telnetu. Data, příkazy a autentizační údaje se přenášejí v tomto protokolu zabezpečeně.

Přenos souborů: FTPS (Secure File Transport Protocol).

Přenos HTML souborů: HTTP (HyperText Transfer Protocol) pro využití rozmanitých služeb a přenos HTML souborů. Zabezpečená verze je HTTPS, který obsahuje specialní vrstvu s protokolem SSL (Secure Socket Layer). Novější verze tohoto protokolu je TLS (Transport Layer Security). Komunikace je u těchto protokolů obousměrně šifrována.

Elektronická pošta: Například využití programu PGP (Pretty Good Privacy) - šifrování a podepisování odeslaných souborů. Perspektivní je použití protokolu S/MIME (Secure MIME) - šifrování a autentizace dig. podpisem.

Komponenty síťové bezpečnosti (8)

Přenos paketů přes IP síť: Využívá se protokol IPsec, který obsahuje:

- Protokol na garanci bezpečnosti toku paketů. Používá se:
  - Protokol ESP (Encapsulating Security Payload) - slouží na šifrování toku paketů.
  - Protokol AH (Authentication Header) - zabezpečuje autentizaci a integritu dat, ne důvěrnost.
- Protokol na výměnu klíčů použitých na zabezpečení paketů. Používa se:
  - Protokol IKE (Internet Key Exchange).

Protokoly IPsec jsou povinné pro protokoly IPv6 a volitelné pro IPv4.

Bezdrátové sítě: většina založena na technologii Wi-Fi (Wireless Fidelity) a standardech IEEE 802.11. Bezpečnost je otevřenou otázkou. Protokol WEP (Wired Equivalent Privacy) a protokol WPA (Wi-Fi Protected Access) nabízí určitou možnost zabezpečení. Norma IEEE 802.11i by měla systematicky řešit otázku bezpečnosti.

Komponenty síťové bezpečnosti (9)

Sytémová bezpečnost Bezpečnost počítačů připojených na vnější komunikační prostředí - komunikační síť. Obsahuje zejména tyto 2 základní apspekty:

- Bezpečné oddělení sítí – vychází z koncepce vytvoření jediného sys. prostředku na bezpečnou komunikaci s externím komunikačním prostředím (potenciální útoky). Komunikace se realizuje výlučně přes tento systémový prostředek (firewall), který dohlíží na realizovanou komunikaci (gatekeeper functions). Firewall vymezuje chráněnou část sítě (perimeter security).
- Bezpečnost interního prostředí – zabezpečují mechanizmy označované: řízení bezpečnosti interního prostředí (internal security control). Tyto mechanizmy monitorují interní aktivity systému a analyzují uložená data z důvodu zjištění útočníka, který pronikl přes kontrolu do IS. K uvedeným mechanizmům patří zejména systémy na identifikaci útočníka a antivirové ochrany.

Firewally (1)

Firewall: soubor technických a programových prostředků zabezpečující bezpečné připojení sítí s různým stupněm bezpečnosti, nejčastěji externí sítě (Internet) a vnitřní sítě (Intranet). Externí síť se všobecně považuje za málo bezpečnou. Firewally můžeme rozdělit na:

1. Klasické: instalace je na vyhrazeném síťovém zařízení nebo na vyhrazeném počítači umístěném na rozhraní 2 sítí. Filtrují celý provoz procházející přes tyto prostředky.
2. Osobní: programové prostředky instalované na konkrétním počítači filtrující provoz tohoto počítače.

Z hlediska vrstvy síťového modelu, na kterém firewally vykonávají svou činnost je rozdělujeme:

- Firewally síťové vrstvy.
  - Jednoduchý filtr paketů.
  - Stavový filtr paketů.
- Firewally aplikační vrstvy.

Firewally (2)

Jednoduchý filtr paketů pracuje podle souboru pravidel, která zakazují komunikaci na jednotlivých portech firewallu. Nezakázaná komunikace je povolená - nevýhoda, na vyšší stupeň bezpečnosti musíme zakázat komunikaci přes vyšší počet portů. Také nelze analyzovat procházející data a povolovat/zakazovat jejich průchod podle jejich významu.

