# 컴퓨터 보안정책을 기술하기 위한 객체-기반 시각 명세 언어 설계 및 구현

## (Design and Implementation of Object-based Visual Specification Language for Description Computer Security Policy)

강철범·김상욱

{zfjiang, swkim}@cs.knu.ac.kr

**1**.

,                                    .

,                                2

                                            3              -

                            .

                                                                    . 4

                    .                      5

                                        .

                            .

,                              .                2.

                            .

                        2.1

                    .

                                    ,          ,          ,              ,

            .                          .

                                                    .

                                        5                    .

                                        :

        .                                              .

                    ,                              .

            ,                          .                  :

                    .                                      .

                .                              (event) -        (condition) -

                            (action)                      .

                    -                              :

                                                    .

                                        :

        .              -

                                        .

,                          ,              :

            .

                                UML[1]

OCL[2]                              .

2.2                                                             .

                                         Ponder[3,4],                                              .
PDL[5], LaSCO[6], PPL[7,8]              .                    LaSCO


                                 .              .

   Ponder:                                                    ,
                                                       .
                                         PPL(Path-based  Policy  Language):


                                                                         .
                                  . Ponder                      ,
subject              ,                                                          .
                             . subject                  PPL
              target
       ,                           . subject
    targe                                      .
                             .            Ponder
                                        2. 3

           .                                                          .
   PDL(Policy Description Language):  Bell-Lab              ,
                                                                    .
     . PDL                          .                 ,                                ,
                                             ,        ,        ,
                                  -        -
              .
   PDL                                      .                .
                                          ,
              .                                              .

        .                                                                -
   LaSCO(Language for Security Constraints on                             .
Object):
                                        3.          -
              . LaSCO

．　　　　　　　　　　　　　．

Unified  Modeling  Language(UML)[7]

．　　　　　　　　　　　　　．

(Class

．　　1　　Diagram)

(State  Diagram)

．　　　　　．
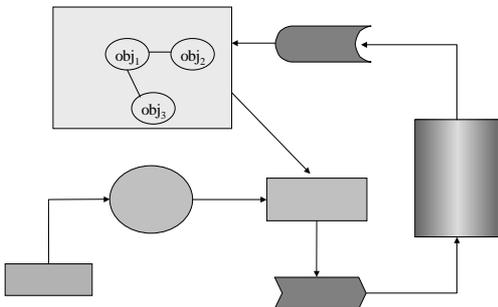
**3.1.1.**

．　　　　　　　．



．

，

，

．　　2

Object

．Object

security_level　　　　　　　　name
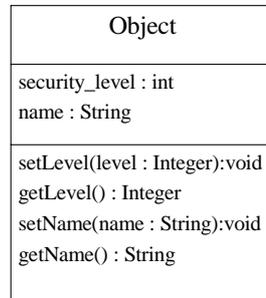
(　　1)

．



| Object |
|---|
| security_level : int<br>name : String |
| setLevel(level : Integer):void<br>getLevel() : Integer<br>setName(name : String):void<br>getName() : String |

，

，

．

，

，

．

(　　2) Object

3.1　　　　　　**3.1.2.**

，

．

(inheritance),                                                      . AND
(aggregation),        (dependency)                              OR
        .                                                                        .

        .                                                      .

                                    .                          .    **4**

                            .                          .



(      4)
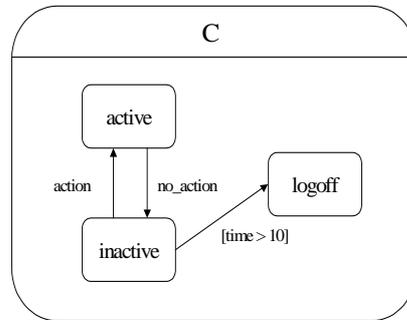
. File            Directory

  . File System          File      , File
        Directory
            File          Directory
File System          File                      .   3. 2
User          File

              editing                                                      .

  . editing            File          read(),                                    .
write(),  delete()                      .                                          .
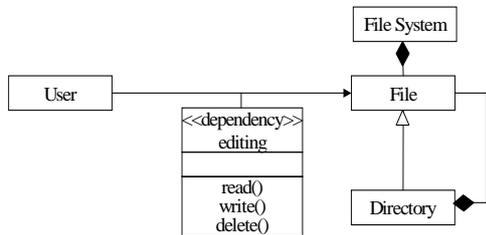


(      3)                                          OCL(Object  Constraints  Language)
                                                                      .
**3.1.3**                                            **3.2.1.**
                                                                        (instance)
                                              ,                          ,
**3.1.3**                                                  .

