IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 9, Issue 3 Ver. VI (May – Jun. 2014), PP 24-30
www.iosrjournals.org

Self Destructing Electronics

Poluka Srilatha
Department of Electronics and Communication Engineering, Sree Vidyanikethan Engineering College(Autonomous), (Affiliated to JNTU, Anantapur), Sree Sainath Nagar, Tirupathi, India.

Abstract: *Self-destruct is a mechanism that can cause a device to destroy itself under a predefined set of circumstances. Self-destruct mechanisms are found on devices and systems where malfunction could endanger large numbers of people. Defence advanced research projects agency (DARPA) is an agency of the United States Department of Defense (DoD) responsible for the development of new technologies for use by the military. DARPA announces the Vanishing Programmable Resources (VAPR) program with the aim of revolutionizing the state of the art in transient electronics.*
DARPA's latest initiative involves the development and manufacturing of electronics, including those for remote sensing and communication, which will be able to self-destruct on command. DARPA has already created transient electronics that vanish in water, with the idea that an injured solider can swallow the device after an injury and it will kill dangerous bacteria, fight infection, and be absorbed harmlessly into the body. These electronics, DARPA suggests, could be used for environmental monitoring and simplified diagnosis, treatment, and health monitoring in the field.
Keywords*: battery, electronics, ssd data security, unhackable drive, VAPR IC*

I. Introduction

Sophisticated electronics can be made at low cost and are increasingly pervasive throughout the battlefield. Large numbers can be widely proliferated and used for applications such as distributed remote sensing and communications. However, it is nearly impossible to track and recover every device resulting in unintended accumulation in the environment and potential unauthorized use and compromise of intellectual property and technological advantage.

The Vanishing Programmable Resources (VAPR) program seeks electronic systems capable of physically disappearing in a controlled, triggerable manner. These transient electronics should have performance comparable to commercial-off-the-shelf electronics, but with limited device persistence that can be programmed, adjusted in real-time, triggered, and/or be sensitive to the deployment environment.

VAPR seeks to enable transient electronics as a deployable technology. To achieve this goal, researchers are pursuing new concepts and capabilities to enable the materials, components, integration, and manufacturing that will realize this new class of electronics.

Transient electronics may enable a number of revolutionary military capabilities including sensors for conventional indoor/outdoor environments, environmental monitoring over large areas, and simplified diagnosis, treatment, and health monitoring in the field. Large-area distributed networks of sensors that can decompose in the natural environment (eco-resorbable) may provide critical data for a specified duration, but no longer. Alternatively, devices that resorb into the body (bio-resorbable) may aid in continuous health monitoring and treatment in the field.

II. Headings

1 Electronics
- 1.1 Definition
- 1.2 Electronic devices and component

2 Self Destructing Electronics
- 2.1 Definition

3 Self Destructing Electronics
- 3.1 Invincible SSD Data security
  - 3.1.1 Introduction to SSD
  - 3.1.2 RUNCORE SSD
- 3.2 Self destructing BOEING spy phone
- 3.3 Self destructing batteries

3.4 Unhackable drive detecting attacks

4 Conclusion

III. Figures

1. Electronics

1.1 DEFINITION :

Electronics deals with electrical circuits that involve active electrical components such as vacuum tubes, transistors, diodes and integrated circuits, and associated passive interconnection technologies. Commonly, electronic devices contain circuitry consisting primarily or exclusively of active semiconductors supplemented with passive elements ; such a circuit is described as an electronic circuit. Today, most electronic devices use semiconductor components to perform electron control.

1.2 Electronic Devices And Components :

An electronic component is any physical entity in an electronic system used to affect the electrons or their associated fields in a manner consistent with the intended function of the electronic system. Components are generally intended to be connected together, usually by being soldered to a printed circuit board (PCB), to create an electronic circuit with a particular function (for example an amplifier, radio receiver, or oscillator). Components may be packaged singly, or in more complex groups as integrated circuits.

