A Ring-Based Cybersecurity Architecture for Critical Infrastructure

Sarayut Chaisuriy[a], Somnuk Keretho[b], Surasak Sanguanpong[c], and Chaiporn Thoppae[d]

[a]Doctoral Candidate in the Department of Computer Engineering, Faculty of Engineering, Kasetsart University, Bangkok, Thailand.
[b]Assistant Professor in the Department of Computer Engineering, Faculty of Engineering, Kasetsart University, Bangkok, Thailand
[c]Head of Applied Network Research Laboratory, Department of Computer Engineering, Faculty of Engineering, Kasetsart University
[d]Vice President Computer Engineering Committee, The Engineering Institute of Thailand Under H.M. The King's Patronage, Bangkok, Thailand

Abstract: A defense-in-depth (DID) approach for securing critical information infrastructure has been a common method used in cybersecurity. However, holistic design guidelines are lacking which precludes organizations from adopting them. Therefore, this paper sets out to outline and detail a holistic framework using ring-based nested network zone architecture for the design and implementation of highly secured networked environments. The proposed cybersecurity architecture framework offers a structural design for holistically designed N-tier system architectures. Several implementation options, including zoning perimeters, are suggested as being capable of offering different security capability levels by trading off amongst various security aspects. Also, the proposed architecture allows adaptability in implementations for various real-world networks. This paper also proposes an attack-hops verification approach to evaluate the architectural design.

Keywords: Cybersecurity, Holistic Architecture Frameworks, N-Tier System Architectures, Thailand, Zero-Day Attack

1. Introduction

Enterprise-wide information technology systems (ITS) and their related software need secure and resilient capabilities to minimize the effects of a cyberattack to reduce vulnerabilities and maintain resilient continuous mission support infrastructure (Bernstein, 2020; Cybersecurity & Infrastructure Security Agency [CISA] Act, 2018). As examples of the critical nature and vulnerability of global networks were the recent state-sponsored attacks on Solar Winds and Microsoft's Exchange Server customer networks in which by March 2021 the ongoing attack had morphed into a global crisis with over 60,000 networks worldwide having been breached and the user data compromised (Turton & Robertson, 2021).

Furthermore, in the United States, CISA has identified 16 critical national infrastructure sectors, which include health care (e.g. Covid 19), transportation systems (e.g. rail and aviation), power generation and power grids, the ITS sector, food, and agriculture, and communications sector. Furthermore, reliance on ITS is nearly 100% across all sectors in developed nations and quickly approaching this in developing economies such as Thailand. However, security and external threats are of great concern as both private and state actors are constantly shifting through the world's computers, servers, and networks looking for a bounty to loot or damage they can cause.

However, by design, ITS infrastructure is inherently resilient, but its interconnected structure and interdependence present security challenges as well as the necessity for coordinating public and private sector preparedness and protection activities. Therefore the ability of ITS architecture to resist, protect, and react dynamically to cyberattacks and vulnerabilities is critical.

Today, according to Moschovitis (2021), cybersecurity rests on four pillars. These include the newly added component of *safety*, and the older elements of *confidentiality, integrity*, and *availability*. Other threat trends include cybercrime's consumerization, the reduction of barriers to participating by technical novices, the ongoing mystique or the *darknet* (aka *dark web*), and low attribution rates.

In response to these significant security challenges, multiple experts over the years have suggested that one of the best strategies is a doctrine of defense-in-depth (DID) inspired by military strategists and national security apparatus (National Security Agency [NSA], 2010). Moreover, the NSA study describes DID as a balanced focus on the primary elements of people, technology, and operations (Government of Canada, 2007), which when implemented via network segmentation, authentication, and encryption helps mitigate vulnerabilities.

Other guiding principles in DID implementations include the design must factor in critical factors such as the technological architecture, the people, policies, and operations. Also, multiple defense mechanisms should be utilized, with the reliance on a single technology or software provider viewed as a potential security back door.

Also, in addition to the NSA's and Canadian recommendations, the International Organization for Standardization (2012, 2015) has outlined European suggestions for cybersecurity in their ISO/IEC 27033 which details how security should be implemented in the administration and use of ITS networks and interconnectivity security. However, as the European Court of Auditors (2019) pointed out in their cybersecurity report, there is a cybersecurity skills shortfall that has limited EU-wide standards for training, certification, and the assessment of cyber threats. Therefore, the authors offer a proposal for a holistic architectural design framework and related guidelines based on ring-based nested network zoning to offer security and resilience for critical infrastructure.

