CYBERHARDEN INDUSTRIAL CONTROL SYSTEMS NOW (OR DEAL WITH THE CONSEQUENCES TOMORROW...)

With national and economic security and public health and safety at risk, it's time for a new solution to reduce the attack surfaces that hackers most commonly use to compromise components of industrial control systems in critical infrastructure.

TABLE OF CONTENTS

INTRODUCTION

In the race for more efficient operations, industrial control systems have become a mash-up with legacy hardware being integrated with software and smart devices. As more and more controllers, servers, remote terminals, monitoring equipment, and sensors are tied to the internet, the cyberattack surface increases exponentially, making our critical infrastructure vulnerable to unprecedented threats.

This paper focuses on the need to add cyberhardening protection directly to software binaries, rather than relying solely on external detection tools such as firewalls, gateways, intrusion detection, and monitoring that identify a problem without actually doing anything to solve it. It introduces Runtime Application Self Protection (RASP) in general, and RunSafe Security's Software Guardian specifically, which is a lightweight, agentless, and automatic one-time binary transformation solution that covers operating systems, applications, and devices.

The traditional decision in cybersecurity investment has always been whether the total cost of ownership (TCO) is less than the annualized loss expectancy (ALE) drawn from risk analysis, as part of the NIST Cybersecurity Framework[1] or other similar approaches. In the past, air-gapped systems were deemed to have relatively low risk, since compromising them would require physical access, with no economies of scale. As has become evident, ALE has increased dramatically with cyberattacks scaling to thousands or even millions of connected devices, each with identical images. An exploit that works on one will work on all.

RunSafe's Software Guardian offers a practical approach to cyberhardening industrial control systems and embedded systems and devices, emphasizing effective risk mitigation, affordability (lowering TCO), ease and speed of implementation. RunSafe's process does not require additional resources – whether hardware footprints, or on an already overburdened IT staff, especially those managing the plethora of false positives from various monitoring agents and services.

YOUR ICS IS EITHER DIRECTLY OR INDIRECTLY UNDER ATTACK

In March 2018, the U.S. government accused Russia of remotely targeting its power grid. The Department of Homeland Security believes Russia has tried to attack targets within energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors since 2016.[2] In December 2017, a new form of malware, named Triton, shut down the operations of a Saudi Aramco facility that used Schneider Electric's safety instrumented systems. Triton targeted hardware and software controls, which monitor physical processes through sensors and acoustics.[3]

Additional evidence of the cyber-physical threat to Industrial Control Systems (ICS) can be seen in the number of vulnerability advisories issued by the ICS Cyber Emergency Response Team (ICS-CERT). This number has increased more than 700% from 2010 to 2017 and shows no signs of abating.[4]

ICS modernization coincides with burgeoning smart device connectivity, the proliferation of the Internet of Things (IoT) and the Industrial Internet of Things (IIoT), predictive analytics, and data sharing via the cloud. The expanded capabilities come at a cost, as both the number and size of potential attack vectors increase. **A confluence of issues compounds ICS cyber vulnerabilities, including:**

- Components of today's ICS are less and less likely to be air-gapped (ensuring that a secure computer network is physically isolated from an unsecured network).
- Digital technologies and applications are being added to analog legacy systems from the pre-internet era (Linux, Windows, and numerous mobile apps are being introduced to enable connections) causing interoperability issues.
- The divide between IT (Information Technology) and OT (Operational Technology) in many organizations is not being bridged effectively, and it is not cybersecurity resilient.

In today's infrastructure, defense in depth security is not often present. Apps, devices, and systems are more directly vulnerable to malware, viruses, spyware, and zero-days. Attacks can come from the outside (nation-state actors/hackers), insider threats, and increasingly from a compromised supply chain. Apps are targeted by new types of file-less attacks that sidestep traditional network and endpoint detection. These include memory corruption attacks (buffer, stack, or heap), and return oriented programming and jump oriented (ROP/JOP) attacks. Buffer overflow attacks are the best known driver of software vulnerabilities.

