ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Method of Detecting Abnormal Program Behavior on Embedded Devices

K. Ramya[1] **P.Sowjanya**[2]

[1] M.Tech (ES), Malla Reddy Engineering College (Autonomous), Hyderabad, India.
[2] Associate Professor, Malla Reddy Engineering College (Autonomous), Hyderabad, India.

Abstract

A potential threat to embedded systems is the execution of unknown or malicious software capable of triggering harmful system behavior, aimed at theft of sensitive data or causing damage to the system. Commercial off-the-shelf embedded devices, such as embedded medical equipment, are more vulnerable as these types of products cannot be amended conventionally or have limited resources to implement protection mechanisms. In this paper, we present a self-organizing map (SOM)-based approach to enhance embedded system security by detecting abnormal program behavior. The proposed method extracts features derived from processor's program counter and cycles per instruction, and then utilizes the features to identify abnormal behavior using the SOM. Results achieved in our experiment show that the proposed method can identify unknown program behaviors not included in the training set with over 98.4% accuracy.

Index Terms— ***Embedded system security, abnormal behavior detection, intrusion detection, self-organizing map.***

I.INTRODUCTION

The widespread use of embedded systems today has significantly changed the way we create, destroy, share, process and manage information. For instance, an embedded medical device often processes sensitive information or performs critical functions for multiple patients. Consequently, security of embedded systems is emerging as an important concern in embedded system design [1], [2]. Although security has been extensively explored in the context of general purpose computing and communications systems, for example via cryptographic algorithms and security protocols [3], such security solutions usually are often incompatible with particular embedded architectures. The reason for this is, that embedded architectures use custom firmware or operating systems, and are normally specific to a certain function with limited cost and resource [4], which makes e.g. conventional antivirus (AV) programs difficult to implement. Generally, the protection of embedded systems can be developed either at hardware or/and at software level.

II.EXISTING SYSTEM

In existing system nodes sending information to target device will be common factor in industries but we don't know whether nodes sending correct information or garbage values or previous values immediately to rectify the situation. To overcome this problem we are implementing the proposed method.

III.PROPOSED SYSTEM

In this proposed method, we are using an advanced open source ARM32 bit microprocessor [6] which is having advanced features support to complete our task. In order to overcome the disadvantage in existing method we are implementing the concept to get the proper information about the status of the modules (Memory Unit and Nodes unit) weather active or inactive stages in runtime to take an immediate action. In general run time modules information up-gradation can be accessible in control panel. In case of runtime devices disconnection we will get an recently updated information or garbage information for the control

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

unit, where they need more response time to identify the updated info will proper or not. In order to reduce troubleshooting time on run time module issues this concept will provide a solution. Nodes unit data will be store on memory unit for any accuracy comparison between time period and the total data will be updated lively on web server through IP (Internet Protocol) Address. In this paper Temperature, Gas and LDR sensors are connected to Nodes unit of the Raspberry pi board. These sensors data will be store on memory unit for any accuracy comparison between time period and the total data will be updated lively on web server through IP (Internet Protocol) Address. If any sensor disconnected we will get recently updated information or garbage information for the control unit, at that time busier will be on.

Block Diagram:

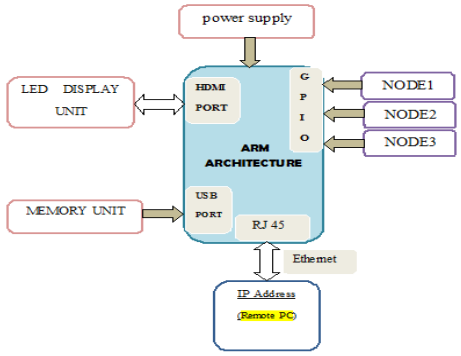

Fig: 1. A Method of Detecting Abnormal Program Behavior on Embedded Devices Block Diagram

IV.HARDWARE IMPLEMENTATION

Raspberry Pi Board:

Fig: 2. Raspberry Pi Board

The Raspberry Pi [7] is a credit-card-sized single-board computer developed in the UK by the Raspberry Pi Foundation with the intention of promoting the teaching of basic computer science in schools. The Raspberry Pi is manufactured in two board configurations through licensed manufacturing deals with Newark element14 (Premier Farnell), RS Components and Egoman. These companies sell the Raspberry Pi online.Egoman produces a version for distribution solely in China and Taiwan, which can be distinguished from other Pis by their red coloring and lack of FCC/CE marks. The hardware is the same across all manufacturers. The Raspberry Pi has a Broadcom BCM2835 system on a chip (SoC), which includes an ARM1176JZF-S 700 MHz processor, Video Core IV GPU, and was originally shipped with 256 megabytes of RAM, later upgraded to 512 MB. It does not include a built-in hard disk or solid-state drive, but uses an SD card for booting and persistent storage.

