Správa identit a přístupů

zahrnuje:

- identifikaci – rozpoznávání entit
- autentizaci – ověřování tvrzení o identifikaci
- autorizaci – řízení přístupu (fyzická, logická, …)
- odpovědnost – tj. kdo co udělal

objekt – pasivní entita, ke které je přistupováno
subjekt – aktivní, přístup žádající/provádějící entita
očividně mnohé subjekty mohou v jiných situacích vystupovat jako objekty a vice versa
přístup – cokoliv, co je subjektu povoleno provádět s objektem
přístup řídíme k

- informacím
- systémům
- zařízením (device)
- prostorám (facility)

Přístup k informacím

zajištění důvěrnosti a integrity

Přístup k systémům

cílem je zachování dostupnosti, utajení, integrity, autenticity a nepopiratelnosti
… ve vztahu ke komponentám systému, poskytovaným službám i spravovaným datům
v rámci systému lze IaM provozovat centralizovaně, i decentralizovaně.

Přístup k zařízením

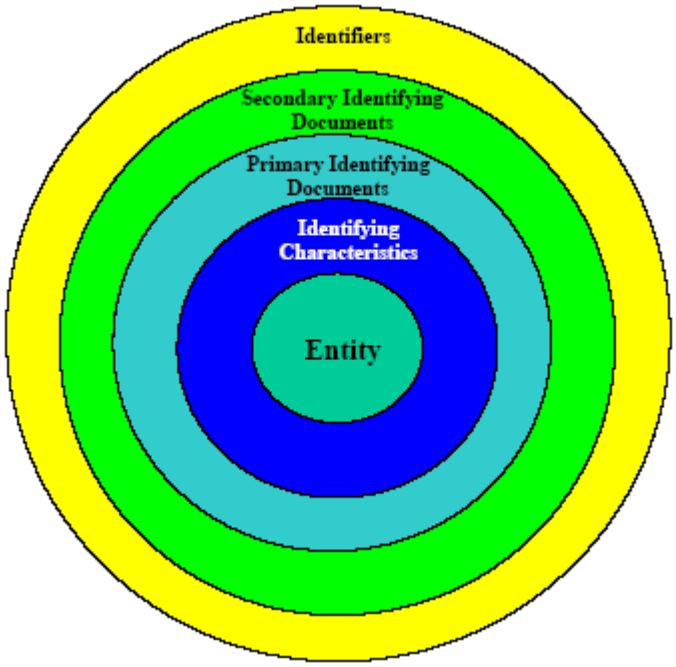
zařízením rozumíme komponentu (informačního) systému
omezení fyzického přístupu pouze na oprávněné subjekty
mobilní zařízení – prostředky pro vzdálenou správu (včetně smazání obsahu)
zvláštní režim pro soukromě vlastněná zařízení využívaná v rámci pracovní činnosti
na druhou stranu zařízení jsou rovněž subjekty a je třeba je umět identifikovat, autentizovat a rozhodnout o jejich přístupu (včetně požadované konfigurace a stavu)

Přístup do prostor

viz fyzická bezpečnost
pozor, často řešíme nejen vstup, ale i výstup, případně chování v prostorách
nejen lité, i zařízení
v současné době je třeba zvážit i případné cloudové, resp. hybridní prostředí
v případě sdílených prostor potom ověření vyhovující politiky poskytovatele

Správa identity

Identifikátory: jméno, userID, rodné číslo
Sekundární identifikující dokumenty:
směnka, výplatní páska, permanentka, ...
Primární identifikující dokumentu:
občanský průkaz, pas, dokumenty svázané přímo s identifikující charakteristikou (např fotografií, otiskem prstu)
Identifikující charakteristika:
biometrika, fotografie, další prostředky rozpoznání jednotlivce
Entita: bytost, místo, věc



Registrace entit (enrollment)

… iniciální přiřazení identifikačních dokumentů entitě
Zásadní důležitost pro spolehlivost a vlastnosti autentizace
Identity assurance level:

- IAL1 – subjekt deklaruje svoji identitu
- IAL2 – spojení subjektu s reálnou identitou, např na základě dodané dokumentace (občanka, pas, …)
- IAL3 – nutná fyzická přítomnost subjektu, formální kontrola předložených průkazů identity školeným pracovníkem

Identita uživatele

Rostou nároky na informace udržované o uživateli, prostou identifikaci nahrazuje komplikovaná struktura označovaná jako ***profil***

- userID, heslo

- jméno, příjmení, tituly, ...
- bydliště
- kontaktní informace
- příslušenství ke skupinám, organizačním jednotkám, ...
- certifikáty, klíče
- personalizace
- oprávnění
-
- ...

