

Multi-Shield Cyber Security Visualization - an Approach to Enhance Cybersecurity Design and Analysis

Erik L. Moore
Regis University
eriklmoore@gmail.com

Steven P. Fulton
United States Air Force Academy
steven.fulton@afacademy.af.edu

Vincent Garramone
Regis University
vgarramone@gmail.com

Daniel M. Likarish
Regis University
dlikaris@regis.edu

Abstract

Multi-Shield Cybersecurity approach is a method designed to increase attention on an understanding of critical relationships when designing and analyzing cybersecurity infrastructure. It can be used in conjunction with the Zero Trust Reference Architecture (ZTRA) or any other security reference architectures. It provides a way of visualizing security control services at a higher layer of abstraction than traditional network connection diagramming or hierarchical service modeling. It was developed using a classical Eulerian approach, referencing graph theory, to analyze cybersecurity architecture problems by formulating definitions, rules and a topological system for analyzing controls. This is also based on direct observation of cyber defense practices in infrastructures that include industrial control systems (ICS) and operations technologies (OT). The goal of the MSC approach and the Multi-Shield Cybersecurity Visualization (MSCV) is to ensure that all security services are implemented at a higher level of resilience than their individual capabilities. Examples are provided.

Keywords: Multi-Shield, Zero Trust, Cybersecurity, Visualization, Resilience

1. Introduction

Digital Information Assurance and Cyber Security have been focused on the concept of defense-in-depth at least as far back as 1991 when it was popularized as a best practice against computer viruses and hacking

(Cohen, 1991). More recently the reference architecture of the Zero Trust Reference Architecture known as “ZTRA” (DISA 2022), or attempting to remove assumptions of inherent trust from a protected network and treat it as a hostile environment, has gained popularity using the method of increasing confidence only in specifically authorized connections (Stuart, 2019; Bobbert, 2022). We propose a new way of looking at information security using a multi-shield approach that is designed to provide a more intuitive visualization across various reference architectures and provide a new analytical method for designing and assessing information systems security. This work is part of a line of research to develop new visualization methods for cybersecurity (Moore & Likarish; 2010, Moore 2013; Moore, 2016; Moore et. al. 2019)

The research below first describes the methodology, then the initial operational observations that prompted this research, a description of the observed behavior identified as the Multi-Shield Cybersecurity approach, and then the examples of Multi-Shield Cybersecurity Visualization (MSCV) process. Finally, we will contrast our methodology alongside the popular ZTRA, discuss implications and outline plans for future work and challenges in this line of research.

2. Methodology

This work generally follows a design science methodology as defined by Wieringa (2014), focusing on understanding the major components of the critical relationships when designing and analyzing

cybersecurity infrastructure. We start with two primary sets of observation, defining the observed behavior in active operations, and present several scenarios to illustrate the observed techniques in an integrated and systemic approach. In our discussion, we indicate how we intend to move from the initial visualization method presented here to quantitative methods using graph analysis in future works.

3. Initial Operational Observations

Two sets of observations are presented here that represent operational behavior in a broad span of organizational size. The authors have been involved in cyber defense and risk reduction with multiple federal, state, regional, and local government entities over a span of 10 years. This was primarily because the authors worked at Regis University, which had been running cyber defense competitions and made those training resources, including facilities, technology, scenarios and faculty, available to multiple groups looking to harden governmental technology infrastructure.

The first set of observations occurred between 2013 and 2018 during events when multiple US states participated in cyber defense exercises at Regis University involving national guard units, state cybersecurity teams, public infrastructure cybersecurity teams, FEMA, FBI, and local governments. These exercises involved temporary infrastructures protected by “blue” defense teams of cyber professionals defending against “red” teams of penetration test experts. While this was a set of staged events on temporary infrastructure, the participants were seasoned professionals engaged in cyber defense simulations that had long-term operational impact on their cyber defense development programs. The defended systems included simulated Industrial Control Systems (ICS) involving hydroelectric dams, public power generation and distribution, and the operations technologies (OT) as well as devices we could categorize as the Internet of things (IoT) in hospitals, airport infrastructure, and street traffic signaling systems. (Moore et al. 2017)

At Regis, teams were observed jumping on temporarily defense networks and rapidly using cybersecurity control systems like Security Information and Event Management systems (SIEM), Identity and Access Management services (IAM), firewalls, Intrusion Detection Systems (IDS), and other tools to create a mesh of defense so that if any one control was compromised, the team could rapidly respond to the compromise of a cybersecurity control. This appeared

to be an initial step of architectural hardening that occurred prior to engagement with the active threat of the red team.

