Analysis of Out-of-Band Management Security Based on IPMI Protocol

Hong Xia [1,a], Xiongfei Zhao [1,b,*]

[1] North China Electric Power University Beijing, Beijing, China

[a]summerday@ncepu.edu.cn, [b]zhaoxiongfeifei@qq.com

* Xiongfei Zhao

Keywords: IPMI, Out-of-Band, Vulnerability.

Abstract. Intelligent Platform Management Interface (IPMI) has been widely used in the out-of-band management functions, IPMI protocol itself has some security issues, and major server manufacturers further develop independent out-of-band management products based on t, but also increased the out-of-band management Chaos. This paper introduces the principle of the standard IPMI protocol, analyzes IPMI vulnerability from three aspects, and puts forward the improvement suggestions.

1. Introduction

With the rapid development of computer technology, big data, cloud computing and mobile Internet technology is widely used, the server is increasingly becoming an integral part of the network. Individual or small companies usually only need one or several servers to meet the demand, large companies or research institutes often need more servers to form a cluster to collaborate computing, storage. These application system management software is running on a dedicated server platform, if these servers have problems, will have no small impact on the user. Large Internet companies and cloud service providers often have hundreds of thousands of servers. Such a large number of servers need to fully consider the power resources, environmental impact, cooling problems, to establish a dedicated data center, its operating costs and management costs are very large.

2. Server management

At present, the management methods of the server are divided into three types: manual-based management, software-based management and hardware-based management:

2.1 Manual-based management

Traditional management services rely on manpower to the site for troubleshooting, this management approach used in early server management. Due to the small number of early servers, you can arrange a professional server maintenance personnel to the scene for server monitoring, inspection and maintenance. This approach is inefficient, and with the increase in the number of servers, limited maintenance personnel is difficult to effectively manage.

2.2 software-based management

Most of the operating system running on the server remote desktop connection, SSH, Telnet and other remote monitoring methods to manage. In addition, third-party server management software can be installed on this basis, These server management technologies are basically in-band management, that is, control information and data information using the same physical link. This reduces the security of server management, on the other hand also increased the network traffic load, likely to cause data congestion. As the software is running at the operating system level, cannot achieve remote installation system, remote boot and other functions. Once the server is down or the operating system is down, the software will quickly lose its ability to manage.

2.3 hardware-based management

Between the software and hardware of the server, it has a separate embedded subsystem. The motherboard has a separate network interface, memory and a microcontroller, that is, the baseboard management controller (BMC). The operation of the host does not have any effect on the BMC system, and the server maintenance personnel can remotely control the BMC through the IPMI interface. As long as the server connected to power, you can remotely turn off the machine, real-time monitoring CPU, memory, fans, network cards, hard drives and other equipment running.

Out-of-band management is currently widely used in a variety of network equipment, mainly through the out-of-band management chip for the administrator to provide hardware-level remote management capabilities. Currently BMC chip and out-of-band management functions have become a server and other network equipment standard.

3. Introduction to IPMI

3.1 Definition of IPMI

IPMI is an open standard hardware management interface specification that defines the specific method of communication between the embedded management subsystem. IPMI information is communicated through the BMC. IPMI is an industry standard for managing peripheral devices used in an Intel-based enterprise system. It was designed by Intel, HP, NEC, and Dell and SuperMicro. As a hardware-level interface IPMI at the bottom of the system management software, as shown in Figure 1:

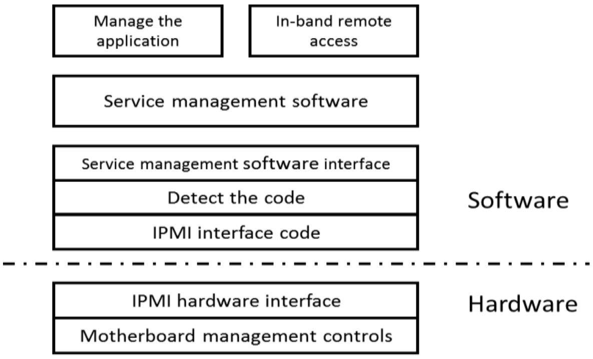

Fig. 1. IPMI and its management software structure

3.2 Principles of IPMI

IPMI is the core of BMC, also known as the server processor, is a dedicated chip. BMC is a stand-alone module, does not rely on the operating system, BIOS or server processor to work, it is installed on the server board a separate board, running alone in the system and no agent management, as long as the IPMI firmware and BMC can work. Because IPMI has a good autonomy, it can run independently of the operating system. When the operating system does not respond or the server is powered off, the administrator can still switch the machine, extract information and other operations, get rid of the operating system management limits. Since IPMI is running independently of the operating system, the administrator can still access and restore the system if the operating system is not responding or the server is powered off.

IPMI uses the instructions specified in its specification to send commands to the BMC to complete all IPMI functions. After the BMC accepts the command, the time message is recorded in the system event log. It is also responsible for describing the sensor in the system and recording the sensor data. IPMI 2.0 newly added Serial Over LAN (SOL) for the remote access system provides a convenient, in the IPMI painting process, SOL can change the direction of the local serial port to provide object emergency management services, Windows dedicated management Console or Linux serial console access control. The BMC can change the direction of transmission to the serial port information on the LAN and can be used to view the server startup status and provide an emergency management console to standardize the diagnosis and repair of faults. This process has IPMI firmware to intercept data, so no need to consider the server vendor. IPMI overall framework, as shown in Figure 2:

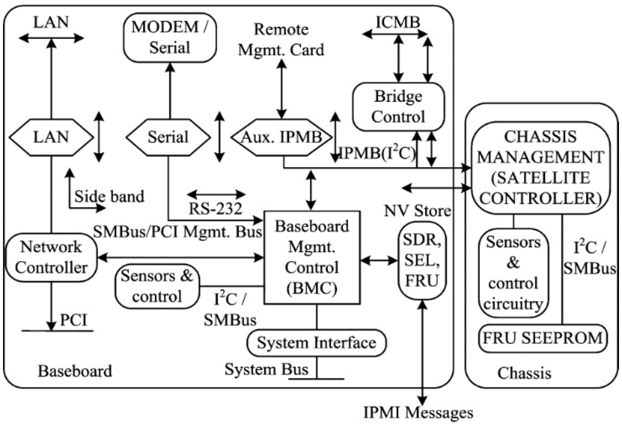

Fig. 2. IPMI framework

4. IPMI vulnerability analysis

In order to facilitate the unified management of the server, multiple servers often share an IPMI password, resulting in hackers once access to IPMI authority, it will have a strong destructive power. IPMI has three types of security issues: IPMI protocol itself, OEM vendor implementation and BMC issues.

4.1 .IPMI protocol vulnerability

IPMI specifications are flawed, allow intruders to access passwords remotely, and grant system-level access without using any passwords. It also requires that the password must be stored in an unencrypted way, which is a very unusual and unsafe practice, which means that anyone who enters the server or has physical access can find the password used to protect the internal company's secret room. Making IPMI so useful with the same flexibility and ability, coupled with the lack of cross-vendor security tools, research and knowledge that makes unsafe implementation.

4.2 OEM vendor vulnerabilities

Vendors often redefine their own IPMI - Dell has iDRAC, HP has iLO, IBM has IMM2, etc. - but they have generally added many features and secret implementations. Almost all vendors have the least secure features of IPMI enabled by default. Fixing BMC security issues is not possible because the vendor only allows it to run its own proprietary software. The user can not view any activity on the BMC, and there is no forensic or auditing tool. As a last trick: BMC's attackers may not be able to remove them without knowing the vendor spoofing or physical damage to the BMC.

