HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

A MANDATORY MODEL OF PROVIDING PRIVACY IN MULTI-LEVEL INFORMATION ENVIRONMENTS: BELL-LAPADULA METHODOLOGY AND STATE MACHINE ANALYSIS

Imamaliyev Aybek Turapbayevich
Associate Professor, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Email: oimamaliyev1987@gmail.com

Annotatsiya: Ushbu maqolada ko‘p darajali xavfsizlik (Multilevel Security — MLS) muhitlarida ma’lumotlar maxfiyligini ta’minlashning fundamental asosi hisoblangan Bell-LaPadula (BLP) mandatli foydalanishni boshqarish modeli tadqiq etiladi. Modelning subyekt va obyektlar munosabatini qat’iy tartibga soluvchi matematik invariantlari, tizim holatining dinamik o‘zgarishlarini boshqaruvchi "Holatlar mashinasi" (State Machine) kontseptsiyasi va Asosiy xavfsizlik teoremasining (BST) mantiqiy asosi chuqur tahlil qilingan. Maqolaning ilmiy yangiligi, ko‘p darajali tizimlarda Troyan otlari va kiber-tahdidlar orqali yuzaga keladigan axborot sizib chiqish jarayonlarini kompiylyatsiya bosqichidayoq bartaraf etish uchun BLP qoidalari asosida xavfsizlikni statik tekshirish (Static Security Analysis) mexanizmlarini matematik modellashtirishdan iborat.

Kalit so‘zlar: Bell-LaPadula modeli, Mandatli foydalanishni boshqarish (MAC), Maxfiylik invariantlari, Holatlar mashinasi, Asosiy xavfsizlik teoremasi, Axborot oqimi inflyatsiyasi, Statik tekshirish, Troyan otlari.

Аннотация: В данной статье исследуется мандатная модель управления доступом Белла-ЛаПадулы (BLP), являющаяся фундаментальной основой обеспечения конфиденциальности данных в многоуровневых системах безопасности (Multilevel Security — MLS). Проведен глубокий анализ математических инвариантов модели, строго регламентирующих взаимодействие субъектов и объектов, концепции «Автомата состояний» (State Machine), управляющей динамическими изменениями системы, а также логической основы Основной теоремы безопасности (BST). Научная новизна статьи заключается в математическом моделировании механизмов статического анализа безопасности (Static Security Analysis) на основе правил BLP, предназначенных для устранения процессов утечки информации через троянские программы и киберугрозы непосредственно на этапе компиляции в многоуровневых системах.

Ключевые слова: Модель Белла-ЛаПадулы, Мандатное управление доступом (MAC), Инварианты конфиденциальности, Автомат состояний, Основная теорема безопасности, Инфляция информационного потока, Статический анализ, Троянские программы.

Abstract: This article investigates the Bell-LaPadula (BLP) mandatory access control model, which serves as the fundamental cornerstone for ensuring data confidentiality within Multilevel Security (MLS) environments. A profound analysis is conducted on the model's mathematical invariants that strictly regulate the relationship between subjects and objects, the concept of the "State Machine" governing dynamic system variations, and the logical framework of the Basic Security Theorem (BST). The scientific novelty of the paper lies in the mathematical modeling of static security analysis mechanisms based on BLP rules, which are specifically designed to eliminate information leakage caused by Trojan horses and cyber threats directly during the compilation phase in multilevel systems.

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

Keywords: Bell-LaPadula model, Mandatory Access Control (MAC), Confidentiality invariants, State Machine, Basic Security Theorem, Information flow inflation, Static security analysis, Trojan horses.

Kirish

Zamonaviy hisoblash infratuzilmalari, bulutli ekotizimlar, korporativ ma'lumotlar omborlari va taqsimlangan kiber-tizimlarning shiddatli rivojlanishi hamda integratsiyalashuvi kiber-himoya mexanizmlari oldiga mutloq yangi strategik talablarni qo‘ymoqda. Axborot texnologiyalari jamiyat hayotining barcha qatlamlariga chuqur kirib borishi natijasida davlat sirlari, harbiy-sanoat majmualari ma'lumotlari, bank-moliya operatsiyalari va shaxsga doir maxfiy ma'lumotlarni ruxsatsiz manipulyatsiyalardan va latent hujumlardan himoya qilish global kiberxavfsizlikning eng dolzarb muammosiga aylandi.