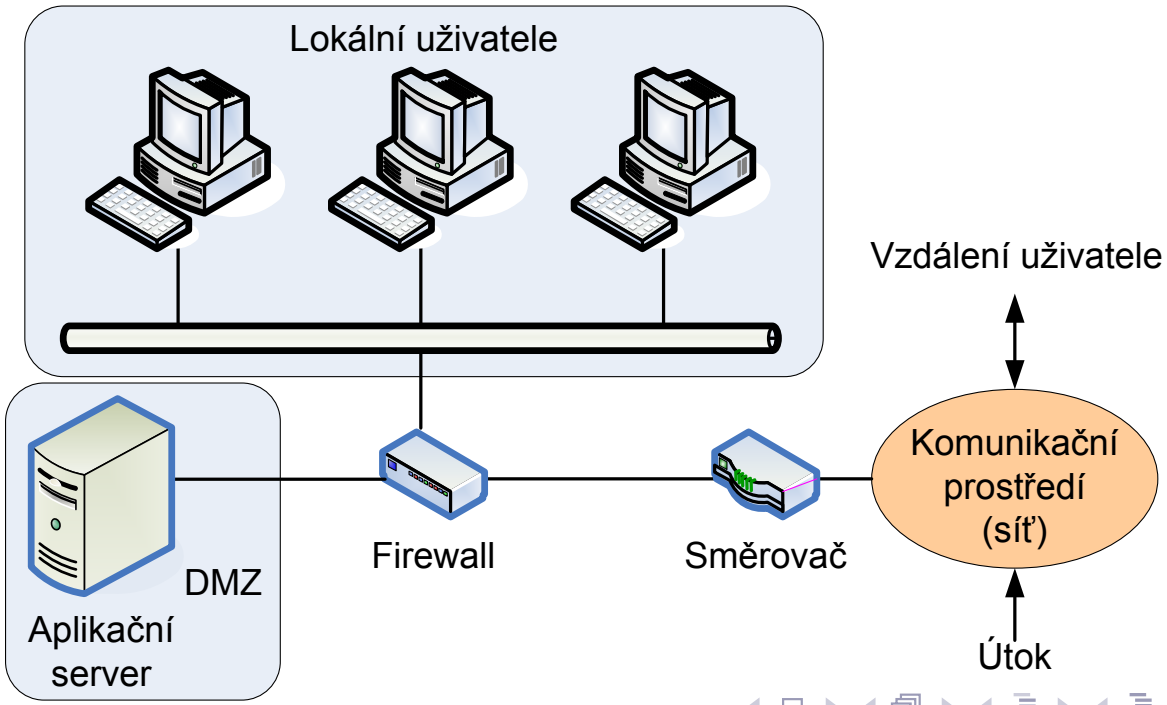
Stavový filtr paketů má definovanou tabulku stavů, kterou upravuje podle síťového provozu. Komunikace se povoluje/zakazuje podle nastavení pravidel a stavové tabulky. Do určité míry je tady možnost kontroly komunikace podle aplikační vrstvy.

Firewally na aplikační vrstvě mají možnost identifikovat pakety podle aplikace a realizovat filtraci podle aplikací. Při kontrole paketů lze zablokovat nežádoucí provoz přes konkrétní porty - zablokovat přístup do chráněné zóny (např. zabránit šíření virů). Příkladem firewallu na aplikační vrstvě je **proxy server** - propouští pakety určité aplikace.

Firewally (3)

Demilitarizovaná zóna – DMZ – je speciální síť, která slouží pro zprostředkování služeb klientů z externí sítě při zachování bezpečnosti počítačů nacházejících se v interní síti.

- Do DMZ vstupují klienti z interní a externí sítě přes firewall.
- Přímá komunikace mezi DMZ a externí sítí není možná.
- Přístup z externí sítě do DMZ je omezený přes porty firewallu.
- V DMZ jsou aplikační servery (poštovní server, web server atd.)



Útočníci a systémy na jejich detekci (1)

Útočník (intruder) je subjekt, který získá nebo chce získat neautorizovaný přístup/oprávnění v počítačovém systému. Můžeme je rozdělit podle různých hledisek:

- poloha útočníka vůči napadenému systému,
- odbornost vedeného útoku,
- úmysl vedeného útoku.

