IPMI: Express Train to Hell

dan farmer/zen@trouble.org/1-28-2013

Imagine trying to secure a computer with a small but powerful parasitic server on its motherboard; a bloodsucker that can't be turned off and has no documentation; you can't login, patch, or fix problems on it; server-based defensive, audit, or anti-malware software can't be used. Its design is secret and implementation old. It's also the perfect spy platform: nearly invisible to its host, it can fully control the computer's hardware and software, and it was designed for remote control and monitoring.

And that's the good news.

The BMC is an embedded computer found on most server motherboards made in the last 10 or 15 years. Often running Linux, the BMC's CPU, memory, storage, and network run independently. It runs Intel's IPMI out-of-band systems management protocol alongside network services (web, telnet, VNC, SMTP, etc.) to help manage, debug, monitor, reboot, and roll out servers, virtual systems, and supercomputers. Vendors frequently add features and rebrand OEM'd BMCs: Dell has iDRAC, Hewlett Packard iLO, IBM calls theirs IMM2, etc. It is popular because it helps raise efficiency and lower costs associated with availability, personnel, scaling, power, cooling, and more.

To do its magic, the BMC has near complete control over the server's hardware: the IPMI specification says that it can have "full access to system memory and I/O space." Designed to operate when the bits hit the fan, it continues to run even if the server is powered down. Activity on the BMC is essentially invisible unless you have a good hardware hacker on your side or have cracked root on the embedded operating system.

Servers are usually managed in large groups, which may have thousands or even hundreds of thousands of computers. Each group typically has one or two reusable and closely guarded passwords; if you know the password, you control all the servers in the group. Passwords can remain unchanged for a long time – often years –not only because it is very difficult to manage or modify, but also due to the near impossibility of auditing or verifying change. And due to the spec, the password is stored in clear text on the BMC.

IPMI network traffic is usually restricted to a VLAN or management network, but if an attacker has management access to a server she'll be able to communicate to its BMC and possibly unprotected private networks. If the BMC itself is compromised, it is possible to recover the IPMI password as well. In that bleak event all bets and gloves are off.

BMC vulnerabilities are difficult to manage since they are so low level and vendor pervasive. At times, problems originate in the OEM firmware, not the server vendor, adding uncertainty as to what is actually at risk. You can't apply fixes yourself since BMCs will only run signed and proprietary flash images. I found an undocumented way of gaining root shell access on a major vendor's BMC and another giving out-of-the box root shell via SSH. Who knows what's on other BMCs, and who is putting what where? I'll note that most BMCs are designed or manufactured in China.

In sum: you may not know it, but your goose may already be cooked and you're simply asking for the orange sauce. There is no easy fix, but a dialogue between customers, vendors, and the security community might be a starting point. Vendors must open up these black boxes for change and review and allow customers and third parties to examine and protect their servers. IPMI awareness, security best practices, FAQs, and tools are needed. The de-provisioning of old servers must be handled even more carefully, since no one knows how or where the IPMI passwords are stored, so eBay attacks are a real threat. Processes and risk management might well need to be changed. And perhaps the IPMI standard itself should be revised. In any case, good luck. We all might need it.