THE UNIVERSITY OF OKLAHOMA

THREE APPROACHES TO INTRUSION DETECTION

Analysis and Enhancements

VI National Computer and Information Security Conference

ACIS – COLOMBIA

by

Pedro A. Diaz-Gomez and Dean F. Hougen

June 2006

Outline

- Goal
- Basic Concepts
- The Three Models
- Denning — Intrusion Detection Model
- Crosbie & Spafford — Genetic Programming
- Mé — Genetic Algorithms
- Conclusions & Future Work

Goal

- To review and analyse three approaches to intrusion detection:
  - An Intrusion-Detection Model

    by Dorothy Denning
  - Applying Genetic Programming to Intrusion Detection

    by Mark Crosbie and Eugene H. Spafford
  - Security Audit Trail Analysis Using Genetic Algorithms

    by Ludovic Mé

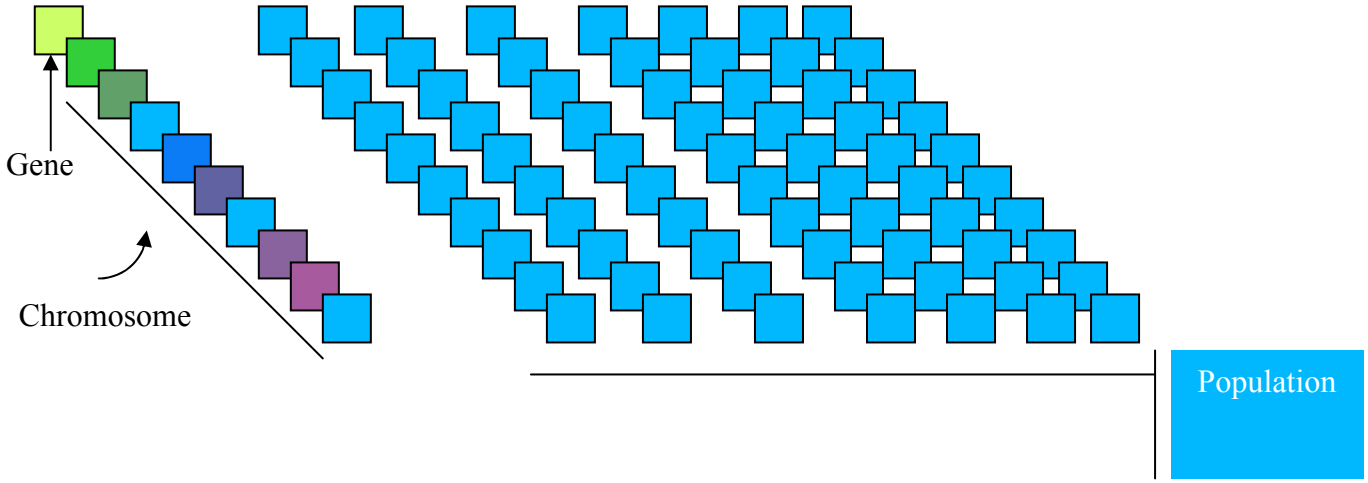
Basic Concepts: Intrusion Detection Systems

