# System Health Monitoring
# and
# Proactive Response Activation

Alireza Shameli Sendi
Michel Dagenais

***DORSAL***

*Dec 9, 2011*
*École Polytechnique, Montreal*

# Content

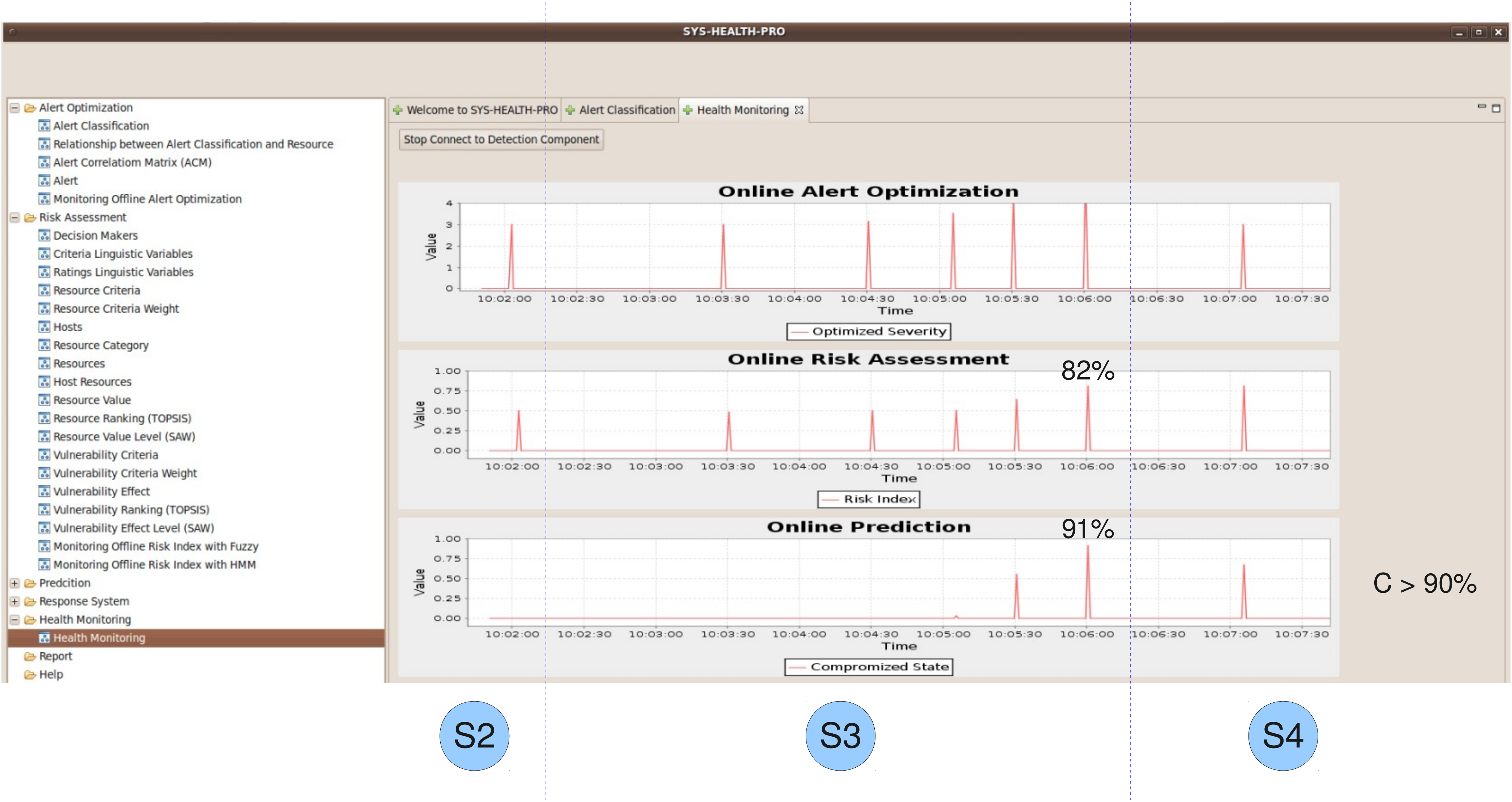
- Scenario of multi-step attack
- Result of risk assessment and prediction
- New architecture of IRS
  - Logical network model of IRS
  - Evaluation criteria
  - Response decision tree
  - Blocking on firewall
  - Decision making table
  - System scenario
  - Results
- Conclusion and Future work
- References

# Scenario of Multi-step attack

| Phase | Name | Time |
|---|---|---|
| 1 | Probing | 10:00 to 10:01 |
| 2 | Bruteforce username and password | 10:01 to 10:03 |
| 3 | Find vulnerabilities | 10:03 to 10:06 |
| 4 | Establish a reverse shell | 10:06 to 10:08 |

- Eventually, the attacker finds 192.168.10.2/test.php?cmd=id
- Attack type:
  - HTTP_Bruteforce_Password
  - HTTP_Vulnerability_Exploit
  - Reverse_Shell

# Result of Risk Assessment and Prediction

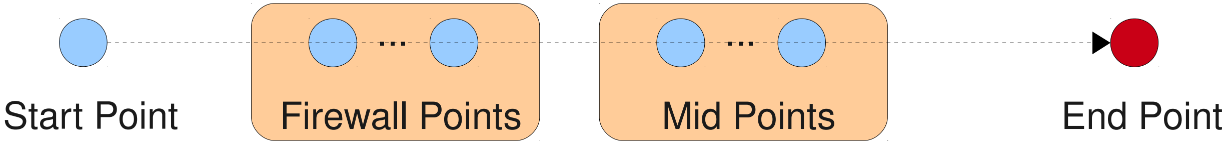


SYS-HEALTH-PRO

- Alert Optimization
  - Alert Classification
  - Relationship between Alert Classification and Resource
  - Alert Correlatiom Matrix (ACM)
  - Alert
  - Monitoring Offline Alert Optimization
- Risk Assessment
  - Decision Makers
  - Criteria Linguistic Variables
  - Ratings Linguistic Variables
  - Resource Criteria
  - Resource Criteria Weight
  - Hosts
  - Resource Category
  - Resources
  - Host Resources
  - Resource Value
  - Resource Ranking (TOPSIS)
  - Resource Value Level (SAW)
  - Vulnerability Criteria
  - Vulnerability Criteria Weight
  - Vulnerability Effect
  - Vulnerability Ranking (TOPSIS)
  - Vulnerability Effect Level (SAW)
  - Monitoring Offline Risk Index with Fuzzy
  - Monitoring Offline Risk Index with HMM
- Predcition
- Response System
- Health Monitoring
  - Health Monitoring
- Report
- Help

# New Architecture of IRS

- Supports dynamic evaluation of "***Response Cost***"
  - Account for the user's need in terms of quality of services (QoS)
  - Account the dependencies of critical processes
- Supports "***Attack Path***" technique
  - Find the best locations where to apply responses, with the lowest penalty cost

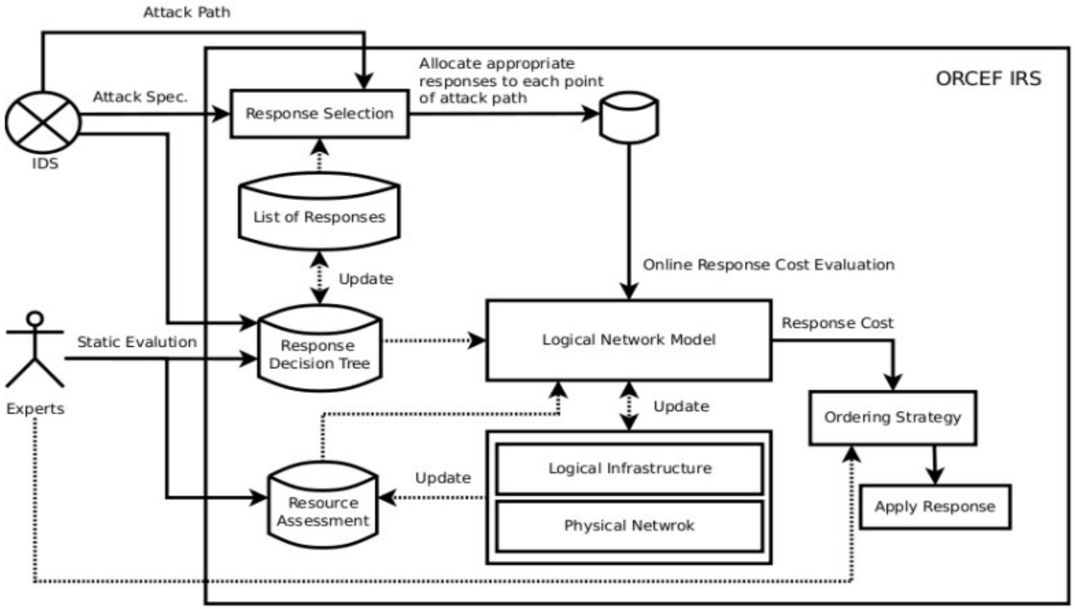


Start Point

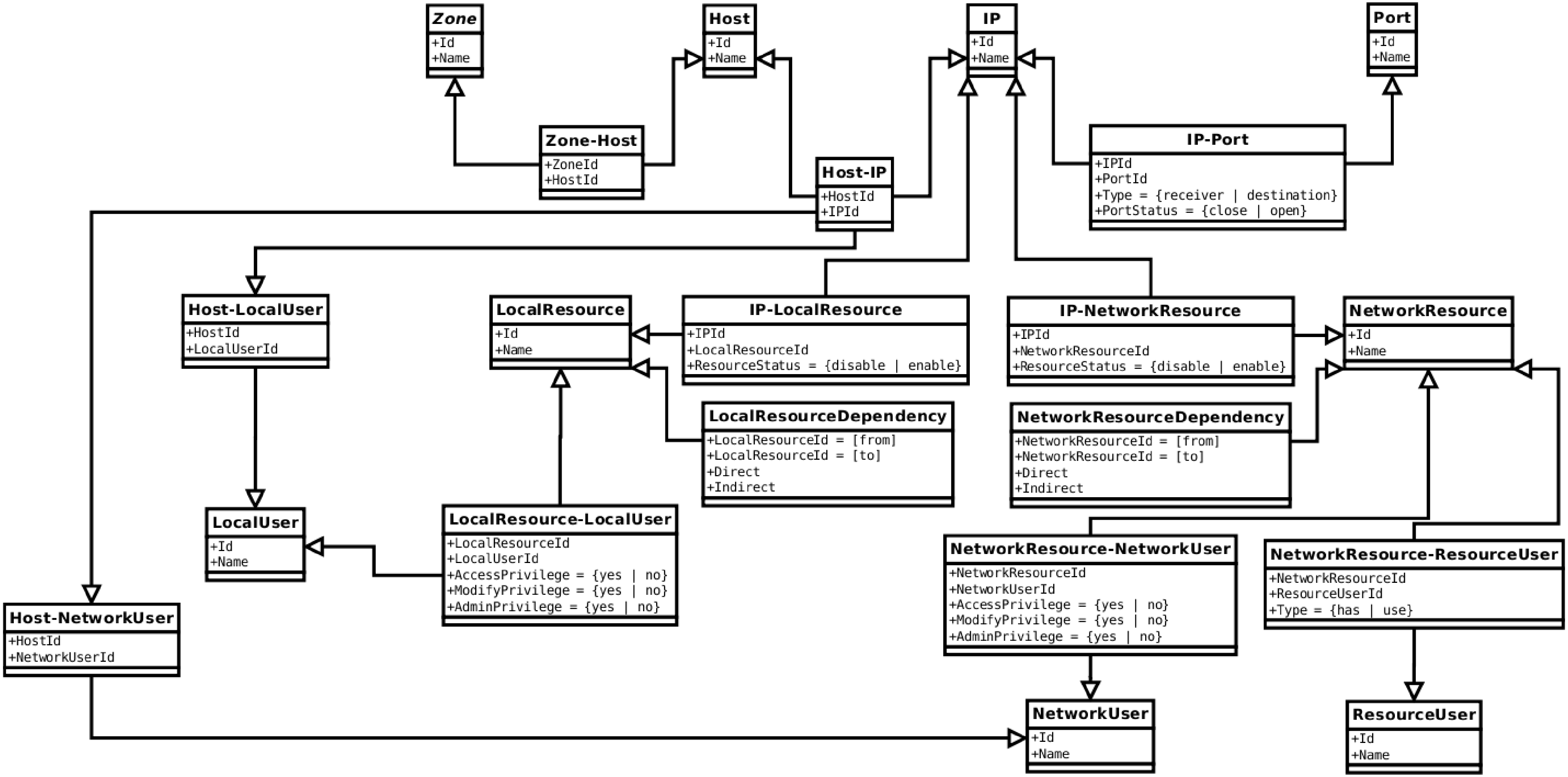
Firewall Points

Mid Points

End Point



# Logical Network Model of IRS



**Zone**
+Id
+Name

**Host**
+Id
+Name

**IP**
+Id
+Name

**Port**
+Id
+Name

**Zone-Host**
+ZoneId
+HostId

**Host-IP**
+HostId
+IPId

**IP-Port**
+IPId
+PortId
+Type = {receiver | destination}
+PortStatus = {close | open}

**Host-LocalUser**
+HostId
+LocalUserId

**LocalResource**
+Id
+Name

**IP-LocalResource**
+IPId
+LocalResourceId
+ResourceStatus = {disable | enable}

**IP-NetworkResource**
+IPId
+NetworkResourceId
+ResourceStatus = {disable | enable}

**NetworkResource**
+Id
+Name

**LocalResourceDependency**
+LocalResourceId = [from]
+LocalResourceId = [to]
+Direct
+Indirect

**NetworkResourceDependency**
+NetworkResourceId = [from]
+NetworkResourceId = [to]
+Direct
+Indirect

**LocalUser**
+Id
+Name

**LocalResource-LocalUser**
+LocalResourceId
+LocalUserId
+AccessPrivilege = {yes | no}
+ModifyPrivilege = {yes | no}
+AdminPrivilege = {yes | no}

