curriculum vitæ of
Yepeng Pan

Network · Cloud · IoT · Cryptography · Security

panyepeng@gmail.com +86 182 7317 7055 Yepeng Pan

Education

Sept. 2021 – Dec. 2022 **MSc.** in information security — University College London, UK

Expected to enroll in UCL in Sept. 2021 and finish my thesis in Sept. 2022

Sept. 2016 – June 2020 **BEng.** in information security — Hunan University, China

Core courses:

- Math: advanced mathematics; linear algebra; discrete mathematics; number theory; probability theory;
- Computer Science: computer organization; computer network; operating system; data structure; digital circuit and logic Design;
- Information Security: cryptography; network security; software security;
- Weighted Average: 88.1 / 100

Research Experience

Feb. 2020 - June 2020 **Privacy preserving cloud image retrival system**

Followed up and improved a recent research about encrypted image retrival system working on the cloud that could preserve user privacy.

Brief introduction of system:

- This system used CNN and PCA-ITQ to process original pictures and exported their features as short binary strings representing original features, after which the system would use random matrix to encrypt user requests and index tree as well as use chaos scrambling to encrypt images so that the cloud server couldn't analyze user requests, retrieval process and statistical law, and as such user privacy could be protected.

Improvements:

- Improved the tree construction process, so it could generate more balanced index trees which could improve accuracy.
- Improved the retrieval process, so it would choose fewer leaf nodes and become more efficient.

Apr. 2019 - May. 2019 **Malicious traffic analysis**

Analysed suspicious traffic of common attacks and found out their features.

Suspicious Traffic Analysed:

- Traffic of DNS amplification attack
- Traffic of SYN flood attack
- Traffic of slow Dos attack

Apr. 2019 - Apr. 2019 **Attack on PUF**

PUF(physical unclonable function) is a kind of security chip that could generate unclonable output by using process variation. This projet used different machine learning models(LR, SVM, CMA-ES) to predict the output of PUF and obtain approximate result.

Apr. 2019 - Apr. 2019 **Adversarial examples**

This project cracked google inception V2 model and let it make wrong prediction by adding specific noise to image samples.

Mar. 2019 - Apr. 2019 **Layer 3 switch design**

Effectuated a switch with basic traffic forwarding function and ARP table updating function with Verilog. By evaluating the traffic (frequency and quantity of ARP packets and conflicts with original arp table) the switch could also detect potential ARP attacks.

Feb. 2019 - Mar. 2019

DNS attack simulation

Simulated different methods of DNS attacks and evaluated approaches detecting these attacks.

Attack Analysed:

- Local DNS cache poison
- DNS server cache poison
- DNS hijack based on arp spoofing

Oct. 2018 - Dec. 2018

Encryption tool development

This project implemented an encryption tool with a series of encryption algorithms, basic key exchange function and signature function.

Implemented algorithms:

- Symmetric encryption: DES, AES
- Stream cipher: RC4
- Asymmetric encryption: RSA
- Hash: SHA-1, MD5
- Key exchange: DH

Sep. 2018 - Nov. 2018

Privilege and app control plug-in for android

Implemented a plug-in of Xposed framework which could monitor all applications and control their behaviors. This plug-in could monitor/audit/block sensitive api calls related to user privacy by hooking all these apis. Blacklist and whitelist were also involved in this plug-in to help manage applications.

June 2018 - Aug. 2018

FPGA design

Implemented a series of functions with different sensors, buttons and LED display.

Implemented function list:

- Reversing radar (using ultrasonic sensor)
- IR remote control
- Coded lock
- Detector with optical sensor and thermal sensor

Dec.2017 - Jan.2018

Basic CPU implementation

Implemented a basic CPU with VHDL that could execute a series of instructions stored in the memory.

Implemented function list:

- 2-stage pipeline
- Implemented components (ALU, AGU, register, decoder, instruction cache, etc.)
- Memory read & write (mov)
- Basic arithmetic operations (add, sub, inc, cmp, imul)
- Basic logic operations (and, or, xor, not, shl, sal, shr, sar)
- Basic control operations (mov, jmp, cmp, etc.)

Work Experience

Nov. 2020 – Apr. 2021

NIO Inc — Information Security R&D Engineer

- Managed security devices (including the management of DLP, firewall, fortress machine, etc.);
- Developed terminal management application;
- Developed automation scripts;

July 2019 – Aug. 2019

Heetian Ltd — Information Security R&D Engineer

Implemented three online courses on the Heetian lab platform:

- Basic web security problems (XSS, CSRF, SQL injection and click hijack);
- Basic reverse analysis (Stack overflow vulnerabilities and existing solutions);
- C++ vulnerabilities analysis (Virtual function vulnerability, Heap vulnerabilities, Vulnerable functions);

Programming Skills

- C & C++
- VHDL & Verilog
- Python
- Go