



Act 2007

BIS 1

Bezpečnost informačních systémů

Petr Hanáček

Faculty of Information Technology

Technical University of Brno

Božetěchova 2

612 66 Brno

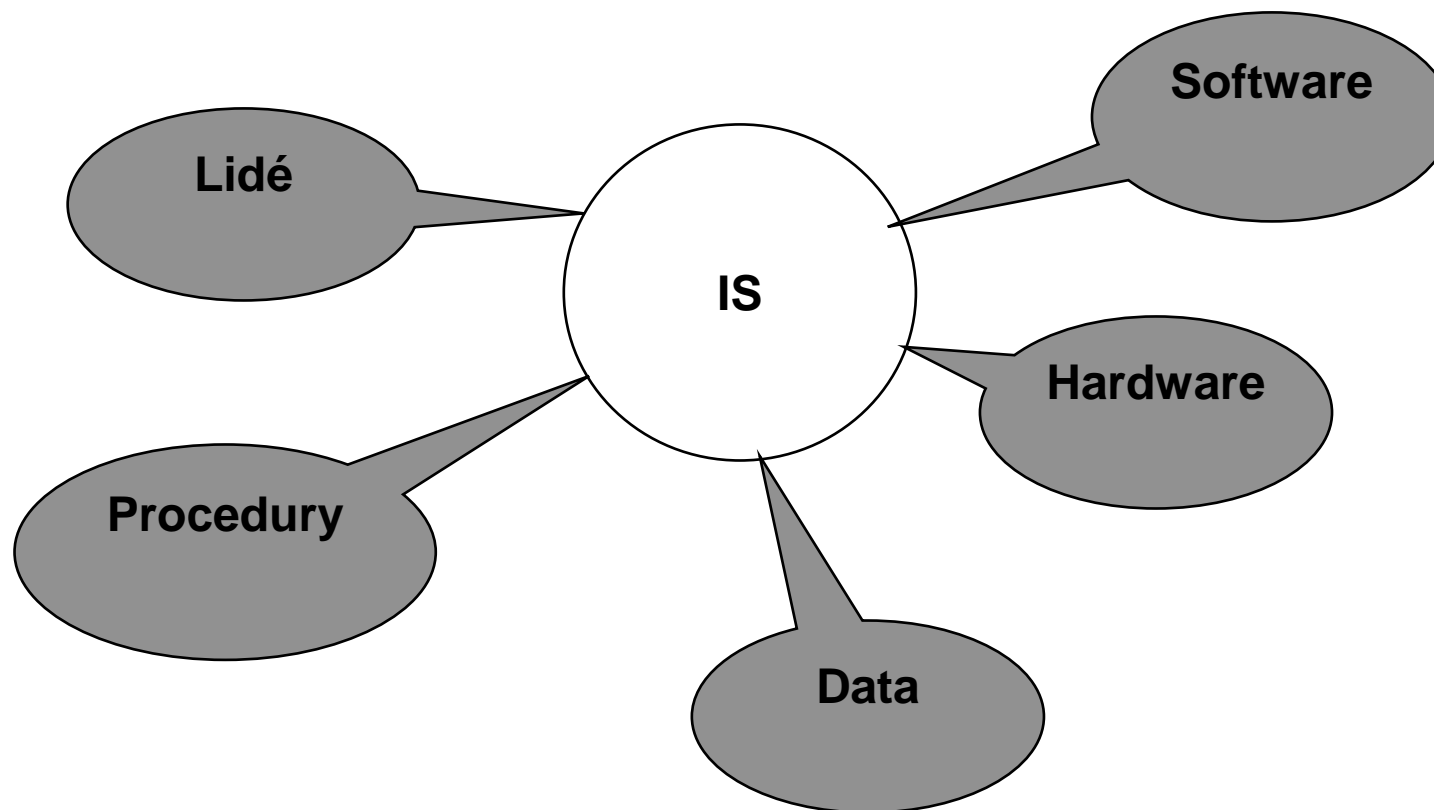
tel. 5 4114 1216

e-mail: hanacek@fit.vutbr.cz

Počítačová bezpečnost

- ... ochrana počítačových prostředků proti náhodnému nebo úmyslnému prozrazení důvěrných dat, neoprávněné modifikaci dat nebo programů, zničení dat, software nebo hardware, a neoprávněnému zabránění v použití počítačových prostředků. Také ochrana proti jiným počítačově provedeným kriminálním aktivitám, jako je počítačem spáchaný podvod nebo vydírání. [Palmer]

Informační systém

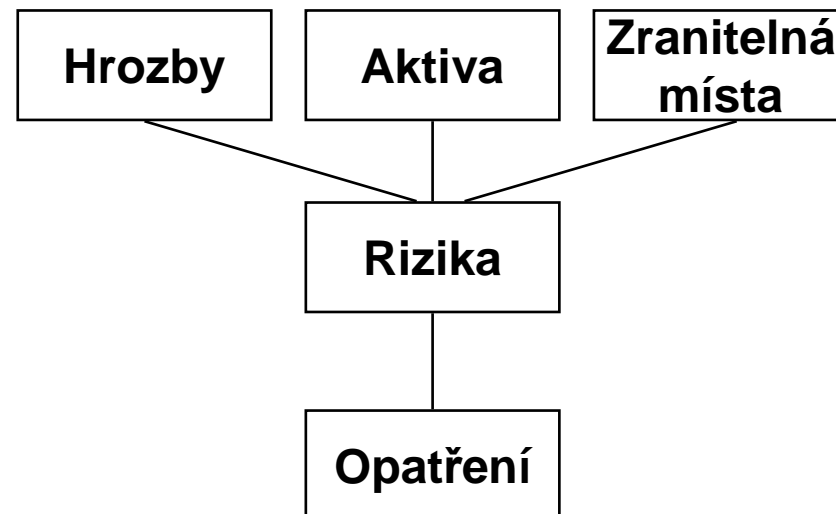


Cíle bezpečnosti IS

- **Confidentiality – důvěrnost – ochrana proti neoprávněnému prozrazení informace**
- **Integrity – integrita – ochrana proti neoprávněné modifikaci informace**
- **Availability – dostupnost – ochrana proti neoprávněnému odepření přístupu k datům nebo ke službám**

Další pojmy v bezpečnosti

- Zranitelná místa (vulnerabilities) – slabiny v informačním systému, která může být využita pro provedení bezpečnostního incidentu (útoku)
- Hrozby (threats) - okolnosti, které mají potenciál způsobit bezpečnostní incident
- Aktiva (assets) – složky IS, které mají hodnotu
- Opatření (measures) – redukuje pravděpodobnost vzniku bezpečnostního incidentu



Riziko

- Zranitelné místo, zkombinované s bezpečnostní hrozbou vytváří riziko.

