A HARDWARE BASED MEMORY ACQUISITION PROCEDURE FOR DIGITAL INVESTIGATION

BY BRIAN D CARRIER, JOE GRAND

PRESENTED BY MD. ENAMUL HAQUE
ID 201204920

COE 589

Course Instructor: Dr. Ahmed Al Mulhem

Agenda

- Introduction.
- Background.
- Previous work.
- H/W based imaging procedure.
- Tribble : Proof of concept device.
- Conclusion.

Introduction

- Digital data must be collected first to investigate the compromised system.
- Data may reside both in volatile and non-volatile storage.
- Most investigations have involved non-volatile storage.
- Non-volatile storage - Hard disks.
- Volatile storage: network traffic, RAM etc.

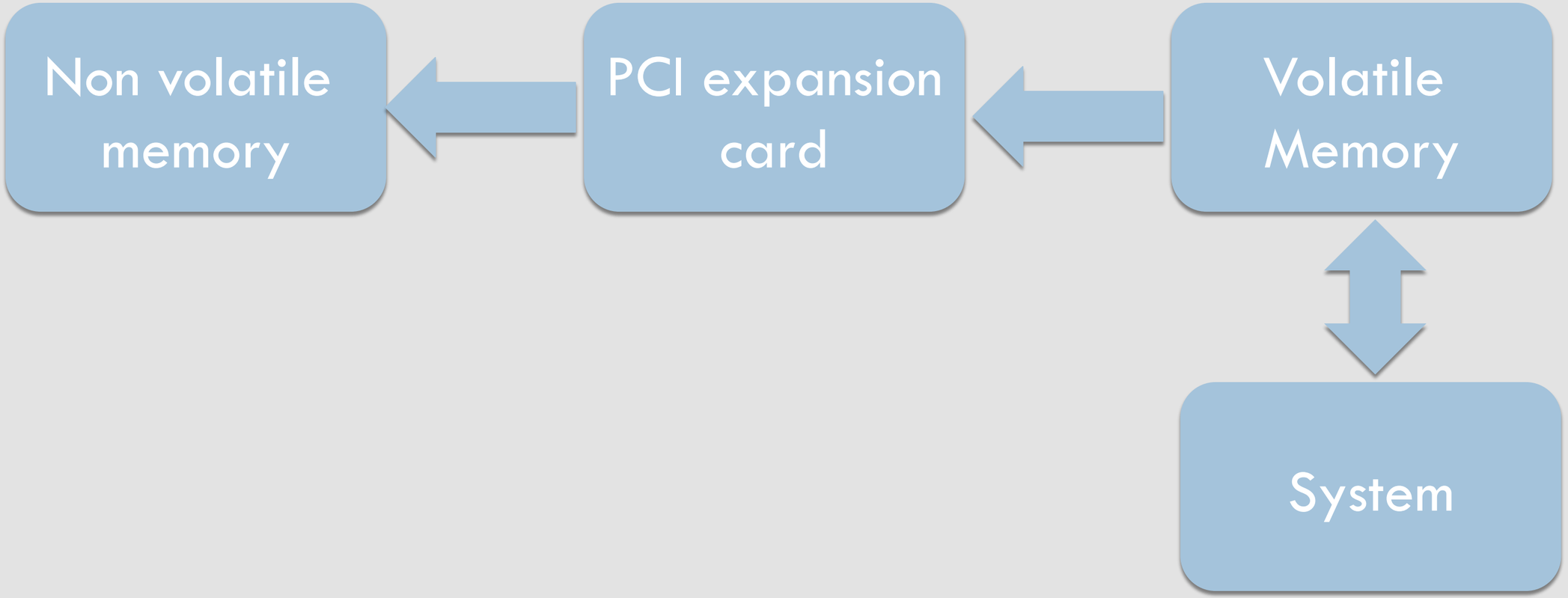
Volatile memory investigation-Reason?

- Can you collect data of the running processes from disks?
- Some apps resided only in memory, doesn't write anything to disks.
- So, memory investigation is necessary for such apps / worms.
- Examples of worms: Code Red, SQL Slammer.

Volatile memory - issues

- Data lost when power is removed.
- Difficult for the investigator to acquire that data in a trusted environment.
- Rootkits and Trojan horses - threat to the OS kernel causing unreliable data.
- Existing methods involve untrusted softwares.
- Invasive - may write to memory and hard disk.
- Many incident responders run *ps*, *netstat* to collect the obvious data only.

