

SPIDeR

A Distributed Multi-Agent Intrusion Detection and Response Framework

Patrick Miller

patrick@spider.doriathproject.com



Black Hat Briefings

July 31st 2003 Las Vegas, NV

Overview



Black Hat Briefings

July 31st 2003 Las Vegas, NV

Goals

- Utilize new and existing sensors collaboratively to generate threat analysis.
- Increased classification rate
- Reduced false positives



Heterogeneity

- Harder to fool
 - Artificial immune systems
- Many heads are better than one
 - Diverse computational models are appropriate when both the data and patterns are widely different.



Related Works

- EMERALD
 - <http://www.sdl.sri.com/projects/emerald/>
- Contego
 - <http://www.trigeo.com/products.php>
- Tivoli
 - <http://www.tivoli.com>
- Ect.



Framework

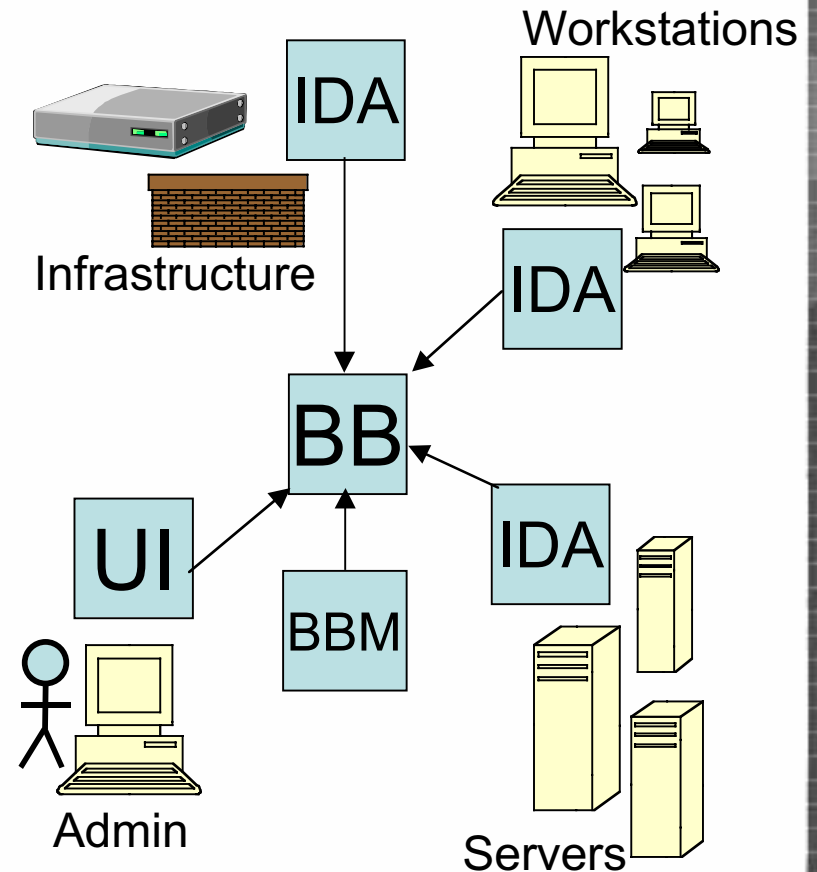


Black Hat Briefings

July 31st 2003 Las Vegas, NV

Architecture

- BB
 - Storage & Collection
- BBM
 - Response System
- UI
 - Configuration Center
- IDA
 - Intrusion Detection Agents



Network Utilization

- Low communication between agents
 - Response
 - Reinforcement signal
- Run on a dedicated network
 - VPN
 - Physical



IDAs

- Intrusion Detection Agents
 - Distributed throughout network
 - Monitor diverse data sets
- Use heterogeneous soft-computing methods
 - Reply with diverse decisions
 - Incremental Machine Learning



