ACM Journals

CALL FOR PAPERS

**ACM Digital Threats: Research and Practice**
*Special Issue on Offensive Machine Learning*

**Guest Editors:**

- **Giovanni Apruzzese**, University of Liechtenstein, Liechtenstein, giovanni.apruzzese@uni.li,
- **Hugo Gascon**, German Cybersecurity Organization (DCSO), Germany, hugo.gascon@dcso.de,
- **Mirco Marchetti**, University of Modena and Reggio Emilia, Italy, mirco.marchetti@unimore.it
- **Fabio Pierazzi**, King's College London, UK, fabio.pierazzi@kcl.ac.uk

Machine Learning (ML) has shown increasing adoption and successes in many domains such as image recognition, recommendation systems, and speech analysis. Intrigued by these promising results, security researchers and practitioners have been exploring how ML can be used to protect systems against digital threats, such as for malware analysis, intrusion detection, and vulnerability discovery. Literature on digital threats related to ML studies the characteristics of novel ML-enabled solutions, highlighting their advantages (e.g., effectiveness at solving a specific task, such as detecting malware) or their vulnerabilities (e.g., susceptibility to adversarial ML attacks, which involve techniques for thwarting a ML-system). In other words, while there has been considerable effort on evaluating the capabilities of ML to solve a problem, very little focus has been put on analyzing ML as a means to *cause* a problem. Limited exploration has been conducted on how ML can be exploited by attackers to perform their malicious deeds. In a world where adversaries continually improve their techniques and refine their offensive capabilities, it is important to consider that ML can be used *also* by attackers. Studying the effectiveness of Offensive Machine Learning is thus critical to ensure that modern and next generation environments are equipped to face the emerging threats allowed by malicious uses of ML. In this context, it is worth noticing that such ML-enabled Digital Threats can target not only defense systems based on machine learning techniques, but also more traditional defenses, as well as standard information systems and even human personnel.

The focus of this special issue is to analyze the Digital Threats resulting from an offensive use of Machine Learning, by exploring how ML could be used to creatively construct effective ML-enabled attacks against any target system (e.g., create fake news, induce misbehaviors in a cyber-physical system, compromise data integrity and service availability). Attackers may also use ML offensively to support phases of sophisticated attacks such as social engineering (e.g., by exploiting speech synthesis, or automatically creating fake websites) or for a smarter target selection. As a result, defenses against ML-enabled attacks may need new paradigms to be defined. For example, Offensive ML may be useful to pentest companies and construct more advanced tools to support hardening. Ultimately, this special issue aims to answer the following questions: "how can ML be used as a means to attack?" and "how can we defend against these emerging digital threats?"

We are interested in both research and practice of Digital Threats of Offensive Machine Learning. More research-oriented contributions may explore novel attacks or defenses, whereas more practical contributions may review the threat landscape or develop tools/datasets to support research in this space.

**Topics**
Topics Include, but are not limited to:

- Novel ML-enabled offensive methods that disrupt existing and future digital systems
- Automatic or semi-automatic ML-based attacks (such as GAN- or RL-based attacks)
- Novel defenses against ML-enabled attacks
- Review of state of the art and threat landscape

**Domains**

Domains of interest include, but are not limited to:

- ML-enabled attacks against existing and next-generation systems, for example:
  - Cyber physical systems
  - Industrial IoT systems
  - Automotive systems
  - Intrusion Detection Systems
  - Phishing Detectors
  - Malware Detectors / Antiviruses
  - Vulnerability discovery systems
  - E-Health systems
  - Recommender systems
  - Video Surveillance systems
  - 5G Telecommunication Systems
- Generation of malicious data through Machine Learning, for example:
  - Adversarial examples
  - Fake news
  - Deep fakes
  - Fake threat intelligence
  - Fake reviews of products/services
  - Fake patient data and simulation results
  - Creation of fake social data for fraud purposes
- Employment of ML to facilitate APTs:
  - Offensive ML to improve memory exploitation attacks
  - Social engineering with ML (e.g., bots to trick someone into a chat)
  - Improving target selection with ML
  - Optimizing malware for evasion with ML mechanisms
  - ML systems to predict gains for attacker
  - Mimicry attacks

**Expected Contributions and Submission Information**

We welcome the following types of research contributions:

- Research Manuscripts reporting novel methodologies and results (up to 25 pages). These also include Literature Surveys reporting concrete and practical information on the state of the art of Offensive Machine Learning (up to 25 pages).
- Field Notes (up to 10 pages) reporting analysis methodologies, detection methods, experience reports, or any other real-world case studies that complement academic research from a practitioners' perspective.

**Important Dates**

- Submissions deadline: **Friday July 30, 2021**
- First-round review decisions: **Monday November 1, 2021**
- Deadline for revision submissions: **Monday January 24, 2022**
- Notification of final decisions: **Tuesday March 1, 2022**
- Tentative publication: **Mid-2022**

**Submission Information**

More information about each category, as well as the DTRAP author guidelines, can be found here https://dl.acm.org/journal/dtrap/author-guidelines. Please submit your papers to https://mc.manuscriptcentral.com/dtrap and select the "*Special Issue on Offensive Machine Learning*"paper type.

For questions and further information, please contact **dtrap_offensiveML@acm.org.**