Address: Saigon City, Vietnam

Email: cothannguyen@gmail.com

Blog: https://cothan.github.io/

Git: http://github.com/cothan/

Duc Tri Nguyen

- Former member of Defcon Ukraine Capture The Flag team, **1st** place in **CTFtime.org 2016**
- Researcher in Security / Cryptography / Computer Forensics
- Highly proficient in Cryptography, Cryptographic protocols, experiences in exploiting flaws in Protocols

Languages & Technologies

ordered by proficiency

Programming Languages:	**Python, Bash, Julia, Go, Javascript, PHP, C**
Mathematical Software:	SageMath, Mathematica, Yafu, CADO-NFS, Pari/GP, Pandas, Numpy, NetworkX, Scikit-Learn, Octave
SMT Solver:	**Z3Prover**, **Boolector**, **Angr** (Binary analysis framework), **Klee** (LLVM Execution Engine)
Skills:	**Cryptography**, **Forensic**, **Reversing**, Binary/Web Exploitation, Machine Learning, Big Data
Microcontroller Programming:	8051, PIC 16F887

Experiences

Graduate Research Assistant
August 2017 - Present
CERG, George Mason University.

Freelancer
June 2016 - Present
Profile (https://www.freelancer.com/u/cothan.html)

Operation Security Internship
VNG Corporation,
Le Dai Hanh, Ho Chi Minh City, Vietnam
December 2014 - April 2015

- Tracked and monitored security events
- Detected and responded to abnormal activities and behavior of sophisticated malware

Education

University of Technology; Ho Chi Minh City
B.S. in Computer Engineering, November 2015
Overall GPA: **7.1 / 10** | IELTS **6.5** | TOIEC **725**

Thesis: Hiding data inside PNG images with a chat & sharing multiplatform application
Thesis Defense score: **8.5 / 10** April 2015

Training & Conferences

Advanced Technologies for IoT Applications (http://rs2017.uet.vnu.edu.vn)
Ha Noi, Vietnam
March 15th - 16th 2017

Topic included: Virtual Reality, Applications in Computer Vision and NLP, IoT Communications and Networking in 5G Systems, Video Coding Technology in IoTs Era

Asiacrypt 2016 (http://www.asiacrypt2016.org/)
Ha Noi, Vietnam
December 5th - 8th 2016

IACR-SEAMS School "Cryptography: Foundations and New Directions"
(http://viasm.edu.vn/hdkh/cryptoschool2016)
Ha Noi, Vietnam
November 27th - December 4th 2016

Provided an introduction of the most important technical and theoretical aspects of modern cryptography, topics included: High-Speed Cryptography, Elliptic Curve Cryptography, Discrete Log Problem, Pollard rho Factorization, Provable Security

The current state of quantum cryptography and the future of information security
NYU Abu Dhabi, United Arab Emirates
November 13rd 2016

A short course on Quantum Key Distribution (QKD), including attacks against QKD, quantum computing, and the future of cryptography. How could current public key cryptography algorithms be broken using Shor's algorithm.

Big Data and Social Analytics Certificate course (https://www.getsmarter.com/courses/us/mit-big-data-and-social-analytics-certificate-course)
MIT Experiential Learning
August - October 2016

Topic included: living labs, viral marketing, the social fMRI approach, graph theory, cluster analysis, personal sensors, big data in industry…

CIMPA-ICTP research school on Lattices and applications to cryptography and coding theory (http://ricerca.mat.uniroma3.it/users/valerio/hochiminh16.html)
Saigon University, Ho Chi Minh City, Vietnam.
August 1st - 12th, 2016

Topics: Number theory, Lattices and Cryptography, Elliptic Curve and Cryptography.

Machine Learning (https://www.coursera.org/learn/machine-learning)
Coursera
November - December 2015

Octave software, Multivariate Linear Regression, Polynomial Regression, Gradient Descent, Cost Function, Evaluating a Hypothesis, Model selection and Train/Validation/Test Sets, Learning Curve.

Cryptography 1 (https://www.coursera.org/learn/crypto)
Coursera
January - March 2015

Discrete Probability, Birthday paradox, Attacking Linear Pseudo Random Generator, Stream Cipher, Block Cipher, Attacking modes of operation of block ciphers, Hash, MAC, HMAC, Key Exchange, Public Key Cryptography

Research & Learning

Individual exploration of current research topics, such as:

- Taking advantage of hidden subgroup to contruct backdoor in Diffie-Hellman (https://eprint.iacr.org/2016/644.pdf)
- Generating Anomalous Elliptic Curves (http://www.monnerat.info/publications/anomalous.pdf)
- Choosing safe curve for Cryptography (http://safecurves.cr.yp.to/)
- Survey of attacks against RSA (https://crypto.stanford.edu/~dabo/papers/RSA-survey.pdf)

Competitions

CTF Team Rating Overall Score *Summarized scores taking into account CTF competitions all over the world* Scoreboard (https://ctftime.org/) *2016*	**1st / DCUA**
International Students' Olympiad in Cryptography 2016 (http://www.nsucrypto.nsu.ru) *An answer to one of the problems nominated as a best solution* Russia *December 14th 2016*	3rd in Round 2 (Professionals)
CSAW 2016 Finalist NYU Abu Dhabi, United Arab Emirates *November 11-12 2016*	1st / DCUA
ASIS Final Round 2016 Iran Cyber Security Contest *September 11st 2016*	1st / DCUA
Hack in the Box Singapore Facebook, Singapore *August 2016*	4th / DCUA
Students with Cyber Security 2014 VNISA, Vietnam *November 2014*	2nd / BKIT-Respawn

Qualifications

IACR-SEAMS School 2016 Cryptography school	**CSAW 2016 Finalist Certificate** NYU Abu Dhabi
CIMPA 2016 Mathematics school	**ECSI Hacker Playground 2015** Silent Signal, Balabit IT Security National Hero Certificate
Advanced Technologies for IoT Applications UTS-VNU Research School 2017	**International Students' Olympiad in Cryptography 2016** 3rd place Diploma

Teaching

Preparing for MATESCTF (https://matesctf.org)

University of Technology

Ho Chi Minh, Vietnam September 2015 - February 2017

Taught a student team in University of Technology (called Efiens) about hacking techniques, Efiens has qualified to the final round of a national security competition organized by Viettel Cyber Security Department.

Number of rounds: ***5*** *qualification rounds +* ***1*** *final round.*

Duy Tan University

Da Nang, Vietnam

Octorber 7th - 12nd 2016

Taught a student team in Duy Tan University about basic exploitation, attacking anomalous Elliptic Curve, Z3 SMT solver, applying SMT into reverse engineering.