Secure Disposable Computing Technology for Low-end Embedded Devices

Sieun Kim
SysCore Lab
Sejong University
Seoul, South Korea
rlatldms2004@naver.com

Dowon Hong
Dept. of Applied Mathematics
Kongju National University
dwhong@kongju.ac.kr

Ki-Woong Park*
SysCore Lab
Sejong University
Seoul, South Korea
woongbak@sejong.ac.kr

***Abstract*— Low-end embedded devices are manufactured in large quantities at low cost in the factory and widely distributed for a variety of purposes. These low-end embedded devices are difficult to include robust security mechanisms due to cost issues. Therefore, in the case of low-end embedded devices that be used in a short period of time and discarded or be periodically replaced, self-destructive techniques are more effective. We investigate existing self-destructing researches for embedded devices to find disposable computing technologies that can be applied to low-end embedded devices. We also will discuss to apply disposable computing technology to low-end embedded devices.**

Keywords— disposable computing; self-destruction; low-end embedded device

I. Introduction

Low-end embedded devices are produced in large quantities at low cost and widely deployed. Low-end embedded devices mean devices which are used for a short period of time and then periodically replaced. These devices can also be called disposable computers. These devices usually do not include security mechanisms because they are usually used for a short period of time and then replaced by other devices.

Therefore, it is better to develop a technology that securely discards the devices rather than applying a security mechanism to low-end embedded systems. Technologies to securely discard devices can be implemented through software or hardware, but software approaches are excluded for several reasons. To execute secure erasure of data stored in device through a software approach, it must be possible to verify the execution of the operation. However, in the case of

low-end embedded devices, it is difficult to prove execution of operation because of the absence of operation module such as a cryptographic accelerator to guarantee operation. A software approach can simply destruct system by breaking the boot loader and causing a device bricking and so on. But, such software-approaches are the possibility of being recovered. Fig. 1 represents advantages of hardware-approaches of secure disposable computing system.

For above reasons, this paper examines the hardware approach that can securely discard low-end embedded devices. Even though the encryption algorithms normally included in security mechanisms are broken, a hardware approach is valid security mechanisms and eliminates the possibility of the abandoned device being used. We examine the researches achieving these objectives, discuss to apply them to low-end embedded devices, and propose the direction to develop security mechanisms that securely disca`rd devices.

We analyze the existing research in Section 2 and analyze the limitations of the related research in Section 3. In last Section, we present the development direction of the technology.

II. Analysis on Existing Disposable Computing Technology

We investigate existing disposable computing technology (as known as self-destructive technology) to find disposable computing technology that can be applied to low-end embedded devices. Our Investigation focused on research that can destroy the computer system itself without including

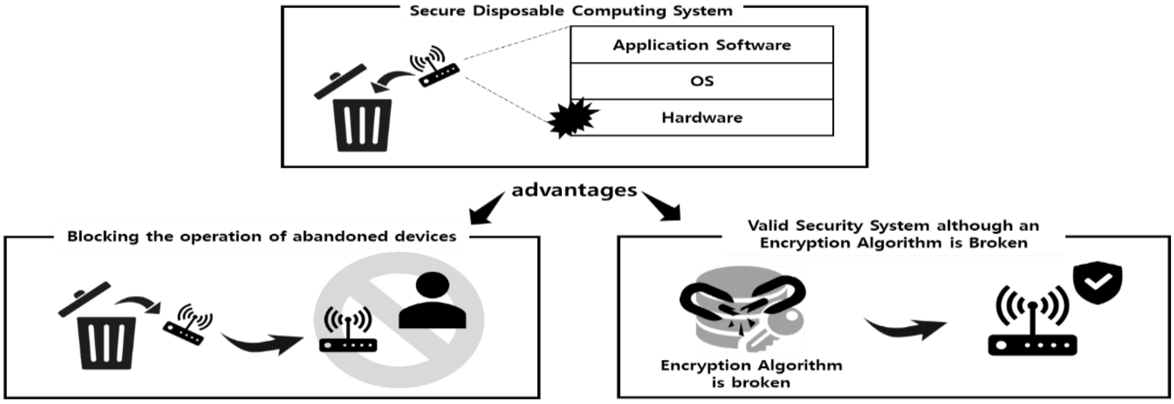
Secure Disposable Computing System
Application Software
OS
Hardware
advantages
Blocking the operation of abandoned devices
Valid Security System although an Encryption Algorithm is Broken
Encryption Algorithm is broken