Raspberry Pi Board features

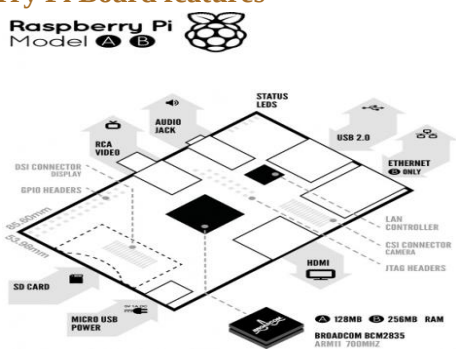

Fig: 3. Raspberry Pi Board features

The Foundation provides Debian and Arch Linux [6] ARM distributions for download. Tools are available for Python as the main programming language, with support for BBC BASIC (via the RISC OS image or the Brandy Basic clone for Linux), C, Java and Perl.

TFT display unit:

TFT stands for Thin Film Transistor, and is a type of technology used to improve the image quality of an LCD. Each pixel on a TFT-LCD has its own transistor

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

on the glass itself, which offers more control over the images and colors that it renders.

While TFT-LCDs can deliver sharp images, they also tend to offer relatively poor viewing angles, meaning they look best when viewed head-on. If you view a TFT-LCD from the side, it can be difficult to see. TFT-LCDs also consume more power than other types of cell phone displays.

Temperature Sensor:

Fig: 4. Temperature Sensor

Temperature sensor is a device which is designed specifically to measure the hotness or coldness of an object.LM35 is a precision IC temperature sensor with its output proportional to the temperature (in °C).With LM35, the temperature can be measured more accurately than with a thermistor. It also possesses low self heating and does not cause more than 0.1 °C temperature rise in still air. The operating temperature range is from -55°C to 150°C.The LM35's low output impedance, linear output, and precise inherent calibration make interfacing to readout or control circuitry especially easy

Light Dependent Resistors:

Fig: 5. LDR

Light dependent resistors are used to re-charge a light during different changes in the light, or they are made to turn a light on during certain changes in lights. One of the most common uses for light dependent resistors is in traffic lights. The light dependent resistor controls a built in heater inside the traffic light, and causes it to recharge over night so that the light never dies. Other common places to find light dependent resistors are in: infrared detectors, clocks and security alarms.

LPG Gas Sensor

Fig: 6. LPG gas sensor

LPG Gas Sensor Module is designed to detect the presence of a dangerous LPG leak in your Home, car or in a service station, storage tank environment by interfacing with Microcontroller without ADC Channels and programming. In this version of LPG Gas sensor module two pots are included, one for trigger level setting and the other for setting sensitivity of the sensor. It allows to determining when a preset LPG gas level has been reached or exceeded.

There are two potentiometers used in Gas Sensor Module. They are as follows:

POT P1:

The on-board POT P1 is used to set tolerance voltage for detecting the LPG presence. When LPG is detected, the OUT pin will be high. This will occurs when the output voltage is greater than the tolerance level set, using the POT P1.

POT P2:

The on-board POT P2 is used to set the sensitivity of the Gas sensor. We recommend you to calibrate the detector for 1000ppm of LPG concentration in air and use value of POT P2 about 20KΩ.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

There are two leads in Gas Sensor Module. They are:
D1: PWR Led. This Green Led indicates the Power input.
D2: STS Led. The red status Led (STS) indicates the various status of LPG Sensor module

Ethernet:

Ethernet LAN Features:

