Detect vulnerabilities in programs
-----mainly in binaries

Xiaogang Zhu
Supervisors: Yang Xiang, Sheng Wen, Seyit Camtepe
Swinburne Uni & Data61
www.data61.csiro.au
• **Bug**: A bug causes a program into an unintended state.

• **Vulnerability**: When a bug can be exploited by an attacker, the bug becomes a vulnerability.

• A vulnerability can be utilized by attackers to get information or control devices from others’ devices.

• My work is to detect vulnerabilities and report to vendors so that they can fix them.
Works

• Techniques: fuzzing and/or machine learning
• Submitted paper: A Feature-Oriented Corpus for understanding, Evaluating and Improving Fuzz Testing. ASIACCS 2019
• Ongoing work: new fuzzing algorithm

Fuzzing:

- Inputs
- Program
- Crash? Or other states?
- Vulnerable

If similar: potential vulnerable

Machine learning:

- Undetected program
- Vulnerable programs
Detecting and Patching Vulnerabilities in Smart Contract

Bushra Sabir
Supervisors: Professor Ali Babar, Dr Raj Gaire
19/03/2019
www.data61.csiro.au
Problem

**Problem**
Third Party Based Contract

![Diagram of Third Party Based Contract]

**Why?**
- Problematic Language
- Poor written Contracts
- Traditional language Inherently dangerous methods

**Solution**
Automate Vulnerability Detection and Patching

**Motivation**
- Attacks (e.g., DOU, Parity Wallet Lockup)
- Time Consuming Manual Analysis (Prone to Errors)
Methodology

**Vulnerability Smart Contract (SC) Detection**
- Dataset of SCs
- Examples
- Vulnerable SC Detector
- Code Analysis

**SC Vulnerability Patching**
- Problematic Code Lines
- Repair Code Lines
- Learn Transformation
- Identify Repair
- Apply Patch

Repaired Code
Receipt-Free, Universally and Individually Verifiable Poll Attendance

Nicholas Akinyokun
The University of Melbourne; Data61 Docklands

Supervisors: A/Prof. Vanessa Teague and Prof. Josef Pieprzyk

21 March 2019

www.data61.csiro.au
Overview of Research

• There is an extensive cryptographic literature on the implementation of receipt-freeness in poll site voting protocols. However, while some protocols have considered participation privacy, which means that the protocol does not reveal whether a person voted, none has modelled the receipt-freeness of attendance at a polling place in a manner that prevents corrupt polling place officials from stuffing the ballots of the voters who did not attend.

• We examine the cryptographic techniques for protecting voters from coercion not to vote in poll site elections.

• The main contributions of this research are as follows:
  - We propose a secure method that will simultaneously allow for each registered voter to verify whether their attendance at the polling place is accurately recorded, without being able to prove to anyone else whether or not that they attended the polling place. This also allows registered voters who did not attend to verify that no vote was cast or recorded in their name.
  - In addition, we describe how to achieve a universally verifiable tally of the total number of eligible voters that attended each polling place in an electoral district.
List of Publications

Topology Discovery in Software Defined Networks

Robert McAuley

Communication Networks Research Group
Cyber Sensing and Shaping Branch
Cyber & Electronic Warfare Division
Progress

Many Controllers

Physical Testbed

Technique From Literature

Data From Our Network
Detecting Duplicate Devices

Naomi Chan \(^1,^2\) & Dean Philp \(^1\)

\(^1\) Communication Networks Research
\hspace{1cm} Cyber Sensing & Shaping
\hspace{1cm} DST Group

\(^2\) School of Computer Science
\hspace{1cm} University of Adelaide
Rule-based

Probabilistic

Machine Learning
Outcomes

- Advanced Topics in Computer Science (University of Adelaide 2018 S2)

- Publication:

- Next Generation Technologies Fund -- Cyber Theme on Situational Awareness
Predictive Security Analytics for Software Systems

Presented by: Triet Huynh Minh Le (triet.h.le@adelaide.edu.au)
Supervisor: Prof. M. Ali Babar – School of Computer Science (CREST)
Software Vulnerability Analytics

