2017 BALPYO FIGHTING PROJECT

7월 5주차 논문 리뷰 미팅

ICT 융합학부
2020055414 지훈

선정 논문

Modeling Realistic Adversarial Attacks against Network Intrusion Detection Systems

네트워크 침입 감지 시스템에 대응하는 현실적인 적대적 공격 모델링

Pubilished on
Cornell University & Association for Computin Machinery(ACM)

Contents

Abstract

1. Current Network Intrusion Detection Systems base on Machine Learning(ML-NIDS) are highly vulnerable to adversarial attacks that create tiny perturbations aimed at decreasing the effectiveness of detecting threats

2. Existing literature didn't assume realistic models, such as attackers having complete knowledge or being able to communicate freely with the target system.

3. In this paper, we discover and model the actual capabilities and environments that an attacker need to launch a real attack.

4. This paper can help researchers by strengthening their defensive systems by helping cyberdefenders address the most vulnerable and realistic problems and by devising new types of adversarial attacks based on realistic threat models.

Introduction

1. The technologies that carry Machine Learning methods are increasingly increasing, and today they are a major target for malicious attacks.

2. Research on ML-NIDS is still very insufficient compared to other fields.

3. Furthermore, papers on this field are doing research that is out of reality, making attackers in perpect condition.

4. In this paper, they model the five essential elements needed for attacks on ML-NIDS through the concept of ‘power’, suggesting realistic environments of attackers, and evaluating ML-NIDS attacks that have been presented.

5. Recently there has been a move to adopt some realistic scenarios.

6. Strengthen defense systems by formalizing ML-NIDS attacks and studying only the attacks that can occur among all attacks.

Motivation

1. Machine learning is increasingly being mounted on a variety of technologies, and malicious attacks are also increasing.

2. Not only are studies in this field vulnerable, but studies conducted are not based on realistic conditions.

3. Therefore, they explain realistic capabilities and environments through the concept of power, and based on this, propose realistic environments and evaluating the existing ML-NIDS attacks.