

I am a Security Engineer at BShield and Verichains, before that I was an active CTF player in team Efians focusing on Reverse Engineering. Throughout the years I have been involved in many projects surrounding compilers, binary analysis, memory forensics. My main focus have always been solutions for binaries security. In the future, I want to explore new research areas surrounding Formal Methods, Symbolic Execution, Type Theory, Operational Semantic as well as keeping myself updated on Compiler and Decompiler Technologies and Binary Analysis.

- Skillful in x86_64/arm binary reverse engineering
- Broad understanding of Windows kernel and Apple system
- Proven track record in national and international security competitions
- Experienced with LLVM Passes and compiler internal

EDUCATION

Bachelor of Engineering, Computer Science

University of Technology, Ho Chi Minh City, Vietnam

2016 — 2020

GPA: 7.56 / 10

RESEARCH

TSSHOCK

2023

At Verichains, our team discovered multiple weaknesses in most implementations of Threshold ECDSA Signature Scheme following the works of [Gennaro and Goldfeder](#). As the result, we presented our findings at [Black Hat USA 2023](#) and [Hack In the Box Phuket 2023](#) titled [TSSHOCK: Breaking MPC Wallets and Digital Custodians for \\$BILLION\\$ Profit](#). We also published a webpage containing all relevant information at [verichains.io/tsshock](#).

Vietnam Citizen Card Security

2023

Vietnam distributed NFC Citizen Card since 2021 and not thoroughly audited. At BShield, we took the initiative and started auditing multiple applications and Hardware devices verifying the Citizen Card.

- Research Citizen Card protocols following [ICAO 9303](#).
- Simulate NFC protocols and detect flaws in applications verifying Citizen Cards.
- Found and reported multiple vulnerabilities in the Government Application ([VNeID](#)) and Government Hardware devices.

Mach-O binary obfuscation and analysis

2020 — 2021 and 2023

Research Apple binary format and Apple's linker [dyld](#) to modify Mach-O binaries without breaking run-time behavior. Started in 2020, I found multiple ways of scrambling the Mach-O binary format without affecting the run-time. Due to task priority, I took a break from this research and come back in 2023 to finalized my unfinished ideas.

- Reverse iOS applications, automate debugging in iOS applications using [Frida](#), injecting code to iOS binary application.
- Published a series of [blog posts](#) about the project.
- Having comprehensive knowledge of Apple's [dyld](#) loader and [Objective-C runtime](#).
- Developed a method hooking framework based on dynamic symbols resolution.
- Effective obfuscation by manipulating the Mach-O binary format and the in memory binary loading process.
- Complete removal of dynamic symbols in a Mach-O binary while maintaining the execution and persistent to binary recovery through memory extraction.

Compilation-based obfuscation using LLVM

2021

- Study and research common and novel obfuscation methods ([Control-flow flattening](#), [Mixed-Boolean Arithmetic](#), ...)
- Instead of white-box approach at source-code level obfuscation such as [Tigress](#), my work applied [LLVM](#) passes to obfuscate compiled binary as inspired from [Obfuscator-LLVM](#).
- Produce obfuscated binary codes for C/C++/Objective-C language with little to no errors. Limited obfuscation support for Golang through [gollvm](#) and Rust language. Webassembly can also be targeted using [Emscripten](#).
- The obfuscator is used to generate a [CTF challenge](#) in TetCTF 2022.

Windows Memory Forensics

2019 — 2020

As part of my bachelor dissertation: "Windows Memory Forensics: Finding hidden processes in a running machine".

- Gather system information without querying APIs by searching kernel memory for process footprints and kernel-structures.
- Research common techniques in memory forensics and proficient in [Volatility3](#). E.g, find open files and network connections.
- Study Windows kernel driver development. Experienced in [WinDbg](#) debugger for User and Kernel processes.
- Outcome: Kernel level [driver](#) with user-space [command line interface](#). [Dissertation Link](#).
- The work is extended in 2023 by [Dung](#) to search for injected processes for his thesis dissertation which I am the advisor.