- Bus topology, Wired LAN in IEEE 802.3physical layer standard
- 10 Mbps, 100 Mbps (Unshielded and Shielded wires) and 4 Gbps (in twisted pair wiring mode)
- Broadcast medium-Passive, Wired connections based.
- Frame format like the IEEE 802.2
- SNMP (Simple Network Management Protocol) Open system (therefore allows equipment of different specifications)
- Each one connected to a common communication channel in the network listens and if the channel is idle then transmits. If not idle, waits and tries again.
- Multi access is like in a Packet switched network

V.SOFTWARE REQUIREMENTS

A. Linux Operating System:

Linux [6] or GNU/Linux is software operating for computers. The operating system is a collection of the basic instructions that tell the electronic parts of the computer what to do and how to work. Free and open source software (FOSS) means that everyone has the freedom to use it, see how it works, and changes it. There is a lot of software for Linux, and since Linux is free software it means that none of the software will put any license restrictions on users. This is one of the reasons why many people like to use Linux.

A Linux-based system is a modular Unix-like operating system. It derives much of its basic design from principles established in UNIX during the 1970s and 1980s. Such a system uses a monolithic kernel, the Linux kernel, which handles process control, networking, and peripheral and file system access. Device drivers are either integrated directly with the kernel or added as modules loaded while the system is running.

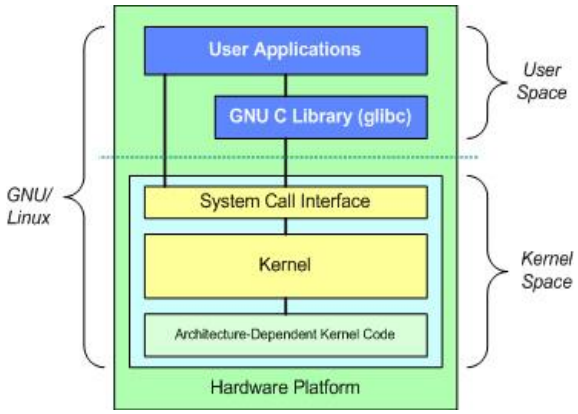

Fig: 7.Architecture of Linux Operating System

B. Qt for Embedded Linux:

Qt [5] is a cross-platform application framework that is widely used for developing application software with a graphical user interface (GUI) (in which cases Qt is classified as a widget toolkit), and also used for developing non-GUI programs such as command-line tools and consoles for servers.

Qt uses standard C++ but makes extensive use of a special code generator (called the Meta Object Compiler, or moc) together with several macros to enrich the language.

Qt can also be used in several other programming languages via language bindings. It runs on the major desktop platforms and some of the mobile platforms. Non-GUI features include SQL database access, XML parsing; thread management, network support, and a unified cross-platform application programming interface for file handling. It has extensive internationalization support.

VI.RESULTS

In this section, we are giving the complete description on the proposed system architecture. Here we are using Raspberry Pi board as our platform. It has an ARM-11

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

SOC with integrated peripherals like USB, Ethernet and serial etc. On this board we are installing Linux operating system with necessary drivers for all peripheral devices and user level software stack which includes a light weight GUI based on XServer, V4L2 API for interacting with video devices like cameras, TCP/IP stack to communicate with network devices and some standard system libraries for system level general IO operations.

The Raspberry Pi board equipped with the above software stack is connected to the outside network and a camera is connected to the Raspberry Pi through USB bus. On the other side we have to host a web server with cloud facility, Temperature, Gas and LDR sensors are connected to Nodes unit of the Raspberry pi board. After connecting all the devices power up the device. When the device starts booting from flash, it first loads the Linux to the device and initializes all the drivers and the core kernel.

After initialization of the kernel it first checks weather all the devices are working properly or not. After that it loads the file system and starts the startup scripts for running necessary processes and daemons. Finally it starts the main application.

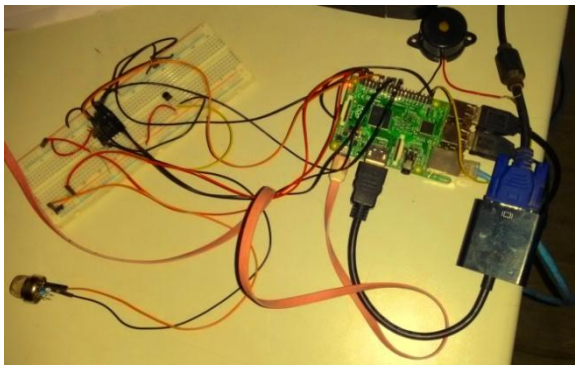

Fig: 8.Rasberry Pi Board Connections

Once the application starts running it first check all the devices and resources which It needs are available or not. After that it checks the connection with the devices and gives control to the user. Then we can enter the program path we can get the sensors output on the LXTerminal window.

