
INTERSYSTEMS

SYMPOSIUM 2005

Zabezpečte si své
aplikace



Tomáš Vaverka
Support Advisor

Vítejte



- Tato přednáška uvede „ Vyspělou bezpečnost Caché 5.1“ a ukáže možnosti jak zahrnout prvky nového bezpečnostního modelu databáze Caché do Vašich současných aplikací.
- Obsahuje: **základy bezpečnostního modelu, zdroje, privilegia a role, autentizace, audit a šifrování.** Zaměření na specifické typy aplikací.
- Další podrobnosti v přednášce **Vyspělá bezpečnost a databáze Caché.**

Bezpečnost - cíle



Cíle

- Nabídnout nejpokrokovější bezpečnost ze všech hlavních databází
- Umožnit vývojářům snadno zabudovat bezpečnostní prvky do aplikací.
- Minimalizovat výkonnostní a provozní zátěž
- Získat bezpečnostní certifikaci

Bezpečnostní “oblasti”



Přímo v aplikaci Caché

Uvnitř Caché

Vně Caché

Aplikace

Caché

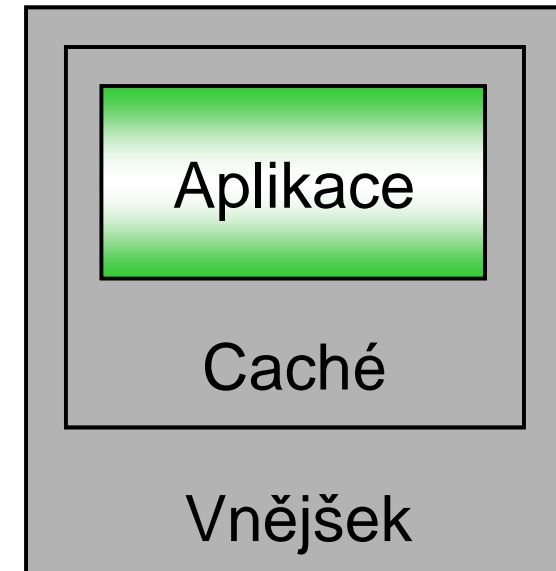
Vnější

Začneme zevnitř...

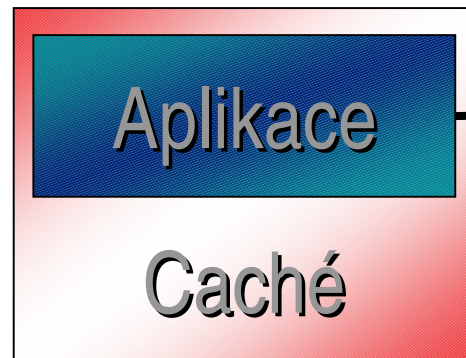


Přímo v aplikaci

- Zaručí, že pouze autorizovaný uživatel může používat aplikaci.
- Zaručuje uživatelům, že mohou používat tu část aplikace, ke které mají oprávnění



Cíle bezpečnosti



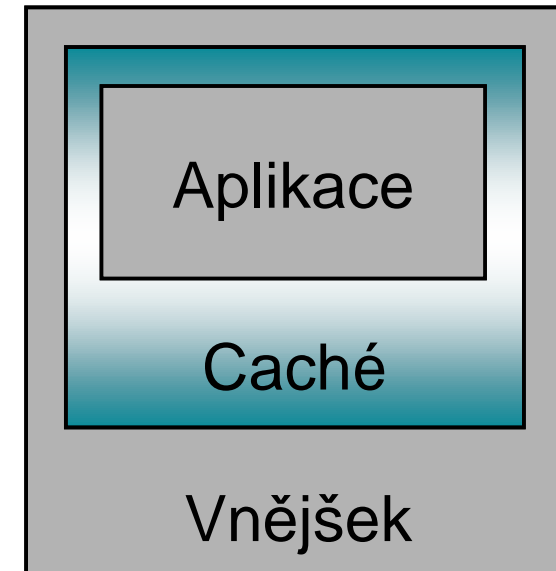
Umožnit aplikačním vývojářům snadno zabudovat bezpečnostní prvky do svých aplikací a uplatnit bezpečnost na úrovni aplikace

Pokročíme ven...



Uvnitř Caché

- Zaručí, že pouze **autorizovaný** uživatel může použít Caché.
- Rídí, co může uživatel delat mimo rozsah aplikace.



Cíle bezpečnosti



Caché

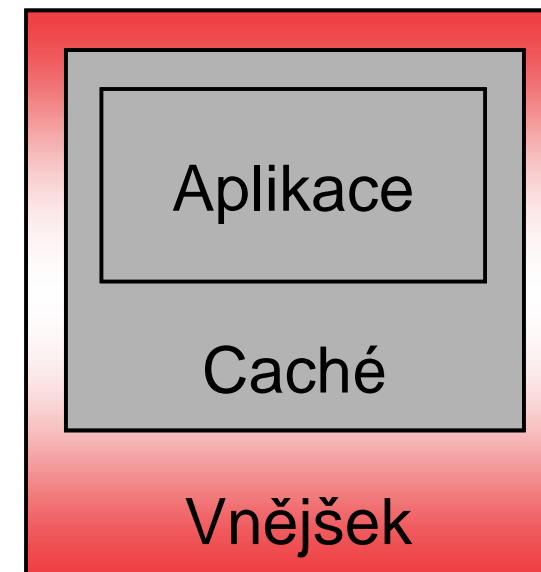
Chránit zdroje a způsobilost
Caché

Vnější hrozby...



Vně Caché

- Bezpečnost vně Caché je většinou působiště programu mimo Caché (t.j. operačního systému, sítě atd.).
- Caché musí umět spolupracovat s těmito vrstvami (nebo jim alespoň nesmí bránit) .