Další příbuzné pojmy:

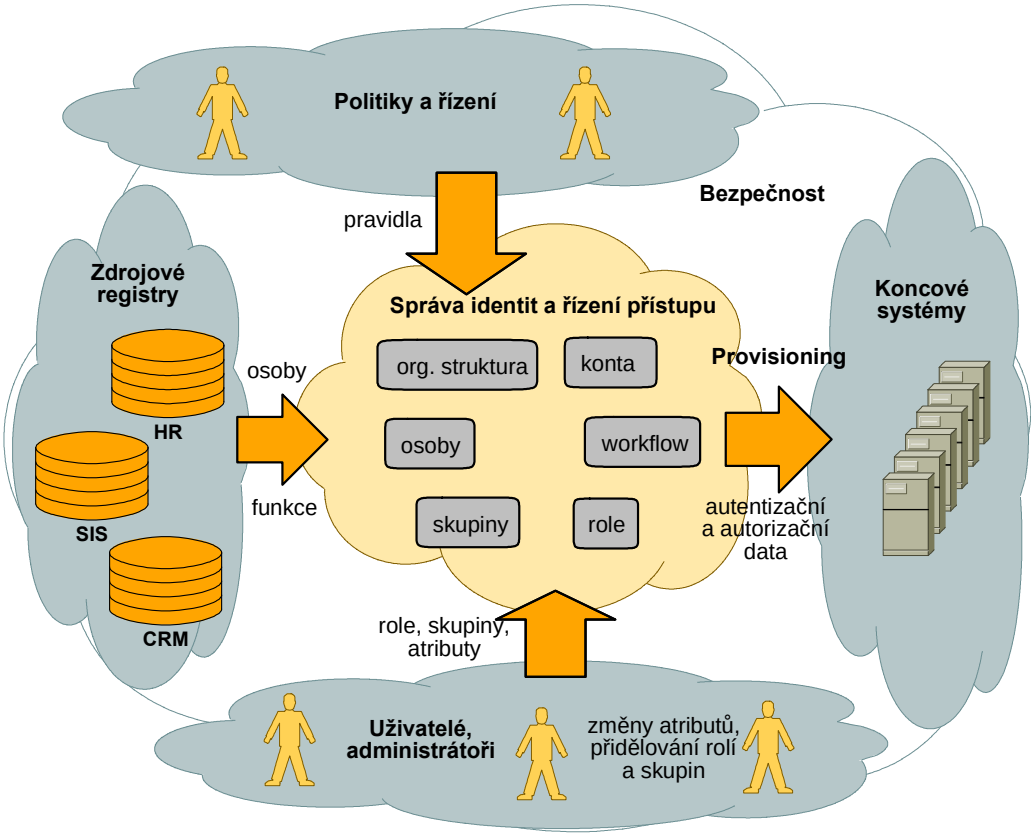
- alias
- anonymita
- pseudonymita

Just-in-time

prostřednitvím např. SAML je možné zcela eliminovat správu identit / úživatelů systémem
identity provider poskytuje potřebná informace on-fly v rámci volání service provideru v rámci odpovídajících ticketů

Federalizace identity

jediná identita uživatele ve všech systémech
konzistentní záznamy o uživateli, změnu záznamů a identifikačních údajů
kredenciály (přenos identity)
může být komplikované vzhledem k technickým omezením jednotlivých systémů
synchronizace vs. externí identita



v ČR vzniká globální federalizační prostředí pro oblast státní správy = JIP (jednotný identitní prostor) se ztotožňováním identit vůči centrálnímu registru osob a obyvatel
na něj navazuje mechanismus KAAS – autentizace a SSO
oba mechanismy představují externí centralizovaný systém správy identit s návazností na řízení uživatelů a jednotné přihlášení
V souvislosti s e-governmentem byl zprovozněn centrální autentizační bod NIA (národní identifikační autorita) integrující různé autentizační mechanismy:

- bankovní identita
- e-občanka
- ICA tokeny
- MojeID
- IIG - international ID gateway
- NIA ID

oba tyto mechanismy autentizují fyzické osoby

Autentizace

jde o proces (mechanismus) zjištění/ověření identity subjektu

zásadní význam pro možnost aplikace bezpečnostních mechanismů
asociace subjektu/identity s příslušnou sadou autorizací
systémy pro správu informací musí zajistit dodání těchto informací autorizovaným uživatelům
navíc autentizace je nutná i při zajišťování např. fyzické bezpečnosti
Mechanismus autentizace může být založen na některém z následujících faktů:

