Tom Mahoney

+61 4 3979 5026 **|** hello@toru173.com **|** https://www.github.com/toru173
https://www.linkedin.com/in/thomas-mahoney-a64b4244/

Professional Summary

I am a highly motivated cybersecurity professional with a strong focus on application security. I am dedicated to constructing robust security infrastructure and thrive in a fast-paced learning environment. I actively keep myself updated on the latest trends and best practices through continuous education and active participation in community security events and conferences. My collaboration and communication skills are exceptional, allowing me to work closely with others to identify vulnerabilities, develop effective mitigation strategies, and provide ongoing support.

Skill Summary

- Proficient in multiple programming languages. Most proficient in Python, but familiar with C and object-oriented C-like languages such as C++, C#, and Swift. Familiar with other languages such as Java, XML, shell scripting, assembly and hardware description (Verilog/VHDL) languages
- Experience in debugging, auditing, disassembling, and reverse-engineering software products including analysing undocumented behaviour from published source code.
- Experience in analysing software and embedded vulnerabilities, including testing in lab-based environments.
- Experience in reverse-engineering hardware devices to facilitate the above, include protocol analyses and decryption.
- Exceptional research and documentation skills

Education and Qualifications

- Master of Information Technology (Cybersecurity and Networks), Queensland University of Technology, GPA 6.7 of 7.0
- Bachelor of Engineering (Mechatronics), The University of Queensland, graduated 2010
- Apple Certified Macintosh Technician (ACMT)
- Apple Certified iOS Technician (ACiT)

Key Academic Achievements:

Cybersecurity Live Fire Exercise (August–November 2019):

- Developed a working knowledge of ESXi and built a model of an SMB/Enterprise network including services such as DHCP, DNS, LDAP, Email, Web Services, VNC, VPN, IDS, SNMP etc.
- Gained hands-on experience with infrastructure routing protocols like BGP and OSPF.
- Demonstrated skills in hardening virtual devices against attacks and successfully withstood intrusion during the live-fire exercise.
- Conducted successful attacks on two other competing networks, showcasing offensive cybersecurity skills.

Reverse Engineering Project (February–June 2019):

- Commissioned industrial control equipment using Modbus and similar protocols with no documentation, demonstrating problem-solving and reverse engineering abilities.
- Gained experience with virtual machine products and disk image formats, valuable for understanding virtualized environments and forensic system analysis.
- Researched and documented packet injection attacks targeting embedded Modbus controllers, showcasing a deep understanding of cybersecurity threats.

Multi-day Capture the Flag Event (October–November 2017):

- Developed a working knowledge of SQL syntax and usage, essential for database security and penetration testing.
- Successfully identified five of the seven total flags found by the team, demonstrating analytical and problem-solving skills.
- Weaponised CVE code to execute a privilege escalation attack and performed penetration testing using tools like Metasploit and nmap.
- Leveraged macOS as a penetration testing platform, highlighting versatility in operating systems and security tools.

Employment History

Continued Professional Development (December 2022 – Current):

I have used this opportunity to grow my network in the Brisbane Cybersecurity community and continue my personal projects to learn new skills and techniques.

Information Systems and Technology Career Experience at *Apple Pty. Ltd.* (June 2021 - November 2021):

- Ported an iOS proof-of-concept software project to macOS, demonstrating adaptability and cross-platform development skills.
- Conducted an InfoSec analysis of the existing project code, identifying potential vulnerabilities and suggesting improvements.
- Developed a novel technique using Wi-Fi signal strength trilateration and probabilistic algorithms to locate users with a goal to enhance user experience in office environments.
- Collaborated with cross-functional teams across APAC, EMEIA, and AMR, presenting project findings to Senior Director-level stakeholders.

Genius at *Apple Pty. Ltd.* (July 2015 – December 2022):

- Provided expert-level hardware repairs and support for desktop, portable, and mobile devices, including iPhone, iPad, and iPod, earning accolades for exceptional customer service and technical expertise.
- Managed and maintained installation and update images for client devices, streamlining the deployment process and reducing downtime.
- Collaborated with internal teams to troubleshoot emerging technical issues, resulting in faster resolution times and increased customer satisfaction.

Personal Interests:

I maintain an active GitHub repository where I explore projects from the embedded design and cybersecurity space. Some of my recent projects are listed below:

Blank-App (private repository):

> This project is a macOS application development template that utilizes Make instead of Xcode for building the app. The repository provides a structure to create a macOS application or installer by running the included Makefile. Although not the conventional approach, this project offers a workaround for building an app outside of the Xcode ecosystem and using GNU-standard tools. The application (and installers) produced successfully pass Apple's application signing requirements, and the project was used to create a small Apple-internal configuration utility for use by teams uncomfortable with using the command line.

pkg2pkgdmg (https://github.com/toru173/pkg2pkgdmg):

> The pkg2pkgdmg project provides a tool that converts a pkg (xar) file with an internal disk image into a hybrid file containing features of both. The resulting pkgdmg file can function as both a macOS disk image (.dmg) and an installer package (.pkg), depending on the file extension. The tool allows optional signing of the pkgdmg file, making it suitable for secure installation. Editing and repackaging the pkgdmg becomes straightforward, ensuring the duality of the file remains intact throughout the editing process. This script was created by binary analysis of a pkgdmg file and reverse engineering the data structures for both file types.

Arcadyan Telnet Project (private repository):

> Although this is a current work-in-progress the goal is to enable Telnet on the Telstra Smart Modem Gen 2 as a way for users to gain more control over their devices. This has been done for the Technicolor DJA0231, but not for the externally identical Arcadyan LH1000. As it stands the script can remotely initiate a reboot of the router by logging in using hashed credentials, matching the encryption algorithms on the device found by analysing the login script and http packets sent between client and router. If able to successfully log in the script sends the reboot command, and the router is rebooted. I intend to use this to fuzz user input to see if any user-controllable strings are not correctly sanitised and thus achieve remote code execution.

Outside of cybersecurity I am naturally curious – I love to learn new information in any domain, and I particularly love learning about new ingredients or cooking techniques. I'm most at home either in front of my computer or in front of my stove.

My favourite book is 'Cryptonomican' by Neal Stephenson, and I will happily rewatch the movie 'Hackers' repeatedly. These combined have inspired me to pursue a career in cybersecurity.