Solution


Non volatile memory
PCI expansion card
Volatile Memory
System

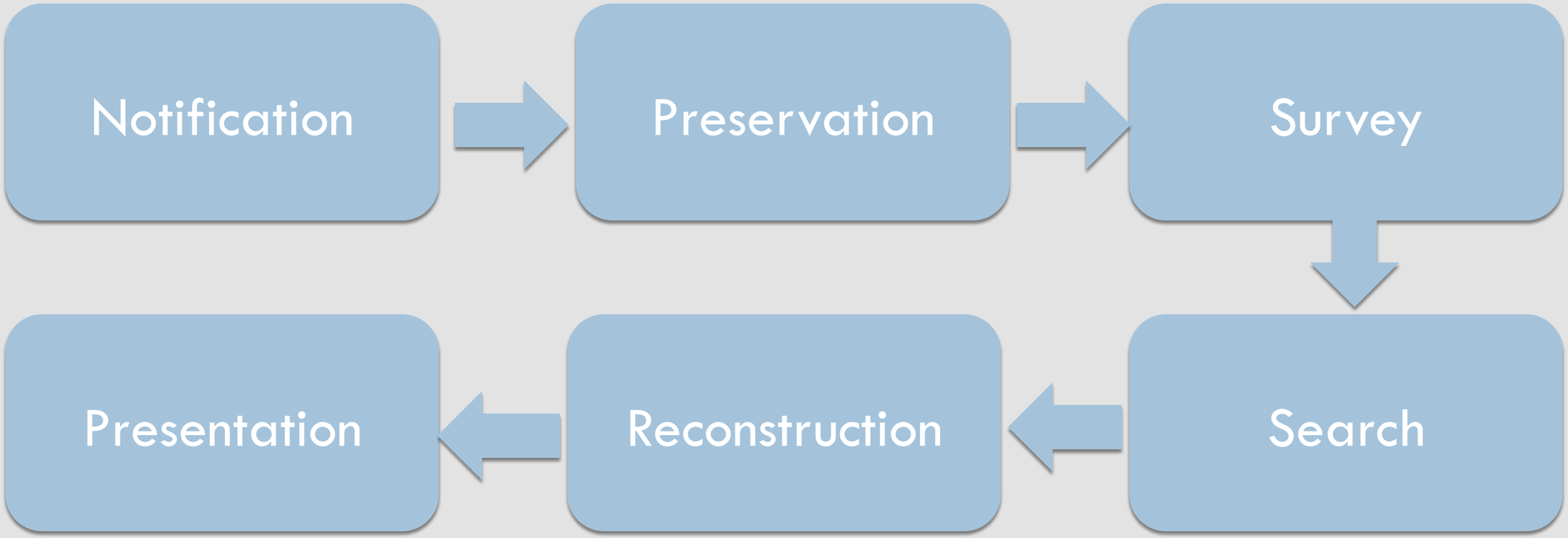
Solution mechanism

- PCI controller on the card is disabled by default.
- PCI card does not reply to the bus queries until it is activated.
- Advantage: Software and OS independent - may not be tampered.
- Limitation: Activated by the incident response team - manually !!

Background

- Investigation phases. (Carrier and Spafford model is used)
  - case study : running bot programs to create unusual no of users / hour in any social website.
- Memory imaging requirements.

Investigation Phases



Notification

- Incident is detected.
- Incident response team deploy.
- Response and investigation process starts.
- Incident verification by the team. [how to do that?!!]
  - if the new users / hour is really increasing?

Preservation

- Goal: Minimize the modification of the digital evidence.
- Making the exact copy of the digital crime scene.
- Preserve the copy and move to the survey phase.
  - capture the user profile database snapshot / profile database server memory snapshot.

Survey

- Crime scene is examined for obvious piece of information.
- Uses existing knowledge of the incident.
- Outcome: One or more hypotheses about the incident.
  - accounts are from same IP / location / fake email ids / time delay.

Search

- Search for additional evidence.
- Support / Refute the hypotheses.
- Digital evidence has been collected.

Reconstruction & Presentation

- Final theory with existing evidence and hypotheses.
- Additional evidence is searched for in some cases.

- Final Theory is presented.

Focus

- Preservation phase.
- Reason: Current technique is unreliable to preserve data.
- Making a reliable copy of HDD is easier compared to volatile memory.
- Create easier mechanism for preservation.

Memory imaging requirements

1. Acquisition tool shall read all digital data from a source and write back to a non-volatile storage which is in accessible format.
2. Tool shall not cause data to be written on the source.
3. Tool shall follow a documented procedure with steps performed with H/W and S/W resources used to read source data.
4. If any I/O errors occur while reading source data, it should be logged in the image with specific value.
5. When Destination > Source : identify the start and end location in the destination.
6. When Destination < Source: notify the user + copy partial / abort.
7. Correct documentation needed.

S/W solutions follow the requirements?

Not all the points are followed. Some are violated.

1. Second requirement is violated due to be loaded in the system memory.

2. Third requirement was added to satisfy the Daubert hearing.

Recommendations

1. Tool should halt the target system while acquisition process to stop changing the memory and page table.
2. Tool should calculate one or more hash values of the data that are read from the source.

