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

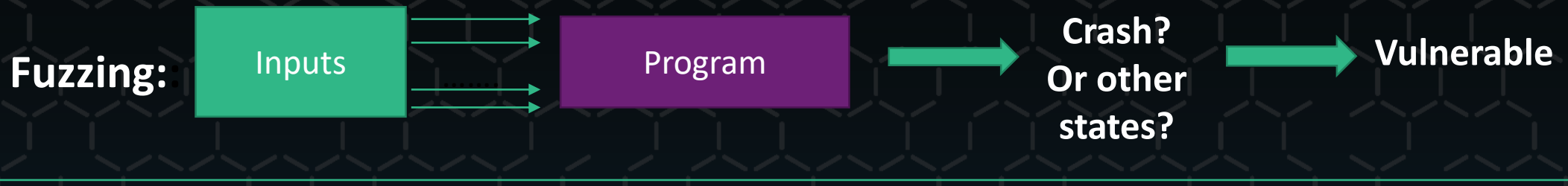
Xiaogang Zhu
Supervisors: Yang Xiang, Sheng Wen, Seyit Camtepe
Swinburne Uni & Data61
www.data61.csiro.au

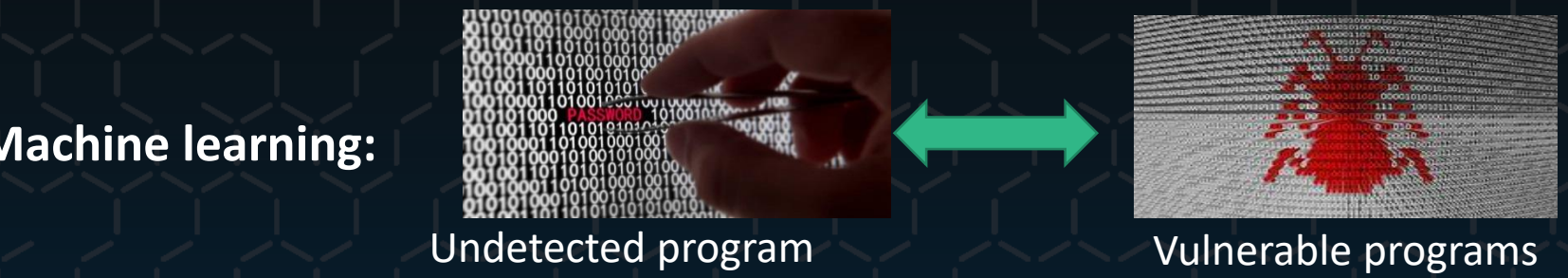
Overview

- 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'
- 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





If similar: potential vulnerable

THE UNIVERSITY of ADELAIDE

Detecting and Patching Vulnerabilities in Smart Contract

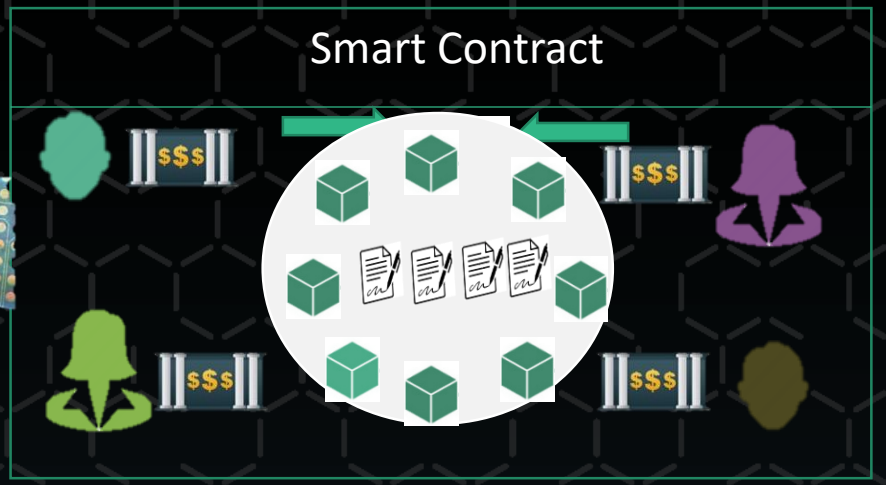
Bushra Sabir

Supervisors: Professor Ali Babar, Dr Raj Gaire

19/03/2019

www.data61.csiro.au

Problem



Problem

Why?

- Problematic Language
- Poor written Contracts
- Traditional language Inherently dangerous methods