The second set of observations occurred between 2011 and 2020 when engaged in research regarding the cyber risk and strategies of Adams 12 Five Star School District. Adams 12 is a public school district peaking at about 45,000 students and covering five cities north of Denver, Colorado. The authors observed the district’s infrastructure team working on a district-wide permanent infrastructure of a regional governmental organization providing critical services. This infrastructure serviced digital classrooms technologies, building OT, two datacenters responsible for both business systems and academic records, a 100 square mile regional fiber optic network control systems, and complementary cloud-based services. (Moore et al. 2020).

In Adams 12, we observed the infrastructure team responsible for the enterprise network posturing control systems in a mesh-like configuration to bolster base-line resilience of each control service to increase its efficacy as cross-supported by other control nodes. This was often done as part of architectural design work and a move away from a layered security model in that it was not based on a hardening of nested security zones or a series of controls along a path, but stretch between services in the cloud, on the network, and in distributed remote devices. While the Zero Trust Reference Architecture (DISA, 2022) was involved in the roadmap to compliance, the team achieved day-to-day resilience by having cyber security control systems cross-check each other. After back doors in the cyber security infrastructure were discovered like the Solar Winds incident of 2020-2021 (Alkhadra, 2021), the team realized that a critical skepticism of all control services was required to have a cybersecurity posture that went beyond trusting assurances of protection from cybersecurity tool makers.

The specific characteristics of this shift in both observation sets of analytical behavior and architectural design practice is described in the following sections. What the authors observed generally in both cases was a proactive bolstering of cybersecurity controls by a mesh of mutual defense rather than a strategy based on existing paradigms of analysis or the seminal concept of defense in depth. While both observed teams had been trained in some form of layered security model as seen in Figure 1, the analytical and design behavior was driven by other factors.

What we have observed is not just a new tool or toolset. The Multi-Shield Cybersecurity approach is designed to reflect this different conceptual method that we have observed in cybersecurity architecting and analysis work. This novel approach emphasizes mutual-bolstering of cybersecurity assets, so that each cybersecurity control service is stronger than when they operate when considered independently.

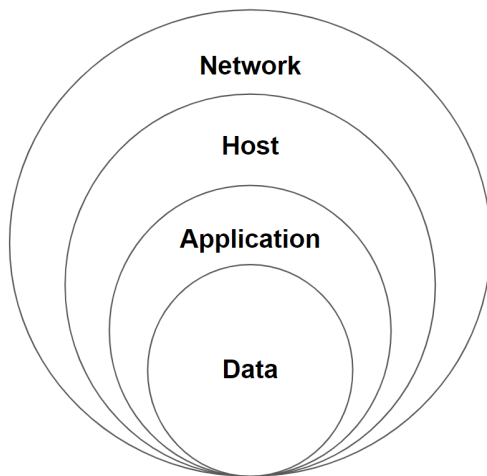


Figure 1. A Simplified Layered Defense Model

4. Defining Multi-Shield Cybersecurity Approach

The Multi-shield cybersecurity approach is a method designed to focus architectural attention on the explicit and active mesh constructed of the active cybersecurity control assets. This is done by analyzing specific shields between security controls that offer mutual assurance of integrity that can be greater than focusing on the security of the individual components of the entire technology infrastructure.

The approach is not to solely create multiple independent barriers against threat as in layered security, but to visualize and measure the protective value of each cybersecurity service as it monitors the effectiveness of the other cybersecurity service and thus actively create failsafe support for those services. The concept of shielding also can represent the reconfiguration of existing technology in a thoughtful deployment to achieve higher defense capabilities. By ensuring that cybersecurity control services are shielded beyond their own functionality, full exposure of vulnerable systems is less likely and time to detect a failure or compromise is reduced during a single cybersecurity control failure.

MSCV is unlike the practice of defense-in-depth (Cohen, 1991) in that it does not emphasize a layered set of control zones. Nor is it like attacking extant graph analysis, uncovering anomalies or simulating likelihood of threat paths (Eberle 2007, 2010). While these methods have demonstrated value, we are not suggesting that defenders use MSCV to either add multiple layers of mitigating redundant measures, or focus on bolster against anticipated attacks discovered through simulated attacks and vulnerabilities. The multi-shield cybersecurity approach is an analytical process observed in active operations codified here to focus attention on a targeted and measured a set of strategic cross-supporting interwoven ‘shields’ strategically placed in the cybersecurity control infrastructure to increase the resilience of security services against adversarial attack along with the assets they protect.