The ICS+IoT context of intertwined hardware, firmware, Operating Systems (OS), libraries, and apps built around low-cost processors presents some unique challenges:

- Constraints of performance, cost and resources can mean traditional security tools offering defense in depth may not be in place
- Adding software, services, and / or hardware agents may lead to performance issues, retooling and retesting, especially in real time environments where jitter could be an issue with non-deterministic execution
- Patching and updating may be infrequent, expensive, and / or unavailable, leading to a potentially indefinite vulnerability window
- Even simple apps leverage libraries and OS calls can add up to hundreds of thousands or even millions of lines of source code
- All vulnerabilities cannot simply be discovered using conventional static or dynamic analysis (SAST or DAST) tools, inspections, or profiling
- Re-engineering with secure libraries and best practices may be cost prohibitive, source for code and libraries may not be available, and changing compilers or OS impractical
- When deploying to tightly bundled environments including components from many suppliers, the supply chain itself may not be trusted, with potentially compromised hardware, firmware, OS, containers, or hypervisors

Some of these challenges are unique to an ICS+IoT environment. However, several of the vulnerabilities extend to mobile devices, communications, and cloud environments, where software deployment and updating occurs via orchestration and automation tools. These vulnerabilities can also be found in virtualized environments, hypervisors, containers, and third-party hardware.

UNDERSTANDING THE MOST COMMON INDUSTRIAL CONTROL SYSTEM VULNERABILITIES

Understanding the various hacking methods is key to minimizing your risk.

- **Buffer Overflows** – Memory corruption, stack, heap, Return Oriented Programming (ROP) chain exploits, and buffer overflows consistently rank as one of the top five cybersecurity vulnerabilities[5]. When a program or process tries to write more data to a fixed length block of memory (buffer) than it is designed to hold, the result is a buffer overflow. These attacks often work because applications fail to manage memory allocations and validate input from the client or other processes.

- **Unauthenticated Protocols** – Authentication protocols, which are used to transfer authentication data between two entities, are an important layer of protection for communication with computer networks, ensuring that only legitimate actors can do things. When an ICS protocol lacks authentication, any computer or device connected to the network can send commands to change or manipulate the operations or compromise processes.

- **Weak user authentication/password management** – Passwords are part of critical access points of entry. User authentication weaknesses in legacy industrial control systems include hard-coded passwords, simply guessed passwords, passwords stored in easily recoverable formats, and passwords sent in clear text. Even knowledge-based authentication can be weak if password management and policies are not kept current or changed regularly.

- **Untimely adoption of software and inadequate testing of patches** - Lack of software signing that confirms the software author and guarantees that the code has not been altered or corrupted allows attackers to trick users into installing software that did not originate from the vendor. ICS often run unpatched operating systems, leaving them exposed to known vulnerabilities. In addition, the improper implementation of patches can also cause security issues.

- **Outdated hardware** – Many organizations use old hardware in their ICS environment that was not designed to counter cyberattacks, such as hardware roots of trust. The additional connected hardware and devices open new opportunities to compromise legacy systems, well beyond the fence that was originally envisioned as “secure.”

HOW THE DAMAGE TO CRITICAL INFRASTRUCTURE IS DONE

- **Insecure / Unsafe Systems (Spoofing)** Sensors measure physical aspects of their environment and relative parameters of processes/equipment (e.g., status presence, power, proximity, distance, flow, level velocity; efficiency of the network, and new activity of IoT smart devices). Sensors can be found across all domains - to assess drones, thermostats, beacons, medical, gas and oil, or telecommunication systems. As networks become entirely dependent on sensor data, they become more vulnerable to spoofing attacks, denial of service, session hacking, or social engineering through low priority systems.

- **Production Shutdown (Controlling Physical Components)** Actuators are components of machinery or industrial processes that are responsible for moving or controlling a mechanism or system, like opening a valve or directing a robotic arm. An actuator needs a control signal and a source of energy. If that signal or energy source is interrupted during a cyberattack, the machinery will either stop operating or misfire in some way.

- **Unreliable Feedback (Forcing Behavior)** When an attacker gets control of a physical or process operation via a critical access point, damage can be done by forcing a system or process to become non-operable, weaken machinery, causing overheating or misalignment in procedures. Further, this type of hack leads to unreliable data.