Heat generated by electronic circuitry must be dissipated to prevent immediate failure and improve long term reliability. Techniques for heat dissipation can include heat sinks and fans for air cooling, and other forms of computer cooling such as water cooling. These techniques use convection, conduction, and radiation of heat energy.

Electronic noise is defined as unwanted disturbances superposed on a useful signal that tend to obscure its information content. Noise is not the same as signal distortion caused by a circuit. Noise is associated with all electronic circuits. Noise may be electromagnetically or thermally generated, which can be decreased by lowering the operating temperature of the circuit. Other types of noise, such as shot noise cannot be removed as they are due to limitations in physical properties.

These electronics find a variety of applications in this modern world. They are of immense value in military and security oriented applications. It is nearly impossible to track and recover every [electronic] device [on the battlefield], resulting in unintended accumulation in the environment and potential unauthorized use and compromise of intellectual property and technological advantage. So here we have an alternate.

2. Self Destructing Electronics

2.1 DEFINITION :

Electronics (transient electronics) capable of dissolving into the environment around them when triggered under a predefined set of circumstances are defined as self destroying electronics.

Transient electronics developed under VAPR should maintain :

1. Current functionality.
2. Ruggedness of conventional electronics.
3. When triggered, be able to degrade partially or completely into their surroundings.
4. One such example of a vanishing programmable resource is

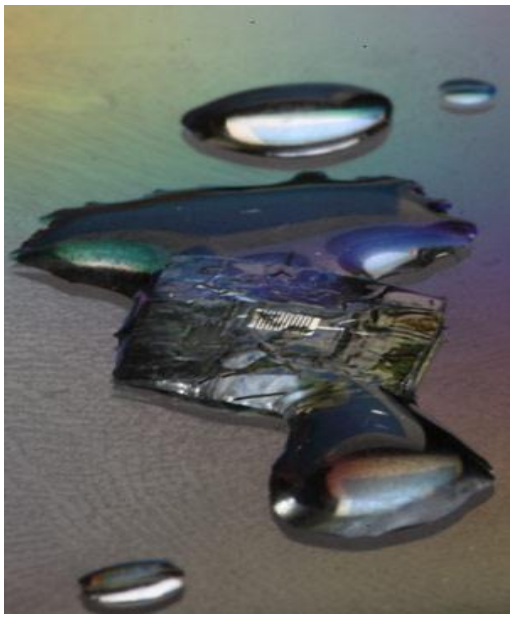

Fig 2.1 A VAPR IC vanishing into water droplets.

3. Selfdestructing Electronic Devices

3.1 Invincible Ssd Data Security

3.1.1. Introduction To Ssd:

A solid-state drive (SSD) (also known as a solid-state disk or electronic disk, though it contains no actual "disk" of any kind or motors to "drive" the disks) is a data storage device using integrated circuit assemblies as memory to store data persistently. SSD technology uses electronic interfaces compatible with traditional block input/output (I/O) hard disk drives, thus permitting simple replacement in common applications. Also, new I/O interfaces like SATA Express are created to keep up with speed advancements in SSD technology.

SSDs have no moving mechanical components. This distinguishes them from traditional electromechanical magnetic disks such as hard disk drives (HDDs) or floppy disks, which contain spinning disks and movable read/write heads. Compared with electromechanical disks, SSDs are typically more resistant to physical shock, run silently, have lower access time, and less latency.

Fig 3.1 Samsung flash ssd with 128GB memory

As of 2010, most SSDs use NAND-based flash memory, which retains data without power. For applications requiring fast access, but not necessarily data persistence after power loss, SSDs may be constructed from random-access memory (RAM). Such devices may employ separate power sources, such as batteries, to maintain data after power loss.

3.1.2. RUNCORE SSD:

The RunCore InVincible is a solid-state drive that comes with two data destruction modes : one that permanently erases data, and one that destroys the physical flash chips.