Without identifying a direction of attack, the physical locations, or network-logical location of assets, the multi-shield cybersecurity approach system of analysis has been observed to answer the question “who watches the watchmen” so there is no security service node that stands unshielded as the achilles heel of control. The Multi-Shield Cybersecurity Visualization (MSCV) representation of this “mesh of controls” is illustrated below to allow for systemic analysis along a new dimension, the shield levels protecting the control services themselves, such as those described in the second version of ZTRA as published by the US Department of Defense (DISA 2022). The objective of the MSCV is to provide an intuitive tangible method for analyzing the implications of a control architecture to determine and assess the level of protection offered by various cybersecurity control infrastructure configuration methods. Our expectation is that having more intuitive methods like those described in the multi-shield cybersecurity approach may help increase the adoption rate of complex security models and reference frameworks (Lemos, 2023). Testing this expectation is planned for investigation in future work.

5. Designing a Formal MSCV Approach

In order to move from a set of observed behaviors to a functional system of analysis, this research develops a multishield-centric security visualization method (MSCV) to illustrate a set of relationships based on the analytical processes that Leonhard Euler (Euler, 1953) used as he established the field of topology. Euler’s method moves from physical representations like maps to topologically abstract

graphs through the application of several sub-processes: 1) develop a visualization technique 2) establish rules that present from the diagrams and 3) form descriptive equations that provide actionable analysis for security analysis of the cybersecurity of integrated systems. This first paper in this specific line of research only presents the visualization technique.

In MSCV, arrows visually represent the projection of cybersecurity shielding and not the flow of traffic or an attack vector. Any path through the mesh is a path along individual directed edges of control composed of those individual projections of shielding to specific nodes. This topology allows for an analytic focus on security control relationships like active protection, detection, and prevention of anomalous behavior or traffic in relation to the shielded nodes. Each shield represents a protective engagement of the shielded node, with the expectation of achieving that shielding regarding specific attributes. Another way to represent graphs like this would be through multidimensional matrices. Though such matrices may not be a pragmatic way to visualize designs, it may be useful later for a quantitative approach.

5.1 Definitions

The following definitions are specific to MSCV visualization, but can be applied to a range of technologies, architectures, and frameworks.

- *Node*: any device, service, process, user, or data resource that can receive discrete shielding against inappropriate manipulation, whether a business asset or a control service. It is represented visually by a circle. In terms of graph theory, the Node is a vertex able to receive control services that are represented as directed edges.
- *Control Node*: any device, service provider, process, user, or data resource that can be provided discrete protective shielding from inappropriate manipulation, whether a business asset or a control service, represented by a circle at the vertex of edges.
- *Control Shielding Service*: a service provided by a control node offering assurance of prevention, detection, observation, intervention, and restoration for assets. These are represented by weighted attributes of directed edges. This representation of cybersecurity controls is drawn visually as an arrow from the service pointing to a semicircle surrounding the target node. The target can be either another cybersecurity control service node for “cross-check” or to

an asset node such as an employee data repository that is not a control node. The semi-circle at the end of the arrow represents one layer of many potential shields protecting a single node. (Eberle 2010, p.3).

- *Infrastructure*: a set of technology under review connected by some shared purpose and communications channels.

Like Euler, once a set of topological objects are defined to represent an abstracted set of tangible objects, rules can be derived or applied to the visualization so that inferences can be made leading to actionable intelligence. Our research will proceed to derive rules and then present examples of the visualization techniques based on those.

5.2 Diagramming Rules

Rule 1: All nodes are drawn as a labeled circle and should be shielded by other nodes to increase confidence above the base resilience of a single control node.

Rule 2: No single node should be considered foundational such that it can go without shielding from other nodes, or it is left with only the confidence level of the raw security product.

Rule 3: Control nodes (represented as a circle as in rule 1) project a security control service along a directed edge (arrow) to a shielded node (security control or business asset node). An arrowhead indicates the direction of control service to the shielded node, ending in a semicircle representing the shielding provided.

Rule 4: Multiple control services (arrows) create nested shielding for each node, with shield characteristics represented by their source nodes.

Rule 5: Each node should have shielding proportionate to the risk, security implications, and value of the node. This offers a graphical way to represent resilience beyond the base product providing the control service.

Rule 6: Cloud-based contexts, satellite links, on-premises connections, and device-based business services should be abstracted out, avoiding the use of distracting traditional network connection diagramming in order to focus on the actual control relationships of nodes.