2. Literature Review

2.1. Generic network zones

Over time, various organizations such as IBM have suggested various network architectures and implementation guidelines to use as a security framework and blueprint (Buecker et al., 2014). Also, these same groups have devised security solution architectures for networks, servers, and endpoints (Buecker et al., 2011), with many using a concept of 'zones' to classify the uncontrolled, controlled, restricted, secured, and external controlled network areas (Figure 1).

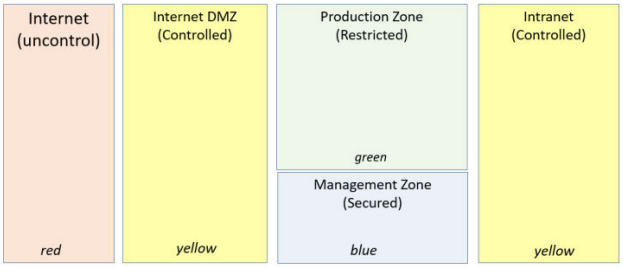

Figure 1.A network security architecture (Buecker et al., 2011)

In Canada, the government published a set of security design recommendations and standards, including a baseline security requirement for network security zones (NSZ) (ITSG-22) (Government of Canada, 2007), an information technology security guideline (ITSG-38), and a guideline for NSZ (Government of Canada, 2009). These Canadian guidelines recommend NSZ's use of routable networks which are connected via a perimeter that contains zone interface points (ZIPs). Moreover, Canada's ITSG-22 specification recommends the use of physical security zones, which use a nested layer defense approach. This Canadian operational security standard is depicted in Figure 2 (Government of Canada, 2013). Previously, Canada's ITSG-22 specification called for the creation of seven NSZs (Government of Canada, 2007).

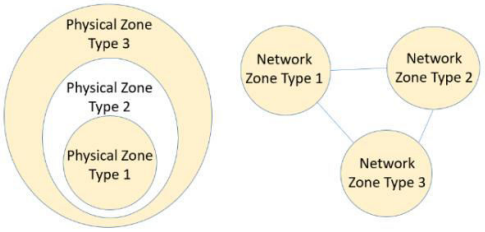

Figure 2. Canada's ITSG-22 specification suggested Physical Security Zones and NSZ (Government of Canada, 2013)

Furthermore, inspiration obtained from a physical security approach using ring-based, nested security zones is proposed for this paper. However, even though Canada's ITSG-22 and the ISO/IEC 27033-2 (International Organization for Standardization, 2012) recommend a DID design as best practice, the documents are lacking in specific guidelines for ring-based nested security design implementations. Also, although the specifications do not offer detailed zoning design guides, they do suggest some essential elements in their use. One of the suggestions is that various zoning perimeters should be implemented from different technology vendors as this reduces the penetration risks of zero-day attacks (ZDAs), which are hacker attacks implemented before a software/hardware vendor being able to develop and install a patch for a known flaw (Taylor, 2018).

Finally, connectivity amongst multiple computer system networks located in multiple data centers or cloud service providers has become increasingly complex. Thus, an examination of connectivity architectures for highly complex and secure networks located in multiple data centers will also be included.

2.2. Zero-Day Attack (ZDA) vulnerability

According to Bavati (2020), ZDA vulnerabilities enable hackers to take advantage of security blind spots, with ZDA security being a complex problem for network and software security experts to overcome. Moreover, data shows that from 2015 to 2016, there was a 125% in ZDAs, with information concerning the attack usually not discovered until after an attack has been completed (Swathy-Akshaya & Padmavathi, 2019). However, various methods have been suggested to thwart a ZDA, one being the establishment of a *honey-pot* virtual machine which opens its doors to attach so that the network owner can better detect and analyze the characteristics of the attack, where the attack was initiated from, and whether it was a private or state actor.

2.3. Security standards and policies

In recent years, the concept of *DevSecOps* has been discussed more and more, which is the practice of integrating security disciplines with the development and operations of ICT and software environments (Heilmann, 2020; Mansfield-Devine, 2018). The importance of this was highlighted in a study by Felderer and Fourneret (2015) in which they stated that any overlooked security vulnerability in a piece of software open the door to the loss of confidentiality, network system integrity, authentication and authorization processes, and the potential for the success or failure of the providing business to a customer.

Furthermore, two commonly discussed security standards for establishing security controls are the ISO/IEC 27000 NIST Cybersecurity Framework and the ISO 27001 from the International Organization for Standardization (Compliance Council, 2020).

