

Context Aware Anomaly Behavior Analysis for Smart Home Systems

Authors : Zhiwen Pan, Jesus Pacheco, Salim Hariri, Yiqiang Chen, Bozhi Liu

Abstract : The Internet of Things (IoT) will lead to the development of advanced Smart Home services that are pervasive, cost-effective, and can be accessed by home occupants from anywhere and at any time. However, advanced smart home applications will introduce grand security challenges due to the increase in the attack surface. Current approaches do not handle cybersecurity from a holistic point of view; hence, a systematic cybersecurity mechanism needs to be adopted when designing smart home applications. In this paper, we present a generic intrusion detection methodology to detect and mitigate the anomaly behaviors happened in Smart Home Systems (SHS). By utilizing our Smart Home Context Data Structure, the heterogeneous information and services acquired from SHS are mapped in context attributes which can describe the context of smart home operation precisely and accurately. Runtime models for describing usage patterns of home assets are developed based on characterization functions. A threat-aware action management methodology, used to efficiently mitigate anomaly behaviors, is proposed at the end. Our preliminary experimental results show that our methodology can be used to detect and mitigate known and unknown threats, as well as to protect SHS premises and services.

Keywords : Internet of Things, network security, context awareness, intrusion detection

Conference Title : ICICS 2019 : International Conference on Information and Communications Security

Conference Location : San Francisco, United States

Conference Dates : June 06-07, 2019