BMCLEECH — INTRODUCING STEALTHY MEMORY FORENSICS TO BMC

Tobias Latzo, Julian Brost, Felix Freiling

Security Research Group
Department of Computer Science
Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)
WHAT IS A BMC?

- Baseboard Management Controller (BMC)
- Microcontroller in a server (usually located on the mainboard)
- Monitor and control servers:
  - Read temperatures and adjust fan speeds
  - Control the server (KVM)
  - Protocols: IPMI, Redfish

RunBMC with an AST2500
MOTIVATION

MEMORY ACCESS HIERARCHY

ring 3
USER LEVEL
user emulators

ring 0
KERNEL LEVEL
kernel modules

ring -1
HYPERVERISOR LEVEL
VMM

ring -2
SYNCHRONOUS MANAGEMENT LEVEL
SMM

ring -3
ASYNCHRONOUS DEVICE LEVEL
DMA devices

BMCs are highly integrated into the system.
Why don’t we leverage the BMC for memory forensics?
UTILIZING PCILEECH

- PCILEech\(^1\) is very powerful
  - Read and write memory
  - Inject kernel code on the target
  - Push/pull files
- Shorting Windows login screen

- PCILEech’s `rawtcp` device:

```c
enum rawtcp_cmd {
    STATUS,
    MEM_READ,
    MEM_WRITE
};
```

```c
struct rawtcp_msg {
    enum rawtcp_cmd cmd;
    uint64_t addr;
    uint64_t cb;
};
```

[1] https://github.com/ufrisk/pcileech
implement the (simple) rawtcp_msg to make use of all of PCILeech's features!
ARCHITECTURE & IMPLEMENTATION

BMCLEECH RUNS ON OPENBMC

- Linux distribution for BMCs
- Big companies want gain control over BMCs in their servers
- RunBMC²: standardization of hardware

ARCHITECTURE

TARGET

CPU

MEMORY

getmem

BMC

BMCLeech

libaspeedxdma

aspeed-xdma

TARGET

FILE

PCILeech

DEDICATED ETH

FORENSIC WORKSTATION

DUMP.BIN

Forensic Memory Analysis
Evaluation
EVALUATION

CRITERIA OF MEMORY ACQUISITION TECHNIQUES

▸ Correctness
  ▸ Actual values when snapshot was taken
  ▸ Atomicity
  ▸ Time between the acquisition of the first and last memory region
  ▸ Integrity
  ▸ How much does the memory acquisition process change memory?

ATOMICITY

- BMCLeech acquires memory via DMA
- DMA-based approaches are not good in terms of atomicity[^4]
- BMCLeech will perform similarly as other DMA-based tools

[^4]: Michael Gruhn and Felix C Freiling. Evaluating Atomicity, and Integrity of Correct Memory Acquisition Methods. Digital Investigation, 16:S1
EVALUATION

INTEGRITY

- DMA-based
- BMCLeech fully preserves integrity
CORRECTNESS

- Methodology

EVALUATION

BiMCLeech

LiME
COMPARISON OF THE DIFFS - LIME

Average Diff Rates:
Page-wise: 8.09%
Byte-wise: 2.38%
COMPARISON OF THE DIFFS – BMC

Average Diff Rates:
Page-wise: 7.88 %
Byte-wise: 2.35 %
COMPARISON OF THE DIFFS – SIMULTANEOUSLY

BMCLeech

LiME

Time

Average Diff Rates:
Page-wise: 6.59 %
Byte-wise: 1.72 %

diff(l_x, b_x)
COMPARISON OF THE DIFFS – SIMULTANEOUSLY (SHIFT)

Average Diff Rates:
Page-wise: 6.96 %
Byte-wise: 2.11 %

diff(l_{x+1}, b_x)
DIFFERENT BYTES PER PAGE
**SUMMARY**

- BMCLeech makes BMCs forensic-ready
  - stealthy
- compatible to established tools (like PCILeech)

**Future Work:**
- Access > 4 GB
- Increase performance
- More platforms
THANKS TO...