# Cool RAM: Prolonging memory decay to perform cold boot attacks (Proposal)

-An Attack Against IoT Devices-

Gordon Deacon
School of Design and Informatics
Abertay University
DUNDEE, DD1 1HG, UK

## ABSTRACT

**Context:** Many people would think that, when a computer system, has a loss of power, the contents of RAM (Random Access Memory) would also be susceptible to this loss of power, causing the loss of data. This is not the case, where data can retain for multiple seconds, or even minutes after the device has lost power. This can lead to sensitive information being stolen through the process of a cold-boot attack.

**Aim:** To determine whether newer IoT devices, such as but not limited to, the Raspberry Pi 3 and 4, are susceptible to cold-boot attacks, where the RAM can be recovered, even after power has been removed.

**Method:** A Raspberry Pi device will be examined to determine if the cold-boot attack is possible on the newer IoT devices. An image will be loaded into RAM, and a copy will be kept original. The RAM chip will be frozen with an air-duster can. The SD card will then be swapped with the attackers, to load into a custom operating system where the attacker can read the contents of memory. The attacker can then search for where the image was placed within RAM, which will then allow the attacker to compare the data recovered, to the original image. This will then give a percentage of how successful the attack was.

**Results:** If the image recovered for the cold-booted RAM was identical to the original image, then it can be determined that the attack was successful. Considering the attack was previously successful on an older model of the device with a similar boot sequence, the probability of the attack being successful is high.

**Conclusion:** The newer IoT devices should be dispatched with higher security, as they are further developed with every iteration of release. Being able to determine if the newer models are vulnerable, will allow for future models of the devices to have a better consideration when it comes to hardware security.

## Keywords

Cold-boot, IoT, Remanence effect, Hardware security

## 1. INTRODUCTION

Most people will know that modern computing devices contain a memory module called Random Access Memory (RAM). This memory module contains capacitors that represent either a 1 or 0. All of these 1's and 0's represent data that is present in the live running machine. This can be anything from running code, temporary variables, or in some cases, encryption keys.

A lot of people, including some technology experts, presume that when the power is removed from the device, the data held within RAM is lost instantly, but this is not the case. As matter of fact, memory decays slowly over time and can be a few seconds to as much as minutes (only in older RAM modules), after the power has been removed. This is also known as the remanence effect.

The remanence effect has been long known (Gutmann, 2001), but was first attacked practically by (Halderman, 2009). This attack was first known as the 'Cold-Boot Attack', where the remanence effect was exploited to reboot a computer into the attackers controlled boot-loader, and boot a simple operating system, that would dump the contents of memory.

The dangerous aspect of this process is that when systems implemented full disk encryption software, the master key was held within memory, and when performing this attack, the key was recoverable with up to a 99.99% success rate (Halderman, 2009). The attack could be made easier with the use of common air duster cans (the type used to clean keyboards etc.). By utilising this process, the attacker could cool the DIMM a considerable amount, to anywhere between -30C to -50C (Halderman, 2009).

The cooling of the module prolongs the memory decay within the chip and allows the attacker a greater amount of time to reboot the device or transfer the chip to another device where they can extract the data held within the memory module.

It has been shown previously that it is completely possible to compromise computer systems, laptops, and many other devices. But, with the rise in IoT devices, it is an area that has very little research.

Raspberry Pi devices are a great tool for creating an IoT device. They are small, cheap computer systems that can add GPIO devices and access internet connectivity. Although here lies one of the problems, they are cheaply built, meaning that minimum security is built into the hardware.

Recently there was research to indicate that the Raspberry Pi Model B+ was vulnerable (Won, 2020).

This paper aims to understand and demonstrate the effectiveness of cold-boot attacks against newer IoT devices

and models. The devices being attacked in this paper are namely the Raspberry Pi 3 and 4. To complete this aim, the understanding of how cold-boot attacks work will need to be comprehended fully. An understanding of IoT memory modules will need to be comprehended. The Raspberry Pi will need to be tested against cold boot attacks, and finally, an analysis of the findings will need to take place, to determine if the newer module is indeed vulnerable.

# 2. BACKGROUND

In this section, a background of the work will be discussed. This will give a good description of the work that has been done in the past and the work that will lead to the completion of this project.

## 2.1 Cold-Boot Attacks

Cold-boot attacks have been explored since 2009 (Halderman, 2009), where Halderman et al, discussed that through the remanence effect, encryption keys could be recovered by cold-booting a computer (or in this case a laptop), and searching through memory to find the encryption keys, therefore compromising the encryption software being used.

This attack was proven to be successful against most encryption software, including Windows BitLocker, Mac's FileVault, and just about any other full disk encryption software that was available (Halderman, 2009).

There have been many research papers discussing this vulnerability since Halderman et al discovered the hardware fault, and how it can be mitigated using hardware and software. (Ooi, 2009) (Simmons, 2011) (Henning, 2013)

## 2.2 RAM

Random Access Memory (RAM) is a volatile storage method that retains information for the live running machine. Once the power is lost, the data from the module begins to dissipate, leaving nothing behind. What most people do not know is that data can be left on the memory module for milliseconds up to minutes (older RAM modules) after the power has been lost (Gutmann, 2001) (Halderman, 2009).

As power dissipates in the capacitor of the RAM module, the memory controller will refresh the capacitor to the value stored in it previously. This stops it from losing data while the power is still running. (Müller, 2013)

This then explains how the remanence effect works, if power is cut and repowered very quickly, the RAM module will begin to refresh once again, retaining the information.

To allow for more time and error, the memory chip can be frozen to prolong the memory decay. As can be seen in Halderman's experiment (Halderman, 2009).

