Australian Government
Department of Defence
Science and Technology

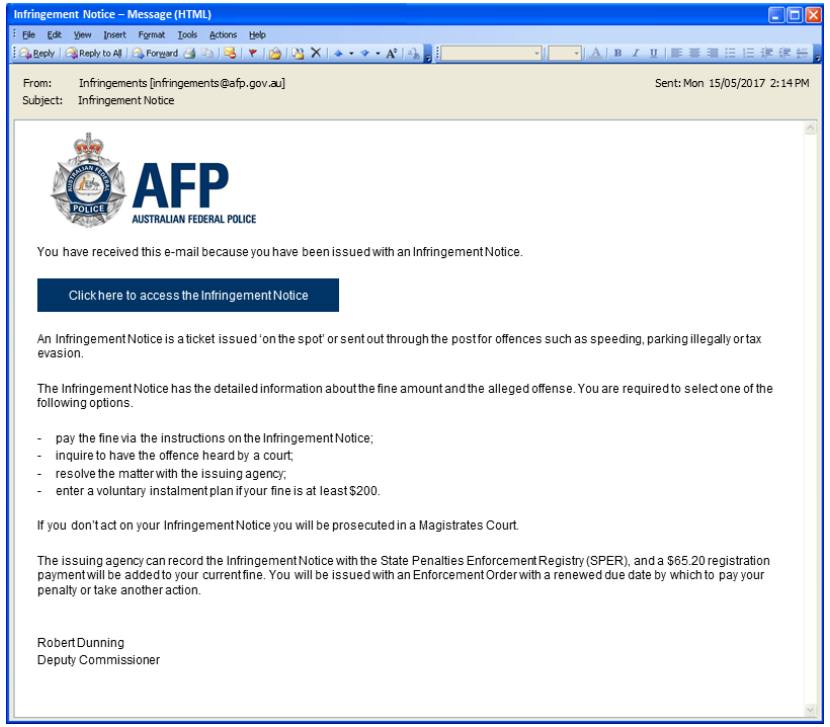
THE UNIVERSITY of ADELAIDE

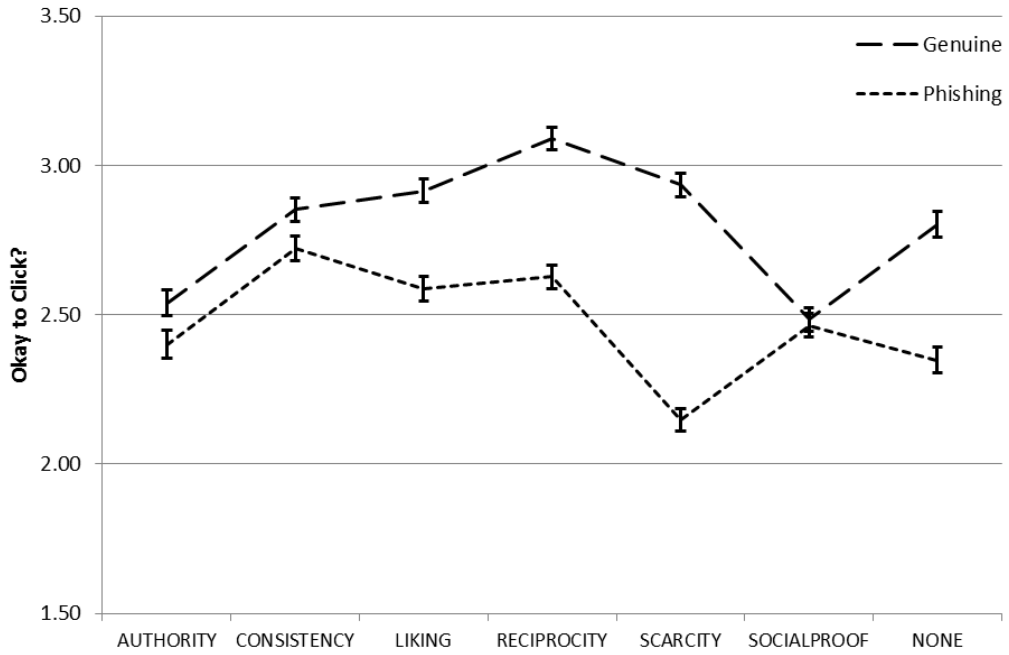
The Psychology of Influence in Cyberspace

Kathryn Parsons

Supervisors: Dr Marcus Butavicius (DST Group)
Professor Paul Delfabbro (University of Adelaide)

Predicting susceptibility to social influence in phishing emails





Outcomes

- Publications:
  - Parsons, K., Butavicius, M., Delfabbro, P., & Lillie, M. (2019). Predicting susceptibility to social influence in phishing emails. *International Journal of Human-Computer Studies, 128*, 17-26.
  - Parsons, K., Butavicius, M., Lillie, M., Calic, D., McCormac, A., & Pattinson, M. (2018). Which individual, cultural, organisational and interventional factors explain phishing resilience? In N. Clarke & S. Furnell (Eds.), *Proceedings of the Twelfth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2018)*. United Kingdom: University of Plymouth.

- Submitted publications:
  - Parsons, K., Butavicius, M., & Delfabbro, P. (2019). When influence principles backfire: An analysis of social media engagement rate in science news. Manuscript submitted for publication.
  - Parsons, K., Butavicius, M., & Delfabbro, P. (2019). The role of individual differences, misinformation, authority and social media news exposure on the processing of online news. Manuscript submitted for publication.

THE UNIVERSITY of ADELAIDE

Australian Government
Department of Defence
Science and Technology

ARE YOU TIRED OF CYBERSECURITY?

adelaide.edu.au

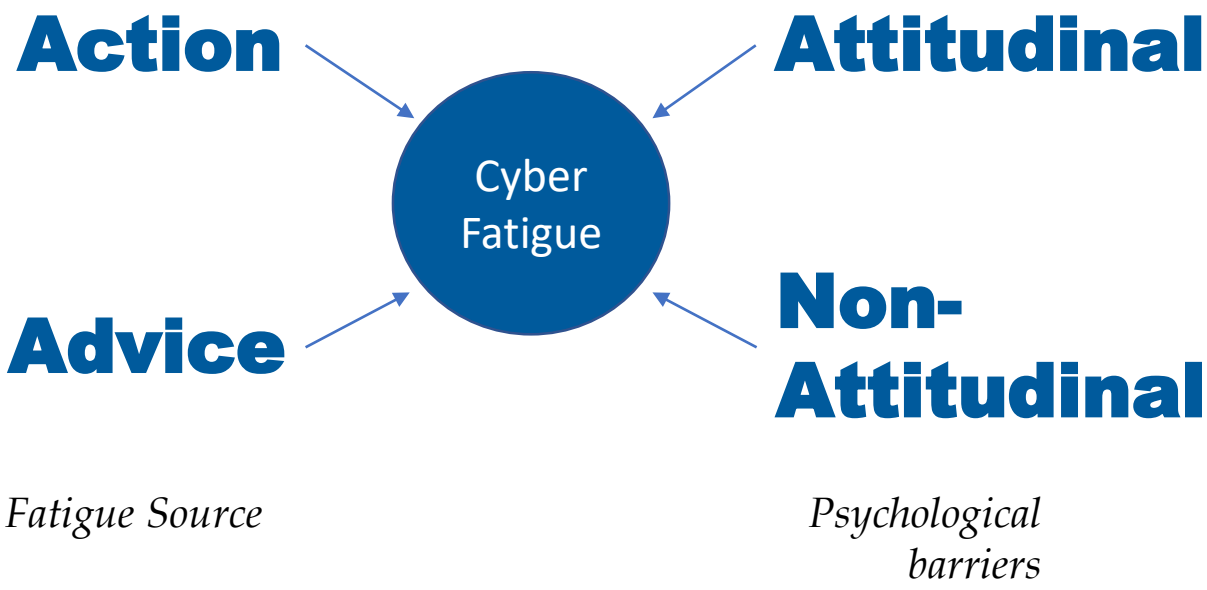
Student: Andrew Reeves
Supervisors: Dr. Dragana Calic (DSTG), Prof. Paul Delfabbro (University of Adelaide)

Are you tired of cybersecurity?

Cyber Fatigue:

A tiredness or aversion to cybersecurity-related workplace behaviours as a result of prior overexposure to cybersecurity.

The four component model



Submitted work

- Reeves, A., Calic, D., Delfabbro, P. "*Do employees care about Cybersecurity? The four-component model of Cyber Fatigue: a case for advice and action*". Submitted to the Journal of Computers in Human Behavior.

5 studies planned for 2019

- **Studies 1 & 2:** Examining the effect of action fatigue on cybersecurity behaviour.
- **Study 3:** A qualitative exploration of cybersecurity advice fatigue.
- **Study 4:** The effect of advice fatigue on cybersecurity behaviour.
- **Study 5:** Examining the interaction between action and advice fatigue.

References

- *Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013). Phishing for the Truth: A Scenario-Based Experiment of Users' Behavioural Response to Emails. In L. J. Janczewski, H. Wolf, & S. Shenoi (Eds.), Security and Privacy Protection in Information Processing Systems - IFIP Advances in Information and Communication Technology (Vol. 405, pp. 366-378): Springer.*
- *Amran, A., Zaaba, Z. F., & Mahinderjit Singh, M. K. (2018). Habituation effects in computer security warning. In (Vol. 27, pp. 119-131): Taylor & Francis.*

Internet of Things (IoT) Aged Care Monitoring Devices: An Investigation into Privacy from Different Stakeholders' Perspective