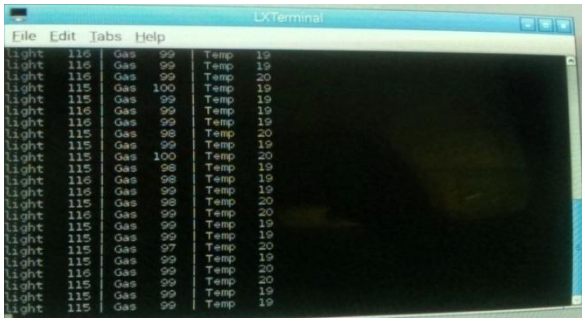

Fig: 9.Sensors Values on LX Terminal Window

IF any sensor is disconnected from the circuit we can get the alert on LXTerminal window. At the same time busier will be on.

Example: If sensor 1 is disconnected we can get Check Sensor 1 alert on the LXTerminal window and sensor 1 get the garbage values.

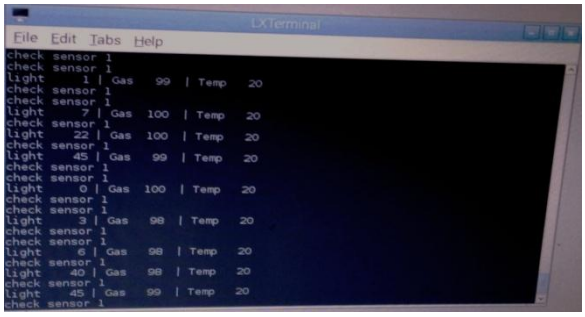

Fig: 10.Identification of Sensor1 (LDR) Disconnection

Enter the ifconfig command on the LXTerminal window we can get internet address. Enter this internet address in another system web browser. At that time we can see the sensors information on that system.

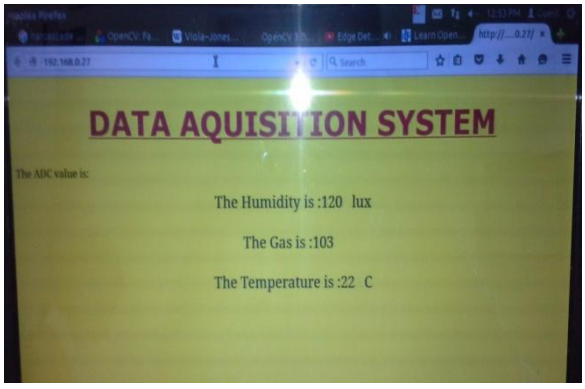

Fig: 10 Data Acquisition System

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

VII.CONCLUSION

The project "A Method of Detecting Abnormal Program Behavior on Embedded Devices" has been successfully designed and tested. It has been developed by integrating features of all the hardware components and software used. Presence of every module has been reasoned out and placed carefully thus contributing to the best working of the unit. Secondly, using highly advanced ARM11 board and with the help of growing technology the project has been successfully implemented.

REFERENCES

[1] D. Arora, S. Ravi, A. Raghunathan, and N. K. Jha, "Secure embedded processing through hardware-assisted run-time monitoring," in Proc. Design, Autom., Test Eur., 2005, pp. 178–183.

[2] D. Arora, S. Ravi, A. Raghunathan, and N. K. Jha, "Hardware-assisted run-time monitoring for secure program execution on embedded processors," IEEE Trans. Very Large Scale Integer. (VLSI) Syst., vol. 14, no. 12, pp. 1295–1308, Dec. 2006.

[3] P. Dongara and T. N. Vijaykumar, "Accelerating private-key cryptography via multithreading on symmetric multiprocessors," in Proc. IEEE Int. Symp. Perform. Anal. Syst. Softw., Mar. 2003, pp. 58–69.

[4] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in Proc. 44th ACM/IEEE Design Autom. Conf., Jun. 2007, pp. 9–14.

[5] Wiki.qt.io.

[6] elinux.org/Processors

[7] www.raspberrypi.org