curriculum vitæ of
Yepeng Pan

Cryptography · Blockchain · Privacy Enhancing Technology · Access Control

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 Core courses:

- Computer Security I; Computer Security II;
- Introduction to Cryptography; Cryptocurrencies;
- Malware; Privacy Enhancing Technologies; Distributed Systems and Security;

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 retrieval system**

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

Brief introduction of the system:

- This system aims to solve the problem that cloud image retrieval system could analyse user's requests and damage user privacy.
- This system uses compressed binary CNN fully connected layer outputs to represent image features, and uses the distance among image features as the classification basis to generate a tree for retrieval. By encrypting the tree and user's requests with random matrix, cloud server can only use encrypted features to calculate distance between user's request and tree nodes, and thus the system can preserve user privacy.

Completed improvements:

- Because the original system's tree generation process only merging nodes with high similarity, it may generate an unbalanced binary tree with large depth, and it will leads to low accuracy since the features of nodes with small depth in the tree will become fuzzy. By involving new threshold and check process, the system will get a chance to merge nodes with low similarity at the right time. Experiments show that the accuracy of the modified system is 8% higher than that of the original system on average, and modified system performs even better when more categories of pictures are used.
- The original system's retrieval process will only pick one node which has the smallest distance with user's request at each level, so the original system doesn't perform well when there are similar nodes at the same level. By involving more (Experiments shows that the maximum of 3 nodes perform the best) similar nodes into consideration, modified system could reach higher accuracy.

Further improvements:

- It is inevitable that the features of nodes will become more fuzzy during the tree generation process, and it will even getting worse if there are more categories of images involved, so that using tags during the tree generation process may achieve higher accuracy and it can also simplify the retrieval process.

Apr. 2019 - May. 2019

An investigation on the security of DNS servers in China

Analysed 500 DNS servers' responses towards 20 different domain names with traceroute, nslookup and wireshark.

Brief introduction:

- This research tests 500 DNS servers provided by Hunan university, google, and different ISPs in China. The 20 tested domain names include 15 common domain names in China, 3 domain names of google and 2 inexistent domain names. By analysing these DNS servers' reply, a series of DNS security problems has been found.

Conclusion:

- Different ISPs in China have different strategies toward inexistent domain names. DNS server provided by China Mobile will direct user to its ads page if requested domain name doesn't exist while other ISPs won't.
- A small amount (3 out of 28) of DNS servers provided by China railway telcom and DNS servers provided by Hunan university can resolve all domain names correctly, while all DNS servers provided by other ISPs will give false replies toward domain names of google.
- When users assign "8.8.8.8" as their DNS server and query domain names of google, ISPs will analyse their requests and reply a false IP before the real DNS server.

Project

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 aimed to use different machine learning models(LR, SVM, CMA-ES) to predict the output of PUF. Experiments showed that LR, SVM, CMA-ES can all predict PUF's output precisely.

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 cryptography: DES, AES
- Stream cipher: RC4
- Asymmetric cryptography: 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);

Honors

Dec. 2019 First class scholarship (2/62) — Hunan University

Sept. 2019 Postgraduate recommendation (6/62) — Hunan University

Jan. 2017 Third prize of programming competition — Hunan University

Programming Skills

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