Bugungi kunda kompyuter tizimlari xavfsizligining buzilishi va konfidensial ma'lumotlarning tajovuzkorlar qo‘liga o‘tib ketishi ko‘p hollarda tashqi kriptografik algoritmlarning zaifligi yoki ularni to‘g‘ridan-to‘g‘ri buzib kirish (brute-force) oqibatida emas, balki tizim ichidagi dasturiy komponentlarning o‘zaro aloqa arxitekturasidagi mantiqiy nuqsonlar hamda foydalanishni boshqarish (Access Control) siyosatining noto‘g‘ri loyihalashtirilishi sababli sodir bo‘lmoqda.

An'anaviy operatsion tizimlarda keng qo‘llaniladigan Diskretsion foydalanishni boshqarish (Discretionary Access Control — DAC) modellari foydalanuvchilarga o‘z resurslari ustidan egalik qilish va obyektdan foydalanish huquqlarini boshqa subyektlarga mustaqil ravishda o‘tkazish (grant/revoke) imkoniyatini beradi. Biroq, subyektlarga berilgan bunday erkinlik tizim ichiga yashiringan troyan dasturlari (Trojan Horses) yoki zararli dasturiy kodlar faollashganda o‘ta zaif xarakter kasb etadi. Troyan oti yuqori imtiyozli foydalanuvchining nomidan tizimga kirib, maxfiy obyektdagi ma'lumotlarni o‘qiydi va uni ruxsatnomalar matritsasini chetlab o‘tgan holda quyi darajadagi (ommaviy) fayl ichiga yozib, tashqariga sizdirib yuborishi mumkin. Bu zanjirli huquq o‘tkazish va ma'lumot sizishi muammosi an'anaviy empirik xavfsizlik devorlari va antivirus dasturlari yordamida mantiqan bartaraf etib bo‘lmaydigan latent zaiflikdir.

Ushbu muammoni tubdan hal etish va axborot xavfsizligining maxfiylik (Confidentiality) ustunini mutloq darajada kafolatlash maqsadida **Mandatli foydalanishni boshqarish (Mandatory Access Control - MAC)** tizimlariga o‘tish zaruriyati yuzaga keladi. MAC tizimlarining eng mukammal matematik poydevori esa 1973-yilda D. Bell va L. LaPadula tomonidan ishlab chiqilgan formal holatlar mashinasi (Formal State Machine) modelidir.

Mavzuning dolzarbligi shundaki, zamonaviy murakkab va reaktiv tizimlarda xavfsizlikni shunchaki kod yozilgandan keyin empirik testlash (testing) orqali ta'minlab bo‘lmaydi. Bell-LaPadula (BLP) modeli subyekt va obyektlar o‘rtasidagi axborot oqimini subyektiv ixtiyorga emas, balki qat'iy markazlashgan va o‘zgartirib bo‘lmaydigan mandatli ierarxik darajalar tizimiga bog‘laydi. Ushbu modelning matematik invariantlarini, dinamik holat o‘tishlarini va dastur kodini dastlabki bosqichdayoq avtomatlashtirilgan statik tahlil qilish (Static Security Analysis) mexanizmlarini tadqiq etish kiber-tahdidlarni amaliyotga ko‘chmasdan turib, loyihalash bosqichidayoq 100% holatda matematik isbotlangan holda (provable security) bartaraf etish imkonini beradi. Bu esa yuqori darajadagi maxfiylikka ega bo‘lgan davlat va korporativ axborot infratuzilmalarini barpo etishda fundamental va dolzarb ahamiyatga egadir.

1. Bell-LaPadula modelining matematik asosi va tarkibiy komponentlari

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

BLP modeli tizimni va undagi barcha operatsiyalarni mavhumlashtirish uchun qat'iy matematik to‘plamlarga tayanadi. Tizimning har qanday o‘zgarish holati quyidagi elementar to‘plamlar orqali aniqlanadi:

S = {s_1, s_2, …, s_n} - Subyektlar to‘plami (faol elementlar: foydalanuvchilar, jarayonlar).

O = {o_1, o_2, …, o_m} - Obyektlar to‘plami (passiv resurslar: fayllar, MB jadvallari).

R ={read, write, execute, append} - Foydalanish huquqlari (ruxsatnomalar) to‘plami.

Modelning o‘ziga xosligi - har bir subyekt va obyektga qat'iy **xavfsizlik darajasi (Security Clearance/Classification)** biriktirilishidir. Xavfsizlik darajalari qisman tartiblangan panjara (lattice) tuzilishiga ega bo‘lgan (L, ≤) to‘plamini hosil qiladi. Masalan:

Unclassified}<Confidential<Secret<Top Secret

Har bir subyekt $s \in S$ uchun uning ishonchlilik darajasi $f_S(s) \in L$ va har bir obyekt $o \in O$) uchun uning maxfiylik darajasi $f_O(o) \in L$ funksiyalari orqali belgilanadi.

