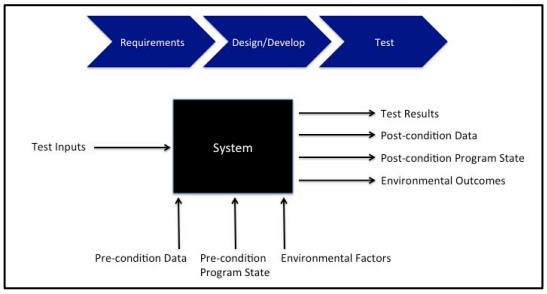
When IoT Attacks

Billy Rios
Jonathan Butts, PhD

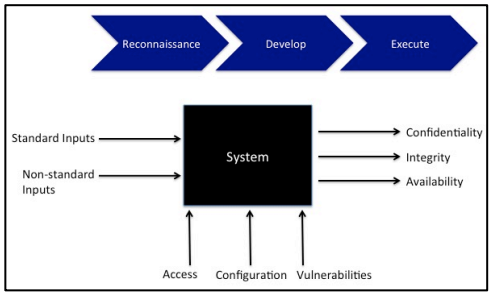
Introduction

The Internet of Things (IoT) manifest as embedded devices interconnected to facilitate information and data exchange. Our primary focus is the class of IoT devices that are associated with cyber physical systems, which integrate software for mechanical system functionality. This area is of particular interest because of the potential safety concerns and ability to achieve physical damage if operating parameters are altered. Indeed, public safety has become reliant on the proper operation of cyber physical systems, ranging from functions associated with medical, power, transportation, and other critical processes to everyday consumer products such as washing machines, door locks and kitchen appliances.

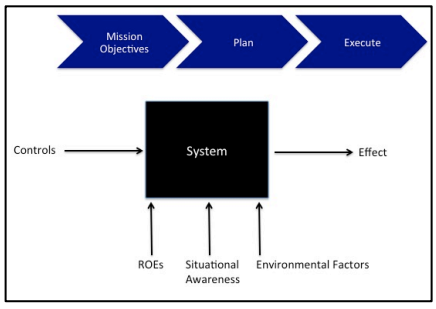
We have performed countless assessments on cyber physical systems, to include civil and military aircraft systems, locomotives, UAVs, medical devices, industrial control systems, building automation systems, and automobiles. Throughout our efforts, we began to notice an interesting trend. Discussions of our findings with the various organizations we worked with centered primarily on the notion of disconnect between the engineers, the cyber security experts and the system operators. Engineers tend to focus on system specifications and develop test inputs to evaluate if the system functions within the design parameters. Cyber security experts often develop test cases using standard and non-standard inputs to the system while evaluating the ability to affect the confidentiality, integrity and/or availability of the system and data. Operators tend to focus on the end state of does the system perform as expected, when expected.



Engineer Perspective



Cyber Perspective



Operator Perspective

The reality, however, of complex systems is that:

Design ≠ Implementation ≠ Reality.

As we started to examine the core issues that ultimately manifest in the exploitation of cyber physical systems, we identified one basic principle: cyber physical systems are inherently vulnerable because software is used as a replacement for mechanical functions. On the surface, this statement appears elementary. In reality, however, this core principle is not a consideration in the design and implementation of cyber physical systems – our hundreds of assessments (involving systems ranging from historical legacy systems to modern-day cutting edge technology) demonstrates the lack of awareness of this fundamental notion and its implications on the overall system safety.

Fundamental Security Principle of Cyber Physical Systems

As a result of our efforts, we introduce the following fundamental principle concerning the security and safety of cyber physical systems.

The Security Law of Cyber Physical Systems:

The mechanical functions of a cyber physical system are bounded only by the physical limits of the hardware components.

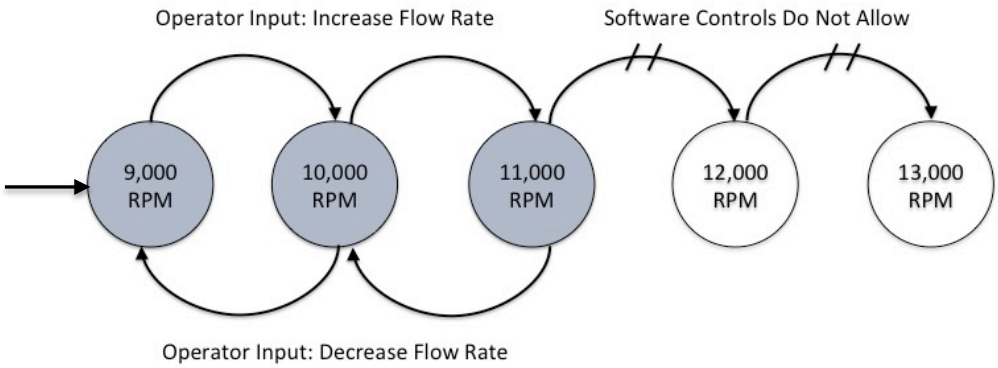
Implication of The Security Law of Cyber Physical Systems:

Software that controls mechanical functionality can be can be manipulated to create any effect possible within range of the hardware components' physical capabilities.

The law defines the fundamental cyber security principle associated with cyber physical systems. Any system functionality that is implemented or controlled strictly by software can be manipulated to a setting within the mechanical range of operations. As an example, consider a compressor designed with a speed range from 9,000 RPM to 13,000 RPM. When installed at a natural gas compressor station, software controls are implemented to limit set points of the compressor from exceeding 11,000 RPM to prevent excessive pressure build up in the pipeline. Relying strictly on software controls to enforce the operational requirements, however, exposes the system to a malicious attack that could have direct safety consequences. As a result, an exploit of system software would allow manipulation of the compressor settings to 13,000 RPM. Without any mechanical/physical restrictions, the resulting action could increase the pressure to limits beyond safe operating parameters and result in a ruptured pipeline.

