MULTI-DIMENSIONAL ACCESS CONTROL IN WEB APPLICATIONS

Pavol Grešša
Master Degree Programme (2), FIT BUT
E-mail: xgress00@stud.fit.vutbr.cz

Supervised by: Dušan Kolář
E-mail: kolar@fit.vutbr.cz

Abstract: Distributed information systems consist of many subsystems that provide services to their users. There is a fundamental need for confidential and safe access to the information managed by these subsystems. Security policy applied for access to domain's assets is diverse and unpredictable. The purpose of this work is the analysis of the best known security models and their unification into particular dimensions.

Keywords: multi-dimensional access, authentication, authorization, distributed systems

1 ÚVOD

Distribuovaný informačný systém pozostáva z množstva samostatných služieb. Každá služba musí zabezpečiť ochranu informácií pred zneužitím, k čomu využíva autentifikácie a autorizácie užívateľov. Tieto vlastnosti sú označované ako AAA (Authentication, Authorization, Accounting).

Ak je každý subsystém zodpovedný za AAA, dochádza k degradácii celého systému z dôvodu netransparentnosti vnútorných procesov, fragmentácii zodpovedností a redundancii dát vzťahujúcich sa k identitám užívateľov. Z týchto dôvodov sa do distribuovaných prostredí nasadzuje jedna autonómna centrálna autorita, ktorá poskytuje AAA služby všetkým subsystémom a preberá zodpovednosť za autentifikáciu a autorizáciu užívateľov. Subsystémy požiadavky na autorizáciu buď delegujú, alebo sú zbavené tejto povinnosti a autorizáciu vykoná priamo centrálna autorita.

Nároky heterogénnych webových informačných systémov ďaleko prevyšujú požiadavky na vnútropodnikové systémy. Rýchlosť odozvy systému na požiadavky, robustnosť a bezpečnosť sú rozhodujúcimi faktormi úspešnosti poskytovanej služby.

Nástrojov a systémov existuje veľké množstvo. Medzi najčastejšie nevýhody patrí hlavne snaha vytvoriť univerzálny nástroj [1], pripravený k okamžitému používaniu. Univerzálnosť riešenia má za následok zložité vnútorné procesy, ktoré výrazne ovplyvňujú rýchlosť odozvy na požiadavky. Problémom sú často aj slabé výrazové prostriedky [4].

2 DIMENZIE PRÍSTUPU

Každý bezpečnostný model [2] je založený na vyhodnotení vstupných dimenzií vzhľadom na bezpečnostnú politiku, ktorú realizuje. Základným vstupom je objekt, subjekt a operácia, ktorú chce subjekt vykonať nad objektom. Bezpečnostný model je definovaný kartézskym súčinom

$$S \times O \times A, \tag{1}$$

kde

- S je množina všetkých subjektov
- O je množina všetkých objektov
- A je množina všetkých operácií nad objektmi z množiny O

Tento model je aplikovateľný na systémy založené na vyhodnotení jednoduchých vzťahov medzi subjektom a objektom. Vyhodnotením sa získa buď kladná odpoveď, teda subjekt je autorizovaný k vykonaniu operácie nad objektom, alebo takýto vzťah v modelu neexistuje. Pridaním dimenzie času sa rozšíri aplikovateľnosť modelu o časové obmedzenie.

Definovaný jednoduchý bezpečnostný model vyhodnotí existenciu resp. neexistenciu práva subjektu aplikovať operáciu na objekt. Existencia resp. neexistencia vyjadruje takzvanú modalitu vzťahu subjektu k právu. Vyhodnotenie "existuje" resp. "neexistuje" vyjadruje vzťah, v ktorom subjekt môže resp. nemôže vykonať operáciu nad objektom. Každý bezpečnostný model definuje vlastnú modalitu vzhľadom na aplikovanú bezpečnostnú politiku. Mandatórny bezpečnostný model používa modalitu "má vlastnosť". Modalita voľného bezpečnostného modelu je "je identity" či "je v skupine", model založený na rolách analogicky "je v roli". Účelom Business Process Modelingu [3] (ďalej len BPM) je štrukturovaný a detailný popis procesov v rámci organizácie a určenie zodpovedností. Výsledok BPM slúži ako podklad pre bezpečnostnú politiku, v ktorej modalita vyjadruje vzťah subjektov k procesu alebo jeho časti, čím identifikuje právo.

