WHITE PAPER

Computing System Manufacturing
Supply Chain Security

intel | Goldman Sachs

The Next Security Frontier: Taking the Mystery Out of the Supply Chain

Understanding the Strategic Importance of Transparency in the Computing Ecosystem

Authors

Michael Mattioli
Goldman Sachs & Co., Principal Engineer, Hardware Engineering

Tom Garrison
Intel Corporation, Vice President & General Manager, Security Strategy and Initiatives, Client Computing Group

Baiju Patel, PhD
Intel Corporation, Intel Fellow – Security, Client Computing Group

Table of Contents

Summary

By the time a Personal Computer (PC) or a server (referred to as computing system in this document) is delivered to its intended customer, the sum of its parts has traveled through a highly complex supply chain. This supply chain includes diverse component suppliers, subsystem manufacturers, integrators, and original equipment manufacturers (referred to as suppliers in this document). The final product may go through several warehouses and may be transported via several shipping companies before it makes it to IT/ end customer.

Considering ever-increasing threats to supply chain, customers have a growing need to know that the final product they received is indeed the product they ordered. Unintentional mistakes/errors, poor handling, or intentional fraud are key risks to the customer not receiving the system they ordered. Additional risks may come from malicious actors, including nation states and well-funded criminal organizations, who are motivated to tamper with systems in the supply chain. The consequences of these risks could include financial or reputational loss to the customer.

While many customers today treat a PC or Computing System as a "Black Box" and trust the supplier and transport, a growing portion of customers – such as Financial or Government Institutions – have additional procurement requirements. They are actively taking steps to ensure that the computing system, as delivered, meets their risk profile and can fulfill their compliance, security, and performance requirements.

Typically, these customers specify their requirements as part of their Request for Quotation (RFQ) process. The systems delivered to them are often evaluated by an in-house team or an external partner to ensure that the systems meet the requirements specified in the RFQ. However, it is only practical to evaluate a small subset of systems and results may not be available right away. This can either delay the deployment of systems or increase the risk by deploying a large number of systems before receiving all the results.

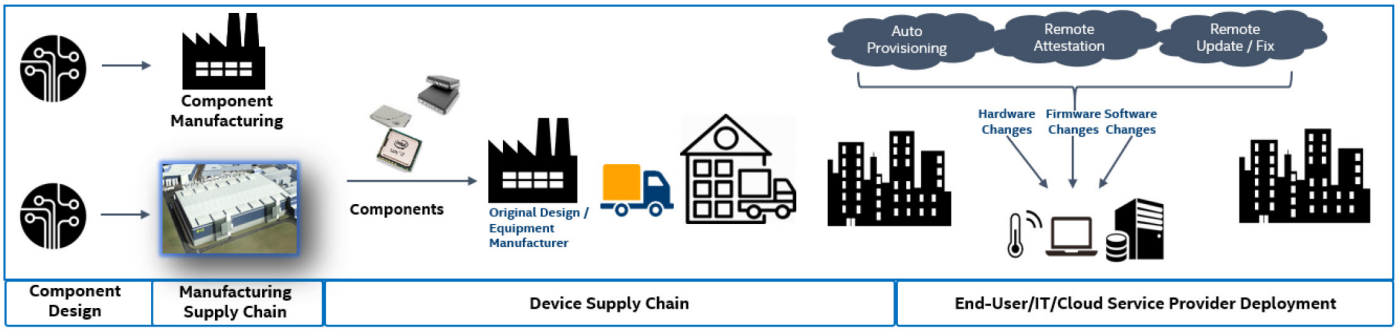

Figure 1. Simplified Supply Chain Process

It is important for the PC supply chain ecosystem to take measures to ensure a growing list of customers can trust the supply chain with increased accuracy and decreased cost. Improving transparency in the supply chain will help meet the need for security and quality assurance among broader customer segments as both awareness and risks continue to grow.