Previous Work

1. Physical memory device.
2. Sparc OpenBoot.
3. Process pseudo-file system.
4. Virtual machines.
5. Hibernation.

Physical memory devices

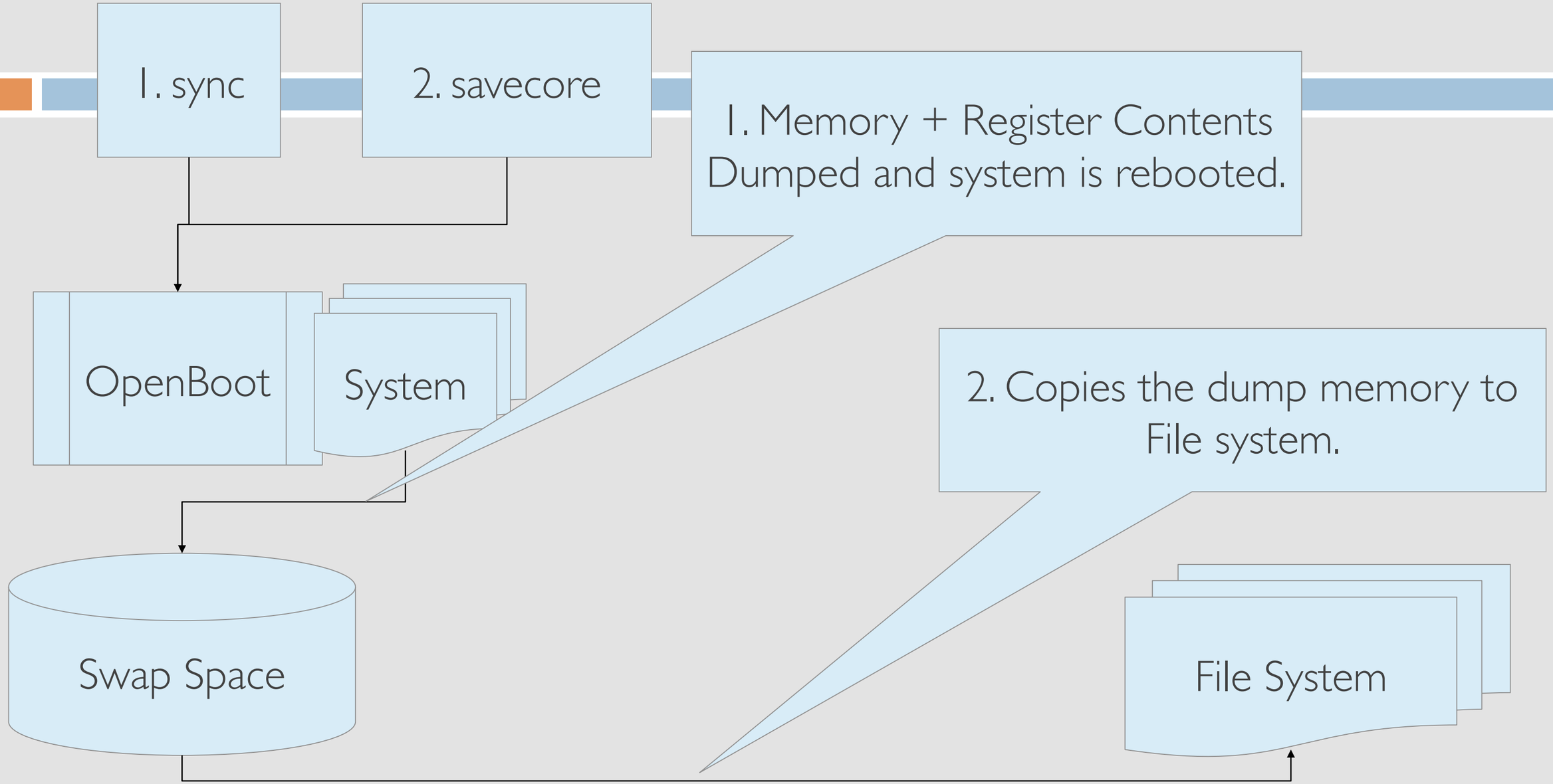
Operating System	Device / Object name for physical memory	Virtual Memory	Tools used
Linux	/dev/mem	/dev/kmem	dd
Windows	\\.\PhysicalMemory		dd

Shortcomings

1. Relies on the local operating system.
2. Requires the responder to run at least one process.
3. Running a process on the target system violates the SOCOND requirement.
4. /dev/mem has been abused in the past; Not reliable. It is not implemented in some system.
5. Analysis of the page table is required to properly piece together the ordering of the contents within physical memory.

Sparc OpenBoot

- Firmware.
- In Sun System.
- Can dump physical memory content to a storage device.
- Accessed by using L1-A / STOP-A keys.


1. sync
2. savecore
1. Memory + Register Contents
Dumped and system is rebooted.
OpenBoot
System
2. Copies the dump memory to
File system.
Swap Space
File System

Advantage

1. H/W based.
2. Executing from ROM – Can not be changed.
3. Provides a mechanism to suspend a system.
4. Additional data and symbols are saved using sync command.

