LETTER

A Lightweight System to Achieve Proactive Risk Management for Household ASIC-Resistant Cryptocurrency Mining

Guoqi LI[†a)], ***Member***

SUMMARY Nowadays, many household computers are used to mine ASIC-resistant cryptocurrency, which brings serious safety risks. In this letter, a light weight system is put forward to achieve proactive risk management for the kind of mining. Based on the system requirement analysis, a brief system design is presented and furthermore, key techniques to implement it with open source hardware and software are given to show its feasibility.

key words: *proactive risk management, cryptocurrency mining, internet of things, rule-based system*

1. Introduction

Although the value and impacts of the cryptocurrency mining are controversial, no one doubt it has been a huge industry, both in terms of economy and technology. Recently, It is estimated that combined annual electricity consumption due to Bitcoin and Ethereum mining is as huge as 80% that of Greece [1].

Cryptocurrency mining can be divided into two kinds: ASIC (Application Specific Integrated Circuits)-allowed and ASIC-resistant. ASIC machines are dedicated hardware for mining and are more powerful, efficient and economical than general purpose computers, but they are limited to unchangeable algorithms. Currently, most of the Bitcoin miners equipped with these machines. On the other hand, ASIC-resistant means the mining must be conducted with general purpose computers. The ASIC-resistance is achieved by applying specifically designed PoW (Proof of Work) algorithms [2]. It is far from conclusion that the ASIC-resistance is necessary, but some cryptocurrency communities insist it firmly. For example, Monero updated its PoW algorithm twice last year (April 6th and October 18th) for the purpose to against the ASIC machines.

Besides using household computers, ASIC-resistant cryptocurrency can also be mined with cloud computing [3] and illegal malware [4]. Due to the computational power of the second method is unstable and the third is limited, the first is dominated and encouraged by the communities. It is not clear how many of this kind of miners exist in the world, but we can estimate that the miners for Monero, which is the most valuable ASIC-resistant cryptocurrency, is from several hundred thousands to millions, according to the pools' information listed in the official website of Monero.

However, There exist many safety threats to mine crytocurrency with household computers. In February 2018, Russia reported a fire accident caused by crytocurrency mining, which finally destroyed several apartments [5]. Usually, the computers for mining are reconfigured to improve yield and save electricity, such as to overlock the frequency of memory and computing units. In most cases, the impact of the reconfigurations have not been evaluated by the hardware manufactures, so it is easy to cause damage to the computers and even lead to serious accidents. Unlike factory buildings or server rooms, home or office usually have insufficient safety equipments and precautions and consequently, the impacts of the possible accidents would be very serious.

So, it is reasonable to apply PRM (Proactive Risk Management) to the household ASIC-resistant crytocurrency mining. The PRM has been explored in depth in healthcare informatics [6] and typically used for senior people or patients [7]. Here we look the computers engaged in mining as weak people in need of special care and attention. In the following section, based on the system requirement analysis, a brief system design will be presented to achieve the PRM for the mining. In Sect. 3, the key techniques to implement the design with open source hardware and software are given to show its feasibility.

2. Safety Requirements and a Brief Design

Briefly the PRM system applied in healthcare is a closed-loop control system, but it is more complicated and adaptive than the traditional ones of the same kind in three aspects. Firstly, it observes the status of all the participant roles, including the living environment, the patients and the medical staff. Secondly, it is capable to control multiple types of devices to affect all the roles respectively. Lastly, it can make decisions needed to drive the system based on knowledge integration from several fields. In this section, we would like to design a similar PRM system for the household cryptocurrency mining. Due to the different participant roles, the system has specific safety requirements and consequently, specific design challenges.

The primary failure mode of the household ASIC-resistant cryptocurrency mining is the overheat of the electric lines or the computers, caused by long time and high workload and consequently, beyond the carrying capacity

Manuscript received October 26, 2018.
Manuscript revised February 24, 2019.
Manuscript publicized March 20, 2019.