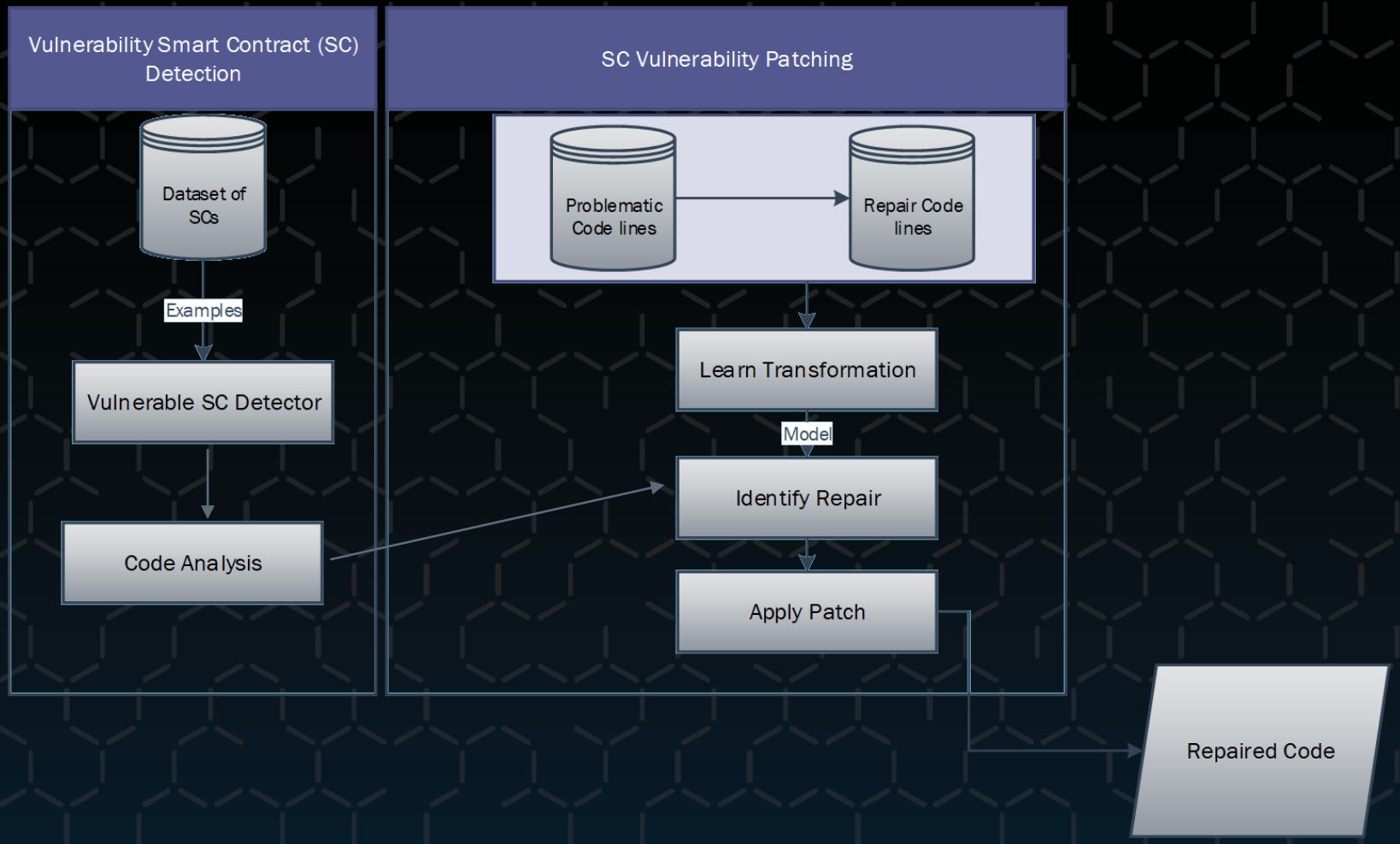
Solution

Automate Vulnerability Detection and Patching

Motivation

- Attacks(DOU, Parity Wallet Lockup
- Time Consuming Manual Analysis (Prone to Errors)

Methodology



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

- Nicholas Akinyokun and Vanessa Teague (2019). Receipt-Free, Universally and Individually Verifiable Poll Attendance. In *Proceedings of the 2019 Australasian Computer Science Week Multiconference* (ACSW '19), Sydney, Australia. January 29 – 31, 2019.

