Whitepaper

Secure Provenance

Shining a light on the security and sovereignty of computing systems and storage

Jason English

Principal Analyst, Intellyx

January 2020

Have you heard about the Asian firmware hack that may have compromised just about any computing device produced over the last five years in the United States?

Perhaps you heard about it and simply forgot about it, because the story either seems as unbelievable as a computer catching the bird flu, or the reality of it is too grim to accept.

Most high-tech OEMs and service providers are powered on hardware and software that could be compromised at its root level by a tiny chip intentionally implanted by state operatives, or an accidental inclusion of malware from a downloaded bit of code.

Like a cereal company whose product is full of cancer-causing pesticides, the world's largest institutions don't want you to focus on how widespread security exploits are in the complete end-to-end supply chain for all of the high-tech products involved in their operations, because it's bad for business.

This paper will educate you on the reasons why transparency into the origins of our hardware and software is important for assuring the integrity of critical systems and data, and how your enterprise can address this challenge by passing the test of secure provenance.

Widespread computing security risks

With globally sourced computing resources and internet-connected devices proliferating throughout every workplace and living space, the world is just starting to wake up to the reality that we are never 100 percent sure where all of our technology components and code came from.

To use a supply chain term, we are looking for **provenance** – knowledge of the origin and history of every component of hardware and software code that has made its way into our finished technology products, from design, to sourcing, components, transport, sub-assembly, system configuration, manufacturing, packaging and delivery.

Who should care about provenance?

National, state and local governments. The US DoD and its supporting defense industry contractors are famous for being serious about security, so you can expect that they care about this issue, offering standards that are difficult (and costly) for suppliers to live up to.

Think about all the other assets beyond defense systems which are managed by governments. All the citizen data, agencies, and infrastructure -- including power grids, water, communications and transport. Compromised equipment or software could cause real public havoc.

Financial firms. Financial institutions have already factored in the expected cost of fraud. Several percentage points are set aside by banks and credit card companies for remediating unauthorized transactions as an expected loss due to thievery.

That is why fintech and insurance IT leaders often underestimate their financial exposure to compromise, since they are not accounting for widespread identity theft, or a partial or complete system downtime event. Regulatory penalties and a loss of customer confidence creates an impact that is felt in the boardroom.

Healthcare institutions such as hospitals don't just guard private patient data and valuable clinical records, they also operate thousands of life-supporting devices. As everything becomes connected, you can bet on many devices to become IoT (Internet of Things) ready and available to the network to improve customer service.

It's probably beneficial that medical devices have a very lengthy development and regulatory approval process for patient safety reasons, but there's a big catch. By the time an electronic medical device is finally rolled out, it may already be designed to outdated security standards, and contain well-known exploits.

Any organization that depends on safe and secure data, and how its customers, employees and partners would be affected by an exploit, should care about provenance.

Challenges of securing technology

No organization can afford to hit the snooze button on provenance risk. Only through ***secure provenance,*** a total certainty of the source of every aspect of the product, can systems possibly be considered secure.

There are several reasons why attaining security provenance is easier said than done:

- **Outsourcing:** Almost all high-tech OEMs, component manufacturers and global brands have outsourced their high-tech supply chains to China or elsewhere in Asia, in a constant drive to minimize production and materials costs.
- **Multi-tier supply chain:** Supply chains are inherently very dynamic, multi-tier relationships between many suppliers and buyers. You might buy a rack unit from a 1st tier company in the US, while 2nd tier companies may do assembly and logistics, and they are using a changing set of 3rd tier suppliers for contract manufacturing, assembly and transport. It is often impossible to gain visibility more than one layer deep in these loosely coupled federated orgs.
- **State Spying:** When you scan the news about major overseas high-tech and telecommunications providers like Huawei, ZTE and Foxconn, there are reports of industrial supervision and spying by government actors, in places where end customer privacy isn't a matter that can be debated. There are several nation-states with economic and strategic incentives to continue snooping and sabotaging systems.
- **Firmware:** Electronics contain firmware, code written directly into chips on the hardware or device to define sub-system level instructions for booting up, power and memory handling. These firmware routines generally run below the OS and don't appear in file systems or software registries. Therefore, scanning with conventional anti-virus, security and auditing tools can miss errant instructions or routines in the firmware that could possibly intercept or transmit data, user sessions and tokens in transit or in memory.
- **New Exploits:** Even the most advanced measures available today can fail tomorrow, as bad actors develop new ways to embed harder to detect exploits. For instance, the tiny 'spy chip' has been replaced by a payload in a less detectable flat piece of silica within the board in newer versions.

Solution: The Clear Box Test

Before you can attain secure provenance, you must prove beyond doubt that you can identify the origin of every element in your systems. Getting there requires passing what I'll call a '***Clear Box Test'*** – providing auditable transparency into:

- The original requirements and design specifications of the device and system, including architecture, operational code, source components and materials.
- All source code for embedded hardware, firmware and software that goes into each device, with known contributors and traceability. Simply copying open source code (e.g. a given Linux version) from a repository doesn't provide transparency, as there are many corrupted copies, alternate versions, updates, and components found in open source repositories, and they may have known vulnerabilities or undeclared customization.
- Open testing and quality assurance processes, from unit to system-wide level, and current test results.
- Observability of the operations of the whole system, not only at the application, UI or OS layer, but from boot cycle, to live operations, to shutdown and idle processes in the firmware.
- Documented custody over time of every single component that went into the finished product, with known persons or contributing entities certified at every stage of its manufacture, assembly, setup and transport.

