White Paper

Security Through the IT Supplier Life Cycle

Sponsored by: Lenovo

Robert Ayoub Christian A. Christiansen

July 2016

IDC OPINION

As more server components are manufactured overseas, customers increasingly wonder about possible threats embedded into the hardware and software during the manufacturing process. As a result, there is a quiet debate around this possible scenario and the threat it poses. IDC thinks that vulnerabilities and malware could be introduced into the components of a system during the manufacturing process. These system vulnerabilities — whether intentionally planted or the result of errors in development — can undermine an organization's entire security infrastructure. In addition, these vulnerabilities are very difficult to detect since they may originate in a component within a trusted vendor's device and below the operating system.

IDC believes that it is time for customers to consider as part of their buying criteria the implementation of IT vendors' security processes across their entire development processes and supply chain. The vendors that satisfy this criteria will not only ship more secure products but lower the number of vulnerabilities across their entire ecosystem, ultimately protecting their customers against attack. These vendors should be able to provide customers additional, validated evidence that the entire product life cycle including the supply chain and design process is held to a high standard of security. As a result, customers can achieve a level of assurance when it comes to system component security.

IN THIS WHITE PAPER

This IDC white paper explores the potential threats faced by IT departments as they evaluate products entering the enterprise. It also illustrates the need for security throughout the entire supply chain and describes steps vendors should take to secure the supply chain. In particular, this white paper examines how managing external development and supplier security can enhance the overall security of all devices, passing that security onto the IT buyer. Finally, this white paper discusses how Lenovo manages its own product development and supply chain and maintains security standards that allow the company to meet even the stringent requirements of the U.S. federal government (a key Lenovo customer).

SITUATION OVERVIEW

In July 2015, a very disturbing article and video illustrated the failure of security through the supplier life cycle. Reported in *Wired* magazine[1], the article described in great detail the ability of a potential attacker to control and ultimately paralyze an operating vehicle on the freeway. The two security

[1] **www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/**

researchers who conducted the hacking exercise found vulnerabilities in several vehicle components, including the entertainment system and cellular data connection.

This attack illustrated the damage that can occur via weaknesses in OEM components. Even though Fiat Chrysler (the vehicle manufacturer) was not the builder of the vulnerable components, ultimately the responsibility (and expense) for recalling and patching the 140 million vehicles, along with the negative public perception, fell on its shoulders. Customers — who felt the brunt of the impact — are concerned about the security of the products they buy, and manufacturers must scrutinize their suppliers.

A parallel to IT departments might be the following: A supplier loses control of the supply chain, and BIOS-level malware is shipped as part of an order of servers. A large customer, say a retailer, places these devices in its datacenter. While the retailer may have appropriate controls in place, these new infected machines automatically bypass all security controls, and the rootkit is extremely difficult to detect. Ultimately, the rootkit causes significant losses for the organization that will then pursue its vendor for losses.

Scrutinizing the suppliers is not trivial and requires a dedicated and organized effort on the part of the vendor. Suppliers may feel that the extra scrutiny is unwarranted, shows a lack of trust, or is an infringement on the trade secrets of the suppliers. Vendors must find ways to perform audits and set standards that validate the security of the system while protecting the intellectual property of the suppliers. At the end of the day, the security of the customer (the IT buyer) is paramount and is beneficial to all parties.

Programs that vendors should establish with their suppliers include, but are not limited to:

- Conducting unannounced audits of facilities
- Putting controls in place that protect supplier components from overwriting other system components
- Developing threat research capabilities to detect and alert on potential attacks against products

IDC recognizes that every supplier relationship is unique and some suppliers may warrant more or less scrutiny than others. Vendors need to understand the level of risk they are comfortable accepting with every supplier and determine how they can minimize the risk of security to the customer throughout the entire product.

