Machine Learning Methods for Computer Security

1. Introduction (2 pages)

1.1 Context

The machine learning and computer security make general context of this article which focuses on three main points to know: machine learning for computer security, secure learning, and future applications of secure learning.

1.2 Background

Machine learning is the subfield of computer science that gives computers the ability to learn without being explicitly programmed.

Computer security, also known as **cybersecurity** or **IT security**, is the protection of computer systems from the theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services they provide.

Adversarial machine learning is a research field that lies at the intersection of machine learning and computer security. It aims to enable the safe adoption of machine learning techniques in adversarial settings like spam filtering, malware detection and biometric recognition.

This document summarizes the presentations and working groups held at the 2012 “Machine Learning Methods for Computer Security” Dagstuhl Perspectives Workshop. Sections 3, 4 and 5 summarize the invited presentations held by the workshop’s participants. Section 6 then provides a short summary of the topics discussed by each of the workshop’s

1.3 Problem and research questions

- Machine learning for security: What security problems can machine learning best help to solve? What scenarios are they ill-suited for?
- Secure machine learning: What are the theoretical limitations of worst-case attacks against learning algorithms under different constraints? How can these constraints be used in practice for protecting learning methods against adversarial data?
- Secure learning beyond security: 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?

2. Related works (Only a comparative table!) (2 pages)

Year	Topic and authors	Overview of AML	Computer Security	Req	Secure learning	Approche	Solution
2012	I. Corona, R. Tronci, G. Giacinto, A Pattern Recognition System to the Protection of Web Services	O	O	X	X	O	X
2012	R. Perdisci, I. Corona, G. Giacinto, Early Detection of Malicious Flux Networks via Large Scale Passive DNS Traffic Analysis, IEEE Trans. on Dependable and Secure Computing, 9(5) pp. 714–726	O	X	X	X	O	X
2011	D. Ariu, R. Tronci, G. Giacinto, HMMPayl: an Intrusion Detection System based on Hidden Markov Models, Computers & Security, 30, pp. 221–241	O	O	X	X	O	X
2009	I. Corona, G. Giacinto, C. Mazzariello, F. Roli, C. Sansone, Information fusion for computer security: State of the art and open issues, Information Fusion, 10, pp. 274–284	O	X	X	X	X	X
2008	G. Giacinto, R. Perdisci, M. Del Rio, F. Roli, Intrusion detection in computer networks by a modular ensemble of one-class classifiers, Information Fusion, (1), pp. 69–82	O	X	X	X	X	X
2003	G. Giacinto, F. Roli and L. Didaci, Fusion of multiple classifiers for intrusion detection in computer networks, Pattern Recognition Letters, 24(12), pp. 1795–1803	O	X	X	X	X	X
2012	Michael Brückner, Christian Kanzow, and Tobias Scheffer. Static Prediction Games for Adversarial Learning Problems.13:2617–2654	O	O	X	X	O	X
2011	Michael Brückner and Tobias Scheffer. Stackelberg games for adversarial prediction problems.	O	O	X	X	O	X
2010	Marco Barreno, Blaine Nelson, Anthony D. Joseph, and J. D. Tygar. The Security of	X	X	X	X	O	X

	Machine Learning. Machine Learning, 81(2):121–148						
2009	Pavel Laskov and Marius Kloft. A Framework for Quantitative Security Analysis of Machine Learning, pages 1–4.	X	X	X	X	O	X
1986	Frank R. Hampel, Elvezio M. Ronchetti, Peter J. Rousseeuw, and Werner A.Stahel. Robust Statistics: The Approach Based on Influence Functions. John Wiley and Sons, New York, NY, USA.	X	X	X	X	O	X
1981	Peter Huber. Robust Statistics. John Wiley & Sons, New York, NY, USA	X	X	X	X	O	X
2006	Nicolò Cesa-Bianchi and Gábor Lugosi. Prediction, Learning, and Games. Cambridge University Press	O	X	X	X	O	X
2012	Daisuke Mashima and Alvaro A. Cardenas. Evaluating Electricity Theft Detectors in Smart Grid Networks. pp 210-229.	X	X	O	X	X	O
2011	Alvaro A. Cardenas and Saurabh Amin and Zong-Syun Lin and Yu-Lun Huang and Chi-Yen Huang and Shankar Sastry. Attacks against process control systems: risk assessment, detection, and response. pp 355-366.	X	X	O	X	X	O
2011	D. Sculley, Matthew Eric Otey, Michael Pohl, Bridget Spitznagel, John Hainsworth, and Yunkai Zhou. Detecting Adversarial Advertisements in the Wild.	X	X	O	X	X	O

