Out-of-Band Network Management

Felix Emmert
Betreuer: Oliver Gasser
Seminar Innovative Internet-Technologien und Mobilkommunikation WS2014
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: felix.emmert@tum.de

ABSTRACT

Out-of-band network management is becoming more and more popular amongst high tech companies since high availability of network services is becoming more and more important. Especially servers with built in out-of-band management capabilities are growing in numbers as the increasing demand in bandwidth forces companies providing web services to outsource their networks to colocation centers that often lack the possibility for physical access. This article describes different benefits for network administrators, especially for administrators of out-of-band management devices for servers. Despite of the benefits this article mainly focuses on security issues surrounding out-of-band management devices for servers, analyzing the firmware of a Dell iDRAC 7 which is the latest out-of-band management device for Dell's rack servers. It shows what privileges potential attackers may gain by compromising out-of-band management devices. Finally some practical advise for system administrators on how to secure their systems against attacks is given.

Keywords

out-of-band, network management, IPMI, BMC, iDRAC

1. INTRODUCTION

Today it has become more and more popular for small and medium sized businesses to no longer host their web services in-house, but to rent computing power from specialized providers. The providers offer the needed infrastructure for storing, computing and delivering huge amounts of data in their colocation centers to many different customers. As a consequence of outsourcing computing needs to providers, it is in most cases no longer possible for system administrators to physically access their companies' servers.

Many systems like servers or networking hardware offer remote in-band management solutions. In-band management is accessible as long as the system is running but it cannot fully satisfy the need of physical access since it lacks efficient strategies to recover the system in case of emergencies like misconfigured networks or boot failures.

Out-of-band management aims to reduce the weak spots of in-band management by providing remote management functionalities independent of the system's operating state. In many cases this is achieved by independent sub-systems connected to the system they are managing (further called the "main system"). Many out-of-band management systems for servers have their own data storage (mainly flash storage) containing an own operating system as well as dedicated power supply and Ethernet ports. That way it is, for instance, possible to remotely power the main system on or off, access the system's keyboard, view the display's output and monitor the system's hardware even if the main system fails to boot.

While out-of-band management systems provide some major benefits for system administrators, they can also serve as backdoors for attackers. After gaining access it is possible to run various attacks like eavesdropping, compromising the main system or even using the out-of-band management system itself for future attacks (like as a botnet client). Once an attacker manages to modify the operating system running on an out-of-band management device, it can be very difficult to detect the intrusion and even more difficult to remove the threat since the malware survives a complete reinstallation of the main system. Malware residing on out-of-band management systems can actually carry over from one owner of the system to another, especially in the event of rented systems like servers in colocation centers.

This article mainly focuses on out-of-band management systems used to manage servers. It is showing their capabilities and security concerns surrounding them. It demonstrates some security issues analyzing Dell's latest iDRAC 7 firmware and gives advise on how to secure existing out-of-band server management devices.

2. RELATED WORK

Parts of this article are based on the work of Anthony J. Bonkoski, Russ Bielawski and J. Alex Halderman [1]. These authors analyze the security of IPMI (Intelligent Platform Management Interface), which is the industry standard for server oriented out-of-band management devices [9]. While they analyze Supermicro's implementation of an IPMI based out-of-band management system for servers they find many security issues similar to those found in Dell's iDRAC 7 which is analyzed in this article. Bonkoski, Bielawski and Halderman found an exploit inside the login system for the web interface of Supermicro's devices. This exploit is caused by the use of the insecure "strcpy" function. Bonkoski et al. developed a proof-of-concept buffer overflow attack to show the risks of the found exploit. Additionally they uncovered shell injection vulnerabilities which allow any user of Supermicro devices to execute system commands and even to run own code by downloading it onto the out-of-band manage-

doi: 10.2313/NET-2015-03-1_10

ment system using "wget" which is a standard GNU/Linux system tool for downloading web content. They found that at least 41,545 devices may be affected by these exploits thus being under immediate threat.

Recently Andrei Costin et al. published an article [2] which analyzes a set of 32,356 different embedded firmwares using a self designed automated system. While these firmwares are from all kinds of different devices the authors report similar security issues like the issues found in this article including the extraction of SSL certificates together with the according unencrypted private keys of about 35,000 devices connected to the Internet. They also found many hard-coded login credentials used for telnet, system or web logins. Additionally they discovered other backdoors like unsecure daemons, exploitable web interfaces and authorized SSH keys which can be used for remote connections.