Cíle bezpečnosti



Zajistit, aby Caché efektivně spolupracovala s „vnějšími“ bezpečnostními technologiemi

Pět pilířů bezpečného systému



- **Autentizace** zajišťuje ověření identity všech uživatelů.
- **Autorizace** zajistí, že uživatelé mají přístup jen a pouze k těm zdrojům, které potřebují.
- **Audit** udržuje záznamy - buď předdefinované systémem nebo speciální události aplikace.
- **Ochrana integrity dat** zabraňuje útokům na data přenášená po síti.
- **Ochrana důvěrnosti dat**, aby např. žádný spyware nemohl získat užitečná data.

INTERSYSTEMS

SYMPOSIUM 2005

Autentizace



Autentizace: Určení totožnosti



- Vyspělá bezpečnost Caché nabízí několik mechanismů k ověření totožnosti:
 - **Kerberos**: Nejbezpečnější cesta autentizace. Dostupná na všech platformách.
 - **Operační systém**: Dostupný pro Windows, UNIX a OpenVMS, autentizace založená na OS používá identifikaci uživatele v operačním systému pro identifikaci uživatele v Caché.
 - **Caché Login**: Caché si udržuje tabulku kódovaných hodnot hesla pro každý uživatelský účet.
 - **Bez ověření**

Kerberós



Kerberós, dle řecké mytologie pes hlídající podsvětí; syn stohlavého obra Tyfóna a položeny-polohada Echidny. Kerberós měl tři hlavy, hady ovinuté kolem šije a ocas končící dračí hlavou. Bdělý strážce podsvětní Hádovy říše; pouze jediný Héraklés vyvedl Kerbera na světlo dne, když ho z příkazu krále Eurysthea přivedl do Mykén.



Kerberos



- Kerberos je **síťový autentizační protokol**, který zabezpečuje bezpečné ověření pro aplikace klient-server s využitím secret-key kryptografie tajného klíče.
- Kerberos byl vytvořen na **MIT** (Massachusetts Institute of Technology- Cambridge).
- Hesla nejsou **nikdy** posílána po síti.
- Dostupný na **všech** platformách podporovaných databázích Caché.
- Přizpůsobený **nestejnorodým** sítím.
- Rychlý **a** snadno přizpůsobitelný.

Kerberos – základy na příkladu



Princip

- Muže být lidský “Uživatel”.
- A/NEBO logicky napojený “klientský” počítač či pracovní stanice...
- ...sloužící jako spojnice mezi uživatelem a KDC nebo SLUŽBOU.
- Uživatel si není vůbec vedom autentizačního procesu.



Authorizovaný uživatel



Pracovní stanice

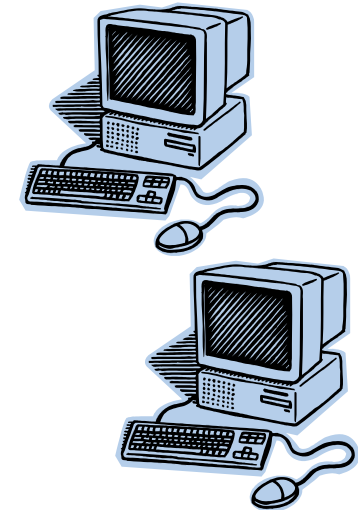
Služby (service) na síti



Principy služby

- Mnoho služeb je poskytováno sítí:
 - Soubory
 - Pošta
 - Tisky
 - atd.
- Caché 5.1 je nyní SÍTOVÁ služba!
- Aby bylo možno použít SLUŽBU, uživatel musí mít vstupenku (ticket) k dané službě od KDC.

síťová SLUŽBA
(napr. servery Caché)



Obdržení vstupenky



Key Distribution Center (KDC)

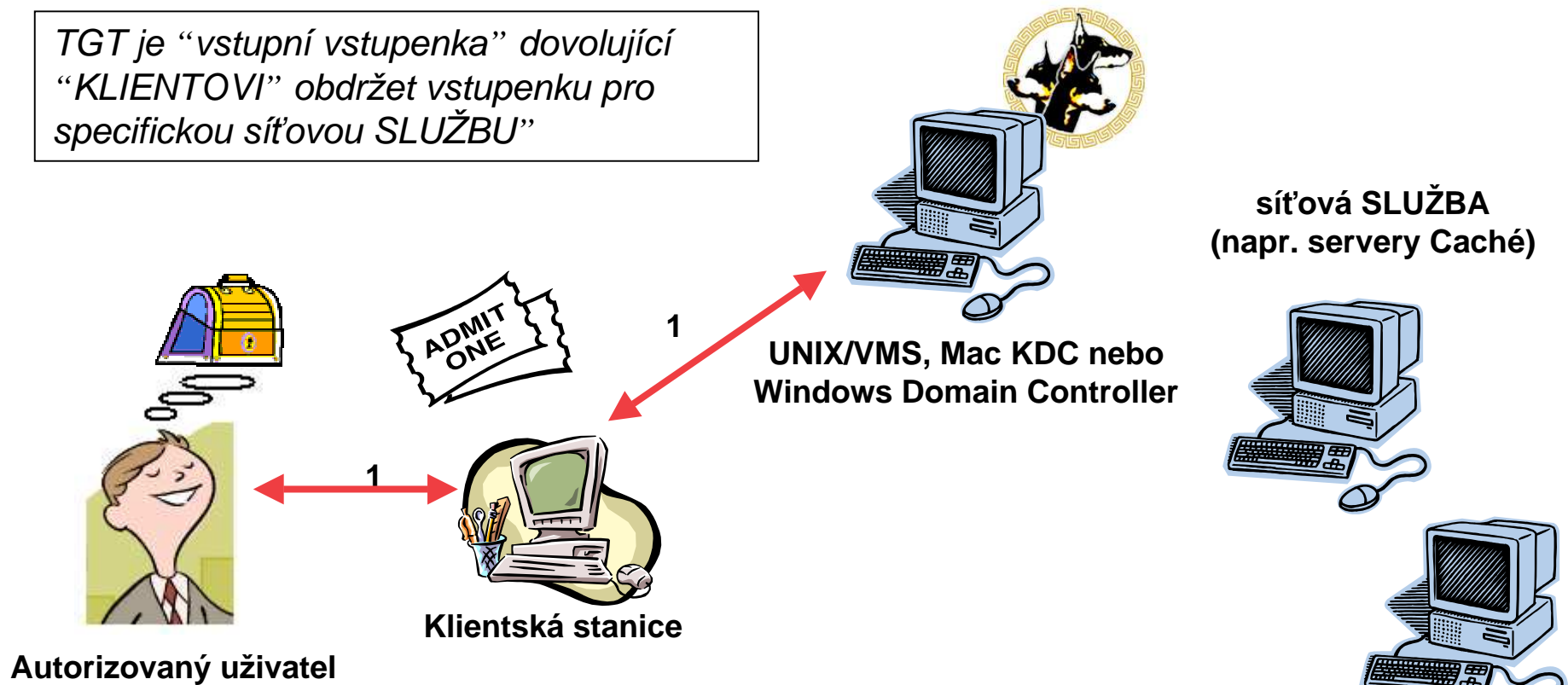
- Spravuje jednu nebo více oblastí - Kerberos Security Realms.
- Dostupný pro UNIX, VMS, Mac OS X a Linux.
- Obsaženo jako část Windows Active Directory Domain Controller.
- Udržuje bezpečnostní databázi Kerberos.
- Prideluje vstupenky pro přístup (Ticket Granting Tickets - TGT) a vstupenky pro služby (Service Tickets).