- **System Disablement/Damage (Disconnection)** By interfering with control system interoperability, many cyberphysical devices and systems can be damaged. For example, denial of service attack can stop air conditioning or heat, putting the operations of data centers out of commission.

- **Loss of Data (Exfiltration)** Malware that executes arbitrary code can be introduced via Human Machine Interface (HMI), communicating through programmable logic controllers and other ICS components. For example, in sending data from a non-cyber-physical infected host to an infected host with internet connectivity, sensitive information about industrial processes can be gleaned.

FAST FACTS

- **In February, cyptocurrency mining malware was discovered in the operational technology network of a water utility in Europe – the first known instance of mining malware being used against an ICS. It had significant impact on systems.**

- **During the second half of 2017, nearly 40% of all analyzed ICS in energy organizations were attacked by malware at least once – closely followed by 35% of engineering and ICS integration networks.[6]**

THE LIMITATIONS OF LEGACY ICS SECURITY

Despite the growing threats, traditional cybersecurity measures continue to focus on detecting symptoms of attacks. They use external network and perimeter technologies such as gateways, firewalls, intrusion prevention and anti-virus agents. In addition, internal approaches such as static and dynamic analysis are used to try to detect vulnerabilities in code.

The problem with such traditional solutions is that they focus more on detecting symptoms rather than addressing the underlying causes. While established tools have worked for decades on known attack types, their effectiveness is diminishing as hackers with time and financial resources become increasingly skilled in designing attacks to avoid detection.

Yes – detection will always be a critical component of the cybersecurity arsenal, because identifying and remediating threats before they spread can alleviate some risk and damage incurred by a cyberattack.

But detection alone is no longer sufficient in this fraught environment. Detection tools offer no protection in cases where the supply chain itself is compromised, in the case of file-less attacks like memory corruption exploits, stack and heap attacks, Return-Oriented Programming (ROP) chain attacks or zero-day attacks.

Host-based detection agents, such as OSSEC, Snort, and Bro, may also create performance issues that can require retooling and retesting to implement. Further, detection monitoring and alerting also requires, time, investment, and expertise.

Finally, re-engineering code adds a requirement for a level of resources, as well as compliance challenges and risk that most companies are unable or unwilling to meet – especially in instances where the software stack might be hundreds of thousands or millions of lines.

RUNSAFE'S SOFTWARE GUARDIAN: A NEW WAY TO MITIGATE THE RISK TO YOUR ICS

The first step in mitigating the risks to your ICS embedded systems and devices is cyberhardening binaries, using RunSafe Security's Software Guardian patented transformation process. As noted, hackers can gain control of cyber-physical systems via memory corruption errors, stack, heap, buffer overflow exploits and ROP attacks. RunSafe hardens binaries (files and programs) against these, whether ICS in power plants and utilities, the vulnerable OT underpinning data centers, or IoT devices like routers and smart devices in vehicles and medical components.

The software from a control system is run through the cyberhardening process, without requiring access to source code, either as part of maintenance or routine updates. This renders threats inert by removing information about attack vectors and denies malware the uniformity required to propagate in scale. By precluding a single exploit from spreading across multiple devices and networks, RunSafe disrupts the traditional economics of hacking and shifts the odds in favor of the defender.