3. OUT-OF-BAND MANAGEMENT TYPES

Out-of-band management systems are common in more sophisticated network hardware like servers. They provide system administrators with possibilities to manage their systems even in the event the main system is not running or otherwise unavailable.

Many routers, switches and hubs made by Cisco come with out-of-band management systems accessible via a "Network Management Module" connected to serial console ports on the devices [3] [4] or directly via a special ethernet ports on newer hardware [5]. That way it is possible to recover devices or entire networks that are no longer accessible via in-band management. The remote management capabilities can be extended to be accessible via backup networks or even wireless (GSM) by using aftermarket hardware [6].

In case of servers without built-in out-of-band management systems one of the most basic solutions for partial out-of-band access is the use of a KVM over IP device like the Peppercon LARA [7]. KVM means "Keyboard, Video, Mouse". KVM over IP devices enable their user to remotely view the system's display output and forward keyboard and mouse input to the system over a TCP/IP network. That way it is possible to interact with the system while it is still booting to change BIOS parameters or to fix boot issues. Some devices also include remote access to the system's hard reset and ON/OFF switch.

More dedicated servers offer built-in solutions like Dell's iDRAC, HP's iLO, Oracle's iLOM, and Lenovo's IMM. Those out-of-band management systems run on an embedded microcontroller called BMC (Baseboard Management Controller) which is integrated into the main system's hardware (either directly or via daughter card) [1]. The BMCs run their own operating system residing on dedicated data storage, mainly flash storage. In many cases the BMCs have access to the PCI bus, various I/O ports and sensors enabling it to fully control the server. Additionally the BMCs have their own network interface controllers (NICs) or at least access to one of the system's NICs via a "side-band" interface. The BMC may have an own power supply and/or a battery.

Figure 1 shows a basic setup of a server featuring an integrated out-of-band management device. It shows how the Dell iDRAC 7 device used for investigation in the making of this article has been connected to the Internet by a popular German colocation center operator.

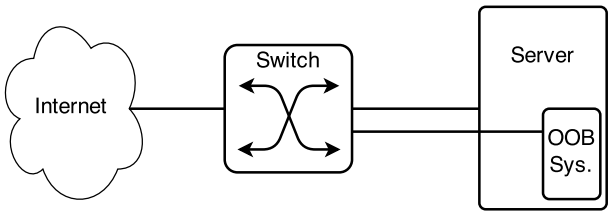

Figure 1: Basic setup of a server with an integrated out-of-band management device

4. SERVER MANAGEMENT

Most out-of-band management system implementations for servers are based on IPMI (Intelligent Platform Management Interface), which is the industry standard. In addition to IPMI many vendors offer additional user interfaces or functionalities. IPMI implementations commonly provide the following core functionalities.

4.1 Chassis Control

IPMI allows users to control the power state of the main system. It is possible to remotely power on or off the main system or perform a hard reset. Additionally vendors may allow to trigger a soft-shutdown (by emulating a fatal overtemperature) as well as pulse diagnostic interrupt or power cycling [9].

Additionally it is possible to perform other chassis operations like physically identifying itself (useful in colocation centers) or configuring power restore settings (like power on after AC power is restored).

4.2 System Provisioning

Many out-of-band management systems for servers include the possibility to provide the server with bootable media needed for installing a new operating system or booting into a live system for recovery. This can be done by simply selecting a physically connected drive to boot from (like USB flash drives) but it is also possible to remotely provide the system with image files (like iso) which are then connected to the server as virtual DVD drives [10]. Network boot via PXE may also be possible if supported by the server's BIOS.

4.3 KVM over IP

KVM over IP provides system administrators with remote access to the system's keyboard, video output and mouse. One major benefit of KVM over IP is the possibility to remotely debug system boot failures as no further software is needed to fully control the server.