According to Kääriäinen (2019), ISO 27001 contains a very large document framework that covers multiple aspects of IS as a whole. Additionally, it is also viewed as a standard that outlines the need for an Information Security Management Systems (ISMS) which is focused on securing customer and stakeholder information, unauthorized modification prevention, and authorizing access by individuals and systems (Compliance Council, 2010). On the other hand, the National Institute of Standards and Technology (NIST) has a voluntary cybersecurity framework that is designed for an organization that wants to secure critical infrastructure. Both the NIST and ISO frameworks are similar in their intent at identifying, evaluating, and managing the acceptable risks to information systems.

The Open Web Application Security Project (OWASP) (2017) Foundation has for many years has focused on being volunteer advocacy for application security as a people, process, and technology problem. Moreover, OWASP formulates a top ten list of what its volunteers consider to be the greatest web application security threats. Another often mentioned security guide also comes from the Open Web Application Security Project (OWASP) (2020) Foundation. Entitled the Software Assurance Maturity Model (SAMM), in the most recent version, OWASP states that SAMM 2.0 allows organizations to better analyze and improve their software security position (Figure 3) (Rohr, 2019).

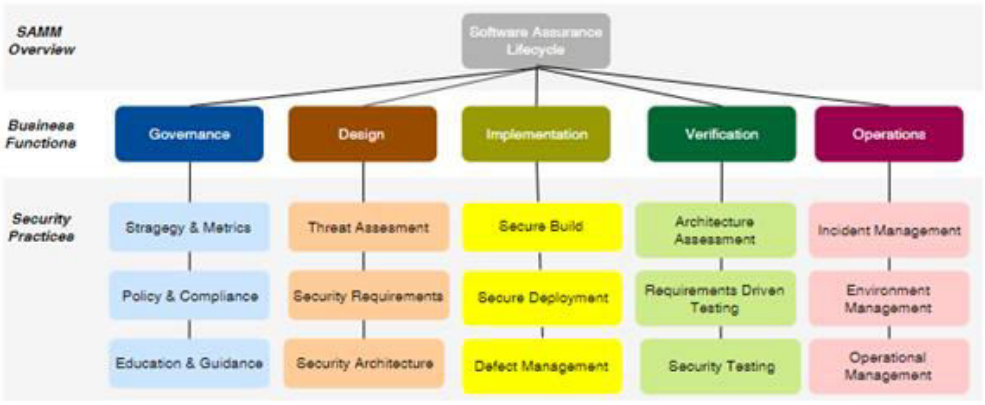

Figure 3. OWASP SAMM 2.0 Beta (Rohr, 2019)

Therefore from the analysis of numerous information security policy studies, the researchers determined that holistic network security framework literature is limited. Therefore, the researchers set out to provide a holistic design framework that is compatible with international network cybersecurity standards and policies.

3. Methods

The researchers' methodology includes the creation of a framework and guidelines from several iterations of improvements gathered from the actual Thai government and private corporate security requirement analysis from 2014 – 2018. The proposed prototype architecture in this study was also used in three separate pilot projects for the Thai Army, a Thai government fund management agency, and a private e-commerce enterprise. The systems and design for this study have been adjusted based on these real-world experiences. Finally, the proposed study made use of formulas created by the authors to evaluate and validate the proposed design.

3.1. The proposed zone architecture

This section details the main principles, rules, and methods used in the design of the ring-based nested network zone architecture (RBNNZA).

3.2. Ring-Based Nested Network Zone Architecture (RBNNZA)

One of the key advantages of an ***RBNNZA*** design is that greater security is achieved by forcing any potential attacker through a series of nested zone perimeters. As such, we propose the following design rules:

Rule A implementations will assure that data only resides in the innermost zone. Data must reside only in the innermost zone, which typically includes the organization's databases and files, secure public data, and backup images.

Rule B implementations assure that the data flow only from an adjacent zone which ensures a higher safeguard for data assets.

Figure 4 highlights the main precepts behind these rules' implementation, while also suggesting that there be three layers or zones of additional protection. It is now common for organizational data centers to adopt three-layer architecture (TLA) approach, as there are numerous advantages to a TLA including development speed, scalability, availability, and performance. Moreover, the N-tier software architecture and naming conventions are shown in Figure 4 are proposed by the researchers, with the rationale for proposing a TLA will be analyzed mathematically in the following section.