Disadvantage

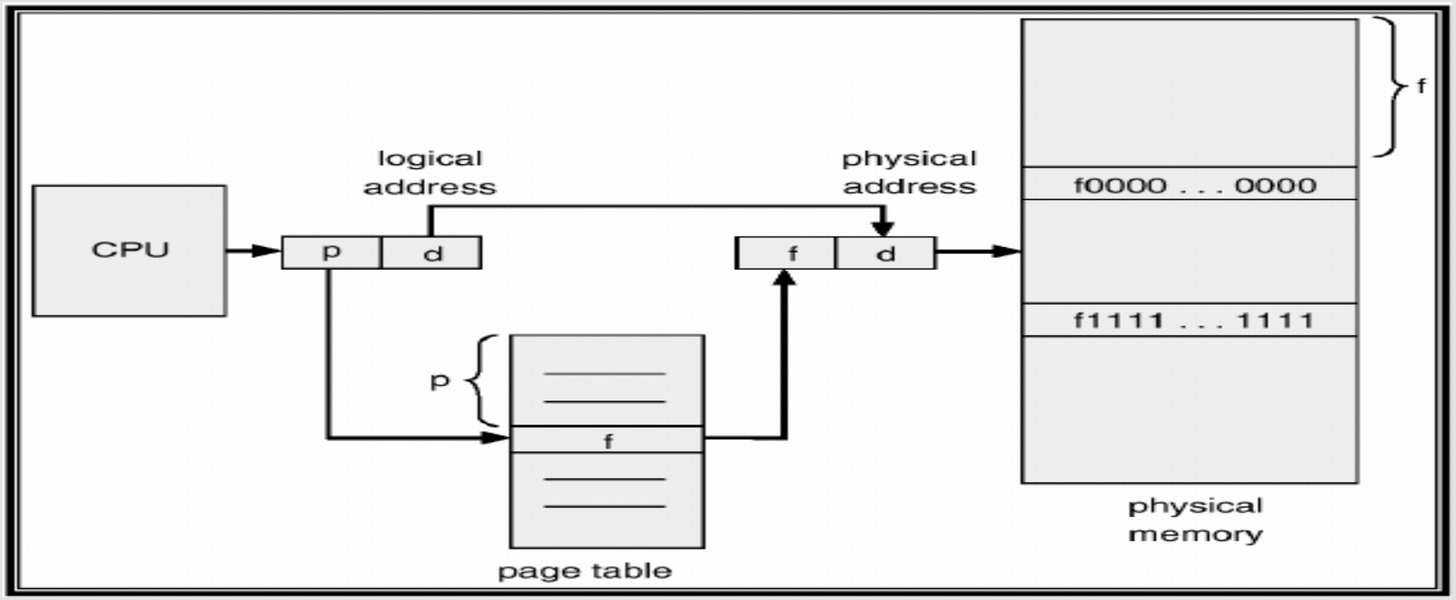
1. Overwrites the data of swap space by default.
2. Requires system reboot.
3. Only available in SPARC system.
4. Other Unix system have savecore command; runs only after kernel panics. [Usually there is no graceful way to make a suspect system panic]
5. Solaris also have savecore; but similar to using /dev/mem device.

Process pseudo-file system

1. For Unix systems.
2. Mounted at /proc/
3. Contains information of kernel and running processes.
4. For physical memory – there is a file (like /dev/mem)
5. For each processes' memory – there are separate files.
6. Already we discussed about advantage and disadvange of using /dev/mem;

