TALHA PARACHA

mtalhapar@gmail.com ⋄ talhaparacha.com

EDUCATION

Northeastern University, Boston 2018 - ongoing
Ph.D. in Computer Science, advised by Prof. David Choffnes. CGPA: 3.97 / 4
Research in Network Security, with a focus on TLS implementations and deployment.

National University of Sciences and Technology, Islamabad 2014 - 2018
Bachelor of Software Engineering. CGPA: 3.81 / 4

WORK EXPERIENCE

Security Engineer Intern, Meta Summer 2022
Internet Security, Authentication ProdSec Org.

Conducted manual security reviews of OIDC related authentication mechanisms in upcoming features.

Research Engineer Intern, Cloudflare Summer 2020 & 2021
Internet Security, Privacy 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, EPFL - Switzerland Summer 2018
Medical Data Security, Blockchains Prof. Jean-Pierre Hubaux

Implemented a blockchain-based access control system for medical data featuring a decentralized design with extensive auditability (more details @ talhaparacha.com/MedChain.pdf).

Research Intern, Rutgers University Summer 2017
Computer Networks, Measurements Prof. Waheed Bajwa

Proposed modification to a distributed average consensus algorithm for packet-switched networks to reduce its bandwidth overhead by ≈ 25% (more details @ talhaparacha.com/communication.pdf).

Research Intern, TUKL NUST R&D Center Spring 2017 & 2018
Machine Learning, Computer Vision Prof. Faisal Shafait

Proposed new techniques for privacy-preserving incremental learning. Resulting group project won the best bachelor's thesis award (more details @ talhaparacha.com/fyp.pdf).

Open-source Developer, Google Summer of Code Summer 2016
Web Development, Internet Security

Built an encryption module for Drupal to secure data-at-rest with users' login credentials.
(more details @ drupal.org/project/pubkey_encrypt)

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 Recepient, NDSS Symposium 2017 at San Diego, & DrupalCon 2017 at Baltimore

TECHNOLOGIES

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

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

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 network 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 differences), in mobile devices (e.g., inconsistent certificate pinning policies), and, in IoT devices (e.g., stale CA root stores).

PUBLICATIONS

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.

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