UNIX/VMS KDC nebo
Windows Domain Controller

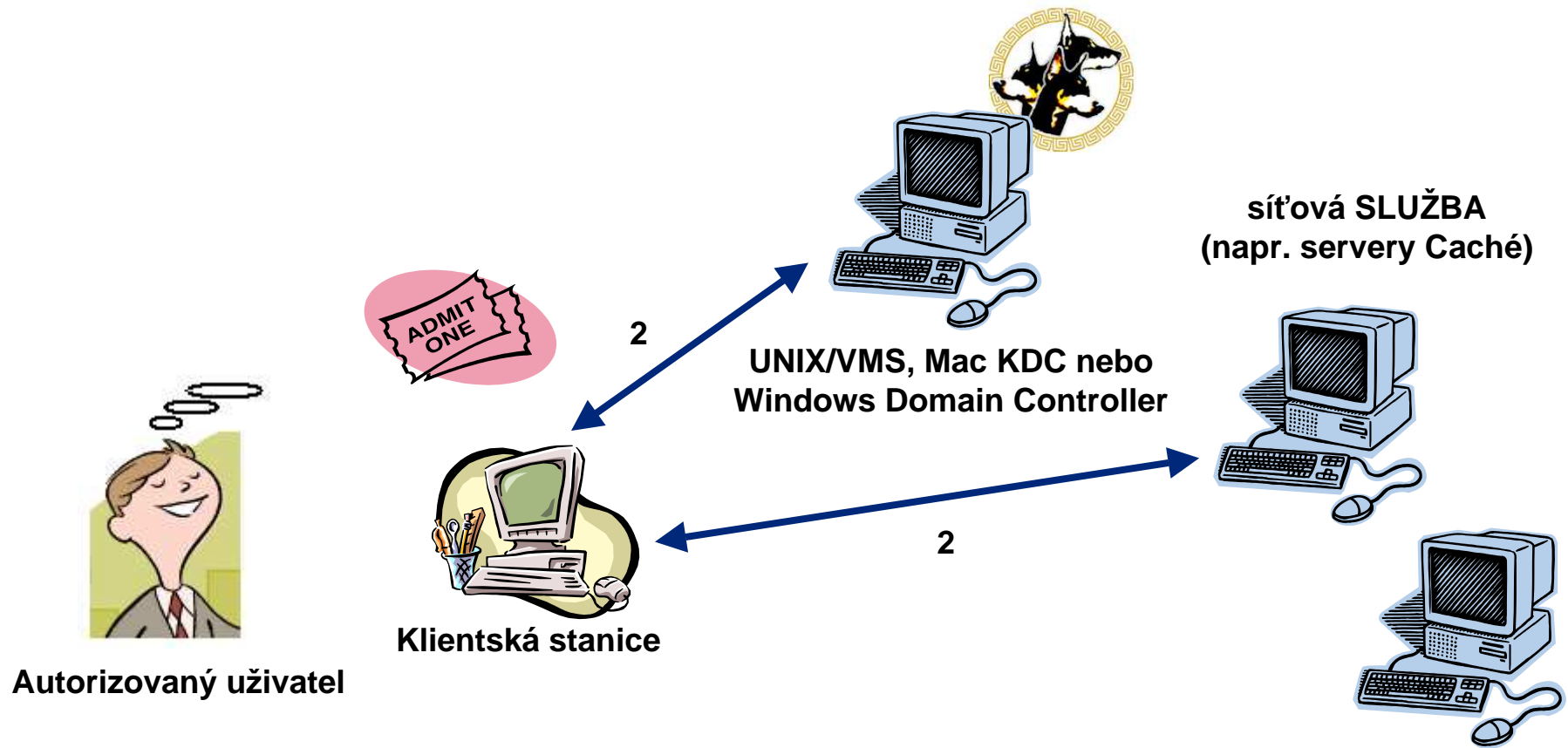
Kerberos v akci – příklad

TGT je “vstupní vstupenka” dovolující “KLIENTOVI” obdržet vstupenku pro specifickou síťovou SLUŽBU



