



---

# The SANS Technology Institute

---

## Security Laboratory

### *Security Laboratory: Thought Leaders*

Stephen Northcutt from the security laboratory conducts in depth interviews with the thought leaders in information security. For every novel security product, there is a thought leader, a man or woman of vision that sees the need and guides the creation of the security product. If there is someone missing whose voice you feel should be heard, drop me a note, [stephen@sans.edu](mailto:stephen@sans.edu)

[What is a Security Thought Leader](#) - March 22nd, 2008

[Gene Schultz, CTO of High Tower](#) - April 4th, 2008

[Tomasz Kojm, original author of ClamAV](#) - April 3rd, 2008

**Bill Johnson, CEO TDI** - April 2nd, 2008

[Gene Kim, Tripwire](#) - March 14th, 2008

[Kevin Kenan, Managing Director, K2 Digital Defense](#) - March 14th, 2008

[Leigh Purdie, InterSect Alliance, co-founder of Snare](#) - March 7th, 2008

[Marty Roesch, Sourcefire CEO and Snort creator](#) - February 26th, 2008

[Dr. Anton Chuvakin, Chief Logging Evangelist with LogLogic](#) - January 28th, 2008

[Kishore Kumar, CEO of Pari Networks](#) - January 23rd, 2008

[Ivan Arce, CTO of Core Security Technologies](#) - October 26th, 2007

[Mike Weider, CTO for Watchfire](#) - Updated July 23rd, 2007

[Jeremiah Grossman, Founder and CTO of WhiteHat Security](#) - July 12th, 2007

[Interview with authors of The Art of Software Security Assessment](#) - Updated July 9th, 2007

[Ryan Barnett, Director of Application Security Training at Breach Security, Inc.](#) - June 29th, 2007

[Dinis Cruz, Director of Advanced Technology, Ounce Labs](#) - June 11th, 2007

[Brian Chess, Chief Scientist for Fortify Software](#) - June 9th, 2007

[Caleb Sima, CTO for SPI Dynamics](#) - Updated May 29th, 2007

[An Interview with David Hoelzer, author of DAD, a log aggregator](#) - May 1st, 2007

[An Interview with Ron Gula from Tenable about the role of a vulnerability scanner in protecting sensitive information](#) - March 22nd, 2007

### **Bill Johnson, CEO TDI**

**April 2nd, 2008**

**By Stephen Nortcutt**

***Bill Johnson, CEO TDI, was the first person in the industry, that I am aware of, to sound the clarion call that we might be vulnerable to attacks via the Baseboard Management Controller (BMC). That certainly qualifies him as a security thought leader, and we certainly thank him for his time.***

## **Bill, what is a Baseboard Management Controller, and why should we care?**

Stephen, every device being shipped today has a service processor or baseboard management controller (BMC). Literally everything, including PBXs, Cisco routers, storage controllers, servers, network devices, and intrusion detection devices, has a BMC. When you buy a computer from a vendor like HP, IBM, Sun, Dell or Fujitsu, you expect you are buying one computer CPU. In fact, you are not. You are actually getting two fully functional CPUs. The problem is, you are protecting only one. You are also getting a "hidden" service processor for managing and controlling that computer remotely as well as the traditional main motherboard computer CPU for running your actual computer or device.

**I understand your company's core competence is secure remote access, that you have a lot of console level experience and that it was a discussion with the intelligence community that helped you see this as a significant problem. We fully understand you are limited in what you can share, but anything you can share about the "aha" moment would be great!**

The most interesting "secret" about this topic is how "in-the-open" it was and nobody ever saw it, not even us. We were with some U.S. Government intelligence agencies for whom we do critical cyber protection work. They told us the service processors were completely subject to "brute force attacks." So we went back into the labs and tried it. That was the "aha" moment. It took us literally moments to completely hack these systems.

Stephen, think about it like this: the service processor commands and controls the motherboard, it is CPU and associated memory. If the motherboard CPU is running Windows or Linux, IT departments have spent a lot of money on security solutions to monitor the motherboard operating system for intrusions, file access, logging and privileged functions.