**NetworkResource-NetworkUser**
+NetworkResourceId
+NetworkUserId
+AccessPrivilege = {yes | no}
+ModifyPrivilege = {yes | no}
+AdminPrivilege = {yes | no}

**NetworkResource-ResourceUser**
+NetworkResourceId
+ResourceUserId
+Type = {has | use}

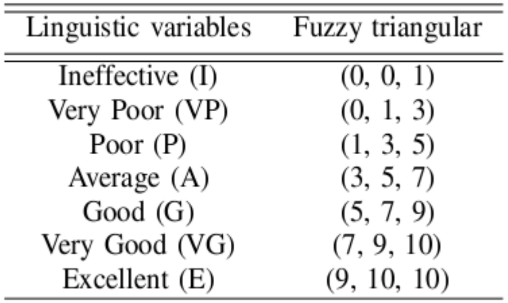
**Host-NetworkUser**
+HostId
+NetworkUserId

**NetworkUser**
+Id
+Name

**ResourceUser**
+Id
+Name

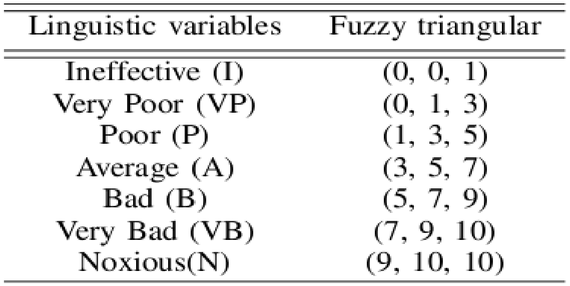
# Evaluation Criteria

- Positive effects
  - Positive Confidentiality (P_C)
  - Positive Integrity (P_I)
  - Positive Availability (P_A)
  - Positive Speed (P_S)



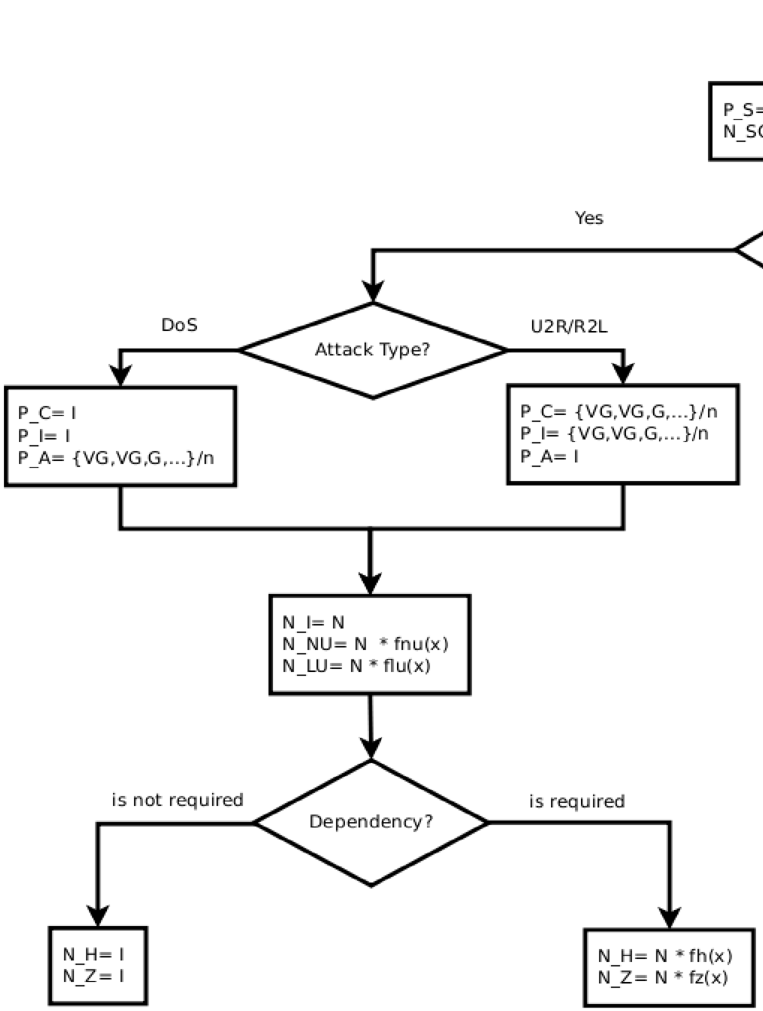
| Linguistic variables | Fuzzy triangular |
|---|---|
| Ineffective (I) | (0, 0, 1) |
| Very Poor (VP) | (0, 1, 3) |
| Poor (P) | (1, 3, 5) |
| Average (A) | (3, 5, 7) |
| Good (G) | (5, 7, 9) |
| Very Good (VG) | (7, 9, 10) |
| Excellent (E) | (9, 10, 10) |

- Negative Impact
  - Negative Itself (N_I)
  - Negative Host (N_H)
  - Negative Zone (N_Z)
  - Negative Network User (N_NU)
  - Negative Local User (N_LU)
  - Negative Setup Cost(N_SC)



| Linguistic variables | Fuzzy triangular |
|---|---|
| Ineffective (I) | (0, 0, 1) |
| Very Poor (VP) | (0, 1, 3) |
| Poor (P) | (1, 3, 5) |
| Average (A) | (3, 5, 7) |
| Bad (B) | (5, 7, 9) |
| Very Bad (VB) | (7, 9, 10) |
| Noxious(N) | (9, 10, 10) |

# Response Decision Tree



x= Resource

P_S= {E,E,E, ...}/n
N_SC= {P,VP,P,...}/n

Known?

Yes

No

P_C= {VG,VG,G,..}/n
P_I= {G,VG,G,...}/n
P_A= {VG,VG,G,...}/n
N_I= I
N_H= I
N_Z= I
N_NU= I
N_LU= I
N_SC= I

Attack Type?

DoS

U2R/R2L

P_C= I
P_I= I
P_A= {VG,VG,G,...}/n

P_C= {VG,VG,G,...}/n
P_I= {VG,VG,G,...}/n
P_A= I

N_I= N
N_NU= N  * fnu(x)
N_LU= N * flu(x)

Dependency?

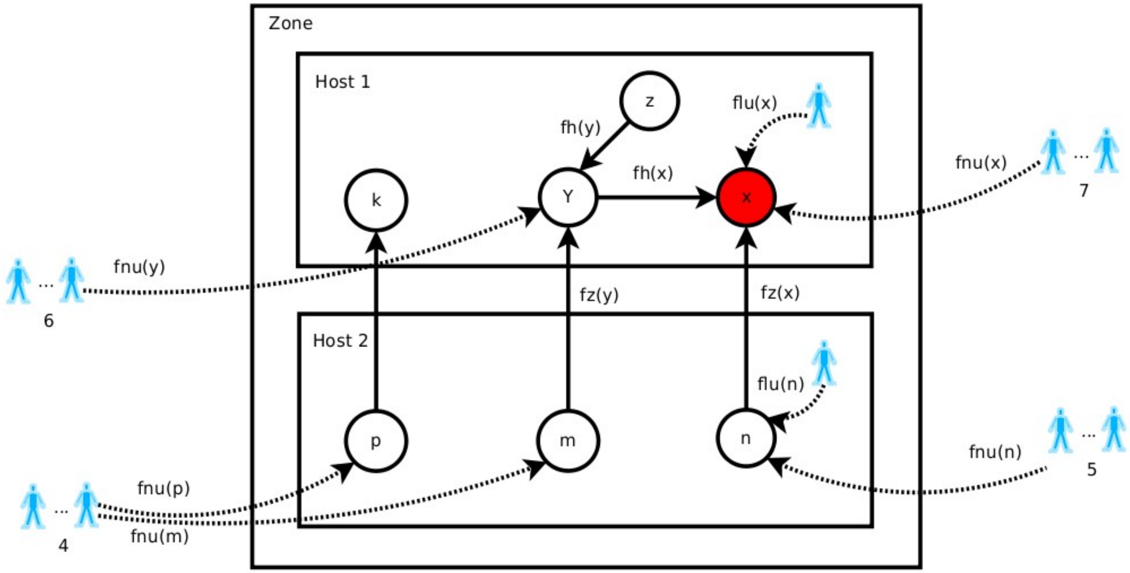
is not required

is required

N_H= I
N_Z= I

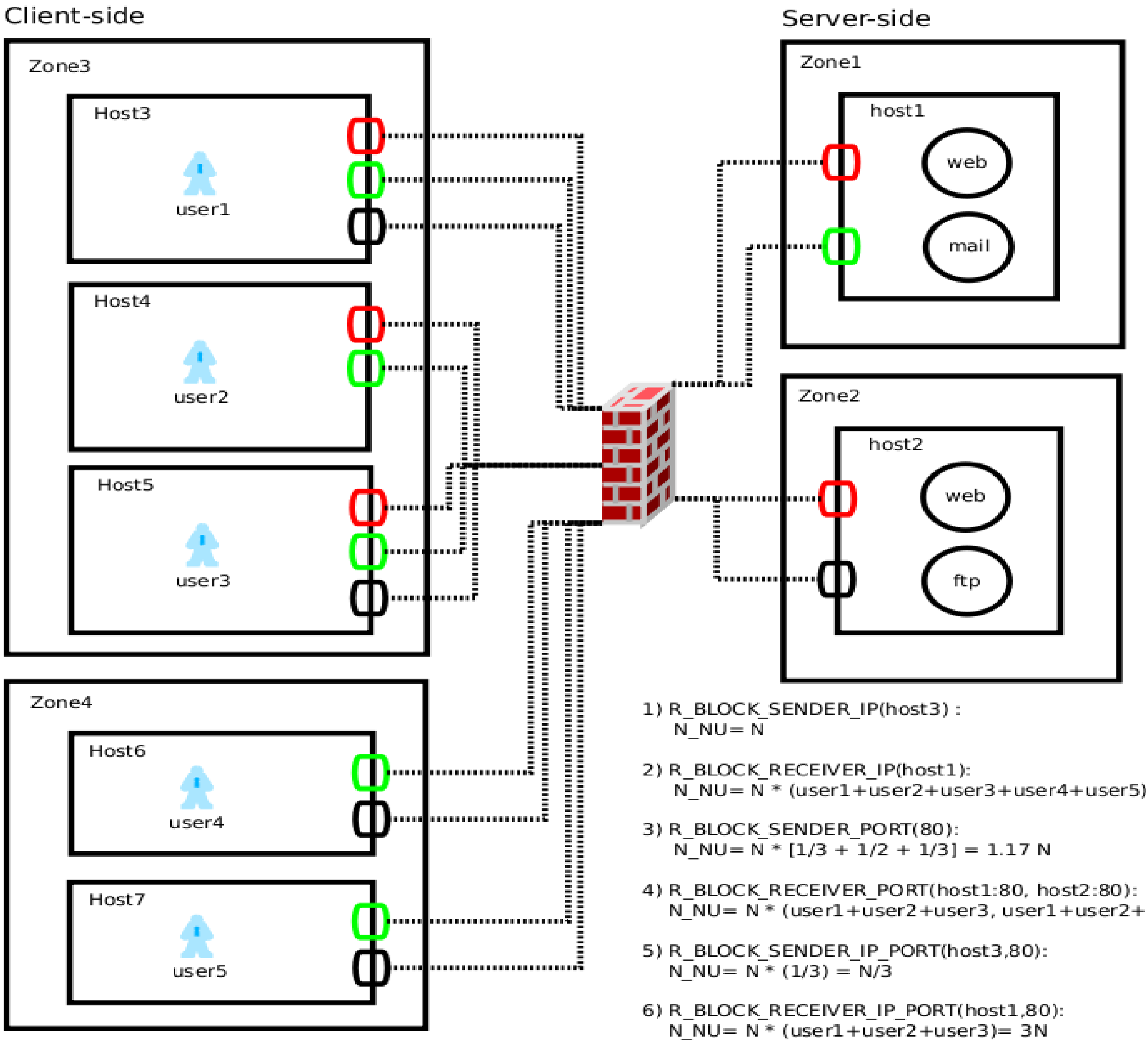
N_H= N * fh(x)
N_Z= N * fz(x)

Kill process decision tree



1) fh(x) = Direct + Indirect = {y} + {z} = 2
2) fz(x) = Direct + Indirect = {n} + {m} = 2
3) fnu(x) = Direct + Indirect = {x:7} + {n:5, m:4, y:6} = 22
4) flu(x) = Direct + Indirect= {x:1} + {n:1} = 2