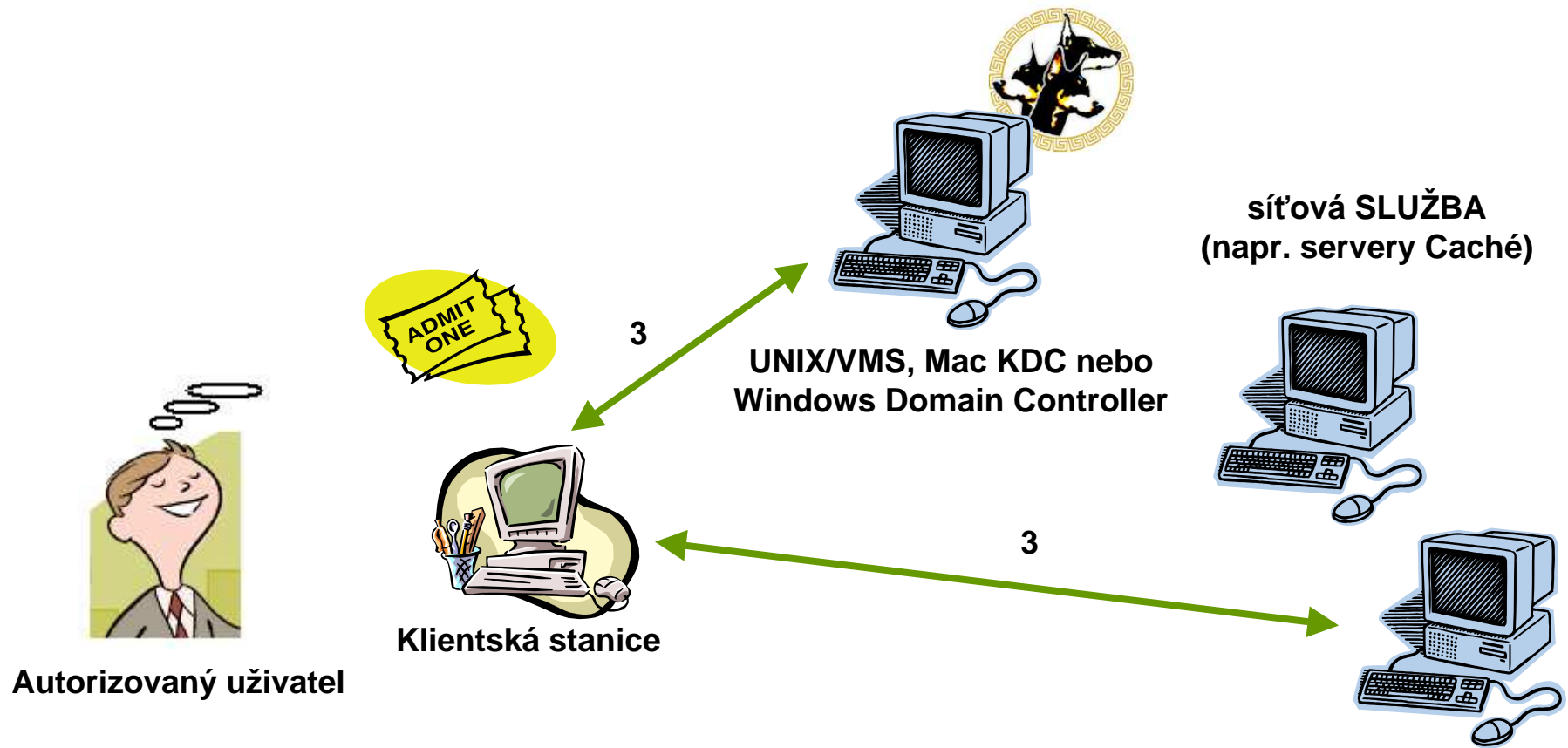
1: Prihlášení do systému (obdržení TGT z KDC)

Kerberos v akci – pokrač. příkladu



2. Počáteční připojení k serveru:
(obdržení vstupenky pro službu z KDC)

Kerberos v akci – pokrač. příkladu



3. Počáteční připojení k serveru:
(obdržení vstupenky pro službu z KDC)

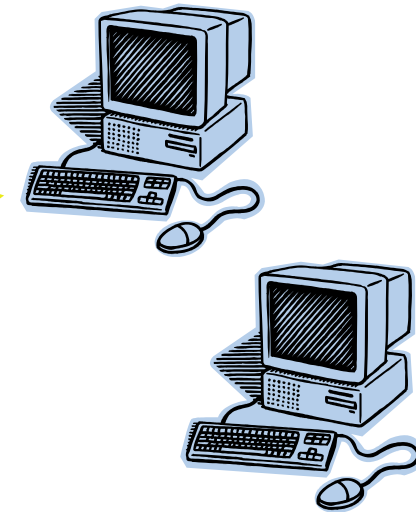
Kerberos v akci – pokrač. příkladu



UNIX/VMS, Mac KDC nebo
Windows Domain Controller



síťová SLUŽBA
(napr. servery Caché)



Autorizovaný uživatel



Klientská stanice

4



4. Následné připojení k serveru:
(obdržení vstupenky pro službu z KDC)

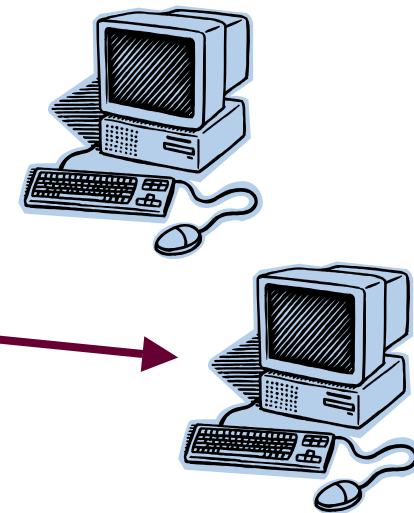
Kerberos v akci – pokrač. příkladu



UNIX/VMS, Mac KDC nebo
Windows Domain Controller



síťová SLUŽBA
(napr. servery Caché)