            .                                                          .

                  AND        OR   "objectName : className"                      .

C
active
action        no_action        logoff
inactive        [time > 10]

File System
User        File
<<dependency>>
editing
read()
write()
delete()
Directory

CompositePolicy ::= CompositePolicy ( logicalOperator CompositePol icy)?
　　　　　 |"{" CompositePolicy "}" | Policy
Policy ::= "[" "on" (Event |SeqOperation |"any" ) "]" "[" Conditions "]" )?
　　　　　PolicyType SeqOperation ( "[" Constraints "]" )?
PolicyType::= "@" | "#" | "!" | ">>"
Event ::= string
SeqOperation ::= Operation ( " " SeqOperation )?
Conditions ::= oclExpression
Constratins ::= oclExpression

.

.

"$"

.　　　　　, "a = $dd"

.

.

AND　　OR

( 　5)　　　　　　EBNF [ 8]

.

Event

Event　　action　　　　.

Implicit Event

,

,

. action

,

from　 to　　　.　　　　　 from

action　　　, from, to

to

. Condition　　　/

.　　　　　　Default,

,　　　(predicate),

Obligation, Constraint　　　　　　　　　.

.　　　　OCL

Default

. Obligation

Boolean, Integer, Real, String

Set, Bag, Sequence, Collection

Constraint

.

"@"

.

"#"　　　　 , "!"　　　　　 , ">>"

.

.

**3.2.2.**

Constraints　　action

action

.

.

condition

(pre-condition)

. condition

,　　　　 ,　　　　　 ,

. condition

.　　　　EBNF[8]　　　　　5

OCL　　　　　　　　　 .

.

6　"

."

, . File
f User
u u f
editing . 7

{u.security_level >= f.security_level}editing XML
.

XML XML
.

OCL

. 8

XML OCL
XML
.



[ **on any** ] [u.security_level >= f.security_level] @editing

( 6)

## 3. 3

XML [9].
XML

.

```
<Policy>
 <Object>            </Object>
 <Event>             </Event>
 <PreCondition>      </PreCondition>
 <PolicyAction>      </PolicyAction>
 <Constraint>         </Constraint>
</Policy>
```

( 8) XML

. 4.

## 4. 1

XML

Linux .



( 7) XML

9 .

，　　　　　　　　，　　，
．　　　　　　　　　OCL

．　　　　　　　　．

．
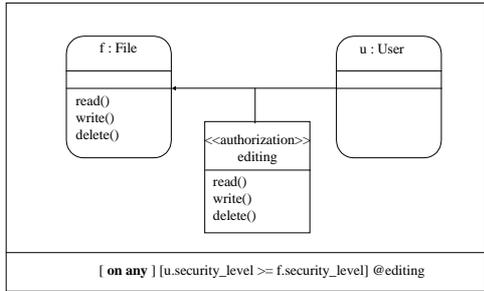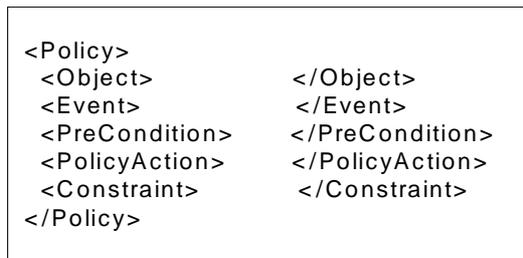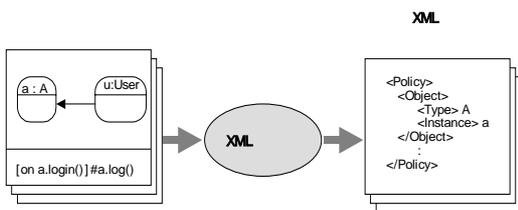
OCL　　　　　OCL
XML　　　　　　　　XML　　　　　　　　　　　　　．Syntactic
．XML　　　　　　　analysis　　　OCL　　　EBNF(Extended
　　　　　　　　　　Backus-Naur-Form)
．



．



( 　　9)

(　　10)