Manufacturers often include KVM over IP abilities into their BMCs. To use built in KVM over IP, a vendor specific client application (most of the time Java based) is needed. This application connects to the BMC via TCP port (commonly port 5900).

doi: 10.2313/NET-2015-03-1_10

4.4 Watchdog Timer

A Watchdog Timer is a function designed to detect system malfunctions. To achieve that it is continuously decrementing a timer [9]. If this timer reaches the value of "0", specific actions like a system reset can be triggered. To prevent this behavior called "timeout", the system needs to continuously reset the timer to prove that it is still running. Apart from that it is possible to completely disable the Watchdog Timer.

Every BMC implementing IPMI must include a watchdog timer that is able to perform system resets [9]. Other possible timeout actions may be system power off or power cycle. Additionally, vendors may include pre timeout interrupt functionality triggering shortly before the actual timeout. This can be used to attempt a nonviolent system shutdown prior to hard resets.

4.5 Serial Over LAN

Serial Over LAN (SOL) is a feature allowing to remotely connect to the main system using the system's serial interface [1]. This can be used to remotely access the server's BIOS and bootloaders like Grub. Additionally some operating systems like GNU/Linux can be configured to accept serial console connections [8].

4.6 Web Interface

Many IPMI implementations operate an optional web interface on ports 80 and 443. The web interfaces enable users to check the system health, view and modify the BMC's settings and access various other features of the out-of-band management system like chassis control or system provisioning. Additionally many implementations allow users to download the application needed to access the KVM over IP feature directly from the BMC's web interface.

4.7 Command Line Interface

Despite web interfaces the most common way in accessing IPMI devices is via command line interface. IPMI specifies a protocol called IPMI over IP on UDP port 623 for this purpose. Additionally, many implementations host an optional SSH daemon on TCP port 22. The command line interface usually offers access to all BMC commands, settings and outputs the user is allowed to interact with.

5. SECURITY CONCERNS

Out-of-band management systems like IPMI devices are built to manage and restore the main system they are connected to. For being able to do so, they often need extensive control over their main system. While this is intended, it also brings huge security concerns along. An attacker that somehow gets access to an IPMI device will be able to misuse it for many different purposes. To make things worse, IPMI devices tend to have quite a large attack surface.

The following sections will shed light on some existing security issues, give an overview on possible threats imposed by compromised BMCs and advise on some best practice to harden IPMI enabled systems.

5.1 Dell iDRAC 7 Attack Surface

This section focuses on the attack surface of Dell's iDRAC 7, but it may also be true for other vendors' IPMI implementations.

A port scan on a Dell iDRAC 7 shows open TCP ports 80 and 443 for the internal appweb web server as well as TCP port 5900 used by the KVM over IP Java application. Additionally theres an SNMP agent on UDP port 161. Other services like an SSH daemon on TCP port 22, a TELNET daemon on TCP port 23, IPMI over IP on UDP port 623 and a VNC server on TCP port 5901 are deactivated by default on the investigated Dell iDRAC 7. All of these network services can be deactivated or configured to run on different ports with the exception of IPMI over IP whose port is fixed.

The internal web server of a Dell iDRAC 7 uses default SSL certificates which are not generated by the BMC upon initialization but instead shipped with the firmware, together with the appropriate unencrypted private keys. Although, it is possible to change the used SSL certificates, system administrators might fail to do so enabling attackers to decrypt the BMC's network traffic or set up phishing sites.

All remote management services do support basic password authentication which is enabled by default. This makes it possible to run attacks using known username/password combinations or brute force. If the system uses it's default SSL certificate for HTTPS traffic, it is also possible to acquire the login credentials by sniffing and decrypting the network traffic or phishing.

A severe weakness in the IPMI over IP protocol allowes for attackers to get the "HMAC" hash of the BMC's login credentials [12] [14]. This enables hackers to perform offline password cracking attacks. Since the BMC tells the attacker whether an username is valid or not without checking the password first, such an attack can be very efficient. This weakness exists since IPMI version 2.0.

While Dell's iDRACs do have default login credentials (root/calvin), the devices do encourage users to change them since firmware iDRAC 7 1.30.30 if the default login credentials are still in use [13]. On the investigated iDRAC 7 devices those credentials have been changed by the colocation center operator (Hetzner) prior to delivery of the system. Still there may be many outdated versions out there that don't warn their users. Additionally some administrators may not be aware of the existence of a BMC inside their servers hence not changing the credentials at all.

Other manufacturers also ship their devices with default login credentials. These credentials are shown in Table 1. The only manufacturer that uses random default passwords for shipping is HP.