The state diagram below identifies the operating behavior for the compressor (abstracted to multiples of 1,000 RPM). The shaded states identify the different possible operating states that are enforced through software. The remaining states are often not considered within the operating behavior for safety implications because it is assumed the system cannot reach those states. This assumption, however, is false. For design and implementation considerations, this means that

any reachable mechanical state must adhere to applicable safety considerations. In the previous example, if the compressor was physically wired to not exceed 10,000 RPMs, the state of operations for 13,000 RPM is not mechanically reachable, and manipulation of software cannot result in that specific unsafe state. This highlights the notion of *intended design vs. system implementation.*



Intended design relates to the engineer's perspective that the system will only operate within the defined parameters. System implementation, however, does not adhere to the strict intended design. The gap extends from the implementation of software for system controls and safety mechanisms. Software is programmed in languages that are not provably secure. Additionally, it is intractable to examine the range of inputs, system calls and system-to-system interactions in a complex system.

Demonstration

The fundamental cyber security principle is applicable to cyber physical systems that integrate software to achieve a mechanical function. The action of using software to implement mechanical controls has some serious consequences concerning safety.

To fully demonstrate the security principle, we performed an assessment of an automated car wash in the context of the law. When considering the various systems to evaluate, we selected one that had the ability to create direct physical harm and would be familiar to a significant number of people.

Exploit details on the car wash will be added prior to presentation.

Cyber Security Perspective

Current processes for evaluating a vulnerability focus on the impact to system confidentiality, integrity and availability. Although sufficient for evaluating traditional information technology systems, this process fails to consider safety ramifications for cyber physical systems. Consider, for example, medical devices. The current scoring system advocated for by US Government Organizations is the Common Vulnerability Scoring System (CVSS). The CVSS evaluates the severity of

an identified vulnerability in the context of system impact. It does not, however, take into consideration the impact to patient safety—the true indicator of the severity of the vulnerability.

The ICS-CERT Advisory ICSA-14-288-01 identifies a hard-coded password vulnerability in the CareFusion Pyxis SupplyStation. The Pyxis SupplyStations are automated cabinets used for dispensing medical supplies. The hard-coded password vulnerability was assigned a CVSS base score of 9.7. In comparison, the ICS-CERT Advisory ICSA-15-174-01 identifies a vulnerability in the Hospira Symbiq Infusion System that delivers medication to patients. The Symbiq Infusion System vulnerability was assigned a CVSS base score of 7.1. From a comparative standpoint, the CareFusion vulnerability allowed an attacker with local access to compromise the automated supply cabinet, to include removing the contents of the automated supply cabinet. The Hospira vulnerability allowed an attacker to remotely control the infusion system and perform unanticipated operations. Although the Hospira vulnerability had direct impact to patient safety via remote access, the CVSS score was less than the CareFusion vulnerability that requires local access and does not directly impact patient safety.

In consideration of the potential impact a software vulnerability in a cyber physical system may have on safety, we have extended the CVSS for medical devices to incorporate two primary factors: (i) Impact Category and (ii) Exploit Chain. The Impact Category has five different levels: Direct Therapy; Indirect Therapy; Direct Diagnosis; Indirect Diagnosis; and Supporting System. The categories enforce a rating such that a vulnerability in a support system cannot be more critical than a vulnerability in a device directly controlling the physical process. The Exploit Chain identifies the reachability of the vulnerability and is identified as Controlled or Uncontrolled. The Controlled chain identifies the scenario when the effect of exploitation the vulnerability is dependent on other system compromises in the exploit chain. The Uncontrolled chain identifies the scenario when the effect is not dependent on the compromise of other system or component exploits.

Predictions Based on the Law

Although research will focus on more secure implementations of software controls and provably secure software, the intractability of the problem for complex cyber physical systems will prevent system implementations from adhering to intended functionality.

If software controls are the only means of enforcing safety mechanisms, the system will be exploited.

The exploitation of a cyber physical system that relies on software controls for implementing mechanical safety will (rather unfortunately) result in dismemberment or the loss of life.

About the Authors

Billy Rios

Billy is the founder of WhiteScope and is an accomplished author and speaker. Billy is recognized as one of the world's most respected experts on emerging threats related to Industrial Control Systems, Critical Infrastructure and medical devices. He has been publically credited by the Department of Homeland Security (DHS) over 50 times for his support to the DHS ICS Cyber Emergency Response Team (ICS-CERT). Billy is a former Technical Lead at Google where he led the front line response for externally reported security issues and incidents. Prior to Google, Billy was the Security Program Manager at Internet Explorer (Microsoft). Billy currently holds an MBA and a Master of Science in Information Systems. He was a contributing author for several publications including: Hacking, the Next Generation (O'Reilly), Inside Cyber Warfare (O'Reilly), and The Virtual Battle Field (IOS Press).

Jonathan Butts, PhD

Dr. Jonathan Butts is the founder of QED Secure Solutions and is the Committee Chair for the IFIP Working Group on Critical Infrastructure Protection. He is a retired Air Force officer and served as research director for the Air Force Center for Cyberspace Research at the Air Force Institute of Technology. He has served as technical director for cyber security efforts supporting Presidential-directed projects and has presented at prestigious security conferences around the world. Jonathan is a respected published author on various topics including critical infrastructure protection, malware analysis, protocol verification and operationalizing military actions in cyberspace. Jonathan has performed research and worked extensively with the Department of Defense, Department of Homeland Security, Department of Energy, National Security Agency, Central Intelligence Agency and U.S. Secret Service.