IoTLS: Understanding TLS Usage in Consumer IoT Devices

Muhammad Talha Paracha, Daniel J. Dubois, Narseo Vallina-Rodriguez, David Choffnes

---

Data Sharing Agreement

To receive full access to the dataset for the paper “IoTLS: Understanding TLS Usage in Consumer IoT Devices”, published at the Internet Measurement Conference 2021, you must agree to the following terms:

1. **LICENSE**. You are given a non-exclusive and non-transferable license to access and use the dataset for the purpose of non-profit research and education.

2. **NON-DISCLOSURE**. You will not disclose the dataset to any person other than those employed by your institute who are assisting or collaborating with you using the dataset. Other entities must request access to the dataset separately by sending a request to *moniotr@ccs.neu.edu*.

3. **MANDATORY CITATION**. If you create a publication (including web pages, papers published by a third party, teaching material, and publicly available presentations) using data from this dataset, you must cite our paper as follows:

● **Title:** IoTLS: Understanding TLS Usage in Consumer IoT Devices

● **Authors:** Muhammad Talha Paracha, Daniel J. Dubois, Narseo Vallina-Rodriguez, David Choffnes

● **Venue:** Internet Measurement Conference (IMC) 2021

Or, in bibtex format:

```
@inproceedings{paracha-imc21,
title={{IoTLS: Understanding TLS Usage in Consumer IoT Devices}},
author={Paracha, Muhammad Talha and Dubois, Daniel J. and
Vallina-Rodriguez, Narseo and Choffnes, David},
booktitle={Proc. of the Internet Measurement Conference (IMC)},
```

year={2021}}

4. **CONFIDENTIALITY**. All data from this dataset is confidential. You agree to protect the confidentiality of the data and to prevent its unauthorized disclosure and use.

5. **ANONYMIZATION**. For any publication or other disclosure, you will anonymize or de-identify any credentials, authentication tokens, unique identifiers, and any other personally identifiable information you find in the dataset.

6. **NO ABUSE**. You will not attempt to use any information that can be derived from the dataset for purposes that are different from non-profit research and education. This includes disclosing any form of credentials or personally identifiable information found in the dataset, or using them for the purpose of gaining unauthorized access to any third-party services or systems. We have done our best to ensure that the dataset contains no data that could be used to compromise our systems; however, if you find any vulnerabilities or credentials in the dataset, you must responsibly disclose them to us or the manufacturers of systems affected by them.

If you agree to these terms, please write an email to *moniotr@ccs.neu.edu* with the subject "*IMC 2021 IoTLS: Full Dataset Access*" In the body of the email, you must state that you have read this agreement and you agree to abide by its terms. Please be sure to include your name and affiliation in your email. We are asking this because, despite our best efforts to anonymize the data, there can still be private or security-sensitive information that we were unable to remove from the traces.