# Blocking on Firewall



1) R_BLOCK_SENDER_IP(host3) :
N_NU= N

2) R_BLOCK_RECEIVER_IP(host1):
N_NU= N * (user1+user2+user3+user4+user5) = 5N

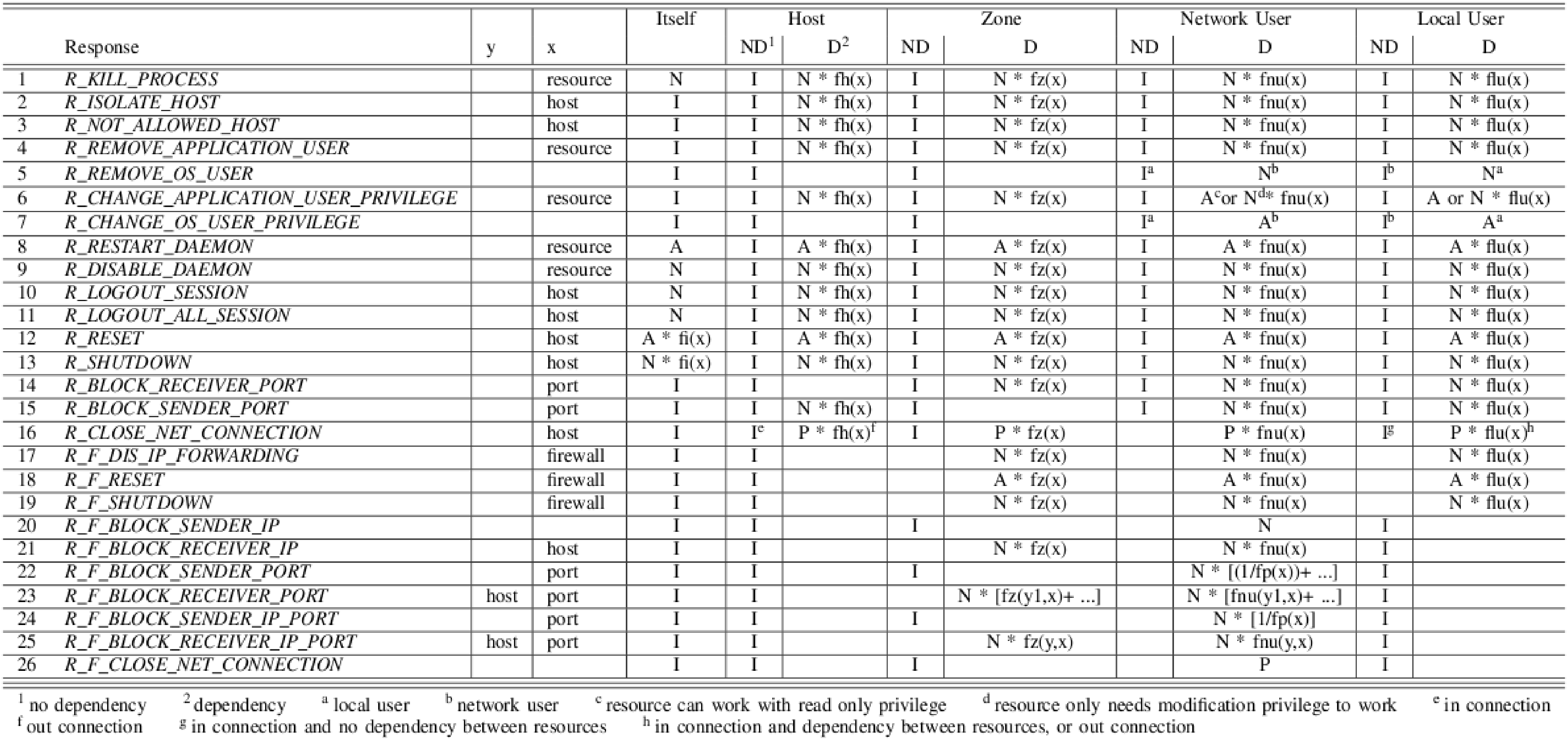
3) R_BLOCK_SENDER_PORT(80):
N_NU= N * [1/3 + 1/2 + 1/3] = 1.17 N

4) R_BLOCK_RECEIVER_PORT(host1:80, host2:80):
N_NU= N * (user1+user2+user3, user1+user2+user3) = 6N

5) R_BLOCK_SENDER_IP_PORT(host3,80):
N_NU= N * (1/3) = N/3

6) R_BLOCK_RECEIVER_IP_PORT(host1,80):
N_NU= N * (user1+user2+user3)= 3N

# Decision making table to calculate negative criteria



| | | | | Itself | Host | | Zone | | Network User | | Local User | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Response | y | x | | ND[1] | D[2] | ND | D | ND | D | ND | D |
| 1 | *R_KILL_PROCESS* | | resource | N | I | N * fh(x) | I | N * fz(x) | I | N * fnu(x) | I | N * flu(x) |
| 2 | *R_ISOLATE_HOST* | | host | I | I | N * fh(x) | I | N * fz(x) | I | N * fnu(x) | I | N * flu(x) |
| 3 | *R_NOT_ALLOWED_HOST* | | host | I | I | N * fh(x) | I | N * fz(x) | I | N * fnu(x) | I | N * flu(x) |
| 4 | *R_REMOVE_APPLICATION_USER* | | resource | I | I | N * fh(x) | I | N * fz(x) | I | N * fnu(x) | I | N * flu(x) |
| 5 | *R_REMOVE_OS_USER* | | | I | I | | I | | I[a] | N[b] | I[b] | N[a] |
| 6 | *R_CHANGE_APPLICATION_USER_PRIVILEGE* | | resource | I | I | N * fh(x) | I | N * fz(x) | I | A[c]or N[d]* fnu(x) | I | A or N * flu(x) |
| 7 | *R_CHANGE_OS_USER_PRIVILEGE* | | | I | I | | I | | I[a] | A[b] | I[b] | A[a] |
| 8 | *R_RESTART_DAEMON* | | resource | A | I | A * fh(x) | I | A * fz(x) | I | A * fnu(x) | I | A * flu(x) |
| 9 | *R_DISABLE_DAEMON* | | resource | N | I | N * fh(x) | I | N * fz(x) | I | N * fnu(x) | I | N * flu(x) |
| 10 | *R_LOGOUT_SESSION* | | host | N | I | N * fh(x) | I | N * fz(x) | I | N * fnu(x) | I | N * flu(x) |
| 11 | *R_LOGOUT_ALL_SESSION* | | host | N | I | N * fh(x) | I | N * fz(x) | I | N * fnu(x) | I | N * flu(x) |
| 12 | *R_RESET* | | host | A * fi(x) | I | A * fh(x) | I | A * fz(x) | I | A * fnu(x) | I | A * flu(x) |
| 13 | *R_SHUTDOWN* | | host | N * fi(x) | I | N * fh(x) | I | N * fz(x) | I | N * fnu(x) | I | N * flu(x) |
| 14 | *R_BLOCK_RECEIVER_PORT* | | port | I | I | | I | N * fz(x) | I | N * fnu(x) | I | N * flu(x) |
| 15 | *R_BLOCK_SENDER_PORT* | | port | I | I | N * fh(x) | I | | I | N * fnu(x) | I | N * flu(x) |
| 16 | *R_CLOSE_NET_CONNECTION* | | host | I | I[e] | P * fh(x)[f] | I | P * fz(x) | | P * fnu(x) | I[g] | P * flu(x)[h] |
| 17 | *R_F_DIS_IP_FORWARDING* | | firewall | I | I | | | N * fz(x) | | N * fnu(x) | | N * flu(x) |
| 18 | *R_F_RESET* | | firewall | I | I | | | A * fz(x) | | A * fnu(x) | | A * flu(x) |
| 19 | *R_F_SHUTDOWN* | | firewall | I | I | | | N * fz(x) | | N * fnu(x) | | N * flu(x) |
| 20 | *R_F_BLOCK_SENDER_IP* | | | I | I | | I | | | N | I | |
| 21 | *R_F_BLOCK_RECEIVER_IP* | | host | I | I | | | N * fz(x) | | N * fnu(x) | I | |
| 22 | *R_F_BLOCK_SENDER_PORT* | | port | I | I | | I | | | N * [(1/fp(x))+ ...] | I | |
| 23 | *R_F_BLOCK_RECEIVER_PORT* | host | port | I | I | | | N * [fz(y1,x)+ ...] | | N * [fnu(y1,x)+ ...] | I | |
| 24 | *R_F_BLOCK_SENDER_IP_PORT* | | port | I | I | | I | | | N * [1/fp(x)] | I | |
| 25 | *R_F_BLOCK_RECEIVER_IP_PORT* | host | port | I | I | | | N * fz(y,x) | | N * fnu(y,x) | I | |
| 26 | *R_F_CLOSE_NET_CONNECTION* | | | I | I | | I | | | P | I | |

[1] no dependency [2] dependency [a] local user [b] network user [c] resource can work with read only privilege [d] resource only needs modification privilege to work [e] in connection
[f] out connection [g] in connection and no dependency between resources [h] in connection and dependency between resources, or out connection

# System Scenario

## The number of online user

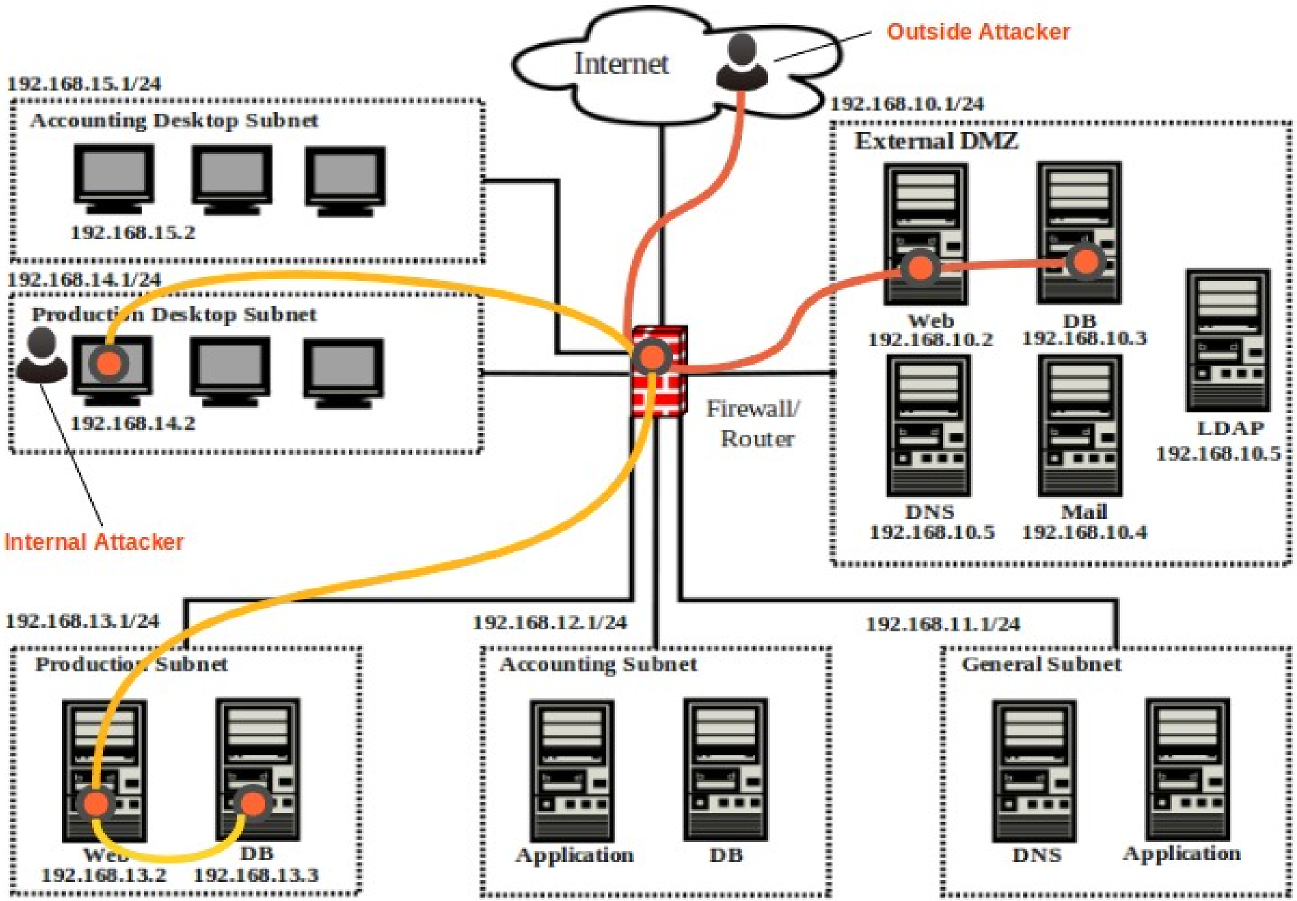
| Type | No. |
|---|---|
| Internal email user | 46 |
| Outside email user | 4 |
| Internal web user | 46 |
| Outside web user | 54 |
| Production software user | 23 |
| Local user | 11 |
| Remote admin user | 1 |
| MySQL user | 2 |

