Endong Liu

+44 7470858976 | @ zzpolariszz.research@outlook.com | GitHub | Portfolio

Research Interests

Systems Security, AI for Security and Privacy, Safe and Trusty AI, Robustness and Resilience

Education

University College London — London, United Kingdom

M.Sc. in Information Security - ***GPA: 76.4/100*** — *Sep 2021 – Dec 2022*

Graduated with Distinction

Selected Modules:

- Computer Security I, Computer Security II, Introduction to Cryptography;
- Distributed Systems and Security, Privacy Enhancing Technologies, Cryptocurrencies;
- Research in Information Security, Information Security Management.

Lancaster University & Beijing Jiaotong University — Weihai, China

B.Sc. in Computer Science - ***GPA: 3.52/4.00*** — *Sep 2016 – Jun 2020*

Graduated with Upper Second Honours

Research Experience

Autonomous Network Defence using Reinforcement Learning — London, United Kingdom

Postgraduate Thesis — *May 2022 – Sep 2022*

- Supervisors: Dr. Vasilios Mavroudis, Dr. Chris Hicks, and Prof. Steven Murdoch
- The research aims to investigate the robustness of a hierarchical RL algorithm to defend against APT attackers.
- The hierarchical RL algorithm consists several subagents that use the Proximal Policy Optimisation algorithm and the Intrinsic Curiosity Module to overcome sparse rewards in the CAGE Challenge in the CyORG environment.
- The main contribution is extending three adversarial strategies to represent sophisticated capabilities of APT attacks and training defending agents to protect the target environment over varying lengths of time.
  - The first strategy is inspired by the ATT&CK Matrix after studying the lifecycle of APT attacks. This strategy helps adversaries hide their artifacts to evade the possible detection.
  - The second strategy tries to add more non-determinate elements by randomising the attacking path. This strategy misleads defencing agents but keeps the attacking process being inherently causally-linked.
  - The third strategy explores the potentiality that adversaries can use the RL algorithm to find a proper approach to execute attacks and recover from the defender's interrupts.
  - The hierarchy of the defending agent consists a controller and several subagents which can distinguish the adversarial strategies and choose the correct action to mitigate the APT attacks.
- The hierarchical RL algorithm overcomes the overfitting problem in defending against one particular adversarial strategy and provides a high and more generalised performance for autonomous network.
- As a contributor of the CAGE challenge repository by fixing issues that the *Restore* action cannot correctly remove malicious files on hosts and the *Impact* action cannot correctly give a -10 reward to defending agents.

A Survey on Privacy Protections in Secure DNS Alternatives — London, United Kingdom

Feb 2022 – Apr 2022

- The research builds a privacy threat model to the traditional DNS protocol.
- There are four DNS over Encryption and five Privacy Enhanced DNS are investigated in the research.
- This research evaluates capabilities of DNS alternatives for defending against passive and active adversaries.
- The results show that none of these alternatives can fully protect user privacy in the entire resolver procedure.
- This research discusses the trade-off between performance and privacy and the service centralization problem.

Enhancing Geographic Routing in Vehicular Delay Tolerant Network Weihai, China
Undergraduate Thesis *Oct 2019 – Apr 2020*

- Supervisor: Prof. Cao Yue
- The research aims to develop a routing algorithm that tries to mitigate the inaccuracy problem in previous research which prefers to use historically topological information when delivering messages in DTNs.
- The core algorithm is based on a geographical metric that predict the possible time consumption between current node and the destination, which involves real-time movement vectors, distances, and communication range.
- This algorithm imports energy levels to implement the energy perception function. It contains selfish and selfless policies that helps to extend system lifetime and keep the number of message copies in a good level.
- The message control mechanism includes two phases: (binary) spray and control. In the spray phase, the message carrier will send half of its message copies to the encountered nodes. When there is only one message copy left, it comes into the control phase and only select a better relay using the geographical metric and energy level. This design finds a trade-off between the network overhead ratio and delivery probability of each message.
- This algorithm is tested on the Opportunistic Network Environment (ONE) simulator and has better performance in delivery probability, overhead ratio, latency, and remained energy level than the DTN mainstream algorithms.
- This research is awarded as a school-level "Excellent Graduation Thesis".

Projects

Breaking XSS Mitigations via Script Gadgets London, United Kingdom
Paper Reproduce *Jan 2022 – Mar 2022*

- The project is to reproduce the vulnerability that enables the XSS mitigation bypassing technologies.
- This vulnerability reuses the existing code blocks (usually trusted) in some JavaScript-based web frameworks.
- This project bypasses three XSS mitigations: HTML Sanitisations, XSS Filter, and Content Security Policy.
- We provide a brief description of the threat model and mitigation goal for each XSS mitigation.
- We provide the involved gadgets and explain how these malicious payloads can bypass a specific XSS mitigation.
- We also implement code-reuse attacks using Flask (a Python-based web framework) and discuss possible defences.

Distributed Tickertape London, United Kingdom
Oct 2021 – Nov 2021

- The project is to build a distributed stock exchange in C that prints all trades in the same order on all servers.
- This project is based on a mini RPC library to build XDR marshaling and unmarshaling routines.
- Each server uses a Lamport's local logical clock, and the total order is synchronized by RPC communications.
- Each server waits for a while before printing a trade to guarantee the trade is broadcasted to all other servers.
- Each server maintains a message queue that contains the logical time, trade state, and real locally elapsed time.
- The logical time determines the print order and the elapsed time is used to tolerate delay and handle failures.

Programming Skills

- Python
- C, C++, Java, MySQL
- JavaScript, Solidity, Erlang
- LaTeX