Defending Against Firmware Cyber Attacks on Safety-Critical Systems

by Chris. W. Johnson DPhil, Mohammed Hashim Saleem, Maria Evangelopoulou, Marco Cook, Rob Harkness and Tom Barker
Glasgow and Gloucester, U.K.

In the past, it was not possible to update the underlying software in many industrial control devices. Engineering teams had to "rip and replace" obsolete components. However, the ability to make firmware updates has provided significant benefits to companies who use Programmable Logic Controllers (PLCs), switches, gateways and bridges, as well as an array of smart sensor/actuators. While these updates — which include security patches when vulnerabilities are identified in existing devices — can be distributed by physical media, they are increasingly downloaded over Internet connections. These mechanisms pose a growing threat to the cyber security of safety-critical applications, which is illustrated by recent attacks on safety-related infrastructures across the Ukraine. This paper explains how malware can be distributed within firmware updates. Even when attackers cannot reverse engineer the code necessary to disguise their attack, they can undermine a device by forcing it into a constant upload cycle in which the firmware installation never terminates. In this paper, we present means of mitigating the risks of firmware attacks on safety-critical systems as part of wider initiatives to secure national critical infrastructures. Technical solutions, including firmware hashing, must be augmented by organizational measures to secure the supply chain within individual plants, across companies and throughout safety-related industries.

Introduction

Industrial Control Systems (ICS) play a crucial role in national infrastructures. In the past, these networks were isolated from the Internet and relied on specialist protocols, including Profibus and Modbus. However, they are increasingly accessible through MODBUS TCP/IP, PROFINET and Ethernet/IP gateways. This helps companies to monitor and control massively distributed production processes without duplicating network infrastructures [Ref. 1]. Organizations create VPN links between their office-based enterprise information systems and their operational networks using TCP/IP interfaces. This informs strategic decision-making and enables managers to continually monitor the productivity of underlying applications. Partly in consequence, IP-based protocols now account for 80 percent of all ICS installations [Ref. 2]. This illustrates a dilemma that is at the heart of this paper:

- Previously, the serial protocols used in ICS applications were inherently insecure — they were never intended to support encryption or strong authentication. However, they provided a degree of protection from mass-market malware because they were not widely understood.
- Today, TCP/IP variants of industrial protocols support encryption and authentication. However, more attackers understand their underlying implementation. ICS applications are vulnerable to denial of service/ransom attacks that were never intended to target safety-related processes.

A number of recent attacks have focused on the firmware that is used in ICS devices. Malicious agents can change the underlying code installed on PLCs, switches, and smart sensor/actuators by first compromising the enterprise information systems and then using TCP/IP gateways to port their malware inside previously isolated industrial systems. PLCs are specialized microprocessor-based industrial devices that can be programmed to automate control of several machines and processes. Smart devices are lower-level components that allow a degree of pre-programming/configuration in proprietary language. These devices include components such as protection relays, temperature controllers and pressure transmitters.

This paper explains how firmware verification tools have been developed and deployed to protect U.K. critical infrastructures. This is complicated because different manufacturers use a host of different mechanisms to structure, encode and verify the updates that are distributed by physical media, including CD-ROMs, as well as different Internet-based firmware servers. This paper later explains how technical innovations, including generalized firmware hashing tools, must be augmented by organizational measures to secure the supply chain within individual plants, across companies and throughout safety-related industries.

Firmware Attack Vectors for Safety-Critical Systems

The firmware that supports an embedded device in an industrial control system plays a similar role to that of an operating system in more conventional applications. It is stored in ROM, EEPROM or Flash memory. Without firmware, these devices are little more than

> “The firmware that supports an embedded device in an industrial control system plays a similar role to that of an operating system in more conventional applications. It is stored in ROM, EEPROM or Flash memory. Without firmware, these devices are little more than ‘bricks.’ With firmware, they can be updated to improve reliability, to address bug reports and, increasingly, to provide security patches.”

