PennState

February 9, 2021
CSE Dept, School of EECS,
Pennsylvania State University,
305 Westgate Building,
University Park, PA 16802
Phone: +1 (765) 409-7038
Email: hussain1@psu.edu

To Whom It May Concern:

It is with great enthusiasm that I write this letter of strong support for the Osmocom project. Before I buckle down into the details of the Osmocom project, first I would like to take the opportunity to briefly introduce myself. I am an Assistant Professor in the Department of Computer Science and Engineering at Pennsylvania State University. Before joining Penn State in fall 2020, I worked as a postdoctoral researcher at Purdue University from where I also received my Ph.D. in December 2018. My research interests broadly lie in network and systems security with a focus on the fundamental improvement of security and privacy analysis of emerging networks and cyber-physical systems, including cellular networks and Internet-of-Things. I have been inducted twice in the *Hall of Fame Mobile Security Research* by GSMA for my contribution in identifying several new protocol flaws in 4G and 5G cellular networks. My research findings have also led to several changes in the 4G and 5G cellular protocol designs and in operational networks.

The Osmocom (**O**pen **s**ource **mo**bile **com**munications) project is one of the largest open-source software and hardware projects focusing on improving the state-of-the-art of mobile communication systems. Though cellular specifications have been publicly available by the standard body, proprietary network equipment and the closed-source nature of cellular devices' implementations have always been obstacles for the research community and small industry. With its open-source hardware and software supports for cellular communication, Osmocom broke this barrier, unrolled complex cellular technologies, and unleashed the opportunity to contribute to the design and development of new technologies for cellular communication systems.

For many of our research projects on cellular network security, we have been using different sub-projects (e.g., PySim and SIMToolkit) of the Osmocom project to build the cellular testbed in our lab. These sub-projects enabled us implementing and evaluating the proof-of-concept of many of our cellular defense proposals and principled security analysis techniques, which could make an impact from national to individual level. For instance, the proof-of-concept implementations of our proposed defense against Stingray-type fake base station is the first work to demonstrate the practical deployment of cellular broadcast authentication and has drawn the attention of the Federal Communication Council (FCC) to mitigate this long-standing issue in mobile communication. This work has also spurred further discussion and research in the cellular standard body and research community to study the feasibility of adopting such a solution in the next-generation cellular networks. In addition, our work on cellular security evaluations built with the Osmocom sub-projects also helped uncover and fix several new critical protocol flaws in the 4G and 5G cellular networks. Similar to PySim and SIMToolkit, other open-source hardware and software sub-projects, including the 2G and 3G core network infrastructures and GSM enabled cellular devices by Osmocom have significantly contributed to the improvement of the security and privacy postures of such critical infrastructures. This open-source communication system has further propelled the development of new cellular technologies and features for next-generation cellular networks. In short, the Osmocom project has greatly helped the community to make ground-breaking research works with their cutting-edge tools and open-source infrastructures.

The open-source tools and infrastructures developed by Osmocom are also being used by many schools and research organizations, including Pennsylvania State University to teach graduate and undergraduate students who are now working to contribute to the research and development of new cellular technologies and security solutions.

In summary, I strongly support the new research and tools by the Osmocom project to continue developing robust and open-source mobile communication systems. This is essential because such open-source mobile communication systems can bring academia and industry to work together in order to build more secure and ultra-high-speed next-generation cellular systems. For this, we encourage all sorts of support and financial contributions to the Osmocom project. I look forward to seeing the growth of the Osmocom project and the exciting new research and tools out of it in the coming years.

Should you have any questions, please feel free to reach out to me.

Sincerely yours,

Syed Rafiul Hussain
Assistant Professor
Department of Computer Science and Engineering
School of Electrical Engineering and Computer Science
Pennsylvania State University
Webpage: https://syed-rafiul-hussain.github.io/