## Attack damage cost

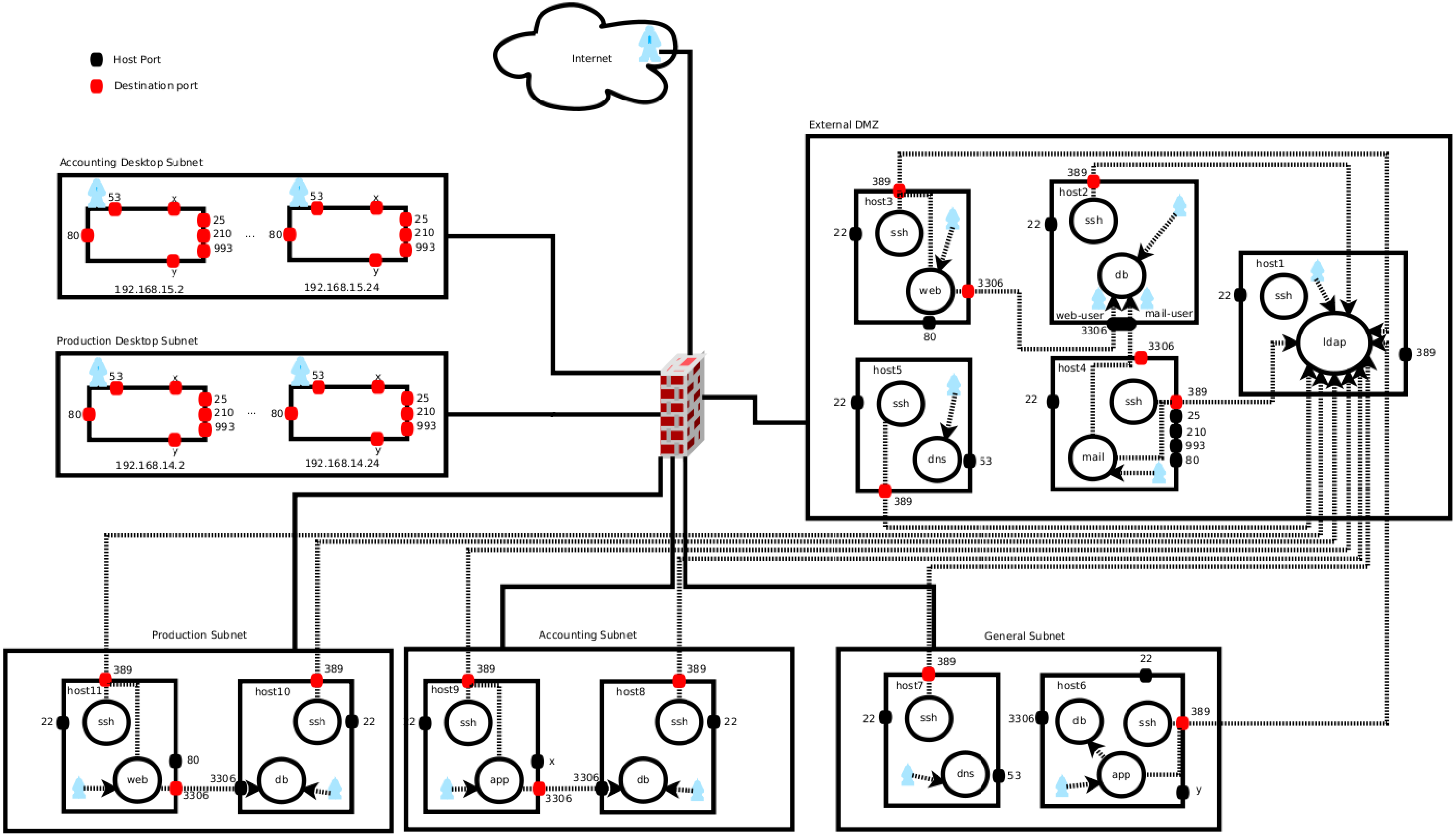
| Type | Cost |
|---|---|
| U2R | 100 |
| R2L | 60 |
| DoS | 35 |
| PROBE | 5 |

## Resource value

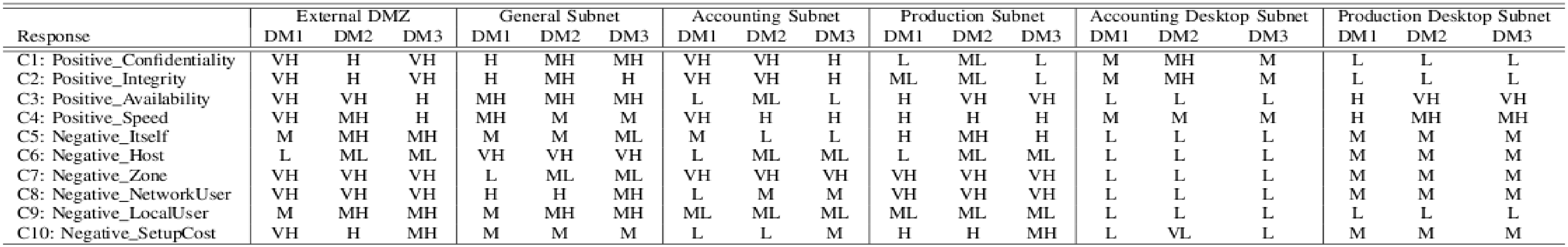
| Name | Fuzzification | Defuzzification | Scale %100 |
|---|---|---|---|
| DMZ.Web | (1.64,2.08,2.43) | 2.06 | 81 |
| DMZ.DB | (1.97,2.31,2.47) | 2.26 | 90 |
| Production.Web | (1.54,1.90,2.25) | 1.88 | 74 |
| Production.DB | (1.76,2.14,2.37) | 2.10 | 83 |



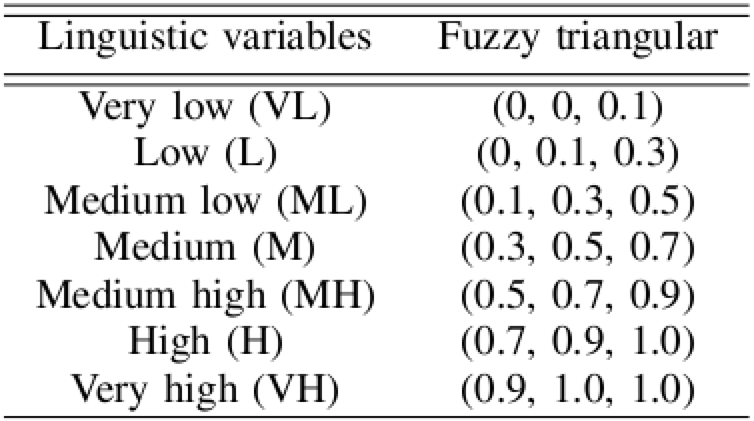
# Services Dependency



# Step1 ) Importance weight of criteria

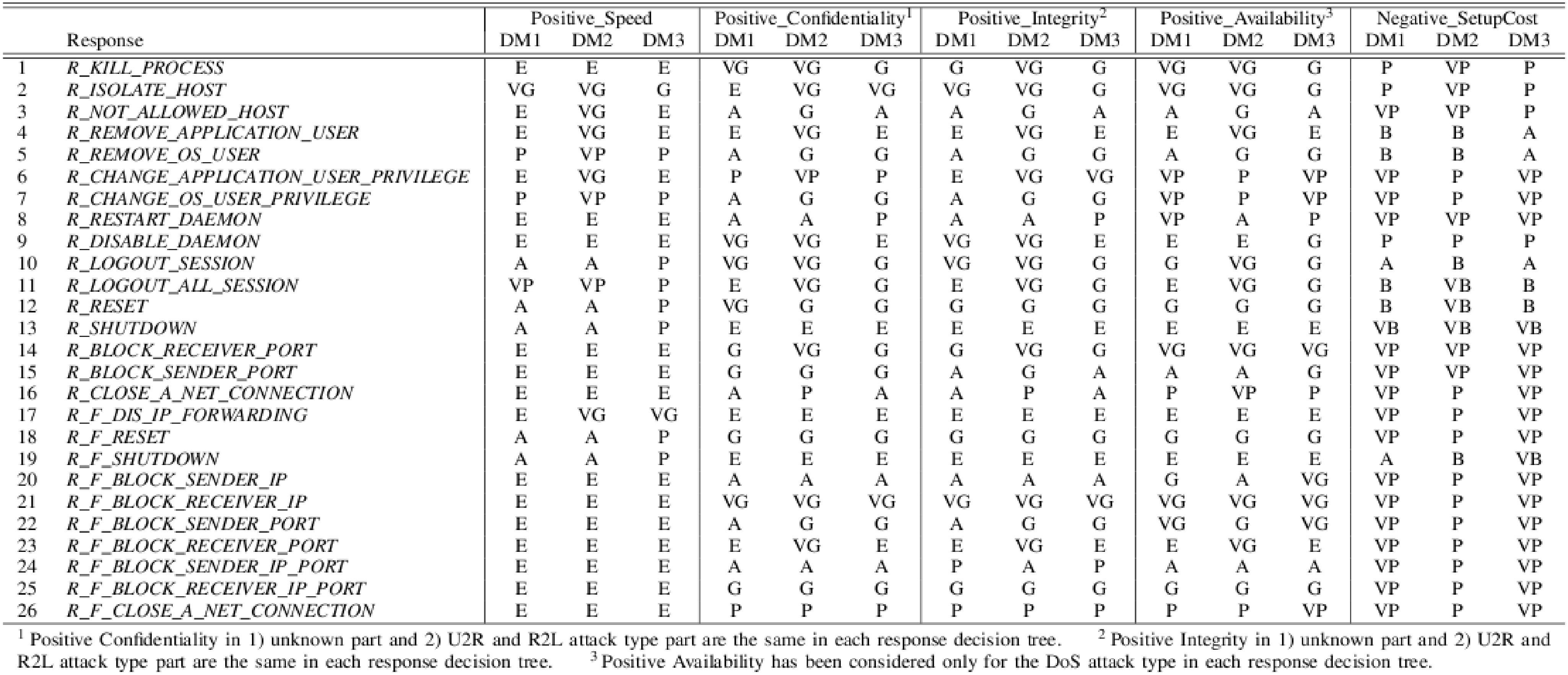


| | External DMZ | | | General Subnet | | | Accounting Subnet | | | Production Subnet | | | Accounting Desktop Subnet | | | Production Desktop Subnet | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Response | DM1 | DM2 | DM3 | DM1 | DM2 | DM3 | DM1 | DM2 | DM3 | DM1 | DM2 | DM3 | DM1 | DM2 | DM3 | DM1 | DM2 | DM3 |
| C1: Positive_Confidentiality | VH | H | VH | H | MH | MH | VH | VH | H | L | ML | L | M | MH | M | L | L | L |
| C2: Positive_Integrity | VH | H | VH | H | MH | H | VH | VH | H | ML | ML | L | M | MH | M | L | L | L |
| C3: Positive_Availability | VH | VH | H | MH | MH | MH | L | ML | L | H | VH | VH | L | L | L | H | VH | VH |
| C4: Positive_Speed | VH | MH | H | MH | M | M | VH | H | H | H | H | H | M | M | M | H | MH | MH |
| C5: Negative_Itself | M | MH | MH | M | M | ML | M | L | L | H | MH | H | L | L | L | M | M | M |
| C6: Negative_Host | L | ML | ML | VH | VH | VH | L | ML | ML | L | ML | ML | L | L | L | M | M | M |
| C7: Negative_Zone | VH | VH | VH | L | ML | ML | VH | VH | VH | VH | VH | VH | L | L | L | M | M | M |
| C8: Negative_NetworkUser | VH | VH | VH | H | H | MH | L | M | M | VH | VH | VH | L | L | L | M | M | M |
| C9: Negative_LocalUser | M | MH | MH | M | MH | MH | ML | ML | ML | ML | ML | ML | L | L | L | L | L | L |
| C10: Negative_SetupCost | VH | H | MH | M | M | M | L | L | M | H | H | MH | L | VL | L | M | M | M |



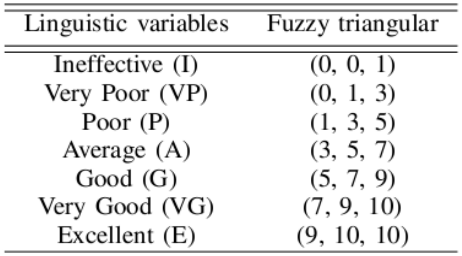
| Linguistic variables | Fuzzy triangular |
|---|---|
| Very low (VL) | (0, 0, 0.1) |
| Low (L) | (0, 0.1, 0.3) |
| Medium low (ML) | (0.1, 0.3, 0.5) |
| Medium (M) | (0.3, 0.5, 0.7) |
| Medium high (MH) | (0.5, 0.7, 0.9) |
| High (H) | (0.7, 0.9, 1.0) |
| Very high (VH) | (0.9, 1.0, 1.0) |