“bricks.” With firmware, they can be updated to improve reliability, to address bug reports and, increasingly, to provide security patches. Firmware updates are usually performed via interfaces provided by the device manufacturer, most often using Ethernet or RS-232 connections.

In safety-critical systems, these update mechanisms pose new challenges. Traditionally, the firmware of many ICS components was never routinely updated because of the additional costs associated with the verification and validation required to demonstrate that the modifications did not compromise safety requirements. In such cases, critical processes remain vulnerable to previously published security exploits. Hence, there is a growing conflict between security requirements to install firmware updates and the safety-related costs of ensuring that any updates do not undermine integrity requirements in industrial processes.

Some vendors now distribute Supervisory Control and Data Acquisition (SCADA) firmware updates from their websites. This exacerbates security concerns. Potential attackers can download a sample of the firmware for embedded devices, enabling them to experiment using second-hand devices that can be bought via Internet-based marketplaces. Penetration testing of embedded firmware can potentially discover back doors. The distribution of firmware patches over the Internet now also means that legitimate users have to ensure that any firmware is not downloaded from a malicious site. “Watering hole” attacks rely on high-value targets being drawn to a compromised website. “Man-in-the-middle” attacks insert illegitimate firmware on the route from a vendor’s website to the intended recipient — for example, by compromising the addressing mechanisms used to identify the manufacturer’s server.

The following list summarizes several different types of firmware attacks [Ref. 3]; any single attack may borrow concepts from more than one category:

- **System-Safety Patch Vulnerabilities** — As mentioned, software system safety requirements mean that many ICS components are unpatched. Hence previously published vulnerabilities can be used and re-used on safety-critical systems.
- **Zero-Day Exploits** — There is a growing marketplace in zero-day vulnerabilities, or attack methods that have not yet been patched. The closer that ICS components move to conventional architectures, the more likely they are to be affected by these attack methods. There is also a growing competence among state-sponsored actors who are focusing on national critical infrastructures.
- **Reverse Engineering** — These attacks build on aspects of the Stuxnet/Olympic Games attacks [Ref. 4]. Penetration testing tools can be used to understand elements of the architectures used by manufacturers in their firmware updates. If digital certificates can be forged or undermined, it is possible to inject malicious code in an update that would otherwise leave the rest of the functionality unaffected until the attack is launched. Schuett et al. managed to modify functions identified during the disassembly stage of reverse engineering and injected them into the PLC firmware, causing denial of service to the operator under certain conditions [Ref. 5].
- **Code Mirroring** — Malicious code may ensure that any attempt to query the firmware will make it seem that a valid installation is being used.
- **Reload Death Spiral** — A simpler and more direct form of attack can be triggered in some devices. If a validation step fails late in the firmware installation, the device may halt while a new version of the firmware is downloaded. If that code is also corrupted, the device will repeat the download indefinitely.
- **Firmware “Bricking”** — A more general version of the reload-death spiral is an attack that successfully installs malformed firmware in a manner that

compromises the device. This is a simplified version of reverse engineering attacks. It is not necessary to understand how to hide malicious code in a valid installation — only to get the device to load the compromised code that need not implement any valid computation [Ref. 4].

It is important to stress that tools are being developed to automate aspects of these attacks. Costin et al. [Ref. 6] describe a system that conducts large-scale static analysis looking for vulnerabilities and correlations across families of firmware. Zhu et al. [Ref. 7] propose algorithms to help determine the image base of firmware; for instance, by identifying literal pools within a firmware file. This can then be used to determine a candidate base address for the firmware image. Their work focuses on devices that exploit ARM processors; however, many of the underlying concepts have more general applications.