Australian Government
Department of Defence
Science and Technology

Topology Discovery in Software Defined Networks

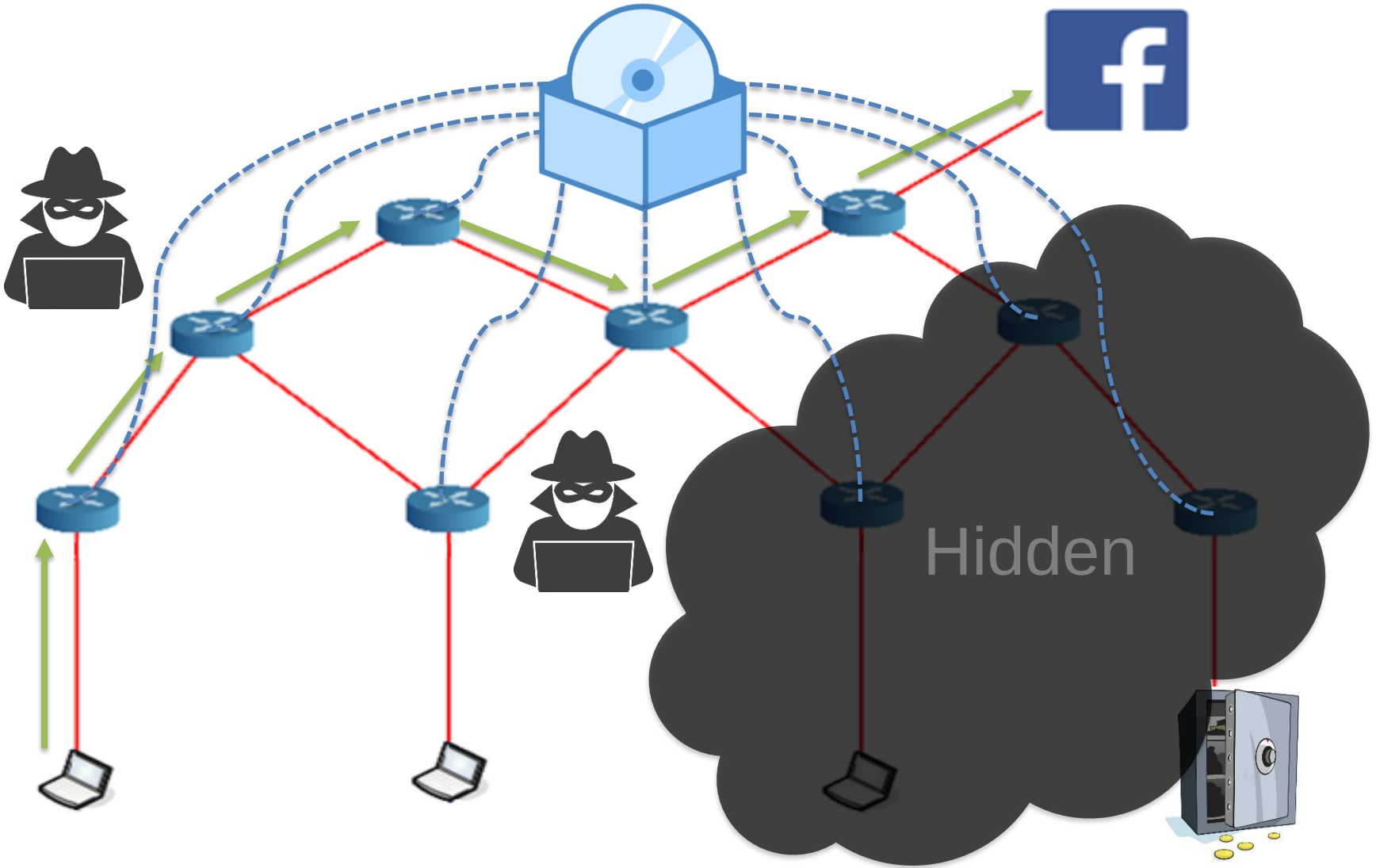
Robert McAuley

Communication Networks Research Group

Cyber Sensing and Shaping Branch

Cyber & Electronic Warfare Division

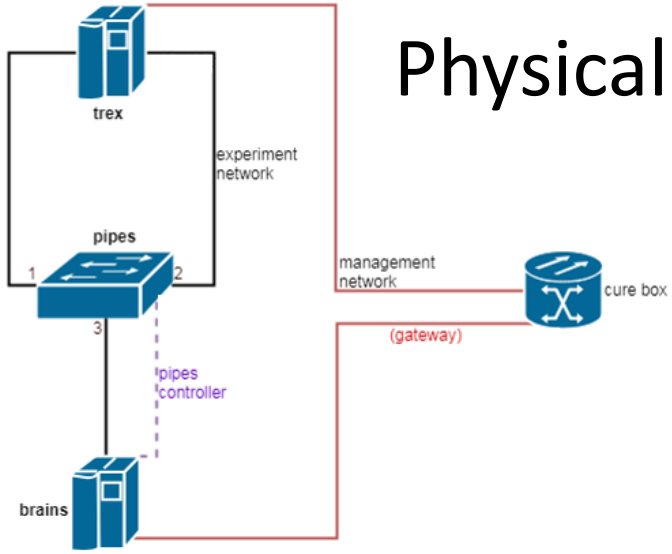
Computer Network



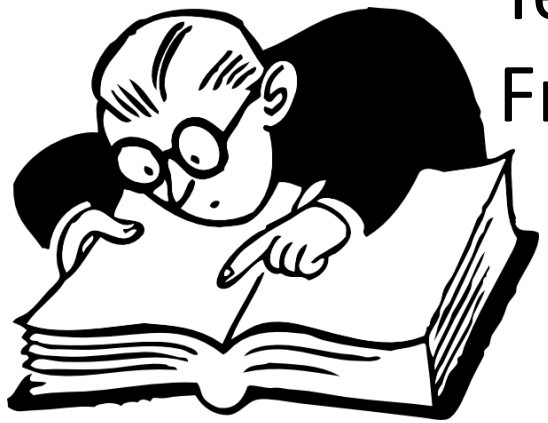
Progress

Many Controllers

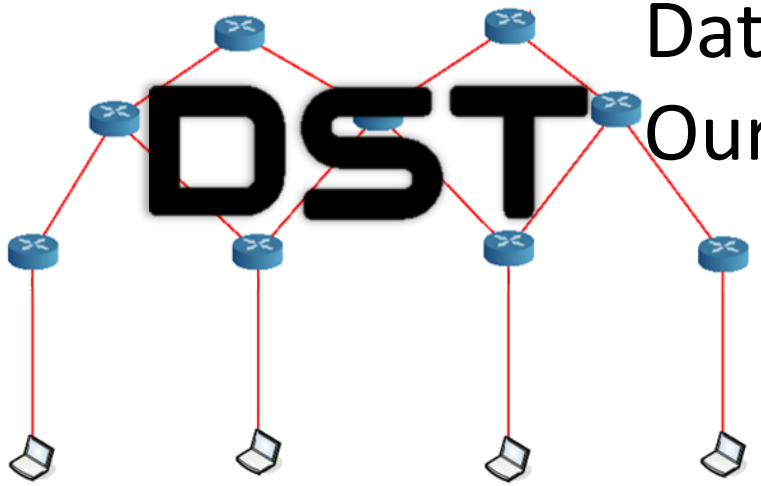
Physical Testbed



Technique From Literature



Data From Our Network



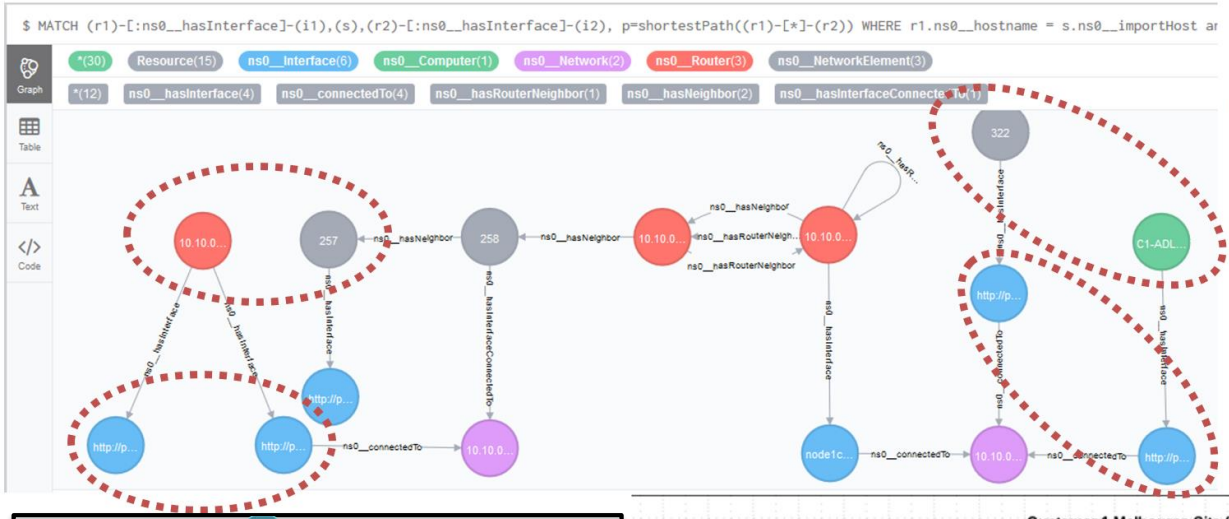
Australian Government
Department of Defence
Science and Technology

