Crytica Security
Protecting the IoT & OT Environments - Part I

"To Go Where No Probe Has Gone Before"

Version As of: 2024-07-28

Crytica Security
7655 Town Square Way
Suite 212
Reno, NV 89523
Website: CryticaSecurity.com
Email: info@cryticasecurity.com

Crytica Security
Protecting the IoT & OT Environments
Part I

Contents

1. THE CHALLENGE OF PROTECTING IoT AND OT ENVIRONMENTS 1

2. THE CYBERSECURITY INDUSTRY'S RESPONSE TO THE CHALLENGE 1

3. A BETTER WAY – MEETING THE CHALLENGE 2

4. HOW CRYTICA'S MALWARE DETECTION WORKS 3

CRYTICA'S MALWARE DETECTION ALGORITHM 3

HOW IT OPERATES 4

The Crytica Probe 4

The Crytica Detector 4

The Crytica Heartbeat – Patented Resiliency to Attack and Compromis 4

5. HOW CRYTICA CAN PROTECT IoT/OT DEVICES THAT OTHERS CANNOT 5

6. CONCLUSION 5

1. THE CHALLENGE OF PROTECTING IoT AND OT ENVIRONMENTS

> *IoT [and OT] devices were not built with security in mind. The ongoing proliferation and diversity of IoT [and OT] devices and communications channels increases the potential for … [an] organization to be exposed to cyber threats.* - Fortinet

The acronyms IoT and OT are defined as:

- **IoT** The **Internet of things** (IoT) describes devices with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks. The Internet of things encompasses electronics, communication, and computer science engineering. "Internet of things" has been considered a misnomer because devices do not need to be connected to the public internet; they only need to be connected to a network and be individually addressable.[1]
- **OT** **Operational technology** (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events. The term has become established to demonstrate the technological and functional differences between traditional information technology (IT) systems and industrial control systems environment, the so-called "IT in the non-carpeted areas".[2]

Gartner has very succinctly stated the challenge of protecting both IoT and OT environments:

> *The amount of information being transmitted from things continues to rise. Much of this data originates outside of the enterprise. The scale of security risks in the Internet of Things (IoT) era is therefore much greater than in the pre-IoT environment, and the 'attack surface' is much larger. Most sensor-based things have minimal computing resources, and the opportunities for antivirus, encryption and other forms of protection within things are more restricted.*[3]

2. THE CYBERSECURITY INDUSTRY'S RESPONSE TO THE CHALLENGE

The cybersecurity industry is experiencing a growing awareness that the vast infrastructure of IoT and OT environments constitute a "soft underbelly", an enormous and vulnerably exposed essential facet of cyberspace. Many recent media headlines are alerting the world to this danger. For example: "EPA warns. Hackers from Russia, China, Iran are targeting water supplies" [Christian Science Monitor, May 21st, 2024].

[1] https://en.wikipedia.org/wiki/Internet_of_things
[2] https://en.wikipedia.org/wiki/Operational_technology
[3] https://www.gartner.com/reviews/market/iot-security

However, abiding by this warning is far from easy. As the respected cybersecurity vendor Fortinet pointed out: "Unfortunately, there is no way to install security software on most IoT devices."[4]

That is a severely limiting premise, and yet it is the one that the cybersecurity industry has whole-heartedly accepted in addressing the challenges of protecting the IoT and OT environments. From the very outset, the industry has been working from the assumption that, because IoT and OT devices tend to be small, with limited computing resources and limited available memory, it is impossible to run malware detection software inside of these devices. It has therefore been concluded that malware detection must be indirect rather direct. This means that to detect a malware infection in an IoT or OT device, instead of having an agent or probe operating inside a device and directly detecting the presence of malware, as is done with servers, desktops, and laptop computers, the mainstream cybersecurity industry relies upon indirect observation of the external operational behavior of a device, or, at best, periodically querying a device to determine whether or not it has been infected.

The weaknesses and shortcomings of this indirect approach are obvious. They include the clear and present dangers of malware that is designed to:

- Mimic normal external behavior (e.g. communications) in such a way that external sensors cannot detect an attack. From the outside, the device appears to be operating normally.
- Report "everything is normal" when queried by the cybersecurity systems, even when everything is not normal. Self-reporting is an easily compromised defense mechanism.

There is simply no way that external monitoring can be as effect as having an actual presence inside of a device. There is simply no way that external monitoring can consistently and viably detect sophisticated malware infections inside of a device. And yet, the cybersecurity establishment sees no alternative. The conundrum seems to have no solution. One cannot put malware detection software into an IoT/OT device if the software is too large to fit into the device and/or it is too resource intense to operate without negatively impacting the device's performance.

3. A BETTER WAY – MEETING THE CHALLENGE

It is often the case that seemingly insoluble problems can be solved if one revisits the initial basic assumptions. That is certainly the case here. The initial assumption that malware detection software is too large and/or too resource consuming to operate inside of IoT/OT devices is not true. Crytica Security has created a malware detection probe, written in compact C code, that is both small enough and resource efficient enough to fit into most IoT/OT devices and run inside those devices without negatively impacting the devices' performance. The Crytica's "Probe", with only a 70 KB footprint in Linux, is so efficient that it can run essentially continuously in almost any IoT/OT device for which a C compiler exists.

[4] https://www.fortinet.com/resources/cyberglossary/iot-security

The Crytica probe is a probe that can go where no cybersecurity probe or agent has gone before.

