ENGINEERING LIFE CYCLE ENABLES PENETRATION TESTING AND CYBER OPERATIONS

Paul Cheney[1] and Ian R. McAndrew[2]

[1]Department of Critical Infrastructure Protection, Capitol Technology University, Laurel MD., USA
[2]Capitol Technology University, Laurel MD., USA

ABSTRACT

This paper discusses the strengths and weaknesses of proper engineering and life cycle management on higher level cyber security operations. Rushing innovation and increasing profits undermines the foundations need to operate and create secure stability in IT based companies. This research argues how it must be considered and how effective engineering processes greatly add to security even post implementation.

KEYWORDS

Risk Management, Cyber Operations, Penetration Testing, NIST.

1. INTRODUCTION

The current environment of computer engineering and networking, along with Cyber Operations, is in a state of decay that will lead to systemic failure if not corrected. Modern Cyber Operation centers fail to properly manage risks: improper foundations, focusing on the more glamorous tasks such as Incident Response and Cyber Intelligence, and Penetration Testing. These are reflexive and reactive reactions, which serve to put a Band-Aid on the problem rather than attack the root cause of issues such as lack of planning, personnel issues, and focus on the lifecycle of operations. Maintenance, too, is often overlooked in favor of cheaper, easier solutions. The human factor cannot be overestimated. The best preparation and solid design and forethought can be undone quickly with untrained, ignorant, or even malicious intervention by people with access to the underpinnings of the system. Additionally, education can be used by attackers to circumvent defenses in the same way education can be used by defenders to plan and implement systems correctly.

2. TECHNICAL

Correctly implementing Critical Infrastructure is a complex problem. Once the system is built and operating, that system is the only one of its implementations in the world. Changes cannot be made easily, leading to a soft-center security issue. In order to update and maintain security of these systems, observance of their behavior can be safely monitored; included in this behavior are changes congruent with new attacks as well changes after patching or configuration alterations. These changes to the system should stand out and can be actioned against. Rarely, as changes are made to the system, this older behavioral data can be used to analyze and compare performance and ensure reliability of the system as well as security.

DOI: 10.5121/ijmit.2021.13403

Behavioral monitoring and integrity checking can be used to mitigate many of these issues. This would require additional hardware and personnel. Passive monitoring is used in the commercial world and it should apply to OT systems as well. However, this model has given way to a series of patches and jury rigging in order to keep systems operational since many of these systems such as electrical grids, water systems, etc. cannot be down for any length of time without a great deal of hardship and upheaval. This is evidenced by the recent problems with the Colonial gas pipeline and the Texas power grid. Ultimately, we will reach the point of no return with many of these antiquated systems with numerous dire and wretched outcomes resulting.

A number of systems are still using COBOL systems, some of these older systems remaining in place after decades of use. A Google search reveals numerous posts about COBOL still being used. "Today's Business Systems Run on COBOL" states the following:

> Some of the largest business systems that run COBOL include:
> Healthcare: 60 million patients
> Banking: 95% ATM transactions
> Travel: 96% of the bookings
> Social security: 60 million lines of code
> Point of sale: 80% of all transactions daily
> IRS: 50 million lines of code[8]

Paradoxically, although these systems are outdated, there is one strength they possess, namely, monitoring, because there is a long history (potentially) of operation and behavior of the system. While these systems may lack modern day connectivity and up to date anti-virus, the simple and more deterministic behavior helps detection more than enough to offset these downsides. Unfortunately, these legacy systems don't have enough skilled personnel to upkeep them.[7]

The broader community need to begin assessing computer systems as a safety critical system. The foundation of critical systems relies on the normal IT structure. While it is novel to categorize OP and IT systems differently, their underpinning are the same. Relying on firewalls is not enough. The same idea is true for so many other scenarios. Storms, floods, computer hacking, electrical outages, and other disasters may not happen often, but can be crippling when they do. Management banking on the small chance of an occurrence at the cost of proper preparedness is truly unfortunate when these disasters do occur.