## 4.2
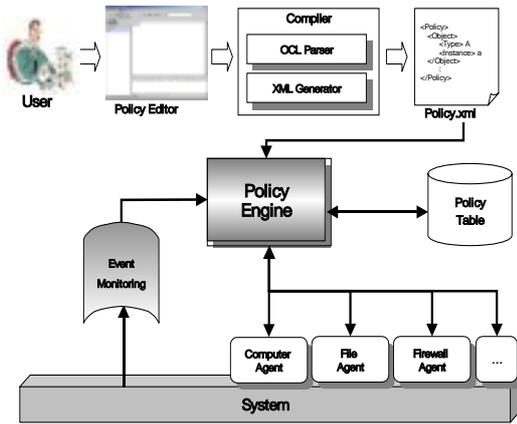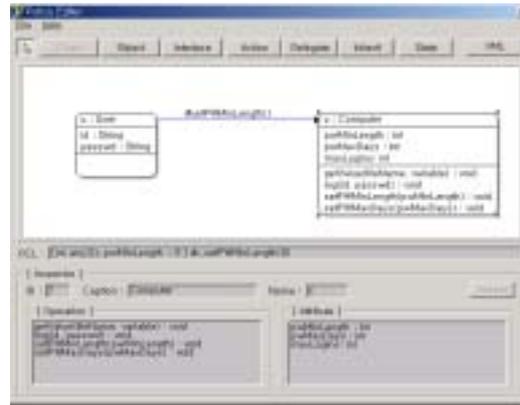
10
．Object
Interface　　　　　　　　　　　．
Action
Delegate　　　　　　　　　Inherit
．States
．XML
OCL
XML　　　　　　．
OCL
EBNF
(Syntax Analyze)　　　　　．
(Lexical analysis)
(Syntactic analysis)　　　　　．
OCL　　　　　　　　　　　　　．

## 4.3

．　　　11
，　　　　，　　　　，
．

XML
ObjectType, Event, Operator, LeftOperand,
RightOperand, PolicyAction
(PolicyEntry)
．

ObjectType
．

，

GetValue()

any          GetValue()

GetValue()



(    11)

XML
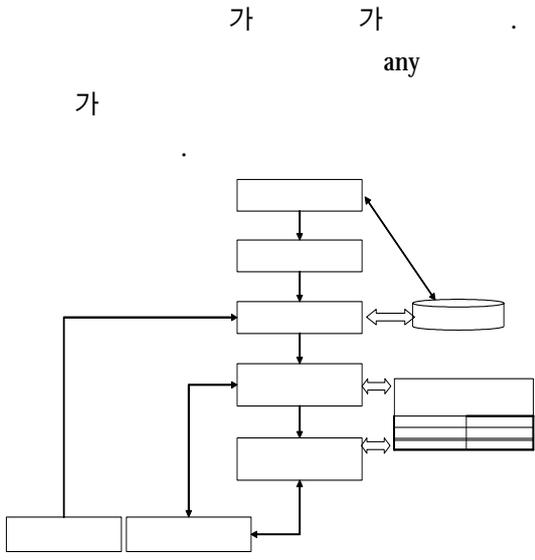
ObjectType, Event, Operator, LeftOperand,
RightOperand, PolicyAction

ObjectType

any

4. 4

GetLeftOperand(),    GetRightOperand()

Linux

12

IP

155.230.159.27                 Reject
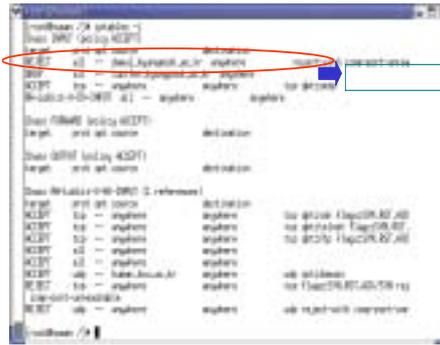
.

(  12)

Linux        IP-tables
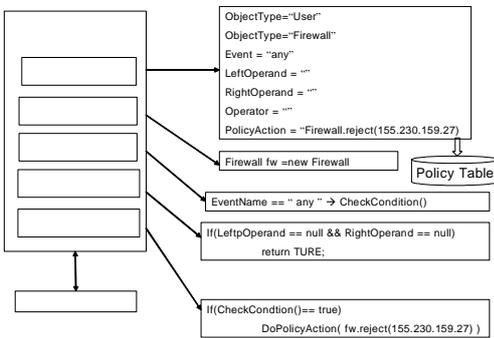
.
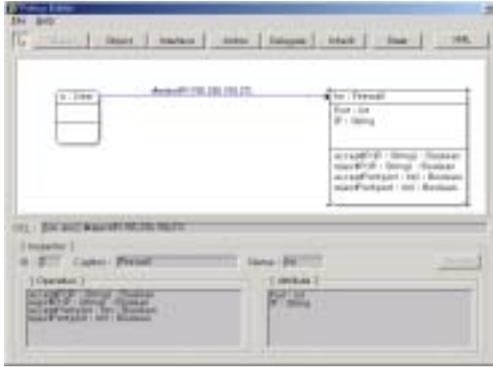
IP-tables

