Wilson Nguyen

wdnguyen@stanford.edu • github.com/MercysJest • https://c.rypto.systems

EDUCATION

Stanford University, Stanford, California, USA — Fall 2016 – Present

- **Computer Science Ph.D (Applied Cryptography Group)** — Fall 2020 – Present
  - **Advisor:** Dan Boneh
  - **Research Focus** Developing Zero Knowledge proof systems and related cryptographic primitives.
  - **CS:** Algebraic Error Correcting Codes (250), Mining Massive Data Sets (246)
- **Computer Science B.S.** — Fall 2016 – Spring 2020
  - **CS**: Advanced Topics in Cryptography (355), Topics in Computer & Network Security (356), Topics in Programming Language Theory (358), Cryptography (255), Computational Complexity (254), Programming Languages (242), Computer & Network Security (155), Automata and Complexity Theory (154), Operating Systems (140), Design & Analysis of Algorithms (161)
  - **Math**: Elementary Theory of Numbers (152), Modern Mathematics Discrete Methods (61DM & 62DM), Linear Algebra & Matrix Theory (113)

RESEARCH EXPERIENCE

Undergraduate Research Assistant – Stanford University

- **Advisor:** Zakir Durumeric — Winter 2018 – Autumn 2020
  - Investigated the state of the TLS ecosystem through internet scanning and massive data set exploration.
  - Developed an SSL/TLS scanning tool (approx. 3 million domains) to probe for version, protocol, ciphersuite, elliptic curve, compression, and extension support.
  - Contributed to existing research libraries and applications such as zcrypto & zgrab2.
  - Built & maintained networking scanning infrastructure and lab environment.
  - Undergraduate Research Internship in CS (CURIS), presented in poster session — Summer 2019
- **Advisor:** Marco Patrignani — Autumn 2019
  - Applied secure compilation techniques to cryptographic domains.
  - Investigated a compiler from the Oxide programming language to Ethereum bytecode to preserve relevant security properties such as linear typing and timing guarantees.

TEACHING

Topics in Cryptography (CS355) – Stanford University

- **Co-Instructor** — Spring 2022
  - Lectured and assign problems sets on topics in modern cryptography including zero knowledge, multiparty computation, elliptic-curve cryptography, cryptanalysis, privacy, and post-quantum cryptography

Hack Lab (IPS/INTPOL 268) – Stanford University

- **Professor**: Alex Stamos
- **Head Teaching Assistant** — Spring 2018 – Autumn 2019
  - Organized & led course staff.
  - Taught students through labs, sections, and examinations.
  - Developed hands-on labs to teach the foundational attacks in cybercrime and cyberwarfare.
  - Designed & constructed isolated practice environments for red teaming exercises and exploitation.

LEADERSHIP

Computer Science Ph.D Student Advisory Council — 2021 – Present

- **Admissions Committee Member** — Winter 2021
  - Reviewed CS Ph.D applications and interviewed potential admits to the program.
- **Ph.D Student Council Member** — 2021–Present
  - Advancing and advocating for Ph.D student needs and resources.

Computer Science Undergraduate and Master's Research Advisor — 2021 – Present

- **Research Advisor** Advising a small team of master students and undergrads on various ongoing projects related to Zero Knowledge proof systems. — 2021–Present
- **CURIS Undergraduate Research Advisor** Advised two undergraduate students on a summer project related to Functional Commitments (below). — Summer 2021

Applied Cybersecurity Organization – Stanford University — 2016 – 2019

- **Co-captain**: National Collegiate Penetration Testing Competition (Awards below) 2017 – 2018
- **Team member**: National Collegiate Cyber Defense Competition (Awards below) 2016 – 2017
- **Technical Advisor**: 2016 – 2019
  - Created lab environments for competition practice and research.
  - Served as organization mentor for security projects, competitions, and research opportunities.
- **Organizer**: Ran security competitions (Capture-The-Flags) for hackathons. 2016 – 2018

RESEARCH +PROJECTS

Functional Commitments – Stanford, California Autumn 2021

- We construct efficient (function hiding) functional commitments for arithmetic circuits of polynomial size. A (function hiding) functional commitment scheme enables a *committer* to commit to a secret function f and later prove that $y = f(x)$ for public x and y without revealing any other information about f. As such, functional commitments allow the operator of a secret process to prove that the process is being applied uniformly to everyone.

An Empirical Analysis of HTTPS Configuration Security – Stanford, California Autumn 2021

- In this work, we empirically evaluate the TLS security posture of popular websites and endeavor to understand the configuration decisions that operators make. We correlate several sources of influence on sites' security postures, including software defaults, cloud providers, and online recommendations.

SGXware - Malware in Intel SGX – Stanford, California Autumn 2018

- Demonstrated the effective use of Intel SGX for malware with a Pay-Per-Enclave (PPE) market ecosystem.
- Provided confidentiality & integrity guarantees for malware code and data, during execution and statically on disk.
- Designed a small syscall forwarding library and secure Domain Generation Algorithm (DGA).

TreeCTF – Stanford, California Spring 2018

- Developed & operated a computer security competition held at Stanford in partnership with TreeHacks, a hackathon with competing university students across the nation.

LASACTF – lasactf.com – github.com/LASACTF Autumn 2015 – Spring 2016

- Developed & operated an online computer security competition for 5000+ high school and college students

INDUSTRY

Google Security Engineer Intern – Sunnyvale, California Summer 2018

- Conducted vulnerability research on Firebase.
- Developed signals to detect dangerous Firebase configurations.
- Performed product security reviews and worked with teams to remediate vulnerabilities.
- Conducted an internal security engagement modeling insider threat.

Praetorian Security Intern – Austin, Texas Summer 2017

- Conducted penetration testing on client companies' commercial and staging environments.
  - Compromised publicly exposed client infrastructure including web servers and application hosts.
  - Created phishing engagements through Gophish Framework, open source intelligence, and Cobalt Strike.
  - Spread laterally through Active Directory domains and obtained system level control of domain controllers.

ACCOLADES

Academic Awards

- **Tau Beta Pi Candidate** – Stanford University 2018 – 2019
  - Top 1/5 of engineering seniors and the top 1/8 of engineering juniors.
  - Invited for both senior and junior year.

Cyber Security Competitions

- **National Collegiate Penetration Testing Competition** – Co-Captain 2017 – 2018
  - Nationals: **1st place** Nov 2017
  - Western Region: **1st place** Oct 2017
  - Conducted a full penetration test on competition infrastructure, navigated client & company interaction, authored follow-up remediation report.
- **National Collegiate Cyber Defense Competition** – Competitor 2016 – 2017
  - Western Region: **2nd place** Mar 2017
  - Western Region Invitational: **1st place** Nov 2016
  - Defended Active Directory environments and domain controllers from live attacks by professional penetration testers.