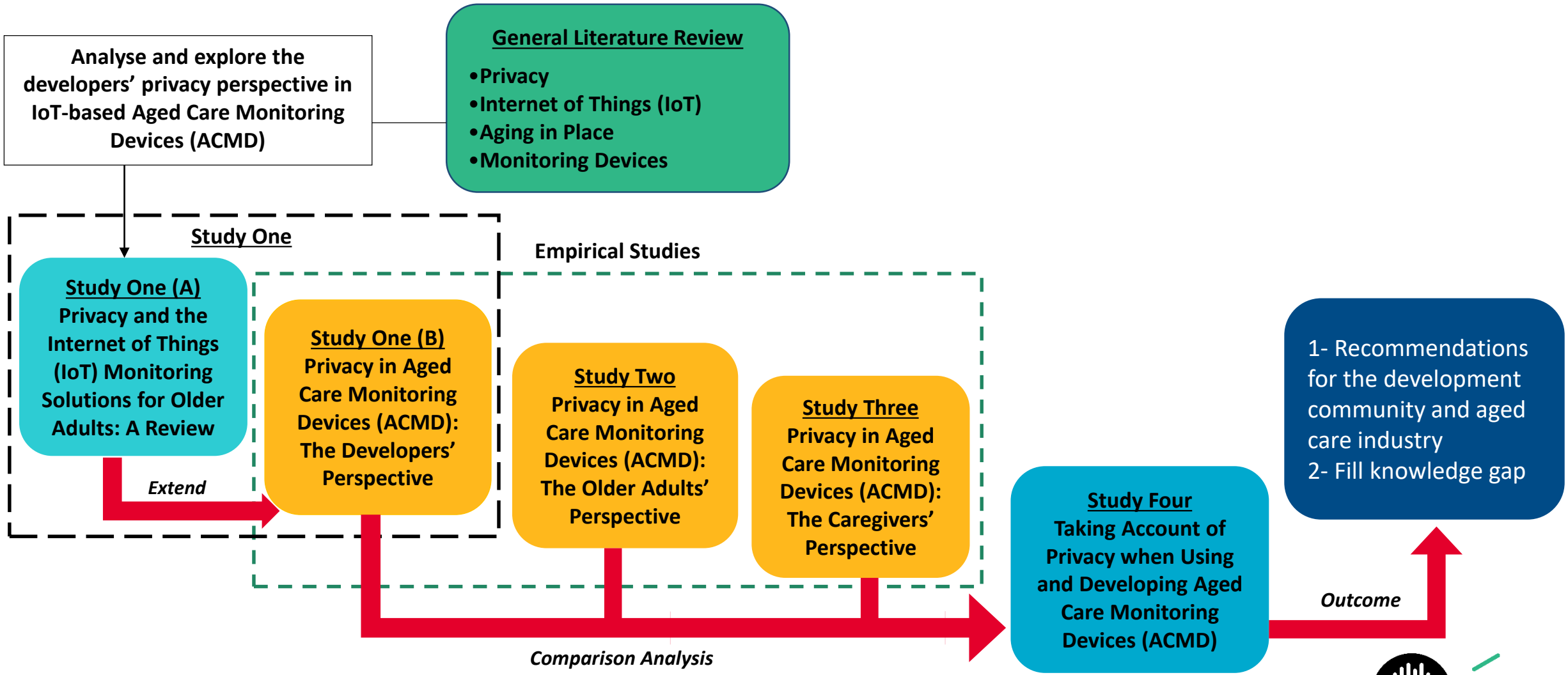
Sami Alkhatib, The University of Melbourne

20 / 03 / 2019

www.data61.csiro.au

Supervisors:
Dr Jenny Waycott, The University of Melbourne
Dr George Buchanan, The University of Melbourne
Dr Shuo Wang, CSIRO's Data61
Dr Marthie Grobler, CSIRO's Data61

Exploring stakeholders' privacy perspective in Aged Care Monitoring Devices



Outcome

- List of Publications:
  - Privacy and the Internet of Things (IoT) Monitoring Solutions for Older Adults: A Review. The 26th Australian National Health Informatics Conference (HIC 2018), Sydney.
- Submitted Work:
  - Privacy in Aged Care Monitoring Devices (ACMD): The Developers' Perspective. HIC 2019 in Melbourne.
- Ongoing Work:
  - Submitted ethics application (pending approval), Melbourne University.
  - Contacting aged care facilities, cooperate on study 2 & 3.

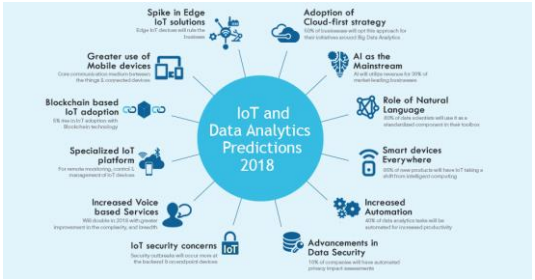
Adversarial machine learning in IoT

Anahita Namvar

Primary Supervisor : Salil Kanhere

Data61 supervisor: Seyit camtepe

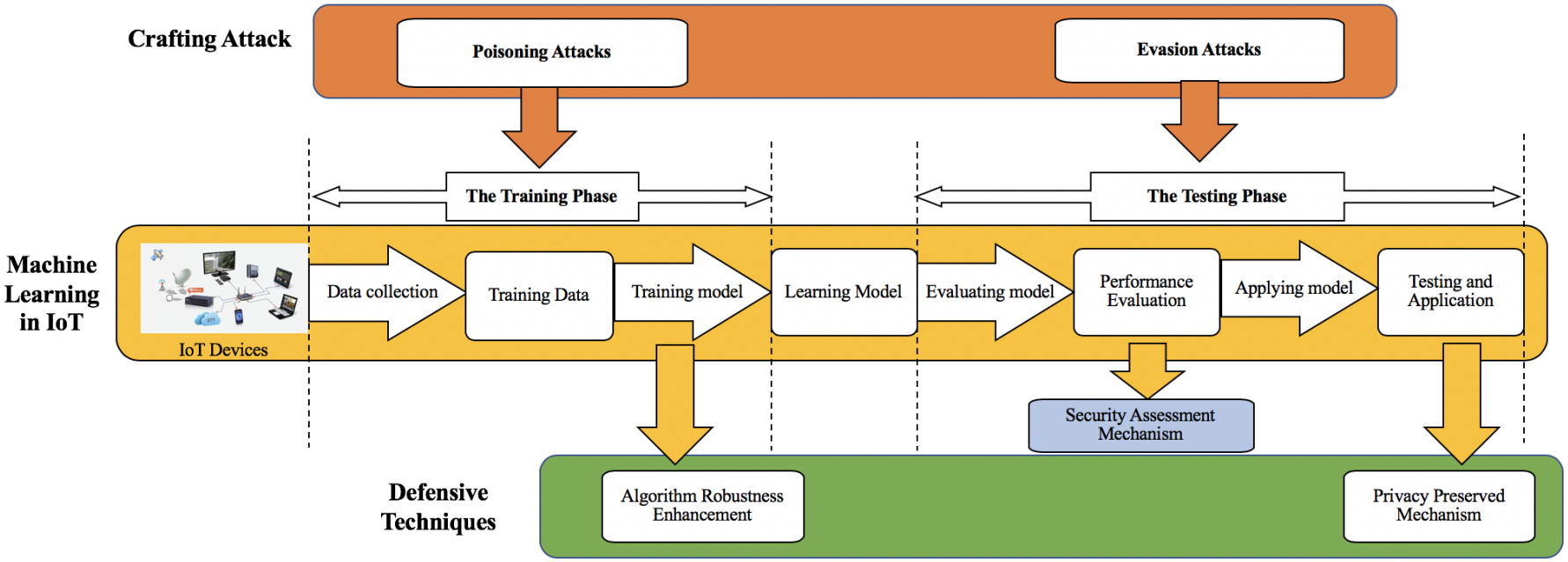
Adversarial Machine learning in IoT



IoT and Data Analytics

Adversarial Attacks in ML

Secure ML & AI systems



Adversarial learning in IoT device identification domain

- We provided a framework to model potential attack scenarios against machine learning based IoT device identification systems
- we performed our experimental results using real-world network dataset
- We implemented white-box evasion untargeted attack against multinomial logistic regression classifier
- The results showed manipulating certain features by crafting data-driven adversarial attack based on Fast gradient sign method can compromise learner and misclassify input data as the wrong device

LSB: Lightweight and optimized blockchain for IoT

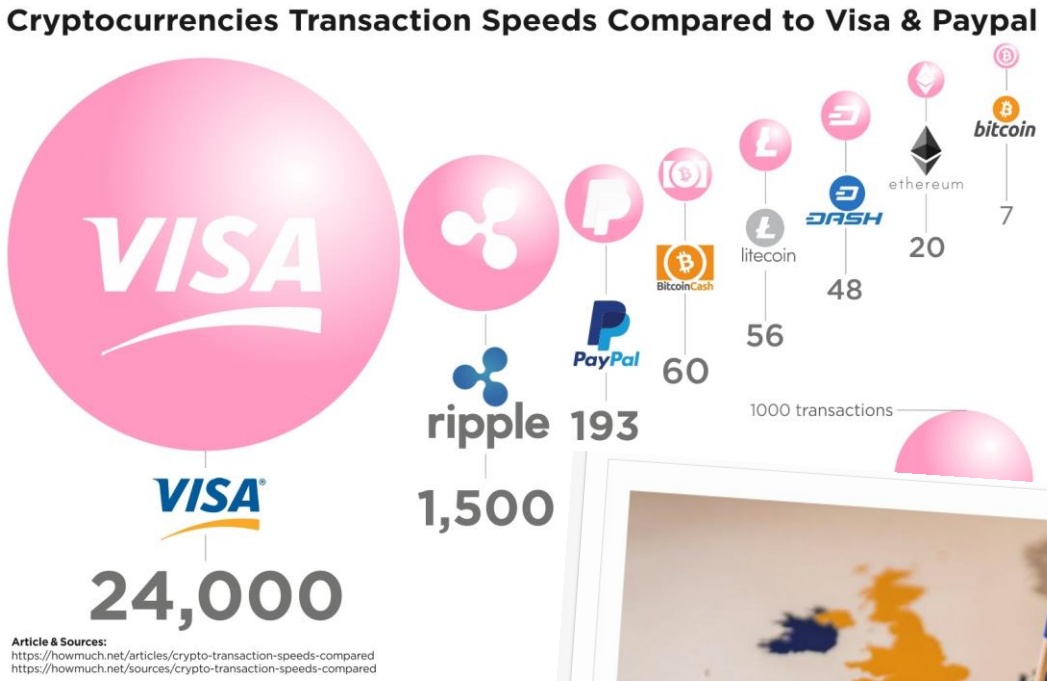
Ali Dorri, School of Computer Science and Engineering, UNSW, and CSIRO

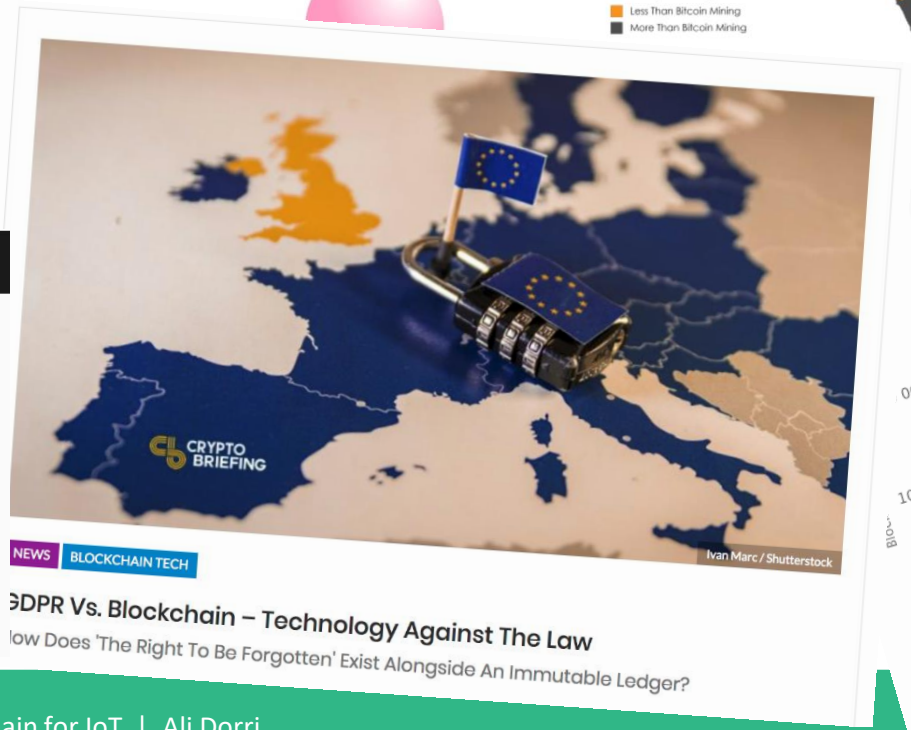
Supervisors: Prof Salil Kanhere, School of Computer Science and Engineering, UNSW.

