Sécurité des Systèmes et Réseaux Travail Personnel de l'étudiant

2016/2017

Topic: Machine Learning Methods for Computer Security

KOUDANBE AMADOU Calvin

and

KOUYIM MELI Armandine Sorel

I. Introduction

1. Context

The rapid development of security exploits in recent years has fuelled a strong interest in data analysis tools for computer security. On the one hand, the sheer number of novel malicious software observed by security researchers transcends the limits of manual analysis. According to AVTEST, 1 more than 200,000 examples of new malware are sighted daily. It is also discover that conventional method for attack detection produce some false positive. All these problems have led researchers to think of a dynamic solution against attacks, the solutions have been proposed by fleshing the association of machine learning with security; It is for this purpose that this work has been drafted

2. Background

2.1 Definition

Machine learning: refers to the development, analysis and to the implementation of methods that allow a machine to evolve through a learning process, and thus fulfill tasks is difficult or impossible to fulfill by algorithmic means more Classics. Machine learning explores the study and construction of algorithms that can learn from and make predictions on data.

2.2 principles of machine learning

The principle of machine learning involves many steps:

- Understand (the nature of data)
- Learn from past data
- Predict into the future
- Adapt – as data changes, different domains, etc.

2.3 application of machine learning for security

Many applications of machine learning is develop for security, we can have for instance: Plagiarism detection, Authorship identification, Copyright enforcement, Sentiment

analysis , Fighting Web spam, detection of network intruders or malicious insiders working towards a data breach

3. Problem and research questions

a- Problem

How to integrate machine learning to the exiting security architectures?

b- Questions

- What security problems can machine learning best help to solve? What scenarios are they ill-suited for?
- What are the theoretical limitations of worst-case attacks against learning algorithms under different constraints?
- What are existing and emerging non-security applications where learning techniques are used and can potentially be exposed to adversarial data? What experience from these applications can be used for development of general methodology of secure learning?
- Where do adversary attacks next?

II. Related works

work	Machine learning method	Security machine learning	Applications	Open issue	Specification of the work
Dorothy E. Denning. An intrusion-detection model. *IEEE Transactions on Software Engineering*, 13(2):222–232, 1987.	Detection of intrusion model	yes	Machine learning for computer security	yes	Integration of machine learning security

Stephanie Forrest, Steven A. Hofmeyr, Anil Somayaji, and Thomas A. Longstaff. A sense of self for Unix processes. In *IEEE Symposium on Security and Privacy*, pages 120–128, 1996.	anomaly-based approach	yes	machine learning techniques	yes	Integration of machine learning security
Marco Cova, Davide Balzarotti, Viktoria Felmetsger, and Giovanni Vigna. Swaddler: An approach for the anomaly-based detection of state violations in web applications. In *Recent Adances in Intrusion Detection (RAID)*, pages 63–86, 2007.	detect logical state violations in web applications	yes	Machine learning for computer security	Yes	Integration of machine learning security
Prahlad Fogla, Monirul Sharif, Roberto Perdisci, Oleg Kolesnikov, and Wenke Lee. Polymorphic Blending attacks. In *USENIX Security Symposium*, pages 241–256, 2006.	learning algorithms deployed in security applications	yes	learning algorithms	Yes	Secure learning
Michael. Kearns and Ming Li. Learning in the presence of malicious errors. *SIAM Journal On Computing*, 22(4):807–837, 1993.	which the error rate can be nearly as high as the fraction of data under the attacker's control	Yes	learning algorithms	Yes	Secure learning
Daniel Lowd and Christopher Meek. Adversarial learning. In *ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)*, pages 641–647, 2005.	near-optimal evasion for exploratory attacks against learners	yes	**Formalization of Secure Learning**	Yes	secure learning
Rainer Dahlhaus. Fitting time series models to nonstationary processes. *Annals of Statistics*, 25(1):486–503, 1997.	algorithms statistical inference for prediction and classification	yes	Secure Learning Approaches	yes	Machine Learning Methods for Computer Security

Kamalika Chaudhuri, Claire Monteleoni, and Anand D. Sarwate. Differentially private empirical risk minimization. *Journal of Machine Learning Research*, 12:1069–1109, 2011.	machine learning algorithms with a few exceptions including	Yes	Data Privacy	no	Machine Learning Methods for Computer Security
Steffen Bickel and Tobias Scheffer. Dirichlet-enhanced spam filtering based on biased samples. In *Neural Information Processing Systems (NIPS)*, pages 161–168, 2007.	adaptive spam filter	yes	State-of-the-art and emerging technologies	yes	Future Applications of Secure Learning
D. Sculley, Matthew Eric Otey, Michael Pohl, Bridget Spitznagel, John Hainsworth, and Yunkai Zhou. Detecting adversarial advertisements in the wild. In *ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)*, 2011.	online advertising system: Google's advertisement networks	yes	emerging technologies	yes	Future Applications of Secure Learning
Battista Biggio, Zahid Akhtar, Giorgio Fumera, Gian Luca Marcialis, and Fabio Roli. Security Evaluation of biometric authentication systems under real spoofing attacks. *IET Biometrics*, 1:11–24, 2012.	The risk of attacks against biometric recognition systems	Yes	Potential Attacks	yes	Future Applications of Secure Learning

III. Methodology employed

To aboard this survey the work were divided in three main topics: The role of learning in security applications, the paradigm of secure learning and feature applications on secure learning.