- Typ 1: Co ví (pouze) dotyčná osoba - heslo, pass-phrase, šifrovací klíč
- Typ 2: Co vlastní - token, schopnost, znalost
- Typ 3: Cosi charakteristického - biometriky
- Typ 4: Adaptivní autentizace – prostředek se volí dle podmínek (založeno na politice)

Hesla

Charakteristika dobrého hesla:

- Obsahuje kromě velkých a malých písmen též číslice a další na klávesnici se vyskytující značky
- Dostatečná délka
- Nejde o obvyklé slovo nebo známou frázi
- Nepravděpodobné - nelze jej odvodit ze znalosti osoby vlastníka
- Často obměňované
- Není nikde po okolí poznamenáno

Passphrases

jde vlastně o dlouhá hesla, mohou to být části písní, básniček, části citátů …
pokud použijeme vhodný kompresní algoritmus, lze passphrázi transformovat ve velmi kvalitní heslo
navíc je možné aplikovat různé další měření - např. rytmus stisku jednotlivých kláves, jež bývá pro každého charakteristický
v současné době preferováno před hesly – snáze zapamatovatelné, odolnější vůči slovníkovým útokům a exhaustivnímu hledání

Skupinová hesla

z různých důvodů občas systémy připouštějí hesla společná skupinám uživatelů - tato hesla jsou málo bezpečná, bývají často vyzrazena

Piny

(personal identification number)

jsou číselné řetězce standardní délky, sloužící k podobným účelům jako hesla
v souvislosti s platebními a kreditními kartami historicky používány 4-místné piny, dnes se pod označením PIN objevují i hesla obvyklého charakteru

Challenge-Response systémy

heslo může být zachyceno v průběhu vkládání, nebo při přenosu cílovému uzlu
časté změny hesla jsou pro uživatele zatěžující
vhodnější je, pokud systém zašle výzvu v podobě náhodné zprávy a uživatel jako heslo vrátí správnou reakci na tuto zprávu - např. její zašifrování tajným klíčem apod.

Jednorázová hesla

ideálně implementováno pomocí tokenů, někdy s nutností aktivace zadáním hesla / pinu
v současné době obvyklá implementace jako aplikace v mobilu
méně vhodná implementace pomocí ověřovacích zpráv / SMS

Vícefaktorová autentizace

kombinace několika autentizačních postupů, např. pin + smart karta
vyšší úroveň bezpečnosti

- několik nezávislých bezpečnostních mechanismů aplikovaných paralelně, nebo
- aktivace silnějšího mechanismu a následná autentizace za použití tohoto mechanismu

Výměna tajností

protokol pro případ, že komunikující strany příliš nedůvěřují svému okolí a nechtějí vyzradit svoji identitu
pokud sdílejí tajný klíč *e*:

1. *A* zašle *B* zprávu **E**(*m, e*)
2. *B* vrátí *A* zprávu **E**(*m* + <*heslo*>, *e*)

pokud tajný klíč nesdílejí, neobejdou se bez centrální autority *C*:

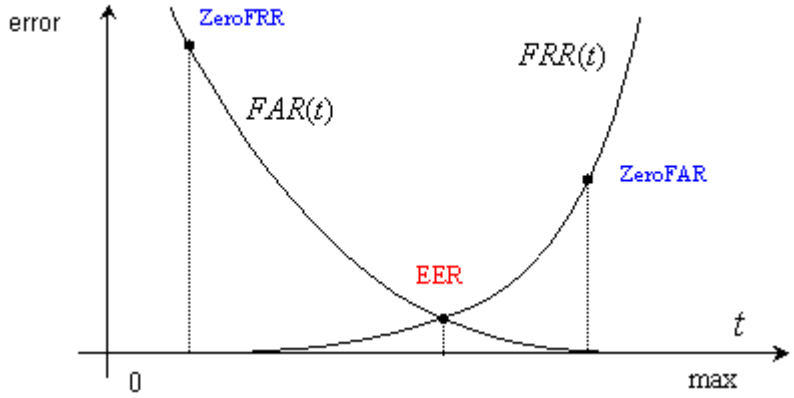
1. *A* zašle *C* zprávu {*B, m*} e_A
2. *C* vytvoří transakční klíč *k*
3. *C* zašle **E**(<*B, m, k,* **E**(<*A, m, k*>, e_B)>, e_A) zpět *A*
4. Dešifrováním zprávy *A* získá *m, k* a **E**(<*A, m, k*>, e_B)
5. *A* zašle **E**(<*A, m, k*>, e_B) uzlu *B*

pro zajištění ochrany proti znovupoužití starých zpráv *m* musí obsahovat timestamp

