2-years Postdoc
Data Augmentation for Reliable training of ML-based Intrusion Detectors

- Advisors : Dr. Jérôme François, Inria (jerome.francois@inria.fr), Prof Isabelle Chrisment (isabelle.chrisment@inria.fr)

- Keywords: machine learning, data augmentation, GAN, intrusion detection, anomaly detection

Context

Cybersecurity is a major concern everywhere with the growth of connected devices that are beyond common computers. To circumvent these problems, decades of research and development have led to build new techniques and tools to fight back against the attacks on the Internet. Nonetheless, the number of attacks and their magnitude still grow. The attack surface continues to increase along with the number of connected devices but also due to the number of applications, services or software that today make the IT ecosystem far from its origin.

Techniques used by both attackers and defenders evolve to complex mechanisms. For example, this leads to the massive use of encryption to avoid data leaks but simultaneously attackers benefit from encryption to hide their own activities. Multiple steps attacks also requires to analyze numerous sources of data. As a result, intrusion detection methods relying on artificial intelligence have been investigated both in research and in industry.

While these techniques hold promise for detecting and mitigating cyber threats, their effectiveness is highly dependent on the quality of the learning phase. Despite significant progress, experiments and reports suggest that these tools still struggle to generalize effectively to new and previously unseen data, particularly when faced with minor variations compared to training data.

Actually, the learning suffers from the lack of enough labeled data to represent the different and possibly infinite variation of attacks. To avoid this problem, different approaches exist. Among them, data augmentation consists into extending artificially the set of input data for learning in a realistic way.

Objectives

The aim of the postdoc is to assess the effectiveness of data augmentation techniques in enhancing the robustness of attack detection mechanisms based on machine learning classifiers. Concretely, it consists in extending datasets of network traffic containing attacks and evaluate the accuracy of the ML classifier with the newly generated data (with or without retraining).

The main challenge is to identify an appropriate data augmentation technique that is relevant to our context. Although Generative Adversarial Networks (GANs) [1] have been widely used to produce models by automating the generation of data, they are susceptible to result in artificially generated data with limited variation and reduced value. Therefore, different improvements have been proposed [2, 3]. In our context, applying a common GAN architecture has been proved to be

inefficient and authors in [4] propose to decompose input data into multiple groups before applying a GAN, in order to augment data for each individual type of attacks.

In addition to GANs, alternative approaches such as using a well-selected sequence of data transformations, also known as a data augmentation policy, have been explored [5].

The baseline technique promoted in [4] will be used as a reference, and the relevant possible data transformations of network traffic traces and strategies will be defined to compare this technique with a transformation-based augmentation technique. The postdoctoral researcher would have to identify relevant transformation for network traces considering the different layers including application payload. A formal definition of these transformations will be leveraged to define an augmentation policy engine. To determine the most appropriate data augmentation policy, an iterative strategy based on reinforcement learning will be proposed.

In addition, the postdoc will have the opportunity to experiment with other approaches, such as using adversarial autoencoders or Kronecker Graphs.

Références

[1] Ian J. Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville et Yoshua Bengio enerative Adversarial Networks Advances in Neural Information Processing Systems 27, 2014
[2] Yan Zuo, Gil Avraham, Tom Drummond : Generative Adversarial Forests for Better Conditioned Adversarial Learning. CoRR abs/1805.05185 (2018)
[3] S. K. Lim, Y. Loo, N. Tran, N. Cheung, G. Roig and Y. Elovici DOPING : Generative Data Augmentation for Unsupervised Anomaly Detection with GAN 2018 IEEE International Conference on Data Mining (ICDM)
[4] M. Al Olaimat, D. Lee, Y. Kim, J. Kim and J. Kim A Learning-based Data Augmentation for Network Anomaly Detection 2020 29th International Conference on Computer Communications and Networks (ICCCN)
[5] E. D. Cubuk, B. Zoph, J. Shlens and Q. V. Le andaugment : Practical automated data augmentation with a reduced search space 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)

Research environment

The offered position is proposed by the RESIST team of the Inria Nancy Grand Est research lab, the French national public institute dedicated to research in digital Science and technology. The team is one of the European research group in network management and is particularly focused on empowering scalability and security of networked systems through a strong coupling between monitoring, analytics and network orchestration. https://team.inria.fr/resist/

This work is in the context of the SuperviZ project. The SuperviZ project is part of the "system security" axis of the PEPR cybersecurity program. It addresses the field of "system, software and network security". More precisely, it targets the detection, response and remediation to computer attacks, subjects grouped under the name of "security supervision".

Application

Applications are to be sent as soon as possible. Tentative starting date: October 2023

Upload your file on jobs.inria.fr in a single pdf or zip file, and send it as well by email to jerome.francois@inria.fr and isabelle.chrisment@inria.fr. Your file should contain the following documents:

• Your CV.
• A cover/motivation letter describing your interest

In addition, one recommendation letter from the person who supervises(d) your work should be sent directly by his/her author to jerome.francois@inria.fr and isabelle.chrisment@inria.fr.

Required qualifications

- Required qualification: PhD in Computer Science
- Required knowledge: networking, network security, machine learning including practical experiences with large datasets
- Languages: Shell, python, ML libraries and others are appreciated
- Fluent in english (writing and oral communication)