5.2 Affected Systems

Having shown some weaknesses of IPMI devices, the next question would be the number of public reachable devices using insecure default settings. To get appropriate data, a network scanning tool is needed. Zmap is a powerful research tool capable of scanning the entire public accessible IPv4 range in less than an hour given enough bandwidth

Manufacturer	Default Username	Default Password
Dell	root	calvin
HP	Administrator	*random 8 char*
IBM	USERID	PASSW0RD
Supermicro	ADMIN	ADMIN
Fujitsu	admin	admin
Oracle/Sun	root	changeme
ASUS	admin	admin

Table 1: Common default login credentials of IPMI devices by manufacturer [14]

[15]. This analysis uses public available HTTPS scan data gathered by Zakir Durumeric et al. on the 29th of January 2014 [16].

The relevant part of the data consists of two tables, one containing all scanned HTTPS enabled IP addresses together with the SHA-1 fingerprint of the used certificate. The other table contains details about every certificate found in the scan. A first check against the SHA-1 fingerprint used in the most recent firmware of Dell's iDRAC 7 at the time of writing (1.57.57) shows 11,659 devices running on public IP addresses.

A deeper check was performed by gathering the SHA-1 fingerprints of every certificate containing the string "iDRAC" inside it's subject and matching against any of them. This results in a total of 46,490 devices on public IP addresses. Since this number contains iDRAC devices including older ones the subtraction of the two numbers shows that 34,831 devices may not be running on the latest iDRAC 7 firmware.

Due to administrators being able to change the certificate used by their devices this number only serves as a lower bound approximation of the total number of Dell iDRAC devices that are accessible via public IP addresses. However, the found devices may be very vulnerable because they do use the default certificate.

Further analysis could be done by accessing the home page of every IP hosting a web interface on well known HTTP or HTTPS ports by pattern matching against known contents like logos or headers.

5.3 Possibilities for Attackers

Attackers who gained access to an IPMI device can benefit from it in several ways. This section shows a selection of different possible use cases for Hackers.

5.3.1 Denial of Service

The easiest thing to do with a compromised BMC is to perform a Denial of Service (DoS) attack on the host system. Attackers can simply turn off the main system and prevent it from rebooting without having to modify any part of the software by changing the boot behavior. While this might not be the smartest of attacks as it is easy to detect the attack and restore the system, it could leave larger networks vulnerable to follow up attacks.

More stubborn attackers could modify the BMC to emulate false hardware faults or manipulate shared NICs to drop legit network traffic. Doing so would make it harder to detect the attack itself or its source (the BMC) possibly causing the system owners to believe that their server is damaged.

5.3.2 Eavesdrop

Once an attacker manages to compromise the BMC, the attacker could start eavesdropping without attracting attention. This can be achieved in various ways.

One method would be packet sniffing on the NIC. This could target the main system as well as other systems connected to the same network. Attackers could try to gain system passwords or capture various sessions. It would even be possible to perform man-in-the-middle attacks trying to spy on weakly encrypted network traffic.

Eavesdropping may also be done by using the KVM over IP features (since KVM over IP shows the server's display output) or by analyzing different system logs.

5.3.3 Take over the main system

One of the goals of many attacks may be getting control over the main system connected to the out-of-band management system. Since the BMC is designed to control the main system, this attack is not very difficult. An attacker could simply boot some live operating system and mount the harddrive as root. That way the attacker will be able to modify any part of the server's operating system to his needs.

Although encrypting the system drive may prevent this from happening, it would still be possible to modify the BMC's system and eavesdrop on the encryption password the next time an administrator enters it at a system reboot. Since system reboots can be enforced using the BMC's abilities attackers won't have to wait for an opportunity (which could take quite some time as it is common that servers are rarely rebooted at all).

Additionally it might also be possible to use the KVM features to gain access to the main operating system without the need of rebooting it.

5.3.4 Persistent rootkits

Attackers who manage to modify the operating system of the BMC may be able to install highly persistent rootkits due to the closed and independent nature of the BMC. Such malware will survive any action taken to clean the main system like reinstallation or even a complete replacement of all system drives as the BMC uses it's own storage. Additionally it may remain undetected for a long period of time and possibly carry over to new owners [1].