Vulnerability + Threat → Risk

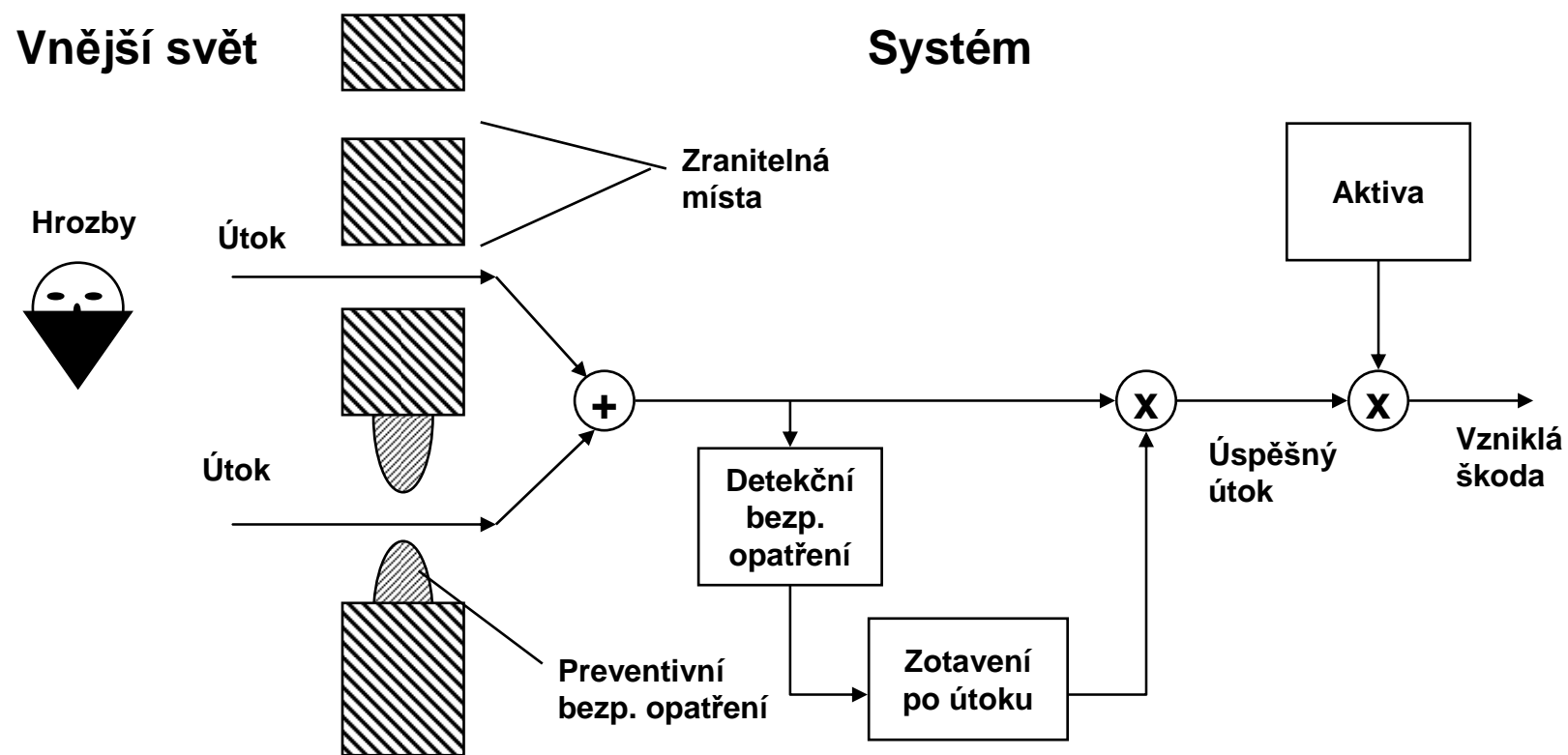
- **Příklad:**

Overflow Bug

+ Hacker Knowledge & Tools & Access

→ Risk of Webserver Attack

Bezpečnostní incident



Aktiva

TABLE 4-1 Categorizing the Components of an Information System

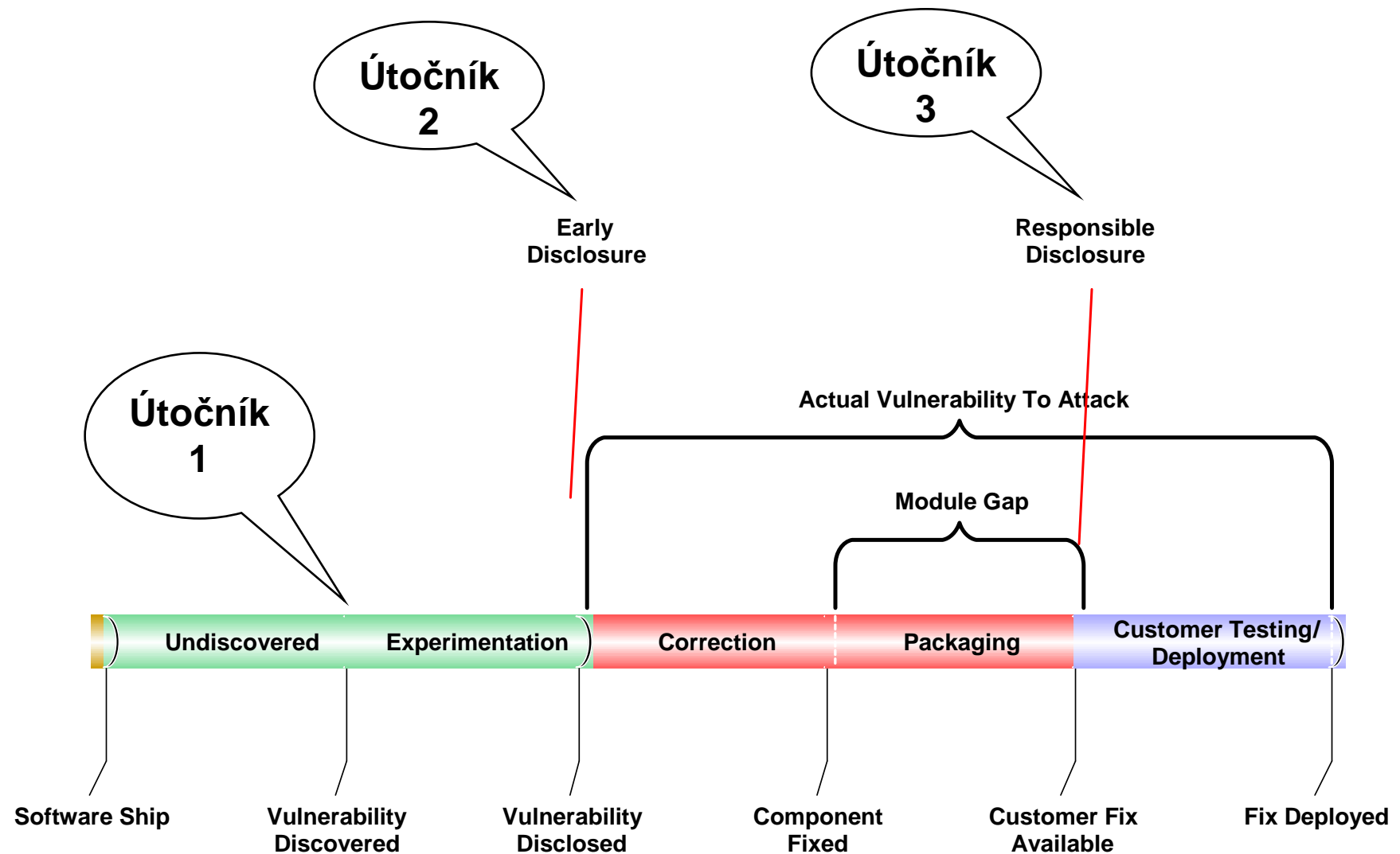
Traditional system components	SecSDLC and risk management system components	
People	Employees	Trusted employees Other staff
	Nonemployees	People at trusted organizations Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive procedures
Data	Information	Transmission Processing Storage
Software	Software	Applications Operating systems Security components
Hardware	System devices and peripherals	Systems and peripherals Security devices
	Networking components	Intranet components Internet or DMZ components

Zranitelná místa

Co je zranitelné místo?

- **Zranitelné místo (zranitelnost) je:**
Chyba nebo slabina v návrhu, implementaci nebo provozu systému, která může být využita pro narušení bezpečnosti systému. (RFC 2828).
- **Zranitelné místo**
 - Při návrhu – chyba architektury
 - Při implementaci -
např. buffer overflow
 - Při provozu – typicky nedodržení postupů