Advantage

1. No need to collect the pages of physical memory and swap space together during analysis using page table.

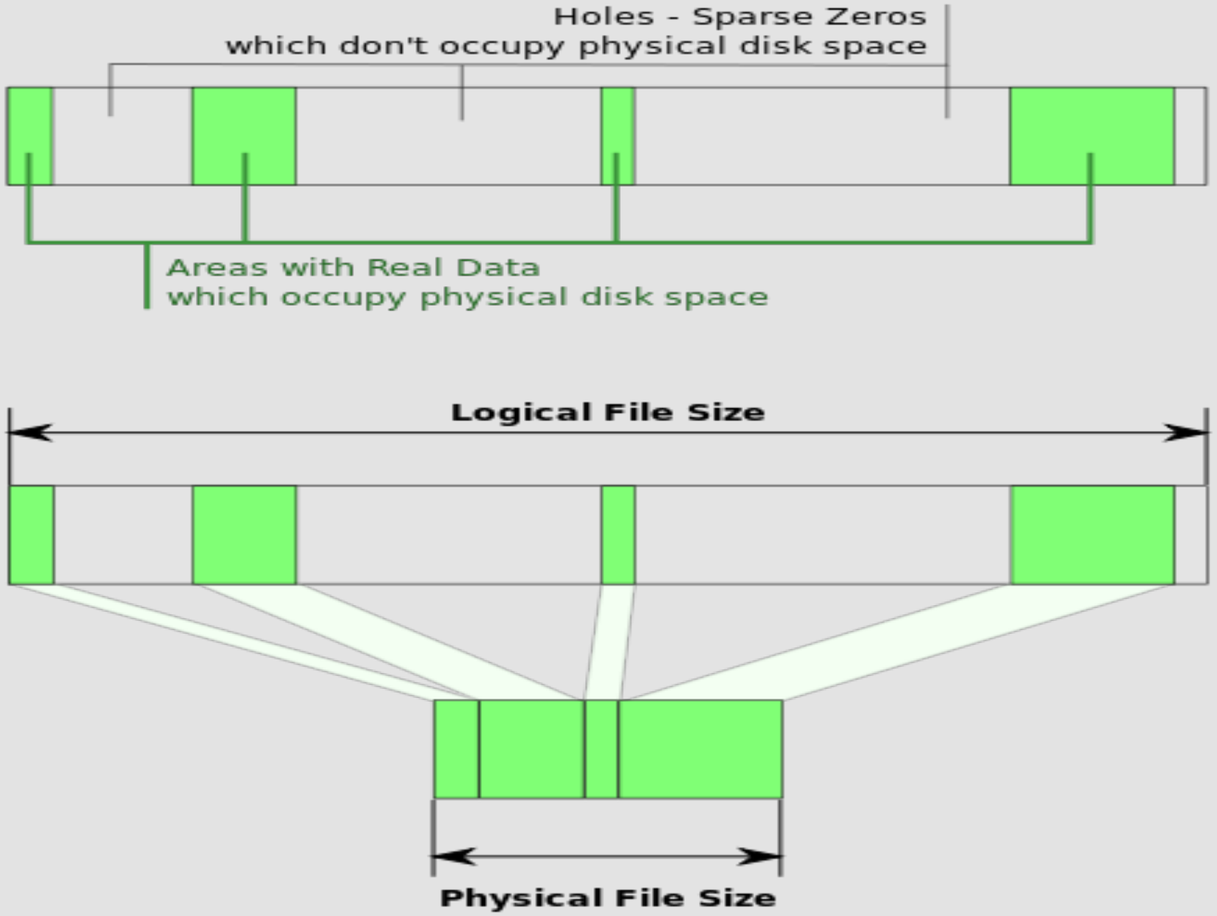


Disadvantage

1. Need to identify the suspect process first.
2. Force the non-resident pages of memory to be read from SWAP and written to PHYSICAL memory.
3. Resident memory pages may be written back to swap space; overwrites unallocated data; second requirement violation.
4. Analyzes only allocated memory, analogous to file backup; full image is not captured.
5. Passwords and other data may reside in the unallocated memory.

The Coroner's Toolkit (TCT)

1. Collection of programs for post-mortem analysis of an Unix system.
2. pcat tool uses ptrace() system call / /proc/ file system to save process memory.
3. Either can save all of the memory as a sparse file / can save only non-zero memory contents.


Holes - Sparse Zeros
which don't occupy physical disk space
Areas with Real Data
which occupy physical disk space
Logical File Size
Physical File Size

Virtual Machines

1. Emulates a computer environment so that an OS and other applications can run inside of it.
2. Virtual machine can be suspended and saved at any time.
3. OS and applications do not always feel that they are running inside emulated environment; thus executes as normal.
4. Some Vms save the disk and memory contents in a raw file. Others save them in a proprietary format.

Disadvantage

1. Impact on system performance.
2. Critical servers running inside of an emulated environment will increase the load on the hardware.

Advantage

1. No special processes are run.
2. Trusted software is used to save system state.

Hibernation

1. Power management feature of most portable and some non-portable systems.
2. Save the state of the computer by disabling processors and devices.
3. Two way implementation:
   - Provide small power to volatile memory to retain its contents.
   - Save necessary contents of memory to disk and restore when needed again.

Current power management systems

1. Uses combination of both hardware and software to support sleep mode.
2. OS can communicate with BIOS to place the system in sleep more.
3. BIOS can initiate sleep mode on its own.
4. Many servers are designed to never turn off and therefore may not have a power management option.

Advantage

1. More reliable than the software solutions.
2. Similar to the OpenBoot procedure.
3. Data is written to a dedicated partition; No overwrite in swap space.

Disadvantage

1. Not clear if the exact contents of the memory is saved during hibernation.
2. It is pretty unlikely that the entire physical memory is preserved.