Biometriky

jde o techniky identifikace lidí na základě jejich osobních charakteristik
navzájem se odlišují různou mírou spolehlivosti, ceny a v neposlední řadě i společenské přijatelnosti
hledáme charakteristiky mající dostatečnou mezi-osobní variabilitu při zachování vnitro-osobní reproducibility
kvalitu biometrik lze charakterizovat:

- četnost nesprávných odmítnutí - autorizovaného subjektu
- četnost nesprávných přijetí - útočníka
- kvalitou senzorů (!)



zdroj: Biometrika.it

' erifikace #lasu

testovaný subjekt přečte systémem náhodně zvolenou frázi, sejmutá zvuková stopa je kmitočtově omezena (nejčastěji na 3kHz) a je proveden rozbor zvuku na základě původu jednotlivých složek zvuku v činnosti hlasového aparátu - fonace, frikace.
Výsledek je vhodným způsobem komprimován na vzorek velikosti 1 až 2 kB a porovnán se srovnávacím vzorkem
Výhodou je přirozenost a možnost provádět verifikaci např. prostřednictvím telefonu.

' erifikace dynamiky podpisu

Sledují se změny tlaku, zrychlení v jednotlivých částech, celkový průběh zrychlení, zarovnání jednotlivých částí podpisu, celková rychlost, celková dráha a doba pohybu pera na a nad papírem apod.

Ze získaných hodnot je opět vytvořen vzorek, který je porovnán se srovnávacím vzorkem.
Výhodou opět přirozenost a sociální akceptovatelnost, nevýhodou malá mechanická odolnost snímačů, a značná variabilita podpisu u některých lidí.

' erifikace otisků prstů

Systém provádí statistický rozbor výskytu tzv. markant - hrbolků, smyček a spirál v otisku prstu a jejich vzájemné polohy
často se provádí testování uživetelem zvoleného výběru několika prstů
Výhodou je vynikající mezi/vnitro-osobní variabilita, a dobrá zpracovatelnost vstupních dat, nevýhodou jsou možné negativní asociace uživatelů, a mnohdy sporná spolehlivost snímačů

(eometrie ruky

Metoda zkoumá délku a šířku dlaně a jednotlivých prstů, boční profil ruky apod.
Výsledkem je velmi malý vzorek - cca 18 bytů. Metoda je poměrně spolehlivá avšak poněkud dražší. Možnost podstrčení odlitku ruky.

) brazy sítnice

Zařízení pořídí obraz struktury sítnice v okolí slepé skvrny, tento obraz je digitalizován a převeden na vzorek délky přibližne 40 bytů (!)
Obrázky sítnice mají stejné charakterizační vlastnosti jako otisky prstů
Výhodnou metody je značná spolehlivost a velmi obtížná napodobitelnost. Proto jde o metodu vhodnou k nasazení v prostředí nejvyššího utajení. Nevýhodou jistá subjektivní nepříjemnost, opět jde o velmi drahou technologii.

Další biometriky

rysy obličeje, Bertillonovy míry, rytmus psaní na klávesnici, EEG, EKG, otisky dlaní a chodidel, otisky chrupu, genetické rozbory, …

Odpovědnost

tj. zajištění odpovědnosti osob a procesů za provedené akce
základem je vědět, kdo a co provedl
Systém bez logů a auditních záznamů je bez paměti – nemůže reagovat na vlivy vnějšího prostředí
Data v systému bez auditních záznamů nemohou být důvěryhodná
Systém, který není monitorován nemůže být spolehlivý