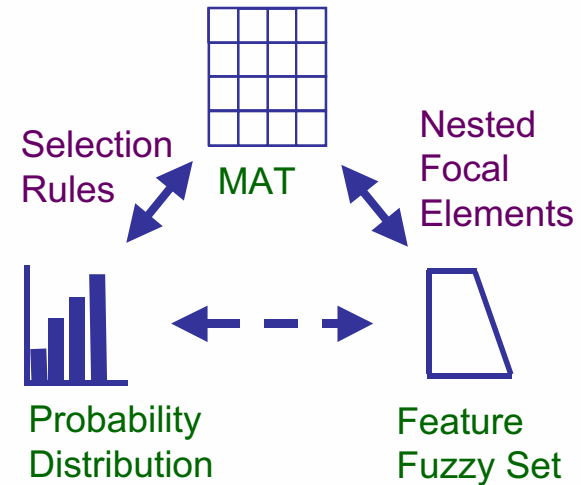
Result Correlation

- Different computational models may generate different decision types.
 - Crisp
 - Probability
 - Probability Interval
 - Fuzzy Set



MAT

- Allows integration of various decision types



- One FS – One PD (via one SR)
- One FS – Many PD (via many SR)
- Many FS – One PD (via many SR)

- Manages consistencies between a probability distribution and a fuzzy set



Team Decision Process

IDA\Decisions	X1	..	X_i	...	X_n
IDA1 (C):w1	0	..0..	1	...0...	0
IDA2 (P):w2	0.5	..0..	..0.2..	..0..	0.3
IDA3 (S):w3	(,)	...	(0.2,0.3)	...	(,)
IDA4 (F):w4	Mid	...	High	...	Low
...					
IDAm (..): w _m					

MAT (with controls on bias)

Team: 1	P1	...	P_i	...	P_n
---------	----	-----	-------	-----	-------



Decision Support

- Response generated -> decision made.
- Response can be adjusted based on
 - Detection confidence
 - Attack type
- Responses configured by administrator
- Response to new attacks
 - Learning algorithm to make best guess
 - User defined defaults



Detection Methods



Black Hat Briefings

July 31st 2003 Las Vegas, NV

Signature Detection

- Useful for detecting
 - Well known attacks
 - Attacks which can be defined by regular expressions
- Quick filtering
 - Regular expressions
 - If-Else rules
 - Good for exception cases as well
- Decision most likely crisp



Anomaly Detection

- Pros
 - Zero-day attacks
 - Privilege abuse
 - Account hi-jacking
- Cons
 - Can be trained to accept malicious use
 - Memory intensive



Anomaly Detection

- Defined in linguistic terms.
 - Normal/strange/whoa!
 - Well suited for fuzzy logic
- Most likely decision output types.
 - Fuzzy, Probability



