Poster: Automatically Protecting Your Vulnerable Smart Devices: An Enhanced Wireless Router Approach

Zhitao Yan[1,2], Binxing Fang[3], Xiang Cui[1,2]
[1]School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China
[2]Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
[3]Institute of Electronic and Information Engineering in Dongguan UESTC, Dongguan, Guangdong
yanzhitao@iie.ac.cn, fangbx@bupt.edu.cn, cuixiang@iie.ac.cn

***Abstract*—It is well known that smart devices are vulnerable and can be intruded by attackers easily. However, most of smart devices cannot install security software or do not have the privileges to control the network traffic (e.g., embedded devices, smart phones without root or jailbreak, etc.). In this poster, we present a new approach to protect smart devices automatically without installing software on them. We design a router-based network protection framework that uses the router's network traffic controllability and computing capacity to protect smart devices. Our preliminary results show that this framework is feasible and can protect vulnerable smart devices automatically.**

***Keywords*—Wireless Router; Smart Device; Protection; Network Traffic**

I. Introduction

With the development of IoT (Internet of Things) devices, the manufacturers launched more smart devices than before. Smart appliances, such as smart TV, smart fridge, smart thermostat, are all launched onto market in last few years. However, the security of these smart devices are not so well as the smart features of them [1]. Some manufacturers value the speed of launching new devices instead of the security of them. Because most of them are embedded devices, the security software cannot be installed to prevent them from being intruded, like PCs. Even if the security software can be installed, we have to develop different models for different architectures, instruction sets and operation systems. The cost is too high for consumers.

Contributions: In this poster, we present a new approach to protect smart devices automatically. Our poster makes two contributions as follows:

1) We design a router-based network protection framework that focuses on how to use the router's network traffic controllability and computing capacity to protect all devices connected to the router without additional requirements.

2) We implement a prototype of the proposed framework and set up different experimental environments to test feasibility of the proposed framework.

II. The Proposed Framework

A. Definitions

Protected Node (PN): The protected node is the device which needs protection. No special software or hardware is required. For example, smart phone, PC, smart TV, IP camera, etc.

Router Node (RN): The router node is the center of the framework. It monitors the network traffic of PNs and responses to abnormal traffic immediately. It is usually build from a wireless router that we can find a way to install custom programs. For example, we can enable the telnet/SSH service in some wireless routers, install and run protection framework through telnet/SSH. If the original operation system in wireless router do not offer these features, we can also replace the operation system with OpenWrt/DD-WRT, which support more features, then install the framework.

B. Framework Architecture

The architecture of protection framework is shown in Fig. 1.

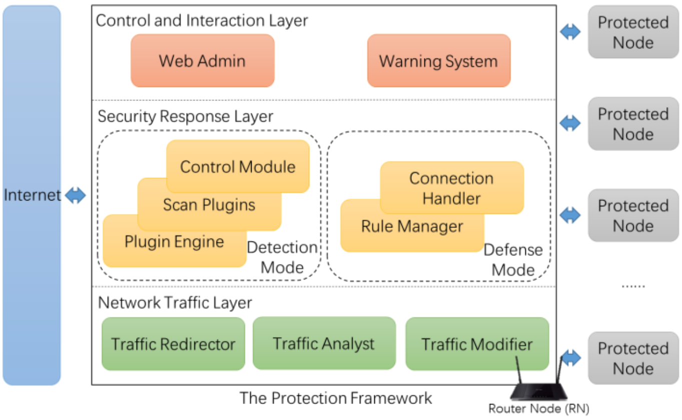

Fig. 1. The architecture of protection framework.

C. Network Traffic Processing

In order to monitor the network traffic, the traffic redirector module of the framework uses iptables to redirect all network traffic to its listening port. The traffic analyst module will analyze the redirected network data. Then, the traffic modifier will try to modify the data or not, according to the analysis result.

D. Protection Modes

The framework protects smart devices based on two modes: detection mode and defense mode.