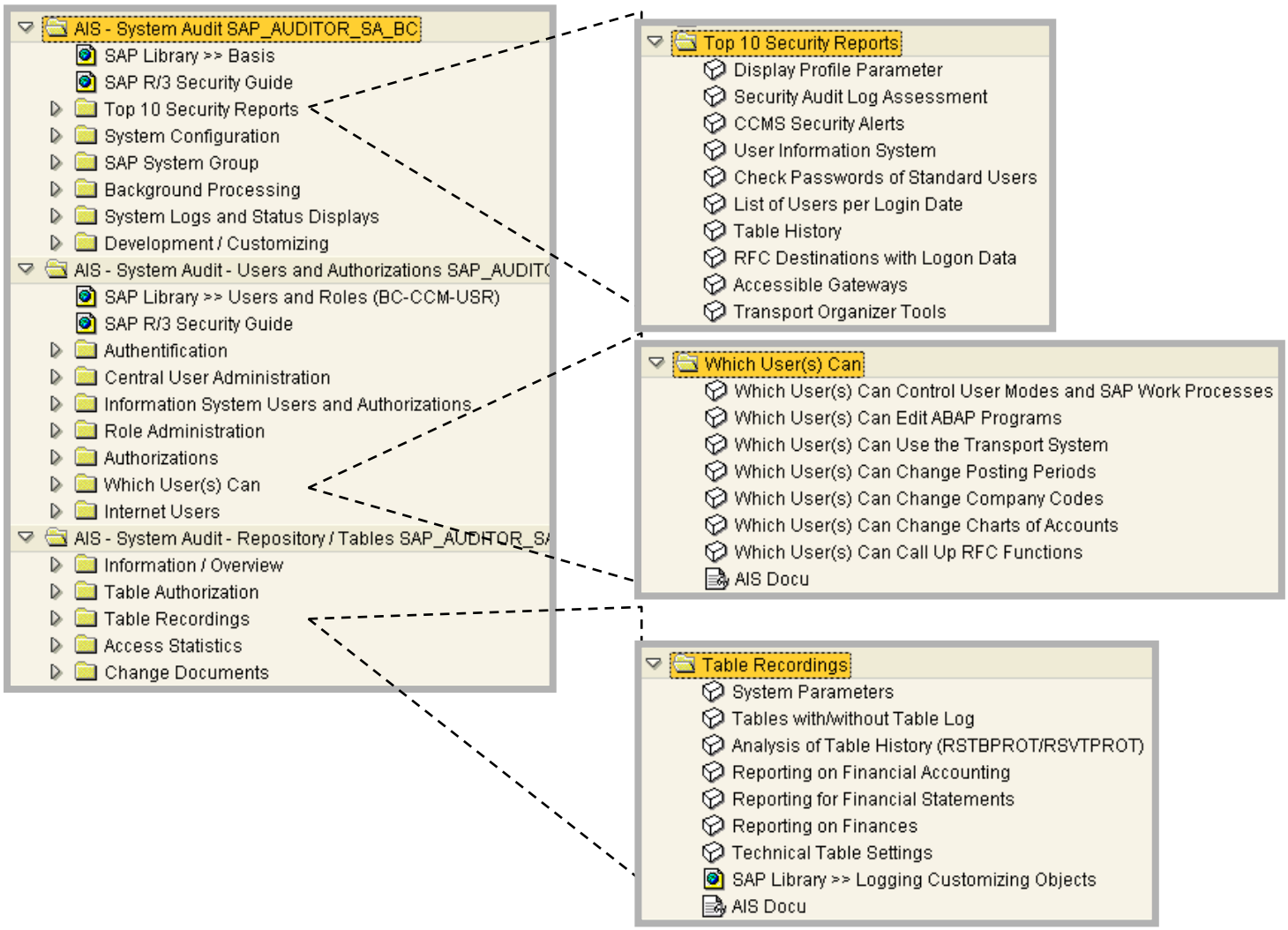
principiálně existují dva druhy logů, které ale společně umožňují zvládat bezpečnostní incidenty:

- auditní logy
- provozní logy (redo logy, historie provozních parametrů, ...)

Požadavky na auditní logy:

- zachycení dat důležitých pro detekci připravovaného incidentu
- uchování všech informací pro rekonstrukci průběhu napadení
- spolehlivost informací (tj. "nepřepisovatelnost" logu)
- úplnost logu – tj. že pokrývá všechny operace, které jsou z hlediska bezpečnosti relevantní

Příklad: systémový audit SAP



Požadavky na provozní logy

- úplnost
- odolnost vůči chybám HW - podpora zotavení

Správa logů

Analýza logů
prvním problémem integrace vznikajících logů
musí být soustavná a pravidelná
* prahy (tresholds)
* trendy,
* grupování
k dispozici celá řada nástrojů na automatizovanou analýzu:

- Security Manager (NetIQ);
- ESM/Security Management System (Symantec);
- Network Security Manager, (Intellitactics);
- Open e-Security Platform (eSecurity);
- Netcool/OMNIbus (Micromuse);
- eTrust (CA);
- Tivoli (IBM);
- NetForensics (netForensics);
- ArcSight (ArcSight);
- Caltarian (RipTech);
- ePolicy Orchestrator (McAfee);
- bv-Control, (BindView);
- Private I Intelligence Suite (OpenSystems).

