ARC VIEW

SEPTEMBER 24, 2020

Take Control of Your ICS, IIoT, and IoT Software Supply Chain Security Risks

By Sid Snitkin

Keywords

ICS Cybersecurity, OT Cybersecurity, Industrial Cybersecurity, ICS Software Supply Chain, aDolus

Summary

Software supply chain security is a hot topic today. Malicious code can get injected into smart industrial control system (ICS) devices and systems at multiple points during their design, manufacture, distribution, and use. Downloads can also contain newly banned modules that might jeopardize regulatory compliance.

Companies are rightfully concerned about the trustworthiness of every piece of software and firmware being used in their plants and products. As ARC learned in a recent briefing with aDolus, effective tools are available to help companies address this extremely challenging issue.

Asset owners and suppliers need to be concerned about the trustworthiness of every piece of software and firmware that is downloaded into their plants and products. While cyber defenses have strengthened, resilient attackers have shifted to more indirect, social engineering tactics to compromise critical assets. Targeted spear phishing of plant personnel for passwords has become commonplace. Similar techniques are being used against vendors to gain access to sites where malware can be injected into trusted software modules and download files. Social engineering is also being used to trick technicians into downloading fake update files for critical systems and IoT devices.

Managing this situation is challenging for asset owners and suppliers. Facilities can include equipment from hundreds of ICS vendors with software and firmware components from a multitude of third parties. Ensuring trustworthiness has to be an ongoing activity across ICS supply chains, but many companies lack the resources to keep ahead of all these threats.

Recently, ARC Advisory Group discussed the challenge of managing ICS software supply chain risks with executives of aDolus Technology Inc. This company offers a platform for asset owners, vendors, integrators/consultants, and security partners to monitor the security of files distributed across their software supply chains efficiently and effectively.

Software Supply Chain Security Is Everyone's Problem

Critical infrastructure operators in industries like oil & gas, power, and manufacturing need to be confident that their control system assets and IoT devices are always secure and trustworthy. Managers in industries like aerospace, automotive, and healthcare equipment have similar concerns regarding the technology used in their products. A compromised ICS device or application could jeopardize health and safety as well as disrupt an organization's profitability.

While most ICS software suppliers strive to ensure the security of their smart devices and applications, their efforts can be compromised by malicious actors throughout the product lifecycle. Security management and trustworthiness verification needs to be a priority for every party in the ICS software supply chain.

While ICS and Industrial IoT (IIoT) suppliers strive to ensure the security of smart devices and applications, their efforts can be undermined by malicious actors throughout the product lifecycle. This begins with programmers releasing software and firmware without fully verifying the trustworthiness of their code and all the third-party modules they use. Even trustworthy product releases can be compromised if distributors lack good site security programs.

Device security can also be compromised during system implementation. Consultants and system integrators may build systems using compromised downloads or obsolete versions of products with known security issues. Likewise, they might be tricked into applying compromised update and patch files.

Given that ICS assets and smart products are designed for decades of use, the highest risk of surreptitious malware injection occurs through the many patch and update files that will be installed during a product's lifetime. Many technicians lack the time and resources to fully verify the morass of patch and update files they receive from vendors and third-party software suppliers. Technicians can also be tricked into downloading fake patch and upgrade files that have valid certificates and digital signatures stolen from suppliers. Suppliers can also fail to address "hidden vulnerabilities" that emerge in third-party modules that are embedded in their products.

ICS product vendors need to accept responsibility for managing the security of all software and firmware they provide. They should know which firmware and software are the correct versions and have the people, processes, and technologies in place to ensure that customers receive secure distribution packs. But they can't do everything. Security management and trustworthiness verification has to be a priority of every party in the ICS software supply chain.

Overcoming Software Trustworthiness Challenges

There are standard approaches that suppliers can use to protect customers from receiving modified software, such as vendor-published MD5/SHA file hashes and code signing. But use of these approaches is far from universal, especially for embedded devices. And they presume that asset owners have the tools and people to check them.