# Step2 ) Assess static criteria

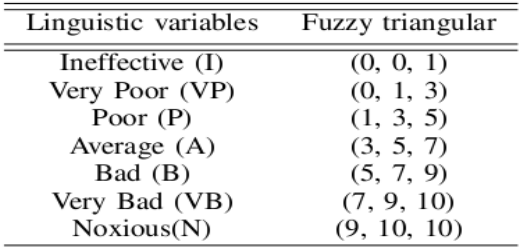


| | | Positive_Speed | | | Positive_Confidentiality[1] | | | Positive_Integrity[2] | | | Positive_Availability[3] | | | Negative_SetupCost | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Response | DM1 | DM2 | DM3 | DM1 | DM2 | DM3 | DM1 | DM2 | DM3 | DM1 | DM2 | DM3 | DM1 | DM2 | DM3 |
| 1 | R_KILL_PROCESS | E | E | E | VG | VG | G | G | VG | G | VG | VG | G | P | VP | P |
| 2 | R_ISOLATE_HOST | VG | VG | G | E | VG | VG | VG | VG | G | VG | VG | G | P | VP | P |
| 3 | R_NOT_ALLOWED_HOST | E | VG | E | A | G | A | A | G | A | A | G | A | VP | VP | P |
| 4 | R_REMOVE_APPLICATION_USER | E | VG | E | E | VG | E | E | VG | E | E | VG | E | B | B | A |
| 5 | R_REMOVE_OS_USER | P | VP | P | A | G | G | A | G | G | A | G | G | B | B | A |
| 6 | R_CHANGE_APPLICATION_USER_PRIVILEGE | E | VG | E | P | VP | P | E | VG | VG | VP | P | VP | VP | P | VP |
| 7 | R_CHANGE_OS_USER_PRIVILEGE | P | VP | P | A | G | G | A | G | G | VP | P | VP | VP | P | VP |
| 8 | R_RESTART_DAEMON | E | E | E | A | A | P | A | A | P | VP | A | P | VP | VP | VP |
| 9 | R_DISABLE_DAEMON | E | E | E | VG | VG | E | VG | VG | E | E | E | G | P | P | P |
| 10 | R_LOGOUT_SESSION | A | A | P | VG | VG | G | VG | VG | G | G | VG | G | A | B | A |
| 11 | R_LOGOUT_ALL_SESSION | VP | VP | P | E | VG | G | E | VG | G | E | VG | G | B | VB | B |
| 12 | R_RESET | A | A | P | VG | G | G | G | G | G | G | G | G | B | VB | B |
| 13 | R_SHUTDOWN | A | A | P | E | E | E | E | E | E | E | E | E | VB | VB | VB |
| 14 | R_BLOCK_RECEIVER_PORT | E | E | E | G | VG | G | G | VG | G | VG | VG | VG | VP | VP | VP |
| 15 | R_BLOCK_SENDER_PORT | E | E | E | G | G | G | A | G | A | A | A | G | VP | VP | VP |
| 16 | R_CLOSE_A_NET_CONNECTION | E | E | E | A | P | A | A | P | A | P | VP | P | VP | P | VP |
| 17 | R_F_DIS_IP_FORWARDING | E | VG | VG | E | E | E | E | E | E | E | E | E | VP | P | VP |
| 18 | R_F_RESET | A | A | P | G | G | G | G | G | G | G | G | G | VP | P | VP |
| 19 | R_F_SHUTDOWN | A | A | P | E | E | E | E | E | E | E | E | E | A | B | VB |
| 20 | R_F_BLOCK_SENDER_IP | E | E | E | A | A | A | A | A | A | G | A | VG | VP | P | VP |
| 21 | R_F_BLOCK_RECEIVER_IP | E | E | E | VG | VG | VG | VG | VG | VG | VG | VG | VG | VP | P | VP |
| 22 | R_F_BLOCK_SENDER_PORT | E | E | E | A | G | G | A | G | G | VG | G | VG | VP | P | VP |
| 23 | R_F_BLOCK_RECEIVER_PORT | E | E | E | E | VG | E | E | VG | E | E | VG | E | VP | P | VP |
| 24 | R_F_BLOCK_SENDER_IP_PORT | E | E | E | A | A | A | P | A | P | A | A | A | VP | P | VP |
| 25 | R_F_BLOCK_RECEIVER_IP_PORT | E | E | E | G | G | G | G | G | G | G | G | G | VP | P | VP |
| 26 | R_F_CLOSE_A_NET_CONNECTION | E | E | E | P | P | P | P | P | P | P | P | VP | VP | P | VP |

[1] Positive Confidentiality in 1) unknown part and 2) U2R and R2L attack type part are the same in each response decision tree. [2] Positive Integrity in 1) unknown part and 2) U2R and R2L attack type part are the same in each response decision tree. [3] Positive Availability has been considered only for the DoS attack type in each response decision tree.

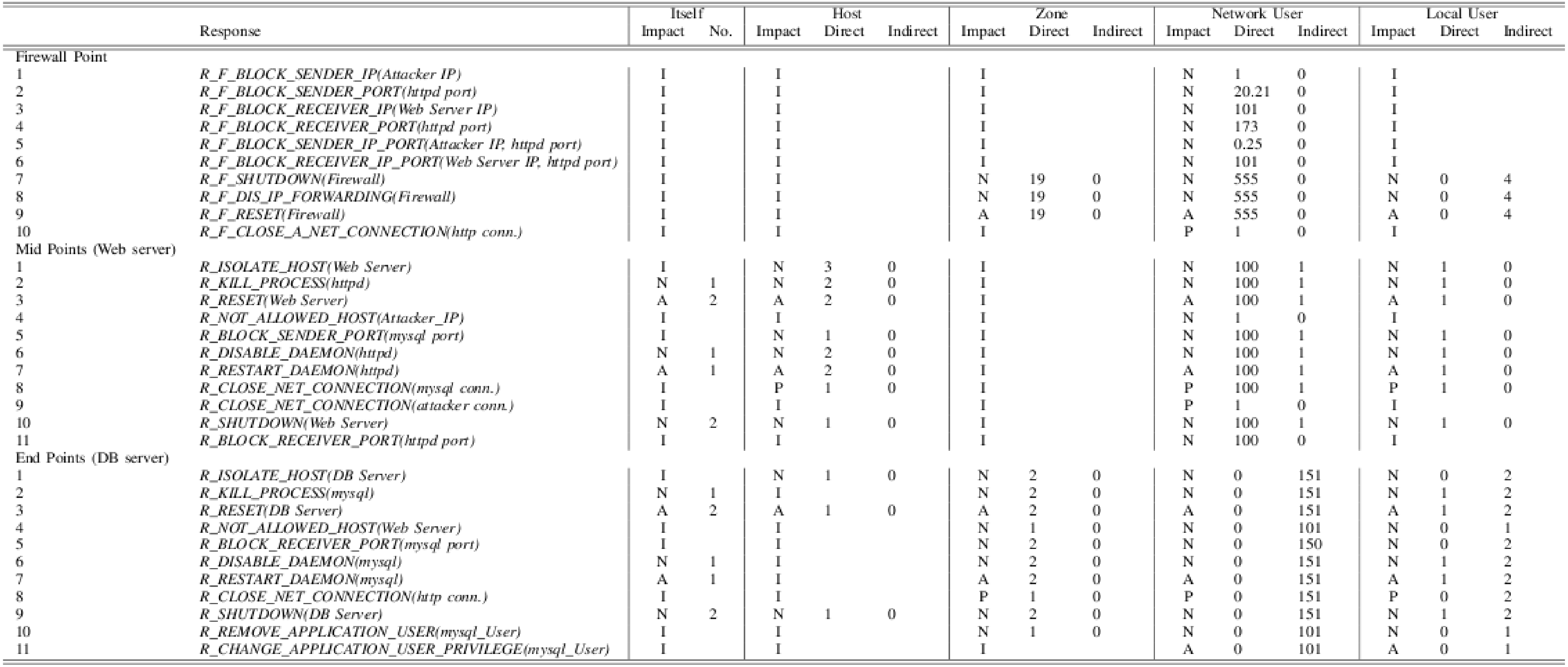


| Linguistic variables | Fuzzy triangular |
|---|---|
| Ineffective (I) | (0, 0, 1) |
| Very Poor (VP) | (0, 1, 3) |
| Poor (P) | (1, 3, 5) |
| Average (A) | (3, 5, 7) |
| Good (G) | (5, 7, 9) |
| Very Good (VG) | (7, 9, 10) |
| Excellent (E) | (9, 10, 10) |



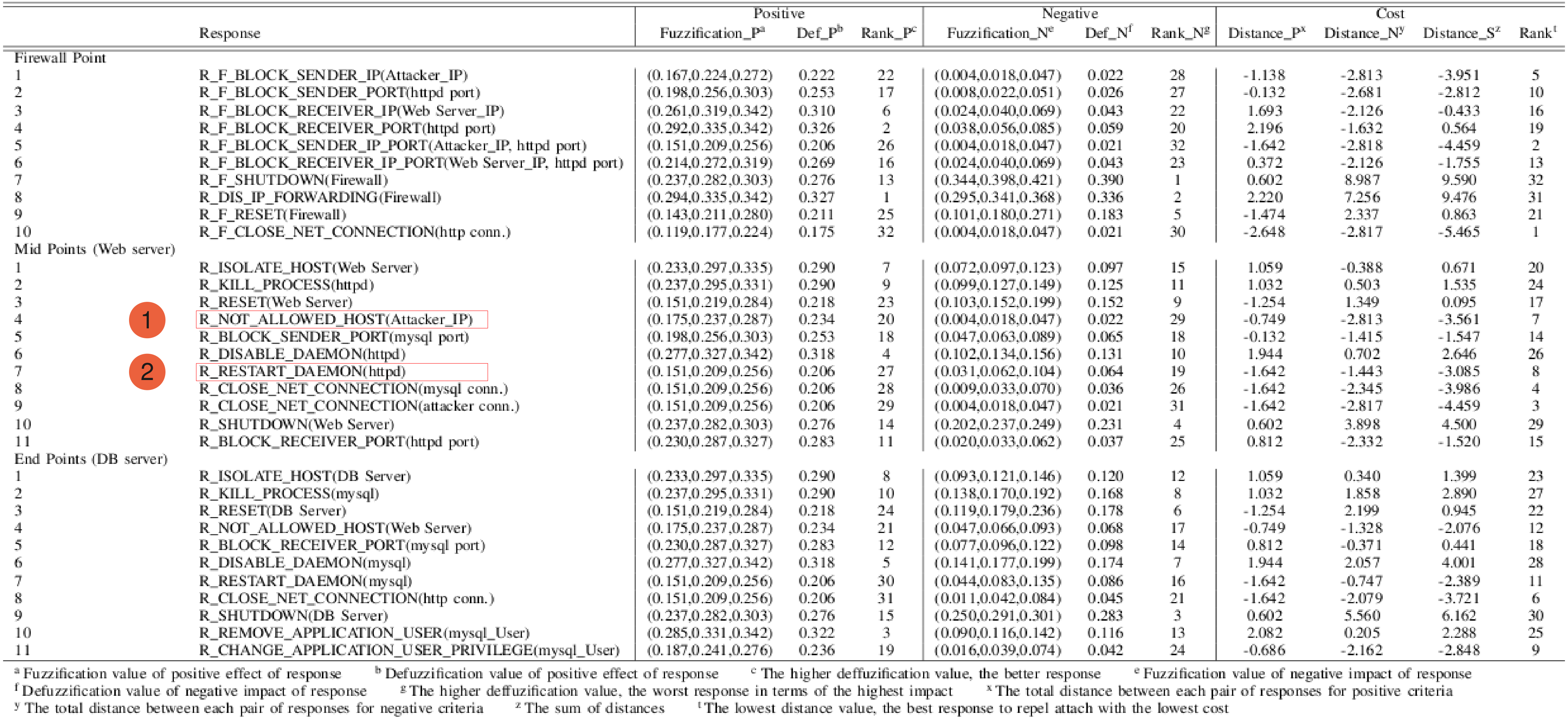
| Linguistic variables | Fuzzy triangular |
|---|---|
| Ineffective (I) | (0, 0, 1) |
| Very Poor (VP) | (0, 1, 3) |
| Poor (P) | (1, 3, 5) |
| Average (A) | (3, 5, 7) |
| Bad (B) | (5, 7, 9) |
| Very Bad (VB) | (7, 9, 10) |
| Noxious(N) | (9, 10, 10) |

# Step 3) The value of negative criteria for outside attacker



| | | Itself | | Host | | | Zone | | | Network User | | | Local User | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Response | Impact | No. | Impact | Direct | Indirect | Impact | Direct | Indirect | Impact | Direct | Indirect | Impact | Direct | Indirect |
| Firewall Point | | | | | | | | | | | | | | | |
| 1 | *R_F_BLOCK_SENDER_IP(Attacker IP)* | I | | I | | | I | | | N | 1 | 0 | I | | |
| 2 | *R_F_BLOCK_SENDER_PORT(httpd port)* | I | | I | | | I | | | N | 20.21 | 0 | I | | |
| 3 | *R_F_BLOCK_RECEIVER_IP(Web Server IP)* | I | | I | | | I | | | N | 101 | 0 | I | | |
| 4 | *R_F_BLOCK_RECEIVER_PORT(httpd port)* | I | | I | | | I | | | N | 173 | 0 | I | | |
| 5 | *R_F_BLOCK_SENDER_IP_PORT(Attacker IP, httpd port)* | I | | I | | | I | | | N | 0.25 | 0 | I | | |
| 6 | *R_F_BLOCK_RECEIVER_IP_PORT(Web Server IP, httpd port)* | I | | I | | | I | | | N | 101 | 0 | I | | |
| 7 | *R_F_SHUTDOWN(Firewall)* | I | | I | | | N | 19 | 0 | N | 555 | 0 | N | 0 | 4 |
| 8 | *R_F_DIS_IP_FORWARDING(Firewall)* | I | | I | | | N | 19 | 0 | N | 555 | 0 | N | 0 | 4 |
| 9 | *R_F_RESET(Firewall)* | I | | I | | | A | 19 | 0 | A | 555 | 0 | A | 0 | 4 |
| 10 | *R_F_CLOSE_A_NET_CONNECTION(http conn.)* | I | | I | | | I | | | P | 1 | 0 | I | | |
| Mid Points (Web server) | | | | | | | | | | | | | | | |
| 1 | *R_ISOLATE_HOST(Web Server)* | I | | N | 3 | 0 | I | | | N | 100 | 1 | N | 1 | 0 |
| 2 | *R_KILL_PROCESS(httpd)* | N | 1 | N | 2 | 0 | I | | | N | 100 | 1 | N | 1 | 0 |
| 3 | *R_RESET(Web Server)* | A | 2 | A | 2 | 0 | I | | | A | 100 | 1 | A | 1 | 0 |
| 4 | *R_NOT_ALLOWED_HOST(Attacker_IP)* | I | | I | | | I | | | N | 1 | 0 | I | | |
| 5 | *R_BLOCK_SENDER_PORT(mysql port)* | I | | N | 1 | 0 | I | | | N | 100 | 1 | N | 1 | 0 |
| 6 | *R_DISABLE_DAEMON(httpd)* | N | 1 | N | 2 | 0 | I | | | N | 100 | 1 | N | 1 | 0 |
| 7 | *R_RESTART_DAEMON(httpd)* | A | 1 | A | 2 | 0 | I | | | A | 100 | 1 | A | 1 | 0 |
| 8 | *R_CLOSE_NET_CONNECTION(mysql conn.)* | I | | P | 1 | 0 | I | | | P | 100 | 1 | P | 1 | 0 |
| 9 | *R_CLOSE_NET_CONNECTION(attacker conn.)* | I | | I | | | I | | | P | 1 | 0 | I | | |
| 10 | *R_SHUTDOWN(Web Server)* | N | 2 | N | 1 | 0 | I | | | N | 100 | 1 | N | 1 | 0 |
| 11 | *R_BLOCK_RECEIVER_PORT(httpd port)* | I | | I | | | I | | | N | 100 | 0 | I | | |
| End Points (DB server) | | | | | | | | | | | | | | | |
| 1 | *R_ISOLATE_HOST(DB Server)* | I | | N | 1 | 0 | N | 2 | 0 | N | 0 | 151 | N | 0 | 2 |
| 2 | *R_KILL_PROCESS(mysql)* | N | 1 | I | | | N | 2 | 0 | N | 0 | 151 | N | 1 | 2 |
| 3 | *R_RESET(DB Server)* | A | 2 | A | 1 | 0 | A | 2 | 0 | A | 0 | 151 | A | 1 | 2 |
| 4 | *R_NOT_ALLOWED_HOST(Web Server)* | I | | I | | | N | 1 | 0 | N | 0 | 101 | N | 0 | 1 |
| 5 | *R_BLOCK_RECEIVER_PORT(mysql port)* | I | | I | | | N | 2 | 0 | N | 0 | 150 | N | 0 | 2 |
| 6 | *R_DISABLE_DAEMON(mysql)* | N | 1 | I | | | N | 2 | 0 | N | 0 | 151 | N | 1 | 2 |
| 7 | *R_RESTART_DAEMON(mysql)* | A | 1 | I | | | A | 2 | 0 | A | 0 | 151 | A | 1 | 2 |
| 8 | *R_CLOSE_NET_CONNECTION(http conn.)* | I | | I | | | P | 1 | 0 | P | 0 | 151 | P | 0 | 2 |
| 9 | *R_SHUTDOWN(DB Server)* | N | 2 | N | 1 | 0 | N | 2 | 0 | N | 0 | 151 | N | 1 | 2 |
| 10 | *R_REMOVE_APPLICATION_USER(mysql_User)* | I | | I | | | N | 1 | 0 | N | 0 | 101 | N | 0 | 1 |
| 11 | *R_CHANGE_APPLICATION_USER_PRIVILEGE(mysql_User)* | I | | I | | | I | | | A | 0 | 101 | A | 0 | 1 |