Rootkits could be further enhanced by being able to detect firmware updates or resets and modify the new firmware on the fly. Doing so would make it close to impossible for most administrators to ever get rid of the rootkit without replacing the whole out-of-band management device.

5.3.5 BMC botnets

Another scenario would be using the out-of-band management hardware itself for future attacks like in a botnet [1].

Botnets are large networks of infected systems which can be used for large scale attacks on single targets (like DDoS attacks) or for attacking huge amounts of different targets. Botnets can also serve as a source of computing power that can be used to do massive calculations like for example cracking passwords or generating crypto currency.

While it might not seem to be very promising to use BMCs for botnets due to their limited computing power, the lifespans of BMC botnets may be very long if combined with persistent rootkits. Other advantages of such botnets would be their huge network bandwidth and availability due to the fact that many servers featuring an out-of-band management system are located inside colocation centers or other facilities with massive network backbones.

Such botnets could come into existence in very short periods of time if attackers manage to remotely capture BMCs as they mostly run a very limited variety of different firmwares. Infected BMCs have already been reported [11] and it is just a small step to combine them into networks.

6. IDRAC 7 FIRMWARE ANALYSIS

This section will focus on a deeper analysis of Dell's iDRAC 7 firmware 1.57.57 which is the most recent firmware for the iDRAC 7 found in a Dell PowerEdge R720 at the time of writing. The firmware is available on Dell's public ftp server [17].

The downloaded .EXE file can be extracted using UnZip 6.0 [18]. The resulting files include the actual firmware image inside a folder named "payload". Examining the image file named "firmimg.d7" using Binwalk v2.1.0 [19] shows that it contains a Linux kernel followed by two "squashfs" filesystems. These filesystems can be mounted using the offset provided by Binwalk or extracted using Binwalk itself.

The first and bigger filesystem contains the Linux root filesystem, the other filesystem contains various default settings as well as installation scripts.

It is possible to detect modifications of the firmware since it is signed by an ASCII armored PGP signature at the end of the file.

Further inspection of the root filesystem shows that it contains the iDRAC 7 default SSL certificate together with it's unencrypted private key. This alone generates a huge risk as attackers may setup phishing sites with the exact same certificate as found on the original iDRAC web interface. So even if some people trust the default certificate of their iDRAC 7 believing it was generated upon first initialization instead of being shipped with the firmware, they also trust every other iDRAC 7 with a similar firmware and they trust the phishing sites. If done right, a phishing site can not be distinguished from a default iDRAC 7 web interface. Such a site may yield a lot of valid login credentials if propagated to administrators managing Dell iDRACs. Since the iDRAC 7 devices used for investigation always got a public IP address that was in the same /30 IPv4 subnet as the main server it may be quite easy to get a lot of correct email addresses of related system administrators.

User	Password as salted MD5 hash
root	1fY6DG6Hu$OpwCBE01ILIS1H/Lxq/7d0
user1	1nVOr80rB$HDAd6FRlG24k/WN4ZuYPC0

Table 2: Account names and password hashes found in the shadow file inside Dell's iDRAC 7 firmware 1.57.57

Additionally to having the ability of creating phishing websites using the default certificate attackers could also decrypt any captured network traffic between a Dell iDRAC 7 and it's operator using the default certificates. This may also provide them with login credentials or they could act as a man-in-the-middle by altering and re-encrypting the network traffic.

Besides that the system's shadow file (shown in Table 2) containing two shell enabled system accounts together with salted MD5 hashes of their passwords has been found. Since the password hash of the root account did not match with the default credentials (root/calvin) these may be the credentials for the underlying GNU/Linux system as opposed to the login credentials for IPMI access.

Dell's iDRAC 7 seems to be running on a Renesas SuperH H4 CPU. Since this architecture is not very common, it is hard to find any free decompiler that works. Instead the disassembly tools of the GNU toolchain for the Renesas SH7751R CPU [20] have been used to inspect parts of the web interface back-end.

Basic analysis of the web interface back-end which is inside the
iDRAC's cgi-bin shows that C's "strcpy" function well known for it's security issues [21] has been used within multiple parts, including the login function. This could potentially result in buffer overflow attacks. Since in-depth analysis of assembly code would go beyond the scope of this article, it has not been further analyzed. If a buffer overflow attack is possible that would mean that anybody could access a Dell iDRAC 7 that runs on a public IP. Moreover this can be an entry point for code injections rendering the system extremely vulnerable to more complex attacks like rootkits.