By accessing the service processor, which controls the mother board compute environment, someone can read or set values in real memory, change boot parameters or other operating characteristics without ever having to login to the operating system running on the main CPU. This effectively gives a novice hacker full access to the internals of the running operating system without ever having to log in to the machine. This access at best could be used for a denial of service attack, at worst actually reboot the machine in stand-alone or administrative mode – and take control of the operating system, its files and services running within. Thus, credit card numbers, Social Security records or confidential data can be taken with no record of the intrusion.

## **Gotcha, so what can the service processor do to the host system Bill?**

As briefly stated above, it can control power of the machine, configure device (BIOS) parameters, access the running operating system, crash the running operating system, restart the machine in a single user mode for console access only

where operating systems TRUST the specific control port for privileged functions, reload a new operating system, and load or patch the on-disk structure or operating system.

**OK. So, while I do not believe in security by obscurity by any means, how easy is it to find these processors?**

These service processors now use a routable protocol that runs over TCP/IP. As a result of having a routable protocol, all of these service processors are basically discoverable. By being discoverable it defines the device as its own computer because it has its own operating system, memory, storage and now network. It also means the service processor is a critical part of the IT infrastructure that is NOT being managed, logged or audited, but should be because of its ability to control the whole machine when accessed. Because the purpose of the service processor is to be used as command and control of the motherboard, it can also be used to load and start the operating system. Logically then, the service processor must meet all compliance requirements around being secured, logged and audited.

**Right, and for that matter, if I can find a live IP address, I can assume there is a service processor, right?**

Yes. Service processors are ALWAYS on as long as power is applied to the machine. This is true even if you have instructed the machine to "power down". When this happens, the BMC will power down the rest of the machine – but it will continue to await the command to "power on" either as a remote command or by someone logging onto the BMC and issuing the command. Because it is ALWAYS ON, if you find an IP address and check the same IP address on the BMCs' network port number – it will respond. A good way to "discover" these devices is to download the utilities directly from the DMTF or use HP's free Insight Manager tool, Dell's OpenManage tool, and Sun has a tool Remote System Control for its Sun Fire hardware.

According to Wikipedia, "a baseboard management controller (BMC) is a specialized microcontroller embedded on the motherboard of many computers, especially servers. The BMC is the intelligence in the Intelligent Platform Management Interface (IPMI) architecture. The BMC manages the interface between system management software and platform hardware.

Different types of sensors built into the computer system report to the BMC on parameters such as temperature, cooling fan speeds, power mode, operating system (OS) status, etc. The BMC monitors the sensors and can send alerts to a system administrator via the network if any of the parameters do not stay within preset limits, indicating a potential failure of the system. The administrator can also remotely communicate with the BMC to take some corrective action such as resetting or power cycling the system to get a hung OS running again. These abilities save on the total cost of ownership of a system."<sup>[1]</sup> In many cases, even if the computer or server is powered off, the BMC is still on and active.

### **Bill, is this a standard, who is in charge of this?**

BMC specifications are developed by the Distributed Management Task Force, identified as [www.dmtf.org](http://www.dmtf.org). The DMTF has about 3,500 active participants, representing 39 countries and nearly 200 organizations from our industry, everyone from hardware to services, to storage, to routers and network devices. The DMTF was formed, as a consortium, made up of all of the industry players, to build and develop a better, ubiquitous method of managing the total datacenter. The entire industry is behind the service processor---it is not going away.

### **So, if I am buying a lot of equipment from a major vendor like HP or Dell, how do I know what I am getting in terms of service coprocessors, how are they managed at the enterprise level?**

Each vendor has their own brand name and implementation; in the case of Dell, the BMC Management Utility is a collection of software applications that enable remote management and configuration of systems equipped with a BMC. The system is orchestrated by their IPMI Shell, a scriptable console application program for the control and management of remote systems using the IPMI 1.5 protocol. The IPMI Shell supports both serial access and LAN access to the BMC. It allows administration of one or more managed systems from a command line shell, rather than a graphical user interface (GUI). Use the IPMI Shell to perform the following tasks:

- System power management
- System identification
- Access to the event log
- System identifier control
- This operates over a network using Serial-Over-LAN Proxy (SOL Proxy)[2]

### **So, SOL is the protocol that works over TCP to connect to the BMC, are there other alternatives to connect to these processors?**

Yes, SSH, TELNET, and WEB browser all work equally well. When the vendor tools just mentioned are used, they provide the automatic discovery of the BMCs as well as give the Windows end user an easy-to-use graphical solution for these interfaces.

