Manh-Dung NGUYEN

07 78 02 61 99 | Appt 68, 3 Parvis de la Bièvre, 92160 Antony, France
strongcourage.github.io | nguyenmanhdung1710@gmail.com | /strongcourage

ÉDUCATION

UNIVERSITÉ GRENOBLE ALPES
Doctorant en Sécurité des Logiciels
Nov. 2017 – Nov. 2020 (*attendu*)

UNIVERSITÉ PARIS SUD
Master 2 Professionnel en Réseaux et Télécommunications
Sept. 2013 – Sept. 2014

INSTITUT POLYTECHNIQUE DE HANOÏ (IPH)
Ingénieur en Systèmes d'Information et de Communication
Addendum au diplôme d'Ingénieur de l'Université Grenoble Alpes
Sept. 2007 - Juil. 2012

COMPÉTENCES

PROGRAMMATION
C/C++ • Python • Ocaml • Assembly • Bash • Java

OUTILS
Fuzzers: AFL • AFLGo • OSS-Fuzz • libFuzzer • honggfuzz
Rétro-ingénierie: BINSEC • IDA Pro
Débogueur: GDB • WinDbg • Immunity Debugger
Pentesting: Metasploit • Burp Suite
Systèmes d'exploitation: Kali Linux

LANGUES
Francais: Avancé (DELF B2)
Anglais: Courant
Vietnamien: Langue maternelle

PRIX

Google Android NextGen chercheurs en sécurité pour participer au Virus Bulletin'19
Bourses de voyage pour étudiants de ISSISP'18, CISPA'18 & ASE'18
Bourse d'accueil de l'Univ. Paris Sud
Bourses d'ingénieur de l'IPH

MOOC

Membre actif sur diverses plateformes de pentesting en ligne: Hack The Box, TryHackMe & Root Me
Piratage Éthique Pratique, Udemy
Élévations de Privilèges sous Windows, Udemy

CENTRES D'INTÉRÊT

Développement des exploits
Chasse aux bogues
Programmation compétitive

ÉXPERIENCE

CEA LIST | Doctorant, France (Nov. 2017 – présent)
Thèse: Techniques avancées de fuzzing pour la découverte de vulnérabilités à grande échelle • ***Superviseurs***: Sébastien Bardin & Matthieu Lemerre

- Proposer des techniques de fuzzing pour trouver efficacement des bogues *"difficile-à-détecter"* comme Use-After-Free (UAF) au niveau binaire
- Contribuer activement au développement de l'outil d'analyse au niveau du binaire BINSEC, surtout sur la partie de fuzzing et de démontage

TSUNAMI CENTRE | Assistant de recherche, Singapour (Août 2015 – Oct. 2017)

- Développer une méthode dynamique de levage du code binaire x86 en LLVM IR
- Développer une méthode de réparer automatiquement de programme sémantique
- **Airbus:** Tests de pénétration de la conception pour la sécurité du drone Skyways

NUS LABS | Stagiaire en recherche, Singapour (Sept. 2014 – Juil. 2015)

- Étudier les concepts avancés de l'exécution symbolique et l'analyse des souillures
- Implémenter des souillures dépendantes du contrôle, des flux implicites & évaluer de la structure de partitionnement sur l'environnement d'exécution fiable (TEE)

TOSHIBA | Ingénieur sécurité, Vietnam (Oct. 2013 – Sept. 2014)

- Implémenter un programme de mise à jour du firmware de TOPPERS/ATK sur la mémoire Flash des cartes de Toshiba en utilisant des algorithmes de chiffrement
- Implémenter & évaluer la bibliothèque LibTomCrypt sur les cartes de Toshiba

ORANGE LABS | Stagiaire en recherche, France (Mars 2013 – Sept. 2013)

- Étudier le TEE et proposer un framework de billetterie mobile sur le TEE utilisant le schéma de signature numérique Schnorr et des signatures partiellement aveugles
- Implémenter une application de billetterie Android sur la plateforme ST-Ericsson

PENTESTING

PROJETS OPEN SOURCE

- **AFLGo** Co-développer et entretenir le *premier* fuzzer en boîte grise à la pointe qui a été intégré dans l'OSS-Fuzz de Google. AFLGo a trouvé *39 noveaux bogues* en 2017
- **BINSEC (1)** Importer le flot de contrôle de l'IDA Pro; **(2)** Améliorer et intégrer le détecteur statique de bogues UAF GUEB dans BINSEC
- **UAFuzz (1)** Développer le *premier* fuzzer en boîte grise à la pointe pour détecter UAF au niveau binaire; **(2)** Construire un benchmark de bogues UAF pour fuzzing. UAFuzz a trouvé *11 nouveaux bogues UAF* en 2019
- **Fuzzing** Créer de collections de corpus & de programmes testés pour le fuzzing

AVIS DE SÉCURITÉ & BOGUES SIGNALÉS

- **14 CVEs** trouvés dans les programmes critiques avec mes fuzzers
- **50+ bogues open source** signalés (PHP, GNU Binutils, GNU Patch, Perl 5 ...)

COURS DE PENTESTING

- **Tests de pénétration avec Kali Linux** (Mars – Mai 2020, *en préparation de la certification OSCP*): analyse des vulnérabilités Web, élévations de privilèges sous Linux & Windows, développement des exploitations et attaques d'Active Directory
- **Virtual Hacking Labs** (Nov. 2019 – Févr. 2020): root *toutes les 43 machines*

PUBLICATIONS & EXPOSÉS

[RAID'20 – rang A] **Binary-level Directed Fuzzing for Use-After-Free Vulnerabilities**
[BlackHat USA'20] **About Directed Fuzzing and Use-After-Free: How to Find Complex & Silent Bugs?**
[RESSI'20, AFADL'20] **Exposés de ma thèse** aux journées scientifiques françaises
[ICSE'18 – rang A*] **Semantic Program Repair Using a Reference Implementation**
[CCS'17 – rang A*] **Directed Greybox Fuzzing**
[Technical Report] **Formal Security Analysis of Unmanned Aircraft Systems**