[†]The author is with Science and Technology on Reliability and Environmental Engineering Laboratory, School of Reliability and System Engineering, Beihang University (BUAA), Beijing China.
a) E-mail: gqli@buaa.edu.cn

DOI: 10.1587/transinf.2018EDL8227

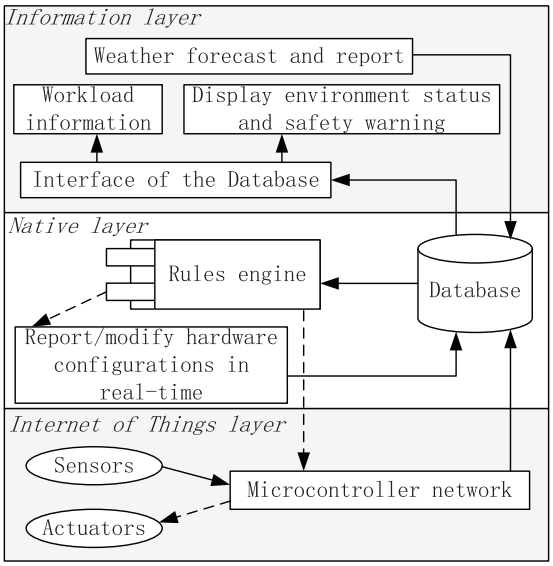

Fig. 1 The schematic diagram of the brief design for the PRM system. The solid lines mean data flow, while the dotted lines refer to control flow. Arrows point to data consumers or control targets respectively.

of the environment. So, the PRM system must be qualified with two functions: have the abilities to predict, monitor and regulate both the environment and the status of the computers in realtime; can recognize potential risks and prevent them in advance by comprehensively applying the abilities mentioned above.

From the technique point of view, there are two difficulties to design the system: components from multiple hardware and software layers must be well integrated and leveraged; the decision-making component, responsible for predicting potential risks and taking proactive measures, must be flexible enough to meet the personalized requirements. Additionally, we must ensure that the introduction of the PRM system will not bring new security and safety problems.

Figure 1 shows a brief design for the system, which has three layers: The top is the information layer and the components in this layer can be deployed in the cloud containers for high reliability as well as deployed in the localhosts; The middle is the native layer and the components must be installed on the localhosts; For the IoT (Internet of Things) layer, it is a microcontroller network with several sensors and actuators to perceive and regulate the indoor environment, control electric power and etc..

To clarify the operation of the system, let's analyze the data flow and the control flow, illustrated in Fig. 1.

From the view of the data flow, there are three data sources located at each of the layers respectively: From the bottom up, the first is the measurements of the sensors, such as temperature, humidity, air quality, electricity consumption and etc.; The second is the report of the current hardware configurations of the computers, especially the computing units; The last is the weather forecast and reports obtained from the Internet. There exist two data consumers: the rule engine is responsible for making decisions of how to configure the computers and how to regulate the environment; the other is interfaces of the database exposed to the top layer to display the status of the environment and possible warning information, as well as to provide workload information of the computers.

The control flows are both originated from the rules engine. For the two ends of the flows, one is the actuators at the base layer, such as relays to control electric power and infrared remote control for air conditioners and etc.. The other is at the middle layer and it can modify the hardware configurations of the computers in real-time.

The components in the base and top layers are easy to understand, while two components in the middle layers need further explanation:

- "Report/modify the hardware configurations in real-time" in the middle layer: For instance, it can change the frequency of memory or close some CPU (Central Processing Unit) cores. Typically the component is implemented with shell script language and execute with root authority. The modifications are achieved by calling operating system commands or interfaces of overclocking software tools.
- "Rules engine" and "Database" in the middle layer: Both the two components are security critical: the former is responsible for making decisions, which further drive the actuators to regulate the environment and invoke functions to modify the configurations; The later stores data from sensors of the rooms, which are very private. Consequently, they should be deployed to an appointed localhost or even a specified IPC (Industrial Personal Computer), instead of the cloud containers. Obviously, this introduces a single point of failure, but it is worth it in the interests of the security.

The design manages to overcome the two difficulties mentioned above by applying the three layer architecture and the rule-based decision-making mechanism respectively. It is easy to figure out that the system designed in this section has the same features with the PRM system described at the beginning of this section, but it uses deferent techniques.

3. Key Techniques for a Concrete Implementation

Table 1 lists the recommended hardware to build the system. For the IoT layer, there are two kinds of nodes, which are both described in details in the table. Typically, one primary node and several secondary nodes are connected to the IPC respectively. The primary node connects to the IPC with wired LAN (Local Area Network), while the Second nodes link to the IPC with WiFi (Wireless Fidelity). Since wired LAN is more reliable than WiFi, safety critical functions should be assigned to the primary node as much as possible.

For a normal scale system, we may need one IPC, one Primary IoT node and four secondary IoT nodes. It is estimated that all the hardware can be get in less than 1000

Table 1 Recommended open source hardware to construct the system.