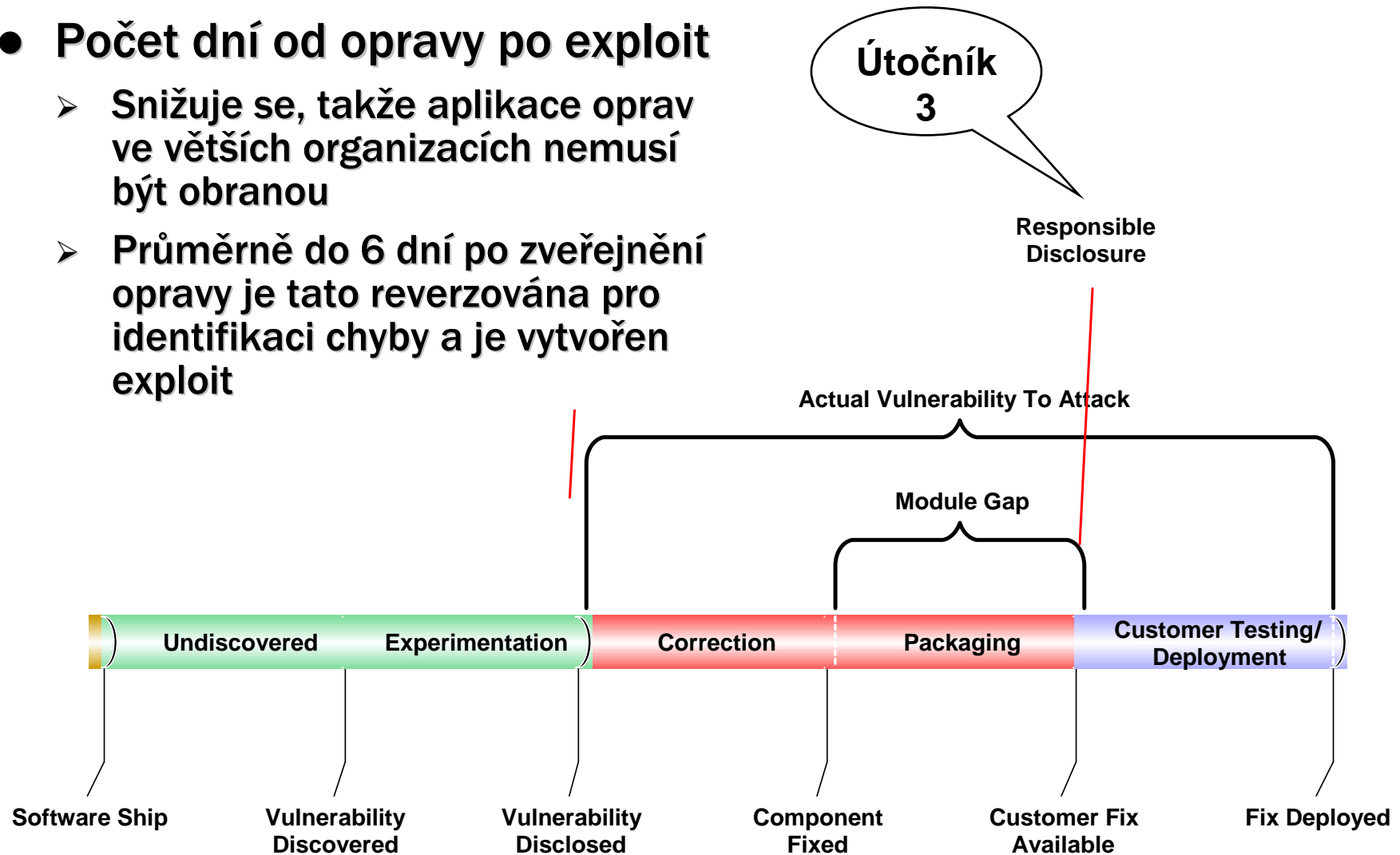
Chyby implementace



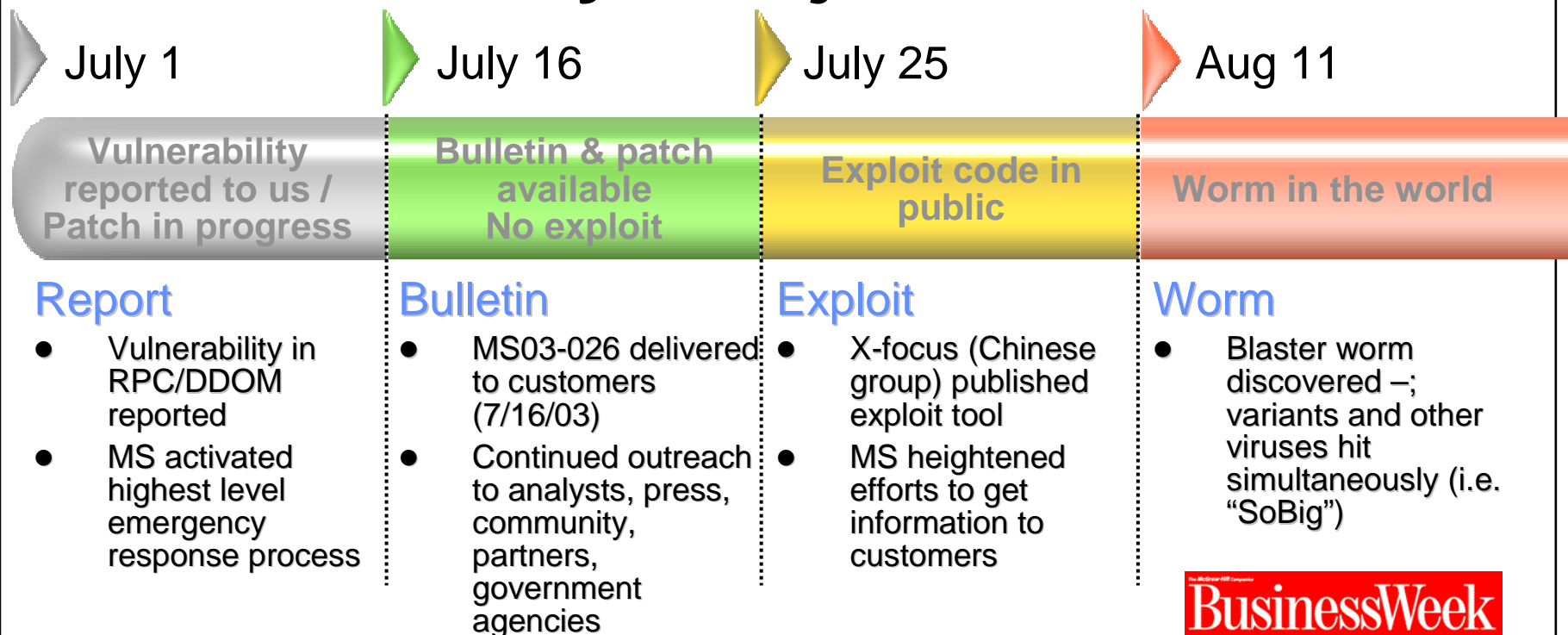
Chyby implementace

- **Počet dní od opravy po exploit**

- Snižuje se, takže aplikace oprav ve větších organizacích nemusí být obranou
- Průměrně do 6 dní po zveřejnění opravy je tato reverzována pro identifikaci chyby a je vytvořen exploit



Životní cyklus jednoho viru



Blaster shows the complex interplay between security researchers, software companies, and hackers



Source: Microsoft

© Petr Hanáček

The World Today

BIS Slide 14

Hrozby

Hrozby

- **Hrozba**
 - Hrozba je taková vlastnost prostředí, která může způsobit narušení bezpečnosti, pokud dostane příležitost.
- **Neúmyslné (nealgoritmické, pravděpodobnostní) hrozby**
 - » živelné události (požár, záplava, výpadek napájení)
 - » poruchy zařízení
 - » chyby v software
 - » selhání osob (omyly)

Hrozby II

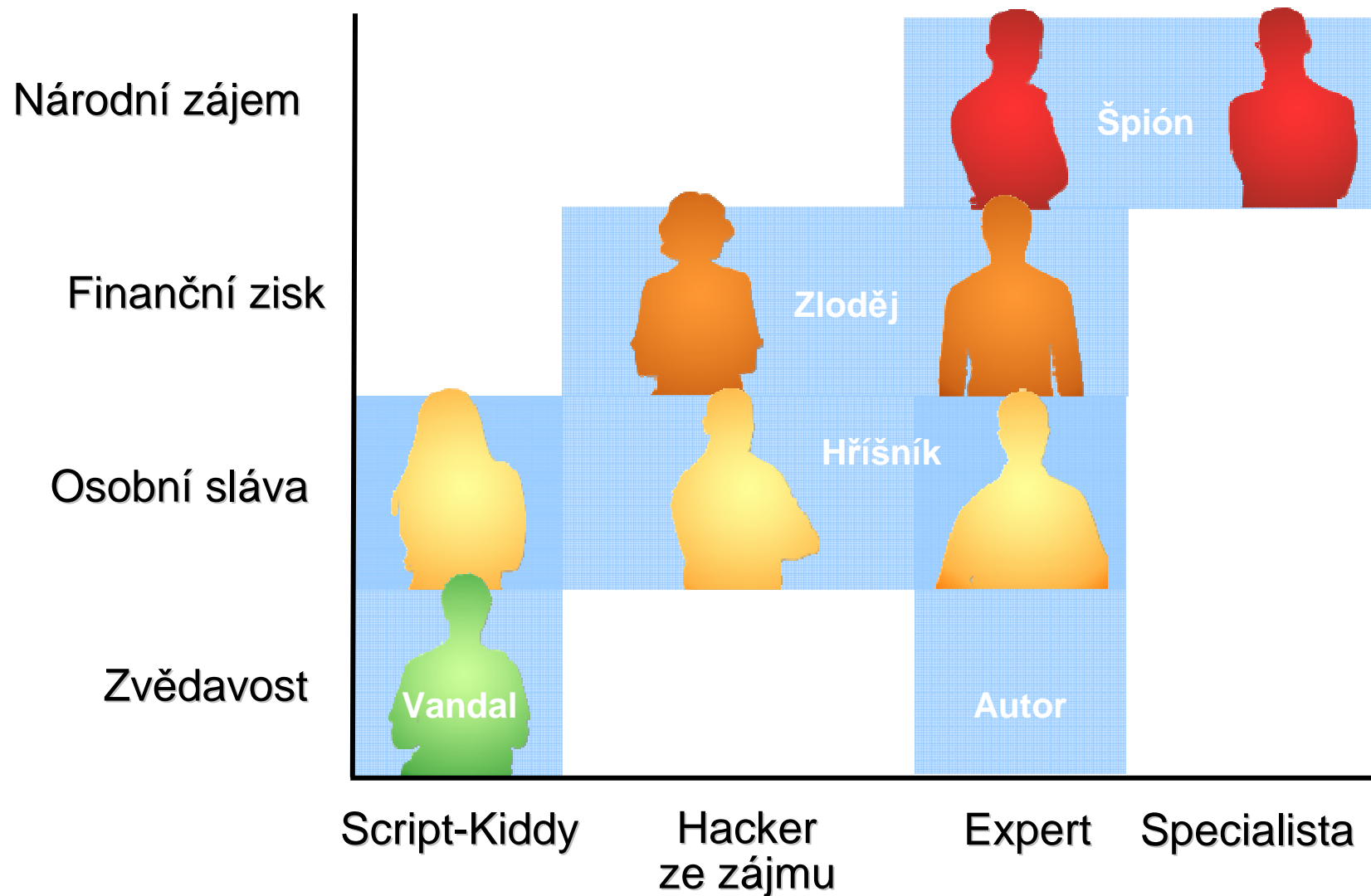
- **Úmyslné (algoritmické) hrozby**
 - cílem nejsou data
 - » krádež HW a médií
 - » úmyslné poškození, zničení zařízení
 - » neoprávněné využívání HW (krádež strojového času)
 - » založený požár, bomba
 - cílem jsou data
 - » krádež SW
 - » krádež dat (prodej, zneužití dat, průmyslová špionáž)
 - » neoprávněná manipulace s daty (modifikace, zničení)
 - škodlivé programy
 - » viry, červi, logické bomby, trojské koně

