Volatile Memory Forensics

by datagram & Vidiot
May 18, 2008
datagram.layerone@gmail.com
Vidiot – infidel@loljazeera.net

About Us

- We really don’t have time for this
  - it would suck anyways

P.S. – We like beer.

Our Agenda

- What is Live Forensics?
- Live Forensic Process
- Hardware vs. Software
- Offline Analysis Basics
- Cold Boot Attacks (the new hotness)
- Countermeasures

What is Live Forensics?

Good…and Bad

Good…

- Scope of information
- Availability
- Combats modern anti-dead forensics

But…

- No data integrity
- All actions affect memory
- Cannot be reproduced

In-Memory Data

- Running Kernel/modules info
- Running/dead processes
- Network connections/configuration
- Memory-mapped files
- User logins
- Firewall settings
- Web caches
- Lots of random shit

Live Forensics Process

- Regular rules apply :)

- Dump live memory (software/hardware)
- Gather volatile data (software)
  - Optional
- Offline analysis of dump
- Proceed with dead forensics

Memory Dumping

- Hardware
  - Custom hardware devices
  - Access memory directly (DMA)
  - Can also be cheated : (
- Software
  - Trusted toolkit
  - WILL alter memory
  - May overwrite evidence
  - Can be cheated by rootkit (e.g. Shadow Defender)

Hardware Dumping

- DMA can subvert OS
- Custom DMA device
  - PCI, PCMCIA, USB, Firewire
  - http://www.csoonline.com/read/050106/ipods_pf.html
- But…can be defeated (Rutkowska, 2007)

Software Dumping

- UNIX/Solaris: /dev/mem
- Linux: /proc/kcore, /dev/mem
- OS X: /var/vm, /dev/mem*
- Windows: \\.\PhysicalMemory*

- e.g.
  dd if=/dev/mem of=memdump.img conv=noerror,sync

Software Preparation

- Create trusted toolkit
  - Statically compiled binaries (gcc –static)
- Prepare remote system (for nc)
- Consider scripts

- Understand your actions!
- Remember your goals

Software Basics

- Gather live info :)

- Use trusted commands
  - statically compiled, read only media
- Remember $PATH!
- nc/cryptcat data to remote system
  - Remember to md5 hash!

Software Basics

- Rootkit hunting:
  - chkrootkit
  - rkhunter*
  - Hunter.o (kernel mod)
  - 99luftballons
  - Manual inspection

Offline Dump Analysis

- More or less Rev. Eng

- String searching
- Carving
- Interpreting Kernel structures

String Searching

- Tried and true :)
  - strings –a –t x dump.img
  - grep * dump.img
- Specialized Algorithms: EnCase, etc
- Hilarious (sometimes)

Hilarity Often Ensues

696195554]0;newb@x:/dev/shm/newb/newb <----------Full path from PS1 ☺
696195591 [newb@x newb]$ rm -rf acycmech.tar
696195671 [newb@x newb]$ cd acycmech
696195752 [newb@x acycmech]$ ./ci
696195818 ./vhost
696195827 -bash: ./vhost: No such file or directory
696195917 [newb@x acycmech]$ ./vhosts
696195951 -bash: ./vhosts: Permission denied <----------Owned by umask
696196034 [newb@x acycmech]$ chmod +x *
696196117 [newb@x acycmech]$ ./vhosts
696196151 ./vhosts: line 1: 127.1.1.254: command not found
696196201 ./vhosts: line 2: 127.25.143.230: command not found
696196254 ./vhosts: line 3: 127.1.1.252: command not found
696196905 [newb@x acycmech]$ ./cin
696196987 ./do
696196993 Usage: ./do <input file> <----------RTFM?

Hilarity Often Ensues (2)

- Attempts at logging out:

696194744 [newb@x acycmech]$ unset HISTFILE;exit
696194789 logout
696194797 There are stopped jobs.
696194823]0;newb@x:/dev/shm/newb/newb/acycmech
696194869 [newb@x acycmech]$ unset HISTFILE;exit
696194930]0;newb@x:/dev/shm/newb/newb/acycmech
696194976 [newb@x acycmech]$ exit
696195006 logout
696195014 There are stopped jobs.
696195040]0;newb@x:/dev/shm/newb/newb/acycmech
696195086 [newb@x acycmech]$ exit
696195116 logout

File Carving

- Grab memory-mapped files
- Affected by Kernel security
- Free tools: Scalpel, Foremost
- Commercial: EnCase, FTK, etc.