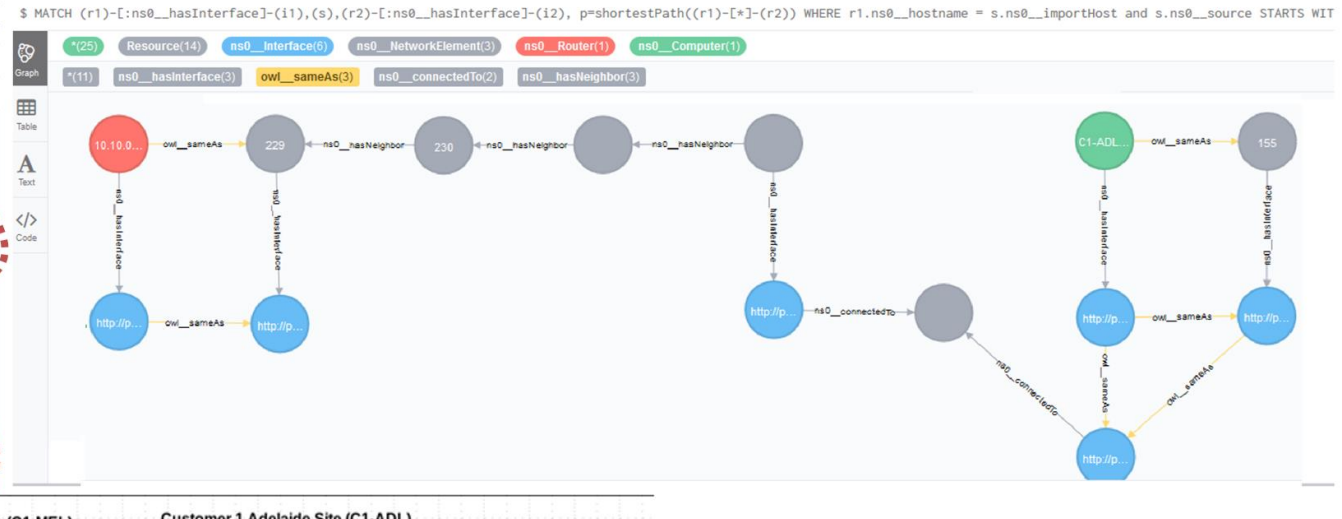
Detecting Duplicate Devices

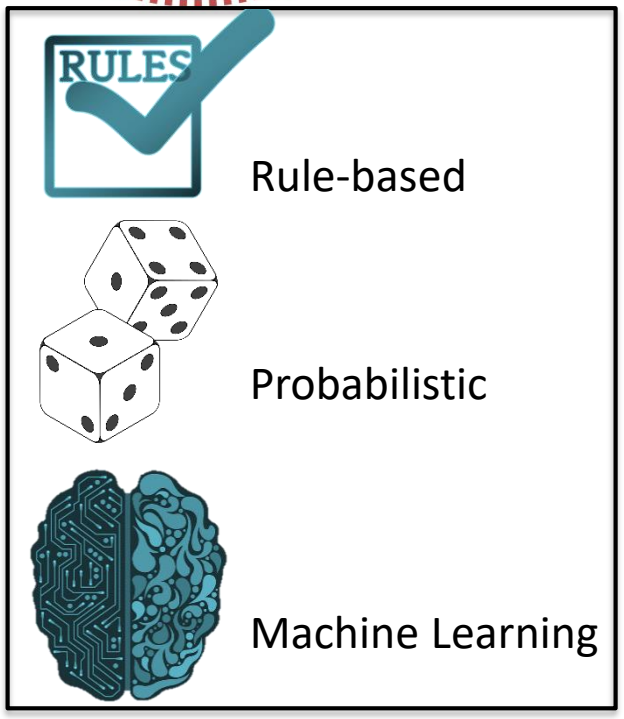
Naomi Chan [1,2] & Dean Philp [1]

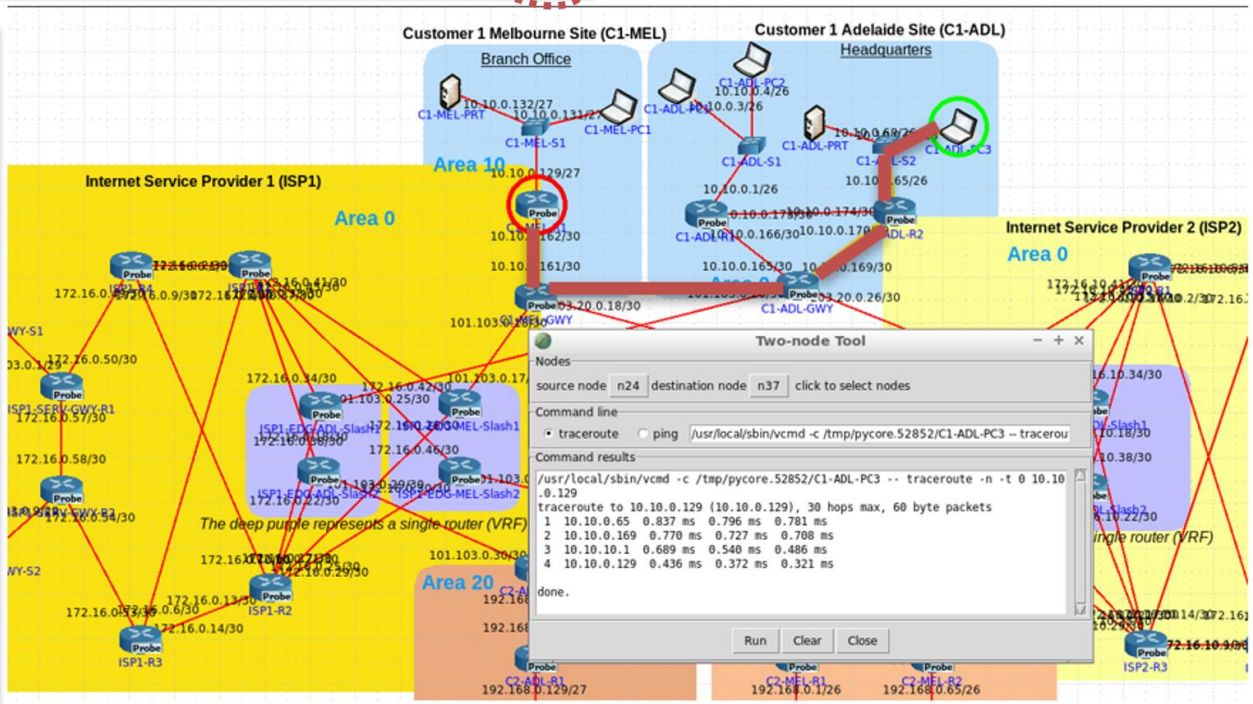
[1] Communication Networks Research
Cyber Sensing & Shaping
DST Group

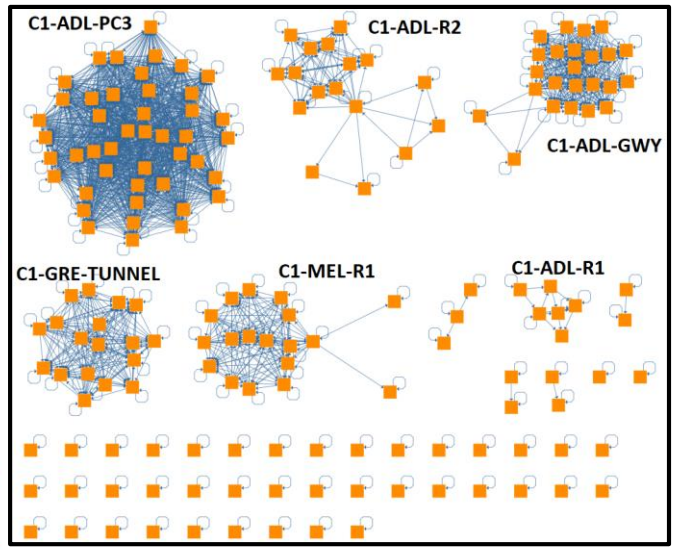
[2] School of Computer Science
University of Adelaide