In detection mode, the protection framework will use scan plugins to scan the local network regularly in order to find out the vulnerable devices, then try to fix the security issues. The framework contains a Lua engine, which is used as a plugin engine to support running scan plugins. It will provide several scan plugins to detect different security issues. For example, the method using default weak password to log in the system and upload malware by Telnet/SSH is a mainstream way for attackers to intrude smart devices. So the framework will run a weak password scan plugin regularly to detect devices which are using default or weak password, try to change them and warn users.

In defense mode, the protection framework will analyze the network traffic and try to find out the suspicious connections. Due to the computing capacity of wireless routers, the framework in RN will only detect the protocol of the network traffic, log its data usage and check whether it is normal to produce this kind of network traffic for this device. If not, the framework will try to block this connection, response and warn user. For example, if an intruded smart fridge starts sending junk emails, the framework will detect this abnormal network traffic because SMTP protocol is not in the allowed list of this PN (the smart fridge). The framework will try to close this connection and send warning messages to users.

III. PRELIMINARY EVALUATION

We implement a prototype of the proposed framework. In order to test feasibility of the framework, we use different wireless routers (RNs) and smart devices (PNs) to set up different environments. The RNs in experiment are four different wireless routers. According to their operation system and instruction sets, we compile and link two kinds of executable files (X86 and MIPS32). We upload the framework prototype to the RN and execute it through Telnet/SSH service. The detailed information of RNs is listed in Table I.

TABLE I. THE DETAILED INFORMATION OF RNS

Manufacturer	Model	Instruction Set	OS
ASUS	RT-AC66U	MIPS32 74K series	BusyBox 1.17.4
PHICOMM	PSG1208	MIPS32 24K/E series	BusyBox 1.12.1
NETGEAR	WNDR4300	MIPS32 74K series	DD-WRT V24 PreSP2
/	Virtual Machine	X86	OpenWRT 15.05

Preliminarily, we simulated eight work scenarios to test feasibility of this prototype version of protection framework. They can be divided into two categories as follows:

- In detection mode, we use plugins to scan the vulnerable smart devices and record the results.
- In defense mode, we use scripts and open source bot (Mirai [2], Lightaidra [3]) simulate attack scenarios to test protection capability of the framework.

The prototype runs well in our experimental devices as expected. More detailed experimental results are listed in Table II.

TABLE II. THE DETAILED EXPERIMENTAL RESULTS OF PROTOTYPE

	Mode	Test Methods	Protected Node	Result
1	Detection Mode	Scan vulnerable device using default weak password	Atsmart Smart Power Socket (M5)	Fixed
2		Scan the device with vulnerability (CVE-2015-3035)	TP-Link Wireless Router (TL-WDR4300)	Detected
3		Scan the device with vulnerability (CVE-2014-4727)		Detected
4	Defense Mode	Brute force crack weak SSH password	Atsmart Smart Power Socket (M5)	Blocked
5		Brute force crack weak HTTP password	HIKVISION IP Camera (DS-2CD3Q10FD)	Blocked
6		Lightaidra bot in PN try to communicate with C&C	ASUS Wireless Router (RT-AC66U)	Blocked
7		Mirai bot in PN try to communicate with C&C		Blocked
8		Test program in PN sends junk emails		Blocked

IV. CONCLUSION AND FUTURE WORK

In this poster, we propose a router-based network protection framework and implement a prototype. Experiments show that the proposed framework is feasible and can protect vulnerable smart devices automatically.

In the future, we will introduce more protection methods for defense mode besides protocol control and data usage control. Meanwhile, these methods should not influence the original network processing capacity considering the limited computing capacity of wireless routers.

ACKNOWLEDGMENT

This work is supported by the National Key Research and Development Program of China (No. 2016YFB0801604), and the Industry-University-Research Cooperation Project of Guangdong Province "Academician Workstation of Healthcare Cloud Security in Guangdong Province" (No. 2016B090921001).

REFERENCES

[1] Arabo, Abdullahi, and Bernardi Pranggono. "Mobile malware and smart device security: Trends, challenges and solutions." 2013 19th International Conference on Control Systems and Computer Science. IEEE, 2013.

[2] Jgamblin. Leaked Mirai Source Code for Research/IoC Development Purposes. https://github.com/jgamblin/Mirai-Source-Code

[3] Eurialo. IRC-based mass router scanner/exploiter. https://github.com/eurialo/lightaidra