Automation relies on technologies that are not tested and not understood. Using these technologies to create the foundation of the next tier of infrastructure has unknown risks. However, programming and computers can outpace humans and the need to be trained and have that training maintained. This is a boon for business but introduces unknown risks.

Maintenance of the system includes more than just standing the system up and keeping it patched. SolarWinds was the first of a situation where patching actually increased risks. While this is ironic, in that patching should increase security, the return on investment was too huge for attackers to ignore. Maintenance and operation of the system must include behavioral and atomic information about the system: IP, MAC Address, and Purpose must be in an accessible location to support further work. Without this information, key tasks cannot be done the system cannot be monitored for attacks and pen-testing and security audits cannot occur. This information is critical for recovery from an attack since it is the bounding box for trust of a system.

2.1. IOT Compared to Critical Infrastructure

IOT Devices and OT Systems share similarities. Critical infrastructure systems are often placed and not touched for fear of breaking them, same goes for IOT. IOT devices lack the larger context and monitoring that is possible in larger, more static systems. While IOT devices are cheaper, ubiquitous and capable, they often aren't touched once employed. Android cell phones are a middle ground example where updates could be deployed, but often aren't. Cell Phone manufacturers, particularly in the Android Ecosystem, hold users' security hostage, by saying "update to get the latest security patches", whereas Apple IOS 15, newly released as 10/3/2021 can be used on Apple devices such as the iPhone 6, released in 2014. Putting electronic devices that can be used in malicious ways without long term plans (such as patching or monitoring) is reckless. Weapon systems for the military also fall into this category." Tests Revealed that Most Weapon Systems Under Development Have Major Vulnerabilities, and DOD Likely Does Not Know the Full Extent of the Problems" [5]

3. BUSINESS

Risk management is integral to this issue. The push to get out new products and code developed in order to support the bottom line of an organization has become the standard by which companies operate. Writing code is hard and time consuming, but taking the time and using the discipline to properly debug programs is not emphasized. The faster code is pushed out, the less time there is for review and testing, and the more risk is incurred. The standard response to this risk is to rely on patching and post publication efforts to mitigate risk such as firewalls. This method does not work with the increase in the use of Zero-Days in attacks and the continuance of successful phishing attacks to bypass Firewalls, and obtain execution on endpoints.

Companies take risks to gain money, they don't take 'risks' in securing their systems. One example is having a blacklist of systems that cannot be scanned. Attackers do not know, nor care about these blacklists. If you are able to induce a failure of the system, by simply scanning the system, then the fragility will only ever be taken into account during a real attack and not during any preparation, including scans, assessment or resiliency planning. Engineering and architecture need to be treated as a continuous improvement process, much as The Capability Maturity Model is applied to 'sexy' cyber operations, so too this model should be applied to Engineering and Architecture. While architectures can be difficult to replace in situ, the learning from their execution needs to be fed back into the organization, and the cycle of cycles should be self-reinforcing.

In the rush to increase profits, organizations induce risks both intentionally and unintentionally. New code is buggy and needs extensive testing. Putting new code over bad bones gives a more fragile code that cannot be completely trusted to do what it is supposed to do correctly. This leads to more down time, unhappy customers, and ironically, reduced profits. Innovation is good; but it must be supported by the full and proper use of the System Life Cycle. Increasing the allotted time to test code increases security, but with proper management it will only lead to a small increase in costs. Properly written code being reused increases security. When bugs are found, new versions are pushed and raise the security bar across the organization. Being self-sufficient for code by developing it in house is a primary pillar of modern security because when you rely on third parties for development, this touches on both business processes: how code is developed as well as the management and timeline effects on personnel. Supply chain attacks and dependency confusion attacks easily undermine security.[2]

Large corporations are held to multiple sets of laws. In order to operate in China, you must use specific software. In Russia, government pressure can force even the largest companies to take certain actions. [4]

These actions can be used to undermine security directly, or indirectly by eroding supporting processes, mechanisms and procedures.