TABLE 4-3 Threats to Information Security

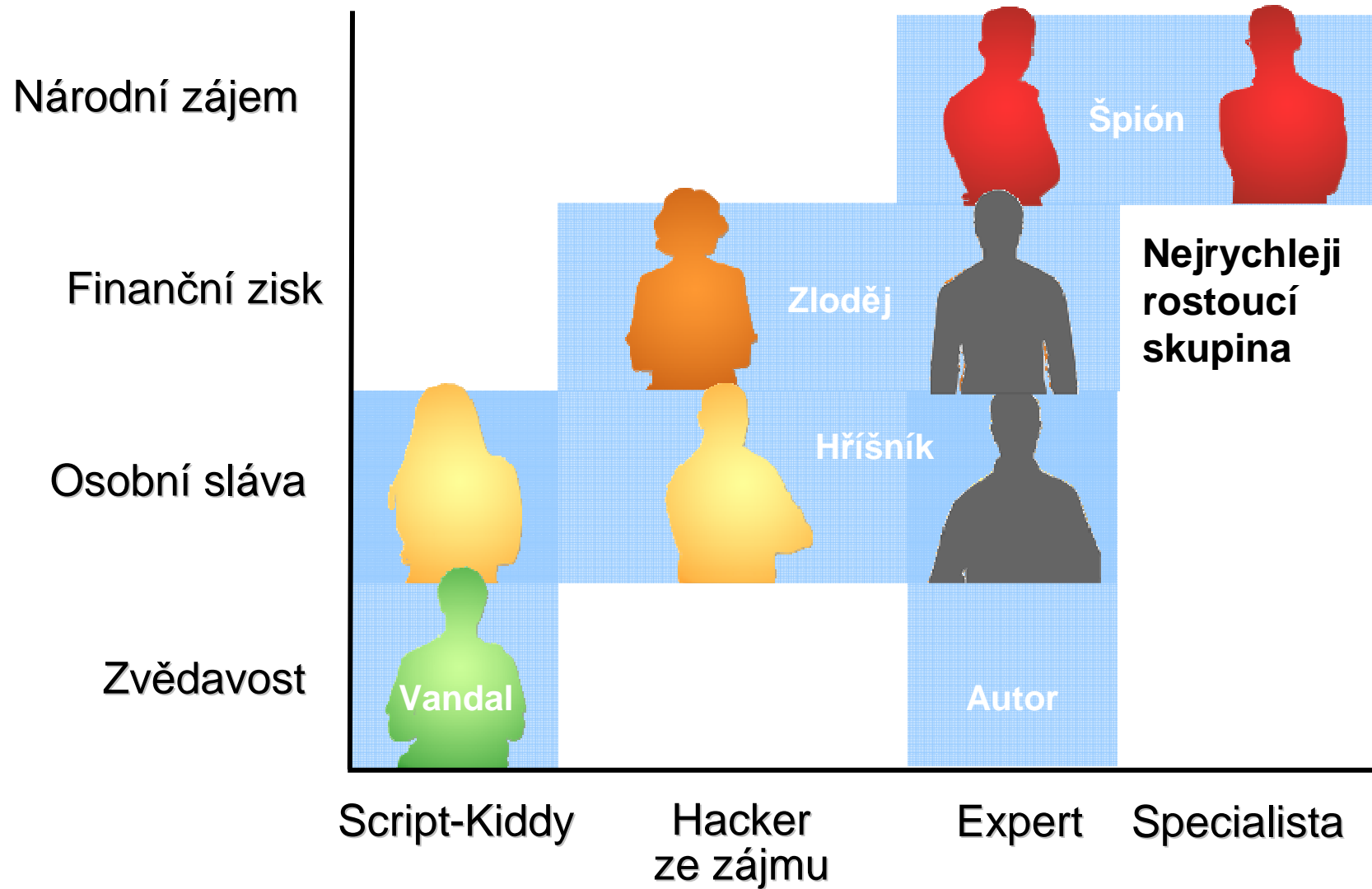
Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial of service
Forces of nature	Fire, flood, earthquake, lightning
Quality of service deviations from service providers	Power and WAN quality of service issues
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

©2003 ACM, Inc., Included here by permission.

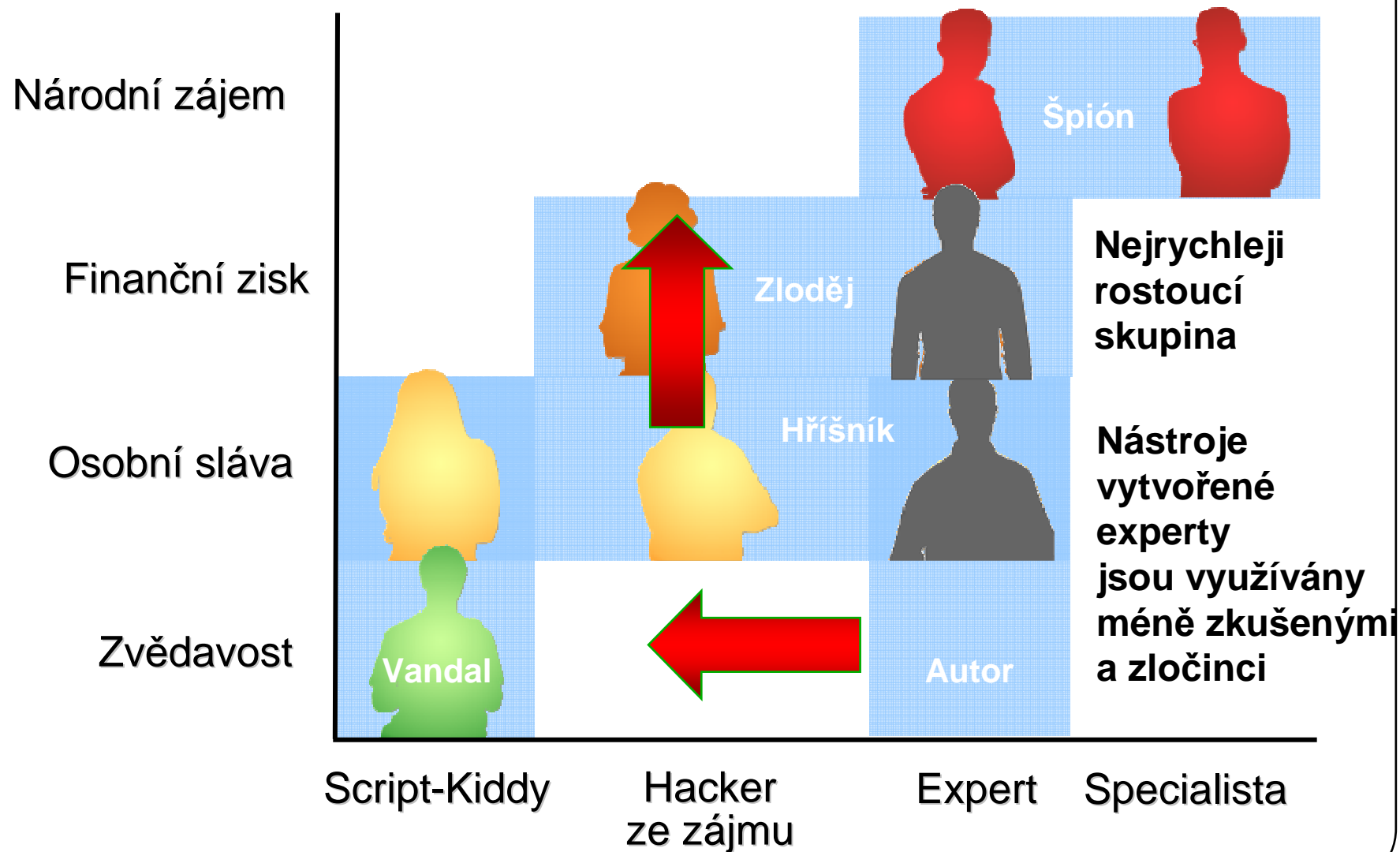
Galerie útočníků



Galerie útočníků



Galerie útočníků



Systemy Honey Pot

- Zkoumají online hrozby v síti
- Typická farma Honey Pot
 - Skupina počítačů s různými verzemi OS připojená k síti
 - Typický výsledek za týden:
 - » Počítače byly skenovány 46255 krát
 - » 4,892 přímých útoků
- Např. Windows XP bez aktualizací
 - Infikováno během 18 minut
 - Během hodiny se z něj stal "bot"

Source: StillSecure,

see <http://www.denverpost.com/Stories/0,1413,36~33~2735094,00.html>

Malware

Co je Malware?

- **„Škodlivý software“**
 - Software, který je v počítačovém systému a provádí neautorizované činnosti, zpravidla bez vědomí nebo souhlasu uživatele
- **Jsou to například**
 - Viry
 - Trojské koně
 - Červi
 - Logické bomby
 - Žertovné programy

Virus

“...program který vytváří kopie sama sebe tak, aby ‘infikoval’ části operačního systému nebo aplikačních programů.”

- *Survivor's Guide to Computer Viruses, Virus Bulletin, 1993.*

- **Provádí replikace**
 - Mezi soubory
 - Z disku na disk
- **Podmínky šíření**
 - široká populace počítačů se stejným operačním systémem
 - neexistence systému přístupových práv
 - rozvinutá výměna programů ve spustitelném tvaru
- **Typicky vyžaduje “hostitelský program”**
- **Musí být spuštěn**
- **Může provádět destrukční činnost**

Typy virů

- **Boot sector viry**
 - Infikuje boot record na disketě nebo disku
- **Souborový infektor**
 - Infikuje spustitelné programy
- **Makroviry**
 - Infikují dokumenty, které mohou obsahovat makra
- **Scriptovací virus**
 - V některém skriptovacím jazyku
- **Multipartitní**
 - Kombinace předchozích typů

Červ

- **Samostatný program**
- **Nepotřebuje hostitelský program**
- **Replikuje se ze systému na systém**
- **Infikuje systémy, ne soubory**
- **Typicky se šíří počítačovou sítí**

Internet worm



- Červ, který 2. listopadu 1988 napadl cca. 60 000 uzlů sítě Internet
 - uzly se vzpamatovaly až 5. listopadu
- Většina uzlů se odpojila od sítě
 - NASA Ames Research Center, Goddard Space Flight Center..
- Jaká slabá místa využíval pro vniknutí
 - zadní vrátka v programu `sendmail` (příkaz *debug*)
 - programátorskou chybu v programu *fingerd*
 - slabá místa v autentizaci - *rexec* a *rsh*
- Která sezení napadal
 - se slabými hesly (žádné, přihlašovací jméno, jméno...)
 - s hesly ve slovníku s 432 slovy
 - s hesly v souboru `/usr/dict/words`
 - sezení, která důvěřovala jiným stanicím pomocí mechanismu *.rhosts*



Trojský kůň

- Program, který úmyslně provádí nějakou skrytou činnost
 - Krádež hesel
 - Mazání souborů
 - Vytváření zadních vrátek
 - Připojování přes síť k jiným počítačům
- Neprovádí replikaci



Trojský kůň - příklad

- **NetBus a BackOrifice**
 - Nástroj pro vzdálenou správu, Remote Administration Tools (RAT)
 - Obvykle zaslán v nějaké hře
 - Dovoluje útočníkovi získat kontrolu nad počítačem
- **Subseven**
 - Přichází e-mailem jako maskovaný soubor (dvojitá přípona)
 - Pomocí IRC informuje autora o úspěchu
 - Poskytuje přístup k systému a může být využit pro DDoS útoky

Logická bomba

- Nereplikuje se
- Část kódu, která se aktivuje na základě splnění naprogramované podmínky
- Typicky provádí nějakou destrukční činnost
- **Příklad**
 - Program zničí data, jakmile jeho autor zmizí z výplatní listiny

Specificky internetové typy malware

- **JAVA**
 - Stažený kód interpretovaný na klientském počítači
 - Ochrana pomocí „pískoviště“ - Sandbox
- **ActiveX**
 - Nativní spustitelný kód, stažený z internetu
 - Může provádět cokoli (žádné pískoviště)
 - Ochrana podepisováním
- ...