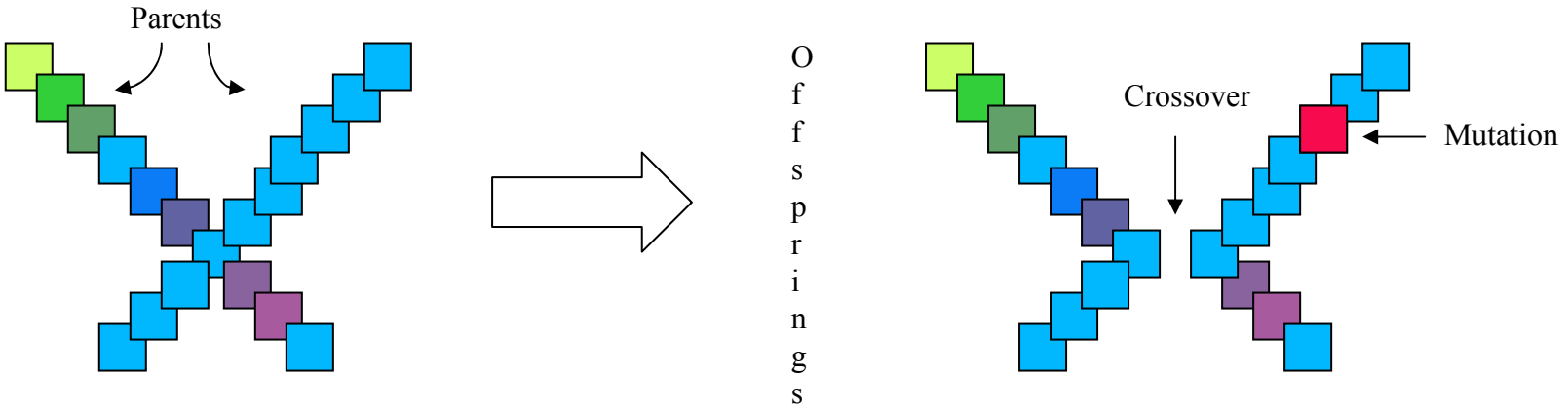
- *Intrusion Detection System* (*IDS*)
  - system to detect intrusions in a computer or computer network
- *Intrusion*
  - unauthorized attempt to access a system
- *Security Auditing*
  - formal examination of actions taken by system users
- *Audit Data*
  - records of actions taken by identifiable and authenticated users

Basic Concepts: Evolutionary Computation (EC)

- Inspired by Biological Evolution
  - Biological Evolution
    - Creates and Modifies Species by Natural Selection
  - Evolutionary Computation
    - Creates and Modifies "Solutions" by Artificial Selection
- *Genes — Hereditary Units that* Determine Characteristics
- *Chromosomes* — Collections of Genes in Individuals
- *Populations — Collections* of Individuals

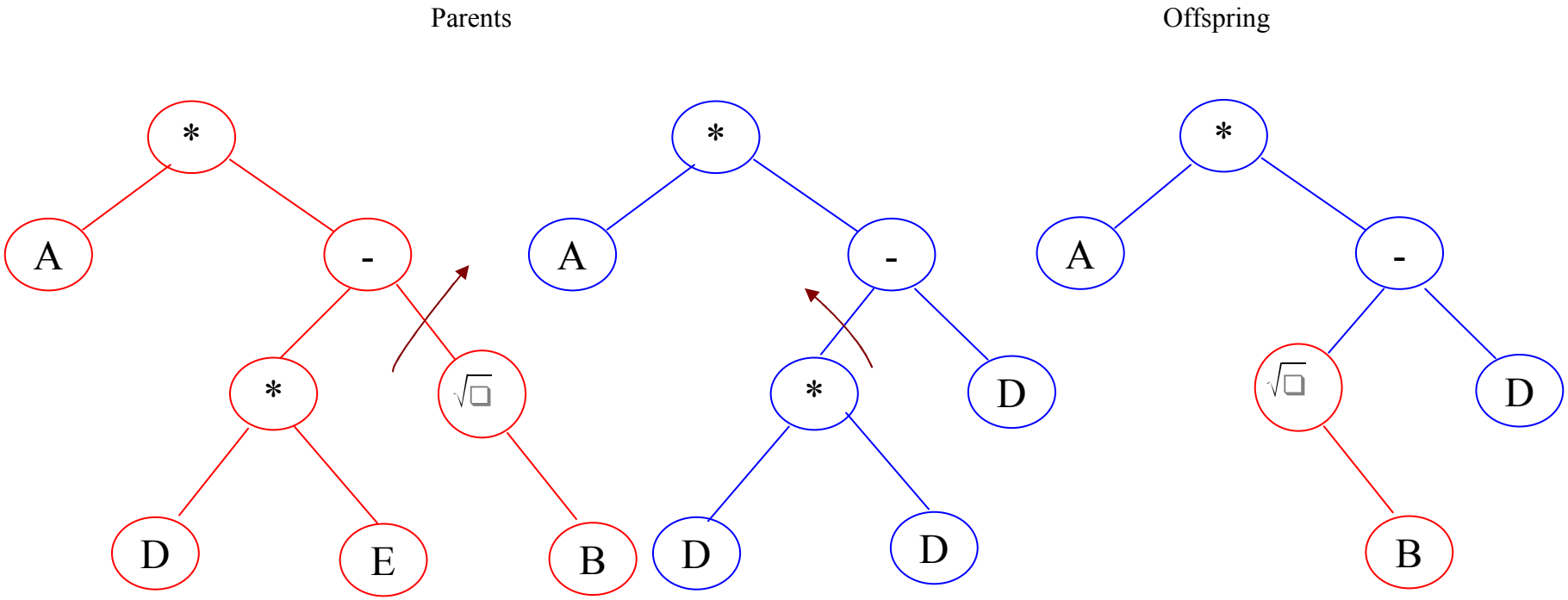
Basic Concepts: Evolutionary Computation (EC)