$ MATCH (r1)-[:ns0__hasInterface]-(i1),(s),(r2)-[:ns0__hasInterface]-(i2), p=shortestPath((r1)-[*]-(r2)) WHERE r1.ns0__hostname = s.ns0__importHost ar
*(30)
Resource(15)
ns0__Interface(6)
ns0__Computer(1)
ns0__Network(2)
ns0__Router(3)
ns0__NetworkElement(3)
*(12)
ns0__hasInterface(4)
ns0__connectedTo(4)
ns0__hasRouterNeighbor(1)
ns0__hasNeighbor(2)
ns0__hasInterfaceConnectedTo(1)
Graph
Table
Text
Code
10.10.0...
257
258
322
C1-ADL...
http://p...
node1c...
ns0__hasNeighbor
ns0__hasInterface
ns0__hasInterfaceConnectedTo
ns0__hasRouterNeigh...
ns0__hasRouterNeighbor
ns0__connectedTo


$ MATCH (r1)-[:ns0__hasInterface]-(i1),(s),(r2)-[:ns0__hasInterface]-(i2), p=shortestPath((r1)-[*]-(r2)) WHERE r1.ns0__hostname = s.ns0__importHost and s.ns0__source STARTS WIT
*(25)
Resource(14)
ns0__Interface(6)
ns0__NetworkElement(3)
ns0__Router(1)
ns0__Computer(1)
*(11)
ns0__hasInterface(3)
owl__sameAs(3)
ns0__connectedTo(2)
ns0__hasNeighbor(3)
Graph
Table
Text
Code
10.10.0...
229
230
C1-ADL...
155
http://p...
owl__sameAs
ns0__hasInterface
ns0__hasNeighbor
ns0__connectedTo


RULES
Rule-based
Probabilistic
Machine Learning


Customer 1 Melbourne Site (C1-MEL)
Branch Office
Customer 1 Adelaide Site (C1-ADL)
Headquarters
Internet Service Provider 1 (ISP1)
Area 0
Area 10
Area 20
Internet Service Provider 2 (ISP2)
Area 0
C1-MEL-PRT
C1-MEL-PC1
C1-MEL-S1
C1-ADL-PC2
C1-ADL-PC3
C1-ADL-PRT
C1-ADL-S1
C1-ADL-S2
C1-ADL-R1
C1-ADL-R2
C1-ADL-GWY
ISP1-R2
ISP1-R3
ISP2-R3
Two-node Tool
Nodes
source node n24 destination node n37 click to select nodes
Command line
traceroute ping /usr/local/sbin/vcmd -c /tmp/pycore.52852/C1-ADL-PC3 -- tracerou
Command results
/usr/local/sbin/vcmd -c /tmp/pycore.52852/C1-ADL-PC3 -- traceroute -n -t 0 10.10.0.129
traceroute to 10.10.0.129 (10.10.0.129), 30 hops max, 60 byte packets
1 10.10.0.65 0.837 ms 0.796 ms 0.781 ms
2 10.10.0.169 0.770 ms 0.727 ms 0.708 ms
3 10.10.10.1 0.689 ms 0.540 ms 0.486 ms
4 10.10.0.129 0.436 ms 0.372 ms 0.321 ms
done.
Run
Clear
Close
The deep purple represents a single router (VRF)


C1-ADL-PC3
C1-ADL-R2
C1-ADL-GWY
C1-GRE-TUNNEL
C1-MEL-R1
C1-ADL-R1

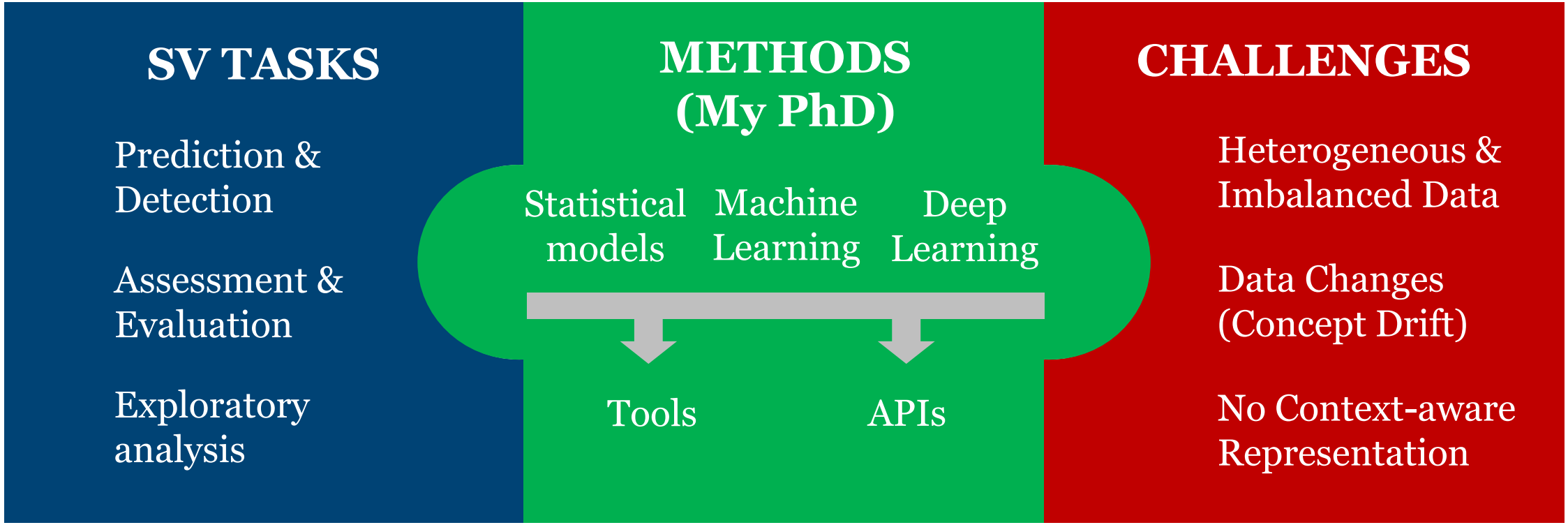
Outcomes

- Advanced Topics in Computer Science (University of Adelaide 2018 S2)
- Publication:
  - Dean Philp, Naomi Chan, Leslie Sikos, "Decision Support for Network Path Estimation via Automated Reasoning", Intelligent Decision Support in Cybersecurity, 11th International KES conference on Intelligent Decision Technologies, June 2019
- 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



OUTCOME (MORE at crest-centre.net)

Accepted paper

- **Triet H. M. Le**, Bushra Sabir, M. Ali Babar, "*Automated Software Vulnerability Assessment with Concept Drift*," the 16th International Conference on Mining Software Repositories (**Rank A**), Canada, 2019.