Stále se zvyšuje rychlost šíření

<i>Malware</i>	<i>Type</i>	<i>Year</i>	<i>Time to #1</i>
Form	Boot Sector	1990	3 years
Concept	Word Macro	1995	4 months
Melissa	E-mail enabled word macro	1999	4 days
LoveLetter	E-mail enabled script	2000	5 hours
NIMDA	E-mail enabled script	2001	22 minutes

Source: ICSA/TruSecure

Techniky skrývání

- **Spoofing/Stealth**
 - Filtrace volání operačního systému tak, aby program byl neviditelný (rootkit)
- **Šifrování**
 - Šifrování kódu programu
- **Polymorfismus**
 - Způsobí, že virus vypadá po každé replikaci zcela jinak
 - Mutační stroje

Netradiční typy malware

- **Spam**
- **Phishing**
- **Spyware**
- **Boty**
- **Root Kity**

Spam

- **Hromadná nevyžádaná pošta**
- **Nekalé obchodní praktiky**
 - Direct mail
- **Podvodné zvyšování provozu webu**
 - Uměle vygenerované odkazy na web
- **Pro podvody**
 - Phishing
 - Krádež identity
 - Získávání hesel a jiných autentizačních informací

Phishing

- **Nalákání na podvodný web**
 - Více než 60% uživatelů navštíví podvodný web
- **Získání dat**
 - Více než 15% uživatelů poskytne nějaká osobní data
- **Ekonomická ztráta**
 - ~ 2% of uživatelů

Source: TRUSTe

From: Ioa@Citizensbank.com [mailto:Ioa@Citizensbank.com]
Sent: Wednesday, August 25, 2004 11:57 PM
To: [REDACTED]
Subject: Citizensbank.com account holdtq



Security key: qjkjazaqwrq

Dear Citizensbank.com Customer,

During our regular update and verification of the Internet Banking Accounts, we could not verify your current information. Either your information has been changed or incomplete, as a result your access to use our services has been limited. Please update your information.

To update your
<https://www.citizensbank.com>
AFTER SUBMITTING
FOR THE NEXT

Note: Requests for
cannot be external

Sincerely,
Citizensbank.com
Business Department

 210.21.224.21
sym.gdsz.cncnet.net
Host unreachable

 210.21.192.0 - 210.21.255.255

 China
shenzhen branch, china netcom corp

 yumei sun
sz-ipaddress@china-netcom.com
china netcom
shenzhen
phone: +86-0755-6983588

 yumei sun
sz-ipaddress@china-netcom.com
china netcom
shenzhen
phone: +86-0755-6983588

 SHENZHEN-CNC
Updated: 22-Dec-2003 by quoyb@china-netcom.com
Source: whois.apnic.net

- **Vložené slajdy Phishing**

Spyware

- **Software který:**
 - Sbírá osobní informace
 - Bez vědomí uživatele
- **Zaznamenávání kláves**
 - Keyloggery
- **Nespolehlivé**
 - Microsoft Watson
 - » Významná část havárií operačního systému je způsobena nějakým spyware

Boty a botnety

- **Ekosystém botů**
 - Bots
 - Botnets
 - Control channels
- **První masové rozšíření červem MyDoom.A**
 - MyDoom.A byl rozšířen po internetu
 - V napadených počítačích vytvořil zadní vrátka
 - Po 8 dnech útočníci skenovali počítače a hledali tato zadní vrátka
 - Nainstalovali Trojský kůň Mitglieder
 - Pak použily tyto stroje jako Boty
 - Využití pro přeposílání spamu

Příklad několika botnetů



Age (days)	Name	Server	MaxSize
02.00	nubela.net	dns.nubela.net	10725
10.94	winnt.bigmoney.biz (randex)	winnt.bigmoney.biz	2393
09.66	PS 7835 - y.eliteirc.co.uk	y.eliteirc.co.uk	2061
09.13	y.stefanjagger.co.uk (#y)	y.stefanjagger.co.uk	1832
03.10	ganjahaze.com	ganjahaze.com	1507
01.04	PS 8049 - 1.j00g0t0wn3d.net	1.j00g0t0wn3d.net	3689
10.93	pub.isonert.net	pub.isonert.net	537
08.07	irc.brokenirc.net	irc.brokenirc.net	649
01.02	PS 8048 - grabit.zapto.org	grabit.zapto.org	62
10.34	dark.naksha.net	dark.naksha.net	UNK
08.96	PS 7865 - lsd.25u.com	lsd.25u.com	UNK
UNK	PS ? - 69.64.38.221	69.64.38.221	UNK

(3 Sep 2004 snapshot)

Využití botnetů

- „Keystroke loggers“ pro získávání hesel a čísel kreditních karet
- Útoky DDOS (Distributed Denial of Service)
 - Proti významným serverům
- Přeposílání spamu: 70-80% veškerého spamu
 - Source SpecialHam.com, Spamforum.biz
- Warez
- Zásoba pro budoucí využití

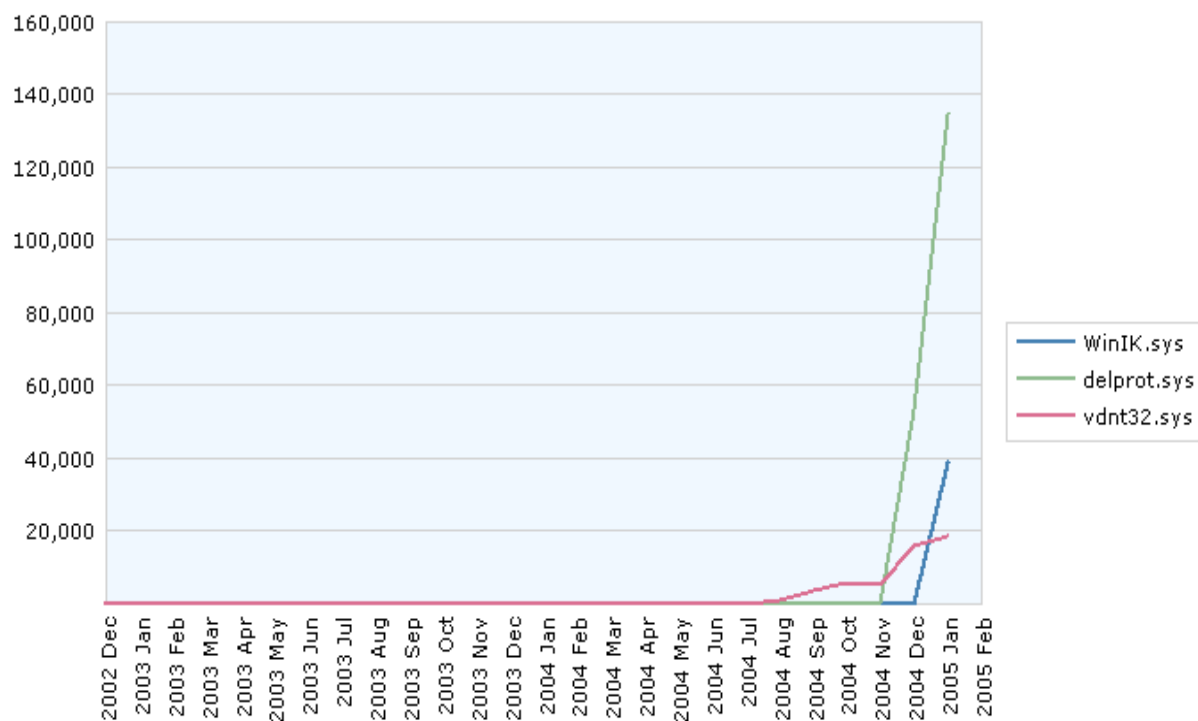
Likvidační potenciál botnetů

10,000-member botnet

Attack	Requests/bot	Botnet Total	Resource exhausted
Bandwidth flood (uplink)	186 kbps	1.86 Gbps	T1, T3, OC-3, OC-12
Bandwidth flood (downlink)	450 kbps	4.5 Gbps	T1, T3, OC-3, OC-12, OC-48 (2.488Gbps) 50% of Taiwan/US backbone
Syn flood	450 SYNs/sec	4.5M SYN/sec	4 Dedicated Cisco Guard (@\$90k) OR 20 tuned servers
Static http get (cached)	93/sec	929,000/sec	15 servers
Dynamic http get	93/sec	929,000/sec	310 servers
SSL handshake	10/sec	100,000/sec	167 servers

Rootkity

- Zvyšuje se rozšíření rootkitů
 - Neodhalitelné běžnými anti-spyware systémy
 - Podporují adware & spyware
 - DRM systémy



Rootkit

- **Rootkit je softwarový balík určený k tomu, aby vytvořil, utajil a spravoval prostředí pro útočníka na kompromitovaném stroji**
- **Binary rootkits**
 - Modifikace systémových souborů
- **Kernel rootkits**
 - Modifikace komponent kernelu
- **Library rootkits**
 - Přepisují systémové knihovny

Rootkit

- **Cíle**
 - **Správa přístupu útočníka**
 - » **Vytvoří zadní vrátka (backdoor) a udržuje je**
 - » **Poslouchá na portu a čeká na příkazy (UDP listener)**
 - » **Bez poslouchání na portu (sniffer) pro snížení možnosti odhalení**
 - **Správa lokálního přístupu**
 - » **Práva roota**
 - » **Ochrana před jinými rootkity**
 - **Lividace důkazů**
 - » **Skrývání**
 - **Zmodifikovaných souborů**
 - **Procesů útočníka**
 - **Používaných síťových připojení**
 - » **Úpravy logů**

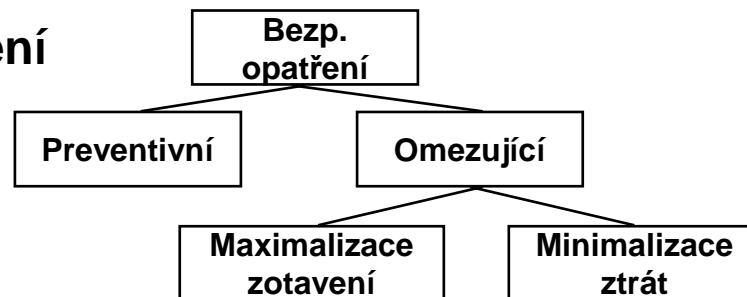
Bezpečnostní opatření

Co je bezpečnost?