Autorizovaný uživatel



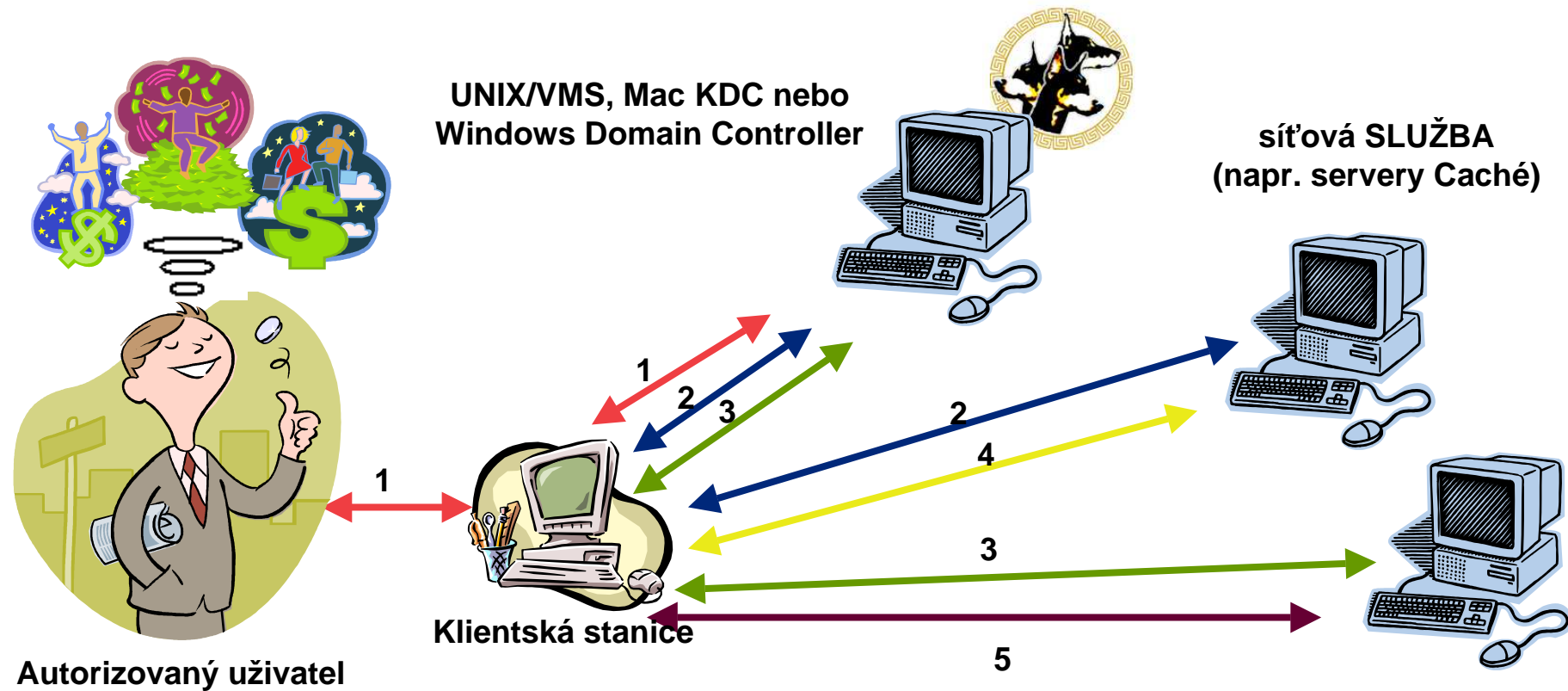
Klientská stanice

5



5. Následné připojení k serveru:
(obdržení vstupenky pro službu z KDC)

Co se děje za scénou...



1: Prihlášení k systému.

2, 3: Počáteční připojení k serveru (uživatel se na chvíli zasní).

4, 5: Následná připojení k serveru.

Musím měnit svou aplikaci Caché pokud chci přidat Kerberos?



- Administrátor sítí musí vytvořit infrastrukturu pro Kerberos, ale po vývojáři nevyžaduje žádnou změnu v kódu aplikace – bezpečnost je řízena uvnitř kódu pro připojení a není viditelná pro aplikaci.
- Odděleno od povolení k použití zdrojů uvnitř Caché (autorizaci).

Kde mohu získat více informací?



Dokumentace Cache 5.1 přináší hlubší informace o bezpečnosti založené na protokolu Kerberos.

Rozličné zdroje na Internetu:

- Základní zdroj informací o protokolu Kerberos:
(<http://web.mit.edu/kerberos/www/dialogue.html>)
- “The Moron’s Guide to Kerberos”
(<http://www.isi.edu/gost/brian/security/kerberos.html>)

Kdy má uživatel ověřený přístup do Caché?



- Uživatel je autentizován do Caché:
 - pro aplikace připojené pomocí ODBC, JDBC, Caché Direct, Caché Objects, Java nebo Call-In, když aplikace volá příslušnou funkci pro spojení.
 - pro uživatele připojené pomocí terminálu či konzoly PC, když Caché vyzve k zadání uživatelského jména a hesla.
 - při použití autentizace pomocí operačního systému, pokud identita uživatele na úrovni operačního systému se shoduje s uživatelským jménem zadaným v Caché.
 - pro nástroje Caché, když je vytvořeno připojení na server Caché.

Vyspělá bezpečnost pro ODBC

- Přidává volbu **Caché Advanced Security** do ovladače ODBC.
- Autentizace je konfigurovatelná **jednotlivě** pro každé DSN.
- Umožňuje buď zvolit metodu **Caché Login** nebo **Kerberos**

The screenshot shows the 'InterSystems Caché ODBC Data Source Setup' dialog box. It is divided into several sections:

- Data Source:** Name: CACHE Samples, Description: Cache Configuration and Namespace.
- Connection:** Host (IP Address): 127.0.0.1, Port: 1972, Caché Namespace: SAMPLES.
- Authentication Method:** Password (selected), Kerberos. Connection Security Level: Clear (selected), Integrity. Server Type: Window (selected), Unig, VMS. Service Principal Name: cacheNELSON-VMWARE.
- Misc:** ODBC Log, Static Cursors, Disable Query Timeout, Use Locale Decimal Symbol, Unicode SQL types.

Buttons: OK, Cancel, Test Connection, Ping, Help.

INTERSYSTEMS

SYMPOSIUM 2005

Autorizace





Autorizace určuje, **co je Vám dovoleno** dělat!

