

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
My degree programme had gave me fundamental mathematics knowledge, computer science knowledge and information security knowledge.
- Math: Advanced mathematics, linear algebra, discrete mathematics; number theory; probability theory;
 - Computer Science: computer organization; computer network; operation systems; data structure; digital circuit and logic Design;
 - Information Security: cryptography; network security; software security;
 - Weighted Average score: 88.1 / 100

RESEARCH EXPERIENCE

- Feb. 2020 - June 2020 **Privacy preserving cloud image retrieval system**
Followed and improved a recent research about encrypted image retrieval 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 which cloud represent original features. Then the system would use random matrix to encrypt user request and index tree, use chaos scrambling to encrypt images so the cloud server couldn't analyse user requests, retrieval process and statistical law, hence it could protect user privacy.
- 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 achieve better efficiency.
- 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 get 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**
Implemented a switch with basic traffic forwarding function and ARP table updating function with Verilog. By evaluating the traffic (frequency and quantity of ARP packets, conflicts with original arp table) the switch could also detect potential ARP attacks.

Feb. 2019 - Mar. 2019	<p>DNS attack simulation</p> <p>Simulated different methods of DNS attacks and evaluted ways to detect these attacks.</p> <p>Attack Analysed:</p> <ul style="list-style-type: none"> • local DNS cache poison • DNS server cache poison • DNS hijack based on arp spoofing
Oct. 2018 - Dec. 2018	<p>Encryption tool development</p> <p>This project implemented an encryption tool including a series of encryption algorithms, basic key exchange function and signature function.</p> <p>Implemented algorithms:</p> <ul style="list-style-type: none"> • Symmetric encryption: DES, AES • Stream cipher: RC4 • Asymmetric encryption: RSA • Hash: SHA-1, MD5 • Key exchange: DH
Sep. 2018 - Nov. 2018	<p>Privilege and app control plug-in for android</p> <p>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.</p>
June 2018 - Aug. 2018	<p>FPGA design</p> <p>Implemented a series of functions with different sensors, buttons and LED display.</p> <p>Implemented function list:</p> <ul style="list-style-type: none"> • Reversing radar (using ultrasonic sensor) • IR remote control • Coded lock • Detector with optical sensor and thermal sensor
Dec.2017 - Jan.2018	<p>Basic CPU implementation</p> <p>Implemented a basic CPU with VHDL that could execute a series of instructions stored in the memory.</p> <p>Implemented function list:</p> <ul style="list-style-type: none"> • 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	<p>NIO Inc</p> <p>Responsibilities:</p> <ul style="list-style-type: none"> • Information security management (Including the management of DLP, Firewall, fortress machine, etc.) • Terminal management application development • Automation scripts development
July 2019 – Aug. 2019	<p>Heetian Ltd</p> <p>Implemented three online courses on the Heetian lab platform;</p> <ul style="list-style-type: none"> • 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