Basic Concepts: Genetic Programming (GP)

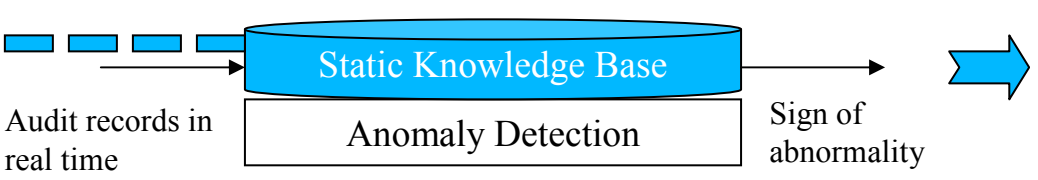
- John Koza has used a form of EC to evolve Lisp programs
- Programs in Lisp can be expressed as *parse trees*



Outline

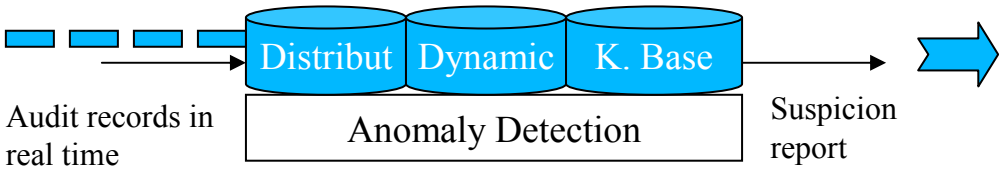
- Goal
- Basic Concepts
- ✓ The Three Models
- Denning — Intrusion Detection Model
- Crosbie & Spafford — Genetic Programming
- Mé — Genetic Algorithms
- Conclusions & Future Work

The Three Models



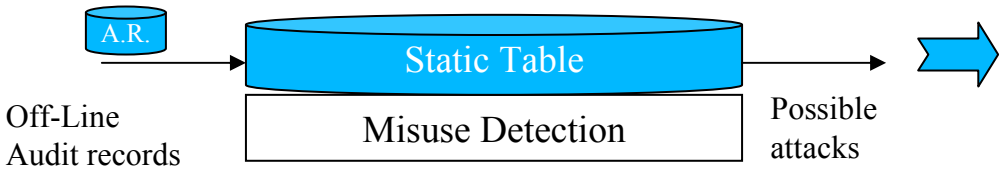
Denning's Model

Rules Pre coded.
Anomaly Detection
Using those Rules.