To ensure a secure supply chain, some server vendors audit and validate that their suppliers adhere to a baseline of requirements. By auditing and validating their suppliers' security, a server vendor can both improve the security of its products and deliver a level of comfort to partners, affiliates, and customers, ensuring that they are not blindly accepting third-party components. Ultimately, this leads to the following benefits for the IT buyer:

- Improves the overall code base, ensures continuous validation, and confirms updates — all of which establish and maintain a chain of trust for upper-layer software and applications
- Prevents unauthorized changes that interrupt operations by signing code, controlling administrative changes, and verifying all changes and updates
- Reduces audit and compliance problems with trusted administrative privileges, full-disk encryption, key management, secure firmware, and rigorous security testing

- Enables security by default, which provides additional protection, closes "vulnerability windows" opened by manual security processes, and improves datacenter reliability

State of the Industry Today

Generally speaking, most IT buyers have little insight into the development of the products they use. They have to assume that the device manufacturer is taking the appropriate steps to ensure the security of the final products. Unlike the automotive industry, some server vendors have addressed security in a coordinated way and continue to do so. The best vendors care very deeply about securing their supply chains, the interoperability of server components and, most importantly, the security of IT buyers.

The more transparent and thorough a vendor can be about its methods of securing its systems, the more trust that vendor can build with customers. There was a time when even the description of security controls was considered a secret – the thought being that if attackers knew the controls, they could get around them. However, in today's security conscious landscape, helping customers understand the steps that their vendors are taking to ensure the security of the products they use can be a competitive advantage.

Why Customers Should Consider Lenovo

Lenovo is a multibillion-dollar global manufacturer of enterprise servers. The company's Data Center Group (DCG) systems division is mostly composed of the former IBM System x and networking offerings and Lenovo ThinkServer groups including storage. According to Lenovo, its multifaceted approach to server security differentiates the company from other companies in the x86 market.

As a result of the company's acquisition of IBM's System x group, Lenovo underwent a review by the Committee on Foreign Investment in the United States (CFIUS). As a part of that process, Lenovo agreed to maintain and enhance the rigorous development, supply chain processes, and controls used by IBM. Security is assured through transparency – Lenovo has agreed to allow the U.S. government and independent auditors to audit these processes at any time, creating what Lenovo believes to be the most transparent, auditable, and secure supply chain in the server industry.

In addition, Lenovo maintains business processes and policies (discussed in the sections that follow) designed to enhance security and mitigate risks.

U.S. Federal Government CFIUS Agreements

The IBM System x acquisition was Lenovo's fifth CFIUS approval. Other acquisitions that required CFIUS approval included IBM's PC Division, Stoneware Inc., EMC's Iomega subsidiary, and Motorola Mobility. In each case, the acquisition was approved by the U.S. government, and Lenovo continued to deliver products that maintain the same level of rigor as before the acquisition. In addition, the U.S. government maintains the right to audit certain business processes at any time.

Trusted Supplier Lists

Lenovo requires suppliers to complete an extensive questionnaire to validate security in manufacturing and products. Questions are related to hardware, software, and facilities security. After review of the questionnaire, Lenovo ensures that its own security and supply chain experts audit and keep its suppliers in check. Several suppliers have been removed as a result of this process.

Incident Response Team

Lenovo maintains a high-level team that responds to vulnerabilities reported or discovered in products. This team is charged with issue resolution; information regarding vulnerabilities and resolution is posted and available to the public.

Secure Software Development Life Cycle

Lenovo developed a secure life-cycle development process validating that software has no known backdoors, malware, or other vulnerabilities. In addition, Lenovo conducts rigorous testing of third-party software that is installed on products.

Building in Security from Design to Manufacturing to Deployment

The Lenovo DCG employs rigorous business processes, product design, and supply chain controls to ensure products meet stringent requirements. In fact, Lenovo believes the company goes above and beyond what other vendors do concerning system security features and quality procedures. As befits perhaps the most scrutinized server vendor, Lenovo's DCG takes extraordinary steps to ensure products are built with components from known, reliable suppliers.

From the initial design stage, Lenovo servers have security built in on multiple levels. At the hardware and processor level, all the latest x86 industry security standards have been incorporated, including Intel security processor features for protection against malware and faster encryption. At this level, System x also incorporates the latest technology from the Trusted Computing Group. On top of these industry standards exists a set of System x platform-specific innovations, together called System x Trusted Platform Assurance. These are features and practices that include development, build, test, and field deployment processes.