Z hlediska polohy útočníka existují tyto druhy útoků:

- Vnitřní útočník (Insider) – subjekt připojen do počítačové sítě, tedy legitimní uživatel, který získal neautorizovaný přístup, nebo subjekt zneužívající svých práv.
- Vnější útočník (Outsider) – subjekt, který nemá autorizovaný přístup do interní počítačové sítě a chce proniknout do této sítě využívajíc jejích zranitelných míst a bezpečnostních děr.

Útočníci a systémy na jejich detekci (2)

Podle odbornosti vedeného útoku můžeme útočníky rozdělit na:

- Amatéři – provádí méně nebezpečné útoky, které jsou adekvátní jejich nízké úrovni vzdělání a vybavení prostředky.
- Profesionálové – špičkoví počítačoví odborníci vybavení vědomostmi a prostředky. Jsou schopni generovat velmi nebezpečné útoky s vážnými důsledky.

Diskutovanou otázkou je dělení útočníků na:

- Hacker – osoba s dobrými až výbornými znalostmi z oblasti výpočetní techniky. Častokrát se podílí na výzkumných SW projektech a jeho znalosti výrazně pomáhají nacházet zranitelná místa a bezpečnostní díry navrhovaných systémů. Jejich činnost je prospěšná a užitečná. Existují hackerské kodexy popisující činnost hackerů.
- Cracker – osoba schopná obcházet protipirátské ochrany počítačových programů a využívající své vědomosti neeticky. Jsou i jiné definice zdůrazňující jinou stránku jejich činnosti.

Útočníci a systémy na jejich detekci (3)

Scriptkiddies – početná skupina útočníků s nízkou úrovní znalostí. Útoky realizují náhodně s využitím skriptů obsahujících kód využívající zranitelnost počítačového systému. Bez hlubší analýzy aplikují takový kód v počítačovém systému. Škodlivé následky jsou značné. Tato forma útoku je nejčastější a nebezpečná.

Detekce útočníků nebo útoků.

- Důležitý aspekt bezpečnosti. Existují speciální SW - Intrusion Detection System - **systémy IDS**. Buď jsou instalovány na jednotlivé klientské počítače (host based IDS) nebo na vhodně zvolený síťový prvek (network based IDS).
- IDS jsou obvykle spojeny s firewallem, kde detekují útok a následně generují pokyny pro firewall, který komunikaci zablokuje a informuje správce sítě.

Útočníci a systémy na jejich detekci (4)

Odhalování útoků pomocí IDS můžeme realizovat dvěma způsoby:

1. Vytvoření a využívání databáze znalostí o projevech jednotlivých útoků. Databáze se musí aktualizovat.
2. Využívání sledování a analýzy podezřelého chování systému nebo jeho projevu. Například náhlý nárůst přenášených dat, komunikace na nepovolených portech atd.

Jednou z variant systémů IDS je technika založená na jeho spojení s pastmi na útočníky – honeypot. Tato technika vytváří fiktivní počítačový systém (server) se záměrně sníženou bezpečností, který se pro útočníky stává cílem útoků. Tento systém plní následující úlohy:

- odvádí pozornost od reálných systémů,
- umožňuje monitorovat aktivity útočníka,
- umožňuje správci sítě přijmout účinná opatření.

Škodlivý software (1)