3. Methodology employed (1,5 page)

Machine Learning for Computer Security

State-of-the-art

Open Issues and Research Directions

Future Applications

Secure Learning: Theory and Methods
- State-of-the-art
- Open Issues and Research Directions
- Secure Learning and Data Privacy

Future Applications of Secure Learning
- State-of-the-art and emerging technologies: Where do adversaries attack next?
- Recommendations and Research Priorities

4. Results found and Perspectives (2 pages)

4.1 Results found

Identification of open issues and research priorities including the need for transparency, interpretability and trust for secure learning approaches, the need for preventive measures and the potential for using learning in penetration testing, and the need for scalable procedures.
Identification of future applications for secure learning including detecting advanced persistent threats, dynamic authentication, autonomous monitoring, and crime prediction.

identification of set of key open questions including what should be achieved by secure learning, how can we know the adversary, and what is the appropriate role of secure learning within a secure system?

compiled list of major research priorities including the need to address poisoning attacks and the need for benchmarks and penetration testing. highlight privacy, non-stationarity of data, and the lack of ground truth as the major hindrances to the production of adequate benchmark datasets for secure learning.

4.2 Perspectives

a- The need for learning approaches to provide a greater degree of trust for seamless integration of these approaches in security applications
b- Design problems for incorporating secure learning technologies into security applications
c- The need for a more methodical approach to secure learning
d- Construction of benchmarks and case studies for secure learning

5. Most important publications for this work. (0,5 page)

N°	Parts	Main Refrences
1	Overview and Adversarial Machine Learning	L. Huang, A.D. Joseph, B. Nelson, B.I.P. Rubinstein, J.D. Tygar, “Adversarial machine learning,” in Proc. of the 4th ACM Workshop on Security and Artificial Intelligence (AISec’11), pp. 43–58, ACM.
2	Adversarial Learning and Game-theoretic Approaches	_____ -M. Brückner, C. Kanzow, T. Scheffer, “Static Prediction Games for Adversarial Learning Problems,” in Journal of Machine Learning Research 13:2617-2654, 2012. -C. Dimitrakakis, “Sparse Reward Processes,” arXiv:1201.2555v2 [cs.LG] , 2012. -Dimitrakakis, A. Mitrokotsa, “Near-Optimal Node Blacklisting in Adversarial Networks,” arXiv:1208.5641 [cs.CR], 2012. -B. Nelson, B. Biggio, P. Laskov., “Understanding the Risk Factors of Learning in Adversarial Environments,” in Proc. of the 4th ACM Wworkshop on Security and Artificial Intelligence (AISec’11). pp. 87-92, ACM. - B.I.P. Rubinstein, P.L. Bartlett, L. Huang, N. Taft, “Learning in a Large Function Space: Privacy-Preserving Mechanisms for SVM Learning,” in Special Issue on Statistical and Learning-Theoretic Challenges in Data Privacy, Journal of Privacy and Confidentiality, 4(1), pp. 65–100, 2012.
3	_____ _____ Secure Learning Applications, Evaluation, and Practices	-D. Sculley, M.E. Otey, M. Pohl, B. Spitznagel, J. Hainsworth, Y. Zhou, “Detecting Adversarial Advertisements in the Wild,” in Proc. of the Int’l Conf. on Data Mining and Knowledge Discovery (KDD’11). -S. Afroz, M. Brennan, R. Greenstadt, “Detecting Hoaxes, Frauds, and Deception in Writing Style Online,” IEEE Security and Privacy, 2012 -Fabian Yamaguchi, Markus Lottmann, and Konrad Rieck. Generalized Vulnerability Extrapolation using Abstract Syntax Trees. Annual Computer Security Applications Conference (ACSAC), December 2012 -V. Zwanger, F.C. Freiling, “Kernel Mode API Spectroscopy for Incident Response and Digital Forensics,” PPREV 2013 (ACM SIGPLAN Program Protection and Reverse Engineering Workshop), Rome.

LIENS

https://en.wikipedia.org/wiki/Adversarial_machine_learning 13/03/17
https://en.wikipedia.org/wiki/Computer_security 13/03/17
https://en.wikipedia.org/wiki/Machine_learning 13/03/17