7. HARDENING IPMI DEVICES

Since IPMI devices tend to have security issues this section aims to give advice on how to harden IPMI devices. Following these suggestions will result in a lower attack surface presented to the public Internet.

Any operator of an IPMI device providing a web interface should install a custom SSL certificate. This certificate should not include information about the nature of the device to make it harder to identify. It is critical that the new certificate is not uploaded using a public network. Doing so would provide attackers with the new certificate since they can decrypt the network traffic which is encrypted with the default SSL certificate. Instead a private network should be used to transfer the certificate. In case of a Dell iDRAC 7 it is also possible to use SSH to do so if the SSH host keys identifying the system have already been securely exchanged. On the investigated Dell iDRAC 7 devices these keys have been

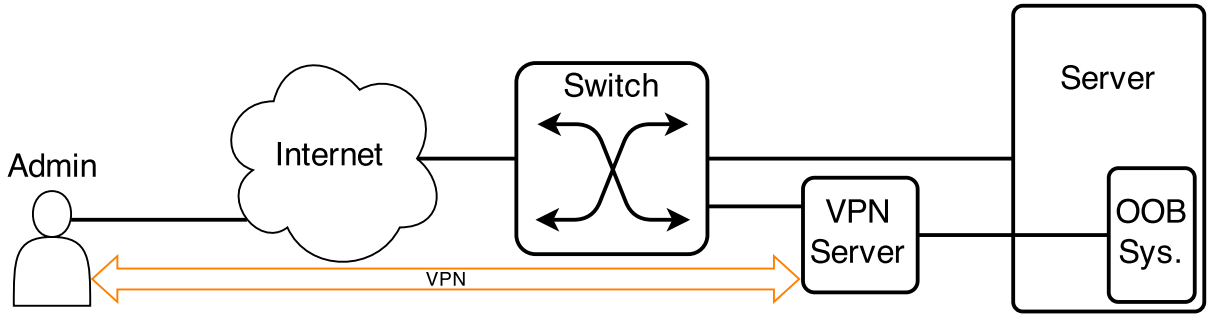

Figure 2: Out-of-band management device secured by a VPN

generated by the BMC upon first initialization.

Additionally, to changing the certificate IPMI devices should always operate inside a secure, closed network. Especially IPMI over IP should never be enabled outside of a secure network due to it's security weakness. In case of some IPMI implementations like a Dell iDRAC 7 it is possible to use VLAN tagging [22] to separate the device from the public Internet. Since remote access is needed in colocation center environments, secure VPNs like IPsec or SSH tunnels can be used. The gateways used to forward traffic to the closed network of IPMI devices have to be secured. Other possibly vulnerable parts of the internal network like web or mail servers should not have access to the gateways. In case high availability is crucial redundant gateways can be used.

Figure 2 shows an example setup of a server with an integrated BMC which is operating in a separated network. Yet it is still reachable by administrators through a VPN. Other BMCs can be connected to the VPN server by adding a network switch between the BMCs and the VPN server.

8. CONCLUSION

Out-of-band management devices do provide users with a lot of useful tools to manage their network devices especially if these devices reside inside colocation centers. Administrators can use them to install, supervise and recover servers they cannot physically interact with. While the benefits provided by such devices may be quite interesting it is important to consider their security flaws. Users of these devices have to be aware of the risks but it is the manufacturers responsibility to make their devices secure especially at times of high profits gained through industrial espionage.

This article showed some of the many features of IPMI devices together with some possible scenarios of what attackers can do with them. The firmware 1.57.57 of a Dell iDRAC 7 has been analyzed which is the most recent firmware at the time of writing. The results show some security issues encouraging administrators to take immediate actions. Finally some practical advice on how to lower the attack surface of IPMI devices has been given.

Administrators should never ignore their IPMI devices since they often run out of the box without any need to be enabled first, especially if the BMC is connected to the public Internet. This is even more important since at least 46,490 Dell iDRAC devices and potentially even more devices made by other manufacturers are running on public IPs. It seems to be common practice of colocation center operators to connect IPMI devices to the Internet after setting up new servers for customers.