Lenovo performs detailed BIOS and firmware design and code reviews to ensure code security, and the company only uses select supplier-certified hardware. Components including Intel controllers, all firmware, BIOS, BMCs, and even USB ports are validated according to the FIPS 140-2 standard. In addition, Lenovo performs ongoing threat assessments including threat modeling and ethical hacking of firmware to continually assess security protection. To further ensure that firmware is not compromised, all firmware requirements, architecture, and design are performed by United States–based teams, thereby maintaining compliance with Lenovo product requirements, design practices, and industry standards. The company has safeguards in place to ensure that products cannot be hijacked and that compromised firmware cannot find its way into servers once deployed.

Whenever code is developed by third parties, U.S. teams perform inspections for quality control. All source code is maintained on United States–based code retention servers, and all code changes are tracked and audited. Build servers, also based in the United States, are where source code is compiled and converted into executable code. Before the code is released, it is digitally signed on secure signing servers. The signing servers are highly controlled and are based in a secure U.S. datacenter with limited and auditable access.

Lenovo also manufactures servers in the United States and offers products built completely within a secure end-to-end process located entirely in the United States by verified U.S. persons for those customers that require this level of assurance. Lenovo owns more than 50% of its manufacturing facilities, which enable an end-to-end business model for vertical integration. By leveraging its own manufacturing capabilities, Lenovo can maintain greater control over both product development and

supply chain operations. As a result, Lenovo manufacturing processes maintain and strengthen the rigorous development and supply chain controls used by IBM.

Finally, a security office works closely with DCG leadership to continuously monitor and report on compliance. This office is led by a security director who is backed by a team of security experts. The team is responsible for resolving all validated incidents and also notifies customers and communicates risk and remediation plans.

FUTURE OUTLOOK

IDC believes that the focus on components by attackers will only continue. While the headlines today are around cars and other physical devices, IT departments must define the criteria they will use to evaluate their vendors before malware enters the datacenter through a supposedly trusted device. Customers who will ultimately be most impacted by security vulnerabilities must ensure that the IT hardware they buy is built to the highest standards. For their part, vendors must perform many of the functions described previously to maintain the trust of their existing customers, win new customers, and avoid the costs associated with a high-profile attack or breach. As the Fiat Chrysler attack illustrated, even the most unlikely component can become the entry point for an attack.

CHALLENGES/OPPORTUNITIES

Customers face challenges when trying to judge the security of a vendor's IT life cycle. Not all server vendors place equal emphasis on security during the design, assembly, testing, and updating of their products' security.

Vendors face several challenges associated with building a secure supply chain and delivering a product that is secure from inception to deployment. For IT buyers, a discussion around the following vendor challenges can form the basis for evaluating server security:

- In light of the constant appearance of new vulnerabilities, how does the vendor help IT buyers' non-security specialists to keep up?
- Manufacturers are often located in countries that are foreign to the vendor itself, so how does the vendor ensure that supply chain partners at the local level maintain the necessary security standards?
- Supply chain partners are often located outside the United States, so how does the vendor ensure that local regulations don't impinge upon the security of the finished products?

IDC believes that Lenovo addresses these challenges that are pervasive throughout the industry. IDC also believes IT buyers can use Lenovo's best practices as criteria for ensuring that server security is consistent and auditable across its supply chain.

CONCLUSION

As the Fiat Chrysler hacking incident demonstrated, a more interconnected world allows for an even greater possibility of attack to the systems we trust most. Weaknesses in any subsystem and within any supplier can be exploited to cause significant damage. Customers whose systems are targeted by attackers must look for suppliers that demonstrate the best security practices throughout the supply chain – from design to manufacturing to deployment. By implementing a repeatable, auditable, security process across the entire supply chain, customers can be reassured that manufacturers are doing their best to ensure the security of the entire system, regardless of where components are developed.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com