Node name	Microcontroller board	Sensors	Actuators and their functions
Primary IoT node	Arduino Mega 2560, Arduino W5100 Ethernet Shield	Electric current sensor detection module	Relay Module is used to control electric power
Secondary IoT node	WeMos D1 WiFi (Arduino compatible) or Arduino UNO	DHT11 (temperature and humidity sensor)	Infrared encoding and transmitting module is used to control air conditioners
IPC	Raspberry Pi 3B+	–	–

USA dollars in most of the world, so cost is not a problem.

For the software of the nodes, all the functions, no matter for data acquisition or reactors control, are implemented in the form of web services. It is easy to get by slightly modifying an Aduino official example program. Furthermore, the simplicity of the framework helps to ensure safety and reliability.

Most of the components in the middle layer of the framework are deployed on the IPC and could be implemented by the following steps:

1. Deploy the MySQL database and create necessary data tables. Furthermore, we should map the port of the database server from the local IP to a public IP, no matter through router or VPN;
2. A Python script is used to periodically visit the web services on the microcontrollers. Fetch the measurements of the sensors and record them to the database;
3. We use CLIPS as a rule engine and design a shell for it. There are two key points for the implementation of the shell. Firstly, turn the newest data, retrieved from the database, to facts and assert them before "run" command. Secondly, provide two sets of custom functions for actions of the rules: one could visit the web services on the microcontrollers mentioned above to operate the reactors; the other could call operating system commands and the interface of the overlocking software tools on the target computers to modify configurations though SSH (Secure Shell) tunnels.
4. Last but not least, give rules according to personalized requirements. For example, two rules are listed in the following. For legibility, we use pseudocode but not CLIPS, which is similar to Lisp and difficult to read.

```
IF current_weather IS sandstorm
    THEN close the ventilation system
    AND heat dissipation condition
        IS poor

IF heat dissipation condition IS poor
AND the indoors temperature > 30
    THEN descend the frequency of
        video memory to 80%
    AND close 50% CPU cores
    AND restart related workloads
```

As indicated above, the MySQL database server has a public address, so it can be visited globally. Thus far, the components in the top layer are easy to be implemented.

Let's review the two rules mentioned above. In sandstorm days, the ventilation system will be closed to prevent dusk pollution. Under this conditions, if the indoor temperature is higher than a threshold, the mining computers would be degraded and reduce workloads to avoid potential system crash. Note that to operate the computers in a degraded manner is better than totally shut down and additionally, the process is automatic without manpower. These are another two advantages we could benefit from the PRM system.

4. Conclusion and Future Works

In this letter we reveal a potential safety problem in cryptocurrency mining and briefly design a light weight system to achieve PRM for it. Furthermore, a concrete implementation shows the design is feasible with low cost open source hardware and software.

As shown in the previous section, the rules and quantized parameters in the rules for decision-making are usually case specific, and at the same time, it takes time and considerable resources to obtain them. So we plan to study Automatic rules acquisition through machine learning to fuel the application in the future works.

Acknowledgments

This work was supported by a grant from the Science and Technology on Reliability and Environmental Engineering Laboratory of China (No.6142004180401).

References

[1] S. Wimbush, "Cryptocurrency mining is neither wasteful nor uneconomic," Nature, vol.555, no.7697, pp.443–443, 2018.
[2] A.R. Zamanov, V.A. Erokhin, and P.S. Fedotov, "Asic-resistant hash functions," 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, pp.394–396, 2018.
[3] D.J. Sandler, "Citrus groves in the cloud: Is cryptocurrency cloud mining a security?," Santa Clara High Technology Law Journal, vol.34, no.3, pp.250–289, April 2018.
[4] H. Tuttle, "Crypto jacking: How hackers steal resources to mine digital gold," Risk Management, vol.65, no.7, p.6, Aug. 2018.
[5] David, "Cryptocurrency mining causes a fire incident in russia," https://coinpedia.org/news/cryptocurrency-mining-causes-a-fire-incident-in-russia/, accessed Feb. 10, 2018.
[6] S. Tomforde, T. Dehling, R. Haux, D. Huseljic, D. Kottke, J. Scheerbaum, B. Sick, A. Sunyaev, and K.H. Wolf, "Towards proactive health-enabling living environments: Simulation-based study and research challenges," Proc. 31st International Conference on Architecture of Computing Systems, pp.155–162, 2018.
[7] L.-B. Chen, W.-J. Chang, K.-M. Lee, C.-W. Huang, and K.S.-M. Li, "A comprehensive medicine management system with multiple sources in a nursing home in Taiwan," IEICE Trans. Inf. & Syst., vol.E99-D, no.6, pp.1447–1454, 2016.