Under-review paper

- Hao Chen*, **Triet H. M. Le***, M. Ali Babar, "*Deep Learning for Source Code Modeling and Generation: Models, Applications and Challenges*," ACM Computing Surveys (**Rank A***), 2019. (*: Equal contribution)

On-going work

- **Partition-based** Learning for Software Vulnerability Assessment using Topic Modeling
- **Context-aware** Representation of Software Vulnerabilities

CREST
Centre for Research on Engineering Software Technologies

THE UNIVERSITY of ADELAIDE

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

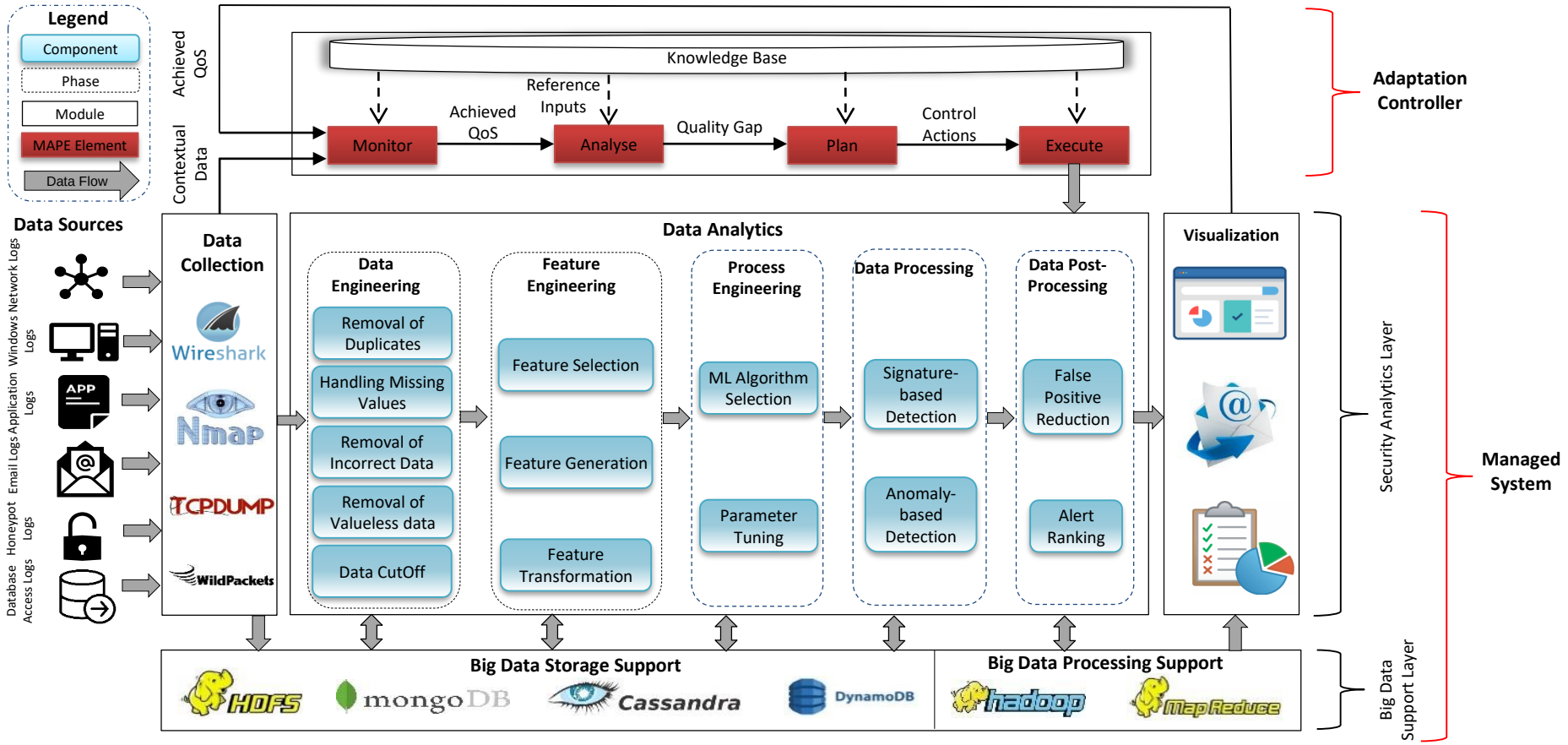
Research Problem and Approach

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

1. Faheem et al., ***Security Support in Continuous Deployment Pipeline***, International Conference on Evaluation of Novel Approaches in Software Engineering, 2017.

2. Faheem et al., ***Data Exfiltration: A Review of External Attack Vectors and Countermeasures***, Journal of Network and Computer Applications, 2018

3. Faheem Ullah and Ali Babar, ***Architectural Tactics for Big Data Cyber Security Analytics***, Journal of Systems and Software, 2019

4. Faheem Ullah and Ali Babar, ***An Architecture-driven Adaptation Approach for Big Data Cyber Security Analytics***, International Conference on Software Architecture, 2019

5. Faheem Ullah and Ali Babar, ***Quantifying the Impact of Design Strategies for Big Data Cyber Security Analytics Systems: An Empirical Investigation***, Submitted to International Computer Software and Applications Conference, 2019

6. Faheem Ullah and Ali Babar, ***A Heuristic-based Approach for the Tactics-driven Design of Big Data Cyber Security Analytics***, under work to be submitted to European Conference on Software Architecture, 2019.

