ABSTRACT

Internet of Things (IoT) in military settings generally consists of a diverse range of Internet-connected devices and nodes (e.g. medical devices and wearable combat uniforms). These IoT devices and nodes are a valuable target for cyber criminals, particularly state-sponsored or nation state actors. A common attack vector is the use of malware. In this paper, we present a deep learning based method to detect Internet Of Battlefield Things (IoBT) malware via the device's Operational Code (OpCode) sequence. We transmute OpCodes into a vector space and apply a deep Eigenspace learning approach to classify malicious and benign applications. We also demonstrate the robustness of our proposed approach in malware detection and its sustainability against junk code insertion attacks. Lastly, we make available our malware sample on Github, which hopefully will benefit future research efforts (e.g. to facilitate evaluation of future malware detection approaches).Robust malware detection for internet of things is a process performed by software and hardware. Input Architecture is the method of translating a user-oriented data definition into a computer-based program. This architecture is necessary in order to prevent mistakes in the data input process and to display the correct way to the management to get the correct information from the computerized system. This is done by designing user friendly data entry screens to accommodate huge data volumes. The aim of input design is to make data entry simpler and error-free. The data entry system is designed in such a way that all data processing can be done. It also offers a record screening service. When the data is entered, it must test the authenticity of the results. Data can be entered with the aid of a phone. Reasonable alerts are received as appropriate so that the consumer is not immediately in maize. The goal of the interface design is therefore to create an interface structure that is simple to navigate.