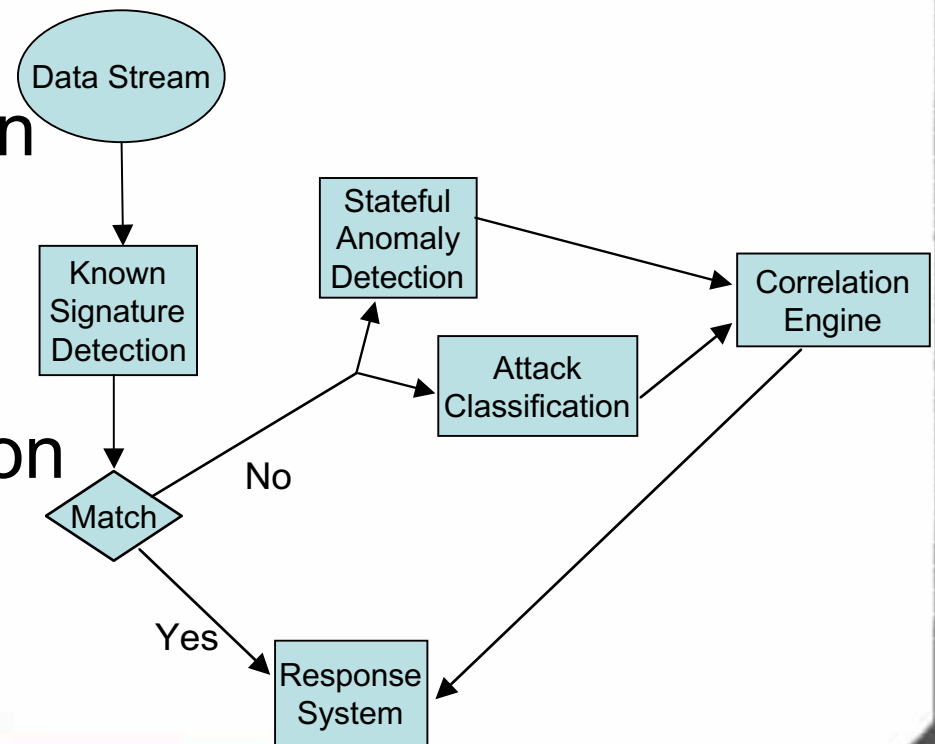
Event Classification

- Useful for
 - Determining a attack type
 - Detecting semi-known patterns of attack.
- Variety of methods
 - Self Organizing Maps
 - Rule-based systems
- Decision may be
 - Fuzzy, Probability



IDAs

- Single IDA can be a miniature multi-agent system.
 - Signature detection
 - Anomaly detector
 - Attack classifier
 - Decision Correlation



Classification Methods



Black Hat Briefings

July 31st 2003 Las Vegas, NV

Soft Computing

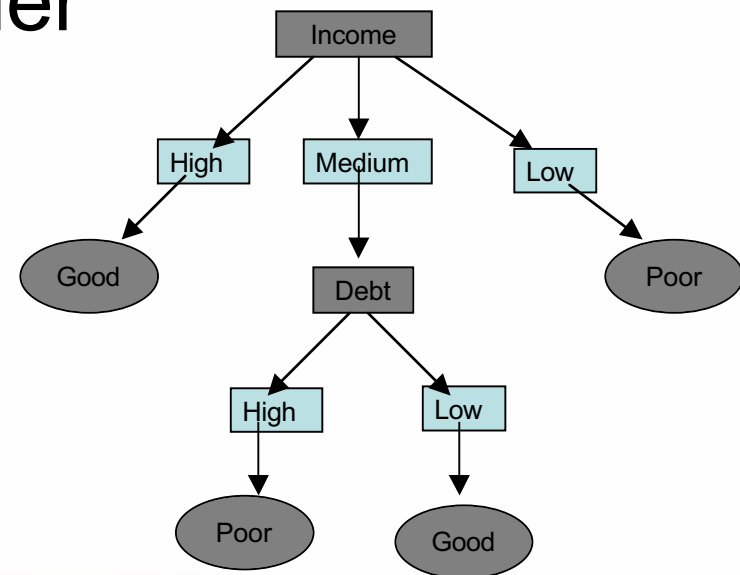
- Computational models

	Anomaly	Classification Signature	Speed	Adaptability	
– Fuzzy Logic	○	○	○	Good	Avg
– Decision Tree	○	○		Best	Poor
– Neural Network	○		○	Avg	Good
– Self Organizing Map	○		○	Avg	Best
– Genetic Algorithm			○	Poor	Good



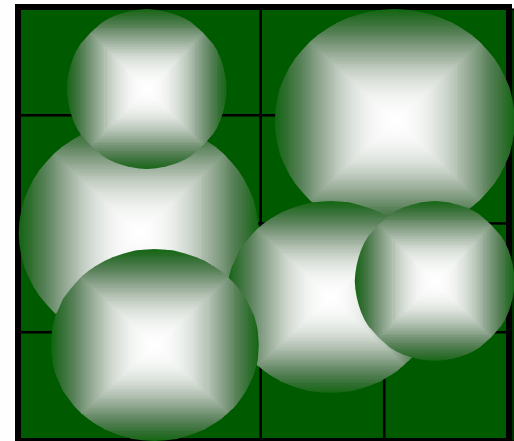
ID3 Trees

- Build decision tree to make evaluations
 - Use information gain, derived from entropy
- Binary or N-ary classifier
- Slow to train
- Fast to execute
- Does not support reinforcement learning