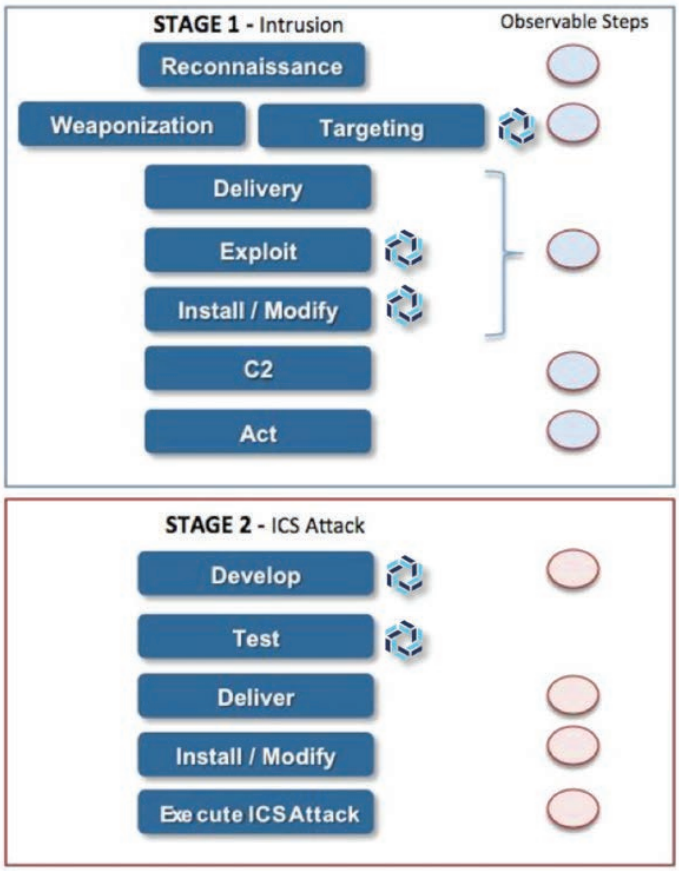
RunSafe's cyberhardening transformation process is remotely deployable and utilizes two Runtime Application Self-Protection (RASP) techniques to make the binary files and memory on each device functionally identical but logically unique. The first is block-level binary stirring (also referred to as randomization) that makes each protected device functionally identical but logically unique. The second is Control Flow Integrity (CFI), which protects against ROP attacks, in which existing code is called out of order to become a hacking script. This prevents malware from changing how commands are executed.

Another way to think about how Software Guardian defends ICS is to consider the Industrial Control System Cyber Kill Chain[7], which is envisioned as a two-stage process. Stage 1 is intrusion preparation and execution, and could be classified as espionage and intelligence gathering. Its purpose is to gain access to specific information about the ICS, learn the system, and create ways to defeat internal perimeter protections to get to production environments. In Stage 2, the hacker uses the knowledge gleaned during Stage 1 to develop, test, deliver, install and execute an attack. See the diagram below for a visual representation of where Software Guardian interrupts the attacker's kill chain, whether applied in Stage 1 or Stage 2.

SOFTWARE GUARDIAN INTERRUPTS THE ATTACKER'S KILL CHAIN

RunSafe's Software Guardian is a patented, agentless transformation process that:

- Cyberhardens vulnerable embedded systems and devices in minutes
- Maintains existing source code/ software with minimal additional overhead
- Leaves each system or device functionally identical but logically unique
- Reduces zero-day threats via binary randomization and control flow integrity
- Denies malware the uniformity required to propagate
- Protects software even if hardware is compromised
- Can be built in or applied to devices already deployed



RunSafe Security is being used by customers in many industries, for these applications:

- Protecting boards used to manage cooling systems in large scale data centers manufactured by a key player in the power, thermal and infrastructure management solutions business;
- Safeguarding routers and switches across core product lines for a preeminent producer of networking equipment; and
- Securing apps provisioned in a marketplace and protecting a differentiated platform for a private cloud provider.

RunSafe SECURITY

HOW RUNSAFE SOFTWARE GUARDIAN WORKS

Unprotected Software Image

- Vulnerable to cyberattacks that side-step traditional network and endpoint protections
- Memory corruption (buffer, stack and heap)
- Return Oriented Programming (R OP)/Jump Oriented Programming (JOP)
- Compromised hardware and software supply chain
- Zero day

RunSafe Transform Function

- Patented Runtime App Self Protection (RASP) process leverages
- Binary randomization and
- Control flow integrity
- Effective and easy to deploy
- No source, compiler or OS changes
- Agentless, so no new hardware, software or services on device