**SV TASKS**
- Prediction & Detection
- Assessment & Evaluation
- Exploratory analysis

**METHODS (My PhD)**
- Statistical models
- Machine Learning
- Deep Learning
- Tools
- APIs

**CHALLENGES**
- Heterogeneous & Imbalanced Data
- Data Changes (Concept Drift)
- No Context-aware Representation

University of Adelaide

Predictive Security Analytics for Software Systems
17
Accepted paper


Under-review paper


On-going work

• Partition-based Learning for Software Vulnerability Assessment using Topic Modeling

• Context-aware Representation of Software Vulnerabilities
Software Architecture Strategies for Big Data Cyber Security Analytics

Presenter: Faheem Ullah

Supervisor: Prof. Ali Babar

CREST – The Centre for Research on Engineering Software Technologies
The University of Adelaide, Australia
faheem.ullah@adelaide.edu.au
**Research Problem and Approach**

**Research Problem:** “How to enable a Big Data Cyber Security Analytics System to ensure optimal accuracy and response time in the face of changes in the operating environment”

**Approach**

1. **Architecture-driven Adaptation** based on monitoring output indicators such as accuracy and response time

2. **Architecture-driven Adaptation** based on monitoring the input indicators such as quality and quantity of security event data
List of Publications


An Empirical Study of The Success and Failure Factors in Developing Secure Mobile Health Applications

Bakheet Aljedaani | School of Computer Science

Supervisors: Professor Ali Babar and Dr Christoph Treude
The number of apps developers for mobile health apps has increased. The number of mHealth apps has also massively increased. Security is still missing and need to be addressed at early stage.

According to recent studies, 95% mHealth apps have at least some chance of potential damage for information security and privacy issues.

Our aim to investigate the factors the influence the development of secure mHealth apps. To the best of our knowledge, there is no clear effort that has aimed at analysing the challenges that prevent mHealth apps developers' to develop secure apps.

Research Outcomes

- Investigating the challenges, approaches and solutions for developing secure mHealth apps from mHealth apps developers point of view.
- Identifying the challenges, approaches and solutions for sharing the security knowledge during the development process of mHealth apps.
- Developing a theoretical framework of practices for developing secure mHealth apps.

Submitted work

- A review paper (Challenges in Developing Secure Mobile Health Applications A Review) has been submitted to SEKE 2019 and it is under review.)
Techniques for Cyber Vulnerability Exploit Prediction

Andrew Feutrill
with Professor Matthew Roughan, Professor Joshua Ross and Dr. Yuval Yarom

commercial-in-confidence
Project Overview

- Create stochastic model of the arrival of vulnerabilities
- Understand the stages of vulnerability lifecycle and produce mathematical models to estimate the probability and hitting times of reaching certain states
- Produce mathematical models of the progression of exploits through particular networks to provide risk scoring for networks
Project Outcomes

• Publication
  – The Effect of Common Vulnerability Scoring System Metrics on Vulnerability Exploit Delay, A Feutrill, D Ranathunga, Y Yarom and M Roughan, The Sixth International Symposium on Computing and Networking (CANDAR), Hida Takayama, Japan, November 27-30, 2018

• Developing long range dependent queueing model of the arrival process of vulnerabilities
• Developing Semi-Markov model to describe the probability and hitting times to reach certain states
• Developing epidemic models of the propagation of an exploit through computer networks
RATAFIA: Ransomware Analysis using Time And Frequency Informed Autoencoders

By Sarani Bhattacharya

Supervisor: Debdeep Mukhopadhyay
Institute: Indian Institute of Technology Kharagpur
Does Ransomware affect the Performance Counters??

We observed five performance counters (in sampling mode) which are likely to be affected by Ransomware (because of its repeated encryption of files).

YES!!
Ransomware do affect these events.
How good is reconstruction error as a decider??

Utilizing Repeated Encryption of Ransomwares

Branch Instructions
Branch Misses
Cache References
Cache Misses
Instructions
FFT of Branch Instructions
FFT of Branch Misses
FFT of Cache References
FFT of Cache Misses
FFT of Instructions