DYnamic and Novel Advances in Machine Learning and Intelligent Cyber Security (DYNAMICS) Workshop

2019 Call for Submissions

About the DYNAMICS Workshop

The 2019 DYnamic and Novel Advances in Machine Learning and Intelligent Cyber Security (DYNAMICS) Workshop will be held on Monday, December 9th and Tuesday, December 10th, 2019. The workshop will be co-located with the 2019 Annual Computer Security Applications Conference (ACSAC) at the Condado Plaza Hilton in San Juan, Puerto Rico, USA.

Machine learning has become critical to the evolution and sustainability of cyber security. While the theoretical objectives and principles behind cyber security are still valid, traditional technologies that require humans to read log files, triage alerts, and harden devices are neither sufficiently fast, nor scalable enough, to meet the demands of modern networks and attacks. While the volume of network data, and the number of networked devices, have grown by orders of magnitude, the rate at which humans can triage alerts has not.

The sophistication of threats has also increased substantially. Sophisticated zero-day attacks may go undetected for months at a time. Attacks can take place over extended periods of time, effectively outwaiting traditional intrusion detection technologies. Worse, new attack tools and strategies can now be developed using adversarial machine learning techniques, requiring rapid co-evolution of defenses that match the speed and sophistication of machine learning-based offensive techniques.

This two-day workshop is intended to focus on novel applied and theoretical work that combines machine learning techniques such as reinforcement learning, adversarial machine learning, and deep learning with significant problems in cybersecurity. We consider both offensive and defensive applications of machine learning to security, with narrow topics grouped into six major topic areas presented over two days.

Technical Paper Submissions

The DYNAMICS Workshop invites submissions of original, previously unpublished technical papers, posters, and panels on research in machine learning and cybersecurity. Papers should be between 5 and 12 pages, and should use the 2019 ACM Proceedings Template: https://www.acm.org/publications/proceedings-template, using the [sigconf, anonymous] options. Submissions will be evaluated using a standard peer review process. While authors may wish to align their submissions with one of the suggested topics below, submissions on other topics related to the workshop theme are welcome. Papers should be submitted through OpenConf, at https://www.acsac.org/2019/openconf-dynamics/.

DYNAMICS Forums

A DYNAMICS Forum is a 1-2 hour extended discussion on a specific topic of interest to the DYNAMICS machine learning and cyber security community. A forum may focus on a specific technical problem, a policy issue, a social concern, or another DYNAMICS-related topic that you believe should be explored in depth. The intent of the forum format is to bring together a community that will not only explore your topic deeply within the context of the DYNAMICS Workshop itself, but that will have the potential to persist and grow beyond the workshop, in order to develop collaborative solutions over the long term. A DYNAMICS Forum is led by one or more moderators, who facilitate a discussion with a fully engaged audience.

If you would like to submit a DYNAMICS Forum proposal, please send an abstract of no more than 2 pages to dynamics@acsac.org. Please be sure to include your proposed topic, moderators, a statement of why your idea is relevant and important to the DYNAMICS community, proposed length, and a high-level outline with your major discussion topics. Your submission will be evaluated for inclusion in the workshop based on its relevance to the workshop theme, the quality of the submission, and the availability of space in the workshop schedule. While proposed topics may be aligned with one of the suggested topics below, submissions on other topics related to the workshop theme are welcome.

Panels
Panel submissions are invited on topics of interest to the DYNAMICS machine learning and cyber security community. To submit a panel, please send an abstract of up to 1 page to dynamics@acsac.org. Please be sure to include your proposed topic, panelists, panel chair, affiliations, and position statements for each panelist. DYNAMICS panels follow the same format as those of the main ACSAC conference. Extensive information about ACSAC's panel requirements can be found at https://www.acsac.org/2019/cfp/panels/.

Posters
Poster submissions are invited on topics of interest to the DYNAMICS machine learning and cyber security community. Posters provide a way for workshop attendees to present early stage, ongoing research that is not yet ready for submission as a peer reviewed paper, Poster presenters also gain feedback from conference and workshop attendees, and spark discussion among conference and workshop participants. Poster dimensions can be up to 36×48 inches (91x122 cm). Poster abstracts are not peer reviewed. Accepted abstracts will be made available on the workshop website prior to the event, but they will not be included in the workshop proceedings. To submit a poster, submit an e-mail with a PDF of your draft poster to dynamics@acsac.org. For questions on posters, please contact dynamics@acsac.org.