Self-Organizing Maps

- Build decision map based on input values
 - Correlates input to a map index indicating a classification type.
 - Updates map during train and execution.
 - Resulting map generated based on initial configuration values.
- Binary or N-ary classifier
- Moderately slow to train
- Moderate execution time
- Highly reinforceable



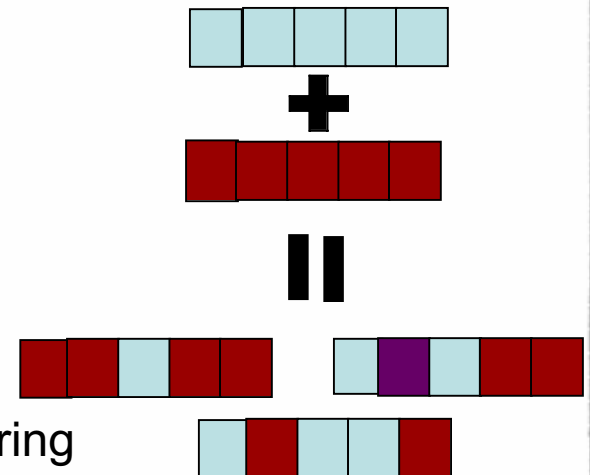
Fuzzy Logic

- Description
 - Expresses responses linguistically
- Strengths
 - Intuitive human interface
 - More human response, harder to detect
- Weaknesses
 - Response may be incorrectly interpreted



Genetic Algorithms

- Description
 - Simulate evolutionary process
 - Copy genes from both parents
 - Allow some random mutations
 - Test child for fitness
 - Use fitness to determine number of offspring
- Strengths
 - Highly scaleable
 - Determine optimal configurations
 - Useful for determining optimal initialization values
- Weaknesses
 - Can be very slow



Reinforcement



Black Hat Briefings

July 31st 2003 Las Vegas, NV

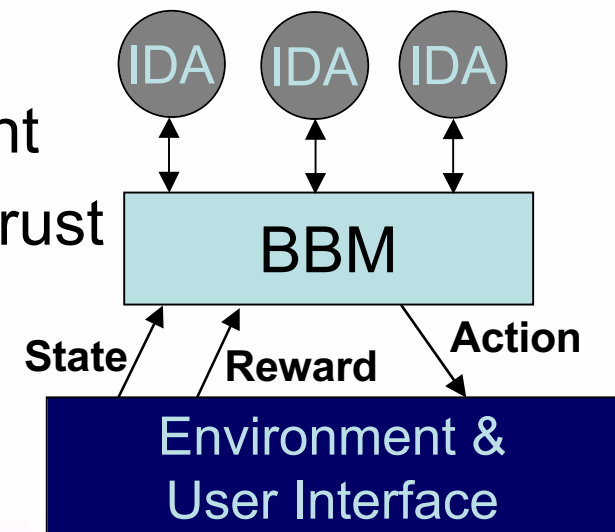
Reinforcement Learning

- Rule updates
 - Internal decision process is self modifying based on live traffic data.
 - Varies with different computational models
- Trust bias
 - Used to weight the response from specific sensors with regard to past performance.



Trust Bias

- Rewards/penalty distributed among IDAs
 - Team adjusts trust of individual IDAs
- Adaptive IDAs
 - React to reward/penalty
 - Notify team of their improvement
 - Team may choose to readjust trust



Bias Distribution

IDA\Decisions	X1	..	Xi	...	Xn
IDA1 (C):w1	0	..0..	1	...0...	0
IDA2 (P):w2	0.5	..0..	..0.2..	..0..	0.3
IDA3 (S):w3	(,)	...	(0.2,0.3)	...	(,)
IDA4 (F):w4	Mid	...	High	...	Low
...					
IDAm (...):wm					

MAT (with controls on bias)