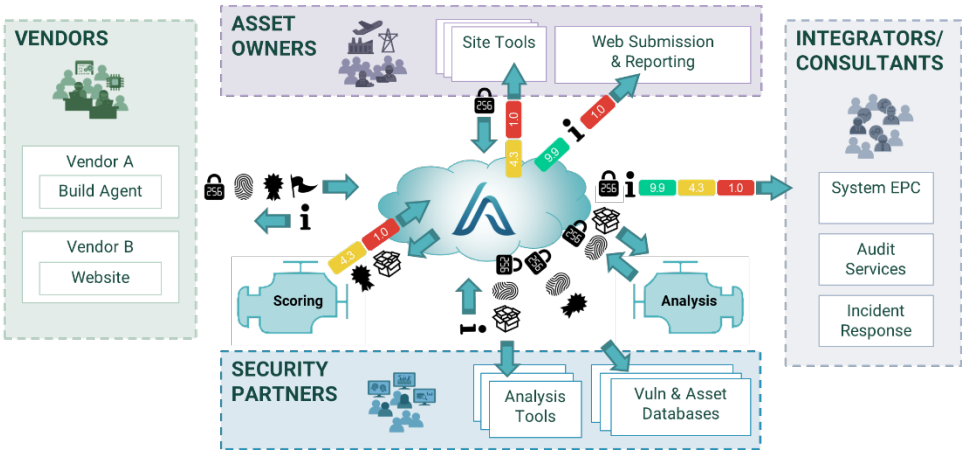
Asset owners have access to a variety of information sources that can help them manage software supply chain risks. There are databases for malware and vulnerabilities and many suppliers offer extensive product knowledge bases. But no factory technician is going to spend days searching the internet before upgrading a PLC, especially when they have other, more pressing, responsibilities. Even if they did, searches may not reveal vulnerabilities in embedded modules or banned software unless the supplier has explicitly released its own product alert. Technicians may also lack the cybersecurity expertise to reconcile search results from inconsistent information sources.

ICS vulnerability management programs have become commonplace. The associated asset inventory tools provide good lists of software modules and associated vulnerabilities, but they don't detect fake versions or malware that was injected into good modules on supplier websites. These kinds of problems need to be trapped before software is loaded into systems. Off-line, pre-testing of software is also not a panacea. Test systems may not reveal sophisticated malware, especially when efforts are focused primarily on avoiding operational problems rather than verifying security.

To address ICS software supply chain risks, companies need convenient ways for everyone to verify the software and hardware downloads they receive from others in the ecosystem. Furthermore, this has to support needs that arise throughout every product's lifecycle, whether it's a download of a new product, an old product, or patch and upgrade files for products in use.

The aDolus Platform Addresses ICS, IIoT, and IoT Needs

aDolus understands the complexity of these challenges and has built a solution that can help organizations ensure software trustworthiness across complex ICS smart device supply chains. With support from the US Department of Homeland Security (DHS), aDolus created a community platform, FACT, that aggregates information on software and firmware to produce a trustworthiness score for software downloads (like a FICO score for credit).



aDolus FACT Platform

As discussed below, the FACT architecture allows each type of user to interact in a way that is best suited to their needs.

Vendors of ICS Products and Applications

Vendors that are certified by aDolus create digital fingerprints of their legitimate software/firmware via an automated agent within the secure perimeter of their software development process. This fingerprint is transferred over an encrypted link to FACT, which verifies the authenticity of the vendor and stores the digital fingerprint in a secure database, creating a repository of trusted artifacts.

FACT then sends the vendor's information to an analysis engine to determine the subcomponents and identify any known vulnerabilities or malware. The system provides a report to the vendor that advises them of problems their customers might experience with the software as well as advice on possible improvements.

Asset Owners

Asset owner technical staff obtain firmware/software releases through a variety of distribution channels (such as USBs or vendor websites). Prior to installing the firmware/software, they use the aDolus web client (or a local tool such as a file analyzer or network traffic analyzer) to generate a digital fingerprint of the unverified firmware/software.

FACT compares the fingerprint of the unverified content against the certified digital fingerprints stored in the repository. FACT also provides a confidence and security rating of the firmware/software and all its subcomponents. Based on this score, asset owners can decide to approve (or reject) the firmware/software for use in their operations.

The API-based design of FACT allows files discovered by any means on the plant floor, such as network monitoring or drive monitoring, to be reported on with a simple API call containing the file's hash. This can then drive reporting to management on the security and quality of ICS software actually being deployed on the plant floor.

FACT also provides the asset owner with an understanding of who is using specific software products or where vulnerable packages may be deployed in their company.

Security Partners

There are hundreds of different databases and analysis tools for software, each providing unique insights to the trustworthiness of software. For example, VirusTotal is a very comprehensive database of malware while the NIST CVE database lists thousands of known software vulnerabilities. FACT reaches out to each of these partners to better understand how the community views each piece of software that is analyzed.