Fig. 1. Advantages of Secure Disposable Computing System

*: Corresponding author

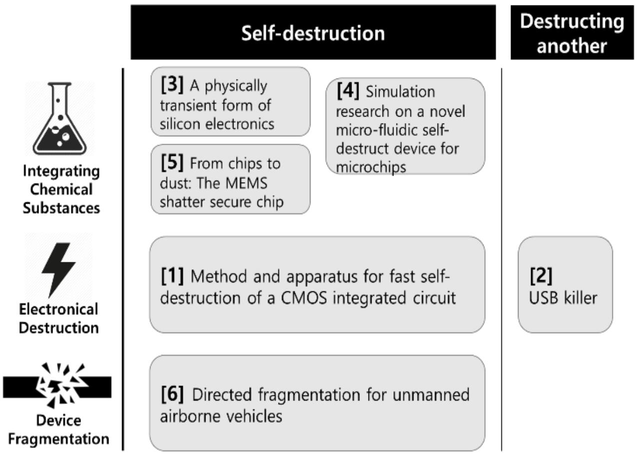
Self-destruction
Destructing another
Integrating Chemical Substances
[3] A physically transient form of silicon electronics
[4] Simulation research on a novel micro-fluidic self-destruct device for microchips
[5] From chips to dust: The MEMS shatter secure chip
Electronical Destruction
[1] Method and apparatus for fast self-destruction of a CMOS integrated circuit
[2] USB killer
Device Fragmentation
[6] Directed fragmentation for unmanned airborne vehicles

Fig. 2. Outline of Disposable Computing Technology

researches that simply destroy storage devices such as flash memory. Also, the software approach of disposable computing is not included in our investigation to benefit from the hardware approach of disposable computing technology. Fig. 2 represents roadmap of related researches that we investigated.

A long time ago, a method of destroying hardware by giving the computer device electronically unacceptable big power has been studied [1,2]. David J. Shield and Derek L. Davis invented a self-destructive circuit [1]. A self-destructive circuit attaches a switch pad with state change to the chip, and when the self-destruction is triggered, it changes the state of the switch to induce a latch-up of the semiconductor device, causing the device to break with unacceptable big power. A Russian security researcher nicknamed Dark Purple has developed a USB killer product that electronically destruct embedded devices by emitting big power collected through multiple capacitors at a time [2]. This product is not a self-destructive technology, but we have included it in our investigation because there are factors that can be applied to hardware destruction technology. Plugging the USB killer into a normally functioning computer system will cause the device to be electrically destroyed by a large amount of current, resulting in a hardware corruption of the embedded system.

There is a way to destruct a computer system by inserting or integrating chemical substances into hardware. Suk-Won Hwang et al. has studied how a chip absorbed in the body can be safely destroyed for medical purposes [3]. They use circuit components whose operational characteristics match those of non-transient counterparts formed in the usual way on silicon wafer substrates. When we add a chemical substance and trigger self-destruction, the chip is dissolved by the chemical substance. In addition, Gu Xinwei, et al. also add chemical substances to dissolve the chip to destroy the device [4]. There is a method of using mechanical stress instead of dissolving chips as described above. N. Banerjee et al. announced a chip that contains a chemical substance that creates stress [5]. When triggered to activate this chemical material, it creates a high level of stress on the chip and destructs the chip like as dust.

Like Amazon's patent [6], you can fragment your hardware. In the developed patent on drones, the flying drone recognizes that it must be destroyed and calculates the geographical factors that do not cause human injury, thus safely fragmenting the device itself. At this time, fragments of the drones are dropped into the water and the hardware of devices are destroyed.

III. Discussion of Related Work

This section begins a discussion on applying investigated securely discarding systems to low-end embedded devices. Our objective in this section is to find methods to efficiently handle large amounts of low-end embedded devices through existing research.

