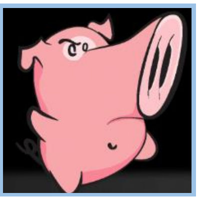
dưới chân tự có đường



Bui Van Cuong
Ngoc Son – Tu Ky – Hai Duong
Birthday: Sat/06/05/1995
Gender: Male
🏠 Chua Lang – Dong Da – Ha Noi

☎ +84985855393
✉ cuongbv765@gmail.com
Cuong Van Bui
nsbvc.blogspot.com
github.com/buivancuong

SYSTEMS

- ✓ Ubuntu, CentOS
- ✓ Windows, Windows Server
- ✓ Apache, NginX
- ✓ Docker

Hanoi University of Science and Technology
Information & Technology
KSTN – CNTT K58
SEDIC Lab

SOFTWARE TOOLS

- ✓ Microsoft Office, LaTeX
- ✓ Git
- ✓ VS Code, Jetbrain IDE
- ✓ Windows Subsystem for Linux

SYSTEM ADMINISTRATOR

- ✓ Hardening Systems: Windows Server, Linux, Apache
- ✓ IDS/IPS: Snort, Suricata
- ✓ ELK Stack

RESEARCHING

- ✓ Parallel Computing
- ✓ Interconnection Network
- ✓ DoS/DDoS Attack
- ✓ Cryptography

SOFTWARE ARCHITECTURE

- ✓ MVC, MVP, MVVP
- ✓ OOP, SOLID, Design Patterns
- ✓ MPI Programming
- ✓ RESTful API
- ✓ API Gateway

DATABASE

- ✓ Language: SQL, QBE
- ✓ MySQL, MariaDB
- ✓ SQLite, Realm (Android)
- ✓ Elasticsearch

PAPER

- ✓ An Efficient Compact Routing Scheme for Interconnection Topologies of the Random Model - SoICT Conference 2017

PROGRAMMING

- ✓ Android (Java), Java/Scala
- ✓ C/C++ (STL, Boost)
- ✓ UNIX Shell, Python
- ✓ Matlab/Octave, R
- ✓ Assembly

MACHINE LEARNING

- ✓ Domain: Generative Model (Bayesian Inference, Topic Modeling), Unsupervised Learning, Deep Learning.
- ✓ Tool: Python frameworks (pandas, scikit – learn), Deep Learning frameworks (Tensorflow, Keras), NLP frameworks (nltk, gensim, spacy)

SEDIC Lab: Security

- Position: Student.
- Defend against **DDoS attack** at **Transport Layer - OSI** with **Bloom filter**.
- Using **Suricata IDS** to defend the system.
- Studying about general of **Cryptography theory**.
- In this time around, I acquired basic knowledge about Information Security, such as **System Admin** (Linux, Firewall, IDS/IPS) and Cryptography theory (Math background of Cryptosystems and Key transfer protocols.

Cục ATTT: Security

- Position: Internship.
- Detect and Defend against **DDoS attack** at **Application Layer - OSI** with the **real-time** speed tool that I developed by C++ programming language.
- In this time around, I focused on using C++ programming language and the related libraries (**STL/Boost**) to develop 1 program that handled Web Application Log to detect DDoS attack behavior with real-time speed.

CMC InfoSec: Security

- Position: SOC Forensics.
- **Hardening** the **Linux** systems (Ubuntu Server, CentOS).
- **Network Security Monitoring** and **Incident response**.
- In this time around, I performed the works related to **operational safety** in the customer's information system. Specifically, I perform hardening the systems as well as reporting statistics (by day/ week/ month) using **automated tools** that I programmed myself based on C++ language programming. This greatly reduces the time required for these regular activities.

[2/16 – 1/17]

[2/17 – 5/18]

[7/18 – 10/18]

[7/18 – 10/18]

[10/18 – 3/19]

[4/19 - Now]

SEDIC Lab: Interconnection Network

- Position: Student.
- Scientific Research Article: “*An Efficient **Compact Routing** Scheme for **Interconnection Topologies** of the **Random Model** - SoICT Conference 2017*”
- Graduation Thesis: *Develop the **Parallel Computing** model the Routing Algorithms in* ***Interconnection Network***.
- In this time around, I focused on the simulation of **Routing** algorithms and **Graph** properties of the **Interconnection Network** that are commonly used in **Data Centers**. Our research team published the paper in that specialized and was accepted in SoICT Conference 2017 (Asia-Pacific caliber). My simulation program was developed end-to-end by myself, based on C++ language programming.

Umbala Network: Android & Back – end.

- Position: Android Developer, Backend Developer.
- On here, I studied about **Software Architecture** (MVC, MVP, MVVP), Software **Design Patterns**, **Microservices** systems, and applied them to **Android** App and Authentication policy on Live streaming protocol.
- I started blogging from this time. The blog address is https://nsbvc.blogspot.com.

CMC InfoSec: Machine Learning on Security

- Position: R&D Developer.
- Study and apply **Machine Learning** techniques to Information Security system to **Anomaly Detection**.
- In this time around, I have studied and applied Machine Learning techniques to **SIEM** systems (CMC SOC & CMC WAF), to detect abnormal events. Specifically, within 6 months, I developed and launched 2 automated modules via the **Docker** platform; successfully integrated into the CMC SOC system. 1 module detects anomalous **connection behaviors** (DNS, SSL, HTTP) using the **Topic Modeling** technique in the **Generative Model**. The other module work for forecasting and detecting anomalies in **network traffic** by using a combination of **Spare Autoencoder** architecture and **LSTM** struct of **Recurrent Neural Networks (RNN)** in **Deep Learning**, was computed on GPU.