It is important to stress that at present, it is not possible to directly validate the firmware that is running on many ICS components. Each manufacturer alters the binary representation of executable and resource files that are transferred between installation environments and the underlying ROM/EEPROM/Flash as the firmware update proceeds. The Glasgow group is actively engaged in developing forensic techniques that conduct this form of analysis on particular components. However, in general, this requires a low-level understanding of specific devices, including firmware architecture, memory encoding, etc. Painstaking reverse engineering can gradually piece this information together, but it must be repeated for different manufacturers and devices. As a pragmatic interim step, we want to update firmware and application software from a trusted source with a high degree of confidence, even if we cannot prove that the software running on a device has not been modified.

To defend safety-related ICS components against firmware attacks, it is first necessary to understand the underlying vulnerabilities. Therefore, we focused our initial work on two very different devices. The first is a widely used PLC; this was chosen because PLCs are the computational workhorses of safety-related processes. The second device was an IP-based security camera; this was chosen because of the obvious consequences of undermining the physical security of safety-related ICS applications[1]. We started to determine whether minor modifications to the firmware of an embedded device can bypass firmware integrity checks.

The first step in attacking the PLC was to determine the version of firmware being run on the device, assuming that an attacker only had remote access to the ICS component. We were able to use public information sources to determine how to do this by inspecting the binary firmware image for the PLC. The same techniques also worked on the camera and PLCs from other manufacturers. Once the firmware version had been obtained for the devices, we downloaded valid firmware already running on both devices from the manufacturers' websites. We were then able to edit the binary files. Our analysis revealed a surprising range of responses on the devices when we made simple changes to the version identifiers. We were able to map out the range of legal and illegal version numbers for the camera. Moving outside the permitted range elicited an error message from the firmware update interface, numbers inside the approved range but still invalid for that version were not reported and the firmware was passed directly to the camera for installation. With the PLC, our edits caused the device-upload interface to hang. We were forced to conduct a manual reset resembling the firmware spiral mentioned as item 5 in the previous list of attack methods. The key point here is that even relatively simple changes provoke inconsistent responses on different ICS components, some of which could be exploited within a malicious attack unless defenders take measures to protect their safety- related systems.

The Glasgow Firmware Defender

A growing number of papers describe firmware attack vectors; fewer provide potential solutions. McMinn uses MD5 hashing and bit wise comparisons on the firmware for a PLC [Ref. 8]. Hashing algorithms calculate characteristic values from a file. Changes to a file can be identified because the hash value will change if it is recalculated. For example, if the number of characters in a file was used as the hash sum, any insertion or deletion would be identified because that value would change. However, if an attacker deleted a valid character and then inserted another one, this might not be detected using this simple algorithm. This is an example of hash collision where the values of the hash function cannot detect the change. Unfortunately, MD5 suffers from a range of vulnerabilities, including known problems with hash collision. More formally, a suitable hash function should ensure:

- **Pre-image Resistance:** Given an unknown message of arbitrary length x and its corresponding hash value y ($H(x) = y$), then it should be computationally infeasible for any other message n for its hash value m ($H(n)= m$) to match y — i.e., $m \neq y$.
- **Second Pre-image Resistance:** Given a message x that produces a hash value y ($H(x) = y$), then it should be computationally infeasible for any differ-

[1] Given the sensitivity of the topic, the identity of both devices is omitted. Further details are available from Chris Johnson, co-author of this paper.

ent message n to produce the same hash value as x $(H(x) \neq H(n))$.

- **Collision Resistance:** Given x; y in M where M is the set of all possible messages, then $H(x) \neq H(y)$.

Others have focused on a range of alternate methods — for instance, modeling hysteresis effects on low-level transmissions from firmware servers. Xiao et al. [Ref. 9] provide a more general architecture intended to secure ROM, RAM, boot-loader and processes within ICS devices. This again illustrates the tensions that arise between safety and security when proposing detailed technical solutions to threats against critical infrastructures. Xiao et al. rely on encryption across the software stack. This would have enormous safety re-certification costs for legacy systems that support European and North American industry. It would incur enormous overheads in the verification and validation processes that would be required to determine whether the upgrades had any impact on functional safety. As a specific example, many encryption techniques deliberately insert non-deterministic timing delays to disguise the algorithms they use. These delays undermine the timing analyses that are required to satisfy a host of safety-related requirements.