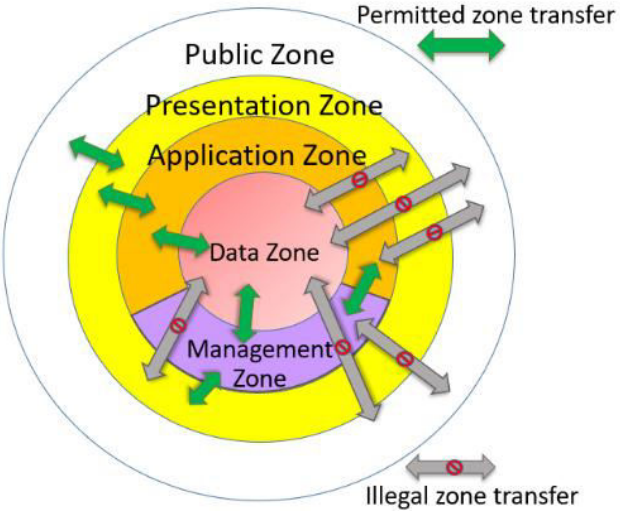

Figure 4.Ring-Based Network Architecture (The authors)

3.3. Layer selection criteria

One Layer – The use of a single layer or zone is considered an unacceptable choice in network security design architecture as any ZDA event could lead to easy penetration of an organization's most sensitive data.

Two Layers - Two nested layers can potentially afford a higher level of security due to the need to penetrate two layers of security. Also, my use of different protection schemes and/or different vendors' equipment or software, security for the innermost data is increased (Buecker et al., 2011, 2014).

Three Layers – Three-tier architectures *are* oftenused in on-premises or cloud-based applicationsas well as insoftware-as-a-service (SaaS*)* applications(LogiReport, 2020) (Figure 5).

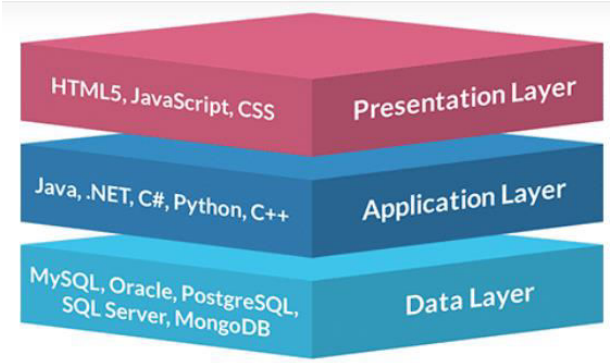

Figure 5. A web-based software architecture design using an RBNNZA (LogiReport, 2020)

Four Layers – Although from the use of the security rationale *p*reviously mentioned for layers 1 -3, a four-layer model is not normally advised due to the high complexity of the implementation, the significant additional cost, and data latency inherent in the design. Therefore, in a practical sense, the authors do not suggest a four-layer approach.

3.4. N-Tier Architecture (NTA)

N-tier or multi-tier architecture refers to software engineering to logically and physically separate data management, presentation, and processing functions (Altvater, 2016). Therefore, to achieve this, the various functions reside on multiple servers or in multiple clusters, with the 'N' being any number from 1. Advantages of an NTA include its scalability, fault tolerance, flexibility, heightened security, and management ease (Watts, 2017). Furthermore, security is enhanced as various methods can be used to secure each tier.

3.5. Network security gateway

According to network security design specifications suggested in ISO/IEC 27033-4:2014, the authors adopted the suggested architecture design for this study from the *International Organization for Standardization* (ISO) (Lepofsky, 2014).

Moreover, in firewall design, multiple types are frequently mentioned and used. Most frequently, firewalls are implemented to divide network nodes from sources that are either external or internal or even specific applications. Firewalls can also take the form of hardware, software, or a cloud-based function, with each form having its unique advantages and disadvantages. However, for this study, a decision was made to implement packet filter firewall architecture (PFFA) as a PFFA implementation is a good choice in a system that is designed to defeat efforts to disable a network's Intrusion Detection System (IDS) before an attack's launch (Bhirud & Katkar, 2010). Therefore, the authors suggest the following additional rules:

Rule C implementations should require a PFFA at each zone perimeter location as this complies with the ISO/IEC 27033-5 that suggests the use of a dual-homed gateway architecture (DHGA) (Bolanio et al., 2021) as a DHGA security gateway can also mask an internal IP address from an external attacker, while also providing user authentication capability which is frequently used in conjunction with IDS to detect possible intruder activities. In our Rule C implementation, we suggest that the number of devices which can do IP forwarding is limited with all application services only being able to offer services inside their zone or an adjacent zone.

Rule D implementations using DHGA can also be strengthened by the use of screened host architecture and/or a screened subnet architecture, which adds another extra layer of protection.