Key Supply Chain Risks to Security

Any typical component or system changes hands dozens of times from inception to deployment and ultimately retirement. Supply chain is a continuous process, ever an evolving one, and may not end even when it leaves the customer's hands (e.g. recycle or donate). Participants in the supply chain also treat their role as Intellectual Property (IP) or business secret, making it even more challenging for a customer to evaluate and manage risk.

Risks at the initial stages of the Build phase: The first window of opportunity to insert risk into computing systems is by attacking the design and manufacture of the individual components that will eventually comprise the system. Schematics can be altered, design tools can be compromised, and collaboration solutions can be manipulated to alter a component from its intended composition.

Subsequent risks are introduced when customers work with the supplier (e.g. original equipment manufacturer) to design and configure a platform. During such engagements, there is room for unintentional human error, such as misinterpretation of calls and emails. Risks might also include intentional malicious action that can cause harm in the process.

Behind the scenes, the customer's vendor also works with their respective suppliers (e.g. original design manufacturer) to do similar functions – source sub-components, assemble components, etc. – which further exacerbates the potential for human error.

Risks during assembly and manufacturing: Further down the line, during assembly and manufacturing, there are more opportunities for malicious actions such as circuit design modification (hardware trojans, scan attacks, etc.) and firmware modifications. A disruption to the supply chain, such as a factory fire or a large-scale disruption like COVID-19, may also force original equipment manufacturers to substitute parts to ensure timely delivery of computing systems to customers. The many levels and layers of the supply chain make it near impossible to keep a watchful eye on every single party involved and ensure that no intentional or unintentional harm was done.

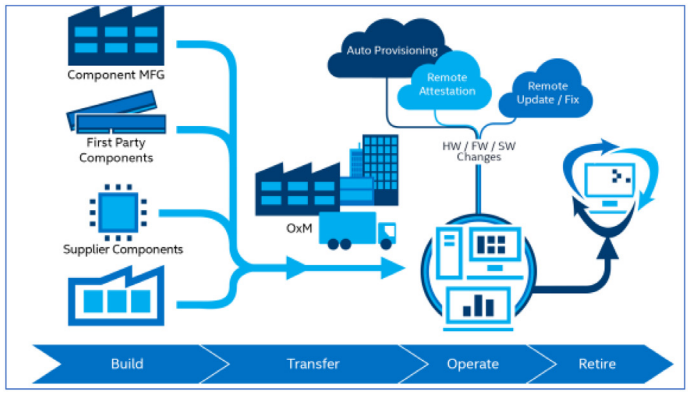

Figure 2. Supply Chain Lifecycle

intel | Goldman Sachs

Risks after the product has been shipped:
After a system has left the factory, there are many opportunities for tampering, modifications, or changes within the hardware, firmware, and software. Once a device is received and deployed, it may be serviced (e.g. components replaced) in different locations or by different parties throughout its lifecycle. It is practically impossible to have complete confidence that a system has not been tampered with in some manner. The potential for tampering applies to each of the functional components of a computing system. For example, a solid-state drive shipped to an original design manufacturer for integration into a computing system could be tempered by having the firmware within the drive replaced with a malicious version.

Risks while in use:
Transparency in supply chain helps the customer ensure that they received exactly what was ordered. This is a significant step in maintaining continuous trust in the PC ecosystem. Since most computing systems are frequently upgraded with the latest functional and security updates, it is extremely important to maintain the current state of the PC through its entire lifecycle.

Ideally, the IT department should have the complete and latest information (e.g. firmware version updates) about each critical component of the computing system and should be able to validate the version updates and configurations against the expected state in real time with reasonable assurance that nothing malicious has modified the system to an unacceptable configuration/state.