- **Aktivum (asset)** je cokoliv, co chceme chránit:
 - databáze Caché je aktivum.
 - schopnost se připojit do Caché pomocí SQL je aktivum
 - způsobilost spustit zálohování je aktivum.
- **Aktiva** jsou zabezpečena pomocí **zdrojů (resources)**.
- **Oprávnění (privilege)** dává **povolení (permission)** něco dělat s jedním nebo více **aktivy chráněnými** pomocí **zdroje**:
 - např. být schopen **číst** databázi zákazníků
 - nebo **spustit** zálohování

Uživatelé, role a aplikace



Uživatelé

Oprávnění mohou být přidělená přímo uživatelům

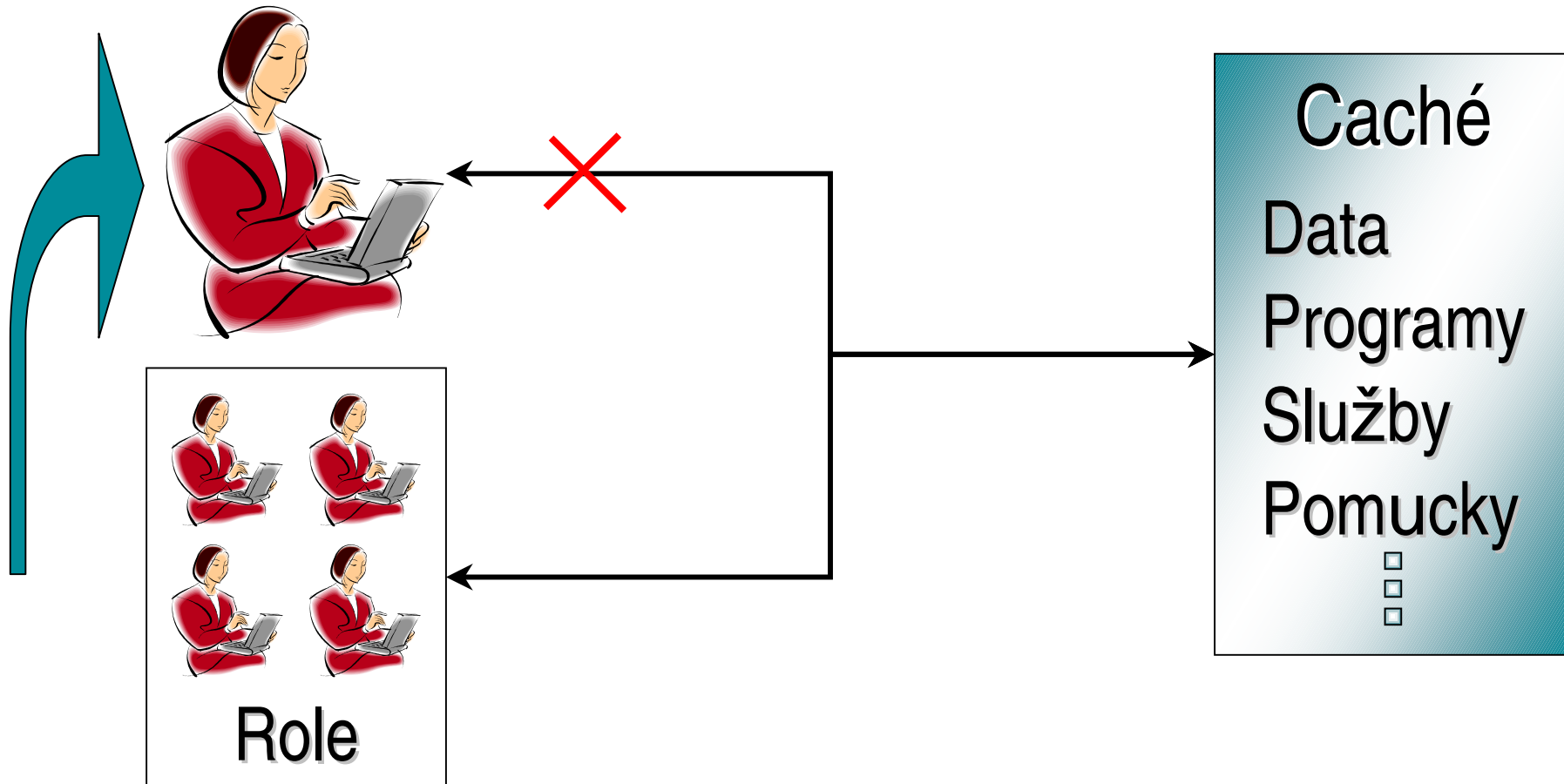
Role

Oprávnění mohou být přidělená rolím a role jednotlivým uživatelům

Aplikace

Oprávnění mohou být přidělená aplikacím a uživatelé mohou být oprávněni spouštět tyto aplikace

Uživatelé a role



INTERSYSTEMS

SYMPOSIUM 2005

System Management Portal



System Management Portal



- Nové rozhraní **založené na webovém prohlížeči**.
- Umožňuje **vzdálenou správu** systémů přes internet **bez** nutnosti instalace klientské části.
- Dostupné nyní i na **jiných** platformách než Windows
- **Minimalizuje** problémy s kompatibilitou mezi verzemi/platformami.
- Toto nové rozhraní **konsoliduje** funkčnost obsluhovanou dříve pomocí nástrojů:
 - Explorer, SQL Manager, Configuration Manager a Control Panel.

INTERSYSTEMS

SYMPOSIUM 2005

Bezpečnostní poradce



Bezpečnostní poradce



- Navržen, aby pomohl systémovým správcům při zabezpečení systému Caché.
- Je to webová stránka portálu, znázorňující současné informace zaměřené na nastavení bezpečnosti systému.
- Doporučené změny nebo oblasti k prozkoumání.
- Odkazy na ostatní stránky k provedení doporučených změn.