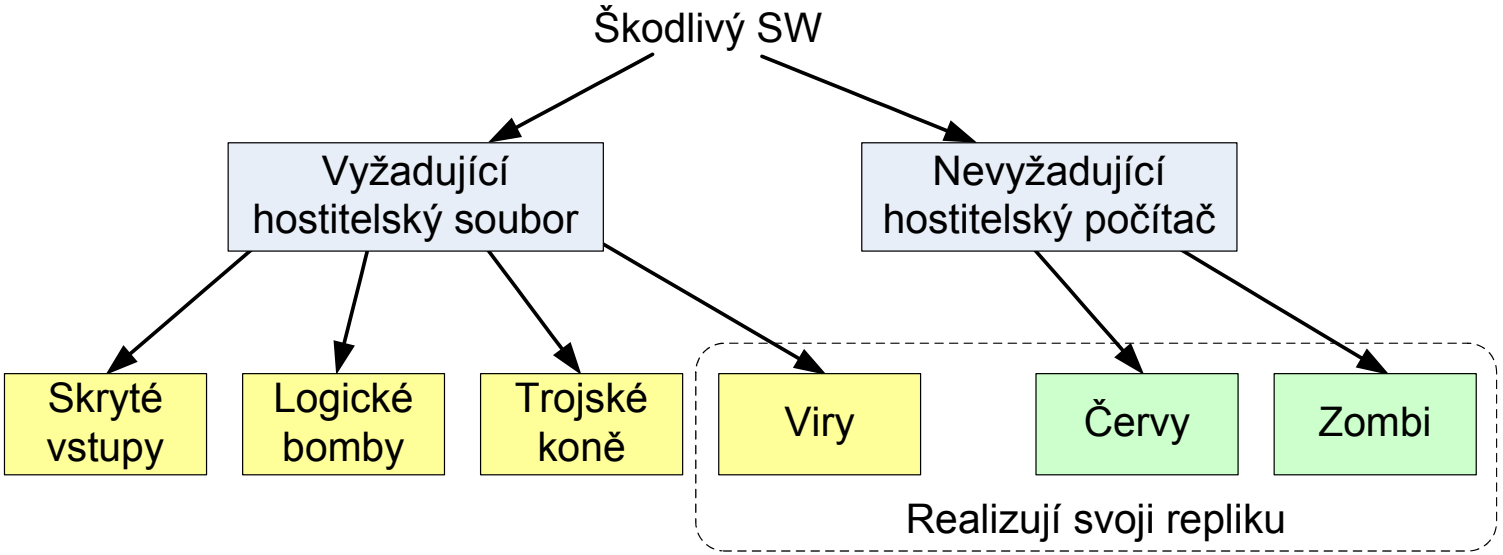
Škodlivý software (malicious software) – cílevědomě vytvořený počítačový program představující softwarové ohrožení počítačového systému. Může způsobit ztráty nebo škody v daném systému. Lze ho rozdělit do 2 základních kategorií:

- SW vyžadující na šíření hostitelský soubor. Dále se dělí na:
  - skryté vstupy,
  - logické bomby,
  - trojské koně,
  - viry.
- SW nevyžadující na šíření hostitelský soubor – SW, který je nezávislý. Dělí se na:
  - červy (worms),
  - zombie.

Škodlivý SW lze rozdělit také na:

- SW negenerující svoji repliku a
- SW generující svoji repliku.

Škodlivý software (2)



Skryté vstupy (Trap doors) – utajené vstupy do programu umožňující získat přístup do systému obcházením mechanizmu bezpečnosti. Uvedené vstupy byly využívány programátory hlavně při ladění a testování programů.

Logické bomby (Logic bombs) – nejstarší druh škodlivého SW. Program integrovaný do legitimního programu, který se aktivuje po splnění určitých podmínek. Příkladem takových podmínek může být přítomnost/nepřítomnost určitého typu souboru v určitý předvolený čas. Logická bomba může způsobit ztráty a škody v počítačovém systému.

Škodlivý software (3)

Trójské koně (Trojan horses) – programy/příkazy vykonávající určité užitečné funkce a současně vykonávající v pozadí nežádoucí a destrukční účinky (mazání dat atd.). Speciální případ je špehovací SW – spyware, který monitoruje a sbírá určité informace (hesla zadávaná přes klávesnici, navštěvované stránky, používaný SW atd.). Spyware tyto informace odesílá po Internetu na zadaná místa.

Viry (Viruses) – programy, které jsou schopné se připojit k jinému programu/souboru a vykonávat nežádoucí efekty. Pro své šíření vyžadují jiné soubory, které mohou modifikovat např. tak, že obsahují repliku viru. Viry mají schopnost napadat jiné soubory, šířit se a vyvolávat ztráty/škody v počítačových systémech.

Životní cyklus viru má 4 fáze:

- fáze nečinnosti,
- fáze šíření,
- fáze aktivizace,
- výkonná fáze.

Škodlivý software (4)

Jeden z možných způsobů dělení virů:

- viry šířící se pomocí spustitelných souborů
- viry šířící se přes zaváděcí programy
- neviditelné viry
- polymorfní viry
- makroviry
- emailové viry