Řízení oprávnění (autorizací)

Granularita - kontrola přístupu může být implementována na různých úrovních (byte, věta, soubor, adresář, …), je potřebné volit mezi režií kontroly a dostatečně jemným rozlišením
existují různé strategie / koncepty pro správu přístupů:

Řízení autorizací založené na rolích (RBAC)

odvozuje oprávnění subjektu od jeho role v rámci organizace
roli chápeme jako sadu činností, které má daný pracovník provádět na základě pozice, oddělení apod.

Řízení autorizací založené na pravidlech (RuBAC)

používá předdefinovaná pravidla, ze kterých se odvozují oprávnění
(např. ACL, rulesety firewallů, black/whitelisty apod.)
důležité je implicitní nastavení – deny all nebo allow all

Povinné/nediskreční řízení přístupu (MAC)

… někdy též nediskreční (nondiscretionary), nebo též centrální
je aplikována systematicky bez rozlišování vztahu k subjektu
založen na označování subjektů a objektů bezpečnostními labely a následné aplikaci pravidel pro přístup na vzájemném porovnání labelů subjektu a objektu
(víceúrovňové modely)

Diskreční řízení přístupu (DAC)

v principu decentralizovaný model
založen na rozhodnutích vlastníků objektů

Řízení přístupu založené na atributech (ABAC)

někdy též řízení přístupu založené na politice
velmi dynamický a flexibilní model
kombinuje atributy subjektu a vyhodnocuje je v závislosti na podmínkách a porovnává s nastavenou politikou
přístup tak může záviset nejen na oprávněních, ale i na době, místu odkud je prováděn, …
např. stavové firewally

Řízení přístupu založené na riziku (risk-based)

přizpůsobuje postupy řízení přístupu situaci, tomu, k čemu je přístup žádán a za jakých okolností
např: při přístupu z nového zařízení požaduje vícafaktorovou autentizaci
omezí počet pokusů o autentizaci v době, kdy detekuje útok

Mechanismy řízení autorizací

Je třeba si uvědomit, že autorizační mechanismus lze vnímat jako dvojici:

- Rozhodovací algoritmus (viz modely)

- Autorizační data … tj. konkrétní parametrizace algoritmu v daném IS

+dresář %directory&

metodu popíšeme pro případ uživatelů systému v roli subjektů a souborů coby objektů, lze ji však snadno rozšířit na libovolné objekty a subjekty
každý soubor má svého vlastníka, který k němu vlastní veškerá práva včetně práva určovat rozsah oprávnění ostatních uživatelů k tomuto souboru
s každým uživatelem je spojena specielní struktura - *adresář* - obsahující odkazy na všechny soubory, k nimž má daný uživatel nějaké oprávnění, včetně popisu tohoto oprávnění
žádný uživatel nesmí zapisovat do svého adresáře

Nevýhodou může být velký rozsah adresářů a velmi obtížná správa a úpravy takto přidělovaných oprávnění. Rovněž udržení přehledu o tom, kdo k danému souboru má jaká práva může být problematické.

, eznam oprávnění %+ccess - ontrol . ist&

opačný přístup k problému
tentokrát je s každým *objektem* udržován seznam informací, které subjekty k němu mají jaká oprávnění
metoda umožňuje snadno přidělovat implicitní práva subjektům případně skupinám subjektů
při vhodném označení subjektů a použití expanzních znaků může být tato metoda dostatečně pružná

Př: Pepek_Group1_Troja
*_Group1_*

seznamy zpravidla bývají udržovány setříděné tak, že záznamy s expanzními znaky jsou na konci - tak stačí hledat první shodu s identifikací subjektu a použít tímto záznamem specifikované oprávnění

/ řístupová matice %+ccess - ontrol 0 atri1&

řádky matice odpovídají jednotlivým subjektům, sloupce objektům
v políčku daném řádkem a sloupcem je záznam o úrovni oprávnění odpovídajícího subjektu k příslušnému objektu
přístupová matice je zpravidla velmi velká záležitost, zhusta řídká

2působilost % - apability&

Způsobilost budeme chápat jako nefalšovatelný token, jehož vlastnictví dává vlastníkovi specifická práva k danému objektu. Lze chápat jako lístek do kina.

jednou z metod zajištění nefalšovatelnosti je, že tokeny se nepředávají přímo subjektům, ale jsou udržovány v chráněné oblasti paměti, přístupné pouze systému

při přístupu k objektu tak systém zkontroluje existenci příslušného tokenu, tento postup lze urychlit tím, že zvlášť udržujeme seznam *Způsobilostí* právě běžícího procesu
výhodou metody je, že dovoluje definovat nové dosud neznámé způsoby používání objektů a přidělovat odpovídající oprávnění
nevýhodou opět poněkud obtížná správa těchto tokenů, zejména odebrání Způsobilosti je netriviální operace