To illustrate the use of these rules, in Figure 2, a SIEM is diagrammed as a product protected at the network core on the left. On the right, we are modeling the MSCV representation with quantitative options. Using rule 1, the SIEM should be actively shielded

with the firewall and the IAMS as seen in MSCV in order to (following rule 2) protect it from its own supply chain threat and emergent zero days within its code, APIs, and underlying operating system/hardware. This can be drawn as a node with (as demonstrates rule 3) arrows of shielding coming from the two other nodes to mitigate these risks. They represent the projection of controls like malware filtering, constraint of traffic to valid external IP addresses, credential confirmation, and internal micro segmentation of its network. Then following rule 4, these controls are represented by layers of shielding that confirm a supportive security architecture. As stated in rule 5, the SIEM's effect is pervasive and because it has high data sensitivity, the analyst can intuitively balance the proportion of shielding and shield characteristics in relation to these risks.

Implementing rule 6: SIEMs use many network paths to retrieve status from servers, industrial control systems, remote site infrastructure, and nested virtualized services. Rather than document all connections, the abstraction level represented in MSCV maintains a clarity of control shielding to make sound security decisions. At this level of abstraction, only security control relationships are drawn, without the underlying connection diagramming, Where the SIEM or IAMS might be traditionally considered a root-level security system, confirming sound implementation of ZTRA, the firewall provides significant shielding to both beyond this assumption of the sound implementation of root devices being sufficient. MSCV's semicircles can also be represented by numerical shield values of different categories.

In Figure 2, The small tables represent an early structure for the labels applied to control shielding received by any node. The headers "T" for type and "V" for value may represent a range of classical security controls like "P" for protective security and "D" for a detective security control. Currently the size and rotation of the shields drawn around the circles are an intuitive representation intended to illustrate a compounding of shielding. It is planned in future versions that the shape, angle and size should relate to characteristics of the shielding.

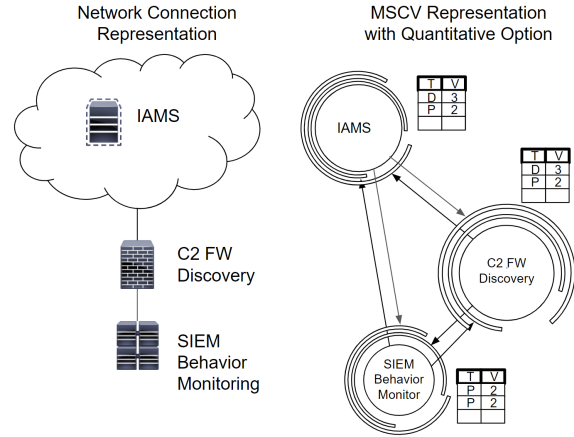


Figure 2. A network Connection diagram compared to MSCV regarding the security relationship of IAMS, firewall, and SEIM security services.

The rules of MSCV define a modeling method that also suggests an architectural strategy. The described use of MSCV in the following sections may emphasize either the modeling method aspect of MSCV or the underlying architectural approach.

Referencing extant work using graph theory for cybersecurity analysis, MSCV can be additionally represented as a graph $G=(V,E)$, where V is a set of vertices representing control services and E is a set of weighted directed edges representing "shielding" applied by the origin to the destination. (Janson et al, 2011) $O(n^2)$ implies that every node is connected to every other node (or close to it). For MSCV, it is useful to note that the number of shielding services intended for control nodes (in the 10's) would generally be relatively small compared to all nodes (in the 100's or 1000's), which will present less of a computational problem on modern hardware. (Gross et al 2013)

6. Comparative Models

In our research, the MSCV is designed to be manually drawn to allow for analysis at the appropriate level of abstraction on the most pertinent characteristics of a security infrastructure. A set of comparisons between traditional network diagramming and the MSCV approach follows.

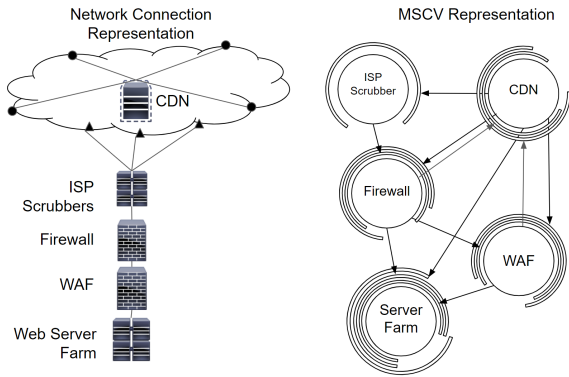


Figure 3. A comparison of connection diagramming and the MSCV in relation to cloud-based content delivery networks and related nodes inside a corporate network behind the firewall.