# Step 4) The results for outside attacker



| | | Positive | | | Negative | | | Cost | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Response | Fuzzification_P[a] | Def_P[b] | Rank_P[c] | Fuzzification_N[e] | Def_N[f] | Rank_N[g] | Distance_P[x] | Distance_N[y] | Distance_S[z] | Rank[t] |
| Firewall Point | | | | | | | | | | | |
| 1 | R_F_BLOCK_SENDER_IP(Attacker_IP) | (0.167,0.224,0.272) | 0.222 | 22 | (0.004,0.018,0.047) | 0.022 | 28 | -1.138 | -2.813 | -3.951 | 5 |
| 2 | R_F_BLOCK_SENDER_PORT(httpd port) | (0.198,0.256,0.303) | 0.253 | 17 | (0.008,0.022,0.051) | 0.026 | 27 | -0.132 | -2.681 | -2.812 | 10 |
| 3 | R_F_BLOCK_RECEIVER_IP(Web Server_IP) | (0.261,0.319,0.342) | 0.310 | 6 | (0.024,0.040,0.069) | 0.043 | 22 | 1.693 | -2.126 | -0.433 | 16 |
| 4 | R_F_BLOCK_RECEIVER_PORT(httpd port) | (0.292,0.335,0.342) | 0.326 | 2 | (0.038,0.056,0.085) | 0.059 | 20 | 2.196 | -1.632 | 0.564 | 19 |
| 5 | R_F_BLOCK_SENDER_IP_PORT(Attacker_IP, httpd port) | (0.151,0.209,0.256) | 0.206 | 26 | (0.004,0.018,0.047) | 0.021 | 32 | -1.642 | -2.818 | -4.459 | 2 |
| 6 | R_F_BLOCK_RECEIVER_IP_PORT(Web Server_IP, httpd port) | (0.214,0.272,0.319) | 0.269 | 16 | (0.024,0.040,0.069) | 0.043 | 23 | 0.372 | -2.126 | -1.755 | 13 |
| 7 | R_F_SHUTDOWN(Firewall) | (0.237,0.282,0.303) | 0.276 | 13 | (0.344,0.398,0.421) | 0.390 | 1 | 0.602 | 8.987 | 9.590 | 32 |
| 8 | R_DIS_IP_FORWARDING(Firewall) | (0.294,0.335,0.342) | 0.327 | 1 | (0.295,0.341,0.368) | 0.336 | 2 | 2.220 | 7.256 | 9.476 | 31 |
| 9 | R_F_RESET(Firewall) | (0.143,0.211,0.280) | 0.211 | 25 | (0.101,0.180,0.271) | 0.183 | 5 | -1.474 | 2.337 | 0.863 | 21 |
| 10 | R_F_CLOSE_NET_CONNECTION(http conn.) | (0.119,0.177,0.224) | 0.175 | 32 | (0.004,0.018,0.047) | 0.021 | 30 | -2.648 | -2.817 | -5.465 | 1 |
| Mid Points (Web server) | | | | | | | | | | | |
| 1 | R_ISOLATE_HOST(Web Server) | (0.233,0.297,0.335) | 0.290 | 7 | (0.072,0.097,0.123) | 0.097 | 15 | 1.059 | -0.388 | 0.671 | 20 |
| 2 | R_KILL_PROCESS(httpd) | (0.237,0.295,0.331) | 0.290 | 9 | (0.099,0.127,0.149) | 0.125 | 11 | 1.032 | 0.503 | 1.535 | 24 |
| 3 | R_RESET(Web Server) | (0.151,0.219,0.284) | 0.218 | 23 | (0.103,0.152,0.199) | 0.152 | 9 | -1.254 | 1.349 | 0.095 | 17 |
| 4 | R_NOT_ALLOWED_HOST(Attacker_IP) | (0.175,0.237,0.287) | 0.234 | 20 | (0.004,0.018,0.047) | 0.022 | 29 | -0.749 | -2.813 | -3.561 | 7 |
| 5 | R_BLOCK_SENDER_PORT(mysql port) | (0.198,0.256,0.303) | 0.253 | 18 | (0.047,0.063,0.089) | 0.065 | 18 | -0.132 | -1.415 | -1.547 | 14 |
| 6 | R_DISABLE_DAEMON(httpd) | (0.277,0.327,0.342) | 0.318 | 4 | (0.102,0.134,0.156) | 0.131 | 10 | 1.944 | 0.702 | 2.646 | 26 |
| 7 | R_RESTART_DAEMON(httpd) | (0.151,0.209,0.256) | 0.206 | 27 | (0.031,0.062,0.104) | 0.064 | 19 | -1.642 | -1.443 | -3.085 | 8 |
| 8 | R_CLOSE_NET_CONNECTION(mysql conn.) | (0.151,0.209,0.256) | 0.206 | 28 | (0.009,0.033,0.070) | 0.036 | 26 | -1.642 | -2.345 | -3.986 | 4 |
| 9 | R_CLOSE_NET_CONNECTION(attacker conn.) | (0.151,0.209,0.256) | 0.206 | 29 | (0.004,0.018,0.047) | 0.021 | 31 | -1.642 | -2.817 | -4.459 | 3 |
| 10 | R_SHUTDOWN(Web Server) | (0.237,0.282,0.303) | 0.276 | 14 | (0.202,0.237,0.249) | 0.231 | 4 | 0.602 | 3.898 | 4.500 | 29 |
| 11 | R_BLOCK_RECEIVER_PORT(httpd port) | (0.230,0.287,0.327) | 0.283 | 11 | (0.020,0.033,0.062) | 0.037 | 25 | 0.812 | -2.332 | -1.520 | 15 |
| End Points (DB server) | | | | | | | | | | | |
| 1 | R_ISOLATE_HOST(DB Server) | (0.233,0.297,0.335) | 0.290 | 8 | (0.093,0.121,0.146) | 0.120 | 12 | 1.059 | 0.340 | 1.399 | 23 |
| 2 | R_KILL_PROCESS(mysql) | (0.237,0.295,0.331) | 0.290 | 10 | (0.138,0.170,0.192) | 0.168 | 8 | 1.032 | 1.858 | 2.890 | 27 |
| 3 | R_RESET(DB Server) | (0.151,0.219,0.284) | 0.218 | 24 | (0.119,0.179,0.236) | 0.178 | 6 | -1.254 | 2.199 | 0.945 | 22 |
| 4 | R_NOT_ALLOWED_HOST(Web Server) | (0.175,0.237,0.287) | 0.234 | 21 | (0.047,0.066,0.093) | 0.068 | 17 | -0.749 | -1.328 | -2.076 | 12 |
| 5 | R_BLOCK_RECEIVER_PORT(mysql port) | (0.230,0.287,0.327) | 0.283 | 12 | (0.077,0.096,0.122) | 0.098 | 14 | 0.812 | -0.371 | 0.441 | 18 |
| 6 | R_DISABLE_DAEMON(mysql) | (0.277,0.327,0.342) | 0.318 | 5 | (0.141,0.177,0.199) | 0.174 | 7 | 1.944 | 2.057 | 4.001 | 28 |
| 7 | R_RESTART_DAEMON(mysql) | (0.151,0.209,0.256) | 0.206 | 30 | (0.044,0.083,0.135) | 0.086 | 16 | -1.642 | -0.747 | -2.389 | 11 |
| 8 | R_CLOSE_NET_CONNECTION(http conn.) | (0.151,0.209,0.256) | 0.206 | 31 | (0.011,0.042,0.084) | 0.045 | 21 | -1.642 | -2.079 | -3.721 | 6 |
| 9 | R_SHUTDOWN(DB Server) | (0.237,0.282,0.303) | 0.276 | 15 | (0.250,0.291,0.301) | 0.283 | 3 | 0.602 | 5.560 | 6.162 | 30 |
| 10 | R_REMOVE_APPLICATION_USER(mysql_User) | (0.285,0.331,0.342) | 0.322 | 3 | (0.090,0.116,0.142) | 0.116 | 13 | 2.082 | 0.205 | 2.288 | 25 |
| 11 | R_CHANGE_APPLICATION_USER_PRIVILEGE(mysql_User) | (0.187,0.241,0.276) | 0.236 | 19 | (0.016,0.039,0.074) | 0.042 | 24 | -0.686 | -2.162 | -2.848 | 9 |

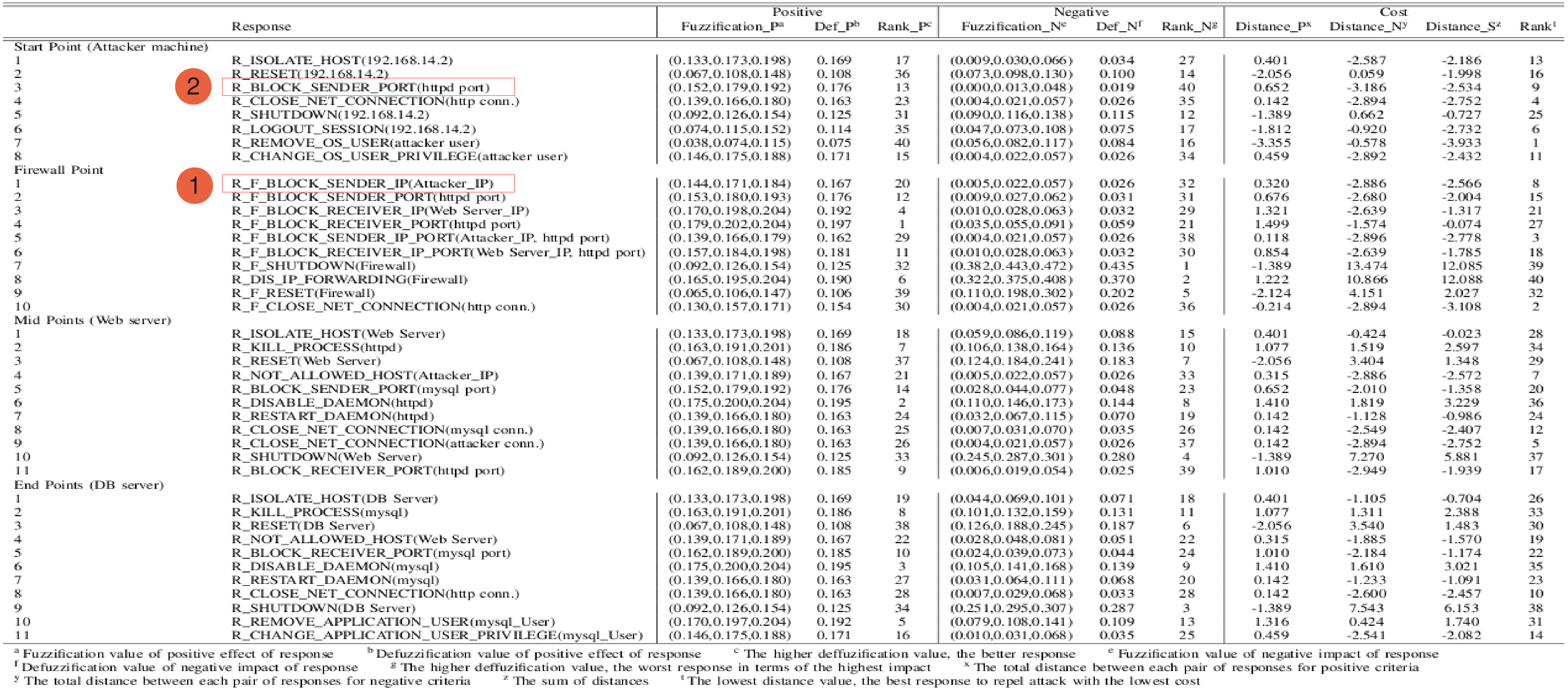
[a] Fuzzification value of positive effect of response [b] Defuzzification value of positive effect of response [c] The higher deffuzification value, the better response [e] Fuzzification value of negative impact of response [f] Defuzzification value of negative impact of response [g] The higher deffuzification value, the worst response in terms of the highest impact [x] The total distance between each pair of responses for positive criteria [y] The total distance between each pair of responses for negative criteria [z] The sum of distances [t] The lowest distance value, the best response to repel attach with the lowest cost