Prof Raja Jurdak, Data61 CSIRO, Brisbane.

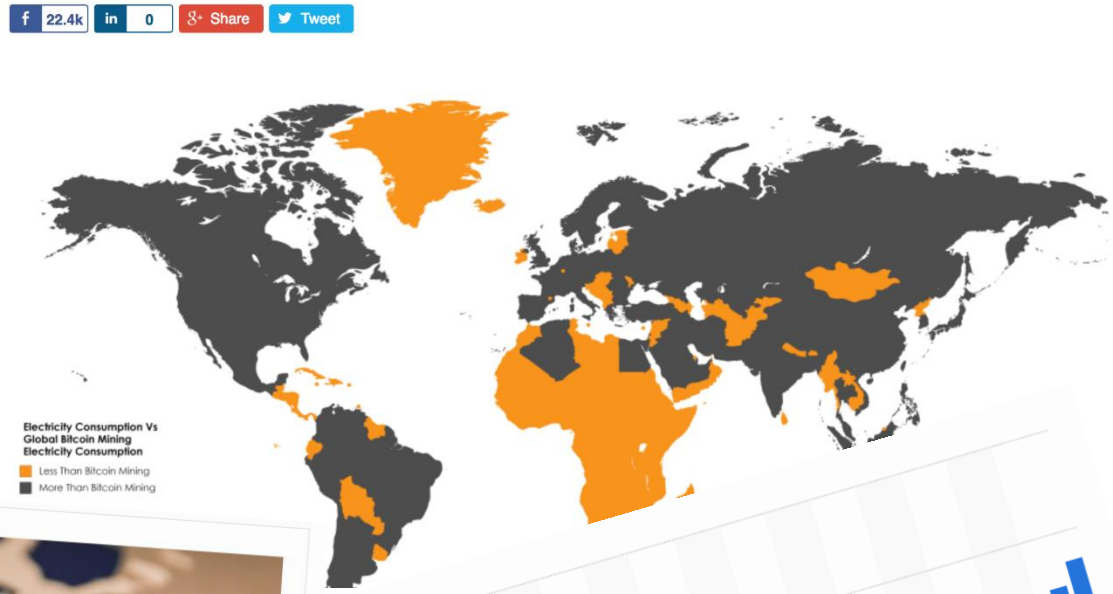
www.data61.csiro.au

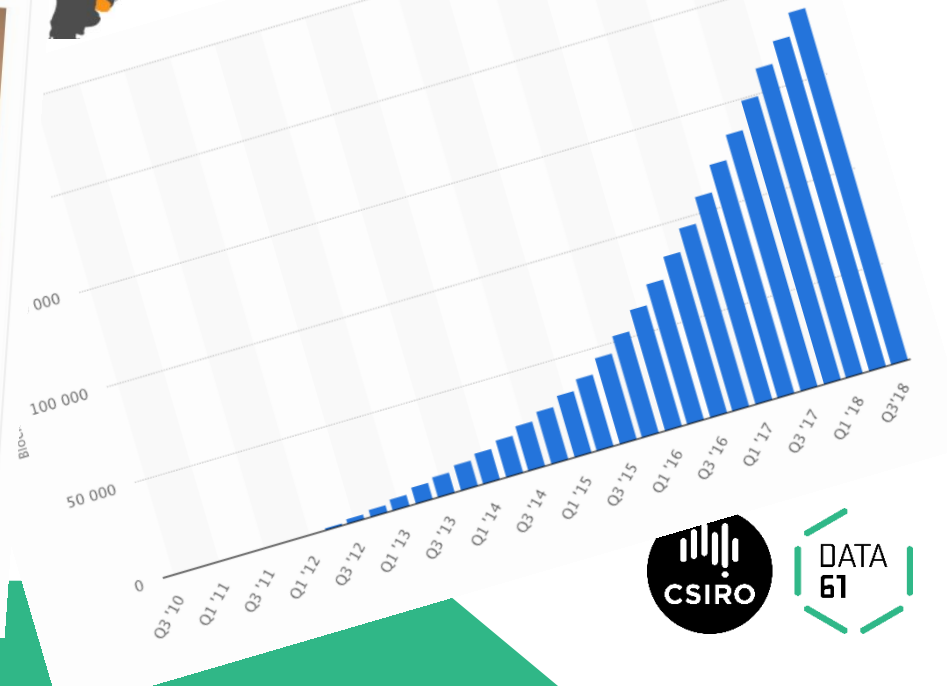
Problem identification





Bitcoin Mining Now Consuming More Electricity Than 159 Countries Including Ireland & Most Countries In Africa





Outcome

Publications

- **Published 13 conference, journal, and book chapters in total.**
  - **Dorri, A.**, Kanhere, S. S., & Jurdak, R. (2019). MOF-BC: A memory optimized and flexible blockchain for large scale networks. Future Generation Computer Systems, 92, 357-373.
  - **Dorri, A.,** Luo, F., Kanhere, S. S., Jurdak, R., & Dong, Z. Y. (2019). Spb: A secure private blockchain-based solution for energy trading. IEEE Communications Magazine (accepted to be published).
  - **Dorri, A.,** Kanhere, S. S., & Jurdak, R. (2018). Multi-Agent Systems: A survey. IEEE Access, vol 6, pages 28573-28593
  - **Dorri, A.,** Steger, M., Kanhere, S. S., & Jurdak, R. (2017). Blockchain: A distributed solution to automotive security and privacy. IEEE Communications Magazine, 55(12), 119-125.
- **Publications received 520 citations, over 60K download, and selected as most popular and top cited papers in their venues, and IEEE and ACM digital libraries.**

Highly efficient Blockchain

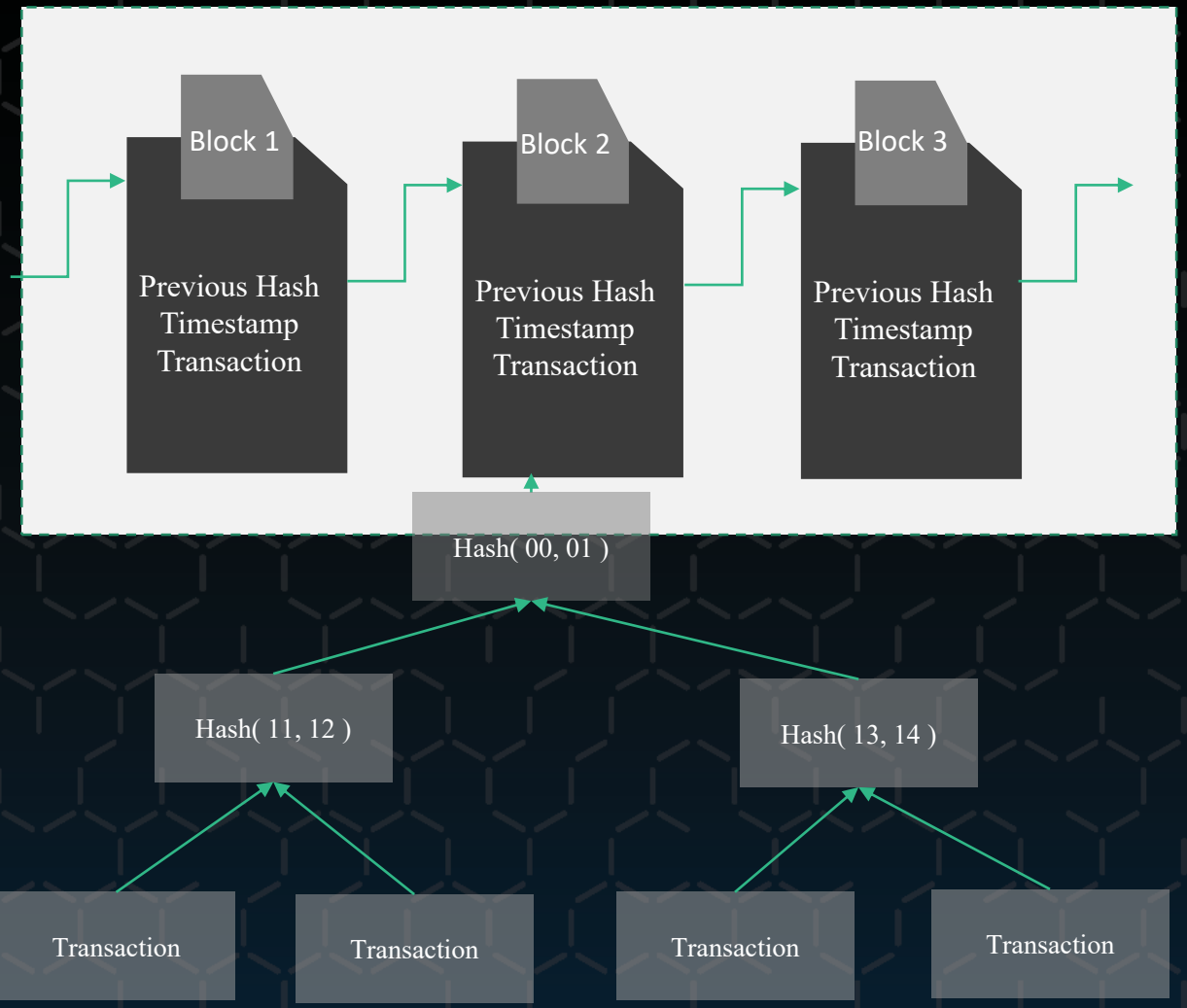
Qin WANG

Supervisors: Yang Xiang, Shiping Chen, Jiangshan Yu

Swinburne Uni && Data61

www.data61.csiro.au

Problem Statement



Bottleneck on TPS
(Transaction per seconds)