Team: 1	P1	...	Pi	...	Pn
----------------	----	-----	----	-----	----



Incremental Machine Learning

- Detection and response systems adapt to changing environment.
 - Normal use changes over time
 - New variations of known attack types
 - Response type may change over time



Optimization



Black Hat Briefings

July 31st 2003 Las Vegas, NV

Dynamic IDA Generation

Improve Accuracy

- **If:**
 - Low confidence decision
 - Anomalies are disproportionate to classified attacks
- **Then:**
 - Build new sensor



Dynamic IDA trimming

Improve Efficiency

- **If:**
 - IDA drops below a trust threshold
 - IDA uses too much processing time
 - determined by the administrator
- **Then:**
 - Refactor decision process
 - Remove IDA



Testing

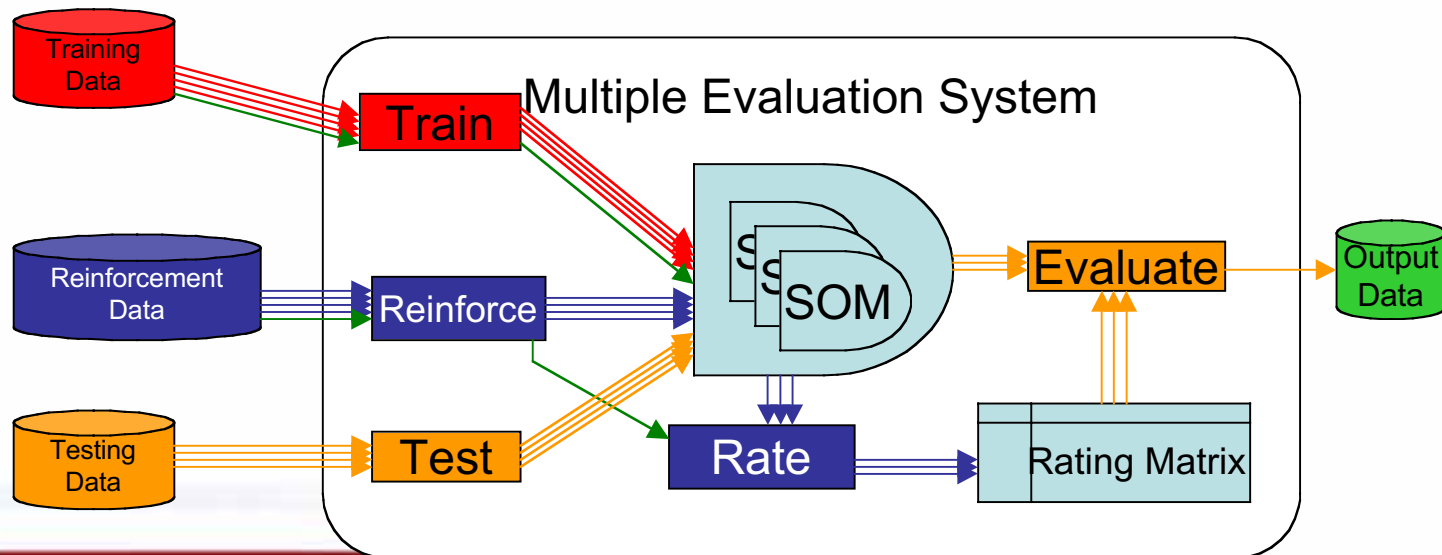


Black Hat Briefings

July 31st 2003 Las Vegas, NV

Prototype

- Multiple SOMs
 - Each SOM has different initial values.
 - SOMs trained with a supervised data set
 - KDD Cup '99 Data set
 - <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>



Results

- Current results available at
 - <http://spider.doriathproject.com/results/>



Experiment Conclusions

- Increase in accuracy
 - Decrease in false attacks
 - Decrease in false normals
- Increase in consistency
 - System reliability increases
- Increase in time
 - Multiple systems take longer to classify
 - Code not optimized for speed