- **Bezpečnostní cíle**
 - Proč?
- **Bezpečnostní funkce**
 - Jak?
- **Bezpečnostní mechanismy**
 - Co?
- **Důvěrnost**
- **Integrita**
- **Dostupnost**
- **...**
- **Desítky funkcí**
- **Neomezené množství mechanismů**

Bezpečnostní opatření

- **Cíle opatření**
 - bariéra mezi hrozbami a aktivy
 - omezují zranitelná místa
- **OMEZUJÍCÍ bezp. opatření**
 - minimalizují ztráty vzniklé útokem (odhalí nebo odvrátí útok)
 - maximalizují zotavení po útoku
- **PREVENTIVNÍ bezp. opatření**
 - snižují pravděpodobnost útoku
 - zvyšují pro útočníka náklady na útok (cena útoku je pro útočníka větší než jeho dosažitelný zisk):
 - » pravděpodobnost a vliv odhalení
 - » bezprostřední náklady na útok
 - » čas, potřebný k útoku



Omezení bezp. opatření

- **Periodicky musí být kontrolována**
 - efektivnost implementace bezp. opatření (odpovídají skutečná bezp. opatření plánovaným?)
 - relevantnost bezp. opatření (nezměnily se hrozby?)
 - potřeba dodatečných bezp. opatření
- **Omezujícím faktorem je CENA**
 - **Jednorázové náklady**
 - » Náklady na zakoupení HW nebo SW
 - » Náklady na vývoj SW a procedur
 - » Instalace
 - **Provozní náklady**
 - » Snížení výkonnosti systému (režie)
 - » Potřebné prostředky (např. spotřební materiál, lidská obsluha)
 - » Údržba bezp. opatření (sledování, kontrola, modifikace)
- **Principy ceny bezp. opatření**
 - Cena bezp. opatření musí být menší než předpokládaná ztráta, pokud by bezp. opatření nebylo instalováno
 - Bzp. opatření by mělo cenu útoku učinit vyšší, než je předpokládaný zisk útočníka.

Typy bezpečnostních opatření

- **Fyzická**
 - opatření, řídící fyzický kontakt osob s informačním systémem (budovy, ploty, zámky, stráže, ...)
- **Administrativní (procedurální)**
 - bezpečnostní procedury, prováděné lidmi (přihlašování, evidence přístupu, zálohování dat, ...)
- **Personální**
 - opatření, omezující hrozby od uživatelů (přijímání a propouštění zaměstnanců, osvěta a školení, ...)
- **Technická (Logická)**
 - HW a SW opatření, implementovaná v počítačové části informačního systému (identifikace, autentizace, řízení přístupu, protokolování, šifrování, ...)

I. Fyzická bezpečnostní opatření

- **Účel**
 - Fyzická bezp. opatření fyzickým způsobem omezují přístup ke komponentám informačního systému
 - zabraňují hrozbám pro fyzické komponenty systému
- **Typy**
 - Fyzická kontrola přístupu - zabraňuje osobám v přístupu k IS
 - » **Příklady implementace**
 - fyzické umístění - do méně přístupných míst
 - strážce a kurýři
 - zámky a elektronické zabezpečovací systémy (EZS)
 - dohlížecí systémy a detektory přítomnosti osob
 - trezory a schránky
 - Ochrana proti vnějším vlivům - opatření (prevence nebo zotavení) proti vnějším vlivům (přírodním nebo umělým, úmyslným nebo neúmyslným)
 - » **Příklady implementace**
 - prevence adetekce požáru - požární hlásiče, protipožární prostředky, budova
 - elektrická energie - filtry, UPS (Uninterruptible Power Supply), generátory
 - prostředí (teplota, vlhkost) - snímače teploty, vlhkosti, klimatizace
 - zátopa - umístění IS, budova, senzory
 - Jiná bezp. opatření
 - zálohování komunikačních médií
 - zálohy HW

II. Administrativní bezp. opatření

- **bezpečnostní procedury, prováděné lidmi**
- **zodpovědnost uživatelů**
 - přihlašování
 - evidence přístupu
 - osobní zodpovědnost zaměstnanců
 - oddělení pravomocí / zodpovědností
- **vstup / výstup**
 - kontrola vstupu a výstupu dat
- **dokumentační bezpečnost**
 - dokumentace
- **vývoj a aktualizace HW a SW**
 - správa změn
- **havárie**
 - zálohovací procedury
 - procedury zotavení po havárii
 - havarijní plány

III. Personální bezp. opatření

Lidé jsou nejdůležitější a nejméně spolehlivou částí informačního systému.

- **Personální bezp. opatření:**
 - mají za cíl snížit pravděpodobnost toho, že zaměstnanci se nebudou chovat v souladu s bezpečnostní politikou
 - jsou namířena přímo na osoby (nikoli prostřednictvím IS)
 - jsou převážně preventivní
 - jsou založena na
 - » důvěryhodnosti pracovníka
 - » spolehlivosti pracovníka

- **Přijímání zaměstnanců**

- **Definice pracovního místa**

Jednoznačná a stabilní definice prac. místa -> odvození potřebného přístupu k IS

- » **Oddělení pravomocí**

Takové rozdělení rolí a odpovědností, které zabrání tomu, aby jediný člověk mohl narušit (padělat, zničit) kritický proces (data)

- » **Nejmenší potřebná oprávnění**

Každý uživatel má mít pouze ta oprávnění, která nezbytně potřebuje k výkonu své funkce

- **Určení citlivosti pracovního místa**

Určení potřebného stupně prověření pracovníka, který má zastávat místo.

- » **Převážně armáda a státní správa (prověření pro práci s tajnými materiály, ..)**

- **Prověřování pracovníků**

- » **Zjištění důvěryhodnosti pracovníka**

- » **Implementace**

- zjištění historie pracovníka - informace od předchozích zaměstnavatelů
 - ověření důvěryhodnosti pracovníka externí organizací
 - periodické zjišťování důvěryhodnosti pracovníka

- **Správa zaměstnanců**
 - **Správa počítačových sezení zaměstnanců**
 - » vytváření sezení
 - » přidělování přístupových práv
 - » neodmítnutelnost zodpovědnosti zaměstnanců
 - **Přesuny zaměstnanců uvnitř organizace**
 - » dočasné změny přístupových práv
 - » odebírání přístupových práv
 - » !! možnost porušení oddělení pravomocí
 - **Audit**
 - » monitorování a protokolování aktivit uživatelů
 - **Detekce neautorizovaných nebo nelegálních aktivit**
- **Osvěta a školení**
 - **účel - zvýšení spolehlivosti zaměstnanců**
 - **zaměstnanci**
 - neumí používat bezpečnostní mechanismy
 - nevědí, že by měli používat bezpečnostní mechanismy
 - nechtějí používat bezpečnostní mechanismy
 - **oblasti**
 - » zvyšování informovanosti v oblasti bezpečnosti
 - » zvyšování obecně technického vzdělání

- **Propouštění zaměstnanců - přátelské ukončení práce**
 - měl by existovat standardní postup propuštění zaměstnance
 - **Možné problémy**
 - » odebrání všech přístupových práv (elektronických i neelektronických)
 - » odevzdání všech dokumentů
 - » odevzdání všech médií
 - » předání dat
 - » předání všech potřebných hesel, kryptografických klíčů a hardwarových autentizačních prostředků
 - » zajištění změny všech hesel a klíčů, které zaměstnanec zná
 - » zajištění důvěrnosti informací
- **Propouštění zaměstnanců - nepřátelské ukončení práce**
 - dtto jako v předchozím případě, ale navíc:
 - » nutnost velmi rychlého odebrání všech přístupových práv
 - » možnost následného zneužívání systému
 - » možnost “logických bomb” v systému
 - » Co je třeba v systému změnit? Které informace si zaměstnanec odnáší?