THE UNIVERSITY of ADELAIDE

CRICOS PROVIDER 00123M

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

adelaide.edu.au

seekLIGHT

Research overview

The number of apps developers for mobile health apps has increased

Leading to

The number of mHealth apps has also massively increased

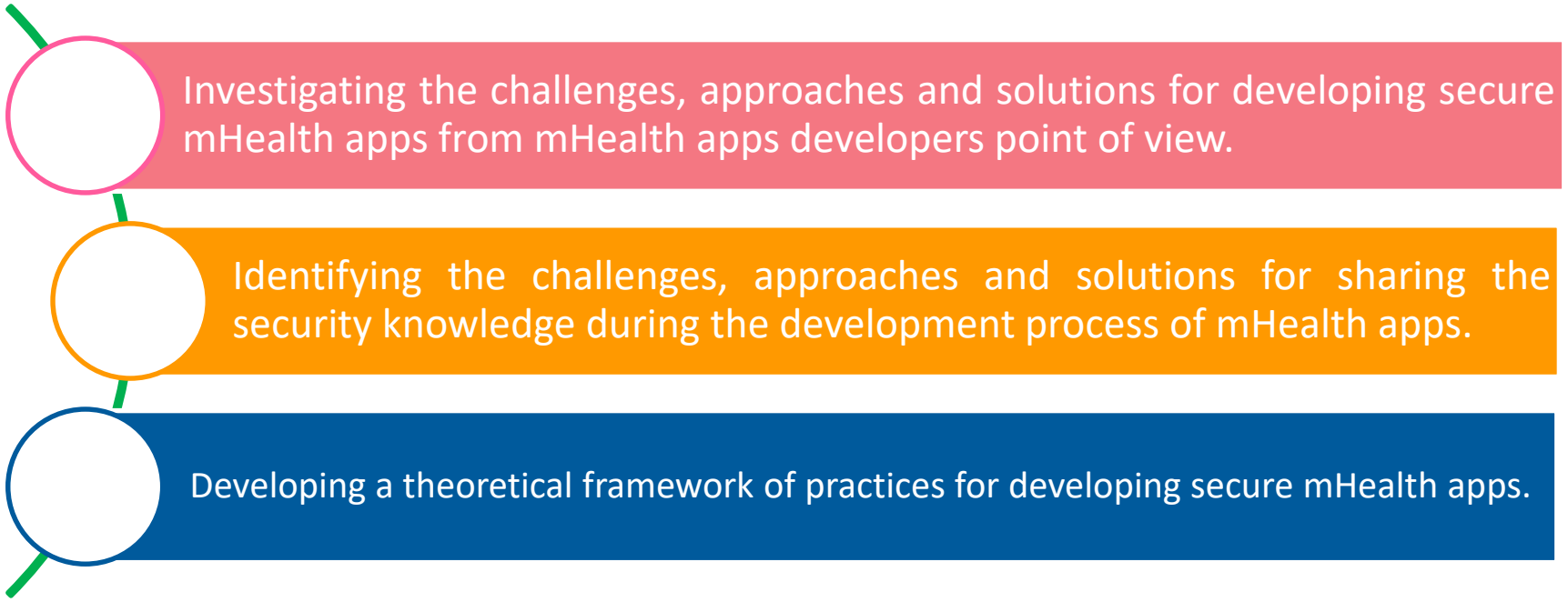
However

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



Submitted work

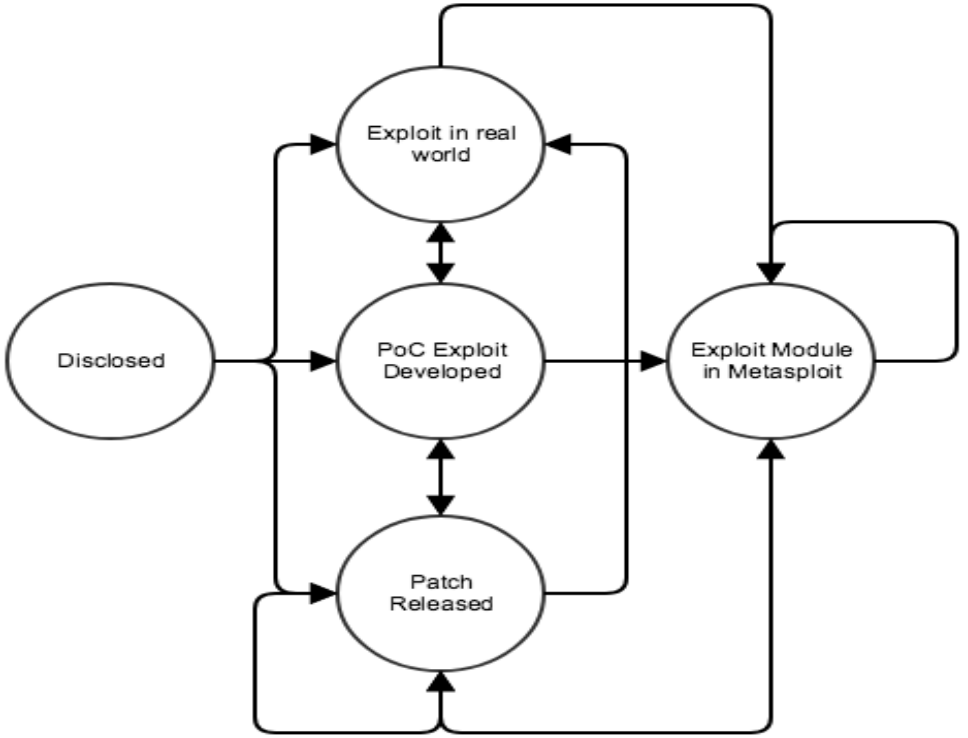
- A review paper (Challenges in Developing Secure Mobile Health Applications A Review) has been submitted to SEKE 2019 and it is under review).

Techniques for Cyber Vulnerability Exploit Prediction

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

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

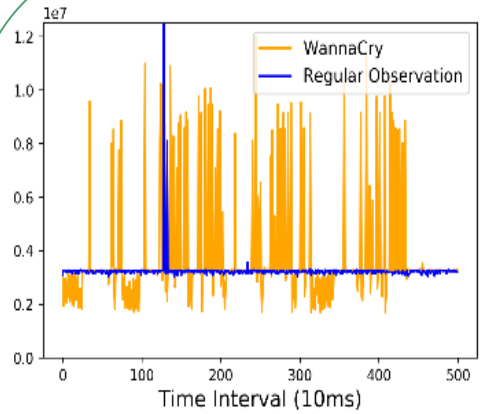
By Sarani Bhattacharya

Supervisor: Debdeep Mukhopadhyay
Institute: Indian Institute of Technology Kharagpur

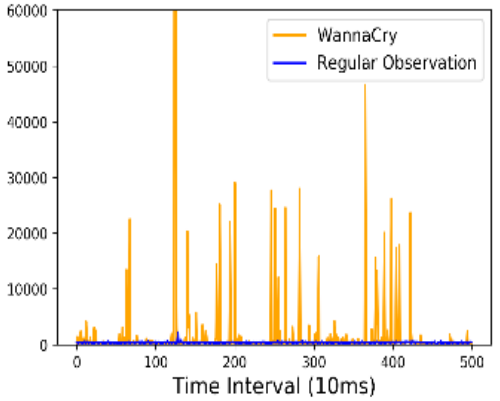
Does Ransomware affect the Performance Counters??