4.3 BMC vulnerabilities

The worst problem with the IPMI protocol is that the protocol requires that the plaintext store or password for the password on the BMC can be recovered on demand. Most modern cryptographic algorithms use a hash code to authenticate. IPMI uses dynamic hash to verify the Request

Auth Code = H(password + temporary session ID + challenge string + password) (1)
(where H(x) is a hashing function):

Before the request, the remote client and the managed BMC determine the challenge string and session ID, and can change with any session request, and the hash cannot be calculated when there is no clear password at hand. Some BMCs seem to save plaintext passwords on "secure" storage, which is hard to read after starting the sequence, but even so, it is easy to scan the password if the attacker has root access on the original BMC memory.

4.4 Improve methods

Formal consideration of IPMI serious loopholes, some companies even take the extreme measures to disable IPMI on the motherboard, of course, this is not desirable. For the IPMI vulnerability that has been discovered, the patch is updated in time, and the latest version of the IPMI standard protocol was introduced in April 2015. Strengthen the server remote management of the authentication mechanism and audit work, regularly update the IPMI password, to avoid a password management hundreds of servers. In addition, the establishment of server-specific remote management link, so that control information and data isolation, so as to avoid being attacked.

5. Summary

With the large data, artificial intelligence and other technologies widely popular, it highlights a series of data security issues have gradually been the concern of scholars. Outside the management of the server approach to expose more and more security risks, but the current focus on the security field in the operating system and software vulnerabilities, such as the eternal blue. This paper first introduces the IPMI concept and firmware structure, analyzes the working principle of IPMI from the aspects of message passing, bus structure and interface standard, discusses the IPMI protocol itself, the implementation way of OEM vendors and the security problems of BMC loopholes in three aspects,

References

[1] Kozak, T., P. Predki, and D. Makowski. "Real-time IPMI protocol analyzer." Real Time Conference IEEE, 2011:1-7.

[2] Drochner, M., et al. "IPMI test software for MicroTCA developments." Real Time Conference IEEE, 2013:1-3.

[3] Zawada, A., et al. "ATCA Carrier Board with IPMI supervisory circuit." International Conference on Mixed Design of Integrated Circuits and Systems IEEE, 2008:101-105.

[4] Leangsuksun, C., et al. "IPMI-based Efficient Notification Framework for Large Scale Cluster Computing." IEEE International Symposium on CLUSTER Computing and the Grid IEEE, 2006:23.

[5] Yu, Zhilou, and H. Ji. "Notice of RetractionResearch of IPMI Management Based on BMC SOC." International Conference on Management and Service Science IEEE, 2010:1-3.

[6] Brandes, S, I. Cosovic, and M. Schnell. "Reduction of out-of-band radiation in OFDM systems by insertion of cancellation carriers." Communications Letters IEEE 10.6(2006):420-422.

[7] Doshi, Bharat T, et al. "ATM network architecture employing an out-of-band signaling network." US, US5568475. 1996.

[8] Garcia-Garcia, Joan, J. Bonache, and F. Martin. "Application of Electromagnetic Bandgaps to the Design of Ultra-Wide Bandpass Filters With Good Out-of-Band Performance." IEEE Transactions on Microwave Theory & Techniques 54.12(2006):4136-4140.

[9] Wong, Sai Wai, and L. Zhu. "Quadruple-Mode UWB Bandpass Filter With Improved Out-of-Band Rejection." IEEE Microwave & Wireless Components Letters 19.3(2009):152-154.

[10] Aparin, V., and C. Persico. "Effect of out-of-band terminations on intermodulation distortion in common-emitter circuits." Microwave Symposium Digest, 1999 IEEE MTT-S International IEEE, 2002:977-980 vol.3.

[11] Zhong Li, et al. "Compact ultra-wide bandpass filter with good out-of-band performance." International Conference on Microwave and Millimeter Wave Technology IEEE, 2008:341-343.