IP

"iptables -A INPUT -s 155.230.159.27 -j REJECT"         .

ObjectType="User"
ObjectType="Firewall"
Event = "any"
LeftOperand = ""
RightOperand = ""
Operator = ""
PolicyAction = "Firewall.reject(155.230.159.27)

Firewall fw =new Firewall

Policy Table

EventName == " any " → CheckCondition()

If(LeftpOperand == null && RightOperand == null)
     return TURE:

If(CheckCondtion()== true)
     DoPolicyAction( fw.reject(155.230.159.27) )

(  13)

14            IP-tables

.

.

(  14)

4.5

.

,

.

(  1)

| | | | | | |
|---|---|---|---|---|---|
| Ponder | O | O | O | O | O |
| PDL | | O | | | |
| LaSCO | O | | O | | |
| PPL | O | O | | O | |
| **OVSPSL** | **O** | **O** | **O** | **O** | **O** |

1                    -

(Object-based Visual

Security Policy Specification Language)　　　　　　.

OVSPSL　　　　　　　　　　　　　　　　　　-

　　　　　　　.　　　　　　　　　　　　[12]

141

,　　　　　　　　　　　　.

,

5.

/

.　　　　　　　　　　　-

2 OVSPSL

.

.

UML

( 2)

OCL

OVSPSL　　　　　　.

OVSPSL

,　　　　,　　　　,　　　　,

| | | | | | |
|---|---|---|---|---|---|
| Ponder | O | O | O | O | |
| PDL | O | | O | | |
| LaSCO | O | O | | O | O |
| PPL | O | | O | O | |
| **OVSPSL** | **O** | **O** | **O** | **O** | **O** |

.

.

2　　　　　　　　Ponder

.

.

-

. OVSPSL

.

[1] OMG, UML specification 1.5, http://www.omg.org/cgi-bin/doc?formal/03-03-01, Mar, 2003.

[2] OMG, OCL specification 2.0, http://www.omg.org/cgi-bin/doc?ptc/2003-10-14, Mar, 2003

[3] N. Damianou, "Ponder: A Language for Specifying Security and Management Policies for Distributed Systems," Workshop on Policies for Distributed Systems and Networks, Bristol UK, pp. 18-39, Jan. 2001.

[4] N. Damianou, "The Ponder Policy Specification Language," Workshop on Policies for Distributed Systems and Networks, Bristol UK, Jan. 2001.

[5] J. Lobo, R. Bhatia, "A Policy Description Language," American Association for Artificial Intelligence, Orlando, US, 1999.

[6] J. Hoagland, A. Pandey, "Security Policy Specification Using a Graphical Approach," Technical Report CSE-98-3, U.C.Davis, 1998.

[7] G. Stone, "Path-based Policy Language," Naval Postgraduate School, Monterey, CA, Manuscript in Preparation, 2001.

[8] Stone, G. N, Lundy, G. G. Xie. "Network Policy Languages: A Survey and a New Approach," IEEE Network, Vol.15, No.1, pp.10-21, Jan./Feb. 2001.

[9] http://www.xml.org

[10] XML, "Understanding XML Schema", http://msdn.microsoft.com/webservices/understanding/xmlfundamentals/default.aspx?pull=/library/en-us/dnxml/html/understandxsd.asp

[11] Moffett, J. D. , M. s. Sloman. "Policy Hierarchies for Distributed Systems Management," IEEE JSAC Special Issue on Network Management, Vol.11, pp.1404-1414, Dec. 1993.

[12] C. C. Wood, Information Security Policies Made Easy, Pentasafe Security Technologies, May. 2001.

1997 ~2001

( )

2001 ~2003

( )

2003 ~

: ,  ,

1975 ~1979

( )

1979 ~1981

( )

1981 ~1989

( )

1988 ~

: ,