INTERSYSTEMS

SYMPOSIUM 2005

Audit



Audit



- Záznam klíčových událostí do bezpečného auditovacího logu je třetím hlavním prvkem Vyspělé bezpečnosti Caché.
- Caché má zabudovanou podporu auditování pro:
 - **události na úrovni systému** (*jako je start Caché a uživatelské přihlášení*).
 - **události na úrovni bezpečnosti** (*jako jsou změny v bezpečnosti nebo nastavení auditu*).
 - **uživatelsky definované události**.
- Aplikace může generovat své vlastní vstupy do auditovacího logu.

Co Caché neaudituje



- Caché automaticky negeneruje záznamy pro:
 - normální aktivitu v databázi.
 - aplikace to může dělat snadno pomocí metod objektů nebo pomocí SQL (triggers).
- Databázová aktivita, jako jsou všechny přístupy, nové záznamy, změny nebo mazání dat by generovalo tak mnoho vstupů do auditu, že by to bylo neúčelné až kontra-produktivní
- Mnohem účinnější je nechat aplikaci vytvořit jednotlivý záznam do auditu než generovat tisíce záznamů nastavením databáze!
- Více v přednášce „Vyspělá bezpečnost Caché“

INTERSYSTEMS

SYMPOSIUM 2005

Šifrování databází



Ochrana dat... Proč?



- Existuje mnoho typů dat **vyžadujících** ochranu před neautorizovaným přístupem nebo modifikací:
 - Finanční a lékařské záznamy, patentované a konkurenční informace firem, vládní a armádní bezpečnostní data.
- Je zde rovněž **mnoho** možných **ohrožení** pro tato data:
 - organizovaný zločin, vládní organizace, terorismus, konkurence, mediální agentury, nepoctiví zaměstnanci, příležitostní hackeři.
- **Zákony**, např. Zákon na ochranu osobnosti, **určují** specifickou **ochranu** pro určitá data.

Ochrana dat v Caché 5.1

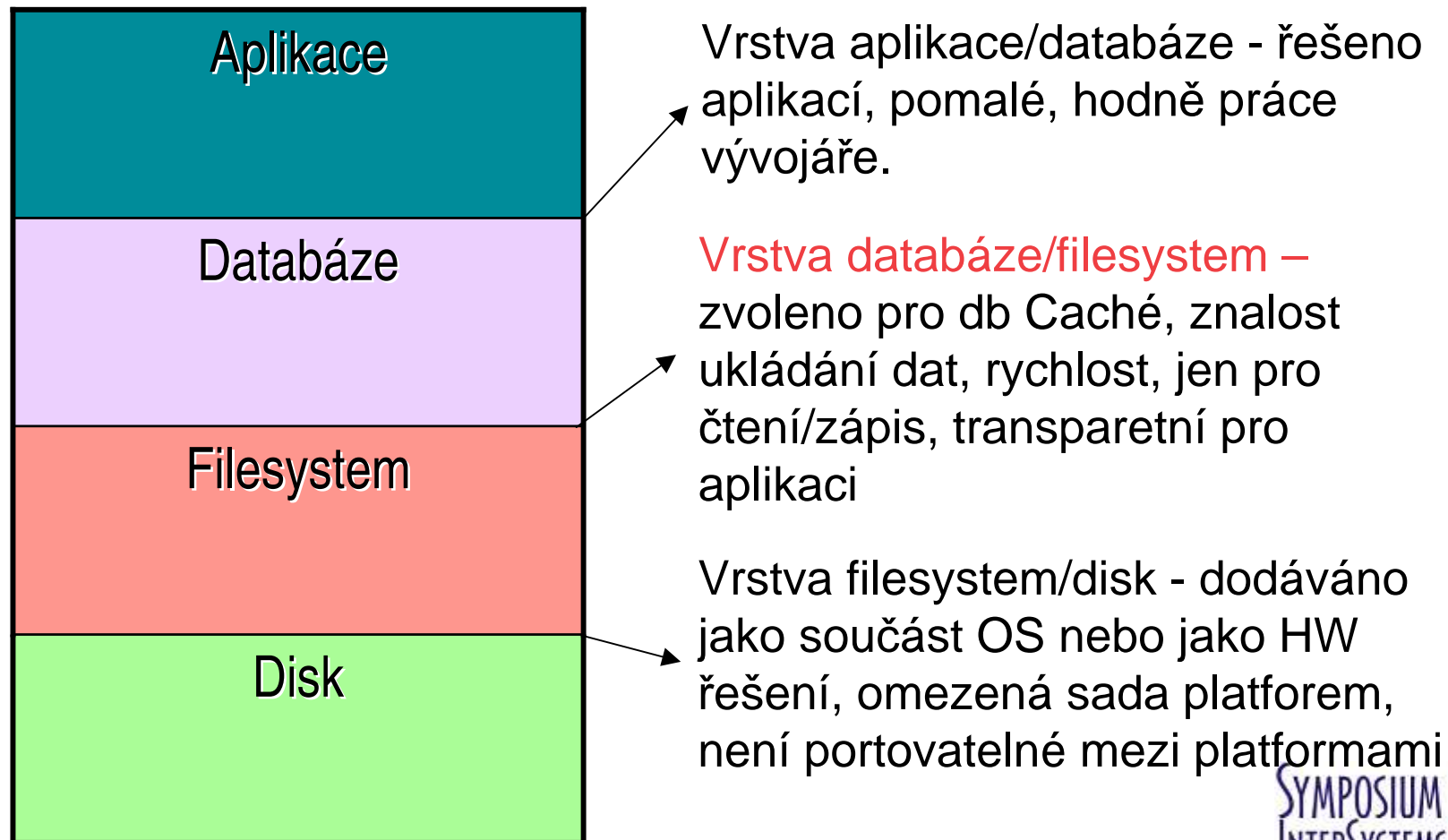


- Data lze nalézt a chránit ve třech základních stavech:
 - **Data používaná:** Caché používá autentizační mechanismus protokolu Kerberos k řízení přístupu k datům v paměti (*jako doplněk k ochraně používané operačním systémem*).
 - **Data v pohybu:** Caché používá Kerberos k zabezpečení integrity dat a utajení služeb při přenosu na síti.
 - **Data v klidu:** Caché umožňuje šifrování databáze na úrovni bloků k ochraně dat uložených na citlivých médiích jako jsou disky nebo pásky.