Fig 3.2 SSD with built-in data destruction

Chinese storage device maker RunCore recently announced the global launch of its solid state drive (SSD) called InVincible, which has a physical self-destruction mechanism designed to prevent sensitive data from

being recovered. Though the RunCore InVincible SSD is hardly something a typical small business will require, it has applications within the Defense industry and other fields where the protection of highly-sensitive information is of paramount importance.

At its core, the InVincible SSD offers relatively mediocre performance of 240MB/s read and 140MB/s write over a SATA II interface. Unlike a standard SSD, the drive ships with a standard SATA interconnect that includes additional sets of cables leading off to two buttons that are colour coded red and green. Clicking the green button will initiate an "intelligent" destruction function, while depressing the red button will trigger a permanent physical destruction. Both features essentially offer a quick way of wiping onboard data without having to deploy specialized tools or software.

Intelligent destruction is essentially a fast erase procedure that overwrites the entire SSD by writing a "1" into each cell to wipe all data. The speed of this operation depends on the total capacity of a drive and the flash memory type used in a particular SSD; the documentation attributes it at more than 2.5 GB/s and lists 13 seconds required to wipe a 32 GB SSD, 25 seconds for a 64 GB SSD, and 50 seconds for a 128 GB SSD. The InVincible SSD can be put back into normal use after recreating the data partitions and formatting it with standard disk management tools.

Physical destruction is achieved by a high voltage and high current in a short time using a "voltage boost circuit," with NAND flash chips targeted one at a time. The destruction procedure takes 10 seconds to destroy the SSD controller and storage media; this suggests that it may be possible to extricate some data off from the NAND chips if power is disrupted within this window of time. The RunCore documentation recommends a reboot to ensure that data still in computer memory is also eradicated.

There is the option of MLC or SLC flash memory, and survivability in different temperatures can be specified. The Ultimate version of the InVincible SSD will work at temperatures ranging from -40 to 85 degrees Celsius (-40 to 176 degrees Fahrenheit), and the Industrial Grade version of the InVincible SSD will work from -20 to 70 degrees Celsius (-4 to 158 degrees Fahrenheit).

A 64 GB Ultimate version of the InVincible SSD with MLC NAND (RCV-III-S2564-M8D) costs $1,200 for low order quantities. There's no pricing information for the Industrial Grade version at this time.

3.2. Self Destructing Boeing ‘Black ‘ Spy Phone:

Boeing unveiled a smart phone that appears to come straight from a James Bond spy movie. Designed for secure communication between governmental agencies and their contractors, Boeing Black can self destruct if it is tampered with, destroying all the data on it.However, the phone is so secure that Boeing will only sell it to ‘approved’ purchasers.

According to Boeing’s spec sheet, the Black is 5.2-inches tall, with a 4.3-inch, 540 x 960 display, and weighs 170 grams. It features three bands of LTE, as well as antennas for WCDMA and GSM. Running it all are dual 1.2 GHz ARM Cortex-A9 CPUs and Google‘s Android, which Boeing says will work “just the way you’d

expect." The hardware itself is being assembled in the US, and can be expanded from its back panel to work with biometric scanners, satellite transceivers, solar chargers, and other accessories.
"Any attempt to break open the casing of the device would trigger functions that would delete the data and software contained within the device and make the device inoperable."

Fig 3.3 Self destructing Boeing "Black" spy phone

Made in the United States, the phone runs on Google Inc's (GOOG.O) Android operating system. The 5.2-by-2.7-inch handset, slightly larger than an I-Phone, uses dual SIM cards to enable it to access multiple cell networks instead of a single network like a normal cell phone.

Most of the documents in the filing are confidential, but the limited images do show that the Boeing "Black" has dual SIM cards, and a variety of options for connectivity, including LTE.
Due to the phone's security features, Boeing is releasing few details about the wireless network operators or manufacturer it is working with, and has not provided a price or date by which the phone might be widely available, but said it has begun offering the phone to potential customers.

3.3. Self Destructing Batteries

Considering that batteries are typically designed for maximum longevity, it may seem odd to learn that the U.S. Defense Advanced Research Projects Agency (DARPA) is ramping up research into self-destructing batteries.