In other words, if you lack transparency into any of the above criteria, then you don't have sovereignty over your systems. You don't have a clear box, you are actually dealing with a black box. Any unknown or unseen actors or components introduced into the lifecycle of your system invalidate the auditability of the whole system.

"Reports that say that something hasn't happened are always interesting to me, because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns — the ones we don't know we don't know."

-- Donald Rumsfeld, former US Secretary of Defense, 2002

Results: What to expect from Secure Provenance

It's important to note that even if your IT product or service passes the clear box test, and is 100 percent verifiable to its origins, secure provenance does not prove your system is free of vulnerabilities, or that it can't be hacked.

What should **secure provenance provide?**

- **Total transparency.** The peace of mind of being able to shine a light into every corner of your systems means there are no 'unknown knowns' lurking at any layer of the architecture. Transparency doesn't just expose bad actors who may be attempting to embed themselves in your systems, it also makes data handling issues, component or code errors, and unauthorized changes much easier to detect in testing.
- **Total responsibility.** You know who has custody of every element of the IT system throughout the design, creation and delivery process -- manufacturing, hardware, software, and the people identified with responsibility for delivering the components. In addition to eliminating outside intervention, it gives you a way to trace any issues back to the responsible parties.
- **Total compliance.** Secure provenance lets you establish a compliance program with confidence, whether you are seeking to pass requirements at the national security level, or in meeting industry IT standards for data security and privacy such as HIPAA for healthcare data, or PII for financial customers.

  If a system passes the above clear box test, chances are most of the hard work and documentation any compliance audit could ask for has already been accomplished anyway!

Is anyone doing secure provenance today?

The above requirements may seem too rigorous to meet, given today's dynamic, globally distributed supply chains and the massive attack surface afforded by today's age of ubiquitous network and service connectivity.

Secure provenance is not out of the question, if you demand it.

SoftIron produces hyperconverged, software-defined storage and transcoding devices with OS, storage, network and compute capabilities built 100% from concept to design, sourcing, manufacturing and delivery in the United States – California to be exact – using all known origin chips, suppliers and development labor throughout the process.

The team delivers a purpose-built "Hyperdrive" device (pictured), tuned for the popular Ceph open source storage format, with certified builds of Ceph, Debian Linux OS and its own resource management software configured on board.

There are several other good reasons a company would maintain such tight resource transparency over hardware and software aspects from the start. Closer agile team collaboration for faster innovation cycles, and better control over the performance, design and quality aspects of their rackmountable devices delivers product value beyond security.

None of those benefits can take away the dividends of auditability and customer peace of mind gained through Softiron's adherence to security provenance measures.

The Intellyx Take

Security provenance may seem a bit over the top, even for very security-minded professionals, but it is worth thought and preparation now, before it is too late to reverse course on a high-tech supply chain that is vulnerable by design.

There was once a time when ‘security by obscurity,’ or closed source, black box technology was thought to be an advantage. With AI-level sophistication of attacks, nation-sponsored cyber surveillance and cyberwarfare programs, and an increased threat surface area as everything becomes connected to the Internet, obscurity’s not good enough anymore.

We’re in uncharted territory here. At no time in history have we seen a threat environment this asymmetrical. The primary zone of conflict—now and in the future—is no longer defined as a battlefield with guns and tanks, it is in defined in software, with attacks moving over fiberoptic cables through racks of servers.

Why stand in the dark about your vulnerabilities, when there is an open, transparent path you can take? If the sovereignty of your data matters, then take a stand on secure provenance.

About the Author

Jason "JE" English (Twitter: @bluefug) is Principal Analyst and CMO at Intellyx. He is focused on covering how agile collaboration between customers, partners and employees accelerates innovation.

He led marketing efforts for the development, testing and virtualization software company ITKO, from its bootstrap startup days, through a successful acquisition by CA in 2011. JE co-authored the book Service Virtualization: Reality is Overrated to capture the then-novel practice of test environment simulation for Agile development, and more than 60 thousand copies are in circulation today.

About SoftIron

SoftIron® makes the world's finest solutions for the data center. The company's HyperDrive® software-defined storage portfolio is built on Ceph; it's custom-designed and purpose-built for scale-out enterprise storage and runs at wire speed. HyperCast™ delivers the best density and value for real-time video streaming. SoftIron unlocks greater business value for enterprises by delivering great products without software and hardware lock-in.

© 2020, Intellyx, LLC. Intellyx retains full secure provenance over the content of this document. At the time of writing, Softiron is an Intellyx customer. None of the other companies mentioned are Intellyx customers. Image source: bluefug (cover), Softiron (product image)