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

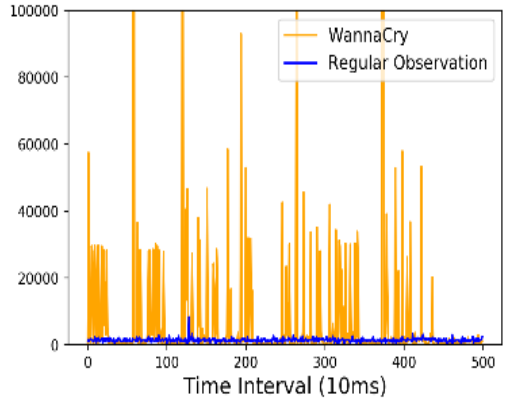
YES!!
Ransomware do affect these events.



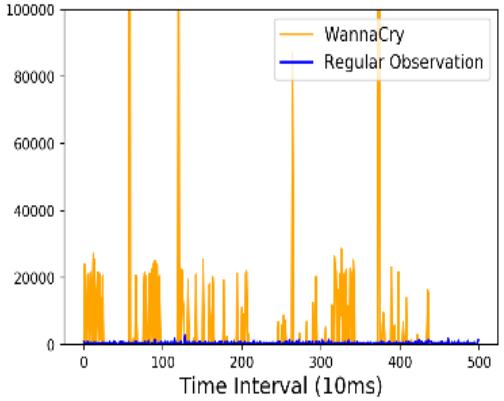
Branch Instructions



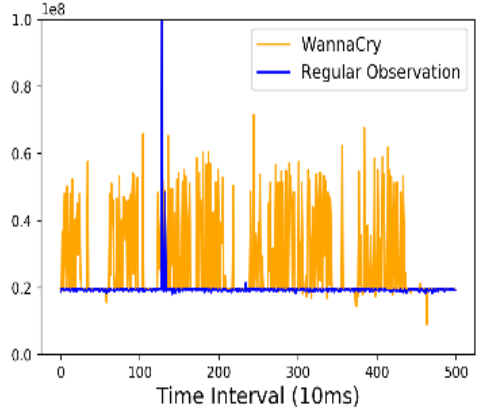
Branch Misses



Cache References

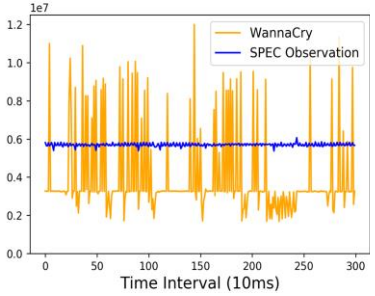


Cache Misses

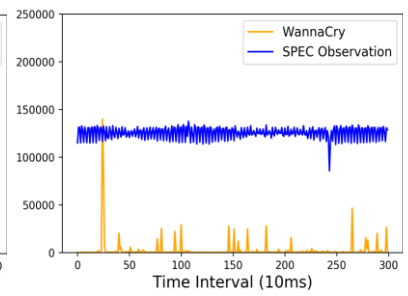


Instructions

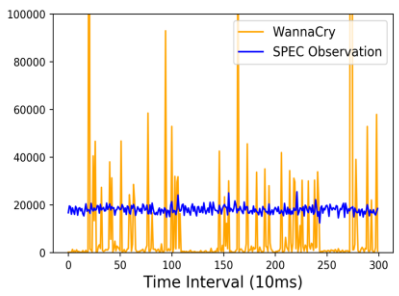
How good is reconstruction error as a decider??



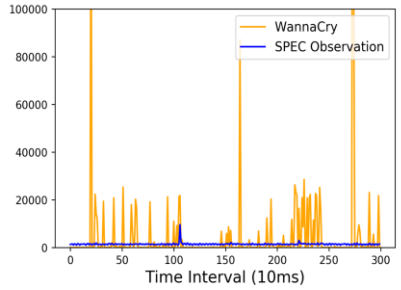
Branch Instructions



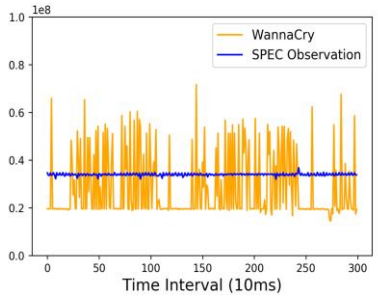
Branch Misses



Cache References

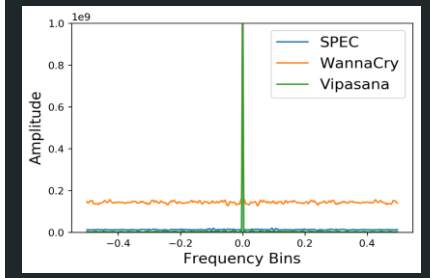


Cache Misses

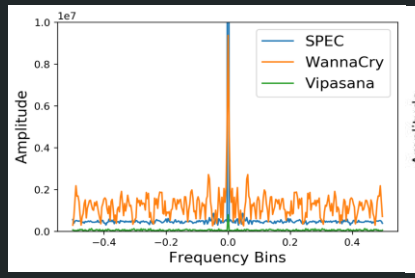


Instructions

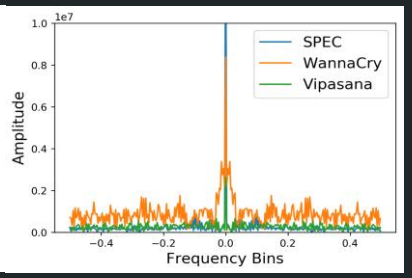
Utilizing Repeated Encryption of Ransomwares



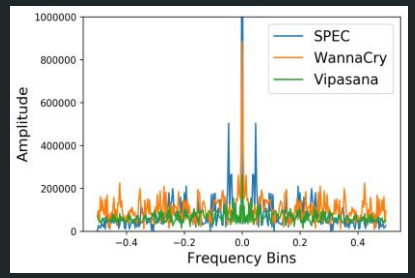
FFT of Branch Instructions



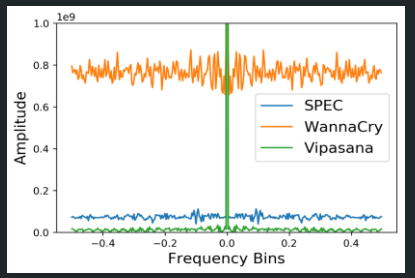
FFT of Branch Misses



FFT of Cache References



FFT of Cache Misses



FFT of Instructions

RATAFIA: Ransomware Analysis using Time And Frequency Informed Autoencoders", Manaar Alam, Sarani Bhattacharya, Swastika Dutta, Sayan Sinha, Debdeep Mukhopadhyay, and Anupam Chattopadhyay, IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, United States of America, May 6-10, 2019.