International Journal of Wireless Networks and Broadband Technologies
Volume 10 • Issue 2 • July-December 2021

Wireless Interference Analysis for Home IoT Security Vulnerability Detection

Alexander McDaid, Letterkenny Institute of Technology, Ireland
Eoghan Furey, Letterkenny Institute of Technology, Ireland
Kevin Curran, Ulster University, UK

ABSTRACT

The integrity of wireless networks that make up the clear majority of IoT networks lack the inherent security of their wired counterparts. With the growth of the internet of things (IoT) and its pervasive nature in the modern home environment, it has caused a spike in security concerns over how the network infrastructure handles, transmits, and stores data. New wireless attacks such as KeySniffer and other attacks of this type cannot be tracked by traditional solutions. Therefore, this study investigates if wireless spectrum frequency monitoring using interference analysis tools can aid in the monitoring of device signals within a home IoT network. This could be used enhance the security compliance guidelines set forth by OWASP and NIST for these network types and the devices associated. Active and passive network scanning tools are used to provide analysis of device vulnerability and as comparison for device discovery purposes. The work shows the advantages and disadvantages of this signal pattern testing technique compared to traditional network scanning methods. The authors demonstrate how RF spectrum analysis is an effective way of monitoring network traffic over the air waves but also possesses limitations in that knowledge is needed to decipher these patterns. This article demonstrates alternative methods of interference analysis detection.

KEYWORDS

Hacking, Internet of Things, Network Security, Wireless Security

1. INTRODUCTION

Wi-Fi and other communication technologies such as Bluetooth have existed for more than two decades and the volume of devices that utilise these technologies have exploded in recent years with a nearly 100% adoption rate. The term The Internet of Things (IoT) is commonly used to name a set of objects (or things) that are directly connected to the Internet via communication protocols such as Wi-Fi (802.11), Bluetooth and numerous other communication protocols. These networks consist of devices known as "Things" which can be constrained by hardware shortcomings that reduce their security effectiveness. Objects in the IoT are controlled via microcontrollers that are constrained in computational power, memory resources and power restrictions. These restrictions limit the devices from being able to utilise the same protocols that are used by higher powered computers like Transmission Control Protocol (TCP) and HyperText Transfer Protocol (HTTP) or modern encryption standards which are too resource consuming to be used on these highly constrained devices. A recent study conducted by HP Fortify on Demand research concluded that 70% of Internet of Things devices on the market are vulnerable to attack (Miessler, 2014). The Internet of Things is a phenomenon

DOI: 10.4018/IJWNBT.2021070104

that is growing rapidly and is expected to include 50 billion devices connected to the internet by the year 2020 according to industry experts such as Michael Dell founder of Dell Inc. (Barajas, 2020). With this growth and the security constraints imposed on these devices by hardware shortcomings and security misconfigurations, it is predicted by Gartner Research that 20% of the overall security budget of major corporations will be spent trying to secure these devices (Woods & van der Muelen, 2016). Applications for this technology include agriculture, manufacturing, power distribution, to smart homes, healthcare, and beyond. All these sensory devices are connected to larger infrastructure produce an extraordinary amount of data. This technology advance acknowledges the reality that human society is moving towards 'smart' and 'smarter' systems. The rapid advances in computer science, software engineering, systems engineering, networking, sensing, communication, and artificial intelligence are converging (Voas, 2016).

With the rise of IoT networks in recent times and their expected exponential growth in the next five to ten years a way to effectively secure them will be of paramount importance (Barajas, 2020). There are few home or business owners that fully understand and recognise how their network exists and interacts with its surroundings and the threats that arise with the constant change in the number and type of devices that connect and disconnect on their networks. This shows the need for a better way to protect these IoT networks which is why the U.S. Federal Trade Commission (FTC) announced the launch of a contest that aims to find solutions for securing the Internet of Things (IoT) devices deployed in consumers' homes (Kovacs, 2017). The FTC said the tool can be a physical device installed on the user's home network, an app, a cloud-based service, or a dashboard. The requirement is that the tool addresses vulnerabilities caused by outdated software, but it can also include other security features, such as ones designed to mitigate the risk of hardcoded or weak passwords.

With the rapid rise of the IoT phenomenon and the introduction of these poorly secured devices onto the network infrastructure have brought with them an avalanche of security concerns that consumers have about this encroachment into the home. These vulnerabilities have been well documented by the OWASP Internet of Things Project (Li, 2020). The vulnerabilities highlighted by this project have been exploited in some recent high-profile attacks. These Direct Denial of Service (DDoS) attacks are nothing new but because of the prevalence of these unsecured devices with high bandwidth capacity these attacks have become devastating against their targets. This form of attack has been levied against some high-profile targets such as Dyn Domain Name Server (DNS) Service (Paganini, 2020). Dyn which services a large portion of the DNS service in the United States was put under intense attack using this DDoS form of attack that utilised many thousands possibly hundreds of thousands of these IoT devices under the control of the Mirai malware. This malware was able to infect these devices to harness them as a huge botnet able to inundate the Dyn Servers with a huge amount of traffic that was able to knock out their service (Paganini, 2020). This attack has also been successful in knocking out the website of well-known security investigator Brian Krebs utilising the same malware to produce an attack that produced 620 Gbps of traffic against his website which was stated as a record amount of traffic for a Denial of Service attack according to Akamai security engineers (Krebs, 2016). Akamai have released a threat advisory explaining how to exploit IoT devices for launching mass-scale attack campaigns against a target and how to protect against this exploitation (Caltum & Segal, 2016).

We therefore aim to investigate the effectiveness of using a set of professional tools that are designed to detect wireless interferences and to fix problems in a network environment. As a result, the objectives of the proposed research are:

- To investigate if a wireless interference and site survey planning toolset can be used as a preliminary scanning technique to detect network vulnerabilities before using network scanning methods.