Crosbie & Spafford Prototype

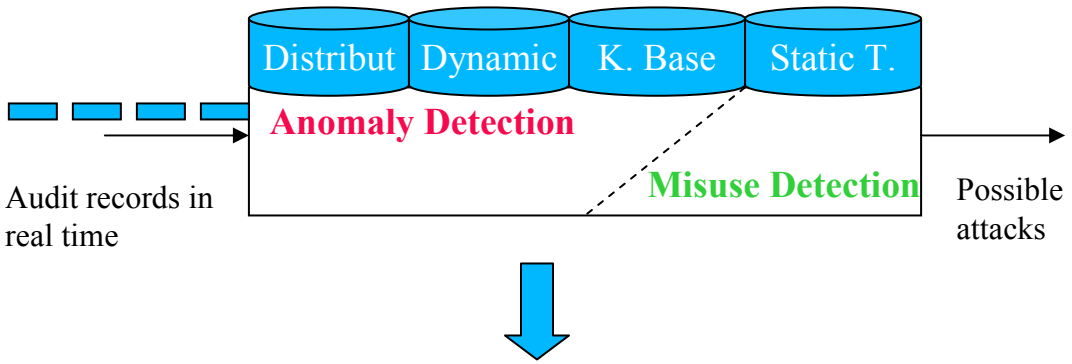
Rules using GP.
Anomaly Detection using
Those Rules



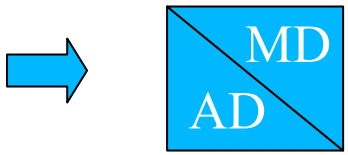
Mé's Audit Trail Analysis

Intrusions Pre coded.
Pattern Matching

The Three Models Complemented



- Distributed K. Base
- Using AI to generate them.
- Known Attacks.
- Real Time System



Outline

- Goal
- Basic Concepts
- The Three Models
- ✓ Denning — Intrusion Detection Model
- Crosbie & Spafford — Genetic Programming
- Mé — Genetic Algorithms
- Conclusions & Future Work

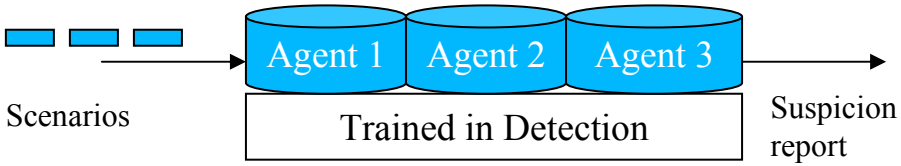
Denning's Intrusion Detection Model Components

- The model has six *components*:
  - Subjects,
  - Objects,
  - Audit records,
  - Profiles,
  - Anomaly records, and
  - Activity rules.

Outline

- Goal
- Basic Concepts
- The Three Models
- Denning — Intrusion Detection Model
- ✓ Crosbie & Spafford — Genetic Programming
- Mé — Genetic Algorithms
- Conclusions & Future Work

A *GP* Intrusion Detection Model



Training Scenarios

Type of scenario	*Outcome*
10 connections with 1 second delay	90%
10 connections with 5 second delay	70%
10 connections with 30 second delay	40%
10 connections every minute	30%
Rapid connections, then random pauses	80%
Intermittent connections	10%
Connections to privileged ports	90%
Connections to any port	70%

Crosbie and Spafford.
Applying Genetic programming to Intrusion Detection.

A *GP* Intrusion Detection Model Suspicion reported by Agents

Suspicion Value

Activities	*Agent 1*	*Agent 2*	*Agent 3*
Connections to privileged ports	83%	100%	98%
Login then long pauses then logins	31%	26%	0%
Logins and ftp with long pauses	73%	47%	25%

