REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
APRIL 2013	CONFERENCE PAPER (Post Print)	JAN 2011 – MAR 2013

4. TITLE AND SUBTITLE

USER SELECTION OF CLUSTERS AND CLASSIFIERS IN BBAC

5a. CONTRACT NUMBER
FA8750-12-C-0011

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
62788F

6. AUTHOR(S)

Michael Mayhew; Aaron Adler; Jeffrey Cleveland; Michael Atighetchi

5d. PROJECT NUMBER
E2BB

5e. TASK NUMBER
BB

5f. WORK UNIT NUMBER
AC

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Raytheon BBN Technologies
10 Moulton Street
Cambridge, MA 02138

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory/Information Directorate
Rome Research Site/RIEBA
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TP-2013-004

12. DISTRIBUTION AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PA Case Number: 88ABW-2013-0128
DATE CLEARED: 14 JAN 2013

13. SUPPLEMENTARY NOTES
Proceedings International Conference on Intelligent User Interfaces (IUI), 2013 Workshop on Interactive Machine Learning, 19-22 March, Santa Monica, CA. This work is copyrighted. One or more of the authors is a U.S. Government employee working within the scope of their Government job; therefore, the U.S. Government is joint owner of the work and has the right to copy, distribute, and use the work. All other rights are reserved by the copyright owner.

14. ABSTRACT

The Behavior-Based Access Control (BBAC) project seeks to address the increasingly sophisticated attacks and attempts to exfiltrate or corrupt critical sensitive information. BBAC uses statistical machine learning techniques (clustering and classification) to make predictions about the intent of actors establishing TCP connections and HTTP requests. Administrators will need to assign new computers to appropriate clusters, to be alerted about changes in cluster assignments, to select classifiers and settings to use, and to monitor accuracy of the system. We discuss the requirements and our current approach in this Interactive ML application domain.

15. SUBJECT TERMS
Interactive, application domain, user, classifier, clustering, user-centered design

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			MICHAEL J. MAYHEW
U	U	U	UU	3	19b. TELEPHONE NUMBER (*Include area code*) N/A

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

User Selection of Clusters and Classifiers in BBAC

Aaron Adler
Raytheon BBN Technologies
10 Moulton Street
Cambridge, MA 02138 USA
aadler@bbn.com

Jeffrey Cleveland
Raytheon BBN Technologies
10 Moulton Street
Cambridge, MA 02138 USA
jcleveland@bbn.com

Michael J. Mayhew
Air Force Research Laboratory
525 Brooks Road
Rome, NY 13441 USA
Michael.Mayhew@rl.af.mil

Michael Atighetchi
Raytheon BBN Technologies
10 Moulton Street
Cambridge, MA 02138 USA
matighet@bbn.com

This work was sponsored by the Air Force Research Laboratory (AFRL). Distribution A. Approved for public release; distribution unlimited (Case Number 88ABW-2013-0128).

Abstract
The Behavior-Based Access Control (BBAC) project seeks to address the increasingly sophisticated attacks and attempts to exfiltrate or corrupt critical sensitive information. BBAC uses statistical machine learning techniques (clustering and classification) to make predictions about the intent of actors establishing TCP connections and HTTP requests. Administrators will need to assign new computers to appropriate clusters, to be alerted about changes in cluster assignments, to select classifiers and settings to use, and to monitor accuracy of the system. We discuss the requirements and our current approach in this Interactive ML application domain.

Author Keywords
Interactive, application domain, user, classifier, clustering

ACM Classification Keywords
H.5.2 [Information interfaces and presentation (e.g., HCI)]: User-centered design.

Introduction
Current cyber security monitoring systems have several shortcomings: they 1) have narrow focus and are signature-based, 2) use static policies, and 3) don't use audit data for analysis until it is too late. This leaves systems vulnerable to sophisticated attacks including

0-day and insider attacks. Behavior-Based Access Control (BBAC) [2] seeks to address these issues by performing analysis at multiple layers, including the network layer, application layer, and document layer. BBAC uses clustering to form groups of computers that have similar behavior. Classifiers are then trained for each cluster. Currently we are using both HTTP and TCP logs in our analyses. The techniques we use for HTTP data processing are similar to those used by Ma et al. [1] to detach malicious URLs. Our architecture is based on a cloud framework that will allow the clustering and classifiers to be trained at least once a day and will allow rapid classification of computer behavior.

User Interaction

The users for BBAC will be system administrators interacting with both the training side of the system as well as the real-time monitoring part of the system.

During the training phase, the system will re-analyze the clusters and build new classifiers. Changes in clustering might trigger user notifications as well as changes in classifier performance. Our system will compare its performance using newly trained classifiers against the previous baseline and note changes in behavior. Depending on operating conditions, different latency, and true positive and false positive rates may be desired. As system administrators are unlikely to be experts in machine learning, a key question we will need to answer is how to best present the accuracy of the re-trained classifiers. Additionally, our system will train multiple classifiers with different settings. A second key question is what data should be provided to enable the user to select a classifier.

New computers will be added to the system and will need to be assigned to a cluster. Initially there will not be any behavioral data for a new computer, therefore the administrator will have to assign it to a cluster manually. Thus clusters must have user-friendly descriptions that permit manual cluster assignments. Once the new computer has been active long enough, it can be automatically re-clustered. These and other changes in clusters should be approved by the administrator.

Alert information must be displayed to the administrator together with some notion of the accuracy and severity of the alert. In some cases the system may be able to immediately curtail the user's action – e.g., block an HTTP request – while other cases might require human review. The appropriate course of action will inevitably depend on the operating context of the system (as controlled by the administrator).

Finally the administrator should be able to see information about the system state – our cloud based architecture will allow additional resources to be used for both training and classification. The administrator should be able to control these settings to adjust the system performance.

In order to make the BBAC system usable, presenting key data to the administrator is vital. The administrator must be able to assign new computers to clusters, select between classifiers, approve changes to clusters, and be alerted to suspicious behavior.

References

[1] Ma, J., Saul, L. K., Savage, S., and Voelker, G. M. Learning to detect malicious urls. *ACM Trans. Intell. Syst. Technol. 2*, 3 (May 2011), 30:1–30:24.

[2] Raytheon BBN Technologies. BBAC home page. `https://dist-systems.bbn.com/projects/BBAC/`, 2013.