- Ordered List = (R2 , R5 , Rn , · · · , R4 )
- N = k * m
- CR(1) = [(DC * CL * K)/SC] * m + (m * RV)/SC
- CR(i+1) = CR(i)

→

- DC= 60, CL= 0.25, RV= 90, N= 32 (m= 8, k=4), SC=100
- CR(1) = 7
- CR(2) = 8

# Step 4) The results for Internal attacker



| | Response | Positive | | | Negative | | | Cost | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Fuzzification_P[a] | Def_P[b] | Rank_P[c] | Fuzzification_N[e] | Def_N[f] | Rank_N[g] | Distance_P[x] | Distance_N[y] | Distance_S[z] | Rank[t] |
| Start Point (Attacker machine) | | | | | | | | | | | |
| 1 | R_ISOLATE_HOST(192.168.14.2) | (0.133,0.173,0.198) | 0.169 | 17 | (0.009,0.030,0.066) | 0.034 | 27 | 0.401 | -2.587 | -2.186 | 13 |
| 2 | R_RESET(192.168.14.2) | (0.067,0.108,0.148) | 0.108 | 36 | (0.073,0.098,0.130) | 0.100 | 14 | -2.056 | 0.059 | -1.998 | 16 |
| 3 | R_BLOCK_SENDER_PORT(httpd port) | (0.152,0.179,0.192) | 0.176 | 13 | (0.000,0.013,0.048) | 0.019 | 40 | 0.652 | -3.186 | -2.534 | 9 |
| 4 | R_CLOSE_NET_CONNECTION(http conn.) | (0.139,0.166,0.180) | 0.163 | 23 | (0.004,0.021,0.057) | 0.026 | 35 | 0.142 | -2.894 | -2.752 | 4 |
| 5 | R_SHUTDOWN(192.168.14.2) | (0.092,0.126,0.154) | 0.125 | 31 | (0.090,0.116,0.138) | 0.115 | 12 | -1.389 | 0.662 | -0.727 | 25 |
| 6 | R_LOGOUT_SESSION(192.168.14.2) | (0.074,0.115,0.152) | 0.114 | 35 | (0.047,0.073,0.108) | 0.075 | 17 | -1.812 | -0.920 | -2.732 | 6 |
| 7 | R_REMOVE_OS_USER(attacker user) | (0.038,0.074,0.115) | 0.075 | 40 | (0.056,0.082,0.117) | 0.084 | 16 | -3.355 | -0.578 | -3.933 | 1 |
| 8 | R_CHANGE_OS_USER_PRIVILEGE(attacker user) | (0.146,0.175,0.188) | 0.171 | 15 | (0.004,0.022,0.057) | 0.026 | 34 | 0.459 | -2.892 | -2.432 | 11 |
| Firewall Point | | | | | | | | | | | |
| 1 | R_F_BLOCK_SENDER_IP(Attacker_IP) | (0.144,0.171,0.184) | 0.167 | 20 | (0.005,0.022,0.057) | 0.026 | 32 | 0.320 | -2.886 | -2.566 | 8 |
| 2 | R_F_BLOCK_SENDER_PORT(httpd port) | (0.153,0.180,0.193) | 0.176 | 12 | (0.009,0.027,0.062) | 0.031 | 31 | 0.676 | -2.680 | -2.004 | 15 |
| 3 | R_F_BLOCK_RECEIVER_IP(Web Server_IP) | (0.170,0.198,0.204) | 0.192 | 4 | (0.010,0.028,0.063) | 0.032 | 29 | 1.321 | -2.639 | -1.317 | 21 |
| 4 | R_F_BLOCK_RECEIVER_PORT(httpd port) | (0.179,0.202,0.204) | 0.197 | 1 | (0.035,0.055,0.091) | 0.059 | 21 | 1.499 | -1.574 | -0.074 | 27 |
| 5 | R_F_BLOCK_SENDER_IP_PORT(Attacker_IP, httpd port) | (0.139,0.166,0.179) | 0.162 | 29 | (0.004,0.021,0.057) | 0.026 | 38 | 0.118 | -2.896 | -2.778 | 3 |
| 6 | R_F_BLOCK_RECEIVER_IP_PORT(Web Server_IP, httpd port) | (0.157,0.184,0.198) | 0.181 | 11 | (0.010,0.028,0.063) | 0.032 | 30 | 0.854 | -2.639 | -1.785 | 18 |
| 7 | R_F_SHUTDOWN(Firewall) | (0.092,0.126,0.154) | 0.125 | 32 | (0.382,0.443,0.472) | 0.435 | 1 | -1.389 | 13.474 | 12.085 | 39 |
| 8 | R_DIS_IP_FORWARDING(Firewall) | (0.165,0.195,0.204) | 0.190 | 6 | (0.322,0.375,0.408) | 0.370 | 2 | 1.222 | 10.866 | 12.088 | 40 |
| 9 | R_F_RESET(Firewall) | (0.065,0.106,0.147) | 0.106 | 39 | (0.110,0.198,0.302) | 0.202 | 5 | -2.124 | 4.151 | 2.027 | 32 |
| 10 | R_F_CLOSE_NET_CONNECTION(http conn.) | (0.130,0.157,0.171) | 0.154 | 30 | (0.004,0.021,0.057) | 0.026 | 36 | -0.214 | -2.894 | -3.108 | 2 |
| Mid Points (Web server) | | | | | | | | | | | |
| 1 | R_ISOLATE_HOST(Web Server) | (0.133,0.173,0.198) | 0.169 | 18 | (0.059,0.086,0.119) | 0.088 | 15 | 0.401 | -0.424 | -0.023 | 28 |
| 2 | R_KILL_PROCESS(httpd) | (0.163,0.191,0.201) | 0.186 | 7 | (0.106,0.138,0.164) | 0.136 | 10 | 1.077 | 1.519 | 2.597 | 34 |
| 3 | R_RESET(Web Server) | (0.067,0.108,0.148) | 0.108 | 37 | (0.124,0.184,0.241) | 0.183 | 7 | -2.056 | 3.404 | 1.348 | 29 |
| 4 | R_NOT_ALLOWED_HOST(Attacker_IP) | (0.139,0.171,0.189) | 0.167 | 21 | (0.005,0.022,0.057) | 0.026 | 33 | 0.315 | -2.886 | -2.572 | 7 |
| 5 | R_BLOCK_SENDER_PORT(mysql port) | (0.152,0.179,0.192) | 0.176 | 14 | (0.028,0.044,0.077) | 0.048 | 23 | 0.652 | -2.010 | -1.358 | 20 |
| 6 | R_DISABLE_DAEMON(httpd) | (0.175,0.200,0.204) | 0.195 | 2 | (0.110,0.146,0.173) | 0.144 | 8 | 1.410 | 1.819 | 3.229 | 36 |
| 7 | R_RESTART_DAEMON(httpd) | (0.139,0.166,0.180) | 0.163 | 24 | (0.032,0.067,0.115) | 0.070 | 19 | 0.142 | -1.128 | -0.986 | 24 |
| 8 | R_CLOSE_NET_CONNECTION(mysql conn.) | (0.139,0.166,0.180) | 0.163 | 25 | (0.007,0.031,0.070) | 0.035 | 26 | 0.142 | -2.549 | -2.407 | 12 |
| 9 | R_CLOSE_NET_CONNECTION(attacker conn.) | (0.139,0.166,0.180) | 0.163 | 26 | (0.004,0.021,0.057) | 0.026 | 37 | 0.142 | -2.894 | -2.752 | 5 |
| 10 | R_SHUTDOWN(Web Server) | (0.092,0.126,0.154) | 0.125 | 33 | (0.245,0.287,0.301) | 0.280 | 4 | -1.389 | 7.270 | 5.881 | 37 |
| 11 | R_BLOCK_RECEIVER_PORT(httpd port) | (0.162,0.189,0.200) | 0.185 | 9 | (0.006,0.019,0.054) | 0.025 | 39 | 1.010 | -2.949 | -1.939 | 17 |
| End Points (DB server) | | | | | | | | | | | |
| 1 | R_ISOLATE_HOST(DB Server) | (0.133,0.173,0.198) | 0.169 | 19 | (0.044,0.069,0.101) | 0.071 | 18 | 0.401 | -1.105 | -0.704 | 26 |
| 2 | R_KILL_PROCESS(mysql) | (0.163,0.191,0.201) | 0.186 | 8 | (0.101,0.132,0.159) | 0.131 | 11 | 1.077 | 1.311 | 2.388 | 33 |
| 3 | R_RESET(DB Server) | (0.067,0.108,0.148) | 0.108 | 38 | (0.126,0.188,0.245) | 0.187 | 6 | -2.056 | 3.540 | 1.483 | 30 |
| 4 | R_NOT_ALLOWED_HOST(Web Server) | (0.139,0.171,0.189) | 0.167 | 22 | (0.028,0.048,0.081) | 0.051 | 22 | 0.315 | -1.885 | -1.570 | 19 |
| 5 | R_BLOCK_RECEIVER_PORT(mysql port) | (0.162,0.189,0.200) | 0.185 | 10 | (0.024,0.039,0.073) | 0.044 | 24 | 1.010 | -2.184 | -1.174 | 22 |
| 6 | R_DISABLE_DAEMON(mysql) | (0.175,0.200,0.204) | 0.195 | 3 | (0.105,0.141,0.168) | 0.139 | 9 | 1.410 | 1.610 | 3.021 | 35 |
| 7 | R_RESTART_DAEMON(mysql) | (0.139,0.166,0.180) | 0.163 | 27 | (0.031,0.064,0.111) | 0.068 | 20 | 0.142 | -1.233 | -1.091 | 23 |
| 8 | R_CLOSE_NET_CONNECTION(http conn.) | (0.139,0.166,0.180) | 0.163 | 28 | (0.007,0.029,0.068) | 0.033 | 28 | 0.142 | -2.600 | -2.457 | 10 |
| 9 | R_SHUTDOWN(DB Server) | (0.092,0.126,0.154) | 0.125 | 34 | (0.251,0.295,0.307) | 0.287 | 3 | -1.389 | 7.543 | 6.153 | 38 |
| 10 | R_REMOVE_APPLICATION_USER(mysql_User) | (0.170,0.197,0.204) | 0.192 | 5 | (0.079,0.108,0.141) | 0.109 | 13 | 1.316 | 0.424 | 1.740 | 31 |
| 11 | R_CHANGE_APPLICATION_USER_PRIVILEGE(mysql_User) | (0.146,0.175,0.188) | 0.171 | 16 | (0.010,0.031,0.068) | 0.035 | 25 | 0.459 | -2.541 | -2.082 | 14 |

[a] Fuzzification value of positive effect of response
[b] Defuzzification value of positive effect of response
[c] The higher deffuzification value, the better response
[e] Fuzzification value of negative impact of response
[f] Defuzzification value of negative impact of response
[g] The higher deffuzification value, the worst response in terms of the highest impact
[x] The total distance between each pair of responses for positive criteria
[y] The total distance between each pair of responses for negative criteria
[z] The sum of distances
[t] The lowest distance value, the best response to repel attack with the lowest cost

- Ordered List = (R2 , R5 , Rn , · · · , R4 )
- N = k * m
- CR(1) = [(DC * CL * K)/SC] * m + (m * RV)/SC
- CR(i+1) = CR(i)

→

- DC= 60, CL= 0.25, RV= 83, N= 40 (m= 10, k=4), SC=100
- CR(1) = 8
- CR(2) = 9

# Future Work

- Complete the implementation of new architecture of IRS
- Connect *Response component* to the *Risk assessment* and *Prediction component*
- Evaluate all components with more scenarios of multi-step attack

# References (1)

[1] F. Xiao, S. Jin and X. Li, “A Novel Data Mining-Based Method for Alert Reduction and Analysis,” Journal of Network, vol. 5, no. 1, 2010, pp. 88-97.

[2] M. Desnoyers and M. Dagenais, “LTTng: Tracing across execution layers, from the hypervisor to user-space,” Linux Symposium, 2008, Ottawa, Canada.

[3] K. Scarfone and P. Mell, “Guide to Intrusion Detection and Prevention Systems,” 2007, http://csrc.ncsl.nist.gov/publications/nistpubs/800-94/SP800-94.pdf .

[4] N. Stakhanova, S. Basu and J. Wong, “Taxonomy of Intrusion Response Systems,” Journal of Information and Computer Security, vol. 1, no. 2, 2007, pp. 169-184.

[5] D. B. Payne and H. G. Gunhold, “Policy-based security configuration management application to intrusion detection and prevention,” IEEE International Conference on Communications, 2009, Dresden, Germany.

[6] A. Curtis. And J. Carver, “Adaptive agent-based intrusion response,” Ph.D thesis, Texas A&M University, USA, 2001.

[7] W. Lee, W. Fan and M. Miller, “Toward Cost-Sensitive Modeling for Intrusion Detection and response,” Journal of Computer Security, vol. 10, no. 1, 2002, pp. 5-22.

[8] T. Toth and C. Kregel, “Evaluating the impact of automated intrusion response mechanisms,” In proceeding of the 18th Annual Computer Security Applications Conference, Los Alamitos, USA, 2002.

