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
Bachelor of Software Engineering. CGPA: 3.81 / 4
Best Bachelor's Thesis Award (co-recipient).

EXPERIENCE

Postdoctoral Researcher, Ruhr University Bochum 2024 - current

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

Product Security Engineer Intern, Meta (Facebook) Summer 2022

Conducted security reviews of OIDC-based authentication mechanisms in upcoming features.

Research Engineer Intern, Cloudflare Summer 2020 & 2021

Developed SSL/TLS Recommender to help improve internal security configurations using insights from academic research. 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/

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. My research has uncovered issues with TLS adoption on the web (e.g., content inconsistencies), in mobile devices (e.g., inconsistent certificate pinning policies), and, in IoT devices (e.g., stale CA root stores).

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

TECHNOLOGIES

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

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

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

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.

Behind the Scenes: Uncovering TLS and Server Certificate Practice of IoT Device Vendors in the Wild (IMC'23)
Hongying Dong, Hao Shu, Vijay Prakash, Yizhe Zhang, Talha Paracha, David Choffnes, Santiago Torres-Arias, Danny Huang, Yixin Sun.

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*

Respect the ORIGIN! A Best-case Evaluation of Connection Coalescing in The Wild (IMC'22)
Sudheesh Singanamalla, Talha Paracha, Suleman Ahmad, Jonathan Hoyland, Luke Valenta, Yevgen Safronov, Peter Wu, Andrew Galloni, Kurtis Heimerl, Nick Sullivan, Christopher Wood, Marwan Fayed.

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.

Blocking without Breaking: Identification and Mitigation of Non-Essential IoT Traffic (PETS'21)
Anna Maria, Daniel Dubois, Roman Kolcun, Talha Paracha, Hamed Haddadi, David Choffnes.

When Speakers Are All Ears: Characterizing Misactivations of IoT Smart Speakers (PETS'20)
Daniel Dubois, Roman Kolcun, Anna Maria, Talha Paracha, David Choffnes, Hamed Haddadi.

THESIS SUPERVISION

Detecting TLS Interception in the Wild
Okan Saracbasi

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

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).