Protected Software Image

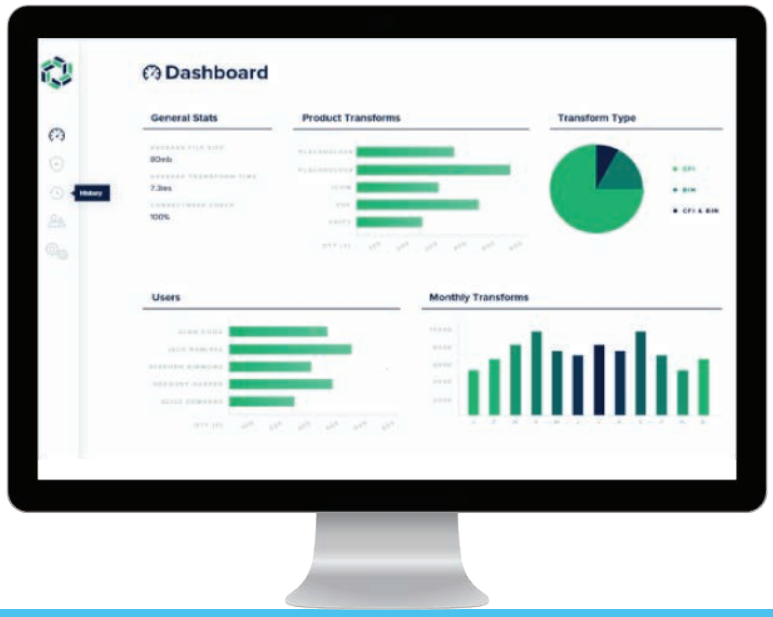
- RunSafe prevents attack scaling
- Each protected image is functionally identical but logically unique

RunSafe SECURITY

START WITH RUNSAFE SECURITY TODAY

Don't wait for a cyberattack to disrupt the operation of your business. Contract RunSafe Security now at (202) 430-6685 or sales@runsafesecurity.com.

RunSafe Guardian is as easy to deploy as downloading software binaries – and can be performed on new builds or equipment in use. The interface enables users to view the process step by step and ensures confidence in the cyberhardened results.



WHAT ELSE CAN YOU DO TO LOWER THE PROBABILITY OF A CYBERATTACK?

Some additional steps that can reduce the risk to your ICS, from the U.S. Department of Homeland Security (DHS)[8]:

- Implement application whitelisting to protect against attempted execution of malware.
- Ensure proper configuration and safe importation and implementation of patches to keep control systems secure.
- Reduce attack surface areas by segmenting networks into logical parts and restricting communication paths.
- Build a defendable environment to limit damage from perimeter breaches.
- Manage authentication with multi-factor systems and strict password policies.
- Implement secure remote access via steps such as read-only, time-limiting, and/or operator control.
- Monitor and respond by being alert to hacker intrusion and have a plan ready.

RunSafe SECURITY

REFERENCES

1. https://www.nist.gov/cyberframework
2. https://www.cnn.com/2018/03/15/politics/dhs-fbi-russia-power-grid/index.html
3. https://www.technologyreview.com/the-download/609789/a-new-industrial-hack-highlights-the-cyber-holes-in-our-infrastructure/
4. https://www.automation.com/automation-news/article/what-lies-beneath-avoiding-the-unseen-dangers-of-ot-vulnerabilities
5. https://resources.infosecinstitute.com/the-top-five-cyber-security-vulnerabilities-in-terms-of-potential-for-catastrophic-damage/
6. https://www.infosecurity-magazine.com/news/energy-sector-ics-infrastructure
7. https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
8. https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

ABOUT RUNSAFE SECURITY, INC.

RunSafe Security is the pioneer of a unique cyberhardening technology designed to disrupt attackers and protect vulnerable embedded systems and devices. With the ability to make each device functionally identical but logically unique, RunSafe Security renders threats inert by eliminating attack vectors, significantly reducing vulnerabilities, and denying malware the uniformity required to propagate. Based in McLean, Virginia, with an office in Huntsville, Alabama, RunSafe Security's customers span the Industrial Internet of Things (IIoT), critical infrastructure, automotive, and national security industries.

RunSafe SECURITY
Zero Days Are Numbered

www.runsafesecurity.com
571.441.5076
sales@runsafesecurity.com