

TALHA PARACHA

mtalhapar@gmail.com [◇ talhaparacha.com](http://talhaparacha.com)

EDUCATION

Northeastern University, Boston Ph.D. in Computer Science, advised by Prof. David Choffnes. Research in Network Security, with a focus on TLS implementations and deployment.	2018 - 2023 CGPA: 3.97 / 4
National University of Sciences and Technology, Islamabad Bachelor of Software Engineering. Best Bachelor's Thesis Award.	2014 - 2018 CGPA: 3.81 / 4

RESEARCH SUMMARY

My research explores security issues related to the implementation and deployment of the TLS protocol. My approach to research is to build novel measurement techniques, and to shed light on unexplored aspects of protocol use that may impact security. In the past, my work 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).

EXPERIENCE

Research Intern, Vienna University of Technology <i>Network Security, Software Security</i>	Fall 2023 Prof. Martina Lindorfer
Security Engineer Intern, Meta (Facebook) <i>Network Security, Authentication</i>	Summer 2022 ProdSec Org.
Research Engineer Intern, Cloudflare <i>Network Security, Privacy</i>	Summer 2020 & 2021 Nick Sullivan
Improved customers' internal security configurations using insights from academic research. Our product, SSL/TLS Recommender, was successfully released as an opt-in feature on the Cloudflare dashboard.	
Orchestrated HTTP/2 connection coalescing experiments for a popular and mission-critical service, CDNjs, to study real-world improvements in connection privacy, performance, and reliability.	
Research Intern, Swiss Federal Institute of Technology in Lausanne <i>Medical Data Security, Blockchains</i>	Summer 2018 Prof. Jean-Pierre Hubaux
Research Intern, Rutgers University <i>Computer Networks, Measurements</i>	Summer 2017 Prof. Waheed Bajwa
Research Intern, TUKL-NUST R&D Lab <i>Machine Learning, Computer Vision</i>	Spring 2017 & 2018 Prof. Faisal Shafait
Open-source Developer, Google Summer of Code <i>Web Development, Network Security</i>	Summer 2016

OTHER ACTIVITIES

- Mentor**, Google Summer of Code 2017 & Google Code-In 2016
- Organizer**, MLH Local Hack Day
- Hackathon Winner**, Women Transport Innovation Hackathon & SEecs Social Hackathon
- Travel Grants Recipient**, NDSS Symposium 2017 at San Diego & DrupalCon 2017 at Baltimore

PUBLICATIONS

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.

TECHNOLOGIES

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

Linux, Git, Travis CI, OpenCV, L^AT_EX, Wordpress, Drupal, Adobe Photoshop.

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).