Some of researches investigated in the Section 2 are not aimed at securely destruction of embedded devices in aspects of information security. For example, a Suk-Won Hwang's research [3] aims at harmless mechanisms in the human body for medical purposes, even if devices are self-destructed. Because these researches are aimed at different objectives than what we are trying to achieve, they are hard to apply because of the cost side in low-end embedded devices.

USB killer [2] destructs the device by plugging the USB into the device. In other words, to apply the technology to the low-end embedded device and destroy the hardware, you must plug in the USB for every device you want to discard. Due to the nature of low-end embedded devices that are produced in large quantities and discarded within a short period of time, there is an inefficiency in applying the technology. Also, you can choose USB killer to destroy your device, but techniques to defend USB killer have been developed. However, the technology we want to find is a technology that destroys low-end embedded devices with little or no security technology, so this is not an obstacle to applying this technology to low-end embedded devices. The last thing to discuss of USB killer is cost and availability. The USB killer can be treated as a terrorist's weapon so is currently difficult to purchase. And you have to pay $ 60 to make a purchase. Therefore, you must decide how many low-end embedded devices you want to destroy and consider them in a cost-effective way.

In the case of explosion or dissolution of chips using chemical substances, there is a problem of stability and coverage due to the inclusion of explosive substances [4]. There is a risk that explosive chemicals will destroy components that should not be destroyed by unintentional explosions, or that small fires can occur. Therefore, there are limitations in applying this technology. Costs must also be considered in terms of including chemical substances [5].

In the case of drone’s self-fragmentation patent [6], the technology coverage is limited because the flying drones fall down and the hardware destruct. For self-destruction, the device must be used in high altitude air.

The last point to be discussed is that most of the studies investigated in Section 2 must go through the manufacturing process. This is disadvantageous in terms of cost, but it is an inevitable choice in terms of enhancing security. Because the technology we are looking for is a hardware destruction of embedded devices, we need a hardware approach rather than a software approach. If there is a cost-effective way to destroy many embedded devices without going through the manufacturer's process, we can apply it, but to our knowledge, such a method does not exist. Therefore, manufacturers manufacturing low-end embedded devices must actively adopt security technologies in view of security considerations.

IV. Conclusion

Low-end embedded devices are vulnerable to attack because they do not have strong security mechanisms, and because they are cheap, it is more efficient to replace them with other devices periodically rather than defending them. So, we discussed how to securely discard low-cost embedded devices. Although disposable computing is a concept that has been known for a long time, there is a difficulty in applying each one of these above works to securely destroy low-end embedded devices. Therefore, our future work is about how to securely destroy low-end embedded devices in a secure manner.

Acknowledgment

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (NRF-2017R1C1B2003957, NRF2016R1A4A1011761).

References

[1] D. J. Shiel and D. L. Davis, “Method and apparatus for fast self-destruction of a CMOS integrated circuit,” US Patent application number 581436, Intel Corporation. Santa Clara. CA. April 1998.

[2] USB killer v2.0, http://habrahabr.ru/post/268421/, unpublished

[3] Hwang, Suk-Won, et al, "A physically transient form of silicon electronics.", Science 337.6102: 1640-1644, 2012.

[4] Gu Xinwei, et al, "Simulation research on a novel micro-fluidic self-destruct device for microchips.", Nano/Micro Engineered and Molecular Systems (NEMS), 2010 5th IEEE International Conference on. IEEE, 2010.

[5] Banerjee, N., et al, "From chips to dust: The MEMS shatter secure chip.", Micro Electro Mechanical Systems (MEMS), 2014 IEEE 27th International Conference on. IEEE, 2014.

[6] [Mishra, Pragyana K., Goyal, Dushyant, “Directed fragmentation for unmanned airborne vehicles”, US Patent 9,828,097, 2017

[7] Pandey, Shashank S., and Carlos H. Mastrangelo, "An exothermal energy release layer for microchip transience.", SENSORS, 2013 IEEE. IEEE, 2013.

[8] Banerjee, Niladri, et al, "Microfluidic device for triggered chip transience.", SENSORS, IEEE, 2013.

[9] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,”, IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987.