Impact

Just as causes of unintended changes to the platform vary, the impact to the customer can vary from benign to more serious consequences rooted in malicious intent, such as:

- **Financial** – Stealing sensitive information can lead to financial gain through access to non-public information.
- **Reputational** – Exposing and fabricating information, or interrupting operations, can cause severe reputational damage to a person/company.
- **Revenge** – Personal attacks against a company or organization by a disgruntled employee or customer can cause a range of potential damages, from physical alterations, compromise of intellectual property, to destruction of reputation.
- **Chaotic** – Some individuals and criminal organizations simply want to "watch the world burn".

Different entities, private and commercial, are exposed to these and other threats at varying levels. While initial focus might be large commercial customers because they have the means to start effectively using supply chain transparency, it is imperative that supply chain transparency is designed to scale to not just different size businesses but to consumers as well over time.

Impact of Transparency

As might be expected, transparency has a cost. Beyond the obvious, managing the supply chain means keeping track of each component through manufacturing, warehousing, and delivery. This in turn limits the flexibility of the manufacturer.

For example, a manufacturer may wish to have multiple sources for a keyboard and wants to be flexible in selecting the keyboard to be integrated into the laptop based on the availability of parts and the cost. However, a customer may require the keyboard from a specific supplier, which may impact a timely delivery and also introduce challenges and additional cost due to inventory management.

Inventory may also be impacted due to unexpected natural calamities or pandemics, such as COVID -19. In order to deal with such disruptions, as well as those caused by smaller unforeseen events, a typical supply chain is designed to include multiple sources for every significant component to support business continuity.

At the same time, suppliers also need to protect their confidential business information, including complex business relationships, procurement processes, and inventory management. This

type of information in the wrong hands can have significant impact to the business and can lead to compliance issues. Therefore, the ecosystem needs to align on the right technology as well as processes to minimize misuse of transparency while meeting customer requirements. Additionally, transparency needs to maintain a balance between the needs of supply chain and the needs of the customer and consider a baseline that may be available to everyone, with additional levels of detail requiring different agreements.

Trust Requires Industry-Wide Participation

A computing system is composed of various components, as shown in Figure 3. The Central Processing Unit (CPU) is the "brain of a computing system". Operating systems and applications run on the CPU. However, a modern computing system also has many other **smart** (also referred to as **intelligent**, or **active**) components that have their own CPU or controller, such as solid-state drive (SSD), Wi-Fi network interface card, and keyboard. These components run their own **firmware**, which is a form of software. The firmware has significant functional capabilities including the ability to not only access, but manipulate, critical or sensitive (personal) data.

The smart components typically are manufactured by different suppliers and in-turn are composed of both active and passive sub-components. It is important that customers have full transparency of active components due to their significant capabilities to access and modify data. Passive components, such as resistors, capacitors, physical packaging, printed circuit board (PCB) or screen, can also pose a risk to customer data if not implemented correctly. For example, if PCB routing had certain wires close to the surface or implemented sockets for expansion or options, an adversary might be able to easily substitute or even add a component without the knowledge of the customer.

While it may not be practical to have full transparency at each passive component level, it is important to have transparency at active component level and to establish trust in the entire supply chain, which requires industry-wide initiative and agreement on key technical underpinnings in order for the initiative to be successful. With the ultimate goal of achieving full transparency, we recommend getting started with small, yet critical, components of the computing system first and then develop technology and processes to progress ahead.

Figure 3. Simplified Components of a Computer

While this document does not attempt to specify the list of smart components for initial implementation of transparent supply chain, some examples that the industry needs to consider as starting points are the **CPU**, **SSD**, **Wi-Fi**, **motherboard**, and **embedded controllers (EC)**. It is not enough to know the manufacturer of these components or subsystems, but to know details such as firmware running on these components, date and location of manufacture, and design revision.

