Jing Wu
Bioengineering
University of California, San Diego
<jiwu@ucsd.edu>

Tony Yang
Psychiatry
University of California, San Diego
<tyang@ucsd.edu>

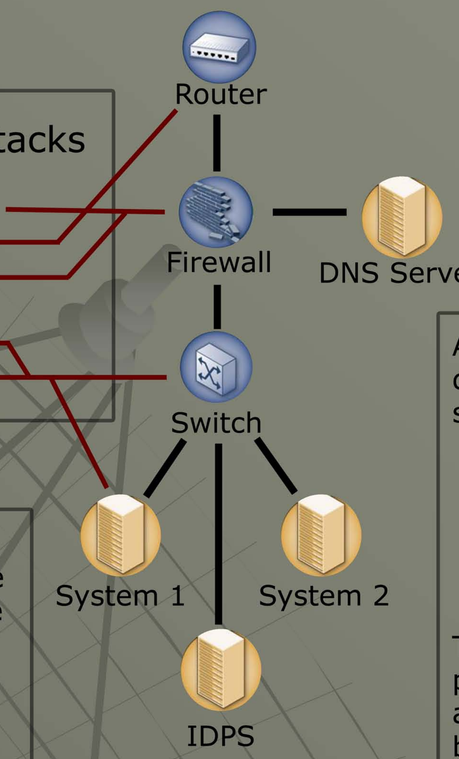
# Pseudo-Emotional Intrusion Detection and Prevention Systems

## Abstract

Intrusion detection and prevention systems have undergone rapid development in recent months; in particular, much attention has been focused toward characterizing their nature and investigating their effective deployment. However, the current state of these systems overwhelmingly relies upon low-level ruleset-based detection algorithms. To facilitate the next generation of intrusion detection systems, an open framework enabling the integration of multi-disciplinary data is necessary to allow for the development of high-level alert correlation and evaluation capabilities in intrusion detection. A framework for the integration of emotional responses in intrusion detection systems is explored here, and demonstrates significant promise.

## Types of Network Attacks

- Attempted break-in
- Masquerade
- Penetration
- Leakage
- Malicious use
- Denial of service




A complete, successful attack upon a network spans across multiple layers and cannot be detected by one sensor alone. It is necessary for an intrusion detection or prevention system (IDPS) to gather, combine, and correlate alerts from a wide range of sensors, including network as well as host sensors.

An integrated intrusion detection or prevention system (IDPS) includes:

- **event collection**
- **pre-processing**
- **attack recognition,**
- **attack correlation**
- **impact analysis**
- **reporting/response**

The more elements present, the higher-level and more intelligent the behavior.

Event Collection (gather data from packet monitors, syslogs) → Pre-processing (order chronologically)

↓ Recognition (recombine multiple events into single attack methods)

↓ Correlation (high-level pattern recognition)

↓ Impact analysis (determine effects of high-level attack)

↓ Reporting/Response (output to log for review or to disrupt attack)

## Sample implementation

### Events

| # | Event |
|---|---|
| 0001 | ICMP echo request |
| 0002 | TCP SYN 0-1023 |
| 0003 | TCP SYN 1024-2047 |
| 0004 | TCP SYN 2048-3091 |
| 0005 | Malformed TCP packet |
| 0006 | Invalid apache request |
| 0007 | Invalid apache request |
| 0008 | Invalid apache request |
| 0009 | New shell process |

### Recognition

Event:
Ping

Portscan ports 0-3091
TCP stack exploit
Apache exploit 1
Apache exploit 2
Apache exploit 3
New shell process

### Correlation

Attack progress:
Ping

Portscan ports 0-3091
TCP stack exploit - unknown
Apache exploit 1 - unknown
Apache exploit 2 - unknown
Apache exploit 3 - success?
Local access

### Impact Analysis

None

Low
Med
Med - repeat exploit from host
High - repeat exploit from host
Critical - repeat exploit (3)
Critical - unauthorized access

### Response

Log activity and severity
Close TCP 80 connection

An emotional framework can be modeled into any part of the IDPS process. Here, repetitive unproductive connections induce a level of anger, and multiple invalid requests increase fear. The biological model increases the rate at which events are sampled.

In the high-level correlation process, pre-existing levels of fear and anger modify the detection process and the assessment of risk. Having an intrinsic model of accumulating emotion is one solution to a long-standing problem of high-level risk assessment -- the level of malicious intent of the attack.

UCSD

it2 Calit2