IV. Logická bezpečnostní opatření

- Jsou implementována v HW a SW informačního systému
- Zajišťují
 - Confidentiality - Důvěrnost
 - » Zabránění neautorizovaného odhalení informace
 - Integrity - Integritu
 - » Zabránění neautorizované modifikaci informace
 - Availability - Dostupnost
 - » Zajištění toho, že autorizovaným subjektům nemůže být bráněno v přístupu k informaci nebo k prostředkům systému
 - *Nepopiratelnost*
 - » *Zajištění toho, že uživatel se nemůže zbavit zodpovědnosti za akce, které provedl*

Bezpečnostní funkce

Bezpečnostní funkce

- **Důvěrnost**
 - prevence proti neautorizovanému odhalení informace
 - » *Řízení přístupu, Skryté kanály, Opětné použití*
- **Integrita**
 - prevence proti neautorizované modifikaci informace
 - » *Řízení přístupu, DVB, Fyzická integrita, Návrat, Oddělení rolí, Autonomní testování*
- **Dostupnost**
 - prevence proti neautorizovanému odmítnutí informace nebo zdrojů
 - » *Přidělování prostředků, Opravitelnost za provozu, Robustnost, Zotavení po chybě*
- **Účtovatelnost**
 - identifikace a monitorování důležitých událostí
 - » *Audit, Identifikace a autentizace, Důvěryhodný kanál*

Další bezpečnostní funkce

- **autentizace** **X** **anonymita & pseudonymita**
- **audit** **X** **nemožnost sledování**
- **anonymita**
 - možnost provést jisté akce tak, aby nebylo možno zjistit, kdo je provedl
 - mechanismus - anonymizační autorita, kryptografické protokoly
- **pseudonymita**
 - možnost provést akci pod pseudonymem
 - zachování všech ostatních bezpečnostních funkcí
 - mechanismus - pseudonymizační autorita, kryptografické protokoly
- **nemožnost sledování**
 - možnost provádět akce tak, aby nemohly být sledovány
 - kryptografické protokoly

důvěrnost

integrita

Řízení přístupu

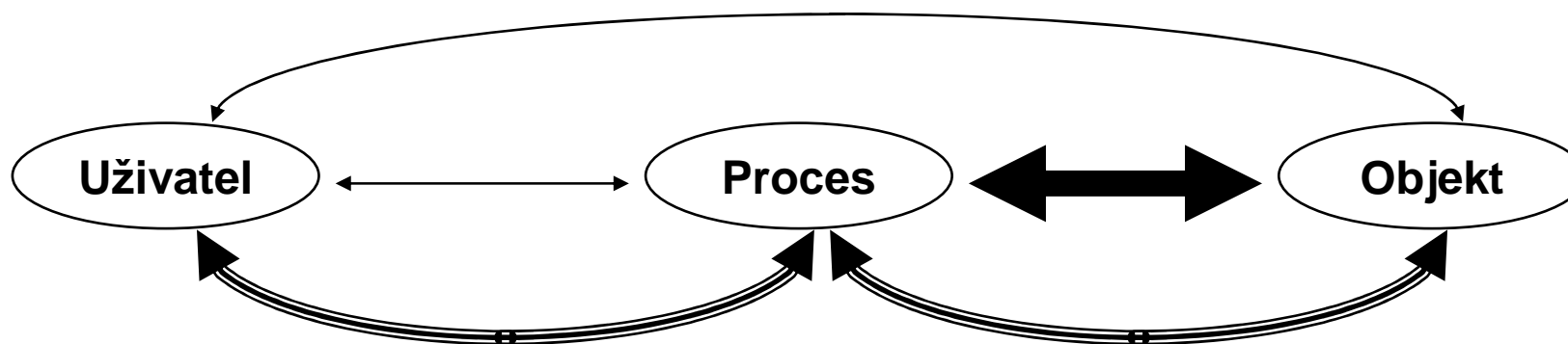





- **nepovinné řízení přístupu**
 - uživatel, proces a objekt dostávají identifikaci
 - přístupová práva k objektu může měnit běžný uživatel (vlastník) - UNIX
 - v rámci systému lze použít pouze jeden stupeň utajení
- **povinné řízení přístupu**
 - uživatel, proces a objekt mají bezpečnostní atributy <stupeň utajení, kategorie>
 - běžný uživatel nemůže měnit atributy a ani přístupová práva
 - atributy a přístupová práva
 - » administrativně určuje správce
 - » se nastavují automaticky tak, aby odpovídaly bezpečnostní politice (viz modely bezpečnosti)
 - lze použít více stupňů utajení

důvěrnost

integrita

Řízení přístupu

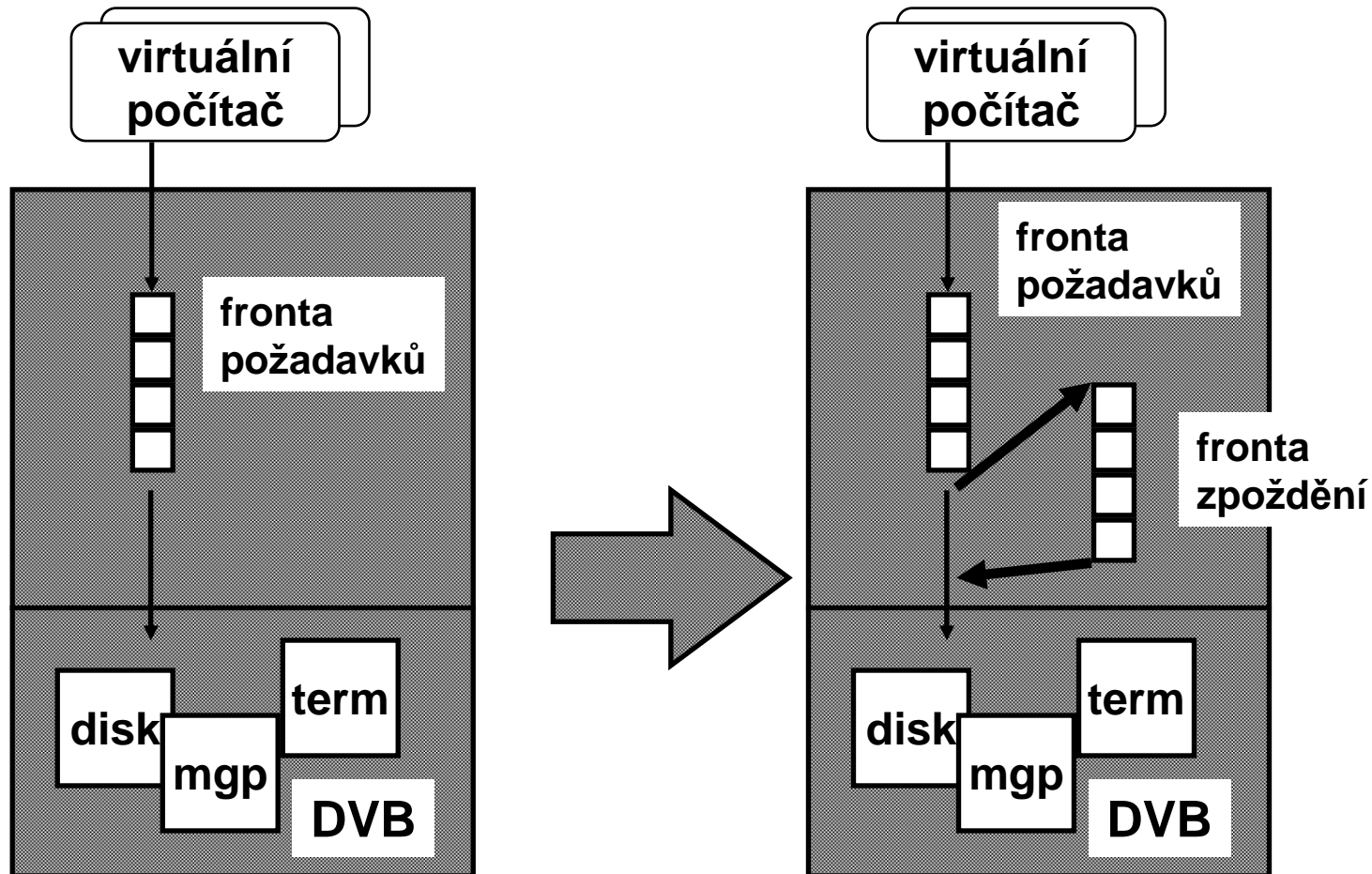


- **minimální** 
 - k některým objektům je možno přistupovat pouze pomocí privilegovaných procesů
- **základní** 
 - uživatel má práva k procesům a objektům (UNIX)
- **vyšší** 
 - přístup na základě kombinace uživatel/proces/objekt (seznam přístupových práv)

Skryté kanály

- **předávání informace v rozporu s bezpečnostní politikou**
- **šířka pásma skrytého kanálu**
- **paměťové skryté kanály**
 - existence / neexistence souboru
 - atributy souboru
 - délka souboru
 - stav sdílených prostředků (V/V zařízení)
 - NIKOLI obsah souboru - v tom zabrání
- **časové skryté kanály**
 - zatížení procesoru
 - zatížení V/V zařízení
- **kombinované**
 - směr pohybu diskové hlavy...

Skryté kanály (pokr.)



- odstranění časového skrytého kanálu

Opětné použití objektů

- **objekt přidělený procesu**
 - nesmí obsahovat žádné informace od předchozího vlastníka
 - nesmí mít žádné autorizace zbylé od předchozího vlastníka
- **mechanismy**
 - fyzické zničení objektu
 - mazání obsahu objektu
 - šifrování obsahu objektu
- **hrozby**
 - sbírání smetí (scavenging)

- **princip DVB (Důvěryhodná Výpočetní Báze) zajišťuje schopnost systému**
 - chránit sám sebe
 - spravovat chráněné objekty
- **ochrana DVB**
 - DVB je schopna chránit sama sebe před vnějšími vlivy a fyzickým útokem
- **nemožnost obejít DVB**
 - veškerý přístup k chráněným objektům musí být prováděn přes DVB

Fyzická integrita

- **evidence fyzického útoku**
 - ochranné nálepky, pečetě, světlocitlivá barva
- **odezva na fyzický útok**
 - zničení objektu při útoku X upozornění na útok
- **odolnost proti fyzickému útoku**
 - útok je velmi obtížný až nemožný
- **Tamper resistance**