In Figure 3, the left diagram describes a content delivery network (CDN) topology using the traditional network connection diagramming dialect. Black dots represent the Internet-wide IP-Anywhere entry points of the CDN. Scrubber collectors are represented by the black set of rectangles at the center, and black triangles represent the co-location points of the internet service provider's (ISP) network infrastructure. The organization's ISP-connecting Firewall and the Web Application Firewall (WAF) are both drawn with firewall icons. What network connection analysis like this implies is that devices are conferred protection when they are behind other devices. Contemporary networks rarely work this simplistically. Thus network connection diagramming is misleading, and by leaving it behind we are also dropping clutter.

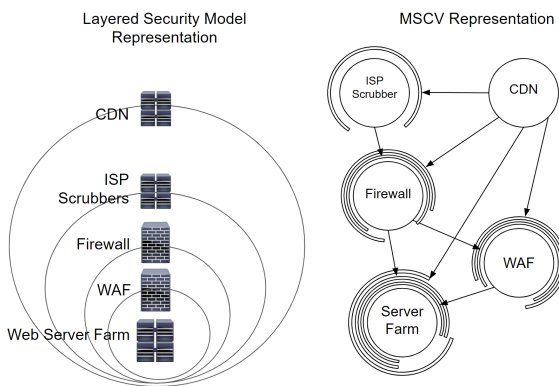


Figure 4. CDN shielding configurations have been applied and projected from the Firewall and WAF to the CDN, visible only in the MSCV representation.

Alternatively, on the right in Figure 3, the MSCV representation explicitly indicates a web of control services regardless of their place in a wiring diagram. We can see that the WAF and Firewall can monitor the efficacy of the CDN even though it is in a forward position. Only in the MSCV version is it graphically indicated by multiple projecting control services that the CDN is clearly of high significance. Functionally, the WAF and the Firewall can monitor the efficacy of the CDN by catching what slips through. In contrast, the connection diagram on the left does not offer any indicators of this type of control relationship which when overlooked would be leaving vulnerabilities unaddressed.

In Figure 4, we show how cybersecurity architecture modeling can be improved compared to layered modeling. The CDN is in the same architectural configuration according to the layered model, offering monitoring protection for the WAF and the firewalls, by initiating redundant sensing of protocol. However, in this example, the WAF and next generation firewall is not configured to monitor the CDN, leaving it exposed. Note that these configuration changes cannot be represented in the Layered Security Model.

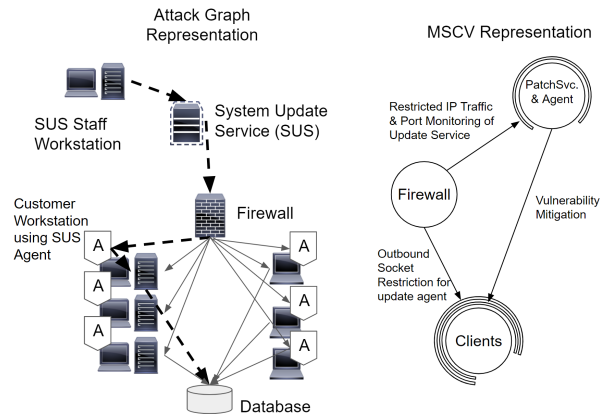


Figure 5. An update agent represented in Network Connection and MSCV.

Likewise, attack graphs have clutter that can distract from the key defensive architectural points emphasized in the MSCV architectural approach. Using this new level of visualization, many previous systemic vulnerabilities can be more easily seen and analyzed based on the control posture represented in MSCV. In Figure 5 on the left side is a classical example of a set of technologies guarding against potential advanced persistent threats (APTs) like the SolarWinds hack (Alkhadra, 2021). The risk to control nodes is not easily represented by attack graphs because it cannot