Odd or not, DARPA awarded a $4.7 million contract last week to SRI International, an independent research organization based in Menlo Park, to develop a transient power supply that, when triggered, becomes unobservable to the human eye.

More specifically, SRI International will design a vanishing silicon, air battery for use by DARPA customers.

Fig 3.4 self destructing battery

The military's rationale for developing such a battery is more persuasive than many people may realize. The U.S. Army has begun deploying a stream of advanced battlefield electronics for soldiers, including next-generation fused thermal and night vision goggles, more accurate laser targeting systems and devices for generating electrical power in the field.

These applications are only the start. Soon, the Army could be deploying computerized, numerically controlled 3-D printing machines in mobile shipping containers, which could be used to create and "print" physical solutions to specific problems encountered in the field.

One factor that could prevent deployment of these new capabilities is the inability to control assets after they've entered the battle space. Equipment can be lost or captured by enemy forces. Sooner or later, the cat will get out of the bag – unless the bag is designed to self-destruct.

That capability is the objective of DARPA's Vanishing Programmable Resources (VAPR), which is developing embedded computing and other electronic components able to decompose into the surrounding environment when no longer needed.

"DARPA is looking for a way to make electronics that last precisely as long as they are needed," says Alicia Jackson, the VAPR program manager at DARPA. "The breakdown of such devices could be triggered by a signal sent from command or any number of possible environmental conditions, such as temperature."

Once triggered to dissolve, these electronics would be useless to any enemy who might come across them. In early December, Honeywell Microelectronics & Precision Sensors won a $2.5 million contract from DARPA to pursue transient electronics for military and medical applications.

3.4. Unhackable Drive Detecting Attacks

The Slim and Slim Duo (two USB heads in one unit) have an automatic self-destruct feature. The devices are capable of detecting brute force attacks— malicious programs that run through thousands of passwords in seconds with the goal of gaining entry to password-protected data—and then destroying the data stored on devices.

When the flash drive's system senses that an invader is getting close to determining the correct password, it triggers an electrical overload in the unit, much like blowing a fuse. All data is then lost. In addition to requiring a password to access stored data, the drives encrypt incoming files to protect against someone who knows the password to the device, but should not read the stored material.

The single drive is available with 4 GB, 8 GB, 16 GB, 32 GB and 64 GB of storage. The double drive consists of two 64 GB units in one casing.

Fig 3.5 Unhackable drive detecting attacks with self destruct mechanism

When the flash drive's system senses that an invader is getting close to determining the correct password, it triggers an electrical overload in the unit, much like blowing a fuse. All data is then lost. In addition to requiring a password to access stored data, the drives encrypt incoming files to protect against someone who knows the password to the device, but should not read the stored material.

The single drive is available with 4 GB, 8 GB, 16 GB, 32 GB and 64 GB of storage. The double drive consists of two 64 GB units in one casing. The 128 GB dual drive is capable of storing 14.6 years worth of uninterrupted music, 50,000 photos taken with a 10-megapixel camera or 18 full length HD movies, according to a VSA statement. Waterproof, shock-resistant and TSA-approved, the flash drives are available online from Swiss Knife Shop, Amazon, B&H Photo and Data vision, starting at $46.

IV. Conclusion

These electronics, DARPA suggests, could be used for environmental monitoring and simplified diagnosis, treatment, and health monitoring in the field. Now, the idea and purpose of these electronic devices are clearly defined and will quite obviously serve a very specific and important purpose.

References

[1] http://www.gizmodo.in/science/Self-Destructing-Electronics-Are-Here-and-They-Are- Awesome/articleshow/33517895.cms
[2] http://gizmorati.com/2014/02/27/boeing-reveals-selfdestructing-black-spy-phone/
[3] http://phys.org/news/2014-03-electronics-press-on-tattoo.html
[4] http://www.techrepublic.com/blog/asian-technology/runcore-debuts-ssd-with-built-in-data-destruction/
[5] http://searchcio.techtarget.com/definition/self-destructing-email