In the long term, it seems likely that vendors and systems integrators will adopt techniques similar to those proposed by Xiao et al., as legacy systems are gradually replaced by more secure counterparts. In the meantime, there are significant threats to our existing infrastructures. Therefore, we began to develop tools that could help secure the firmware that is being deployed in European infrastructures. Our tool's sole purpose is to verify whether a given suspect file is genuine. It is possible to conduct byte-by-byte comparisons. The size of firmware images creates significant computational overheads for such an analysis, although hardware support can be provided. Therefore, we also built on the techniques pioneered by McMinn [Ref. 8]. Recall that both the MD-5 and SHA-1 algorithms have been found to have high collision probabilities [Ref. 10]. Attackers can exploit these collisions by manipulating a firmware image to produce the same MD-5 or SHA-1 hash value as the baseline. Rather than relying on a single algorithm with known vulnerabilities, our toolset exploits several hash functions, eventually triggering byte-by-byte comparisons if doubts persist.

It is important to stress that many industrial processes rely on thousands of low-level devices, each running bespoke firmware. The techniques described in this paper create significant potential overheads if the Firmware Defender raises a large number of false alarms. This might occur if, for example, the tool was incorrectly configured using incorrect hash values for baseline versions of legal ICS firmware. Conversely, an attacker could undermine our system if they could register an illegal hash value that characterized their compromised version of the firmware. For this reason, we had to develop extensive verification and access control measures to protect the integrity of the tool itself.

Before the defender can be used, it is first necessary to survey all the valid versions of manufacturers' software that might be deployed within a particular organization. Although most suppliers compute their own hash values, they use different techniques both to encode the files needed to install the firmware and also to calculate characteristic values. Therefore, we developed common algorithms that can be applied in a consistent way across the archives being transferred between many different suppliers and their safety-related customers. We can then re-compute the hash functions across different forms of firmware for many different devices. However, for this approach to be successful, it is necessary to obtain a verified baseline copy. Safety-critical organizations must deploy physical and digital mechanisms to increase confidence that initial hash values are computed from reliable sources for the manufacturers' firmware. In the near term, this might be avoided if the ICS industry could agree on standard techniques for the generation of hash values across multiple suppliers.

Working with a number of industrial sponsors, we found that end users often operated many different firmware versions on a single family of devices deployed across a single production facility. Deployment of the tool helped these companies audit the firmware being used across a range of critical legacy processes.

The safety-critical nature of this project meant that acceptance testing of the tool had to involve authorized participants from critical infrastructure companies. During a pre-deployment study, we determined whether plant engineers could use the tool to identify modified firmware during a simulated update on ICS components. One issue that arose during this initial evaluation was the additional time that might be required to train a sufficient number of staff to ensure that all updates were verified on a 24/7 basis. We initially focused on firmware — partly because this had been a target in recent attacks on critical infrastructures in the Ukraine[2]. The engineers involved in our evaluation argued that the same level of protection should be extended to other levels of the software stack. In consequence, the application of our tools was extended in line with the Good Automated Manufacturing Practices (GAMP) [Ref. 11] software categories illustrated in Table 1. For example, our tool was extended to perform periodic checks on the configuration data associated with the smart sensor/actuators, mentioned in the opening paragraphs.Working with a number of industrial sponsors, we found that end users often operated many different firmware versions on a single family of devices deployed across a single production facility. Deployment of the tool helped these companies audit

Table 1 – Using Good Automated Manufacturing Practices (GAMP) in the Validation of the Firmware Defender.