represent control capability beyond the base security products. Thus in attack graphs it would be difficult to illustrate vulnerabilities or mitigations for the supply chain threat and agent-based security nodes in Figure 5. The System Update Server (SUS) that provides the patching services is represented by the letter “A” in the Attack Graph Representation and is connected through a series of links to the system update agents, deployed on a sampling of machines on a network. In the MSCV representation, the firewall’s configuration as a shield to limit the agent’s outbound traffic of both the patching service and the clients is clear. This makes the security relationship more obvious than the Attack Graph representation. The firewall configuration is the critical control addressing the vulnerabilities of the SolarWinds update product and similar agents. Physical network connections are less significant in the analysis in comparison to control service relationships. This would be true whether it was a supply chain attack, a code injection attack, or a vulnerability discovery of a deployed product. Specifically, shielding provided by the firewall includes limiting the “phone home” capabilities of the clients to only authorized IP addresses, and the update service is only allowed to connect to nodes where its products are installed. If the agents on those clients are corrupted to point to a malicious IP, the firewall blocks the traffic, reducing the risk.

7. The Multi-Shield Cybersecurity Approach in the Context of Zero Trust.

MSCV also allows for a visual analysis of the interdependence defined in the Zero Trust Reference Architecture (DISA p26). Rather than a hierarchical model of controls illustrated in ZTRA (p27), MSCV visualizes security control protection to directly analyze strengths and weaknesses in relation to the baseline protections of individual security services [9].

A more explicit way to mitigate risk and to understand the risk/cost proposition is to realize that any individual security service provider can be compromised, regardless of its place in a zero trust hierarchy or where it sits in a layered model. An example is a web application firewall service feature in a content delivery network, by which the risk of application attack might be considered covered. But unless there is a separate control service implemented by the customer organization to validate the effectiveness of even a commercial CDN, it will be subject to vulnerabilities in the cloud, and the customer may not become aware of a cloud compromise or

degradation for long periods of time. Therefore a strategy using a traditional WAF or Application Program Interface (API) firewall closer to the applications can continuously confirm that the intended capabilities of the WAF are functioning as expected. This may seem like a double expenditure for the same function, but it is actually creating a much more resilient and threat-sensitive model of higher capabilities than either the CDN or the WAF. This notion of an architectural strategy applies broadly when creating types of cybersecurity fortified infrastructures that have higher resilience and assurance than any of their individual nodes. By perceiving these relative control node risks, an organization should be able to deploy attention and resources prior to initial compromise, reduce reliance on a single third party and reduce zero-day infection rate or dwell time generally.

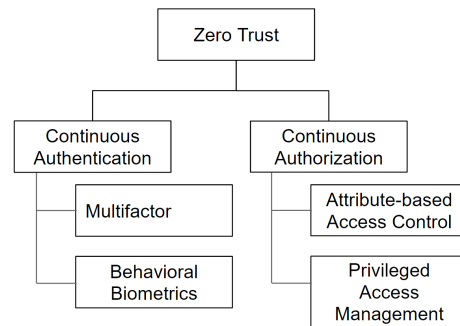


Figure 6. Derived from the DoD Zero trust Reference Architecture Version 2 (Defense Information Systems Agency, 2022, pg 7).

MSCV is designed to be an explicit way of analyzing the implicit functions described in Elgan’s analysis of ZTRA (2023) by moving the focus of attention to a layer of abstraction not traditionally drawn in cybersecurity analysis: *security control shielding*. Additionally, MSCV is designed to facilitate analysis across a broader range of reference architectures and models, making it an extensible tool compatible with multiple approaches. Every asset within the terrain has its own explicit set of shields for fortification that were designed to support a walkable and proactive path towards robustness as organizations work to attain ZTRA adoption in meaningful ways. (Tan, 2023). The continuous awareness of the ZTRA’s implicit interdependencies becomes more systematically exposed in MSCV by explicitly representing the individual shielding in the visualization.

As seen in Figure 6, the ZTRA hierarchical diagrams apparently leave the actual authentication and authorization accountable to the rather abstract authority of Zero Trust itself as an implicit nature of the architecture rather than an explicit deterministic check of specific controls. Beyond this vaguity of ZTRA, analysis with MSCV is designed to prompt designers to apply multiple shields for individual control services, offering a level of fortification that can not be intuitively estimated by zone-based defense analysis either as seen in the defense-in-depth model. MSCV also explicitly delineates lines of resilience along the specific shielding devices and types that each node receives.

Multiple layers of shielding are not intended to offer implicit trust. Even the control services providing shielding are also not necessarily trusted but are intended to be provided with their own shielding from other control services. Shielding provides an increased confidence that a particular node has supporting security services that can detect, prevent, monitor, and compensate for any particular control issue beyond its own initial level of resilience. The goal is to raise a mesh of multi-shielding to higher security capability than the component parts.