As the cost of direct attacks against well-protected organizations increases, attackers prefer to attack their supply chain, which provides the additional motivation of a potentially large-scale and cross-border impact. This migration has resulted in a larger-than-usual number of supply chain attack cases reported, with a forecast of four times more supply chain attacks in 2021 than in 2020[10].

This equivalent of a 'business world' supply chain attack is just as insidious as software supply chains that linger and have long term, innumerable effects.

Additionally, laws limiting the types and implementations of cryptography, have the same effect. The chain is only as strong as the weakest link, and applies especially to cryptography as these laws are well known and allows attackers to easily focus on these weak spots, compromising security of the entire system.

Corporations will often farm out the creation of the system, which will then be stood up and the implementation and design teams dissolved. This is the wrong method for numerous reasons. First, an incident response needs behavioral and atomic information about the system to decide if the system is infected, how badly the system was hacked, and if malicious actions continue to happen. This most elementary information should include the mac address, IP address, hostname, process list and network connections as the system was stood up. Without specific and granular information about the system, security assessments and audits cannot occur. If the system is stood up and forgotten about, if it is living in non-contiguous IP space, it may never be scanned by responsible parties, instead turning into a ripe target for attackers who are not judicious with their packets and port scans.

4. PEOPLE

Management is not blameless for the current state of unpreparedness, fragility and brittleness of our current infrastructure. The ability to plan and adapt has always been a hallmark of managerial success; unfortunately, this has only been words and not taken to heart. Examples of this are not hard to find. One manager actually tried to initiate a backup site for operations, only to be soundly rebuffed by personnel from the other possible locations. When one library's sprinkler system was accidentally triggered and the thousands of books drenched, no one was sure where the cut off for the system was not what to do with the wet books. Commercial recovery teams do exist, but that also has its own set of bureaucratic roadblocks: they are geographically distant, require a contract before responding, will only do what's in the contract and not one single thing more. If a proper disaster preparedness plan was in place, the damage could have been minimized. Deming's 94% figure comes to play here greatly. [9] In order for companies to succeed in securing their systems [1], the management must adapt, which is counter-intuitive to them since that was not the way they got their positions in the first place.

Personnel has its own set of issues. When a person is hired for a position, they are given a cursory interview, their resume scanned for obvious typos, and the person given a superficial vetting. No real delving into what the person actually knows and actually can do. Obviously, the candidate will not reveal their weaknesses, some intend to bluff their way into the job and then do the minimum to get by. Of course, there are actually qualified candidates who want to do the job and improve the workflow and increase productivity, but many are simply out for the money and not to do the job right. Added to this are the employees who are simply out to do the minimum to get by. Unfortunately, some may work their way into critical positions. This laziness has infected many people; it has been said that the younger generation simply has their own way of doing things, but many do not seem to be willing to put out much effort and very few have the drive and ambition to improve things.

Training is another area that needs attention. So many jobs require on the job training, such as operators of wastewater treatment plants, electrical grids, etc. Poor training is a downhill slope, since a person cannot train what he/she does not know. The small but important details tend to get lost when the generations of operators turn over, and little by little the quality of the oversight and work slips. Those people who do take the time to properly train and equip the new operators are to be lauded. During the problems with the electrical grid in Texas, it was only through the quick action of the controllers that the system was saved from a total disaster. The question is, what if they were not trained so well? Disaster situations always have post mortems to determine what went wrong, but they would be well advised to put the effort in before the disaster hits to possibly curtail or mitigate the damage when disaster does strike.