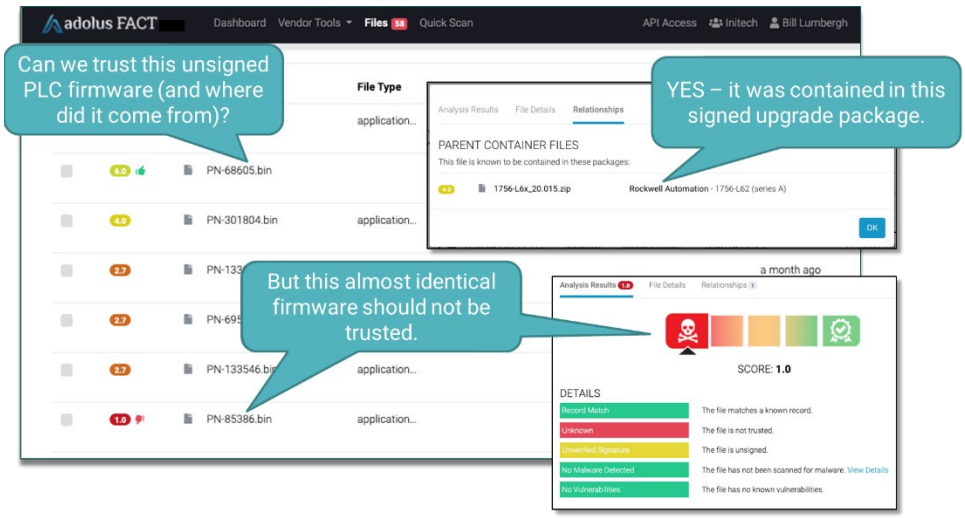
Similarly, partners offering security services, such as traffic and anomaly analysis, can make calls to FACT to learn more about the files they discover on a client's network or computers.

Integrators/Consultants

Integrators can use FACT to verify the trustworthiness of files they use in building systems. Consultants offering security services, such as audit or incident response services, can also make calls to FACT to learn more about the files they discover on a client's network or computers.

FACT Supports Many Use Cases and User Needs

The FACT solution serves mission-critical systems in any industry by bringing together the information needed to ensure that software/firmware is authentic and safe to use. The figure below shows the kind of information a technician with software/firmware updates for a PLC can get from a FACT analysis.



aDolus FACT Enables Deep Analysis of File Trustworthiness

The ability to deconstruct a complex installer and create a database of associations enables FACT to validate "unsignable" binaries as well. In this example, a lone upgrade package for a ControlLogix PLC is associated back to an original installation package signed and released by Rockwell Automation.

FACT can also check the consistency of a certificate signing chain, helping protect against threats like stolen keys that have been used in attacks like Stuxnet. This is useful to both vendors and asset owners.

Vendors also have the ability to tag their software as 'Supported," "Update Recommended," or "End of Life" so that FACT can communicate this to users of that product instance. The benefit to both users and vendors is that notices are tailored to exactly the software in use at a site, so people don't have to deal with bulk notices that reference all software produced by a vendor and directed to their full subscriber list.

Conclusion

The security of industrial control systems is a critical matter. A cyber compromise or unauthorized change can impact the health and safety of people, damage costly equipment, and disrupt operations for extended periods. Digital transformation is increasing the likelihood of such events with the proliferation of new devices and software from suppliers around the world.

Fortunately, many industrial companies already recognize these risks and work is also underway in the ISA working group responsible for the IEC 62443 to include requirements for managing software supply chain cyber risk. Power industry regulations, like NERC CIP-013, are likewise forcing owners and operators to require vendors to address software supply chain security. This includes disclosure of known vulnerabilities related to their products and services as well as verification of software integrity and authenticity of all software and patches they provide.

While ARC applauds these efforts, it is also important that every company recognize that managing malware injection across complex ICS software supply chains can be overwhelming. So, every company in the supply chain needs to make sure it has the tools to do its part in ensuring that all devices and applications remain safe, secure and reliable.

The aDolus FACT solution offers a means to address these needs throughout the industrial software ecosystem. Prudent companies will learn more about these types of solutions to ensure the security of their critical infrastructure.

For further information or to provide feedback on this article, please contact your account manager or the author at srsnitkin@arcweb.com. ARC Views are published and copyrighted by ARC Advisory Group. The information is proprietary to ARC and no part of it may be reproduced without prior permission from ARC.