Category	Extending the Scope of Software Authentication
1. Infrastructure software	Verify infrastructure software tools, such as ladder logic interpreters, and commercially available software, such as anti-virus applications
2. Firmware	Verify firmware in devices that present some form of risk to the system
3. Non-configured Products	Verify non-configurable software, such as plug-in software, for certain applications that cannot be altered
4. Configured Products	Verify configurable software such as software programs that are loaded onto PLCs, compute hash values on configuration data
5. Custom Applications	Verify bespoke software, which is developed in-house or from a third party. Examples of such software include macros, scripts, tools and applications used to automate laborious procedures.

the firmware being used across a range of critical legacy processes.

The safety-critical nature of this project meant that acceptance testing of the tool had to involve authorized participants from critical infrastructure companies. During a pre-deployment study, we determined whether plant engineers could use the tool to identify modified firmware during a simulated update on ICS components. One issue that arose during this initial evaluation was the additional time that might be required to train a sufficient number of staff to ensure that all updates were verified on a 24/7 basis. We initially focused on firmware — partly because this had been a target in recent attacks on critical infrastructures in the Ukraine[2]. The engineers involved in our evaluation argued that the same level of protection should be extended to other levels of the software stack. In consequence, the application of our tools was extended in line with the Good Automated Manufacturing Practices (GAMP) [Ref. 11] software categories illustrated in Table 1. For example, our tool was extended to perform periodic checks on the configuration data associated with the smart sensor/actuators, mentioned in the opening paragraphs.

Conclusions and Future Work

This paper describes work to defend European critical infrastructures against a growing range of cyber attacks. Many industrial control systems rely on devices that are hard to protect; they were never designed to be resilient against the threats that are emerging. New ranges of PLCs and of sensors provide support for onboard encryption and authentication. Unfortunately, it will be many years before these devices are used throughout the legacy systems that support national critical infrastructures [Ref. 12]. Such improvements also depend on the ability of engineers to identify ICS components that offer appropriate levels of security — not only for the threats that we see today, but also for new forms of attack that will emerge over the lifetime of any devices that are procured for future systems. We are developing a systematic set of criteria that can be used to compare the levels of security that are provided by ICS components. The intention is that these questions will augment an existing set of characteristics that are considered by a subset of European infrastructure providers when they implement the IEC 61508 standard. In other words, we are integrating questions about cyber security that are intended to guide the application of existing safety-related acquisition criteria.

Earlier in this paper, we identified longer-term objectives for research in this area. Many of these relate to the tensions between safety and security. In particular, we have argued that there is an urgent need for techniques that can be used to speed up the validation and verification of firmware patches in safety-related applications. Without this, many ICS components will retain known security vulnerabilities because we cannot demonstrate that these updates will preserve safety requirements. We have also identified specific concerns about conventional security techniques, including the insertion of non-deterministic delays to frustrate timing attacks on cryptographic algorithms. Further work should consider means of bounding these delays across complex systems so that the cumulative effect of these mechanisms does not undermine system safety.

In the meantime, we have the pragmatic aim of defending existing legacy infrastructures. To better under-

[2] The recent attacks on Ukrainian infrastructures are presented in a companion paper for ISSC 2017 — C.W. Johnson, M. Evangelopoulou and T. Pavlova, "Applying Lessons from Cyber Attacks on Ukrainian Infrastructures to Secure the Gateways onto the Industrial Internet of Things."

stand the threat, we have described the effects of uploading compromised malware onto a PLC and also onto a security camera used to preserve the physical security of ICS applications. We also described the design and high-level implementation of a tool that can detect firmware modifications. Ideally, this should be capable of reverse engineering the code running on a suspect device. However, this raises many of the intellectual property barriers and manufacturer differences that complicate ICS forensics. In contrast, our tool integrates a broad range of hashing tools that can be used across the software supply chain to authenticate any code that is transferred onto particular components. The tool has been developed in close cooperation with field engineers. We claim that, although firmware verification is far from the perfect defense, it helps to increase confidence in the integrity of safety-critical infrastructures at a time when a growing array of state-sponsored cyber threats pose an existential threat to the systems on which we all depend.