, ecurity . abel

s každým subjektem a objektem asociujete bezpečnostní label popisující pověření/klasifikaci entity
podpora víceúrovňových modelů

/ rocedurálně orientovan3 přístup

namísto přidělování obecného přístupu k subjektu (čtení, zápis, …) můžeme přidělovat právo používat některých funkcí z rozhraní, prostřednictvím kterého je objekt zpřístupňován
metoda podporuje koncept skrývání a zapouzdřování informací popsaný v minulé lekci
nevýhodou je jistá ztráta efektivity a rychlosti přístupu

Zvládání granularity autorizace

) c#rana po skupinác#

uživatelé jsou podle svého zaměření, pracovního zařazení, …, vhodně rozděleny do skupin
pro účely ochrany objektů je svět rozdělen na vlastníka souboru, skupinu, do ktere vlastník patří a ostatní uživatele
předpokládá se, že uživatelé v rámci skupiny potřebují sdílet data
při vytvoření objektu vlastník specifikuje, jaká práva přiděluje sobě, uživatelům ve stejné skupině, ostatním

metoda je jednoduchá, snadno implementovatelná leč neposkytující dostatečně jemné rozlišení, navíc je většinou nutné, aby každý uživatel byl právě v jedné skupině, jinak nastávají problémy s přidělováním práv skupinám

4esla nebo "in5 tokeny

při vytvoření objektu vlastník specifikuje hesla, potřebná pro jisté módy přístupu k objektu, heslo zašle uživatelům, kteří mají mít přístup
systém splní žádost o přístup k objektu pouze tomu, kdo se prokáže odpovídajícím heslem
nevýhodou je, že v případě zapomenutí není možno zjistit, jak heslo vypadalo, v případě, že dojde k vyzrazení hesla je složité nastavit nové, stejně obtížné je odejmout právo přístupu

6očasn5 propů"čení oprávnění

mechanismus známý ze systému UNIX.
stejné přidělování práv jako v případě ochrany po skupinách, navíc je možno stanovit, že (spustitelný) soubor smí být prováděn s oprávněním vlastníka
prostřednictvím rutin běžících s oprávněním vlastníka lze řízeně přistupovat k objektům, ke kterým uživatel přímý přístup nemá

problémem popsaných schémat je jistá těžkopádnost, uživatel nemůže selektivně přidělovat práva jistým uživatelům k jistým skupinám objektů
kontrolní matice a podobné metody jsou zase příliš rozsáhlé a obtížně spravovatelné

) becn3 identifikátor 7 #ierarc#izace oprávnění

ke každému souboru může uživatel vytvořit *Seznam oprávnění* udávající kdo má jaká práva
každý uživatel je členem jedné skupiny, navíc administrátor může vytvořit skupinu typu *obecný identifikátor* , a tuto skupinu mohou uživatelé uvádět v *Seznamech oprávnění*
Seznamy oprávnění mohou být též použity pro přidělování přístupu k ostatním systémovým zdrojům

6ědění

Systém vytváří hierarchie objektů (adresáře, souboru, skupiny uživatelů, …), oprávnění lze přidělit do libovolné vrstvy hierarchie
lze povolit / zakázat „zdědění“ oprávnění od nadřazených objektů

) rganizační struktura

autorizace se přidělí nikoliv přímo uživatelům, ale do uzlů organizační struktury
zařazením pracovníka na příslušné pracovní místo se mu „zdědí“ všechna oprávnění z celé cesty stromem od kořene až k jeho místu

$mpersonace

autentizační mechanismus umožní autentizované entitě přepnutí identity na jinou entitu, tzn. pro závislé systémy vše vypadá jako by se přihlásila impersonovaná identita
vhodné pro administrační zásahy (sudo), nezbytné pro testování

, yst5m rolí a skupin

oprávnění jsou sdružována do ucelených souhrnů – tzv. rolí – které odpovídají svým obsahem okruhu práce, kterou vykonává pracovník na určitém zařazení (správce uživatelů, finanční účetní, skladník, ..)
uživatel nezískává oprávnění „po jednom“, ale přidělením role
pro zjednodušení práce bývá k dispozici systém kompozitních rolí, odvozených rolí atd.
namísto práce s jediným uživatelem může být možné definovat a hromadně spravovat celé supinu uživatelů, majících stejná oprávnění