'Another area of concern is how much of a factor is automation going to be for the workforce of DOD. The Army's approach in Serbu's article takes a modernization approach in re-architecting their network for the future,'(Serbu, 2019). As Serbu stated, 'the Army would instead rely upon an RFI (Request For Information) for vendors to restructure their IT infrastructure in a quicker way that speeds up their modernization efforts (Serbu, 2019).' In International Journal of Managing Information Technology (IJMIT) Vol.12, No.3, August 2020 7 outsourcing their efforts to quickly adopt their modernization efforts, the effects on the workforce could be a major concern for IT workers looking to maintain and update their skills. New technology forces workers to adopt a new approach in keeping up with the ever growing changes in the IT field. [3]

5. CONCLUSIONS

In conclusion, the current frangible state of networks and computer systems is a crisis that must be addressed quickly in order to avert wholesale catastrophe. There are multiple reasons for this, but as long as there are restrictions on what security personnel can scan, the attacker, once he/she is in a network, will always know more about the network than the network operators. Management directed or 'inherent' network blacklisted IP addresses in a network gives blind spots or shadows where information about the defense of the network is lost. This precludes effective Penetration Testing, Vulnerability Management, Incident Response and Incident Recovery. Having a blacklist in a network is a finding that the architecture is not sufficient. Proper engineering is not just something that is done when the system is stood up. Architecture and Behavioral Diagnostics of these systems must be used to enable effective Cyber Operations in order to enable effective Cyber Defense as a continual process. "In today's under regulated markets, it's just too easy for software companies like SolarWinds to save money by skimping on security and to hope for the best. That's a rational decision in today's free-market world, and the only way to change that is to change the economic incentives."[6]

ACKNOWLEDGEMENTS

The authors would like to family and friends and the larger security and engineering communities.

REFERENCES

[1] "Deming.pdf." Accessed: Sep. 26, 2021. [Online]. Available: https://www.stat.auckland.ac.nz/~mullins/quality/Deming.pdf

[2] A. Birsan, "Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies," Medium, Feb. 09, 2021. https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610 (accessed Sep. 27, 2021).

[3] C. L. Gorham, "Developing Enterprise Cyber Situational Awareness," IJMIT, vol. 12, no. 3, pp. 1–8, Aug. 2020, doi: 10.5121/ijmit.2020.12301.

[4] Reuters, "Google, Apple remove Navalny app from stores as Russian elections begin," Reuters, Sep. 17, 2021. Accessed: Sep. 28, 2021. [Online]. Available: https://www.reuters.com/world/europe/google-apple-remove-navalny-app-stores-russian-elections-begin-2021-09-17/

[5] "WEAPON SYSTEMS CYBERSECURITY DOD Just Beginning to Grapple with Scale of Vulnerabilities," United States Government Accountability Office, GAO-19-128.

[6] "National Security Risks of Late-Stage Capitalism - Schneier on Security." https://www.schneier.com/blog/archives/2021/03/national-security-risks-of-late-stage-capitalism.html (accessed Sep. 26, 2021).

[7] "The IBM i And Its RPG Decade Of Crisis," IT Jungle, Sep. 29, 2021. https://www.itjungle.com/2021/09/29/the-ibm-i-and-its-rpg-decade-of-crisis/ (accessed Sep. 30, 2021).

[8] "Today's Business Systems Run on COBOL." https://techchannel.com/Enterprise/03/2021/business-systems-cobol (accessed Sep. 30, 2021).

[9] D. Andrew, "Who's to Blame? 94% Chance It's a System Failure, Not You," Mission.org, Apr. 18, 2018. https://medium.com/the-mission/whos-to-blame-94-chance-it-s-a-system-failure-not-you-26396b2b3811 (accessed Sep. 27, 2021).

[10] European Union Agency for Cybersecurity., *ENISA threat landscape for supply chain attacks.* LU: Publications Office, 2021. Accessed: Oct. 28, 2021. [Online]. Available: https://data.europa.eu/doi/10.2824/168593

AUTHORS

Paul Cheney is a researcher working in the fields of Risk Management, Artificial Intelligence and Critical Infrastructure Security and Operations.

Ian R. McAndrew is the Dean of Doctorate Programs and has been publishing for 30 years. He has been leading the Doctorate programs at Capitol Technology University since 2018 and is a frequent chair or keynote speaker at many international universities.