About the Authors

Chris Johnson is Professor and Head of Computing Science at the University of Glasgow in Scotland. He leads a research group devoted to improving the cyber security of safety-critical systems. He has developed forensic guidance on behalf of the UK civil nuclear industry and helped develop European policy for the cyber-security of aviation — including ground-based and airborne systems.

Maria Evangelopoulou is a Research Assistant working on a joint FAA/US Navy project in Glasgow University, looking at safety and security analysis of network data. She attained her MSc in Intelligence and Security Informatics from the University of Abertay and a BSc in Technology Management from University of Macedonia in Greece. Maria's current research is concerned with the investigation of Cyber Situation Awareness Methods and Techniques in Cloud Networks and other kinds of systems. ⬣

References

1. Johnson, C.W. "Securing the Participation of Safety-Critical SCADA Systems in the Industrial Internet of Things. In C. Sandon," R. Piggin, M. St. John Green, Paul Casely and Chris Johnson (eds.), *Proceedings of the 11th International Conference on System Safety and Cyber Security*, The IET, Savoy Place, London, U.K. October 11-13, 2016.
2. Zhang, L. *An Implementation of SCADA Network Security Testbed*, arXiv preprint arXiv:1701.05323, 2017.
3. Loukas, G. *Cyber-Physical Attacks: A Growing Invisible Threat,* Chapter 5, pp165-166. Butterworth Heinemann/ Elsevier, Waltham, Massachusetts, 2015.
4. Basnight, Z.H. *Firmware Counterfeiting and Modification Attacks on Programmable Logic Controllers*. Master's thesis, Graduate School of Engineering and Management Air Force Institute of Technology Air University, Wright Patterson Air Force Base, Ohio, 2013. Retrieved from: http://www.dtic.mil/cgi- bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA583401.
5. Schuett, C., J. Butts, and S. Dunlap. "An Evaluation of Modification Attacks on Programmable Logic Controllers," *International Journal of Critical Infrastructure Protection*, 7(1):61-68, 2014.
6. Costin, A., J. Zaddach, A. Francillon, D. Balzarotti, and S. Antipolis. "A Large-Scale Analysis of The Security of Embedded Firmwares," *Proceedings of the 23rd USENIX Security Symposium*, pp 95-110, August 20–22, 2014, San Diego, California.
7. Zhu, R., Y.-A. Tan, Q. Zhang, Y. Li, and J. Zheng. "Determining Image Base of Firmware for ARM Devices by Matching Literal Pools," *Digital Investigation*, 16:19-28, 2016. Retrieved from: https://doi.org/10.1016/j.diin.2016.01.002
8. McMinn, L.R. *External Verification of SCADA System Embedded Controller Firmware*, Master's thesis, Graduate School of Engineering and Management Air Force Institute of Technology Air University, Wright Patterson Air Force Base, Ohio, 2012. Retrieved from: https://www.hsdl.org/?view&did=756306.
9. Xiao, M., Y.-Q. Li, S.-h. Chen, and J.-S. Su. "Security Enhancement on Firmware for the Internet of Things," *DEStech Transactions on Computer Science and Engineering* (WCNE), 2016. Retrieved from: http://dpi-proceedings.com/index.php/dtcse/article/view/5146
10. Gauravaram, P. and L. R. Knudsen. "Cryptographic Hash Functions," *Handbook of Information and Communication Security*, Springer Verlag, Heidelberg, Germany, pp 59-79, 2010.
11. DeSpautz, J., K.S. Kovacs, G. Werling. "GAMP Standards for Validation Of Automated Systems," *Pharmaceutical Processing*, March 11, 2008. Retrieved from: http://www.pharmpro.com/article/2008/03/gamp-standards-validation-automated-systems.
12. Johnson, C.W., R. Harkness, and M. Evangelopoulou. "Forensic Attacks Analysis and the Cyber Security of Safety-Critical Industrial Control Systems," *Proceedings of the 34th International System Safety Conference*, Orlando, FL August 8-12, 2016, International System Safety Society, Unionville, Virginia.