9. REFERENCES

[1] Anthony J. Bonkoski, Russ Bielawski, and J. Alex Halderman: *Illuminating the Security Issues Surrounding Lights-Out Server Management*, In Proceedings of the 7th USENIX Workshop on Offensive Technologies (WOOT '13), August 2013

[2] Andrei Costin, Jonas Zaddach, Aurélien Francillon, and Davide Balzarotti, Eurecom: *A Large-Scale Analysis of the Security of Embedded Firmwares*, In Proceedings of the 23rd USENIX Security Symposium, August 2014

[3] Cisco: *FastHub 300 Series Installation and Configuration Guide*, chapter Out-of-Band Management, `http://www.cisco.com/c/en/us/td/docs/switches/lan/hubs/fhub316c_t/install_config/guide/fh300icg/rptroutb.pdf`

[4] Cisco: *FastHub 300 Series Hubs Network Mgmt Module Instal Note*, `http://www.cisco.com/c/en/us/td/docs/switches/lan/hubs/fhub316c_t/expansion_mods/install/notes/4089_01.html`

[5] Cisco: *Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6*, chapter Configuring Interfaces, `http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/interface_start.html`

[6] Perle: *Console Servers for Out of Band Management of Cisco Routers, Switches and Firewalls*, `http://www.perle.com/supportfiles/cisco_tech_note.shtml`

[7] Daxten: *Peppercon LARA - KVM remote administration*, `http://www.daxten.com/uk/kvm-over-ip.html`

[8] ArchWiki: *Working with the serial console*, October 2014, `https://wiki.archlinux.org/index.php/working_with_the_serial_console`

doi: 10.2313/NET-2015-03-1_10

[9] Intel, Hewlett-Packard, NEC, and Dell: *Intelligent Platform Management Interface Specification Second Generation*, October 2013, http://www.intel.com/content/dam/www/public/us/en/documents/product-briefs/ipmi-second-gen-interface-spec-v2-rev1-1.pdf

[10] Paul Ferrill, ServerWatch: *Server Management Tools: A Closer Look at HP's iLO and Dell's iDRAC*, http://www.serverwatch.com/server-reviews/server-management-tools-comparison-a-closer-look-at-hps-ilo-and-dells-idrac.html

[11] Web Hosting Talk forum post: *SuperMicro IPMI Security*, October 2010, http://www.webhostingtalk.com/showthread.php?t=992082

[12] NIST, National Cyber Awareness System: *Vulnerability Summary for CVE-2013-4786*, October 2013, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-4786

[13] Dell TechCenter: *iDRAC7 now supports Default Password Warning feature*, iDRAC7nowsupportsDefaultPasswordWarningfeature

[14] HD Moore, Metasploit: *A Penetration Tester's Guide to IPMI and BMCs*, https://community.rapid7.com/community/metasploit/blog/2013/07/02/a-penetration-testers-guide-to-ipmi

[15] Zakir Durumeric, Eric Wustrow, and J. Alex Halderman: *ZMap: Fast Internet-Wide Scanning and its Security Applications*, In Proceedings of the 22nd USENIX Security Symposium, August 2013

[16] Zakir Durumeric, James Kasten, Michael Bailey, and J. Alex Halderman: *HTTPS Ecosystem Scans*, https://scans.io/study/umich-https

[17] Dell US: *DELL iDRAC 1.57.57 Driver Details*, http://www.dell.com/support/home/us/en/19/drivers/DriversDetails?productCode=poweredge-r720&driverId=XH6FX

[18] Info-ZIP: *Info-ZIP's UnZip*, http://www.info-zip.org/UnZip.html

[19] Binwalk: *Firmware Analysis Tool*, http://binwalk.org/

[20] Renesas: *Linux & Open Source @ Renesas*, SH7751R Linux BSP, https://oss.renesas.com/modules/download/index.php?cid=52

[21] CERN Computer Security: *Common vulnerabilities guide for C programmers*, https://security.web.cern.ch/security/recommendations/en/codetools/c.shtml

[22] IEEE Standards for Local and metropolitan area networks: *Virtual Bridged Local Area Networks*, IEEE Std 802.1Q™, 2003 Edition

doi: 10.2313/NET-2015-03-1_10