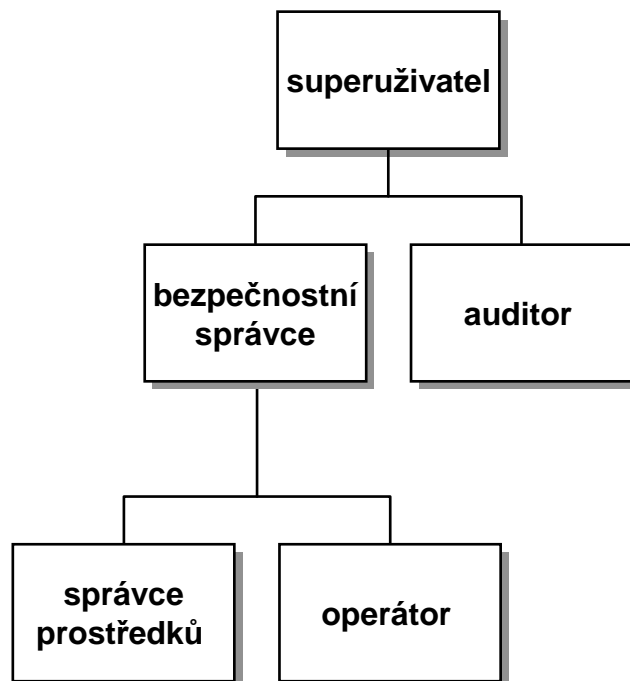
Návrat (zálohování)

- **schopnost vrátit se k předchozímu stavu**
 - po chybě uživatele
 - po fyzickém útoku
 - po zničení dat (poruchou, požárem...)
- **metody**
 - transakce
 - zálohování dat na nezávislá média
 - » fyzické uložení záložních médií
 - » interval zálohování
 - » počet záložních kopií

Oddělení rolí

- **definice různých rolí pro různé funkce**
- **1 - základní oddělení rolí**
 - správce X uživatel (viz UNIX)
- **2 - oddělení rolí správců**
 - více rolí správců (sezení, audit, péče o programy...)
- **3 - oddělení rolí uživatelů**
 - více rolí uživatelů (ne pouze skupiny)

Oddělení rolí (AIX)



- **superuživatel**
 - konfiguruje systém
 - vlastní většinu souborů
- **bezp. správce**
 - stará se o prosazení bezp. politiky
- **správce prostředků**
 - dělá běžnou práci správce systému
- **operátor**
 - rutinní práce (archivace, údržba)
- **auditor**
 - analýza auditních dat
 - detekce narušení bezp. politiky

Autonomní testování

- **system je schopen ověřit, že se nachází v bezpečném a správném stavu**
 - testování funkce hardware
 - testování integrity software (kontrolní součty, kryptografické testy integrity)
 - » úmyslné změny software a konfigurace - viry, trojské koně
- **1 - manuální autonomní testování**
 - vyžaduje zásah člověka
- **2 - autonomní testování při inicializaci**
- **3 - autonomní testování během činnosti**

Přidělování prostředků

- **kontrola množství prostředků a služeb přidělovaných procesům a uživatelům**
 - » prostor na disku
 - » čas procesoru
 - » doba relace
 - » počet tiskových stran
- **0**
- **1 - kvóty**
 - uživatelům jsou přiřazeny kvóty čerpání prostředků
- **2 - opatření proti neposkytnutí služby**
 - žádný uživatel nemůže vyčerpat prostředky systému (viz 1)
- **3 - prioritní přidělování**
 - uživatelům nebo skupinám lze přiřadit priority přidělování prostředků

Opravitelnost za provozu

- **system je opravitelný za provozu, pokud dovoluje výměnu některých komponent při nepřerušném poskytování služeb**
- **0**
- **1 - omezená opravitelnost**
 - některé komponenty lze vyměnit za provozu
- **2 - plná opravitelnost**
 - všechny komponenty lze vyměnit za provozu

Robustnost

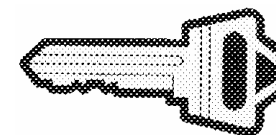
- schopnost systému poskytovat služby i při poruše některých komponent
- 0
- 1 - odlonost proti poruchám některých komponent
- 2 - omezená funkčnost
 - odolný proti poruchám všech komponent s omezenými službami
- 3 - plná funkčnost
 - odolný proti poruchám všech komponent bez omezení služeb

Zotavení po chybě

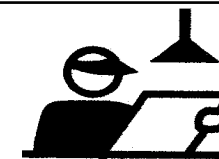
- **system je schopen se po chybě vrátit zpět do bezpečného stavu**
- **0**
- **1 - manuální zotavení po chybě**
 - požaduje zásah správce
- **2 - automatické zotavení po chybě**
 - nepožaduje zásah

Identifikace a autentizace

- **Identifikace** - zjištění totožnosti uživatele
- **Autentizace** - ověření totožnosti uživatele na základě to, že uživatel:
 - něco zná
 - » heslo, PIN
 - něco vlastní
 - » klíč, magnetická karta, smart karta, autentizační kalkulátor
 - někým je
 - » antropometrická autentizace
 - » hlas, otisk prstu, vzorek sítnice, tvar dlaně
- **slabá X silná autentizace (kryptografická)**
- **jednosměrná X obousměrná autentizace**

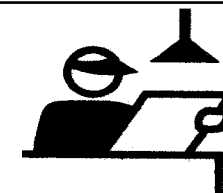


Audit



Provádí rozpoznávání, záznam a možnost analýzy událostí významných pro bezpečnost.

- **ochrana auditních dat**
 - » bezpečnostní správce
- **fyzické uložení auditních dat**
 - » diskový prostor !!
- **granularita auditních dat**
 - » podrobnost dat X objem dat
- **analýza auditních dat**
 - » podpůrné prostředky, UI
- **detekce a poplach**
 - » okamžitá odezva systému na události
- **IDS**

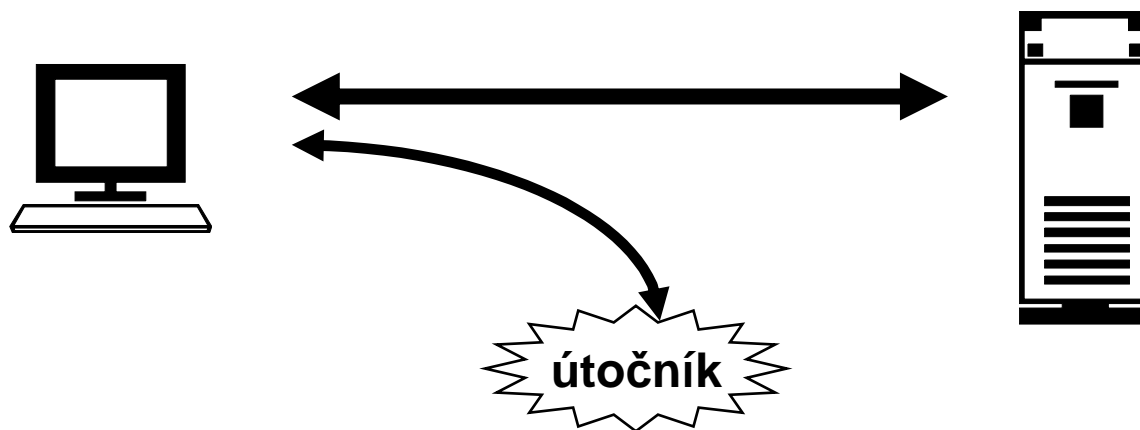


- 0
- 1 - externí audit
 - systém je schopen předávat auditní informace jinému systému
- 2 - Audit
 - lokální úschova auditních informací
 - auditní informace musí být chráněny
- 3 - Audit s poplachem
 - upozornění správce na události, které nejsou v souladu s bezpečnostní politikou
- 4 - Detekce útoku
 - průběžná analýza auditních záznamů a detekce pokusů o narušení bezpečnosti systému

Důvěryhodný kanál

Zaručené propojení mezi uživatelem a DVB

- 0
- 1 - autentizační důvěryhodný kanál
 - uživatel je schopen inicializovat důvěryhodný kanál pro účely identifikace a autentizace
- 2 - úplný důvěryhodný kanál
 - uživatel nebo DVB je schopen podle potřeby inicializovat důvěryhodný kanál kdykoli během relace



Přenos dat

Bezpečnostní služby ISO 7498-2

- **Autentizace**
 - Autentizace spojení
 - Autentizace odesílatele
- **Řízení přístupu**
- **Důvěrnost**
 - Důvěrnost spojení
 - Důvěrnost přenosu zpráv
 - Důvěrnost toku dat
- **Integrita**
 - Integrita spojení s opravou,
 - Integrita spojení bez opravy
 - Integrita přenosu zpráv
- **Nepopiratelnost**
 - Nepopiratelnost odesílatele
 - Nepopiratelnost doručení

Autentizace

- **Jednoznačné ověření totožnosti**
- **Autentizace spojení (Entity authentication)**
 - Předpokládá službu se spojením
 - Ověření prohlašované identity v konkrétním okamžiku
 - Typicky při navázání spojení
 - Chrání před vydáváním se za jiného uživatele a útokem replay
- **Autentizace odesílatele**
 - Předpokládá zasílání zpráv (bez spojení)
 - Ověřuje identitu zdroje dat
 - Nechrání před útokem replay

Důvěrnost

- **Ochrana proti neoprávněnému prozrazení informace**
- **Důvěrnost spojení**
 - Předpokládá službu se spojením
- **Důvěrnost přenosu zpráv**
 - Předpokládá zasílání zpráv (bez spojení)
- **Důvěrnost toku dat**
 - Proti útokům, kdy se útočník nesnaží dešifrovat přenášené zprávy ale sbírá informace o těchto zprávách (časy, délky, adresy...)

Integrita

- **Ochrana proti neodhalené neoprávněné modifikaci informace**
- **Integrita spojení s opravou**
 - Nepoužívá se
- **Integrita spojení bez opravy**
 - Předpokládá službu se spojením
- **Integrita přenosu zpráv**
 - Předpokládá zasílání zpráv (bez spojení)
 - Nechrání před útokem replay

Nepopiratelnost

- **Ochrana proti popření autorství, obsahu a zaslání nebo přijetí zprávy**
- **Nepopiratelnost odesílatele**
 - Ochrana proti popření autorství, obsahu a zaslání zprávy
- **Nepopiratelnost doručení**
 - Ochrana proti popření přijetí zprávy