Data v klidu - možnosti...



Šifrování je možno implementovat na kterékoliv úrovni:



Cíle návrhu – ochrana dat v klidu



- Dva rozhodující požadavky pro **efektivní** a **užitečné** řešení šifrování dat:
 - Zabezpečit **silnou** bezpečnost podle **standardů** moderní kryptografie
 - Řešení **nesmí** mít podstatný **vliv** na **výkon databáze** (propustnost dat a zpoždění při čtení a zápisu).
- **Výsledkem** je pružné, na platformě nezávislé šifrování databází, které je **transparentní** pro kód aplikace!

Šifrování databází Caché : ochrana dat v klidu



- **Navrženo** k zamezení neautorizovaným uživatelům, aby viděli nebo používali data z databáze Caché.
- **Šifrování** je nastaveno na úrovni jednotlivé databáze v okamžiku jejího vytvoření
- Caché zavádí šifrování a dešifrování s využitím algoritmu **AES (Advanced Encryption Standard)**.
- **Šifrování** a **dešifrování** probíhá v okamžiku čtení či zápisu do databáze... „za letu“.
- Soubor **WIJ** je rovněž **šifrován**.
- **Minimální** vliv na výkonnost!

Šifrovací klíče



- Každá instance Caché může vytvořit **unikátní** klíč k šifrování databáze.
- Je to **trvalý** klíč, takže jej nemusíte měnit po jeho vytvoření a aktivaci
- Caché umožňuje použití **128, 192, or 256-bitových** klíčů.
- Klíč je spolu s účtem administrátora klíče uložen v **souboru šifrovacího klíče**.

Soubor šifrovacího klíče



- Obsahuje několik **šifrovaných** kopií šifrovacího klíče.
- Každá kopie je k přiřazena jednomu **účtu správce klíče** (uživatelské jméno a heslo).
- Tento účet je **vyžadován k aktivaci** šifrovacího klíče a ke správě šifrované databáze.
- Jakmile si klíč uložíte, můžete jej **přesunout** na libovolné místo dle výběru.
- Ztráta nebo zničení klíče může učinit všechny šifrované databáze trvale nečitelné .
- Je nezbytné, abyste si **kopii** souboru s klíčem uložili na bezpečné místo, které nemůže být zničeno... doporučen je vyjímatelný USB Flash disk.

Vytvoření šifrované databáze



- Databáze je šifrována v okamžiku jejího vytvoření (pokud je zvoleno).
- *Poznámka: nelze šifrovat již existující databázi! Řešením je import dat a rutin do nové, šifrované databáze.*
- Cache musí obsahovat **aktivovaný** šifrovací klíč key před tím než **vytvoříte** nebo **namontujete** šifrovanou databázi.
- Jakmile je databáze šifrována (s aktuálně “aktivovaným” šifrovacím klíčem), nemůže být navrácena do nešifrované a je trvale spojena s daným šifrovacím klíčem.
- K trvalému “odšifrování” dat je nutné vytvořit nešifrovanou databázi a data do ní zkopírovat.

Šifrování databází – další doporučení



- Vždy zabezpečte, aby šifrovaná databáze, soubor s klíčem a informace o účtu administrátora klíče byly uloženy odděleně od sebe!
- Jestliže šifrovaná databáze leží na disku, který dříve uchovával citlivá, nešifrovaná data, chovejte se k tomuto disku, jako by tato data na něm byla stále obsažena:
 - S využitím vespělé mikroskopové technologie lze stará data z disku získat i po několikanásobném přepsání!

INTERSYSTEMS

SYMPOSIUM 2005

Bezpečnostní certifikace



Základní informace



- Pro mnoho zákazníků z veřejného i soukromého sektoru je bezpečnostní certifikace rozhodující záležitost.
- V minulosti byla certifikace problematická, protože neexistoval univerzální (nebo všeobecně akceptovaný) certifikační proces.
- Existovala a stále existuje velké množství oddělených certifikačních protokolů a agentur po celém světě.
- Tato situace se zlepšila vyvinutím certifikace „Common Criteria“.

Stav certifikace...



http://www.cse.dnd.ca/en/services/common_criteria/ongoing_evals.html

Industry Programs
Cryptographic Services
ITS Cryptomaterial Management & Assistance Centre (CMAC)
Public Key Infrastructure
Common Criteria

[CCS Overview](#)
[Certified Products](#)
[Archived Certified Products](#)
[Products in Evaluation](#)
[Protection Profiles](#)
[Canadian Evaluation Facilities](#)
[International Partners](#)
[Documentation](#)
[How do I...?](#)
Engineering Services
Contact Sources

Common Criteria

Products in Evaluation

The following products are currently undergoing evaluation within the Canadian Common Criteria Evaluation and Certification Scheme.

| Product | Vendor | Evaluation Assurance Level | Evaluation Facility |
|--|--|----------------------------|---------------------|
| Alteon Switched Firewall version 2.0.3.0 | Nortel Networks | EAL 4 | EWA-Canada |
| Caché version 5.1 | InterSystems Corporation | EAL 3 | EWA-Canada |
| Check Point VPN-1/FireWall-1@ NG FP1 | Check Point Software Technologies Inc. | EAL 4 | EWA-Canada |
| CipherOptics SG-series v3.1 | CipherOptics Inc. | EAL 2+ | Domus ITSL |

SYMPOSIUM
INTERSYSTEMS 2005

Závěrem...



Co získají Vaše aplikace?



- Bezpečnost světové třídy
 - silná, konsistentní, snadná a rychlá,
- certifikovaná,
- dobře začleněná jako důležitá část Caché a InterSystems,
- budovaná s potěšením pro trh a naše zákazníky.

INTERSYSTEMS

SYMPOSIUM 2005

Děkuji za pozornost!

