IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, May 2026
Impact Factor: 8.2

Securing Data From Cold Boot Attack By Monitoring Device Temperature

Raghuvinder[1] and Avininder Singh[2]
[1,2] Assistant Professor, Department of Computer Science and Engineering,
Chaudhary Devi Lal University, Sirsa
raghuvinder@cdlu.ac.in1, avininderapc@cdlu.ac.in2

Abstract: *The goal of this research initiative is to treat securing data from Cold boot attack by monitoring device temperature concepts and results at the highest possible and abstract level thereby achieving generality and simplicity at the same time. Many result in data securing for instance in the area of indistinguishability proofs can be simplified and generalized substantially when considered at an abstract level. DRAM used in modern computer retain their contents for several seconds after power is lost, even at removed from a motherboard and even at room temperature. DRAMs become less reliable when they are not immediately erased, they are not refreshed and Their contents persist sufficiently for malicious (or forensic) acquisition of usable full-system memory images. We use cold reboots to mount successful attacks on popular disk Encryption systems using no special devices or materials. We experimentally characterize the extent and predictability of memory reminisce and report that reminisce times can be increased dramatically with simple Colding techniques*
To save data from this cold boot attack we monitor the temperature of a device when temperature of a device go below the threshold of a temperature value we remove the data from the memory so that attacker cannot steal the data from memory by freezing the memory.

Keywords: Cold Boot Attack, Encryption, Decryption, PGP, Obfuscation, Binary, ASCII, Symmetric key, Asymmetric key.

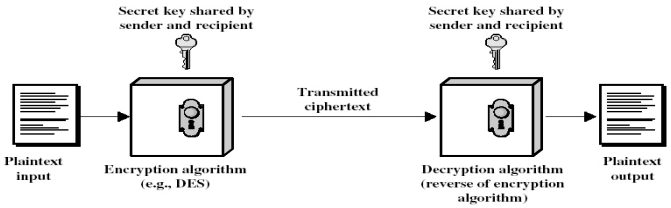
I. INTRODUCTION

A cold boot attack is a process for obtaining unauthorized access to a computer's encryption keys when the computer is left physically unattended.
[1]Dynamic random access memory (DRAM) chips retain data for a brief period of time after a computer is turned off the amount of time can be increased if the chips are removed from the motherboard and kept at low temperatures, This can be a accomplished by spraying them with an inverted can of compressed air. The chips can then be quickly reinserted into the machine and their contents read.
Cold boot attacks demonstrate that disk encryption programs which are used to protect data on desktops laptops and various other computing devices have no reliably secure location in which to store their keys the attack is carried out by performing a cold boot of the System and dumping the contents of the DRAM to a CD or USB token.[1] The memory image is then scoured for data structures that store the decryption key. With this data an attacker can obtain encryption keys wither by copying the entire encrypted partitions or rebooting the machine and using the computer's encryption software to decrypt it.
[2]Encryption means it is conversion of data into a form, called a cipher text. That cannot be easily understood unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.
It is use some terminology first one is Symmetric encryption it is both sender/receiver use the same algorithms/keys for encryption/decryption and second one is Asymmetric encryption it is sender/receiver can employ different keys use for encryption/decryption.

DOI: 10.48175/IJARSCT-36048

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, May 2026
Impact Factor: 8.2

II. ENCRYPTION MODEL



The purpose of this research is highlight the advantages and disadvantages of different secure authentication methods and provides awareness to authentication method in a particular scenario the part I of describes paper, part II describes purposed work. At the end of the paper conclusion is presented to guide contributors for the development of more secure authentication method.

III. COLD BOOT ATTACK

To execute the attack, a running computer is cold-booted. [3]Cold-booting refers to when power is cycled "off" and then "on" without letting the operating system shut down cleanly, or, if available, pressing the "reset" button. A removable disk with a special boot sector is then immediately booted (e.g. from a USB flash drive), and used to dump the contents of pre-boot memory to a file. Alternatively, the memory modules are removed from the original system and quickly placed in a compatible machine under the attacker's control, which is then booted to access the memory. Further analysis can then be performed against the information that was dumped from memory to find various sensitive data, such as the keys contained in it (automated tools are now available to perform this task for attacks against some popular encryption systems).

The attack has been demonstrated to be effective against full disk encryption schemes of various vendors and operating systems, even where a Trusted Platform Module (TPM) secure crypto processor is used. This is because the problem is fundamentally hardware (insecure memory) and not a software issue. While the focus of current research is on disk encryption, any sensitive data held in memory is vulnerable to the attack.

Compressed air cans can be improvised to Cold memory modules, and thereby slow down the degradation of volatile memory

With certain memory modules, the time window for an attack can be extended to hours by Colding them with a refrigerant such as an inverted can of compressed air. Furthermore, as the bits disappear in memory over time, they can be reconstructed, as they fade away in a predictable manner. In the case of disk encryption applications that can be configured to allow the operating system to boot without a pre-boot PIN being entered or a hardware key being present (e.g. Bit Locker in a simple configuration that uses a TPM without a two-factor authentication PIN or USB key), the time frame for the attack is not limiting at all.

This is not the only attack that allows encryption keys to be read from memory—for example, a DMA attack allows physical memory to be accessed via a 1394DMA channel. Microsoft recommends changes to the default Windows configuration to prevent this if it is a concern.

The ability to execute the cold boot attack successfully varies considerably across different systems, types of memory, memory manufacturers and motherboard properties, and is more difficult to carry out than software-based methods or a DMA attack.