In practice, the Multi-shield Cybersecurity approach has been seen to enable the analyst to point to an explicit control service and observe the specific shielding that protects the control service. In later research, the authors intend to automate this process so that the analyst can determine, through prescriptive analytics, the appropriate shielding for each node in the mesh of shielding (the terrain). Visualizing a specific piece of terrain using MSCV is designed to offer security awareness across multiple points of reference, locations within a system, and attack/vulnerability exposures. To calculate cumulative shielding for any particular node on the MSCV diagram as analysis moves to operational scenarios, analysis does then take into account the topological locations of threat actors, adversary strengths and techniques, the fortification type and level of each shield, and the path to the assets that suggests a depth of resilience. The MSCV visualization method helps the analyst make a paradigmatic shift that the tree of exploits is not penetrating a network, but overcoming a set of controls regardless of the geographic or connection environment

8. Implications and Conclusions

While strategic configurations to control services can provide additional shielding with no additional

capital outlay, the MSCV diagramming method may also increase awareness of needed hardware, software, cloud, and other forms of shielding services that may require budgetary allocations.

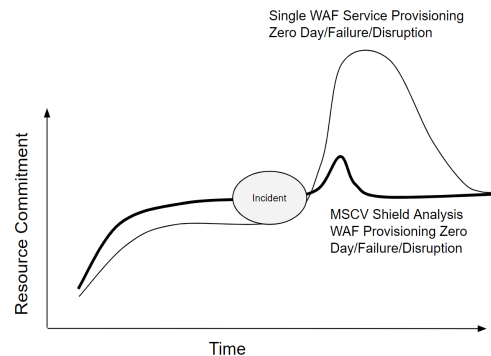


Figure 7: Proposed initial measure for MSCV in relation to risk reduction.

In our initial observations, Figure 7 illustrates examples of how MSCV-style provisioning can slightly increase pre-incident cost, by spurring justifiable gap-filling work, and describes the resultant reduction in incident response costs and other risks associated such as control service failure, degraded services. This was observed even for cloud-based and failover cluster services. Yet this will need to be demonstrated rigorously in future work, and is a situation many control architectures achieve in various ways when successfully implemented.

Regardless of the underlying network styles, the authors observed in practice a differentiation between the traditional resilience of redundant failover and the MSCV Control Service fall-back functions. If a control service fails in an MSCV configuration, it is allied monitoring services in current operations that take over a defense function instead of duplicate standby control services.

As illustrated in figure 4, when a content delivery network service must fail open to maintain web services, our proposed MSCV analysis illustrates immediate shielding relationships. This may facilitate the analysis of confidence in compensating controls using next generation firewalls and WAF. For organizations that enforce separation of duties practices, MSCV may also provide analysis of staff risks by separating the cross-shielding responsibilities of individuals. For instance, the CDN administrator may introduce configuration vulnerabilities that the WAF administrator catches.

As seen in Table 1, traditional redundancy failover has trouble shielding newly discovered vulnerabilities in existing equipment because all elements of a control

service have a common set of vulnerabilities coming from a common supply chain. The MSCV fallback plan utilizes diverse related technologies to more effectively shield against vulnerabilities. Diverse redundancy as described by a traditional defense in depth model (i.e. Cisco and Palo Alto Firewalls in a series to cover the same control set) could benefit from an MSCV style analysis to determine their ability to shield each others' control service ensuring coverage of fail over and the expected shielding of other control services.

Table 1: MSCV fallback functionality versus traditional redundant failovers

Recovery Type	Traditional Redundant Failover	MSCV Fallback Alternative
Functionality	Duplicate Equipment	Diverse Control Services
Ecosystem Risk	Usually a single Supplier	Independent Supply Chain
Strengths / Weakness	Common vulnerabilities and controls across a single control service	Diversity of vulnerabilities and controls across allied services

From a broader perspective, this multi-shield cybersecurity architectural approach has been observed to create a self-reinforcing grid of cybersecurity control services that can be expanded with greater assurance than any of its components.

9. Future Work

Based on this finding presented above, the authors consider that the Multi-Shield Cybersecurity method offers a viable path forward for analysis of the web of critical cybersecurity control services. The continued development of the MSCV model, as also informed by contemporary graph theory, is intended to refine this analytical technique to more effectively bring each control service to a higher state of resilience than it offers as an independent service.

Future work needs to be done to determine if the systemic effect of using this approach can yield a reduction in monetary loss in the event of a single control service compromise, an ability to follow risk of individual control services, and a quantitative basis for claiming an increased capability in assessing relative risk. The authors intend to continue this line of research into a quantitative phase.