Bitcoin 7 TPS

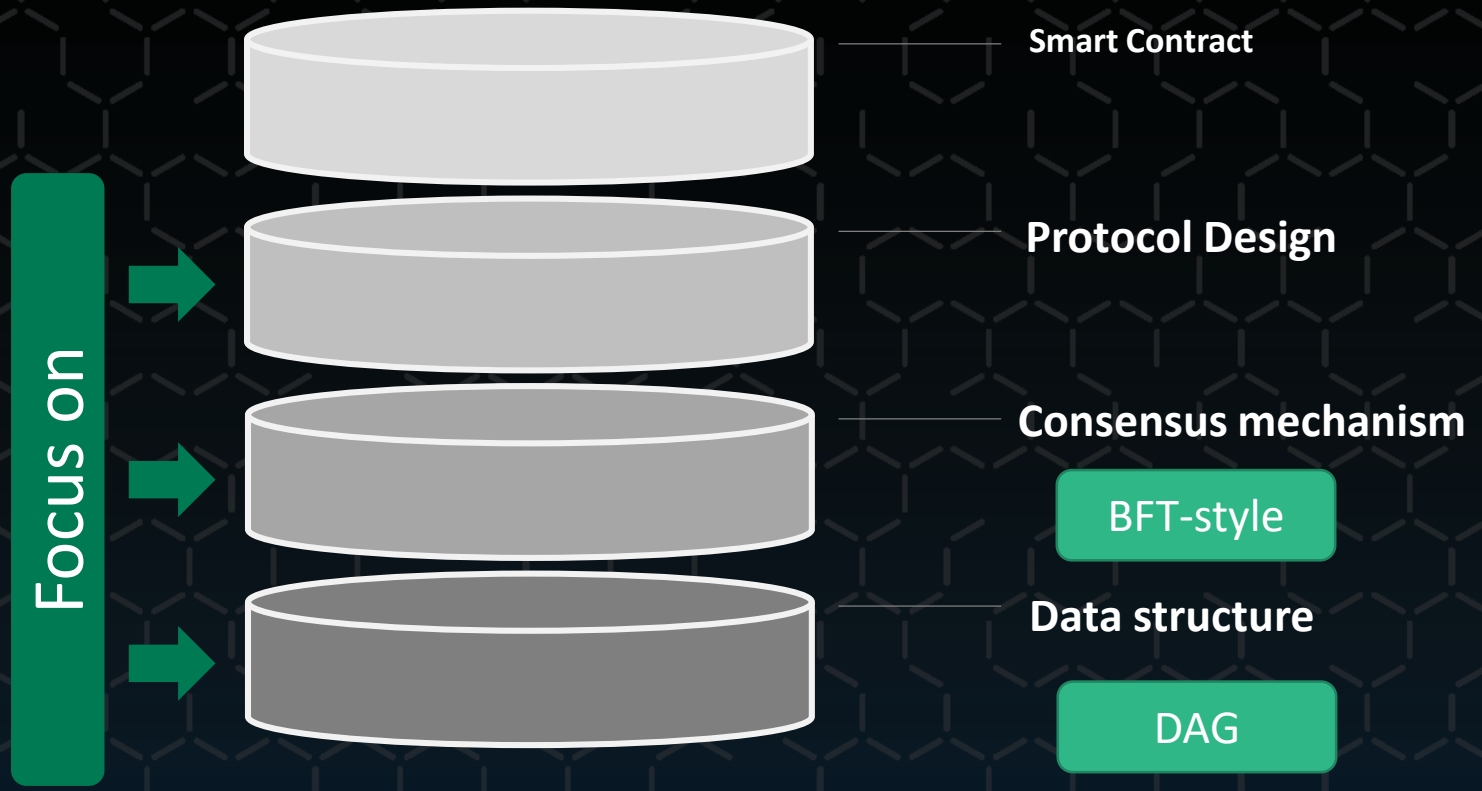
Ethereum 30 TPS

Gap

Visa 56000 TPS

Accessibility for large-scale applications

Work on:



Submitted paper:

- Anonymous Blockchain-based System for Consortium. *ACM TMIS*
- pAuditChain: A Personal/Bulk Data Auditing Framework for Energy Supply Industries. *IEEE TII*
- Security Analysis on NEO. *ASIACCS 2019*

Security-Enhancing Commodity OS (Operating System) Kernels

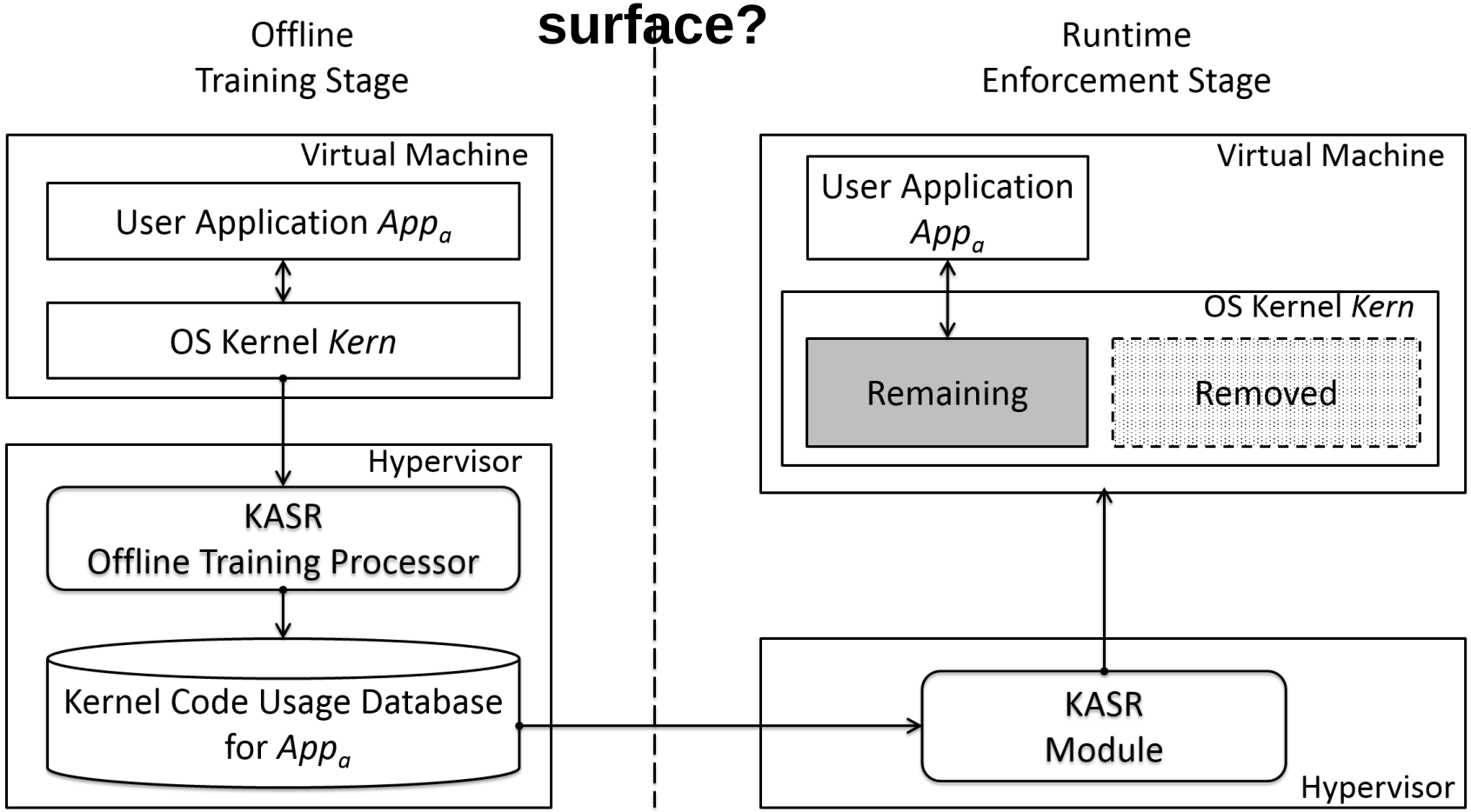
Zhi Zhang

Supervisors: Surya Nepal (Data61, CSIRO) and Fethi Rabhi (the University of New South Wales)

www.data61.csiro.au

Overview

What can be done to reliably and practically reduce the kernel attack surface?



Outcome

- **Accepted: Zhang Z.**, Cheng Y., Nepal S., Liu D., Shen Q., Rabhi F. KASR: A Reliable and Practical Approach to Attack Surface Reduction of Commodity OS Kernels. In: Bailey M., Holz T., Stamatogiannakis M., Ioannidis S. (eds) Research in Attacks, Intrusions, and Defenses. RAID 2018. Lecture Notes in Computer Science, vol 11050. Springer, Cham.
- **Submitted:** Yueqiang Cheng, **Zhi Zhang**, Surya Nepal, Zhi Wang. CATTmew: Defeating Software-only Physical Kernel Isolation. (N.B., I am the co-first author in alphabetical order. We are required to do a major revision to make the paper accepted by IEEE Transactions on Dependable and Secure Computing.)
- **Accepted:** Yueqiang Cheng, **Zhi Zhang**, Surya Nepal**,** Zhi Wang. Winter is Coming Back: Defeating the Advanced Rowhammer Defense to Gain Root and Kernel Privileges. In Black Hat Asia 2019. (N.B., I am the co-first author in alphabetical order.)

Developing a Systematic Approach to Evaluate the Usability of Security APIs

Chamila Wijayarathna

Supervisors : Dr. Nalin A. G. Arachchilage, Dr. Marthie Grobler

2019-03-22

UNSW CANBERRA

Humans are the Weakest Link in Information security..

