TALHA PARACHA

mtalhapar@gmail.com ◇ talhaparacha.com
Canadian Legal Permanent Resident ◇ 263 Dupont St, Toronto, ON

I am a Software Engineer and a recent CS PhD graduate with skills in network security, and prior industry experience at Meta (Facebook) and Cloudflare. Looking forward to a role in industry, collaborating with people from diverse backgrounds, and solving interesting problems.

EDUCATION

Northeastern University, Boston 2018 - 2023
Ph.D. in Computer Science, advised by Prof. David Choffnes. CGPA: 3.97 / 4

National University of Sciences and Technology, Islamabad 2014 - 2018
B.E. in Software Engineering, with the Best Graduate Thesis Award (co-recipient). CGPA: 3.81 / 4

EXPERIENCE INDUSTRY

Product Security Engineer Intern, Meta (Facebook) Summer 2022

Conducted manual security reviews of OIDC-based authentication methods in upcoming features. Helped improve and triage alerts from automated static and dynamic analysis frameworks to scale coverage.

Research Engineer Intern, Cloudflare Summer 2020 & 2021

Developed SSL/TLS Recommender to detect website support for security protocols and improve customer configurations. Our product was successfully released as an opt-in feature on the Cloudflare dashboard.
blog.cloudflare.com/ssl-tls-recommender/

Designed HTTP/2 connection coalescing experiments for a popular and mission-critical service, CDNjs, to study real-world improvements in connection privacy, performance, and reliability.
blog.cloudflare.com/connection-coalescing-experiments/

Open-source Developer, Drupal, Google Summer of Code Summer 2016

Developed an encryption module for Drupal to secure data with user login credentials.
drupal.org/project/pubkey_encrypt/

EXPERIENCE ACADEMIA

Postdoctoral Researcher, Ruhr University Bochum 2024 - current

Lead developer on network security projects with a current focus on using language models (LLMs) for testing TLS implementations, and deploying a Kubernetes-based global measurement platform.

- Developed MLCerts, a novel approach that leverages generative language models to create synthetic X.509 TLS certificates for testing. Using our approach, we find significantly more distinct discrepancies between the five TLS implementations OpenSSL, LibreSSL, GnuTLS, MbedTLS, and MatrixSSL than the state-of-the-art benchmark Transcert (+30%; 20 vs 26, out of a maximum possible of 30).
- Developed SoftsecGLOBE, a distributed global measurement platform to help improve reliability in research experiments. Responsible for engineering, security and software infrastructure of the project. Using Headscale + MicroK8s + Kata Containers to manage nodes, Tailwind for the frontend, Gin Web Framework for the backend, and Drone CI for build automation.

Graduate Research Assistant, Northeastern University 2018 - 2023

Developed software for network security and measurement research. Designed static and dynamic analysis techniques to study how diversity in TLS implementations and deployments influences protocol security.

TECHNOLOGIES

Python, Golang, Java, PHP, C, C++, MySQL, NoSQL, HTML + CSS + Javascript.

Linux, Git, Travis CI, Drone CI, OpenCV, LaTeX, Wordpress, Drupal.

SELECTED PUBLICATIONS

Hallucinating Certificates: Differential Testing of TLS Certificate Validation Using Generative Language Models (ICSE'26)
Talha Paracha, Kyle Posluns, Kevin Borgolte, Martina Lindorfer, David Choffnes.

A Comparative Analysis of Certificate Pinning in Android & iOS (IMC'22)
Amogh Pradeep, Talha Paracha*, Protick Bhowmick, Ali Davanian, Abbas Razaghpanah, Taejoong Chung, Martina Lindorfer, Narseo Vallina, Dave Levin, David Choffnes.*
**equal contribution*

IoTLS: Understanding TLS Usage in Consumer IoT Devices (IMC'21)
Talha Paracha, Daniel Dubois, Narseo Vallina-Rodriguez, David Choffnes.

A Deeper Look at Web Content Availability and Consistency over HTTP/S (TMA'20)
Talha Paracha, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin.

THESIS SUPERVISION

Detecting TLS Interception in the Wild
Okan Saracbasi

Signed Certificate Timestamps: A Never-Failing Promise?
Luis Wengenmair

OTHER ACTIVITIES

Volunteer, ENGin English Language Practice & Cultural Exchange for Ukrainians

Mentor, Google Summer of Code 2017 & Google Code-In 2016

Hackathon Winner, Women Transport Innovation Hackathon & SEECS Social Hackathon

GRADUATE COURSEWORK

CS 6740	Network Security	A
CS 5770	Software Vulnerabilities and Security	A
CS 7600	Intensive Computer Systems	A
CS 6140	Machine Learning	A
CS 7250	Information Visualization	A-
CS 7400	Intensive Principles of Programming Languages	n/a

REFERENCES

David Choffnes Associate Professor, Northeastern University (choffnes@ccs.neu.edu).

Alan Mislove Professor, Northeastern University (amislove@ccs.neu.edu).

Christo Wilson Associate Professor, Northeastern University (cbw@ccs.neu.edu).

Taejoong Chung Assistant Professor, Virginia Tech (tijay@vt.edu).