Technology Choices

Technology choices we make to establish transparency will have long term impact on the industry, both from longevity and cost point of view. Two models to consider are: 1) Ledger or Database and 2) Self-reporting. Each of these are described below:

Ledger or Database

As a computing system goes through assembly and delivery in the Supply Chain, each entity makes an entry in a ledger, thus creating a record that can be retrieved later by the customer to meet their need for transparency. Once a computing system is delivered to the customer, the same process can be used to record changes, including

changes of ownership, to maintain a continuous record for the entire lifespan of the computing system. Two fundamental approaches exist here:

- **Centralized approach** – this is when a trusted third party maintains the ledger or database of all the transactions and manages updates to and retrieval of information per agreement between trusted third-party and members of the supply chain. The fundamental trust model is based on the idea that without collaboration between multiple member companies in the Supply Chain, any inconsistency (intentional or otherwise) might not be detected. For example, if a system manufacturer entry shows they shipped 1M computing systems with specific SSD from a specific supplier, a corresponding entry by the supplier in their database is necessary to corroborate.
- **Block Chain Approach** – Application of block chain technology to ingredient Supply Chains has been widely discussed. A 2019 Fortune article[1] outlined Bumble Bee Tuna's use of block chain to create an electronic and distributed ledger chronicling a fish's capture, processing, and travel history to ensure freshness and product quality. Beyond this ability to track ingredients, the distributed ledger can be expanded to keep a running and growing record over the operational lifecycle for each system. Tightly controlled and permissioned ledger entries can continue for updates, changes, and ownership transitions that occur as the system travels through distribution and integration, then ultimately provisioning, operation, and modification by the end-user or owner. The private and public cryptographic controls inherent in existing blockchain infrastructures can be applied to balance the simultaneous needs of all ecosystem participants. Component suppliers can contribute product information into the blockchain without worry of sharing sensitive product details to competitors. Similarly, system manufacturers can create system-level ledgers from component and sub-system vendors in private transactions shared only with those whose access permissions have been cryptographically proven. Ownership can be transferred to operators who can manage ledger updates to track key information regarding location, application, upgrades, updates, and usage statistics. The usefulness of this ledger can extend from the resale of the device into the secondary market, with the ledger providing sellers with better insights into possible IP loss based on usage and application, and buyers a better understanding of the provenance of the device.

Self-reporting

Tracking the components in the supply chain while the device is manufactured and readied to be delivered to the end customer helps ensure that intended components are used in the device. Once the device is in the hands of the end customer, the device can provide a cryptographic report (often referred to as Attestation) of the current configuration of all the smart components in the device. The configuration can include current firmware version, security version, hardware ID, etc. Each report may further include information about non-active or passive components that are part of the smart component or even include a report-out of smart sub-components as well as revision or change log for additional transparency.

In order to establish customer trust into the report, the smart component needs to include a cryptographic key and associated certificate (similar to how web sites use certificates for HTTPS or TLS servers), and when queried, produces signed report along with certificate so that customer can validate authenticity and trust in certificate and subsequently trust the report.

Finally, the entire computing system can either collect report-out from each of the smart components and may produce a comprehensive report for the entire system or may leave it up to the customer to query each smart component of interest. The benefit of a system-level report-out is that the customer gets the full picture without necessarily having to understand how to query each of the components (as the manufacturer of the system has the best understanding), and would require the system to also have a trusted smart component that can not only collect

all the information but is able to produce a cryptographically signed comprehensive report.

The shortcoming of this type of approach is that each component has additional cost of obtaining certificate and complexity of providing a report-out, and such approach provides information only about components that include report-out capability. However, the customer does not have the benefit of transparency from any component that does not implement this capability.

Figure 4. Simplified Components of a Computer, with a Certificate of Authenticity

Governance

Self-regulated or market driven: Each participant in Supply Chain may choose their own degree of participation in transparency. And customers, based on their purchasing preference, will drive Supply Chain to adopt the "right" level of transparency to meet market needs.

Industry group or consortium: Computing system Supply Chain participants form a consortium to establish technical direction and a governance model to provide consistent and sufficient transparency to meet broad industry needs.