Users

Information Workers

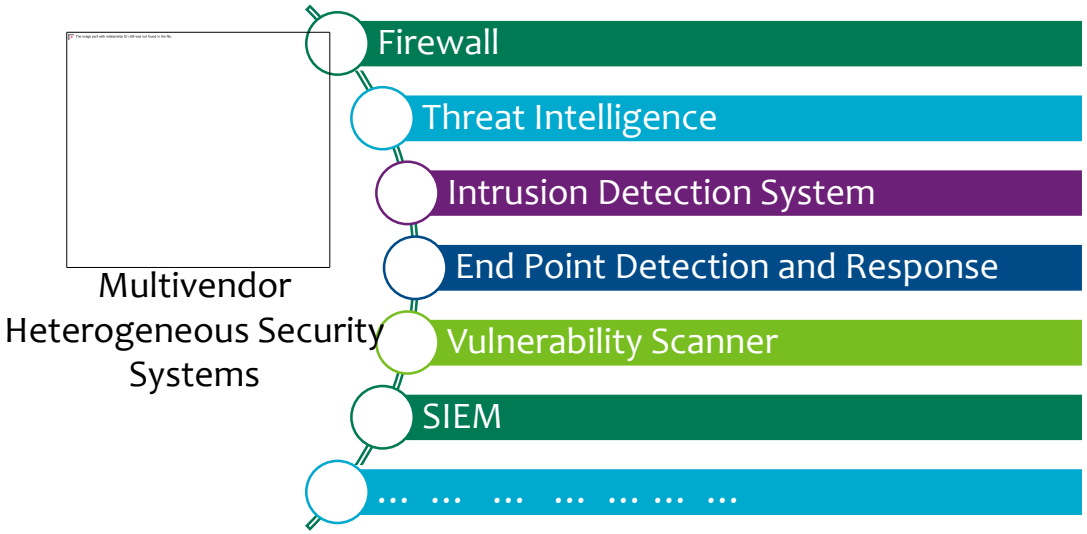
Research Outcome : Publication

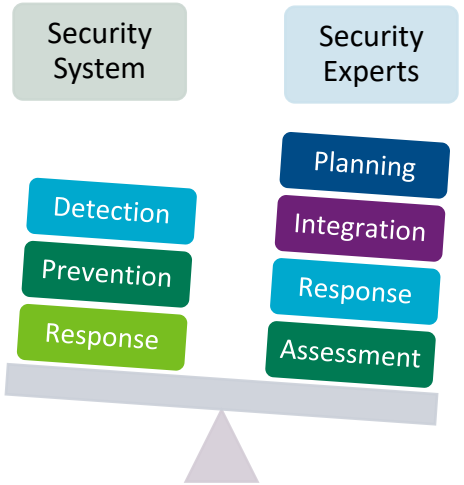
- Chamila Wijayarathna, Nalin Asanka Gamagedara Arachchilage, and Jill Slay. "A generic cognitive dimensions questionnaire to evaluate the usability of security APIs." International Conference on Human Aspects of Information Security, Privacy, and Trust. Springer, Cham, 2017.
- Chamila Wijayarathna, Nalin Asanka Gamagedara Arachchilage, and Jill Slay. “Using cognitive dimensions questionnaire to evaluate the usability of security APIS”, Proceedings of the 28th annual meeting of the psychology of programming interest group (2017)
- Chamila Wijayarathna, Nalin Asanka Gamagedara Arachchilage, “Why johnny can’t store passwords securely?: A usability evaluation of bouncycastle password hashing”, Proceedings of the 22nd international conference on evaluation and assessment in software engineering, ACM(2018), pp. 205-210, 10.1145/3210459.3210483
- Chamila Wijayarathna, Nalin Asanka Gamagedara Arachchilage, “Why Johnny can’t develop a secure application? A usability analysis of Java Secure Socket Extension API,” Computers & Security, Volume 80,2019,Pages 54-73,ISSN 0167-4048, https://doi.org/10.1016/j.cose.2018.09.007.
- Chamila Wijayarathna, Nalin Asanka Gamagedara Arachchilage, “Am I Responsible for End-User’s Security? A Programmer's Perspective,” 4th Workshop on Security Information Workers, 2018.
- Chamila Wijayarathna, Nalin Asanka Gamagedara Arachchilage, “A methodology to Evaluate the Usability of Security APIs,” 9th IEEE International Conference on Information and Automation for Sustainability, 2018.
- Chamila Wijayarathna, Nalin Asanka Gamagedara Arachchilage, “Fighting Against XSS Attacks: A Usability Evaluation of OWASP ESAPI Output Encoding,” 52nd Hawaii International Conference on System Sciences (HICSS), 2019.
- Chamila Wijayarathna, Nalin Asanka Gamagedara Arachchilage, “An Empirical Usability Analysis of the Google Authentication API”, Proceedings of the 23nd international conference on evaluation and assessment in software engineering (2019) (To appear)

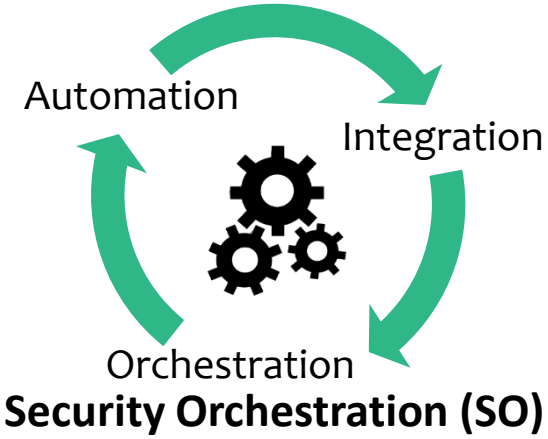
Architecture Support for Security Orchestration

Presented by: Chadni Islam
Supervisor Team: Professor M. Ali Babar and Dr. Surya Nepal

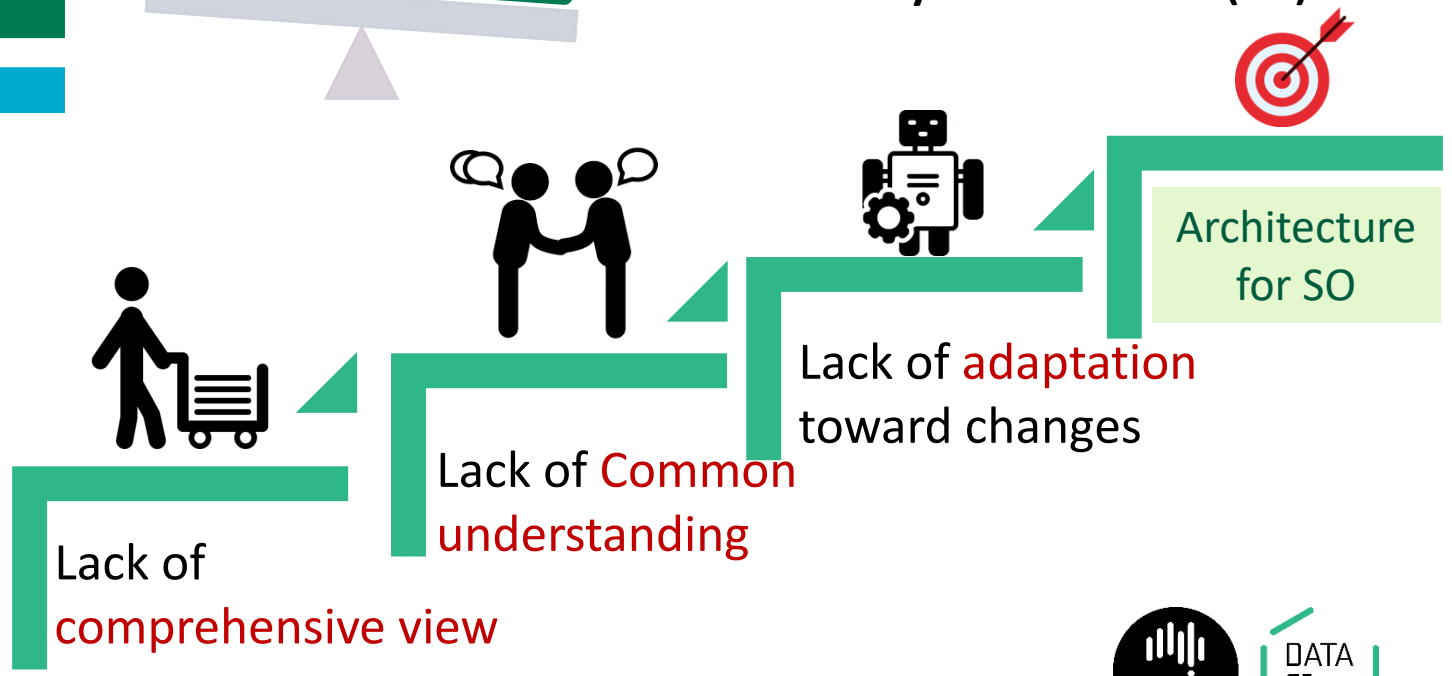
Problem Identification







- Security data generated and ingested by Security System are *diverse* in nature
- Lack of *Interpretability* of the generated data and *Interoperability* among different security systems



Publication Outcome and Ongoing Work

- **Publication**

- Chadni Islam, M. Ali Babar and Surya Nepal, “A Multi-vocal Review on Security Orchestration”, ***ACM Computing Survey***, 2019, **Accepted, *In press*** (**Rank A***)
- Chadni Islam, M. Ali Babar and Surya Nepal, “An Ontology-Driven Approach to Automating the Process of Integrating Security Software System”, ***International Conference on Software and Systems Process (ICSSP)***, 25-26 May, 2019, Montreal, Canada, **Accepted,** (**Rank A**)
- Chadni Islam, M. Ali Babar and Surya Nepal, “Automated Interpretation and Integration of Security Tools Using Semantic Knowledge”, ***31st International Conference on Advanced Information Systems Engineering, (CAiSE)***, 3-7 June 2019, Rome, Italy, **Accepted,** (**Rank A**)

- Ongoing Work

- API Driven Architecture for Security Orchestration
- A Learning-based Framework for a Self Adaptive Security Orchestration Platform

Detecting Malicious Network Activities for Enterprise Networks

Presented by: Jawad Ahmed

Data61 Supervisor: Craig Russell

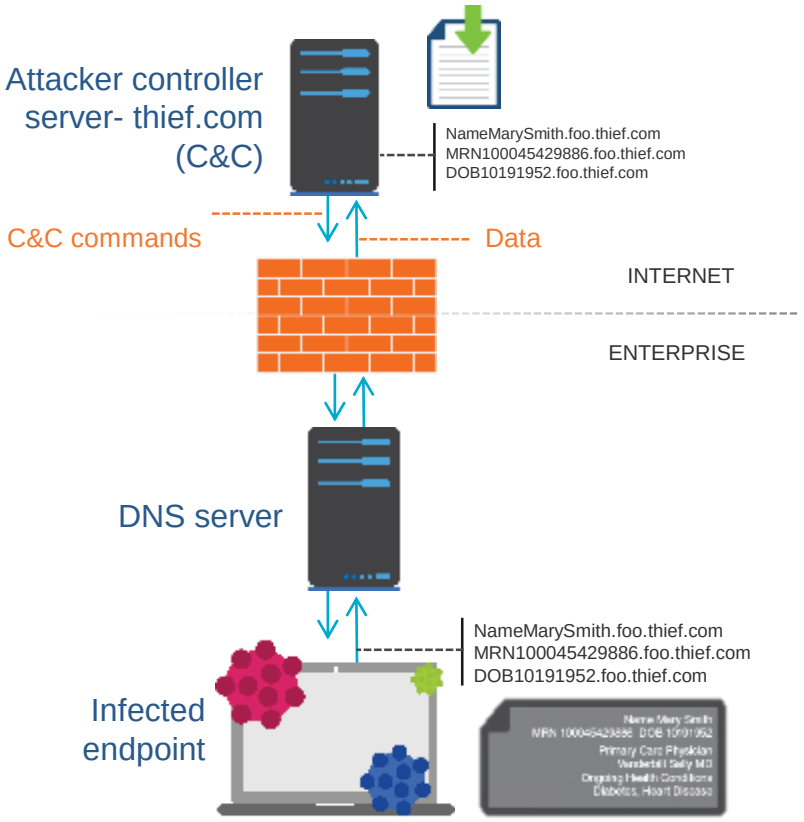
UNSW Supervisor: Vijay Sivaraman

UNSW Co-supervisor: Hassan Habibi

Problem Statement

- Detecting Malicious Network Activities for Enterprise Networks
  - DNS-related attacks (e.g. Exfiltration, Tunneling)
- Real-time at Scale
- Demonstrate efficacy of solution in our Campus and CSIRO networks