2. Xavfsizlikning fundamental qoidalari

BLP modelida axborot faqat quyi darajadan yuqori darajaga qarab oqishi ruxsat etiladi. Buning uchun tizimda ikki ta asosiy xavfsizlik qoidasi qat'iy bajarilishi shart:

A. Oddiy xavfsizlik xossasi (Simple Security Property yoki "No Read Up")

Subyekt (s) obyekt (o) ni faqat va faqat uning xavfsizlik darajasi obyektning maxfiylik darajasidan yuqori yoki teng bo‘lgandagina o‘qiy oladi (read amali):

$$\forall\, s \in S, o \in O: (\text{read} \in A[s,o]) \Longrightarrow f_S(s) \geq f_O(o)$$

Mantiqiy mazmuni: Maxfiylik huquqi past bo‘lgan askar yuqori darajadagi maxfiy buyruqlarni o‘qiy olmaydi.

B. Yulduzcha xossasi (*-Property yoki "No Write Down")

Subyekt (s) obyekt (o) ga ma'lumotni faqat va faqat uning joriy xavfsizlik darajasi obyektning maxfiylik darajasidan quyi yoki teng bo‘lgandagina yozishi yoki qo‘shishi mumkin (write yoki append amali):

$$\forall\, s \in S, o \in O: (\text{write} \in A[s,o]) \Longrightarrow f_S(s) \leq f_O(o)$$

Mantiqiy mazmuni: “Top Secret” darajadagi general tasodifan yoki qasddan “Unclassified” (ommaviy) hujjat ichiga maxfiy ma'lumotlarni yozib qo‘ya olmaydi. Bu qoida tizimdagi Troyan otlari (Trojan Horses) orqali ma'lumotlarning quyi qatlamga sizdirilishini to‘liq bloklaydi.

3. Tizim dinamikasini ifodalovchi “Holatlar mashinasi” (State Machine) modeli

BLP modeli tizimni statik tuzilma sifatida emas, balki buyruqlar ta'sirida uzluksiz o‘zgarib boruvchi **Dinamik holatlar mashinasi (State Machine)** sifatida ifodalaydi.

Tizimning joriy holati $v \in V$ uchlik ko‘rinishida tavsiflanadi:

$$v=(b,M,f)$$

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

$b \subseteq S \times O \times R$ - Joriy faol aloqalar (current access set). Ya'ni ayni vaqtda qaysi subyekt qaysi obyekt ustida qanday amalni bajarayotganligini ko'rsatadi.

M - Foydalanish matritsasi (Access Matrix). Tizimdagi barcha ruxsat etilgan potentsial huquqlarni saqlaydi.

$f = (f_S, f_C, f_O)$ - Xavfsizlik funksiyalari to'plami (joriy va maksimal ruxsat etilgan darajalar).

Tizim holatining o'zgarishi RCF (Request-Decision-Transition) tsikli orqali amalga oshadi. Foydalanuvchi tizimga biron bir so'rov $q \in Q$ yuborganda, xavfsizlik yadrosi qaror $d \in \{allow, deny\}$ qabul qiladi va tizim yangi v' holatiga o'tadi:

$$\Sigma: V \times Q \rightarrow V \times D$$

Bu yerda:

Σ (Sigma) - Holatni o'zgartiruvchi o'tish funksiyasi (yoki operatori). U operatsion tizim yoki xavfsizlik yadrosining (Reference Monitor) mantiqiy algoritm hisoblanadi.

V(States) - Tizimning barcha mumkin bo'lgan holatlari to'plami. Tizimning har bir holati joriy faol aloqalar, ruxsatnomalar matritsasi va xavfsizlik darajalarini o'z ichiga oladi: $v = (b, M, f)$.

Q(Requests) - So'rovlar to'plami. Subyektlar tomonidan tizimga yuboriladigan amallar (masalan: open_file(read), create_object, close_file, change_clearance).

D(Decisions) - Qarorlar to'plami. Tizimning so'rovga beradigan yakuniy javobi. U odatda ikkita qiymatdan iborat bo'ladi: $D = \{yes, no\}$ yoki $D = \{allow, deny\}$.

Ushbu funksiya holatlar mashinasining (State Machine) asosi bo'lib, quyidagicha o'qiladi:

1. Kirish parametrlari ($V \times Q$): Funksiya joriy vaqtdagi tizim holatini ($v \in V$) va kelib tushgan so'rovni ($q \in Q$) qabul qiladi.

2. Chiqish parametrlari (\(V \times D\)): Ushbu so'rovni BLP modelining invariantlari (Simple property va *-property) asosida tekshirib, yangi holat ($v' \in V$) va unga mos qaror ($d \in D$) qaytaradi.