Lightning Talks
A Lightning Talk is timed, 5-minute talk on a topic of interest to the DYNAMICS machine learning and cyber security community. While lightning talks may be given on works in progress, or other topics of relevance to the workshop, you can even use a lightning talk to ask a question, find a community of shared interest on a topic, engage people in an issue, ask a question, or solicit feedback! A good lightning talk is fast paced, engaging, and high energy, and can use any desired presentation format.

Note that although Lightning Talk abstracts are reviewed by the DYNAMICS Workshop committee for relevance, they are not peer reviewed, and will not appear in the workshop proceedings. To submit a Lightning Talk, please e-mail your proposed topic to dynamics@acsac.org

Publication
Papers that have been accepted by the DYNAMICS workshop will be published in the workshop proceedings.

Presentation Requirements
By submitting a paper, DYNAMICS Forum, poster, panel, or lightning talk to the DYNAMICS workshop, you agree that if your submission is accepted, one or more of the submission's authors will present the final version of the submission at the workshop.

Important Dates

Technical paper submission deadline:	**September 30th, 2019 (11:59 PM Eastern Time)**
Technical paper acceptance notification:	**October 15th, 2019**
Final technical paper PDF submission deadline:	**November 1st, 2019 (11:59 PM Eastern Time)**
DYNAMICS Forum submission deadline:	**October 1st, 2019 (11:59 PM Eastern Time)**
DYNAMICS Forum acceptance notification:	**Rolling acceptances through the deadline**
DYNAMICS Forum presentation materials due:	**November 1st, 2019 (11:59 PM Eastern Time)**
Panels, posters, and lightning talks	**Submissions accepted through November 1st, 2019**

Suggested Topics

Attacking and Defending Machine Learning-Based Systems, Models, and Data Sets

- Trojan attacks on machine learning models
- Attacking and defending ML supply chains
- Attacking and defending autonomous systems and sensors
- Trustworthy ML-based systems

Data Generation and Preparation:

- Data generation and labeling for machine learning-based security
- Feature extraction, weighting, and validation
- Data set validity
- Standardized data sets and data generation environments for scientific algorithm comparison

Feature Finding and Event Analysis:

- Detection of malicious code and events in large data sets
- Attack detection
- Insider threat detection
- Zero-day attack detection
- Large-scale network data analysis using machine learning
- Detection of threats with evolving behaviors or implementations

Adversarial Machine Learning for Cybersecurity:

- Training environments for adversarial machine learning-based security
- Training data poisoning: Adversarial ML attacks on training data
- Adversarial ML-derived strategies for attacking and defending networks
- Adversarial ML for deception
- Training humans and non-humans using adversarial ML

Machine Learning-Based Defense and Response:

- Automated responses to attacks
- Machine learning for autonomous and resilient cyber defense
- Machine learning-based cyber deception
- Automatic detection of zero-day attacks
- Machine learning-based vulnerability analysis
- Machine learning-driven access controls, security policies, etc.
- Counter-machine learning techniques, such as data poisoning and deception
- Real-time threat detection, decision making, and response
- Deep learning for automated recognition of novel threats or threat implementations

Machine Learning-Based Offensive Techniques

- Machine learning-driven cyber offense
- Adversarial machine learning for network attacks

Trustworthy Analytics

- Trust of data sources
- What makes an analytic trustworthy?
- Trust of analytic behavior
- Analytic validation
- Attacking analytics
- Manipulating analytic results with deception
- Trusted Execution Environment (TEE)-based analytics

How to Contact the Workshop Organizers

If you have questions related to the workshop, please e-mail them to dynamics@acsac.org.

2019 DYNAMICS Workshop Organizers

Workshop Chair:
Dr. Michael Clifford, Noblis

ACSAC Workshops Chair:
Dr. Harvey Rubinovitz, The MITRE Corporation

Workshop Committee:
Evita Bakopoulou, UC Irvine
Dr. Matt Bishop, UC Davis
Dr. Michael Collins, USC-ISI
Dr. Ebrima Ceesay, Noblis
Dr. Karl Levitt, UC Davis
Dr. Anthony Palladino, Boston Fusion
Dr. Nidhi Rastogi, Rensselaer Polytechnic Institute
Daniel Kats, Symantec