DNS Exfiltration



Outcome

- J. Ahmed, H. Habibi Gharakheili, Q. Raza, C. Russell and V. Sivaraman, **"Real-Time Detection of DNS Exfiltration and Tunneling from Enterprise Networks"** in IFIP/IEEE IM'2019 Washington D.C. USA
- J. Ahmed, H. Habibi Gharakheili, Q. Raza, C. Russell and V. Sivaraman, **"Demo Abstract: A Tool to Detect and Visualize Malicious DNS Queries for Enterprise Networks"** in IFIP/IEEE IM Demo'2019 Washington D.C. USA
- J. Ahmed, H. Habibi Gharakheili, Q. Raza, C. Russell and V. Sivaraman, **"Monitoring Enterprise DNS Queries for Detecting Data Exfiltration from Internal Hosts"** under review in IEEE Transactions on Network and Service Management (TNSM)

Securing an Enterprise Network using Network Programmability and Forensics

Speaker: Minzhao Lyu (Data61, CSIRO and UNSW Sydney)

Supervisors: Craig Russell (Data61, CSIRO), Hassan Habibi Gharakheili and Vijay Sivaraman (UNSW Sydney)

www.data61.csiro.au

Problem Statement

- Specific Designed Hardware Firewalls:
  - Using static security rules and configuration files
    - Difficult to add new features.
    - Need Professions in Cyber-Security.
- CPU-based Software Intrusion Detection Systems:
  - Using signatures to isolate malicious traffic.
    - Hard to scale up to large-enterprise level.
    - Need Professions in Cyber-Security.

Publications and On-going Works

- **Protecting an Enterprise Network from DNS Volumetric Attacks**
- **Understanding DNS traffic profile of enterprise hosts**
  - M. Lyu, H. Habibi Gharakheili, C. Russell, and V. Sivaraman, "Mapping an Enterprise Network by Analyzing DNS Traffic," *in Proc. Passive and Active Measurement (PAM)*, Puerto Varas, Chile, Mar 2019.
- **Detection of DNS volumetric attacks on enterprise networks**
  - Paper submitted, under double-blind review.
- **Protecting an Enterprise Network from DDoS Attacks (Ongoing Work)**
  - Constructing and maintaining volumetric traffic profile of an enterprise network
  - Detection of DDoS attacks on enterprise networks

Enhancing Security in Random Wireless Network with the Aid of Friendly Jammers

Jishan E Giti

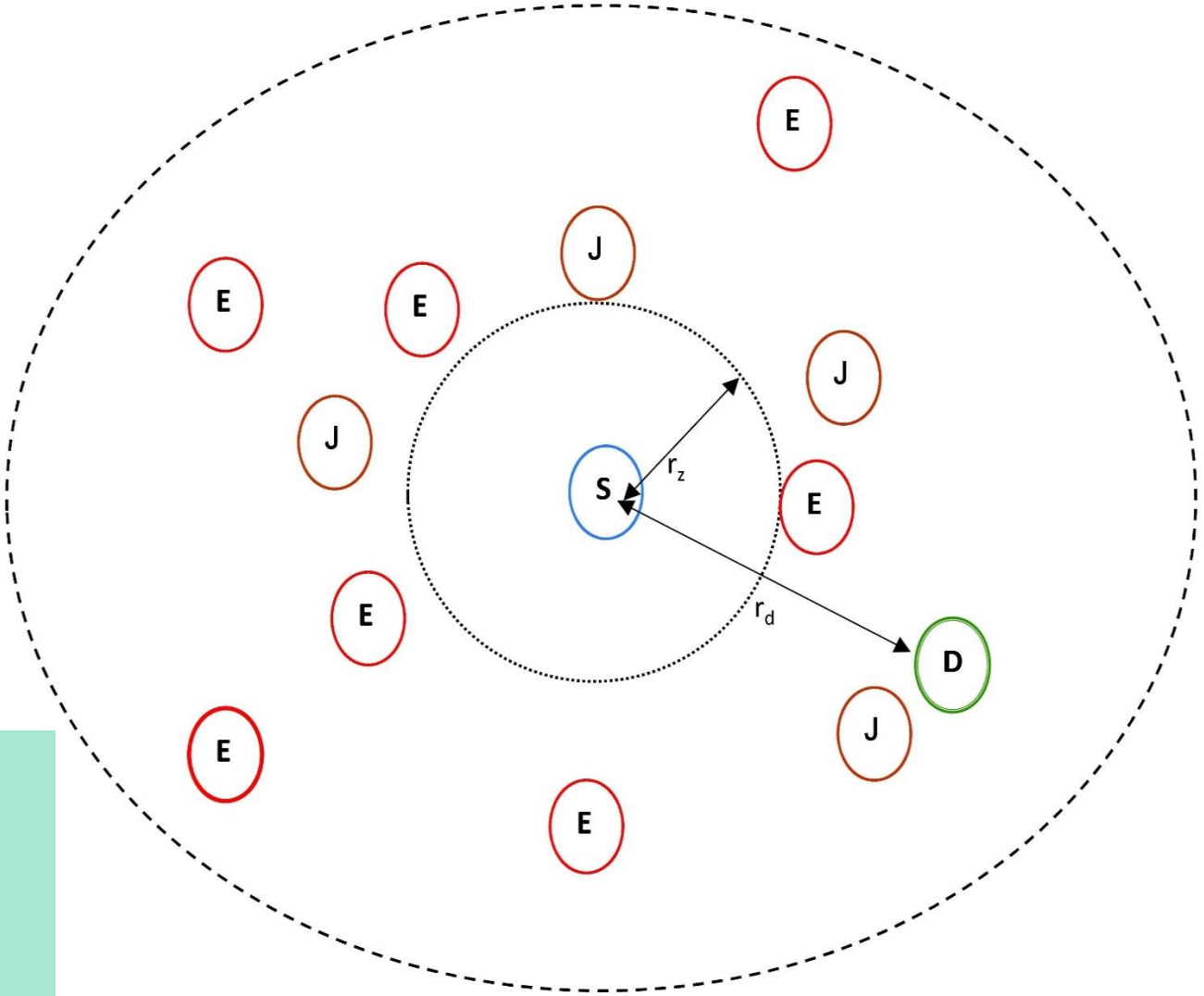
Supervisors:
Dr. Amin Sakzad (Monash University)
Prof. Balasubramaniam Srinivasan (Monash University)
Prof. Joarder Kamruzzaman (Federation University)
Dr. Raj Gaire (CSIRO|Data61)

www.data61.csiro.au

5/04/2019

Random wireless network with secrecy protected zone and adaptive eavesdroppers.

S- source
D- destination
E- eavesdropper
J- friendly jammer



Goal of the project:
To tackle adaptive/active eavesdropping with the aid of cooperative friendly jammers.

Publications

1. J. E. Giti, B. Srinivasan and J. Kamruzzaman, “Impact of Friendly Jammers on Secrecy Multicast Capacity in Presence of Adaptive Eavesdroppers”, **IEEE GLOBECOM 2017 Workshops: 5th IEEE GLOBECOM Workshop on Trusted Communications with Physical Layer Security**, Singapore, 4-8 December, 2017. (Published)

2. J. E. Giti, A. Sakzad, B. Srinivasan, R. Gaire and J. Kamruzzaman, ”Impact of Friendly Jammers on Secrecy Outage Probability in Presence of Adaptive Eavesdroppers”, **IEEE International Symposium on Information Theory (ISIT)**, Paris, France, 7-12 July, 2019. (Submitted)

Data Access Control for Multiple Domains and Storage Systems

Ahmad SALEHI SHAHRAKI (PhD student (Cybersecurity LAB) at Monash University)

Supervisors:

A/Prof. Dr. Carsten Rudolph (Monash University)

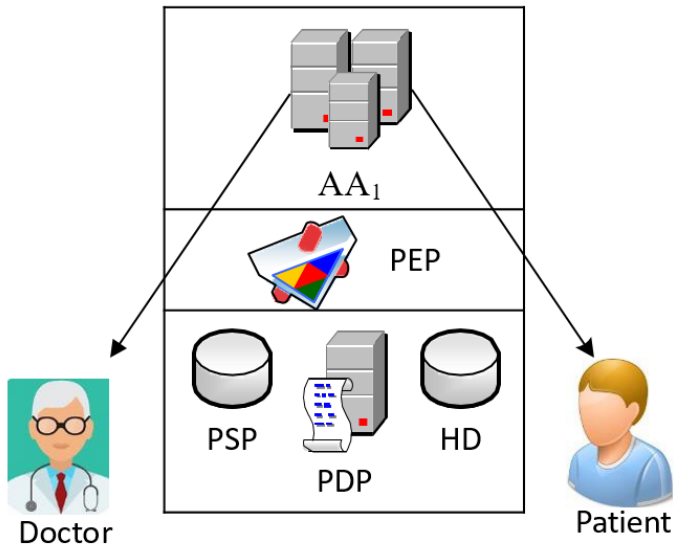
Prof. Dr. Bala Srinivasan (Monash University)

Dr. Marthie Grobler (Data61)

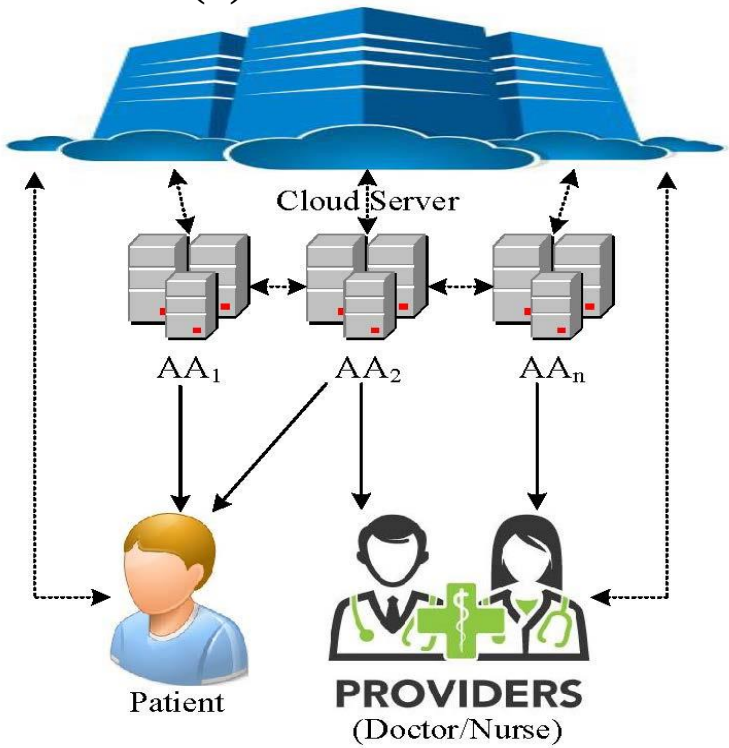
www.data61.csiro.au

An overview and contribution

(1) Single domain



(2) Multi-domain



A) Health Insurance Portability and Accountability Act (HIPPA)
B) National Institute of Standards and Technology (NIST)