Univerzálny bezpečnostný model [1] je definovaný kartézskym súčinom piatich dimenzií

$$S \times O \times A \times M \times T, \tag{2}$$

kde

- S je množina všetkých subjektov a určuje dimenziu KTO
- O je množina všetkých objektov a určuje dimenziu S ČÍM
- A je množina všetkých operácií nad objektmi a určuje dimenziu ČO
- M je množina všetkých modalít a určuje dimenziu MODALITA
- T je množina všetkých časových údajov a určuje dimenziu KEDY

Univerzálny bezpečnostný model pracuje s dotazmi v rámci celej päťdimenzie:

KTO ČO MODALITA S ČÍM KEDY

Príklad:

> "Môže (MODALITA) daný aktér (KTO) vykonať operáciu (ČO) na daný objekt (S ČÍM) v aktuálnom čase (KEDY)?"

Spôsob vymedzenia prvkov z jednotlivých dimenzií [1] je závislý na charaktere aplikácie. Väčšina aplikácií vystačí s použitím definície bezpečnostnej politiky v 2 s jednou modalitou "môže" resp. "nemôže". Modalita "nemôže" sa dá eliminovať pravidlom: "všetko, čo nie je povolené, je zakázané".

2.1 VYMEDZENIE DIMENZIE SUBJEKTOV (KTO)

Dimenzia subjektov je vymedzená užívateľom. U informačných systémov založených na rolách sú subjekty tiež vymedzené rolami. Subjekty môžu byť vymedzené aj samostatnými procesmi, ktoré operujú automaticky v rámci systému.

2.2 VYMEDZENIE DIMENZIE OPERÁCIÍ (ČO)

Model je možné napevno zviazať so základnými operáciami manipulácie s dátami – READ, WRITE, DELETE. Dimenzia môže byť vymedzená aj operáciami vyššej úrovne, napríklad publikovanie článku či schválenie dokumentu.

2.3 VYMEDZENIE DIMENZIE MODALÍT

Modalita je zviazaná s použitým bezpečnostným modelom. Často sa jedná o modalitu "môže" resp. "nemôže". K odhaleniu modalít sa použije BPM. Vymedzenie potom predstavuje jednoduché ukázanie na zodpovednosť v rámci procesu.

2.4 VYMEDZENIE DIMENZIE OBJEKTOV (S ČÍM)

Dimenzia objektov je vymedzená vzhľadom na charakter aplikácie a identifikácie aktív systému. Základnou vymedzovacou zložkou sú objekty systému podliehajúce obchodnému procesu. Aplikovaním abstrakcie nad základnými objektmi sa vymedzujú skupiny objektov s nejakou spoločnou vlastnosťou:

1. *typ objektu* – všetky dokumenty
2. *účelovo zoskupené objekty* – rozpracované dokumenty
3. *viazané objekty k inému objektu* – všetky dokumenty k projektu A
4. *účelovo vytvorené kombinácie 1, 2, 3* – všetky rozpracované dokumenty projektu A

2.5 VYMEDZENIE DIMENZIE ČASU (KEDY)

Základným vymedzovacím nástrojom je časový interval OD–DO. Možné je aj vymedzenie na základe periodicky sa opakujúcej formy času – každý 2. deň v mesiaci. Sofistikovanejšie vymedzenie vzhľadom k dimenzii KTO – prístup člena týmu A k dokumentom týmu B po dobu trvania projektu.

3 ZÁVER

Unifikovanie bezpečnostných modelov slúži ako stavebný kameň pre AAA systém, umožňujúci aplikovať akúkoľvek bezpečnostnú politiku. Na centrálny AAA systém budú subsystémy delegovať autorizačné požiadavky vo forme definovanej päťdimenzie a ich vymedzených prvkov. Vyhodnotenie požiadavky bude závislé na logike požadovanej modality.

Takýmto spôsobom zostáva zodpovednosť za vyhodnotenie na AAA autorite, redundancia je minimálna a procesy sú transparentne umiestnené na jednom mieste.

LITERATÚRA

[1] Procházka, F.: eTrium – Univerzální nástroj pro správu přístupových práv. In *Sborník konference DATAKON 2003*, Masarykova Univerzita v Brňe, Fakulta informatiky, Masaryk University, 2003, s. 265-275.

[2] Castano, S., Fugini, M. G., Martella, G. aj.: Database Security. Acm Press Books, 1996, ISBN 978-0201593754

[3] Havey, M.: Essential business process modeling. O'Reilly Media, 2005, ISBN 978-0596008437

[4] DACS, DSS Distributed Systems Software Inc, URL: http://dacs.dss.ca/