Interpreting Kernel Structures

- Un-fucking /dev/mem--/proc/kcore dump
- Few ready-to-use Linux tools… : (
- IDETECT (http://forensic.seccure.net)
- Read:
  - Understanding the Linux Kernel, (Bovet & Cesati)
  - Digital Forensics of Physical Memory (Burdach)

Cold Boot Attacks

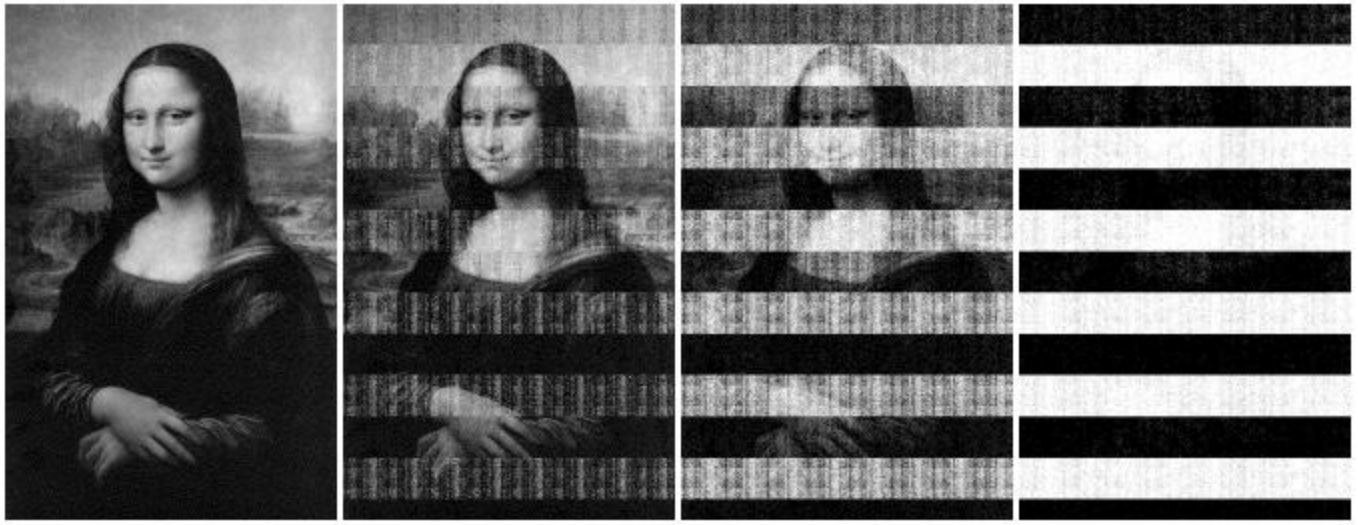
- Not our research
- Developed at Center for Information Technology Policy, Princeton University
  - Read: “Lest We Remember: Cold Boot Attacks on Encryption Keys”
- Based on unexpectedly long decay rate of DRAM memory.
- Almost every disk encryption system is vulnerable.
  - BitLocker, FileVault, dm-crypt, TrueCrypt, etc.

Cold Boot Attacks

- DRAM remanence effects
  - Different from the Gutmann “burn in” effect.
  - Assuming memory loss is instantaneous = FAIL
  - Memory decay occurs as DRAM MOSFETS return to their ground state.
    - Can be 0 or 1 depending on whether the fixed conductor of the capacitor is wired to ground or power.
  - Complete decay can equal several thousand refresh cycles.
  - Decay rate is a function of temperature.
  - Decay rate pattern = slow, fast, slow
  - Higher density (newer) DRAM has a shorter decay period.

Cold Boot Attacks

- Patterns and predictability in decay
  - Eventual state can often be predicted.
  - Relative order of decay often stays constant, regardless of temperature.



5 sec. 30 sec. 60 sec. 5 min.