1) Do not create a central data-base
2) Let all entities define their own policies
3) Support decentralised policy decision and policy enforcement
4) Keep the role of any central trusted authority minimal

List of publications

- Publications:

1) User-Centered Attestation for Layered and Decentralized Systems," Workshop on Decentralized IoT Security and Standards (The Network and Distributed System Security Symposium) (DISS-NDSS) 2018" Rank-A
2) A Dynamic Cross-Domain Access Control Model for Collaborative Healthcare Application, "IFIP/IEEE International Symposium on Integrated Network Management (IM'19)" - Rank A

- Others:

1) InnoHealth Australia AWARD (2017-2019), April 2018

Class-level Obfuscation for Android Apps Based on Class Liveness Analysis

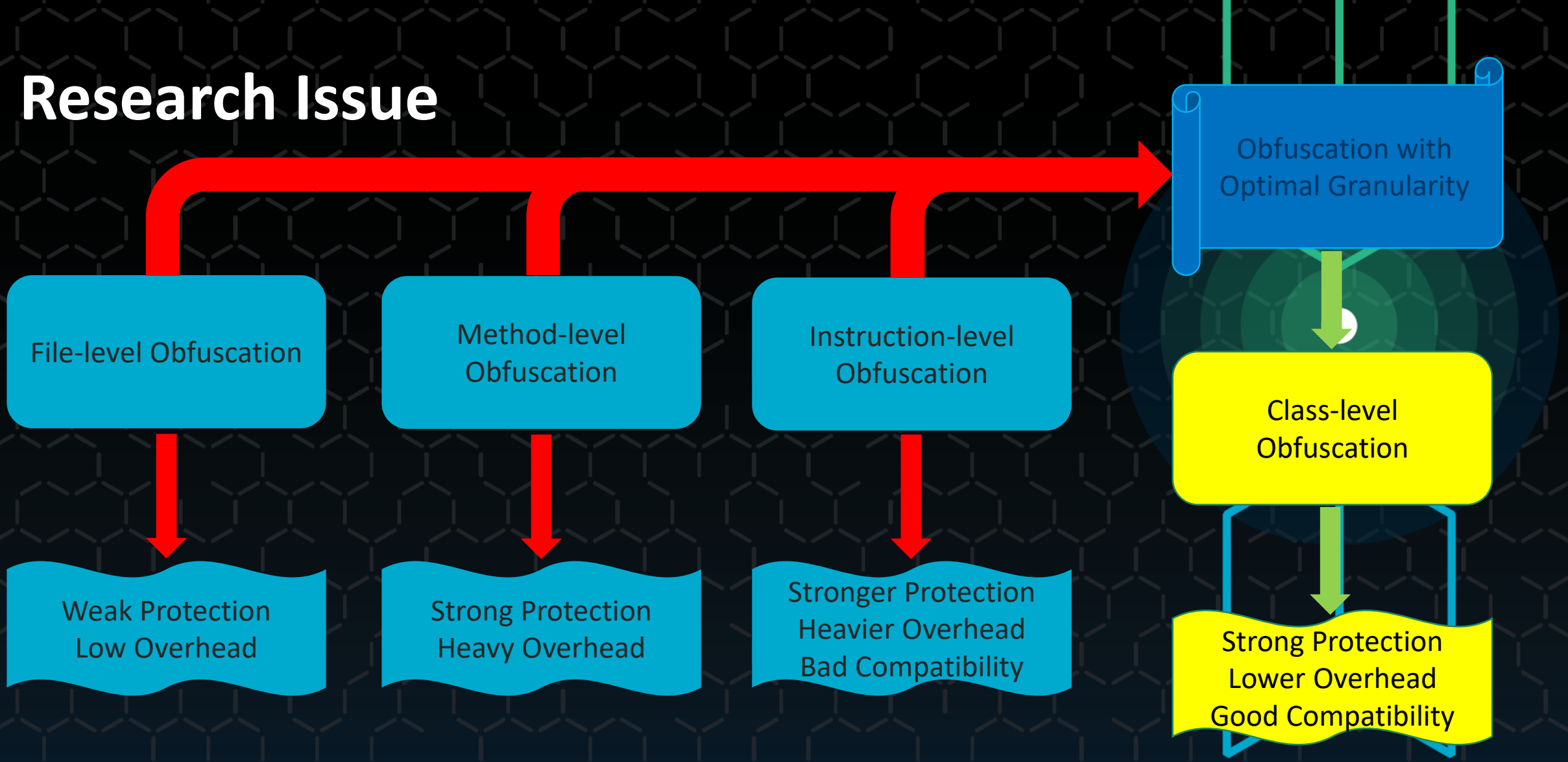
Yueqian Zhang, UNSW, Data 61

Supervisors: Prof. Jingling Xue, UNSW

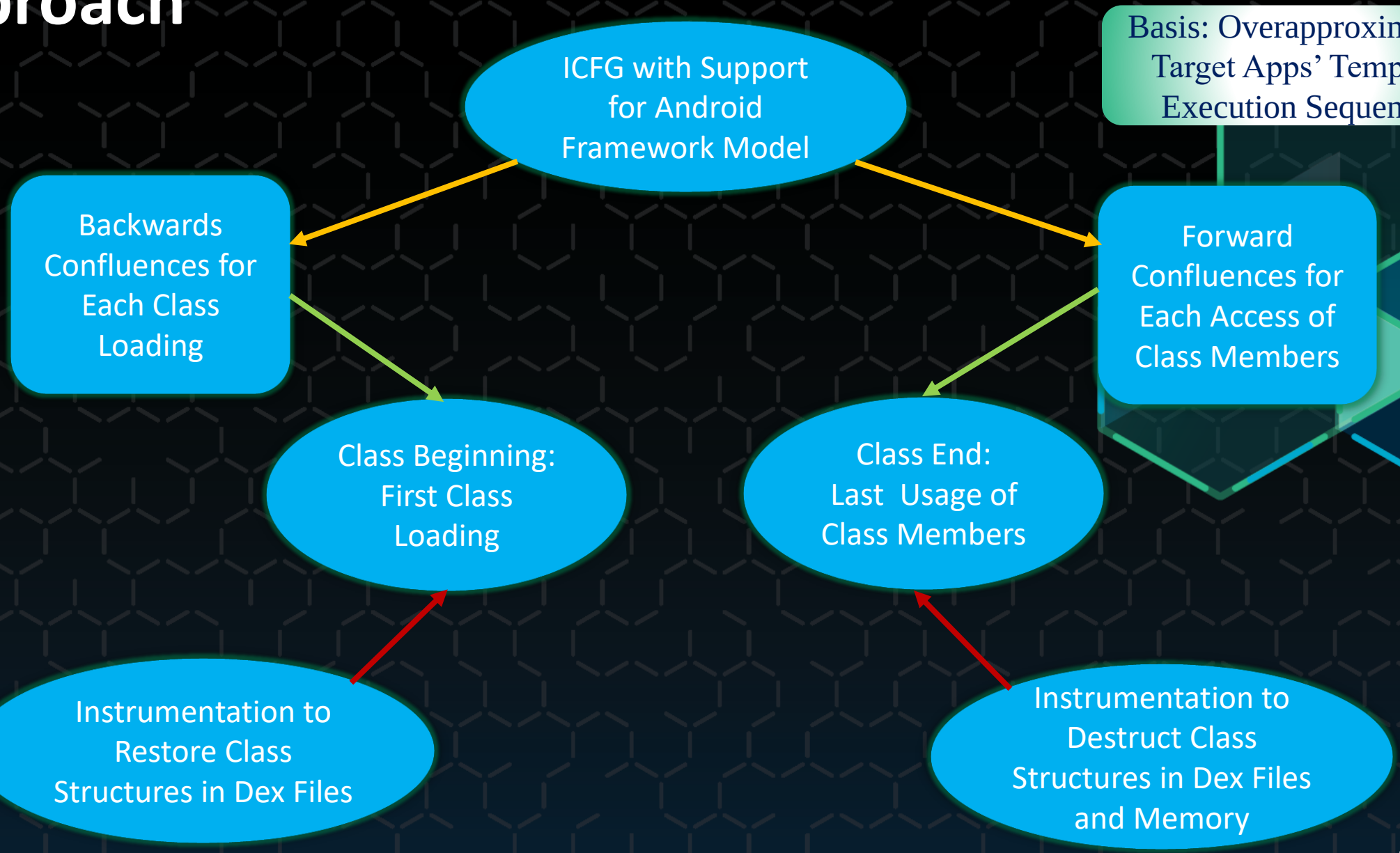
Dr. Shipping Chen, Data 61

UNSW SYDNEY

Research Issue



Approach


ICFG with Support for Android Framework Model
Basis: Overapproximating Target Apps' Temporal Execution Sequences
Backwards Confluences for Each Class Loading
Forward Confluences for Each Access of Class Members
Class Beginning: First Class Loading
Class End: Last Usage of Class Members
Instrumentation to Restore Class Structures in Dex Files
Instrumentation to Destruct Class Structures in Dex Files and Memory