Training Scenarios

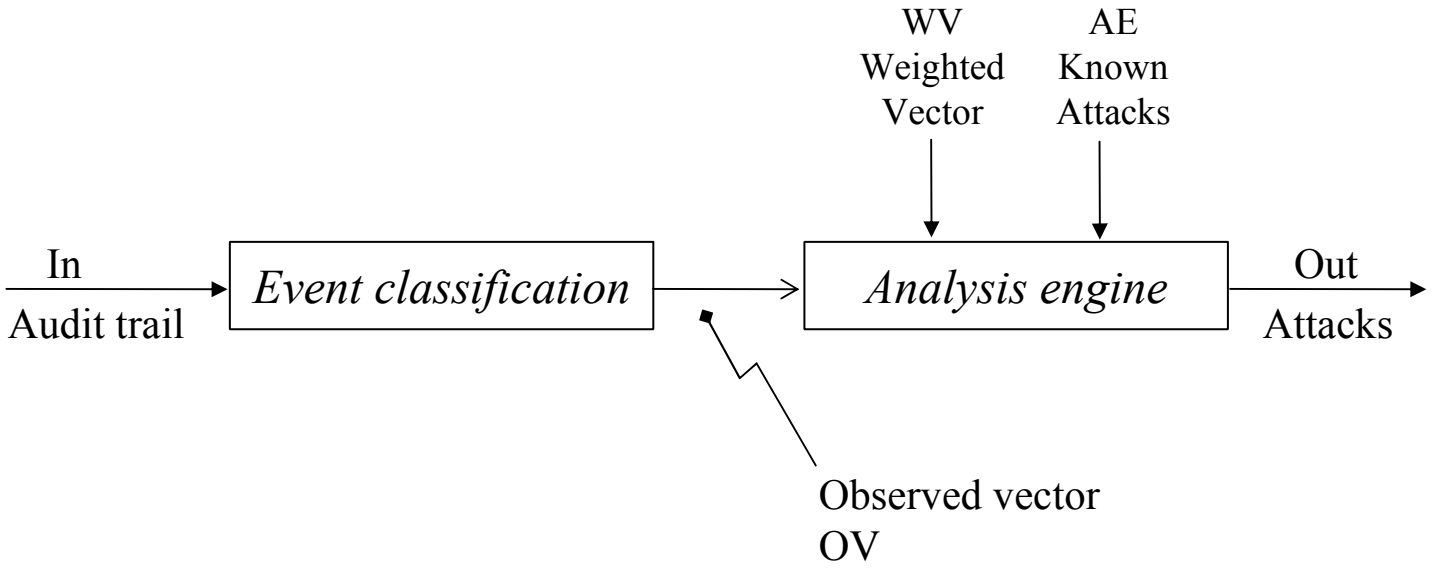
Type of scenario	*Outcome*
10 connections with 1 second delay	90%
10 connections with 5 second delay	70%
10 connections with 30 second delay	40%
10 connections every minute	30%
Rapid connections, then random pauses	80%
Intermittent connections	10%
Connections to privileged ports	90%
Connections to any port	70%

Crosbie and Spafford.
Applying Genetic programming to Intrusion Detection.

Outline

- Goal
- Basic Concepts
- The Three Models
- Denning — Intrusion Detection Model
- Crosbie & Spafford — Genetic Programming
- ✓ Mé — Genetic Algorithms
- Conclusions & Future Work

A *Genetic Algorithm Approach* Architecture



THE UNIVERSITY OF OKLAHOMA

A *Genetic Algorithm Approach* - Constraint

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	I	MV	Ov	Fails
0	3																								0	0	0	0
1					1																				0	0	0	0
2				1																					0	**1**	0	1
3		3																							1	0	0	0
4			3																						0	0	0	0
5		3							8																1	**8**	0	1
6						5														1		5			1	**10**	0	1
7						30																			1	30	76	0
8							5																		1	**5**	0	1
9										3															0	0	0	0
10											2														1	2	20	0
11												3													1	**3**	0	1
12															10	1									1	0	0	0
13																1									0	0	6	0
14																1									0	0	0	0
15																								4	0	4	4	0
16																				1					0	0	0	0
17		3				35	5		8	3	2	3			10	3		300		2		5		4	0	62	94	0
18																			100						1	**100**	0	1
19								5																	0	5	42	0
20														10											1	0	0	0
21																				1					1	0	0	0
22															10										0	0	0	0
23																						5			1	5	5	0
24																							1			0	0	0
25					1																3					3	459	0
26													30													30	1335	0
27																	50									0	0	0