Conclusions



Black Hat Briefings

July 31st 2003 Las Vegas, NV

Pros

- Increased effectiveness of attack detection and classification.
- Reduced false positives
- Increased ability to detect IDS avoidance methods.
- Able to integrate with existing devices



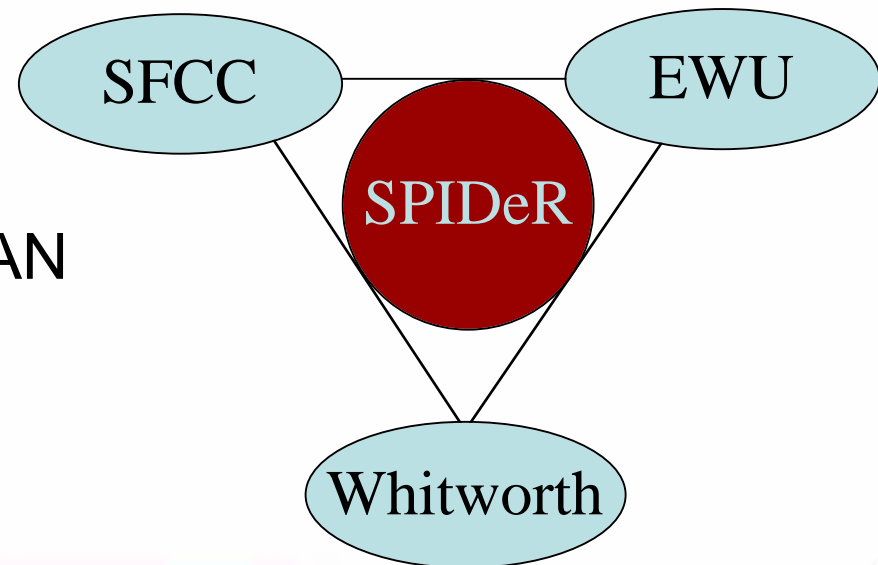
Cons

- Increased time to process inputs
- Requires dedicated systems
- Secondary network to secure communication



Current work

- SPIDeR-NeST
 - Live implementation
 - IP traffic
 - Firewall Logs
 - VP-Net
 - High bandwidth WAN



Contact Info

- Patrick Miller
patrick@spider.doriathproject.com
- Atsushi Inoue
atsushi.inoue@ewu.edu
- Web Site
<http://spider.doriathproject.com>



References

- [1] S. Axelsson, "Intrusion Detection Systems: A Survey and Taxonomy," Technical Report 99-15, Department of Computer Engineering, Chalmers University, March 2000.
- [2] T. M. Mitchell, Machine Learning, McGraw-Hill, 1997.
- [3] L. A. Zadeh, "From Computing with Numbers to Computing with Words: From Manipulation of Measurements to Manipulation of Perceptions," IEEE Transactions on Circuits and Systems I, Vol. 45, No. 1, pp. 105-119, 1999.
- [4] D. Dubois, H. Prade, "Possibility Theory in Constraint Satisfaction Problems: Handling Priority, Preference, and Uncertainty," Applied Intelligence 6, pp. 287-309, 1996.
- [5] M. Togai, H. Watanabe, "Expert System on a Chip: An Engine for Real-Time Approximate Reasoning," IEEE Expert, Vol. 1, no. 3, pp. 55-62, 1986.
- [6] G. Nieto, et. al., "A VHDL Library for Hardware Implementation of Fuzzy Knowledge Based Expert Systems Represented on a FPN," Proceedings of IPMU-2000, pp. 902-909, Madrid, Spain, 2000.
- [7] J.F. Baldwin, et al., FRIL: Fuzzy and Evidential Reasoning in AI, Research Studies Press, 1995.
- [8] G. Shafer, A Mathematical Theory of Evidence, Princeton University Press, 1976.
- [9] L. A. Zadeh, "Toward a theory of fuzzy information granulation and its centrality in human reasoning and fuzzy logic," Fuzzy Sets and Systems 90, pp. 111-127, 1997.



Fin



Black Hat Briefings

July 31st 2003 Las Vegas, NV