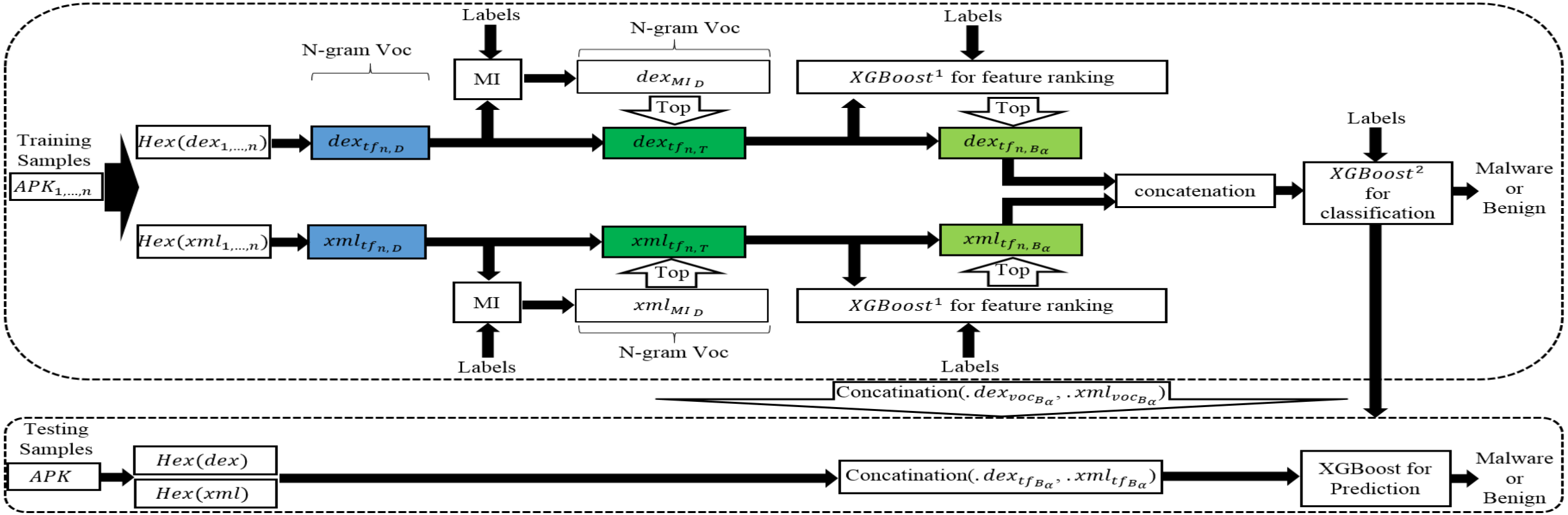
MIFIBoost: a Tool for Android Malware Detection and Family Identification

Presented by: Mahmood Yousefi-Azar

Supervision Committee: Len Hamey, Vijay Varadharajan, Shiping Chen

MIFIBoost

- Static Analysis; Byte n-grams
- No reverse engineering
- Resilient to Obfuscation



Evaluation Results and Outcomes

Comparison with state-of-the-art methods

Dataset	Technique	FNR	f1-score	FPR
Drebin	MIFIBoost	**0.68**%(±**0.19**%)	**99.06**%(±**0.18**%)	**1.21**%
	MAMADROID [9]	3.00%	96.00%	–
	Grosse et al. [68]	6.37%	–	3.96%
	Zhang et al. [56]	6.00%	–	7.90%
DexShare	MIFIBoost	**1.21**%(±**0.16**%)	**98.87**%(±**0.11**%)	**1.05**%
	MalPat [165]	–	98.24%	–
	Malytics [18]	4.72%	95.96%	3.30%
AMD	MIFIBoost	**0.35**%(±**0.03**%)	**99.62**%(±**0.02**%)	**0.41**%
	Li et al. [173]	0.80%	99.28%	0.93%

The FNR of MIFIBoost comparison with state-of-the-art methods, PRAGuard dataset (obfuscated samples)

Technique	Features	Tri+SE	Tri+SE +Ref	Tri+SE Ref+CE	Tri	SE	REF	CE	Average
MIFIBoost	.dex+.xml n-grams	**2.08**%	**2.96**%	2.08%	**1.60**%	**2.16**%	**1.44**%	2.40%	**2.10**%
MI+XGBoost	.dex+.xml n-grams	2.96%	5.52%	2.80%	2.24%	2.48%	1.60%	5.04%	3.23%
Sen et al. [132]	CoAV-1	5.76%	5.76%	1.15%	6.10%	6.10%	6.10%	**1.15**%	4.59%
Sen et al. [132]	CoAV-2	3.45%	3.62%	**0**%	3.45%	3.54%	3.45%	6.91%	3.48%
Vendors [174]	Signature	59.00%	57.70%	61.50%	9.00%	11.50%	2.00%	34.50%	33.6%
DroidSieve [3]	Static features	–	–	–	–	–	–	–	7.62%
DroidCat [2]	Dynamic features	–	–	–	–	–	–	–	3.31%
AndrODet [133]	Static features	–	–	–	7.89%	18.59%	–	–	–

- M Yousefi-Azar, L Hamey, V Varadharajan, S Chen, "MIFIBoost: Automatic Byte N-gram Feature Re-ranker for Android Malware Detection" IEEE Transactions on Information Forensics and Security (TIFS), 2018. (Under revision)

STRIVE - Security and Trust in Virtualized Environments

Hagen Lauer (PhD student at Monash University)

Supervisors:

A/Prof. Dr. Carsten Rudolph (Monash University)

Dr. Surya Nepal (Data61)

www.data61.csiro.au

MONASH University

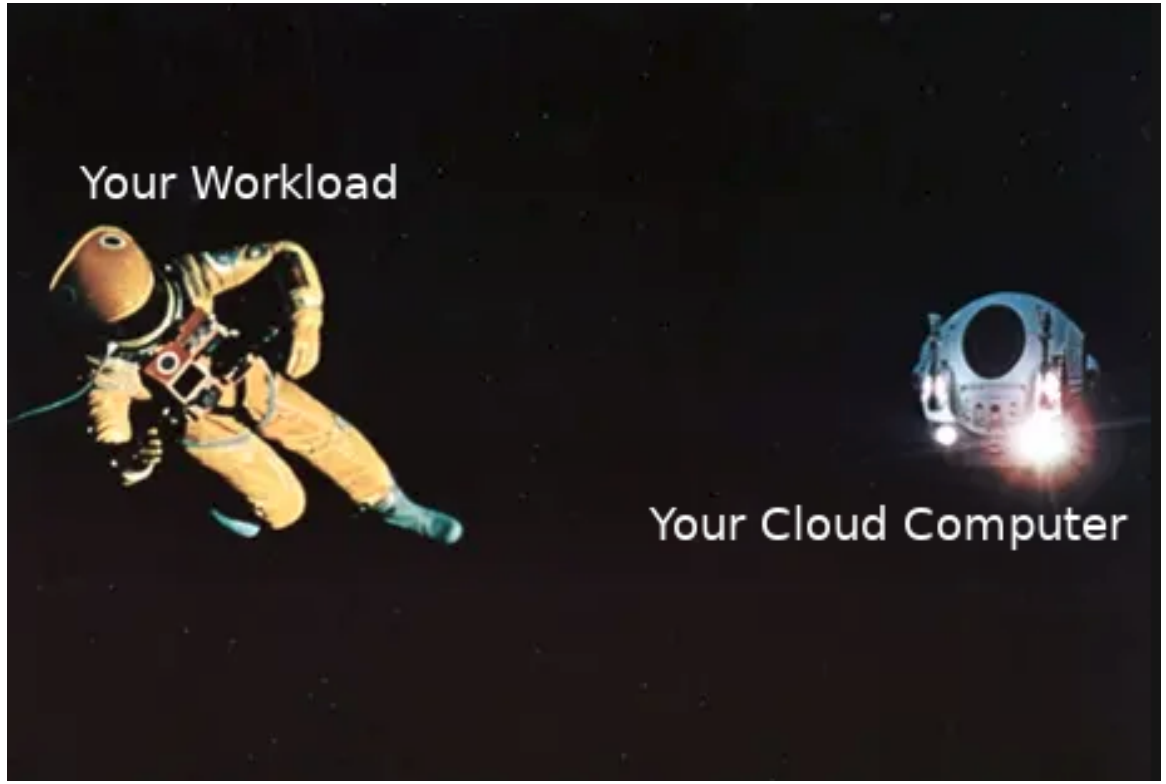
An overview and contribution

„An entity can be trusted if it always behaves in the expected manner for the intended purpose.” - TCG

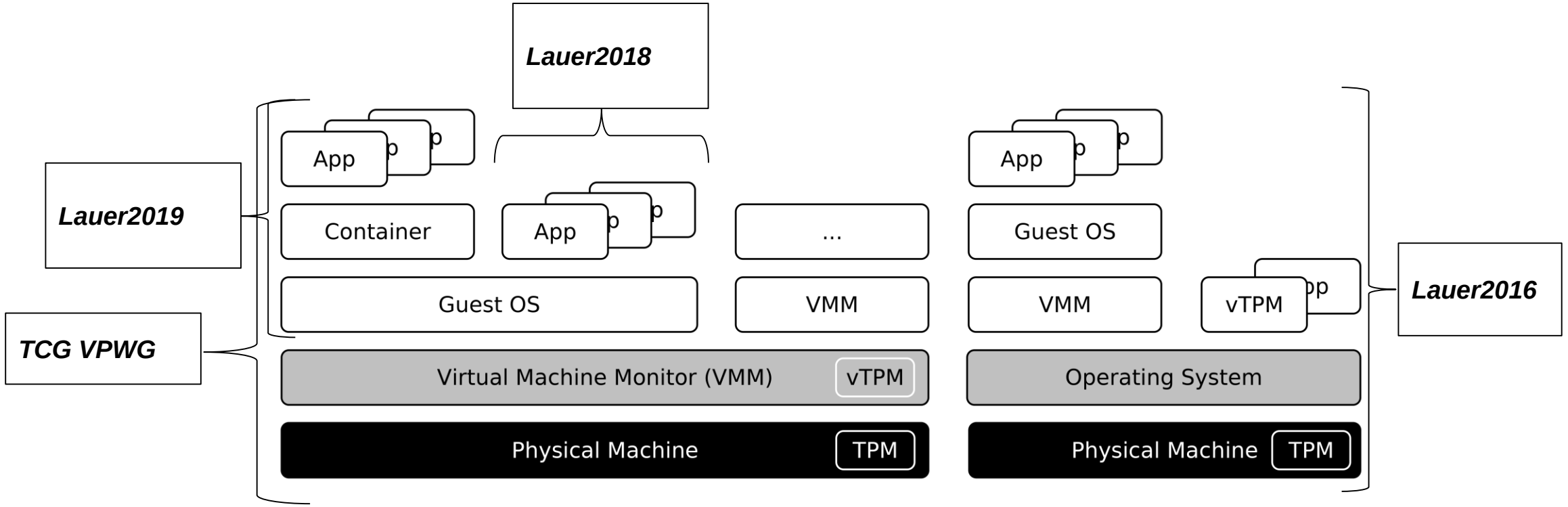
→ Let’s *report the integrity* of the computing stack.

Contribution:

- ❑ Prove to remote party what software is loaded on a host system.
- ❑ System may use only mutually *trusted* hardware and software as roots of trust.
- ❑ Design and formally verify a trustworthy integrity measurement architecture.
- ❑ Formally specify properties of secure and trustworthy virtualization systems.



Publications



For details, please visit:
https://hagenlauer.github.io