## 2.3 IoT

The Internet of Things is becoming more and more a part of today's society, with the likes of personal assistants (Amazon Alexa or Google Home), smart appliances and smarter homes/cities. This is all well and good for practicability, but what about security?

To test this, a practical look at the hardware of the Raspberry Pi will be looked at.

## 2.4 Raspberry Pi

*"The Raspberry Pi is a low cost,* ***credit-card sized computer*** *that plugs into a computer monitor or TV and uses a standard keyboard and mouse."* (Raspberry Pi, 2021).

The Raspberry Pi is a brilliant development platform that allows for the development of IoT prototypes and software without needing to develop single-use, expensive prototypes. It can also be found in production equipment in the wild. This then leads to the need for tougher security measures.

To examine this, the Raspberry Pi 3 Model B+ will be examined to determine if the SDRAM is vulnerable to cold-boot attacks.

## 2.5 Related Work

Halderman et al (Halderman, 2009), and many others, have explored this work within computers and laptops, proving the flaw exists and showing many countermeasures to the problem, (Henning, 2013) (Ooi, 2009) (Simmons, 2011), but not many people have had an interest in IoT devices that may hold sensitive information.

Some work has been conducted with the Raspberry Pi 1 Model B+ (Won, 2020), and this work suggests that as the boot sequence seems the same on the newer models, that the newer models would be vulnerable too, but no work has gone into this assumption, none that could be found anyway. This is the issue that this paper will help address.

Some mitigations will also be talked about, and some mitigations from these related papers will also be discussed to see if they are a viable option for this type of device.

# 3. METHOD

In this section, a description of the work to be completed will be discussed to give an overview of the adopted methods. The following procedures will take place:

- Research Raspberry Pi boot-sequence
- Load data into memory and keep a source copy
- Freeze the memory retaining the information
- Replace the SD card to perform Cold-Boot
- Analyze data to determine success

## 3.1 Boot Sequence

It was identified that the RAM on the Raspberry Pi 1 Model B+, was initialized after the boot sequence (Won, 2020). This meant that if the attacker could boot into a kernel image that they own to recover the contents of RAM, then the attacker could possibly recover sensitive data.

The same research team also stated that the newer Raspberry Pi boot sequence was identical to the older model, meaning it could also be vulnerable to this type of attack. Further analysis of the boot sequence is needed and further research on this attack needs to take place.

## 3.2 Load Data

To represent some form of sensitive data, a photo will be loaded into RAM. This allows for a visual representation of the attack to take place, allowing for a better analysis of the data.

The photo that will be loaded into RAM will be the famous picture of the Mona Lisa, which can be seen in Figure 1 - Mona Lisa (As shown in most other research papers).

**Figure 1 - Mona Lisa**

## 3.3 Freeze memory

In this step, the memory module will be frozen to retain the data from decaying. As memory is built onto the chip, and it cannot be removed, this must be done while the device is running. Once the chip is below freezing it is time to cold boot the device.

## 3.4 Cold-Boot

After the memory is frozen to an acceptable standard, the SD card (from which the boot sequence is loaded (Won, 2020)), is replaced and the device is booted into a standalone operating system, where the attacker can dump the contents of RAM (Halderman, 2009). Once the contents of the memory have been dumped, either to the console or an external USB, they can then be used for analysis.

## 3.5 Analysis

Now that the contents of the memory have been gathered, they can be examined. The attacker will need to search through the memory dump to find the image if it is still present. If the image can be found, then it will be examined to determine how accurate the image is compared to the original. This will be how the success of the attack will be determined.

# 4. Summary

To summarize, RAM does not lose its contents as soon as the power is removed from the device, and it can persist for multiple seconds or even minutes after power loss. By rebooting the device, the contents of RAM that were stored before power-off can be recovered.

Raspberry Pi's are amazing devices to allow for prototyping and implementation of IoT devices. These devices have not been looked at in detail, when it comes to cold-boot attacks, especially newer models. This leaves users unaware of the dangers that this vulnerability may cause.

Conducting this research will clarify whether newer IoT devices, such as the Raspberry Pi 3 and 4 are vulnerable and start to conclude on mitigations that can be cost-effective and reliable in preventing these types of attacks.

As these devices are presumed to have identical boot sequences, then the expected outcome of this examination should be that the device is vulnerable to cold-boot attacks. This will need to be explored further to determine if there is any practical application of this attack in the wild.

# 5. REFERENCES


Gutmann, P., 2001. Data remanence in semiconductor devices. *Proceedings of the 10th conference on USENIX Security Symposium*, 10(1), pp. 4-4.

Halderman, J. A., 2009. Lest we remember: cold-boot attacks on encryption keys. *Communications of the ACM, Volume 52, Issue 5*, pp. 91-98.

Henning, P., 2013. *Braving The Cold: New Methods For Preventing Cold Boot Attacks.* [Online]
Available at:
https://www.youtube.com/watch?v=hp4DEmLbuLc

Müller, M. G. a. T., 2013. On the Practicability of Cold Boot Attacks. *International Conference on Availability, Reliability and Security*, pp. 390-397.

Ooi, J. G., 2009. A Proof of concept on defending cold boot attack. *Asia Symposium on Quality Electronic Design*, 1(1), pp. 330-335.

Raspberry Pi, 2021. *Raspberry Pi.* [Online]
Available at: https://www.raspberrypi.org
[Accessed 2021].

Simmons, P., 2011. Security Through Amnesia: A software-based solution to the cold boot attack on encryption. *Proceedings of the 27th Annual Computer Security Applications Conference*, 11(27), pp. 73-82.

Won, Y.-S., 2020. Practical Cold boot attack on IoT device. *IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*, pp. 1-4.