Buni funksiya ko'rinishida yozsak:

$$\Sigma(v,q)=(v',d)$$

Misol. Aytaylik, tizimda joriy holat v mavjud. Subyekt s (xavfsizlik darajasi: Secret) obyekt o ni (maxfiylik darajasi: Top Secret) o'qish uchun read so'rovini (q) yubordi.

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

Xavfsizlik yadrosi Σ funksiyasini ishga tushiradi:

1. **ekshiruv:** BLP modelining “No Read Up” qoidasiga ko‘ra, subyekt darajasi obyekt darajasidan katta yoki teng bo‘lishi kerak: $\mathbf{f_S(s) \geq f_O(o)}$. Bizda esa: **Secret <Top Secret**. Qoida buzildi!

2. **Natija Σ(v, q) = (v', d):**

– **Qaror (d):** no (rad etish).

– **Yangi holat v' :** Tizim holati o‘zgarmasdan joriy holatda qoladi **(v' = v)** , chunki ruxsat berilmadi va faol aloqalar to‘plamiga **(b)** hech narsa qo‘shilmadi.

Agar subyekt o‘zidan quyi darajadagi faylni o‘qishni so‘raganda edi:

– **Qaror (d):** yes (ruxsat).

– **Yangi holat (v'):** Tizim yangi **v'** holatiga o‘tadi, chunki faol aloqalar to‘plamiga yangi element qo‘shiladi: **b' = b ∪ {(s, o, read)}**.

Asosiy xavfsizlik teoremasi (BST) bilan bog‘liqligi. Ushbu Σ funksiyasi BLP modelining asosi bo‘lgan **Asosiy xavfsizlik teoremasini** (Basic Security Theorem) isbotlash uchun xizmat qiladi. Teoremaga ko‘ra: Agar tizimning boshlang‘ich holati v_0 xavfsiz bo‘lsa va tizimdagi barcha mumkin bo‘lgan holat o‘tish funksiyalari (Σ) faqat xavfsiz o‘tishlarni amalga oshirsa, u holda tizim har qanday so‘rovlar ketma-ketligidan keyin ham har doim xavfsiz holatda qoladi.

Matematik tilda bu invariant quyidagicha ifodalanadi:

$$\forall\ v \in V, q \in Q : (v \text{ is safe} \wedge \Sigma(v,q) = (v', d)) \Longrightarrow v' \text{ is safe}$$

Ushbu qat’iy funksiya Bell-LaPadula modelini statik qoidalar to‘plamidan dinamik va xavfsiz ishlashga qodir **operatsion tizim yadrosi arxitekturasiga** aylantiradigan asosiy mantiqiy mexanizmdir.

4. Axborot xavfsizligini Statik tekshirish (Static Security Analysis)

Bell-LaPadula (BLP) modelining mantiqiy to‘g‘riligini real dasturiy ilovalarga tatbiq etishdan oldin dastur kodini **Statik tekshirish (Static Security Analysis)** usuli qo‘llaniladi. Ushbu yondashuv dasturiy ta’minot ishga tushmasdan (runtime bosqichiga o‘tmasdan) turib, manba kodi (source code) ichidagi barcha o‘zgaruvchilar va ma’lumotlar oqimini (Information Flow) tahlil qiladi. Statik tahlilning asosiy maqsadi — yashirin kanallar yoki Troyan otlari orqali yuqori maxfiy qatlamdan quyi ommaviy qatlamga yo‘naltirilgan ruxsatsiz axborot oqimlarini (High-to-Low explicit/implicit flows) kompilyatsiya yoki linter tekshiruvi bosqichidayoq taqiqlashdir.

Zamonaviy dasturlash amaliyotida, xususan, Python ekotizimida ushbu jarayon **Atributlar asosidagi tiplash (Type Hinting)** va xavfsizlik metadata tahlilchilari yordamida amalga oshiriladi. Quyida BLP modelining Oddiy xavfsizlik xossasi (No Read Up) va *-xossasi (No Write Down) tamoyillarini dastur kodi darajasida tekshiruvchi formal Python modeli keltirilgan:

```
from enum import IntEnum
```

