Contribution ID: **24** Type: **Lightning Talks (5 minutes)**

Exploring machine learning for DDoS mitigation

Wednesday, 10 April 2024 15:35 (5 minutes)

The frequency and diversity of DDoS attacks continue to increase annually. With the rise in computational capabilities, motivated attackers orchestrate large-scale attacks of higher complexity. Contemporary attacks exhibit adaptive behaviour, rendering effective mitigation challenging for conventional DDoS protection systems. The analysis of attacks must be precise - to avoid blocking legitimate traffic by mistake, fast - to react to the changing vector of the attack and minimalistic - to avoid overwhelming the mitigation components with a multitude of blocking rules. To meet these demands, we at CESNET have integrated a state-of-the-art machine learning algorithm based on autoencoders into our DDoS mitigation solution - the DDoS Protector. This innovative method enables swift identification and instant blocking of DDoS attacks while minimising the impact on legitimate traffic compared to traditional mitigation methods.

Our presentation aligns seamlessly with the theme of the GÉANT Security Days 2024 event as it addresses the pressing issue of DDoS attacks, which pose a significant threat to the availability of online services. Our autoencoder-based machine learning method is a powerful tool for detecting DDoS attacks that traditional methods cannot or that require significant effort from a trained analyst to block. This talk offers security management professionals, CSIRT members, and security strategists a preview of the potential behaviour of future DDoS mitigation systems, encouraging valuable discussions on management of these systems and the unique challenges posed by machine learning. Additionally, developers of security services can find inspiration for enhancing their systems based on the insights shared in our presentation. We believe our talk will contribute meaningfully to the discourse at GÉANT Security Days 2024, offering valuable perspectives on addressing and mitigating DDoS threats in the evolving landscape of cybersecurity.

Our aim is for the audience to recognize the significance of employing machine learning methods for DDoS attack detection while also understanding the associated risks. It's crucial to acknowledge that traditional DDoS protection methods are no longer fully effective against modern attacks, highlighting the potential necessity of incorporating machine learning in the future. Additionally, we will delve into key configuration principles and effective ways of presenting machine learning methods to users. We appreciate your consideration of our lightning talk for the GÉANT Security Days 2024 conference and look forward to further discussions on advancing DDoS protection strategies.

Primary author: MAN, Jakub

Presenter: MAN, Jakub

Session Classification: Lightning Talks

Track Classification: Lightning Talks