4. HOW CRYTICA'S MALWARE DETECTION WORKS

Crytica's Malware Detection Algorithm

As part of its efficient and non-rearward based design strategy, Crytica's malware detection algorithm eschews large virus signature databases. It does not rely upon previously observed malicious behavior. Indeed, it does not look at all to the recorded history of malware. Instead, it is based upon the very basic understanding that any computing device is "merely" a machine, one capable of executing a set of instructions. Many such instruction sets may reside concurrently in a device. Those instruction sets may be very complex and intricate, but they are finite and specifically defined.

Every computing device contains within it a collection of these "authorized" instructions, those that are intended to be there and authorized to be there. When understood in the context of the existence of authorized instruction sets, malware can be defined as essentially any unauthorized change to the authorized instruction sets. It might consist in added instructions, modified instructions, deleted instructions, and/or modifications to the essential metadata associated with the instructions, e.g., changes to permissions, owners, et cetera. But in all cases, malware is essentially an unauthorized alteration to a device's authorized sets of instructions.

Crytica's malware detection algorithm, therefore, consists in identifying all unauthorized changes to a device's authorized instruction sets. As such, it is both binary and deterministic:

1. Either a change to the authorized instruction sets has taken place or it has not.
2. If a change has taken place, then the change is either an authorized change or is it not.
3. If the change is not authorized, the change must be reported, that is, an "alert" must be issued.

Although it is true that not all such unauthorized changes are malware, all such changes must precipitate an alert. Consider the possible causes of an unauthorized change. These include:

- A malware attack – Malware has been injected into the device. This definitely requires an immediate alert.
- A rogue user – An unauthorized user has made changes to a device's instruction set or an authorized user has not followed the appropriate change/update protocols. This definitely requires an immediate alert.
- A software glitch/bug – The patch management or system update software is not operating as it should. This definitely requires an immediate alert.

Proper computer hygiene requires that all of these anomalies be noted and addressed. Crytica's algorithm detects all of these anomalies, so that the appropriate response(s) may be initiated.

Note: Because Crytica's algorithm is binary and deterministic, it does not suffer from the plague of "false positives" that today consumes so many cybersecurity resources.

How it Operates

As part of its unique and patented resiliency to attacks and compromises, Crytica utilizes a distributed intelligence architecture. The three types of components that are most relevant to the IoT/OT environment and to Crytica's patented resiliency to attack are:

1. The Crytica Probe – a small, application-layer, process that continuously scans each protected device.
2. The Crytica Detector – an "appliance" type device, one that can be physical and/or virtual. The Detector receives "scans" from its associated Probes and interprets those scans.
3. The Crytica "Heartbeat" – a communications-based self-check to ensure that all of Crytica's components are functioning as they should.

The Crytica Probe

One of the reasons that the Crytica's probe is so small and efficient is that it does a conceptually very simple task. Written in highly compact and efficient C code (with a footprint of around 70 KB in Linux environments) it continuously scans its host device for instruction sets. When it finds one, e.g., a computer program, it hashes the contents of the instruction set and its associated metadata. After cycling through the entire device, it sends its "scan" off to its parent Crytica Detector and begins its next scan cycle.

The Crytica Detector

Each Crytica detector can manage many Crytica probes. As each probe finishes its scan, it sends the results to the detector, and then begins its next scan. The detector matches each successive scan to the previous scan. If there is an anomaly, e.g., if instructions have been added, deleted, or modified, the detector issues an alert. When an authorized update is made, the detector, typically via an API (Application Programming Interface) is notified and is thus able to distinguish between authorized and unauthorized changes.

When a detector senses an alert condition, it can notify (also typically via an API) the appropriate cybersecurity stack (e.g., an MDR system) to immediately begin response and remediation activities.

The Crytica Heartbeat – Patented Resiliency to Attack and Compromise

All of Crytica's components are connected via a communications "heartbeat", a series of customizable, messages that travel between the other Crytica components. Via this heartbeat, each component, in a mutually monitoring mesh of components, can monitor the health (and even the existence) of its associated components. When an anomaly is detected, that is, whenever a component is determined to be not functioning as it should. That component can be "killed", discarded and replaced with a new one. Crytica's

components are designed to be disposable, replaceable piece parts, all interconnected by a health-checking heartbeat.

5. HOW CRYTICA CAN PROTECT IoT/OT DEVICES THAT OTHERS CANNOT

Crytica can protect IoT/OT devices more effectively in ways that others cannot:

1. Crytica's Probes are able to fit into and run non-disruptively in small IoT/OT devices; devices that others cannot fit into. That is direct rather than indirect monitoring.
2. Crytica's Malware Detection Algorithm detects malware that is invisible to others. It can detect even the newest, previously undocumented, unseen, malware because it does not rely upon previously documented malware in order to detect a malware injection. Critically, it detects the malware at the time of injection! It does not need to wait for the malware to launch and exhibit malicious behavior in order to detect it.
3. Crytica's Components are resilient to attacks and compromise; being discardable, replaceable piece parts, Crytica's system can continue to operate in the face of attacks that would obliterate others.

6. CONCLUSION

In a cybersecurity environment in which the major players have already surrendered IoT/OT devices to the enemy, relegating them to the lesser protections provided by indirect monitoring rather than direct monitoring, Crytica is forging a different path. Crytica is providing even small IoT/OT devices with the more effective defense of direct monitoring (rather than indirect monitoring). It provides the type of defense IoT/OT devices deserve, especially in the face of the growing threats against them. And Crytica does so using inexpensive and uniquely resilient technology.