Limitations of Software procedure

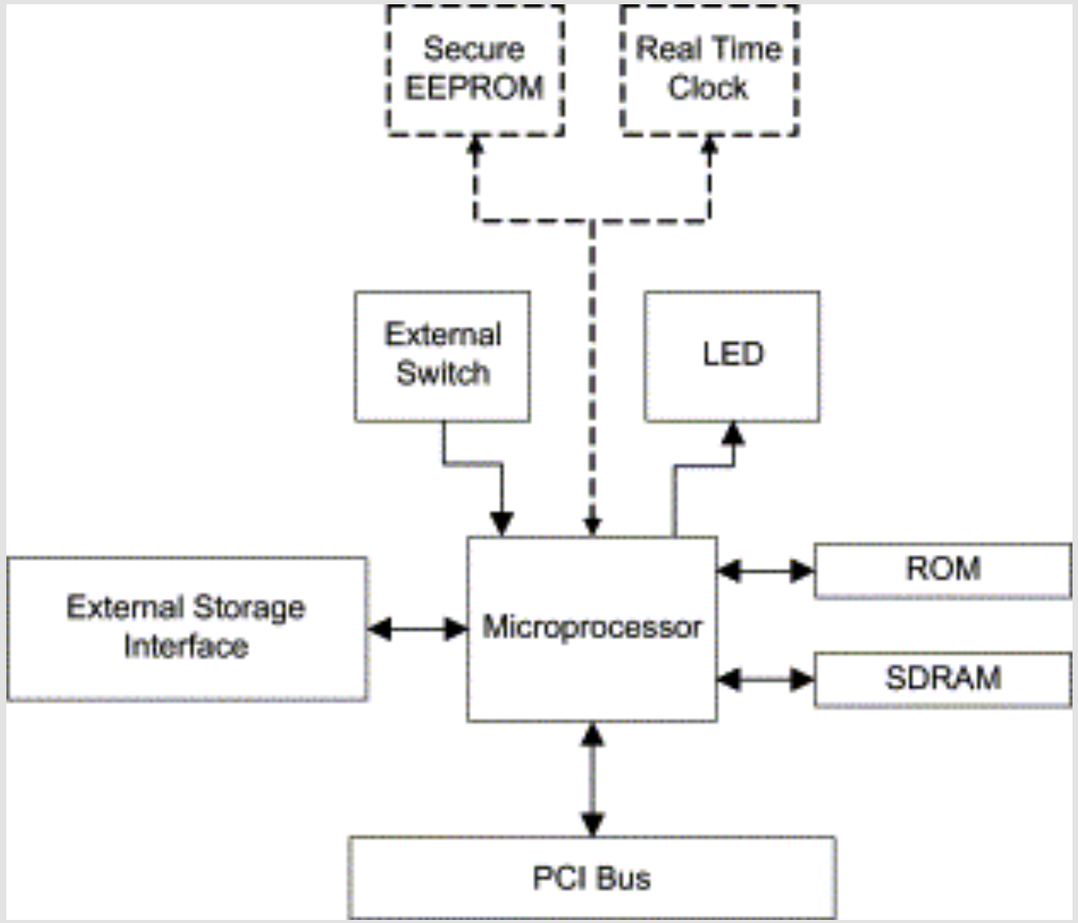
1. Volatile memory acquisition procedures rely on untrusted resources (OS kernel).
2. Applications can be run from ROM but kernel is needed to extract data from memory.
3. No way to avoid using kernel with a software solutions.
4. Kernel controls the scheduling of access to the processor, controls all data flow to the storage locations.
5. Always require process and kernel memory to execute; overwrite possible evidence.

Solution

1. Patch the needed area of the kernel memory with trusted code.

2. Issues: untrusted kernel decreases the reliability of the evidence.

A Hardware based imaging procedure



Goal of the work

1. Implement a procedure that can make an accurate copy of volatile data.
2. Minimize the modification of both volatile and non-volatile data on the target system.
3. As OS and software applications are not much reliable, chose to use a H/W based solution.
4. Benefits:

- Can access memory without relying on the OS.
- No need to use system memory while running.

System level design

1. Primary components: Microprocessor, PCI controller, DMA.
2. Microprocessor is connected to ROM, SDRAM and external switch, an LED, and an external storage interface.
3. On board ROM – Firmware operating code for acquisition card.
4. SDRAM – To store variables, program stack, and other operating data.
5. LED – Provides device operation and status information to the user.
6. External Switch – Used to begin the imaging procedure.
7. Optional Components – Real-time clock, Secure serial EEPROM.

Role of PCI

1. Primary interface between the external adapter cards and internal system resources.
2. North bridge connects the host processor bus to the PCI bus.
3. North bridge also allows devices on the PCI bus to access system memory at speeds approaching the target processors's full native bus speed.

How DMA is used in the system

1. Provides block transfer of data between the PCI bus and the target's local processor memory.
2. No resource required from target machines processor.
3. During acquisition process:
   - Card takes control of the PCI bus.
   - Specifies the desired base address and block size of the system memory.
   - Card requests a DMA transfer of the system memory.

Imaging procedure

1. The acquisition card is powered on and completes its hardware initialization routines.

a. The acquisition card conducts a Power On Self Test. And halts if a failure occurs.

b. The acquisition card does not enable its PCI controller.

c. The acquisition card remains idle until the external switch is activated.

