



Te Roopu Owhiti

Cybersecurity Research Group



VICTORIA UNIVERSITY OF
WELLINGTON
TE HERENGA WAKA

Te Roopu Owhiti Cybersecurity Research Group

Associate Professor Ian Welch
Te Herenga Waka – Victoria University
of Wellington
2025



BE Honours (CYBR major)

Year 1

Cybersecurity
Fundamentals

Engineering courses

Mathematics
courses

Programming
courses

Year 2

Code Security

Programming
courses

Networking courses

Year 3

Applied
Cryptography

System and
Network Security

Governance,
Compliance and
Risk

Group project

Year 4

Cybercrime
Investigation

Malware Analysis

Attack and Defence
Techniques

Individual Project

Extracurriculars



Congratulations to the NZCSC24 Winners!

Grand Prize Winner: Jamie McClymont and Thomas Hobson

VUW Alumni!!!



THE 15TH
INTERNATIONAL
CYBERSECURITY
AND GENERATIVE
AI COMPETITION
(CyberAI Cup 2024)

Organised by us!!



#whoami

- Paraparaumu College – wanted to be *astrophysicist*
- BCom (VUW) – wanted to *chartered accountant*
- Worked in industry “big 4” and government
- MSc and PhD (Newcastle-upon-Tyne)
 - Formal methods (petrinets)
 - Metaobject programming (reflection for Java)
- Senior research associate @ Centre for Software Reliability
 - Intrusion-tolerant middleware using byzantine fault tolerant group communications (*MAFTIA*)
 - Structured handling of online interface upgrades (*DSoS*)

Te Roopu Owhiti

- Research, teaching, technical staff
- Dedicated security lab for network experiments
- Teaching environment for penetration testing, forensics etc.



PhD students (2025)

Graduating

- Lisa Patterson, “Data Privacy and Security: Investigating Safety of Internet Technologies for Non-Technical Users” with Dr Sue Chard, Dr Bryan Ng
- Maryam var Naseri, “AI-Driven Adaptive Honeypots Using Markov Decision Processes”

Confirmed

- Abdullah Mamum, “APT Detection using Machine Learning” with Dr Harith Al-Sahaf
- Dedy Hendro, “Explainable AI in cybersecurity” with A/Prof Yi Mei
- Paul Dagger, “Solving Trusted Execution Requirements at the IoT Edge” with A/Prof Kris Bubendorfer
- Jamey Hepi, “Classification of Aotearoa Taonga species” with A/Prof Yi Mei and Dr Kevin Shedlock

Writing proposal

- Jay Nowitz, “Operationalising Māori Data Governance Principles” with Dr Kevin Shedlock
- Luke Pearson, “Improving Triage in Incident Response” with Dr Simon McCallum
- Andy Prow, “Digital Safety – Beyond Security” with Dr Andreas Drechsler
- Ibnul Arnub, “Lightweight Framework for Multi-Modal Attack Detection, Prevention and Monitoring in Autonomous Vehicles”

Incoming

- Grace Ngeheim, “Cultural Factors in Cybersecurity Behaviour” with Dr Kevin Shedlock
- Meremine Auelua, “Developing CSIRTs for Pacific Nations” with Dr Kevin Shedlock

Project funding

- Development of a community informatics centre for Pasifika peoples (*Department of Internal Affairs, 2005-2008*)
- Play it again – a playable archive of Australasian games (*Australian Research Council, 2009-2012*)
- Establishment of software defined networking research centre (*Google, 2015-2018*)
- Survey of opportunities and threats for Agricultural IoT in New Zealand (*Cisco, 2018*)
- Catalyst Cybersecurity Research Programme (*Ministry of Business and Innovation, 2019-2023*)
- Development of online microcredential for security (*Cisco, 2021-2022*)
- Community engagement for protection of digital taonga (*Ministry of Culture and Heritage, 2022-2023*)
- Catalyst grant supporting Japan-New Zealand research for vehicle safety (*MBIE, 2023-2025*)

Current research topics

- Deception technologies
- Situational awareness for defenders
- Human-centred security
- Māori data governance

Deception Technologies

- Honeypots are decoy systems for studying attackers
 - **simulate** real production systems
 - **record** attackers' interaction
 - **carefully controlled and monitored** environment.
- We have built or extended tools for client side and server side honeypots.
 - **Capture-HPC** (Windows) – MITRE, NL and Polish CERTs
 - **YALIH** low interaction honeypot (cross platform)
 - **Cowrie** ssh honeypot – contributed code back to project

Situational awareness

- Understanding attacks helps defenders but doesn't support automation of response.
- Machine learning allows binary and multiclass classification to provide situational awareness (knowledge).
- More recently – organisational issues:
 - How to triage alerts
 - Standing up CSIRTS in ways that work with the communicat

Human-centered Security

- “People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems.” (*Secrets and Lies: Digital Security in a Networked World*, Bruce Schneier, 2000)
- ... This is user blaming and neglects human superiority in detecting attacks (*In Defence of the Human Factor*, *Frontiers of Psychology*, Ciarán Mc Mahon, 2020)

***Reality is somewhere in between these two poles
we want to encourage good behaviours &
build more usable systems***

Māori Data Governance

- Māori have digital taonga
 - Waitata
 - Oral histories
 - Drone data
- Want control over their data
- Ongoing research into
 - Infrastructure
 - Reflecting Māori culture in user interfaces
 - Expressing cultural constraints



Thank you and questions



Prior research topics

- Software defined networking for traffic management and security (*with Dr Bryan Ng and Trung Truong*)
- Trustworthy and privacy preserving decentralised auction systems (*with A/Prof Kris Bubendorfer*)
- Privacy preserving and verifiable digital provenance for digital items and services (*with Dr Ben Palmer & A/Prof Kris Bubendorfer*)