EXPERIENCE

Security Engineer

Sep 2019 — Present

BShield and Verichains, VNG Corp

Vietnam

I started at BShield in 2019 as an Intern and now I am a Security Engineer at both BShield and Verichains working on Security Research with occasional audit and exploitation research.

BShield is founded (and funded) in VNG. In 2022, VNG acquired Verichains and put both teams under one leader. Because of my versatility and broad knowledge across multiple fields, I have been given the opportunities to work on both teams' projects.

BShield is now re-branded as part of Verichains in 2023.

- Thorough research in iOS Application Security methodology. Mostly through binary modifications to hinder analysis.
- Extensive research and implement an in-house compiler with obfuscation using [LLVM](#) to deliver obfuscation to any C/C++/Objective-C/Go/Rust projects.
- Audited multiple projects across different areas including Mobile Application, Smart Contract, Blockchain architecture, NFC, etc.
- Audited Zero Knowledge Proof (ZKP) technology and projects using ZKP.
- Audited Vietnam Citizen Card system, including its protocols, architectural design, and Government applications/hardware devices.

Malware Analyst (Intern)

Jun 2019 — Aug 2019

Viettel Cyber Security

Vietnam

Performed practical binary reversing and analysis with real-world malware.

SKILLS

Programming Languages

C/C++/Obj-C, Javascript, Python, Golang, Rust, Haskell

Assembly Languages

Intel x86/64, ARM

Tools

[Binary Ninja](#), [LLDB Scripting](#), [z3-solver](#), [Volatility3](#), [WinDbg](#), [Frida](#)

Languages

Vietnamese, English, Japanese, Chinese, Korean

AWARDS & HONORS

As a dedicated member of Efiens, I actively engaged in international competitions, with a focus on Capture The Flag (CTF) challenges. Here are some of the notable achievements I attained alongside my teams:

Year	Competition	Prize
2021	Google Capture The Flag (Team vh++)	19 th
2020	Google Capture The Flag (Team pwnPHOfun)	11 th
2020	International Olympiad in Cryptography (Team vanthanh9c001, luibo , __D)	Team Prize 2 nd
2019	ASEAN Student Contest on Information Security	Finalist
2019	VIETTEL MATES CTF	2 nd
2018	ASEAN Student Contest on Information Security Qualify Round	3 rd
2018	VIETTEL MATES CTF	Finalist
2018	VNPT SecAthon	3 rd

SERVICE

Efiens Cyber Security Club Former Leader

2019 — 2020

Efiens is a highly advanced student group in Reverse Engineering, Cryptography, Pwning and Web Exploitation. See our [competition achievement](#). Our members are Flare-on, Olympiad in Cryptography winners, and National cyber security competition winners.

Bachelor Thesis Advisor

I am entrusted by Dr. [Khuong Nguyen-An](#) to be an advisor for his students' bachelor thesis.

- Vo Van Tien Dung, 2023, [Windows Memory Forensics: Detecting hidden injected code in a process](#).

TALKS

TSSHOCK: Breaking MPC Wallets and Digital Custodians for \$BILLION\$ Profit

Authors: Duy Hieu Nguyen, Anh Khoa Nguyen, Huu Giap Nguyen, Thanh Nguyen, Anh Quynh Nguyen

At [Black Hat USA 2023](#) and [Hack In the Box Phuket 2023](#)

[\[website\]](#)[\[whitepaper\]](#) [\[slides\]](#) [\[code\]](#)

REFERENCES

Khuong Nguyen-An, PhD

Researcher and Lecturer at Ho Chi Minh University of Technology

Email: nakhuong@hcmut.edu.vn

[[Scholar](#)] [[dblp](#)] [[LinkedIn](#)]

Thanh Nguyen

Vice President, CTO at VNG, Co-Founder at Verichains and Polaris Infosec, Co-Founder of VNSecurity

Email: thanh@verichains.io

[[LinkedIn](#)]

Anh Quynh Nguyen, PhD

Principal Research Fellow at Nanyang Technological University, Co-Founder of Verichains, Creator of [Capstone](#) and [Unicorn](#)

Email: aqnguyen@ntu.edu.sg

[[dblp](#)] [[LinkedIn](#)]