

Zonghan Xu

zonghan37@hotmail.com | 519.721.1782

SKILLS

PROGRAMMING

C • C++ • C# • MATLAB
Python • Scheme

INFORMATION SECURITY

Security Compliance • Penetration Testing
Network Security • Tool Automation
Vulnerability Management

SECURITY SOFTWARE

Splunk • InsightVM • Netwitness
QualysGuard • Cisco NGFW

SYSTEMS

Linux • Windows

OTHER

Git • JIRA • LaTeX • Excel

EDUCATION

UNIVERSITY OF WATERLOO

BACHELOR OF MATHEMATICS

Major in
Computer Science &
Combinatorics and Optimization &
Computational Mathematics

COURSEWORK

GRADUATE

Communication Complexity
Computational Geometry
Randomized Algorithms

UNDERGRADUATE

Algorithm Design and Analysis
Applied Cryptography
Coding Theory
Computer Networks
Game Theory
Graph Theory
Operating Systems
Optimization

LINKS

Github:// [59412](#)
LinkedIn:// [Zonghan Xu](#)

EXPERIENCE

CITADEL SECURITIES | SECURITY ENGINEER

May 2019 - Aug 2019 | Chicago, Illinois, US

- Built a fully-automated network reconnaissance system that enumerates and evaluates the external-facing attack surface of the enterprise network, using mainly **Python** and **bash**
- Created automation using **Python/C#** for several critical security systems including SIEM and IDS
- Conducted security reviews for several open source software and vendor products
- Participated in suspicious log investigation and incident response using SIEM system

NCC GROUP | SECURITY RESEARCHER

Sept 2018 - Oct 2018 | Waterloo, Ontario, CA

- Performed **C** language SDK penetration test on Texas Instrument TI-3200 IoT Wi-Fi Launchpads
- Researched on the security of cryptographic and key management protocols

BANK OF MONTREAL | INFORMATION SECURITY ENGINEER

Jan 2018 - Apr 2018 | Scarborough, Ontario, CA

- Set up the authentication protocol for next-generation firewall system, while providing appropriate documentations
- Evaluated and modified vulnerability scan templates for 13 operating systems, 4 databases and 8 web servers including numerous versions of Windows, allowed vulnerability scan results to satisfy both national requirements and company demands
- Installed and tested network bypass switches on enterprise network, which enables Fail-Open state on security systems to keep them online during incidents

BANK OF MONTREAL | INFORMATION SECURITY ANALYST

Jan 2017 - Apr 2017 | Scarborough, Ontario, CA

- Operated Data Loss Prevention system to eliminate false positives and detect system failure, also created several automation scripts using **C#**
- Evaluated vulnerability scan templates for several operating systems, databases and web servers
- Participated in threat intelligence gathering process, provided several reports about new vulnerabilities to the InfoSec department

ACADEMIC RESEARCH

MULTI-PARTY COMMUNICATION COMPLEXITY

Graduate Seminar, University of Waterloo | 2019

- Attempted to prove the lower bounds of several well-known problems on the multi-party peer-to-peer setting
- Discussed how the lower bounds/reducibility of a two-party communication problem can be inherited by the multi-party variant

Zonghan Xu

zonghan37@hotmail.com | 519.721.1782

PROJECT

ECHO

iOS Social Software | 2020

- An in-development project for a social software that stores photo, video and music according to geological locations, and allows various sharing methods

FILE EXCHANGE PROGRAM

Coursework Project, University of Waterloo | 2017

- Network project in **Python** that allows clients to exchange files through uploading to and downloading from a server
- Developed for the University Networking course final project, received a final mark of 96

MONOPOLY

Coursework Project, University of Waterloo | 2016

- Monopoly Game written in **C++** for the University OOP course final project
- Developed by a team-of-3, received a final mark of 90

AWARDS

TERM DEAN'S HONOURS LIST Faculty of Math, University of Waterloo, Fall 2019 & Winter 2020