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

```
from typing import Generic, TypeVar, Any
class SecurityLevel(IntEnum):
UNCLASSIFIED = 1
CONFIDENTIAL = 2
SECRET = 3
TOP_SECRET = 4
T = TypeVar('T')
class SecureData(Generic[T]):
"""
BLP modelidagi obyekt va uning xavfsizlik darajasini
inkapsulyatsiya qiluvchi matematik klass.
"""
def __init__(self, value: T, level: SecurityLevel):
self._value = value
self.level = level
class SecurityKernel:
"""
Tizim xavfsizlik yadrosi (Reference Monitor).
Axborot oqimi qoidalarini statik va dinamik tekshiradi.
"""
@staticmethod
def read(subject_level: SecurityLevel, data: SecureData[Any]) -> Any:
# Simple Security Property: No Read Up
if subject_level < data.level:
raise PermissionError(
f"Xavfsizlik buzilishi! {subject_level.name} darajali subyekt "
f"{data.level.name} darajali ma'lumotni o'qiy olmaydi."
return data._value
@staticmethod
```

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

```
def write(subject_level: SecurityLevel, target: SecureData[Any], value: Any) -> None:
# *-Property: No Write Down (and No Read Up for context-strict write)
# Axborot oqimi faqat teng yoki yuqori darajaga yo'nalishi shart
if subject_level > target.level:
raise PermissionError(
f"Xavfsizlik buzilishi! {subject_level.name} darajali subyekt "
f"{target.level.name} darajali obyektga yo'za olmaydi (Write Down taqiqlangan)."
target._value = value
```

Ushbu arxitekturada axborot oqimining inflyatsiyasi va BLP qoidalariga muvofiqligi quyidagi ssenariylar orqali statik tahlil qilinadi:

```
# Tizim elementlarini initsializatsiya qilish
low_fayl = SecureData("Ommaviy hujjat matni", SecurityLevel.UNCLASSIFIED)
high_fayl = SecureData("Harbiy strategik reja", SecurityLevel.TOP_SECRET)
# 1-Ssenariy: Secret darajadagi subyekt harakatlari
user_level = SecurityLevel.SECRET
# A. O'qish amali (Read)
# Qonuniy axborot oqimi (Secret >= Unclassified) -> Muvaffaqiyatli
clear_text = SecurityKernel.read(user_level, low_fayl)
# Xavfsizlik buzilishi (Secret < Top_Secret) -> Statik tahlilda bloklanadi (No Read Up)
# security_kernel.read(user_level, high_fayl) -> PermissionError
# B. Yozish amali (Write)
# Qonuniy axborot oqimi (Secret <= Top_Secret) -> Muvaffaqiyatli
SecurityKernel.write(user_level, high_fayl, "Yangi maxfiy direktiva")
# Xavfsizlik buzilishi (Secret > Unclassified) -> Bloklanadi (No Write Down)
# SecurityKernel.write(user_level, low_fayl, "Maxfiy ma'lumot sizishi") -> PermissionError
```

Oqim tahlili (Data Flow Analysis) mexanizmi

Python mantiqiy modelida ko‘rinib turganidek, statik analizator SecurityKernel.write operatori bajarilayotganda source_level > target_level shartini tekshiradi. Agar subyekt o‘zining joriy darajasidan quyi bo‘lgan obyektga ma’lumot yozishga urinsa, axborot oqimi qat’iy ravishda uziladi.

Ushbu model asosi MyPy yoki Pyright kabi Python statik tahlil vositalarining maxsus plaginlari bilan integratsiya qilinadi. Natijada, dasturchi kodni yozish jarayonidayoq, o‘zgaruvchilar o‘rtasidagi

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

noto‘g‘ri o‘zlashtirishlar (low_var = high_var) linter tomonidan xatolik sifatida terminalga chiqariladi. Bu esa reaktiv tizimlarda maxfiy ma’lumotlarning tashqi muhitga chiqib ketish xavfini runtime bosqichiga yetmasdan turib nolga tushiradi.

Xulosa

Bell-LaPadula modeli ko‘p darajali xavfsizlik muhitlarida maxfiylikni ta’minlashning matematik jihatdan mukammal va isbotlangan namunasidir. Modelning “Holatlar mashinasi” kontseptsiyasi yordamida tizim dinamikasini boshqarish va xavfsizlik invariantlarini qat’iy nazorat qilish, murakkab kiber-infratuzilmalarda axborot sizib chiqish xavfini yo‘qotadi. Zamonaviy xavfsiz operatsion tizimlar (masalan, SE-Linux) va maxfiy ma’lumotlar bazalari arxitekturasini loyihalashda BLP modelining formal-mantiqiy asosi hamon ishonchli fundamental poydevor bo‘lib xizmat qilmoqda.

Foydalanilgan adabiyotlar

1. Bell, D. E., & LaPadula, L. J. (1973). Secure Computer Systems: Mathematical Foundations. Mitre Corp Technical Report.
2. McLean, J. (1987). Reasoning about security models. Proceedings of the IEEE Symposium on Security and Privacy, 113-131.