IV. FULL MEMORY ENCRYPTION

Software-based full memory encryption is similar to CPU-based key storage since key material is never exposed to memory, but is more comprehensive since all memory contents are encrypted.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, May 2026
Impact Factor: 8.2

Dismounting Encrypted Disks

Most disk encryption systems overwrite their cached encryption keys as encrypted disks are dismounted. Therefore, ensuring that all encrypted disks are dismounted (secured) when the computer is in a position where it may be stolen may eliminate this risk, and also represents best practice. This mitigation is typically not possible with the system disk that the operating system is running on.

Advanced Encryption Modes

[3][4]The default configuration for Bit locker uses a TPM without a boot PIN or external key—in this configuration, the disk encryption key is retrieved from the TPM transparently during the operating system startup sequence without any user interaction. Consequently, the Cold Boot Attack can still be executed against a machine with this configuration, even where it is turned off and seemingly safely secured with its keys in the TPM only, as the machine can simply be turned on before starting the attack.

Two-factor authentication, such as a pre-boot PIN and/or a removable USB device containing a startup key together with a TPM, can be used to work around this vulnerability in the default Bit locker implementation. In this mode, a PIN or startup key is required when turning the machine on or when waking from hibernation mode (a power off mode). The result is that once the computer has been turned off for a few minutes, the data in RAM will no longer be accessible without a secret key; the attack can only be completed if the device is obtained while still powered on. No additional protection is offered during sleep mode (a low power mode) as the key typically remains in memory with full disk encryption products and does not have to be re-entered when the machine is resumed.

V. POWER MANAGEMENT

Shutting down a computer causes a number of well-known encryption software packages to dismount encrypted data and delete the encryption keys from memory. [3] When a machine is shut down or loses power and encryption has not been terminated (such as in the event of sudden loss of power) data may remain readable from tens of seconds to several minutes depending upon the physical RAM device in the machine. Ensuring that the computer is shut down whenever it might be stolen can mitigate this risk. For systems using the hibernation feature (ACPI state S4), the encryption system must either dismount all encrypted disks when entering hibernation, or the hibernation file or partition would need to be encrypted as part of the disk encryption system. By contrast sleep mode (ACPI states S1, S2 and S3) is generally unsafe, as encryption keys will remain vulnerable in the computer's memory, allowing the computer to read encrypted data after waking up or after reading back the memory contents. Configuring an operating system to shut down or hibernate when unused, instead of using sleep mode, can help mitigate this risk.

VI. BOOTING

The boot device options in the BIOS may make it slightly less easy to boot another operating system, [3]many BIOSes will prompt the user for the boot device after pressing a specific key during boot. Limiting the boot device options will not prevent the memory module from being removed from the system and read back on an alternative system either. In addition, most chipsets allow the BIOS settings to be reset if the main board is physically accessible, allowing the default boot settings to be restored even if they are protected with a password.

VII. PASSWORD ATTACKS

Brute Force Attacks: [3][4]In this type of attack, all possible combinations of password apply to break the password the brute force attack is generally applied to crack the encrypted passwords where the passwords are saved in the form of encrypted text. Early Linux systems use MD5 hashing schemes for storing the passwords there is a password file in the operating system which contains the user's passwords with user names. If the file is stolen by the attacker then the password can be caught. The original password is not in the file but it is encrypted in the form of MD5 Hash. The encrypted password seems to be safe but in fact it is also vulnerable to brute force attack. For this, the attacker first converts all combinations of passwords into their MD5 Hashes In order to break the password the attacker first extracts

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 13, May 2026 Impact Factor: 8.2

the MD5 hash of suspected password from the password file placed in the system. The hash is then matched with all MD5 hashes one by one. When the hashes are matched, the corresponding password is selected Brute force attacks are very time consuming as searching a hash from all possibilities is a time taking process. For example a user enters a password of 8 characters and all characters are lower case letters then to break the password using the brute force attack it requires (26) combinations which is equal to 208827064576. If a single computer takes 1000 passwords to check in one second then total time will be 208827064576 / 1000 = 208827064.576 seconds which is equal to 58007.52 hours. This shows that brute force attack is effective for smaller passwords

Dictionary Attack: This type of Attack is relatively faster than brute force attack. Unlike checking all possibilities using brute force attack, the dictionary attack tries to match the password with most occurring words or words of daily life usage. Many users generally write passwords related to the names of birds, familiar places, famous actors names etc. These passwords can be judged by the dictionary attack. The attacker makes the dictionary of most commonly used words that might have been be used as a password. The attacker then applies all these words to break the password. Although the dictionary attack faster than brute force attack, it has some limitations too i.e. brute force attack contains limited words and sometimes it is unable to crack the password because remains a possibility that password to be cracked may not be present in the dictionary itself.

VIII. OUR PROPOSAL

To secure keys and data from cold boot attack we keep track of the device temperature constantly or at a specific interval of time not more than 5 sec .By constantly we mean keeping track of temperature of device at the interval of 100 millisecond. If the temperature of the device go below the threshold of the specified temperature value keys and data present in the memory at that time is overwritten by the pseudo data or by random bits generated by random number function of the specific language. This threshold is lowered in the conditions where device is being operated at a cold places where the room temperature is cold.

IX. CONCLUSIONS

In this paper we try to tackle the cold boot attack which is very dangerous in its category of attack on computers and data stored in the digital form on the computers. These type of physical attack on computers always perform with speed by using different logic and give perfect results which makes them a great threat to computers. Proposed solution work without any problem and secure data at highest possible rate.

REFERENCES

[1] Lest We Remember: Cold Boot Attack on Encryption Keys. proc. 2008 USENIX Security Symposium. February 21, 2008.
[2] Network Security Essentials, Applications and Standards, 2nd Edition by William Stallings –Chapter2
[3] http://en.wikipedia.org/wiki/Cold_boot_attack
[4] A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication. Comsats Institute of Information Technology, Wah Cantt., 47040, Pakistan