REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
24-06-2008	Final Report	1-Apr-2005 - 30-Jun-2008

4. TITLE AND SUBTITLE
Final Report of "An Information-Theoretic Framework for Evaluating and Optimizing Intrusion Detection Performance"

5a. CONTRACT NUMBER
W911NF-05-1-0139

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS
Wenke Lee

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Georgia Institute of Technology
Office Of Contract Administration
Program Initiation Division
Atlanta, GA 30332 -0420

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
48310-CI.1

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
We conducted in-depth study of performance metrics used in evaluating intrusion detection systems. We define Intrusion Detection Capability as the ratio of mutual information between the IDS input and output to the entropy of the input. It integrates all the important factors into a single metric. We showed that this new metric is very sensitive to IDS operation parameters. We also defined information-theoretic metrics to measure the effectiveness of an IDS in terms of feature representation capability, classification information loss and the overall intrusion detection capability. We showed that intrusion detection capability is equal to the feature representation capability minus the classification information loss. Finally,

15. SUBJECT TERMS
intrusion detection, performance metrics, information theory, alert fusion, decision theory

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Wenke Lee
U	U	U	SAR		19b. TELEPHONE NUMBER 404-385-2879

Report Title

Final Report of "An Information-Theoretic Framework for Evaluating and Optimizing Intrusion Detection Performance"

ABSTRACT

We conducted in-depth study of performance metrics used in evaluating intrusion detection systems. We define Intrusion Detection Capability as the ratio of mutual information between the IDS input and output to the entropy of the input. It integrates all the important factors into a single metric. We showed that this new metric is very sensitive to IDS operation parameters. We also defined information-theoretic metrics to measure the effectiveness of an IDS in terms of feature representation capability, classification information loss and the overall intrusion detection capability. We showed that intrusion detection capability is equal to the feature representation capability minus the classification information loss. Finally, we proposed a decision-theoretic IDS alert fusion technique based on the likelihood ratio test (LRT).

List of papers submitted or published that acknowledge ARO support during this reporting period. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Number of Papers published in peer-reviewed journals: 0.00

(b) Papers published in non-peer-reviewed journals or in conference proceedings (N/A for none)

Number of Papers published in non peer-reviewed journals: 0.00

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts): 0

Peer-Reviewed Conference Proceeding publications (other than abstracts):

1. Measuring Intrusion Detection Capability: An Information-Theoretic Approach. ?Guofei Gu, Prahlad Fogla, David Dagon, Wenke Lee, and Boris Skoric. ?In Proceedings of ACM Symposium on InformAction, Computer and Communications Security (ASIACCS '06), Taipei, Taiwan, March 2006.

2. Towards an Information-Theoretic Framework for Analyzing Intrusion Detection Systems. Guofei Gu, Prahlad Fogla, David Dagon, Wenke Lee, and Boris Skoric. ?In Proceedings of The 11th European Symposium Research Computer Security (ESORICS 2006) , Hamburg, Germany, September 2006.

3. Principled Reasoning and Practical Applications of Alert Fusion in Intrusion Detection Systems. Guofei Gu, Alvaro A. Cardenas and Wenke Lee. In Proceedings of ACM Symposium on InformAction, Computer and Communications Security (ASIACCS '08), Tokyo, Japan, March 2008.

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts): 3

(d) Manuscripts

Number of Manuscripts: 0.00

Number of Inventions:

Graduate Students

NAME	PERCENT_SUPPORTED
Prahlad Fogla	0.50
Guofei Gu	0.50
FTE Equivalent:	**1.00**
Total Number:	**2**

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Wenke Lee	0.25	No
FTE Equivalent:	**0.25**	
Total Number:	**1**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period:	0.00
The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:.....	0.00
The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:.....	0.00
Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):	0.00
Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:	0.00
The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense	0.00
The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:	0.00

Names of Personnel receiving masters degrees

NAME
Total Number:

Names of personnel receiving PHDs

NAME
Prahlad Fogla (August, 2007)
Guofei Gu (August, 2008)
Total Number: 2

Names of other research staff

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Sub Contractors (DD882)

Inventions (DD882)

I. Project Activities and Findings:

We conducted in-depth analysis of existing metrics used in evaluating intrusion detection systems, and illustrated the shortcomings and limitations of these metrics. We define Intrusion Detection Capability as the ratio of mutual information between the IDS input and output to the entropy of the input. It integrates all the important factors into a single metric. We showed that this new metric is very sensitive to IDS operation parameters. This means that the new metric can be used to guide the fine-tuning of IDS. This work was published in the ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS '06).

We also worked on an information-theoretic framework for analyzing intrusion detection systems. We defined information-theoretic metrics to measure the effectiveness of an IDS in terms of feature representation capability, classification information loss and the overall intrusion detection capability. We showed that intrusion detection capability is equal to the feature representation capability minus the classification information loss. This means that each IDS step/component need to preserve "information" from the raw data, e.g., feature selection/construction algorithms need to be improved to distinguish attack/normal samples. This work is to appear in the 11th European Symposium on Research in Computer Security (ESORICS 2006).

We also worked on IDS alert fusion (i.e., how to effectively use multiple IDSs). It is generally believed that by combining several diverse intrusion detectors (i.e., forming an IDS ensemble), we may achieve better performance. However, there has been very little work on analyzing the effectiveness of an IDS ensemble. We studied the following problem: how to make a good fusion decision on the alerts from multiple detectors in order to improve the final performance. We proposed a decision-theoretic alert fusion technique based on the likelihood ratio test (LRT). We evaluated this technique using empirical studies, and formally analyzed its practical interpretation based on ROC curve analysis. Through theoretical reasoning and experiments using multiple IDSs on several data sets, we showed that our technique is more flexible and also outperforms other existing fusion techniques such as AND, OR, majority voting, and weighted voting. This work was published in the ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS '08).