A *Genetic Algorithm Approach* Fitness Function

- The fitness function proposed by Ludovic Mé

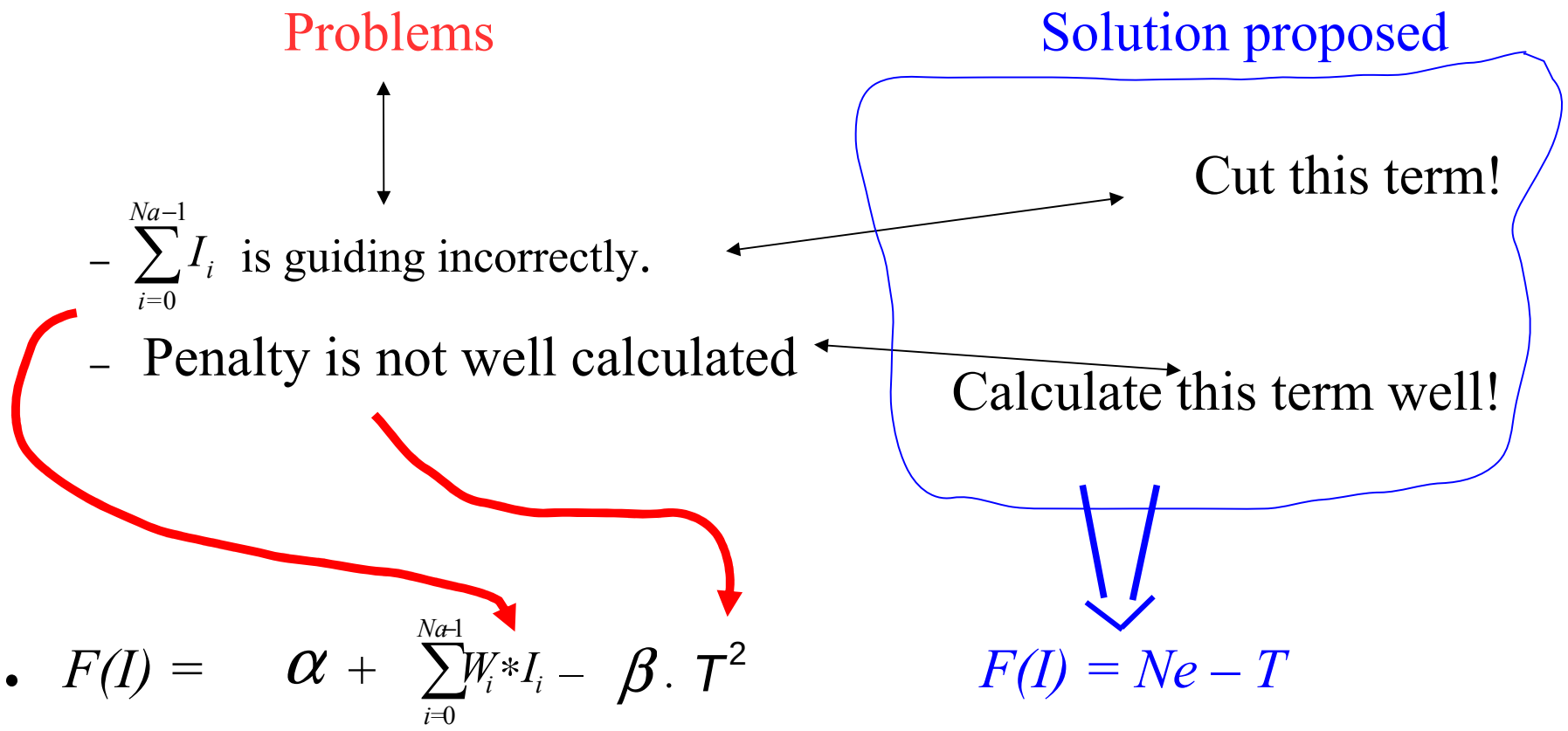
$$F(I) = \alpha + \sum_{i=0}^{Na-1} W_i * I_i - \beta . T^2$$

  - Hypothesis *I* is found such that:

    - $\sum_{i=0}^{Na-1} W_i * I_i$ is maximized, and

    - $\sum_{j=0}^{Na-1} AE_{ij} * I_j \leq O_j$, for all $1 \leq i \leq N_e$. Constraint.