In the first part talk about the recent usage of learning approaches by the security practitioner's .the authors in prove the necessity to integrate machine learning in security architecture.

In the second topics is focused of current approaches and methodical challenges for learning in sensitive adversarial domains,

In the last topics here authors proposed learning algorithms with security guarantees.

IV. Results found and Perspectives

In this work, the result and perspectives is present in three main part according to the different topics treated.

In the first topics it is proved that the atomic security applications of machine learning is detection of malicious activities in operating system and network that some applications the learning-based systems is significantly outperform conventional approaches depending on expert knowledge. For instance in web application, the learning-based systems is very important because web application is so versatile and it is not easy to devise signature for specific attacks patterns. The learning-based security is an important solution for auto detection of malware on the system. Many security approaches are develop through machine learning for example: ASG (Automatic Signature Generation).the result of this topic is that machine learning is widely recently used in security architectures.at the end of this topics some open issues are proposed and future research directions for machine learning for security:

- Integration of machine learning with security mechanisms
- Reactive approaches
- Machine learning for offensive security

In the second topics which is the secure learning, authors affirmed that the traditional machine learning methods were not designed to operate in the presence of adversaries.in this case it is crucial to secure the learning process against attackers to which the objective is to produce a wrong result.in this topics many attacks against learning algorithms is mentioned for example: ***poisoning*** (erosion of a model of normality) and ***mimicry*** (insertion of a normal content into the target data). Another interesting example of an attack is the ***polymorphic blending*** technique, a transformation of packet payload to match a certain histogram of byte occurrences. At the end of this topics, some open issues is proposed:

- **Formalization of Secure Learning**
- **empirical techniques for performance evaluation of machine learning algorithms**

- **Development of Secure Learning Approaches**
- **Data sanitization:** it consist to identify and destroy malicious data
- **Secure Learning and Data Privacy**

The computer security is not only the domain in which we have attacks against machine learning. Recent attacks was recently found on intrusion detection systems and similar methods appeared for evasion of statistical spam filters. The realization of novel application in machine learning will conduct to novel attacks by attackers for monetary profit by abusing data-driven technologies.in the last topic which talk about future applications of machine learning, authors present the analysis of the main factors, which may make specific application domains attractive for novel attacks against learning methods and survey the situation in several domains, in which learning technologies play a crucial role.it is found after this survey that applications in which attacks are detected are : Plagiarism detection, Authorship identification, Copyright enforcement, Sentiment analysis ,Fighting Web spam and **Computer Vision Systems.in this topic ,** some methodical recommendations that may have repercussions in several potential application domains are given(poisoning, penetration testing, cases studies, privacy issues, non-stationary of the data, Lack of ground truth) .

At the end of this work we deduced that secure learning play a crucial role in a large number of data-driven applications.

V. Most important publications for this work

Due to the number of occurrence of the reference of some publication of the article, we have deduct that the most important publication use on this work are:

- Battista Biggio, Blaine Nelson, and Pavel Laskov. Poisoning attacks against Support Vector Machines. In *International Conference on Machine Learning (ICML)*, 2012.
- Prahlad Fogla, Monirul Sharif, Roberto Perdisci, Oleg Kolesnikov, and Wenke Lee. Polymorphic Blending attacks. In *USENIX Security Symposium*, pages 241–256, 2006.
- Marius Kloft and Pavel Laskov. Online anomaly detection under adversarial impact. In *International Conference on AI and Statistics (AISTATS)*, pages 405–412, 2010.

- Marius Kloft and Pavel Laskov. Security analysis of online centroid anomaly detection. *Journal of Machine Learning Research*, 13:3133–3176, 2012.
- Daniel Lowd and Christopher Meek. Adversarial learning. In *ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)*, pages 641–647, 2005.
- Roberto Perdisci, David Dagon, Wenke Lee, Prahlad Fogla, and Monirul Sharif. Misleading worm signature generators using deliberate noise injection. In *IEEE Symposium on Securityand Privacy*, pages 17–31, 2006.

REFERENCES

- Nils J. Nilsson Robotics. *INTRODUCTION TO MACHINE LEARNING AN EARLY DRAFT OF A PROPOSED TEXTBOOK*. Laboratory Department of Computer Science Stanford University Stanford, CA 94305 e-mail: nilsson@cs.stanford.edu November 3, 1998
- Vitaly Ford and Ambareen Siraj. *APPLICATIONS OF MACHINE LEARNING IN CYBER SECURITY*.Vitaly Ford and Ambareen Siraj Computer Science Department, Tennessee Tech University Cookeville, TN, 38505, USA vford42@students.tntech.edu, asiraj@tntech.edu
- https://www.quora.com/What-are-the-principles-of-machine-learning; visit the 16/03/2017