Image excerpt from: Lest We Remember: Cold Boot Attacks on Encryption Keys, Princeton University, 2008, pg. 7

Cold Boot Attacks

- 3 Types of attack
  - Reboot to custom kernel
    - Pros: Fast and easy
    - Cons: Data destruction during OS shutdown, potential to overwrite data in DRAM at restart
  - Hard power cut, Reboot to custom kernel
    - Pros: Fast and easy, prevents data destruction during shutdown
    - Cons: Potential to overwrite data in DRAM at restart
  - Transplant DRAM to second PC
    - Pros: prevents data destruction from shutdown or overwrite
    - Cons: More complicated, requires preparation & hardware
- Network attack also possible via PXE
  - Compromised server setup as PXE boot server, DOS attack or software flaw causes other machines to reboot and load PXE memory dumper. EX: Retrieving SSL private keys from web server.

Cold Boot Attacks

- Locating keys in memory dump
  - Search for known contents or known structure
  - Example: Locating an RSA private key
    - Searching memory dump for known public modulus might reveal private key.
    - Searching for known format – (0x30) followed a few bytes later by the DER encoding of RSA version number and then by beginning of DER encoding of the next field (02 01 00 02).
      - PKCS#1 standard is an ASN.1 object of type RSAPrivateKey with the following fields: version, modulus n, publicExponent e, privateExponent d, prime1 p, prime2 q, exponent1 d mod (p−1), exponent2 d mod (q −1), coefficient q−1 mod p, and optional other information, packaged in DER encoding.
    - Also, searching for data with low Hamming distance to known values may reveal keys in decayed memory.

Cold Boot Attacks

- Hamming Distance
  - The number of positions for which the corresponding symbols are different between two strings of equal length.
  - For binary strings, calculated *a xor b*.
  - EX. 1001101 and 1011001 = 2.

Countermeasures

- Scrubbing memory
  - Avoid storing keys in memory and overwrite them when no longer needed.
  - Alternatively, systems can be configured to perform a destructive memory test on POST.
    - i.e. – disable quick boot, or use ECC RAM
    - Will not prevent transplant attack.
- Limit booting from network or removable media
    - Again, Will not prevent transplant attack.

Countermeasures

- Pass/key required to wake system
  - Suspending (sleep mode) a system will not protect keys already in memory.
  - Hibernation mode also vulnerable unless an external secret is required to resume normal function.
  - TPM systems may be vulnerable
    - BitLocker is vulnerable in default mode because disks are mounted automatically on boot.

Countermeasures

- Avoid precomputation
  - Precomputing can speed cryptographic operations, but often leads to redundant storage of key information.
- Key expansion
  - Applying a transformation to the key prior to storing it in memory can significantly hinder an attackers attempts to find or reconstruct a key in the presence of bit errors.

Countermeasures

- Architectural changes
  - Build DRAM with faster decay rate
  - Build key management hardware into motherboard
  - Encrypt the contents of RAM
  - NOTE: Will not help existing machines

Countermeasures

- Encryption in disk controller
  - Enable a write-only *key register* into which software can write a user derived symmetric key.
  - Data blocks are encrypted by disk controller prior to being written to disk.
  - Disk encryption keys never touch RAM

Countermeasures

- Advances in Trusted Computing
  - Current TPM's do not implement bulk encryption
    - Instead they monitor the boot sector to determine if it is safe to store a key in RAM.
  - TPM can prevent a key from being placed in RAM, but cannot protect it once it is there.

Countermeasures

- Physical Defenses
  - Encase RAM (epoxy, etc) to frustrate transplant attack.
  - Trip switches, accelerometers, motion sensors, RFID, etc.
  - Almost endless potential.
  - Lot’s of opportunity to be silly.

Conclusions

- Exercise caution
- Understand your actions
- Not a solution, an addition
- Think about physical security
- Have fun

- Good luck!

Q&A?

More!

- Google :D
- Mariusz Burdach, (forensic.seccure.net)
  - IDETECT tool
- Joanna Rutkowska, Black Hat Feb 2007
  - Anti-DMA Forensics Attacks
- FATKit framework
  - http://www.4tphi.net/fatkit/
- Aaron Walters, Nick Petroni, Jr.
  - Volatools toolkit (Windows)
- Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition
  - http://www.ncjrs.gov/pdffiles1/nij/187736.pdf
- Hot Plug
  - http://www.wiebetech.com/products/HotPlug.php
- Lest We Remember: Cold Boot Attacks on Encryption Keys
  - Princeton University
  - http://citp.princeton.edu/pub/coldboot.pdf
- Msramdmp
  - Wesley McGrew
  - http://mcgrewsecurity.com/projects/msramdmp/
- Basic Stamps and Accessories
  - http://www.parallax.com/