Technical Disclosure Commons

Defensive Publications Series

May 2020

Automatic Erasure of Persistent Storage for Data Security

Marcus Boerger

Automatic Erasure of Persistent Storage for Data Security

ABSTRACT

Non-volatile memories (NVMs) such as phase change memory (PCM) have speeds, latencies, and bandwidths close to those of random access memory (RAM). The performance and economy of PCM (and other NVMs) have led computer system designers to use NVM as swap space. However, swap data can include user information, including potentially sensitive information. The storage of such information in a NVM swap partition can enable an attacker to steal information from a victim's computer, e.g., by forcing it to sleep and then reading the content of the NVM in another system. Per the techniques of this disclosure, such attacks on the swap partition are foiled by encrypting (and possibly compressing) the swap partition, and by deleting or otherwise rendering unreadable the encryption (or compression) key.

KEYWORDS

- Phase-change memory (PCM)
- Non-volatile memory (NVMe)
- Persistent storage
- Encrypted storage
- Cryptographic erasure
- Swap data
- Swap partition
- Operating system
- Encryption key

BACKGROUND

Non-volatile memories (NVMs), e.g., phase change memory (PCM), have speeds, latencies, and bandwidths close to those of random access memory (RAM). Aside from using NVRAMs conventionally, e.g., as a cache for flash or for extending RAM to a non-uniform memory access (NUMA) mode, the performance and the economy of PCM (and other NVMs) have led computer system designers to use PCM as swap space.

However, swap data can include sensitive information such as personally identifiable information (PII), unencrypted passwords, etc. This gives an attacker the ability to easily steal information from a victim's computer by forcing it to sleep and then reading the NVM content in another system. This can be particularly problematic if the NVM sits on a module that can easily be read by another computer that the attacker controls.

DESCRIPTION

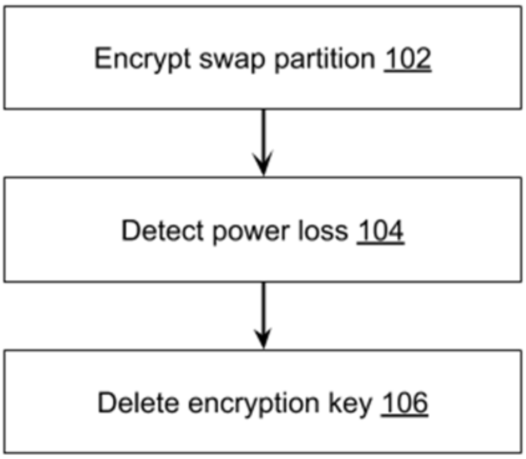

Fig. 1: Automatic Erasure of Persistent Storage

Fig. 1 illustrates the automatic erasure of persistent storage upon the computer entering a sleep state, shutdown state, or other similar state, per the techniques of this disclosure. An attack on the swap partition stored on a non-volatile memory is foiled by encrypting (and possibly compressing) the swap partition (102). The encryption (or compression) key is deleted (106) prior to the device entering such a state, e.g., a planned or unplanned shutdown of the device that is detected as power loss (104). The deletion of the key can be done in any suitable manner, such as, for example:

Immediate invalidation command: Per this technique, a new command is defined for the NVM device that immediately deletes or invalidates data, e.g., by modifying metadata that represents the contents of a configurable area of the NVM. For example, this can be done by supporting NVM namespace erasure in a manner similar to the way the NVM supports cryptographic erase, e.g., removal of the storage encryption key. This functionality can be triggered even in the event of a power (battery) failure or removal of the storage module, by ensuring a transient power supply to the NVM just prior to complete power loss supplied by, e.g., a capacitor coupled to the NVM.

Watchdog functionality: Per the techniques, watchdog functionality can be provided that, when triggered, erases a configurable area of the PCM, including an area where encryption keys for the data are stored. This can be integrated, for example, into an NVM keep-alive command set. By restricting the necessary action to deleting the encryption key or simply making it unusable, the action can be performed in a very short amount of time using tiny amounts of energy, such that even an unplanned shutdown (or removal of the storage module) cannot interfere with the triggering and execution of the watchdog functionality.

The tiny amount of energy needed for triggering and executing the watchdog functionality can be provided by existing capacitors that are coupled to the NVM. Thus, a physical controller can relatively easily support such an action at very low or no additional cost. Beyond direct command integration, as explained above, key deletion can be accomplished by simply observing bus operation. For clocked bus systems (e.g. PCIe) it is likely sufficient to watch the clock signal and trigger as soon as the clock (or bus) is quiescent, such quiescence being an indication of a loss in power. Observation of the bus or clock lines can be enabled by additional commands that support extended sleep states.

In this manner, the described techniques enable a secure, encrypted swap partition that renders data inaccessible in the event of system shutdown, without additional power consumption for this feature. The techniques of automatic erasure (or invalidation/ cryptographic deletion) can be applied in any computer (e.g., consumer device, servers, cloud infrastructure, etc.) where access to a persistent storage, module, or board can result in disclosure of data. The techniques can be implemented in operating systems and with hardware extensions to PCM or other non-volatile memory devices.

CONCLUSION

The performance and economy of PCM (and other NVMs) have led computer system designers to use NVM as swap space. However, swap data can include user information, including potentially sensitive information. The storage of such information in a NVM swap partition can enable an attacker to steal information from a victim's computer, e.g., by forcing it to sleep and then reading the content of the NVM in another system. Per the techniques of this disclosure, such attacks on the swap partition are foiled by encrypting (and possibly compressing) the swap partition, and by deleting or otherwise rendering unreadable the encryption (or compression) key.