After this initial work on control nodes is complete, the approach is expanded to include shielded assets that are not control nodes. One challenge the authors see ahead is that as additional asset nodes are incorporated into the model the number of nodes and

edges corresponding to "fortifications" will increase dramatically. Even though there will still be a small number of origin nodes with directed edges to a much larger number of destination nodes, efficient sorting algorithms and data structure designs will need to be considered to answer various questions that may be asked of an MSCV graph.

10. References

- Alkhadra, R., Abuzaid, J., AlShammari, M., & Mohammad, N. (2021). SolarWinds, Hack: In-Depth Analysis and Countermeasures. IEEE International Conference on Computing, Communication and Networking Technologies.
- Bobbert, Y., & Scheerder, J. (2022). Zero Trust Validation: from Practice to Theory: An empirical research project to improve Zero Trust implementations. 29th Annual Software Technology Conference (STC) (pp. 93-104).
- Cohen, F. (1991, October). Current best practice against computer viruses. In Proceedings. 25th Annual 1991 International Carnahan Conference on Security Technology (pp. 261-270). IEEE.
- DISA (2022), Defense Information Systems Agency., Zero Trust Reference Architecture Version 2.0. DoD.
- Gross, J. L., & Yellen, J., Zhang P. (Eds.). (2013). Handbook of graph theory. Chapman and Hall.
- Eberle, W., Holder, L., (2007) Discovering Structural Anomalies in Graph-Based Data, Seventh IEEE International Conference on Data Mining Workshops, pp. 393-398
- Eberle, W., Graves, J., & Holder, L. (2010). Insider threat detection using a graph-based approach. Journal of Applied Security Research, 6(1), 32-81.
- Elgan, M. (2023, January). Why Zero Trust Works When Everything Else Doesn't, Security Intelligence. <https://securityintelligence.com/articles/why-zero-trust-works/>
- Euler, L. (1953). Leonhard Euser and the Koenigsberg Bridges. Scientific American, 189(1), 66-72.
- Janson, S., Luczak, T., Rucinski, A. (2011). Random Graphs: Wiley.
- Lemos, R. (2023, January). Companies Struggle with Zero Trust as Attackers Adapt to Get Around It, <https://www.darkreading.com/remote-workforce/companies-struggle-zero-trust-attackers-adapt>, last accessed 2/26/2023
- Moore, E. (2013, March). A vulnerability model for a bit-induced reality. In ICIW 2013-The Proceedings of the 8th International Conference on Information Warfare and Security (pp. 169-176).
- Moore, E. (2016, July). Managing the loss of control over cyber identity. In 2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC) (pp. 233-238). IEEE.
- Moore, E., Fulton, S., Likarish, D. (2017). Evaluating a Multi Agency Cyber Security Training Program Using Pre-post

- Event Assessment and Longitudinal Analysis. In: Information Security Education for a Global Digital Society. WISE 2017. IFIP Advances in Information and Communication Technology, vol 503. Springer, Cham.
- Moore, E., & Likarish, D. M. (2010, January). Multi-Method Virtualization: An Architectural Strategy for Service Tuning. In 2010 43rd Hawaii International Conference on System Sciences (pp. 1-10). IEEE.
- Moore, E. L., Fulton, S. P., Mancuso, R. A., Amador, T. K., & Likarish, D. M. (2019). A short-cycle framework approach to integrating psychometric feedback and data analytics to rapid cyber defense. In Information Security Education. Education in Proactive Information Security: 12th IFIP WG 11.8 World Conference, WISE 12, Lisbon, Portugal, June 25–27, 2019, Proceedings 12 (pp. 45-58). Springer International Publishing.
- Moore E., Likarish D., Bastion, B., brooks, m. (2020). An Institutional Risk Reduction Model for Teaching Cybersecurity, the proceedings of the World Conference on Information Security Education, WISE 2020, Advances in Information and Communication Technology, Springer, Cham
- Stuart, H. (2019). Zero trust architecture design principles., United Kingdom National Cyber Security Center <https://www.ncsc.gov.uk/blog-post/zero-trust-architecture-design-principles>.
- Tan, A. (2023, February 26). Zero-trust implementations remain work in progress. <https://www.computerweekly.com/news/252529605/Zero-trust-implementations-remain-work-in-progress>
- Wieringa, R. J. (2014). Design science methodology for information systems and software engineering. Springer.