

SECURITY OF IOT CONNECTIVITY PROTOCOLS: A SURVEY

ANALYSIS OF CURRENT STATE, THREATS AND POSSIBLE COUNTER-MEASURES

Security has been neglected in Internet of Things (IoT) solutions, partially due to the market's fast demands and its resource constraints. The number of IoT devices is increasing and diverse protocols are being used to achieve connectivity, such as Bluetooth, LPWA, 6LoWPAN, etc. This lack of standardization is one of the main problems with respect to security, since it is hard to find a one size fits all solution and each protocol has its own limitations and security issues. As the "IoT Developer Survey 2017" [1] presented by the Eclipse Foundation's vice president of marketing shows, heterogeneity is not only restricted to communication protocols, indicating a challenging environment for suggesting effective counter-measures against security threats.

Considering this scenario, the main goal of this work is to assess the current state of the art concerning security of the connectivity protocols being used in IoT solutions. After identifying and analyzing existing threats, a deep and thoughtful discussion presenting possible counter-measurements is expected.

LEARNING OPPORTUNITIES AND SUPPORT

This topic is highly research and theoretical oriented, since it requires reading and understanding security threats, checking existing solutions and suggesting improvements considering a range of different connectivity protocols. For the ones willing to pursue academic positions, it is a great starting point to get a better feeling of how literature research is done. For the ones aiming at industry positions, it is interesting because it gives an overview and improves the understanding of the current IoT protocols being used.

REQUIREMENTS

The presented topic is challenging not only because of the obstacles that IoT solutions inherit as a consequence of their heterogeneous nature, but also due to the literature research required. Usually the amount of work that surveys demand is underestimated, nevertheless they are very time-consuming and most of the time not trivial. A good understanding of connectivity protocols, their possible flaws and creativity to present feasible solutions to overcome the problems is required. Ability to work independently is expected.

INTERESTED?

Please contact **Carolina Nogueira** (nogueira@cs.uni-kl.de). Do not forget to send a brief introduction about yourself, your interests and relevant qualification.

ABOUT US

We are the distributed computer system (disco - <https://disco.cs.uni-kl.de>) research group, located at the 4th floor of building 36. Our research focus is on performance and security of distributed systems.

REFERENCE

- [1] Ian Skerrett. "IoT Developer Survey 2017",
<https://ianskerrett.wordpress.com/2017/04/19/iot-developer-trends-2017-edition/>.
Accessed on 11 Oct 2017.