"Security is not my field, I'm a stats guy":

A Qualitative Root Cause Analysis of Barriers to Adversarial Machine Learning Defenses in Industry

Jaron Mink*, Harjot Kaur†, Juliane Schmüser§, Sascha Fahl§, Yasemin Acar‡
*University of Illinois at Urbana-Champaign, jaronmm2@illinois.edu; †Leibniz University Hannover, kaur@sec.uni-hannover.de
§CISPA Helmholtz Center for Information Security, {juliane.schmueser, sascha.fahl}@cispa.de; ‡George Washington University and Paderborn University, acar@gwu.edu

Motivation

Machine learning is used for various critical tasks in many modern organizations.

Adversarial machine learning attacks evolve and have appealing targets.

Research in attacks and defenses is abundant.

Implemented Defenses are insufficient, and threats widely misunderstood.

Research Questions

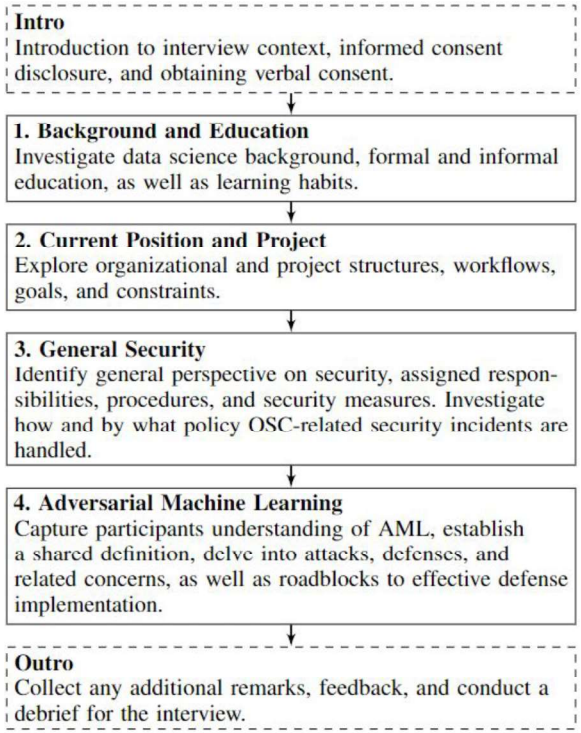
RQ1. What barriers prevent ML practitioners from adequately understanding AML attacks, and their corresponding risks and defenses?

RQ2. What barriers prevent ML practitioners from adequately assessing the risk AML poses to their systems?

RQ3. What barriers prevent ML practitioners from effectively implementing AML defenses in their systems?

Methodology

- Semi-structured online interviews
- One pilot interview
- Eligible participants for main study: ML practitioners with at least one year of industry experience
- 21 interviews conducted
- Analysis: descriptive and inductive coding with 3 coders



Selected Challenges

Exposure and Learning: *"So honestly, I consider computer science and cybersecurity completely separate fields."*

Risk Assessment: *"If the client is like saying that if he observe some errors, then we look into this and see what's going on."*

Defense Implementation: *"There's no person as such, responsible for the security."*

Recommendations

Establish a Security Culture in Machine Learning by introducing security advocates, and integrating security in machine learning processes.

Promote Practitioner AML Awareness by improving curriculums to cover adversarial machine learning, and expanding educational resources and their reach.

Provide Accessible Monitoring and Assessment Solutions by increasing toolset awareness, and with solutions that accommodate business constraints.

Published at Usenix 2023
https://www.usenix.org/conference/usenixsecurity23/presentation/mink