



# ANH KHOA NGUYEN

Security Engineer



 nganhkhoa.com

 ng.akhoa98@gmail.com

 (+84) 0975991198

 github.com/nganhkhoa

 Vietnam

 LinkedIn  twitter

## SUMMARY

I have expertise in Computer Systems, especially at the intersection of computing and security. My background includes various security principles, with a focus on binary analysis.

I want to explore new research areas in computer systems, both practical and theoretical. Practical through building tools; Theoretical through building foundations in computation.

## SKILLS

**Programming:** C, C++, Python, Javascript, Golang, Rust

**Technologies:** Linux, Docker, LLVM

**Languages:**

<b>Vietnamese</b>	Native	
<b>English</b>	IELTS 7.5	(C1)
<b>Japanese</b>	JLPT N2	(B2)

## EDUCATION

2016 - 2020 **Bachelor of Engineering, Computer Science** Ho Chi Minh University of Technology

## PROJECTS

Cryptography 2023 **TSShock: Private key recovery for libraries implementing Threshold ECDSA based on GG18** tsshock

- Implemented attacks in multiple libraries implementing GG18
- Perform brute-force search in parallel using CUDA
- A basic understanding of multiparty computation (MPC) and Zero-Knowledge Proofs (ZKP)

NFC security 2023 **Vietnam Citizen Card security audits**

- In-depth understanding of the ICAO 9303 protocol and PACE protocol
- Simulate the protocol for testing of software and hardware
- Create counterfeit cards through simulation
- Bypass security of multiple software and hardware

Obfuscation 2019-2023 **Simulating Loader for Mach-O Binary Obfuscation and Hooking** preprint

- Thorough understanding of the Mach-O binary format, the loader dyld and Objective-C runtime
- Understand basic and advanced Mach-O obfuscation techniques
- Created a new method for API obfuscation in Mach-O binaries

Obfuscation 2021-2022 **Source code obfuscation using LLVM**

- Use Obfuscator-LLVM
- Update obfuscation passes to LLVM 14 and port them to New Pass Manager
- Integrated with Golang using gollvm, Web Assembly using emscripten, and Rust

Memory Forensics 2019-2023 **Live memory forensics without memory extraction** dissertation / preprint

- Understand Windows memory model
- Familiar with memory forensic techniques and malware techniques
- Apply memory forensics directly on virtual memory through a kernel driver
- Controlling of kernel drivers using IOCTL with a user space process
- Implemented and modified Pool Tag Quick Scanning to run in virtual memory

## RELEVANT EXPERIENCES

9/2019 – Present **Security Engineer** BShield - Verichains, VNG

- Mobile security for iOS devices
  - Code obfuscation using LLVM
  - Code obfuscation for Mach-O binary
  - Performed audits for Vietnam Citizen Card
  - Performed audits for blockchain projects
  - Performed audits for cryptographic libraries
- BShield / BShield Secure-ID / TSShock

6/2019 – 8/2019 **Malware analyst intern** Viettel Cyber Security

- Malware analysis
- Malware removal and prevention

## AWARDS AND HONORS

---

I usually participated in Capture the Flag (CTF) competitions during my undergraduate years. Below is the list of competitions I participated in with members of my university club or with the Vietnamese security community.

2021	<b>Google Capture The Flag (Team)</b>	19 <sup>th</sup>
2020	<b>Google Capture The Flag (Team)</b>	11 <sup>th</sup>
2020	<b>International Olympiad in Cryptography (Team)</b>	2 <sup>nd</sup> <b>Prize</b>
2019	<b>ASEAN Student Contest on Information Security (Team)</b>	<b>Finalist</b>
2019	<b>VIETTEL MATES CTF (Team)</b>	2 <sup>nd</sup>
2018	<b>ASEAN Student Contest on Information Security Qualify Round (Team)</b>	3 <sup>rd</sup>
2018	<b>VIETTEL MATES CTF (Team)</b>	<b>Finalist</b>
2018	<b>VNPT SecAthon (Team)</b>	3 <sup>rd</sup>

## SERVICES

---

2019 - 2020	<b>Efiens Cyber Security Club Former Leader</b> 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.
2022 - Present	<b>Bachelor's thesis co-advisor</b> My former advisor, Dr. Khuong Nguyen-An, invites me to be a co-advisor for his students' bachelor's thesis. <ul style="list-style-type: none"><li>• Vo Van Tien Dung, 2022 - 2023, Windows Memory Forensics: Detecting hidden injected code in a process</li><li>• Do Dinh Phu Quy, 2023 - 2024, Sandboxing Powershell scripts for ransomware detection</li></ul>

## TALKS

---

Black Hat USA 2023	<b>TSSHOCK: Breaking MPC Wallets and Digital Custodians for \$BILLION\$ Profit</b> <small>conference / video</small> Duy Hieu Nguyen, <b>Anh Khoa Nguyen</b> , Huu Giap Nguyen, Thanh Nguyen, Anh Quynh Nguyen
Hack In The Box Phuket 2023	<b>TSSHOCK: Breaking MPC Wallets and Digital Custodians for \$BILLION\$ Profit</b> <small>conference / video</small> Duy Hieu Nguyen, <b>Anh Khoa Nguyen</b> , Huu Giap Nguyen, Thanh Nguyen, Anh Quynh Nguyen

## PUBLICATIONS

---

Preprint	<b>Simulating Loader for Mach-O Binary Obfuscation and Hooking</b> <small>pdf</small> <b>Anh Khoa Nguyen</b> , Thien Nhan Nguyen
Preprint	<b>Live Memory Forensics on Virtual Memory</b> <small>pdf</small> <b>Anh Khoa Nguyen</b> , Dung Vo Van Tien, Khuong Nguyen-An
Whitepaper 2023	<b>New Key Extraction Attacks on Threshold ECDSA Implementations</b> <small>pdf</small> Duy Hieu Nguyen, <b>Anh Khoa Nguyen</b> , Huu Giap Nguyen, Thanh Nguyen, Anh Quynh Nguyen

## REFERENCES

---

VNU-HCM	<b>Khuong Nguyen-An, PhD</b> <small>nakhuong@hcmut.edu.vn</small> Faculty of Computer Science and Engineering University of Technology, VNU-HCM, Vietnam  scholar /  dblp /  LinkedIn
Verichains	<b>Thanh Nguyen</b> <small>thanh@verichains.io</small> Vice President, CTO at VNG Co-Founder at Verichains and Polaris Infosec Co-Founder of VNSecurity  LinkedIn
NTU	<b>Anh Quynh Nguyen, PhD</b> <small>aqnguyen@ntu.edu.sg</small> Principal Research Fellow at Nanyang Technological University Co-Founder of Verichains  dblp /  LinkedIn