Recommendation

With increasing reliance on information technology for business-critical and personal data, having transparency of Supply Chain, as well as information on the current state of the computing systems, is vital to the economic health of the information technology ecosystem. Transparency by itself is of limited value without the information needed to assess risk or compliance. Beyond the ability to verify that what the customer received is indeed what they ordered, there is additional value of transparency post deployment as well. For example, if a security risk is identified (e.g., a publication in the Common Vulnerabilities and Exposures system), the customer can use transparency to precisely pinpoint impacted systems and take appropriate remediation steps.

It is proposed that due to the diverse and complex nature of the ecosystem, no one company can single handedly solve this problem. The choice of technologies and collaboration will have long term implication on evolution of capabilities to meet current and future needs, as well as the ability to scale and manage costs. It is therefore strongly recommended that industry leaders come together and take a comprehensive long-term approach to address this important problem.

intel | Goldman Sachs

[1]https://fortune.com/2019/03/08/tuna-blockchain-bumble-bee-sap/

Printed in USA 0820/TG/EGP/PDF ♻ Please Recycle 344165-001EN

ENDORSEMENTS

intel | Goldman Sachs

ZOTAC

"A distinguished innovator of custom computing solutions for over 23 years, ZOTAC continues to successfully fulfill the unique requirements of customers through its diverse R&D capabilities. We welcome this initiative and embrace transparency into our manufacturing and supply processes."

– Gary Lau
President, ZOTAC USA

Lenovo

"Lenovo recognizes the importance of trust and security for our customers. In our complex and ever-changing PC landscape, our priority is ensuring our customers have confidence in our products and solutions. Rigorous, trackable, and auditable security standards are built into every step of our secure and transparent supply chain. Bringing component-level traceability and software verification to platforms and systems increases confidence and reduces the risk of counterfeit electronic parts while also facilitating procurement standards. This is the right direction for the industry."

– Jerry Paradise
Vice President, Global Commercial Portfolio & Product Management, Lenovo Inc.

Jabra GN

"A secure and seamless supply chain is essential to maintaining trust and product quality, and transparency is at the core of this. As supply chain ecosystems become increasingly complex, it is imperative for companies across the industry to address manufacturing challenges and create a more streamlined path forward, which ultimately benefits all industries."

– Stefan Bergfors
Vice President, Global Operations, Jabra Inc.

C.H. ROBINSON

"C.H. Robinson, a leader in Transportation and Supply Chain Technology and Services, endorses heightened attention to security and visibility for the emerging threat on PC manufacturing Supply Chain. As attacks on technology increase in sophistication, bad actors are maturing and shifting their tactics to less hardened and upstream targets. While progress has been made to secure software, network and identity layers of the technology stack, hardware is coming in to focus as a new attack vector and must be addressed by the leaders in the industry to preserve the integrity of the entire supply chain."

– Mike Hon
Director IT, C.H. Robinson

LG

"By LG Electronics' full dedication to supply chain transparency and customer satisfaction, we commit to taking support of PC ecosystem transparency initiatives and setting up an industry standard of supply chain security."

– Bong-Soak Kim
Senior Director, LG Electronics Inc.

secunet

"secunet, a leading IT security vendor in Germany and Europe for high security encryption and biometric solutions, servicing government, defense, health care and critical infrastructure customers, believes that trustworthiness is paramount for our customers, and transparency is key for trustworthiness. With every building block of our solutions we strive to achieve transparency, and very much value such initiatives to build in more transparency, and therefore security, in this innovative ecosystem of suppliers. We support this and believe our customers will appreciate this!"

– Kai Martius
Chief Technology Officer, secunet

AMD

"AMD has established extensive controls to help ensure our products are securely built, tested, tracked, stored and transported from manufacture to authorized distribution. We look forward to contributing to industry-wide initiatives focused on promoting secure supply chain best practices and developing new technologies and standards to address emerging risks."

– Keivan Keshvari
Senior Vice President of Global Operations, AMD

NYU Center for Cybersecurity

logitech

VERTO WAVE
YOUR IT TRANSFORMATION PARTNER

GLOBAL CYBER ALLIANCE