Adv Automob Eng 2018, Volume 7
DOI: 10.4172/2167-7670-C1-012

IoT malware analysis and detection based on association link

Alsa Tabatabaei
University of Salford, UK

With the widespread adoption of Internet-of-Things (IoT) devices and services in autonomous cars, many convenient IoT services have been provided to drivers. However, modern cars are exposed to security risks just as are IoT devices. Accordingly, hackers are expanding the scope of their attacks beyond the existing PC and Internet environment into autonomous vehicles. A successful attack on the IoT automotive infrastructure can tamper with the car's functions. While car companies focus on automobile safety feature and driving experience, cyber attackers are stepping up their efforts. Malicious software is becoming more advanced to evade the cyber defence system. Therefore, even the best car-related software security products may not see an unseen threat coming. Making matters worse, IoT devices often have a number of vulnerabilities, both known and unknown. Nonetheless, we need to consider the potential risks by combining IoT with smart cars, with a mechanism to detect attacks automatically sooner rather than later. In this research, we present a machine learning based approach to detect IoT malware by analysis malicious frequent sequential patterns. Specifically, our proposed method mines the link between the patterns of different IoT families and also non-malicious applications. We then demonstrate that our proposed approach outperforms Random Forest, K-Nearest Neighbors, Support Vector Machine, in terms of accuracy rate, recall rate, precision rate and F-measure.

S.Alsadattabatabaei@edu.salford.ac.uk