A *Genetic Algorithm Approach*
Fitness Function – Our Proposal



A Genetic Algorithm Approach
Fitness Function – Our Proposal

$$F(I) = Ne - T$$

User	Average of 10 runs			% deviation		%
	False +	False -	Detected	False +	False -	Detected
2051_7	0	0	3	0%	0%	100%
2051_11	0	0	4	0%	0%	100%
2506_15	0	0	4	0%	0%	100%
Zero Vector	0	0	0	0%	0%	100%
One Intrus.	0	0.1	0.9	0%	10%	90%
Two Intrus.	0	0	0	0%	0%	100%
Three Intrus.	0	0	3	0%	0%	100%

Outline

- Goal
- Basic Concepts
- The Three Models
- Denning — Intrusion Detection Model
- Crosbie & Spafford — Genetic Programming
- Mé — Genetic Algorithms
- ✓ Conclusions & Future Work

Conclusions & Future Work

- Denning's Model
  - The assumption of abnormal as deviation from normality is a good start

- Our proposals
  - Could be complemented with *misuse* detection
  - Use of *sentinel profiles* for non common activity
  - Use of tendency of the mean

Conclusions & Future Work

- Denning's Model
  - Use of profiles, metrics and models is a great idea

- Our proposals
  - Try to overcome the heavy of the system
    - *Distributivity*
    - *Maintenance*
    - *Risk analysis*

Conclusions & Future Work

- Denning's Model
  - Use of Classes of Profiles is prominent

- Our proposals
  - Take into account the *number of users in each Class*
    - Complement with the use of the tendency of the mean

Conclusions & Future Work

- Crosbie & Spafford Model
  - Idea of use of distributed Agents is excellent

- Our proposals
  - Take into account
    - The *control* of those
    - The *overload* impose in the system

Conclusions & Future Work

- Crosbie & Spafford Model
  - Use of GP in order to improve the capture of novel attacks

- Our proposals
  - *Specification* of
    - Fitness function and its parameters
    - Parameters of the evolution
    - SAL and MUX

Conclusions & Future Work

- Crosbie & Spafford Model
  - Use of GP in order to improve the capture of novel attacks

- Our proposals
  - *More test*
  - *Compare future results with other approaches*

Conclusions & Future Work

- Mé Model
  - Join objective and constraint in the fitness function

- Our proposals
  - *New fitness function* that uses only the constraint and
  - The objective is obtained with a new operator: the *union operator*

Conclusions & Future Work

- Mé's Model
  - Good idea to use a matrix of misuse, and to encode intrusions as a chromosome

- Our proposals
  - Augment the system with the possibility of
    - *Consider different users*
    - *Consider more intrusions*
    - *report user activity not considered in the analysis*

Conclusions & Future Work

- Mé's Model
  - Use a matrix of misuse, and to encode intrusions as a chromosome

- Our proposals
  - Augment the system with the possibility of
    - *capture novel attacks*
    - *capture abnormal activity*
    - *disaggregate intrusions as exclusive*

THE UNIVERSITY OF OKLAHOMA

Thanks!

I would like to thank The University of Oklahoma for sponsoring this trip to Acis-Colombia.

I would like to thank Dr. Dean Hougen, for his advising, support and patience. From him, I learned not only in the classroom, but with his example, the way to do science and be better.

I would like to thank ACIS for this opportunity to share our research experiences and learn from a selected group of Panellists

Bibliografy

- D. E. Denning. An Intrusion-detection Model. In proceeding of the 1986 IEEE Symposium on Security and Privacy
- M. Crosbie and G. Spafford. Applying Genetic Programming to Intrusion Detection. In Papers from 1995 AAAI Fall Symposium
- L. Mé. Gassata, a Genetic Algorithm as an Alternative Tool for Security Audit Trail Analysis. In First International Workshop on the Recent Advances in Intrusion Detection. Belgium 1998
- P. Diaz-Gomez and D. Hougen
  - Analysis of an Off-Line Intrusion Detection System. A Case Study in Multi-Objective Genetic Algorithms In Proceedings of the Florida Artificial Intelligence Research Society Conference 2005
  - Improved Off-Line Intrusion Detection using a Genetic Algorithm In Proceedings of the Seventh International Conference on Enterprise Information Systems, 2005
  - Analysis and Mathematical Justification of a Fitness Function used in an Intrusion Detection System In Proceedings of the Seventh Annual Genetic and Evolutionary Computation Conference 2005

QUESTIONS