[9] C. P. Mu and Y. Li, “An intrusion response decision-making model based on hierarchical task network planning,” Expert systems with applications, vol. 37, no. 3, 2010, pp. 2465-2472.

[10] C.P. Mu, X. J. Li, H.K. Huang and S.F. Tian, “Online risk assessment of intrusion scenarios using D-S evidence theory,” 13th European Symposium on Research in Computer Security, pp. 35-48, Malaga, Spain, 2008.

[11] K. Haslum, A. Abraham and S. Knapskog, “DIPS: A framework for distributed intrusion prediction and prevention using hidden markov models and online fuzzy risk assessment,” In 3rd International Symposium on Information Assurance and Security, pp. 183-188, Manchester, United Kingdom, 2007.

# References (2)

[12] K. Haslum, M. E. G. Moe and S. J. Knapskog, “Real-time intrusion prevention and security analysis of networks using HMMs,” 33rd IEEE Conference on Local Computer Networks, 2008, Montreal, Canada.

[13] B. Zhu and A. A. Ghorbani, “Alert correlation for extracting attack strategies,” International Journal of Network Security, vol. 3, no. 3,2006, pp. 244-258.

[14] C. Kruegel, F. Valeur and G. Vigna, “Alert Correlation,” In Intrusion Detection and Correlation, 1st ed., vol. 14., New York: Springer, 2005, pp. 29-35.

[15] G. Stein, C. Bing, A. S. Wu and K. A. Hua, “Decision Tree Classifier For Network Intrusion Detection With GA-based Feature Selection,” In Proceedings of the 43rd annual Southeast regional conference, Georgia, ISBN:1-59593-059-0, pp. 136-141, 2005.

[16] D. Yu and D. Frincke, “Improving the quality of alerts and predicting intruder's next goal with Hidden Colored Petri-Net,” Computer Networks, pp. 632–654, 2007.

[17] N. B. Anuar, H. Sallehudin, A. Gani and O. Zakaria, “Identifying False Alarm for Network Intrusion Detection System Using Hybrid Data Mining and Decision Tree,” Malaysian Journal of Computer Science, ISSN 0127-9084, 2008, pp. 110-115.

[18] T. Ozyer, R. Alhajj and K. Barker, “Intrusion detection by integrating boosting genetic fuzzy classifier and data mining criteria for rule pre-screening,” Journal of Network and Computer Applications, SSN:1084-8045, 2007, pp. 99-113.

[19] H. Jin, J. Sun, H. Chen and Z. Han, “A Fuzzy Data Mining Based Intrusion Detection Model,” 10th IEEE International Workshop on Future Trends of Distributed Computing Systems, pp. 191-197, 2004.

[20] Q. Xu, W. Pei, L. Yang and Q. Zhao, “An Intrusion Detection Approach Based On Understandable Neural Network Trees,” Journal of Electronics, 2007, pp. 574-579.

[21] Y. Bouzida and F. Cuppens, “Neural networks vs. decision trees for intrusion detection,” IEEE/IST Workshop on Monitoring, Germany, September, 2006.

# References (3)

[22] R. C. Chen, K. F. Cheng, Y. H. Chen, C. F. Hsieh, “Using Rough Set and Support Vector Machine for Network Intrusion Detection System,” First Asian Conference on Intelligent Information and Database Systems, pp. 465-470, 2009.

[23] L. Khan, M. Awad and B. Thuraisingham, “A new intrusion detection system using support vector machines and hierarchical clustering,” ISSN:1066-8888, pp. 507-521, 2007.

[24] J. C. Liu, C. H. Lin, J. L. Yu, W. S. Lai and C. H. Ho, “Anomaly Detection Using LibSVM Training Tools,” International Journal of Security and Its Applications, Vol.2 , No.4, ISBN: 978-0-7695-3126-7, 2008, pp. 166-177.

[25] R. Zhang, S. Zhang , S. Muthuraman and J. Jiang, “One class support vector machine for anomaly detection in the communication network performance data,” Proceedings of the 5th conference on Applied electromagnetics, wireless and optical communications, Spain, ISBN:1790-5117, pp. 31-37, 2007.

[26] A. Abraham, R. Jain, J. Thomas and S. Y. Han, “D-SCIDS: Distributed soft computing intrusion detection system,” Journal of Network and Computer Applications, pp. 81–98, 2007.

[27] Abdelhamid, “Réseaux Bayésiens Naïfs Augmentés TAN pour les Systèmes de Détection d’Intrusions,” PhD thesis, Université de Nice Sophia Antipolis, 2007.

[28] N. Abouzakhar, A. Gani, G. Manson, M. Abuitbel and D. King, “Bayesian Learning Networks Approach to Cybercrime Detection,” Proceedings of the 2003 PostGraduate Networking Conference, Liverpool, United Kingdom, 2003.

[29] Difference between Signature Based and Anomaly Based Detection in IDS, URL http://www.secguru.com/forum/difference_between_signature_based_and_anomaly_based_detection_in_ids.

[30] http://www.prelude-technologies.com/en/welcome/index.html.

[31] L. Feng, W. Wang, L. Zhu and Y. Zhang, “Predicting intrusion goal using dynamic Bayesian network with transfer probability estimation,” Journal of Networks and Computer Applications, vol. 32 n. 3, 2009, pp. 721-732.

[32] A. O. Adetunmbi, S. O. Falaki, O. S. Adewale and B. K. Alese, “Network Intrusion Detection based on Rough Set and k-Nearest Neighbour,” International Journal of Computing and ICT Research, Vol. 2, No. 1, 2008, pp. 60–66.

# References (4)

[33] A. Lazarevic, L. Ertöz, V. Kumar, A. Ozgur, J. Srivastava, "A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection," Proceedings of the Third SIAM International Conference on Data Mining, 2003.

[34] V. Chandola, A. Banerjee and V. Kumar, "Anomaly Detection: A Survey, ACM Computing Surveys," Vol. 41(3), 2009.

[35] S. Cherednichenko, "Outlier Detection in Clustering," 2005.

[36] Q. Wang and V. Megalooikonomou, "A Clustering Algorithm for Intrusion Detection," The SPIE Conference on Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security, Florida, vol. 5812, pp. 31–38, 2005.

[37] J. Hanand M. Kamber, "Mining: Concepts and Techniques," 2nd ed., San Francisco: Elsevier, 2006.

[38] P. Domingos and G. Hulten, "Mining high-speed data streams," In Proc. 2000 ACM SIGKDD Int. Conf. Knowledge Discovery in Databases (KDD'00), pp. 71–80, Boston, MA, Aug. 2000.

[39] P. Domingos and G. Hulten, "Mining High-Speed Data Streams," Proceedings of the Association for Computing Machinery Sixth International Conference on Knowledge Discovery and Data Mining, pp. 71–80, 2000.

[40] G. Hulten, L. Spencer, and P. Domingos, "Mining time-changing data streams," In Proc. 2001 ACM SIGKDD Int. Conf. Knowledge Discovery in Databases (KDD'01), San Francisco, CA, Aug. 2001.

[41] M. Gaber, A. Zaslavsky and S. Krishnaswamy, "Mining Data Streams: A Review," ACM SIGMOD Record, Vol. 34, 2005.

[42] C. Aggarwal, J. Han, J. Wang, and P. Yu, "A Framework for Projected Clustering of High Dimensional Data Streams," Proceedings of the 30th VLDB Conference, Toronto, Canada, 2004.

[43] MIT Lincoln Laboratory, 2000 darpa intrusion detection scenario specific data sets, 2000.

# References (5)

[44] J. Han, H. Cheng, D. Xin, and X. Yan. “Frequent pattern mining: Current status and future directions,” Data Mining and Knowledge Discovery, 2007.

[45] G. Manku and R. Motwani, “Approximate frequency counts over data streams,” In Proc. 2002 Int. Conf. Very Large Data Bases (VLDB’02), pp. 346–357, Hong Kong, China, 2002.

[46] T. Zhang, R. Ramakhrisnan, M. Livny, “BIRCH: An Efficient Data Clustering Method for Very Large Databases,” Proc. ACM SIGMOD Int. Conf. Management of Data, 1996.

[47] North Carolina State University Cyber Defense Laboratory, “Tiaa: A toolkit for intrusion alert analysis,” http://discovery.csc.ncsu.edu/software/correlator/ver0.4/index.html.

[48] L. R. Rabiner, “A tutorial on hidden Markov models and selected applications in speech recognition,” Proc. IEEE, 77, pp. 257-286, 1989.

[49] RealSecure Signatures Reference Guide. Internet Security Systems, http://documents.iss.net/literature/RealSecure/RS_Signatures_6.0.pdf.

[50] The Snort Project, Snort users manual 2.8.5, 2009.

[51] G. Antoniol. Keynote paper “Search based software testing for software security: Breaking code to make it safer,” In ICSTW ’09: Proceedings of the IEEE International Conference on SoftwareTesting, Verification, and Validation Workshops, IEEE Computer Society, 2009.

[52] G. Stoneburner, A. Goguen, and A. Feringa, “Risk management guide for information technology systems,” http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

[53] H. Debar, D. Curry and B. Feinstein, “The Intrusion Detection Message Exchange Format (IDMEF),” http://www.ietf.org/rfc/rfc4765.txt.

[54] http://wiki.eclipse.org/DSDP/TCF.

# References (6)

[55] G. Matni and M. Dagenais, “Automata-based approach for kernel trace analysis,” Canadian Conference on Electrical and Computer Engineering, pp. 970-973, 2009.

[56] NCSA Security Research, “Mithril: An Experiment in Adaptive Security,” 2006, http://security.ncsa.illinois.edu/research/mithril/Mithril.html.

[57] Y.-M. Chen and Y. Yang, “Policy management for network-based intrusion detection and prevention,” In IEEE Network Operations and Management Symposium, 2004.

[58] G. White, E. Fisch and U. Pooch “Cooperating security managers: a peer-based intrusion detection system,” IEEE Network, Vol. 10, 1996, pp. 20–23.

[59] P. Porras and P. Neumann, “EMERALD: event monitoring enabling responses to anomalous live disturbances,” National Information Systems Security Conference, 1997.

[60] B. Foo, Y.-S. Wu, Y.-C. Mao, S. Bagchi and E. Spafford, “ADEPTS: adaptive intrusion response using attack graphs in an e-commerce environment,” International Conference on Dependable Systems and Networks, pp. 508–517, 2005.

[61] I. Balepin, S. Maltsev, J. Rowe and K. Levitt “Using specification-based intrusion detection for automated response,” In 6th International Symposium on Recent Advances in Intrusion Detection, pp. 136–154, 2003.

[62] T. Toth, and C. Kruegel, “Evaluating the impact of automated intrusion response mechanisms,” In 18th Annual Computer Security Applications Conference, 2002.

[63] S. Tanachaiwiwat, K. Hwang, and Y. Chen, “Adaptive Intrusion Response to Minimize Risk over Multiple Network Attacks,” ACM Trans on Information and System Security, 2002.

[64] N. B. Anuar, M. Papadaki, S. Furnell and N. Clarke, “An investigation and survey of response options for intrusion response systems,” Information Security for South Africa, pp. 1-8, 2010.

[65] K. Nielsen, “Gentoo Security Handbook,” 2010.

# References (7)

[66] K. Fenzi and D. Wreski, “Linux Security HOWTO,” http://tldp.org/HOWTO/Security-HOWTO .

[67] J. Turnbull, “Hardening Linux,” USA: Apress, 2005.

[68] M. F. Yusof, “Automated Signature Generation of Network Attacks,” B.S thesis, University Teknologi Malasia, 2009.

[69] A. S. Sendi, M. Jabbarifar, M. Shajari, and M. Dagenais, “FEMRA: Fuzzy Expert Model for Risk Assessment,” Fifth International Conference on Internet Monitoring and Protection, pp. 48-53, Barcelona, Spain, 2010.

[70] A. S. Sendi and M. Dagenais, “Real Time Intrusion Prediction based on improving the priority of alerts with Hidden Markov Model,” has been submitted to the *Journal of network*.

[71] P. Arnes, F. Valeur and R. Kemmerer, “Using hidden markov models to evaluate the risk of intrusions,” Int. Symp. Recent Advances in Intrusion Detection, Hamburg, Germany, 2006.

[72] W. Li, Z. Guo, "Hidden Markov Model Based Real Time Network Security Quantification Method," nswctc, International Conference on Networks Security, Wireless Communications and Trusted Computing, pp. 94-100, 2009.

[73] G. Stoneburner, A. Goguen, and A. Feringa, “Risk management guide for information technology systems,” http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

[74] International Standard Organization, ISO/IEC 27005, Information Security Risk Management, 2008.

[75] Z. Li, Z. Lei, L. Wang and D. Li, “Assessing attack threat by the probability of following attacks,” in Proceedings of the International Conference on Networking, Architecture, and Storage, IEEE, pp. 91–100, 2007.

[76] N. Stakhanova, S. Basu and J. Wong, “A cost-sensitive model for preemptive intrusion response systems,” Proceedings of the 21st International Conference on Advanced Networking and Applications, IEEE Computer Society, Washington, DC, USA, pp. 428–435, 2007.

# References (8)

[77] C. Strasburg, N. Stakhanova, S. Basu and J. S. Wong, "A Framework for Cost Sensitive Assessment of Intrusion Response Selection," Proceedings of IEEE Computer Software and Applications Conference, 2009.

[78] https://help.ubuntu.com/community/AppArmor.

[79] A. S. Sendi, M. Dagenais, J. Desfossez and M. Couture, "A Health Framework for Automated Intrusion Response System," has been submitted to the *Ninth Annual Conference on Privacy, Security and Trust.*

[80] http://www.nsa.gov/research/selinux/.