Encrypted RAM

Initial Summary for Research Done on Encrypting RAM

By

Dhruv Pandya

Under the supervision of

Dr. Michael Soltys

Summer 2016

6/9/2016 – 8 /2/2016

- Random Access memory a.k.a. RAM allows data items to be accessed (read or written) in almost the same amount of time irrespective of the physical location of data inside the memory.
- RAM is a volatile memory which makes it easily vulnerable to attacks.
- RAM contains loads of logical data like Passwords, Login credentials, information exchanged by OS.
- Physical attacks possible on RAM are :
    - Using Direct Memory Access (DMA)
      Common example of a DMA attack is using Firewire.

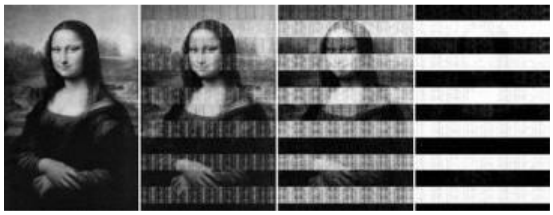

Fig1: Example DMA access to RAM using Firewire.

Fig: 2 Firewire.

- Using Cold Bot Attack
  Freezing the RAM below 0 degree C

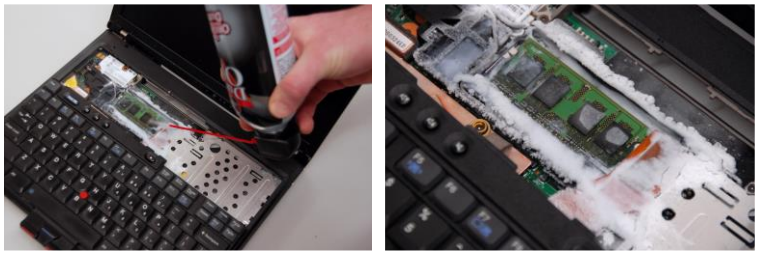

FIG 4

- ## Quick Description of Scenario :

- Encrypting RAM involves challenges like the real-time data encryption and applying perfect encryption technique.
- RAM is a primary memory which is responsible for the functioning of OS as well as Data exchange.
- So applying an Encryption technique which would be more costly on the processing had no meaning.
- Using trial and error method we worked out to determine a perfect technique for encryption.
- Also placement of the key for encryption was most tricky part, and so far we have decided to place it on a hard drive.
- Now for using RAM we created a Virtual RAM using C language which is a very general and basic example of a virtual RAM

- ## Encryption Techniques :

- We worked on different encryption techniques namely AES, Holomorphic and RC 4.
- Holomorphic Encryption :
    - Homomorphic encryption is a form of encryption that allows computations to be carried out on cipher text, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext.
    - As the theory suggest we can do the data processing on cipher text and hence it won't leave the RAM vulnerable for minute fraction of second.
    - Thus it solves the problem of part encryption and leaving the RAM vulnerable for a possible attack.
    - But one problem which perish using holomorphic encryption was the cost of using it and amount of real-time processing it would consume.
    - Hence to overcome this problem we applied the part use of RC4.
- RC4 Encryption :
    - In cryptography, RC4 (Rivest Cipher 4 also known as ARC4) is a stream cipher. Remarkable for its simplicity and speed in software.
    - Now combining the approaches together we can encrypt the data using RC4 and encrypt the key for the Steam Cipher using Holomorphic encryption which is depicted in the diagram 5.
- Further stage for the research would be the actual practical implementation of the program .

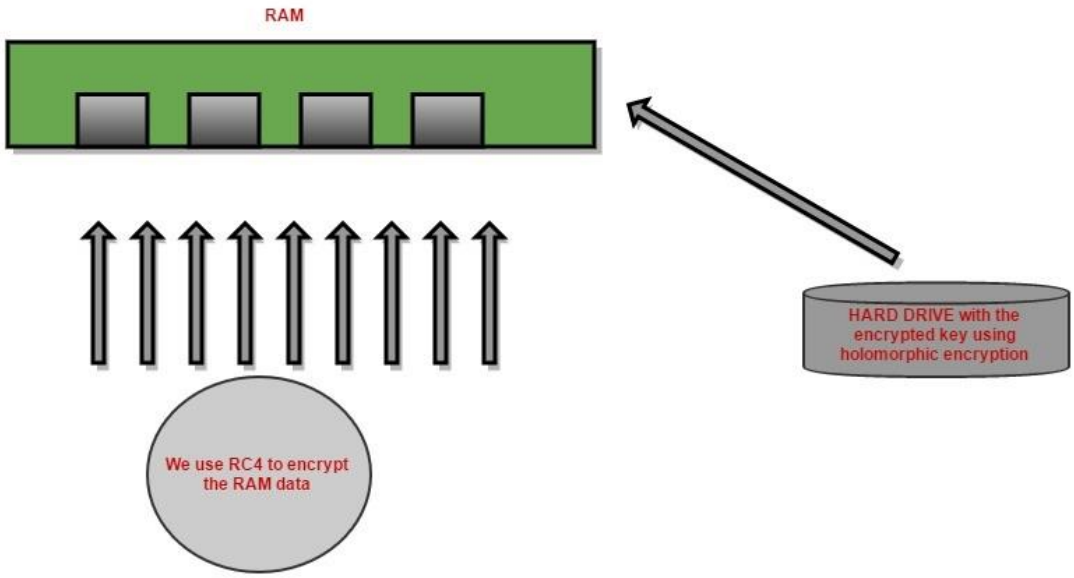

Fig 5

Reference:

RamCrypt: Kernel-based Address Space Encryption for User-mode Processes

Cryptkeeper: Improving Security with Encrypted RAM