### **Bill, what is the danger? Clearly they can shut down the machine, but are there security implications I should be aware of?**

With the BMC you can issue commands to examine and deposit values into the main motherboard's memory subsystem. As a result, an attacker could potentially

change someone's privilege level, or cause applications such as security event monitor or logging solutions to actually crash, or do something even worse. Where this gets really scary is the possibility of attacking a server running multiple virtual machines; if you could get access to the hypervisor via the BMC, you could then control the virtual machines. Remember that the BMC **\*is\*** the command and control for the **\*whole\*** machine. From it, I can restart the operating system without having to login in a single user mode and then access the disk and applications as well as patch the operating system to allow access to files or applications it otherwise would not have when it comes back up in production mode. This can all be accomplished without the visibility of traditional security solutions ever knowing what's happening.

### **Can you expand of the virtual machine part of this? What are the particular implications of virtualization?**

Virtualization is essentially an instantiation of the physical environment. Virtual machines actually have a console interface – it is generally provided as an SSH or TELNET session to the Hypervisor and then a specific PORT number for the specific virtual machine console. Generally these virtual consoles are NOT connected, but instead are available for connection – leaving them vulnerable. Traditional logging systems do not run on the hypervisor. So, who or what is watching the connections to and from the hypervisor and then to the guest machines?

As such, if the BMC is compromised it can be used to access the hypervisor, compromise it, and then the hypervisor can be used to compromise the guest VM. This is not complicated: it's the same reason we keep people out of the computer room – physical access says that you own the machine. And, this is because the physical access would allow you to plug in a PC to the BMC and do what ever you want to the machine.

The BMC provides a virtual computer room tour – without all the logging and auditing we expect.

We have been advised by several of the major hardware manufacturers that virtualization will be a BIOS level function in 18 months or less. Then virtualized environments will be doubly threatened.

**Bill, one of the things I always try to do is focus on the management application of information, if I am a manager what can I do with this information?**

There are two fundamental things we have to do to achieve information assurance: configure the system correctly and detect attacks. The primary defense for the BMC in most implementations is a password. As a manager you want to make sure this is a strong password and investigate higher security options with your vendors. Also, you want to validate that your log analysis system collects event logs from the BMC subsystems. Remember that our regulatory compliance requirements state that we must also log and audit all configuration and change control in the IT infrastructure. Controlling the BMC access so that it is logged, keystroke for keystroke, ensures that ALL access, change control and even single user mode access is appropriately logged and auditable.

**If you had one message for all our readers, what is the most important thing you would like to share?**

The Baseboard Management Controller is here to stay. We should not fear it as it has many valuable capabilities. Instead we need to understand it, manage it and control it, at least as much as we do the traditional operating system, if not more. It **\*is the most powerful\*** and **\*vulnerable access point\*** in the whole machine and most, if not all, machines have one, so there are many of them. Be knowledgeable, informed and make sure the BMC is a serious and major part of any security policy or strategy.

**And can you tell us something about yourself? What do you do when you are not in front of a computer?**

Sure, I have been married for 13 years, have a 6 year old son and we all love the outdoors. I like water skiing, snow skiing, horses, 4 wheeling, riding my Harley, hunting, fishing and flying when I have time. As a family, we spend time camping and with friends generally outside grilling or traveling. And yes, on occasions, I take the quiet dinner and movie with my wife while our son is home with the sitter.

All links were active March 27, 2008

1. [http://en.wikipedia.org/wiki/Baseboard\\_management\\_controller](http://en.wikipedia.org/wiki/Baseboard_management_controller)
2. <http://support2.jp.dell.com/docs/software/smbmcmu/12OM451/en/ug/bmcugc0d.htm>
3. The observation the BMC can be discovered and attacked via a network and must be logged is credit Bill Johnson, webcast March 26, 2008 (SANS Portal Account Required): <https://www.sans.org/webcasts/show.php?webcastid=91798>

**Bill Johnson is CEO TDI, <http://www.tditx.com/>**