Imaging procedure (contd.)

2. Acquisition process begins when external switch is activated.

a. Activation and initialization of the external storage device.

b. Acquisition card enables its PCI controller.

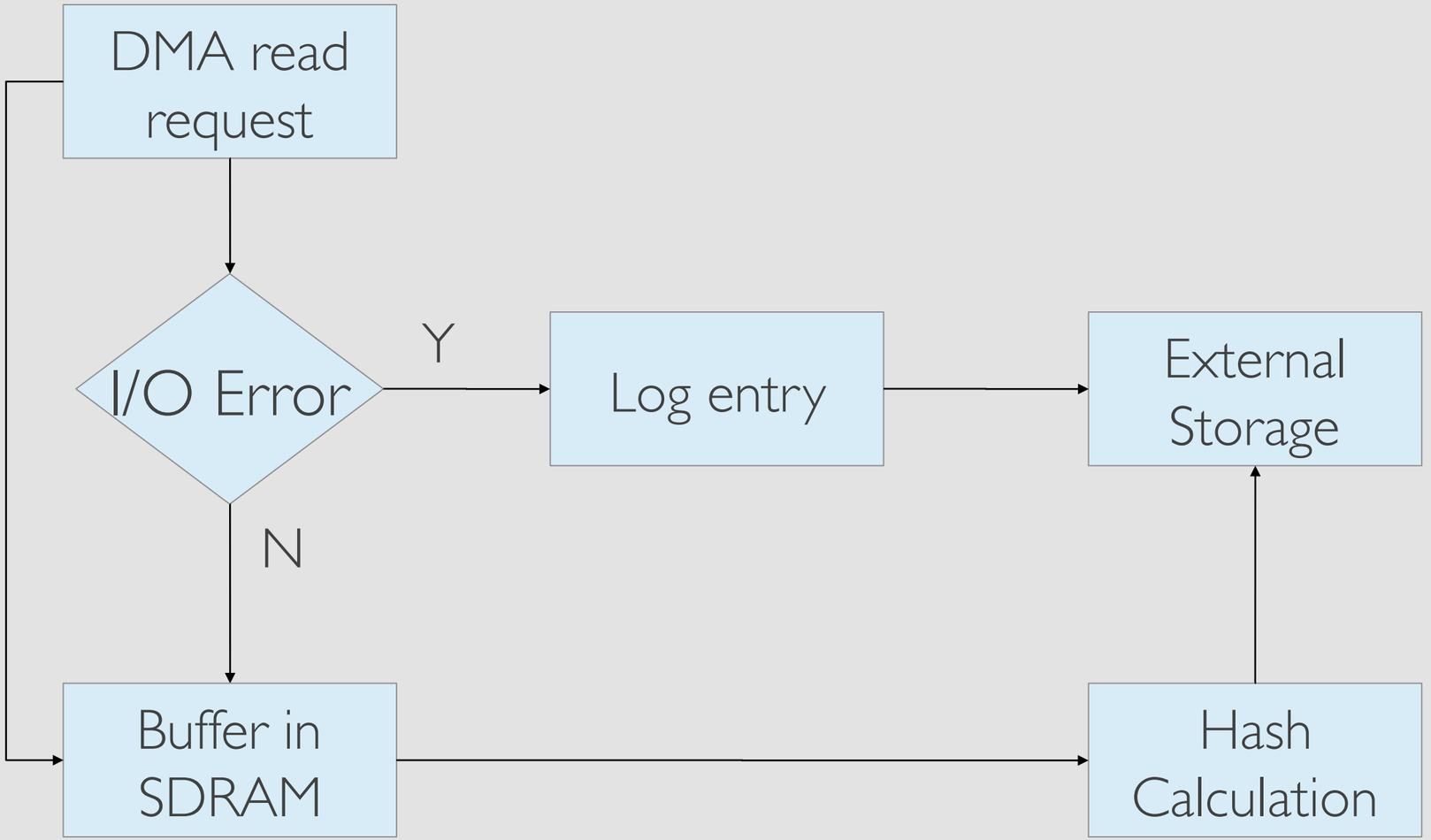
c. Acquisition card halts the processor, if possible.

d. A log entry is saved in the external storage.

e. Volatile system memory data is saved to the external storage device starting at physical memory address 0.

Imaging procedure (Loop.)

1. If next X bytes are protected, read the unprotected areas and write '00'h to the memory image.
2. Perform a DMA memory read request for next X bytes. Write it in SDRAM buffer.
3. If I/O error occurs, X bytes of '00'h are written to the memory image.
4. If no I/O error occurs, the acquisition card writes from SDRAM to the external storage.
5. If a hash value of the data is being calculated, then X bytes of data are added to the hash calculation.


DMA read request
I/O Error
Y
Log entry
External Storage
N
Buffer in SDRAM
Hash Calculation

Imaging procedure (contd.)

f. Hash value is added if needed.

g. Final log entry saved in the external storage

h. Acquisition card disables PCI controller, deactivates external storage.