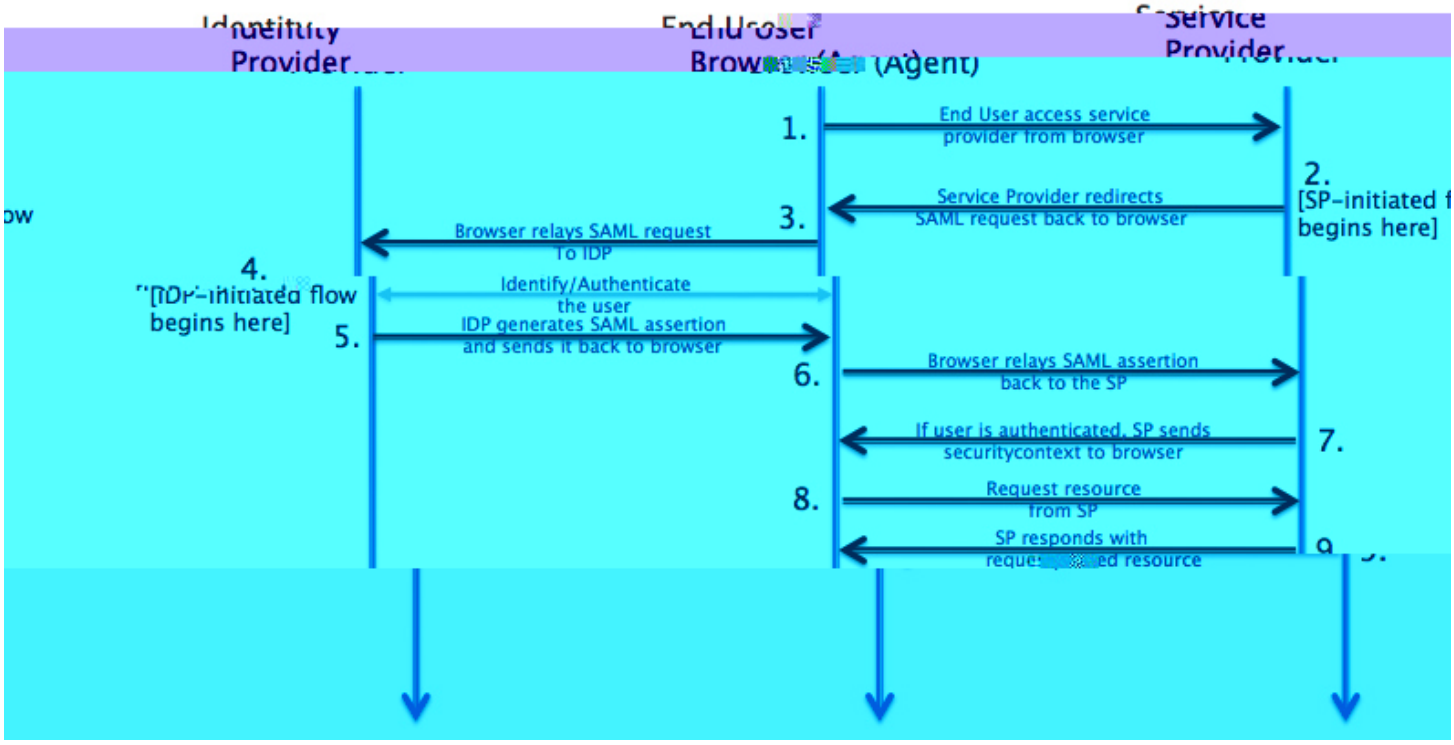
8eferenční u!ivatel5

předpřipravené vzory častých typů uživatelů obsahující např. přiřazené role oprávnění, personalizaci, nastavení ...
- ulehčují správu oprávnění

Security Assertion Modeling Language (SAML)

protokol pro sjednocení správy identit a řízení přístupu, založený na XML formátování
poskytuje služby jednotného přihlášení, jit řízení autorizací a provisioningu a jednotného odhlášení
Principal – v naší notaci subjekt
Identity provider – správa identit a zpravidla i autentizační a autorizační autorita
Service provider – cílový systém poskytující službu
Tvrzení (assertion) je token obsahující informace o subjektu (kdo byl autentizován, jaká oprávnění, další atributy)

Vazby (bindings) – určují způsob, jak jsou realizovány jednotlivé kroky SAML komunikace prostředky hostitelského protokolu (http post/redirect, SOAP, artefakty, …)
Profily – určují, jak jsou jednotlivá SAML tvrzení vkládána do SAML zpráv a jak jsou následně zpraovávána (web browser, proxy, identity provider, single logout, name identifier, artifact resolution, assertion query/request, atribute, …)



zdroj: OKTA