3. Acquisition card returns to an idle state.

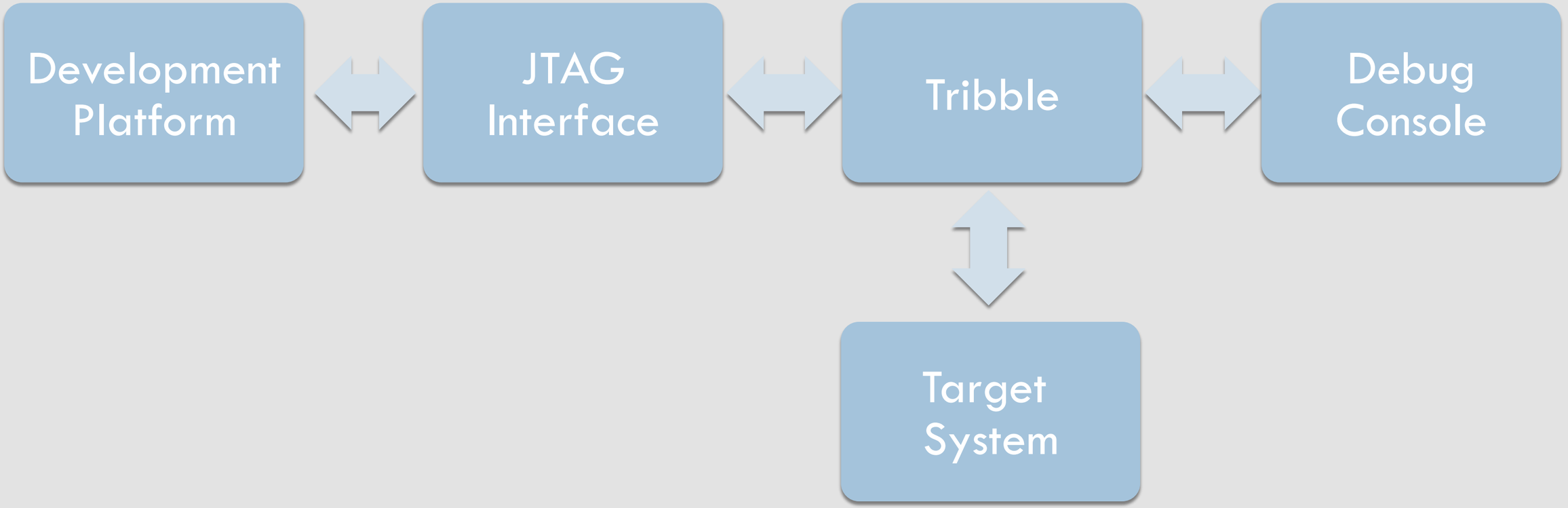
Tribble: The proof of concept device

- Intel IQ 80303 processor.
- 100 MHz Intel 80960JT core.
- Glueless interface to ROM and SDRAM.
- I2C bus interface.
- PCI-to-PCI bridge.
- DMA controller. Etc.
- http://www.youtube.com/watch?v=vJszLtalylk

Development Platform

- Dell Inspiron 8200 laptop.
- Windows 2000
- 1.8 MHz Intel Pentium 4M processor.
- 512 MB RAM
- Spectrum Digital SP1610 JTAG interface.
- Intel i960 CTOOLS.(gdb960 debugger)

Development Environment



Goal of the proof of concept

- To prove that system memory can be read via PCI device without modifying its contents.
- External switch was implemented – acquisition process was performed programmatically.
- External storage device was not implemented – contents of the retrieved memory was viewed using gdb960.

Test Procedures and Results

What to test?

Tribble reads actual volatile memory or not.

DMA reads memory requests or not.

Configured to read 4096 byte page of memory.

Later same page was read using dd and \\.\PhysicalMemory.

Output : Same result.

Test Procedures and Results (contd.)

- SoftICE tool was used (wrote 4 new byte data) to verify if dd and \\.\PhysicalMemory is providing correct result.
- Memory location with known value is read multiple times to check if the value is modified or not.
- Final test was done by acquiring all the memory space. Both cases results were almost same.
- Skipped memory from 0XA0000 to 0XC0000 (UMA)

Limitations

- Need to be installed prior to the incident.
- Plug and play features may pop up some notification regarding new device found, which may lead the attacker to make device driver to attack the card itself.
- Output can be analyzed only by using ‘strings’,’grep’ and hex editors. No automated tools yet.
- Difficult for the end user to operate.

Conclusion

- General process for volatile memory acquisition.
- Satisfy the process
- Initial results.
- Provides more reliable evidence than software based solution.

Future Work

- Performance test
- Halting target system without ill effects.
- Investigate potential attack against the card.
- Verify that the system memory is not written to during acquisition process.

THANK YOU