Rule E implementations using screened host architecture (SHA) and/or a screened subnet architecture (SSA) complies with security recommendations in ISO/IEC 27033-2 (International Organization for Standardization, 2012), which suggest that multiple security controls/security techniques are used to defend different potential vectors.

Rule F implementations suggest the use of multiple vendor software and hardware in the various zones (Buecker et al., 2011, 2014; Taylor, 2018).

3.6. Trusted Communication Path (TCA)

In the United States, the Department of Defense (1985) discussed how their *trusted computing base* (TCB) would support a *TCA* between the government and military TCB and the end-user for initial login and authentication, with only the user initiating communications via this path. Atrusted communication path was typically implemented by using only the Transport Layer Security (TLS), and its now-deprecated predecessor, Secure Sockets Layer (SSL). However, this is not secure enough for critical infrastructures, because of the potential man-in-the-middle attacks (MITM) and information hijacking (Publico, 2017) coupled with some government powers control over the certificate authority (CA). Therefore, the authors propose additional application-level encryption at the Open Systems Interconnection (OSI) application 7 level. Also, the implementation of HyperText Transfer Protocol Secure (HTTPS) at the transport layer is suggested.

Finally, the proposed trusted communication path supports security control standards outlined for data transfer in ISO/IEC 27002 (International Organization for Standardization, 2013), the Cryptographic Based Services in ISO/IEC 27033-1 International Organization for Standardization (2015), and also the Sensitive Data Exposure from the OWASP Top 10 Application Security Risks – 2017 (Open Web Application Security Project (OWASP), 2017). These mechanisms, therefore, promote the concept of atrusted communication path by adopting two encrypted layers for better security as shown in Figure 6.

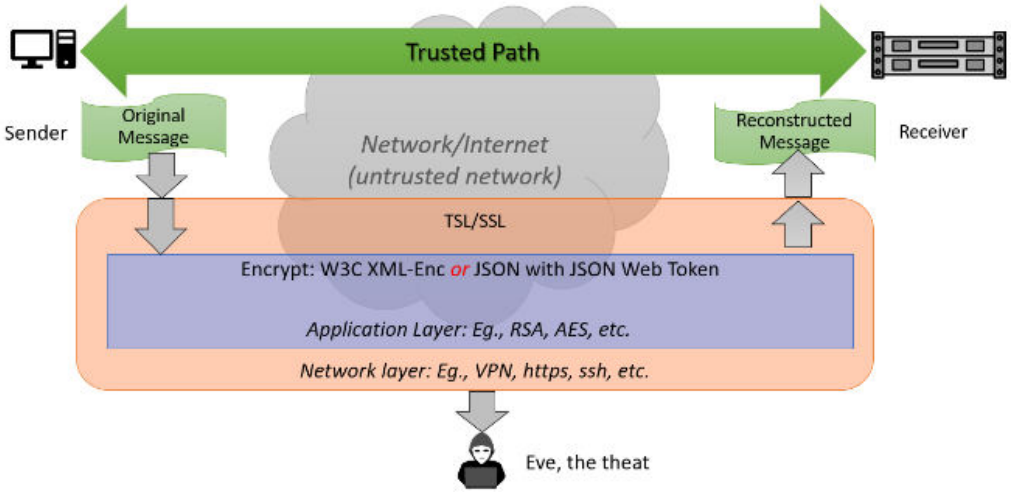

Figure 6. Trusted Communication Path (TCP) using two encryption layers

3.7. Management Zone (MZ)

The MZ is another critical part that needs to be carefully designed. Therefore, the authors took guidance from IBM's architecture guidelines (Buecker et al., 2011, 2014) and Canada's security (Government of Canada, 2007, 2009, 2013), which suggest that an MZ should be adjacent to the presentation zone, the application zone, and the data zone. Therefore, the proposed architecture is designed for the MZ to reside in Layer 2 (Figure 7 and Figure 8).

3.8. Operation area or outside Intranet

Also, IBM guidelines (Buecker et al., 2011, 2014) (Figure7) suggest that intranets should be internal and have easy access to the network's production zone. In this case, the production zone shown in Figure 7 and Figure 8 is also the same as the data zone used in this paper. In the author's discussion about network security, Wall (2013) added that an internal zone is less vulnerable than an external zone and complies with the ITSG-22 specifications. Therefore, a Rule G implementation is proposed in which threats from the Intranet (operation zone) are at the same level as the external zone. In the design of Rule G's implementation, the operation area is off-loaded to another data center as suggested in Figure 7, which can be collocated with the data center as well as being able to share some devices in the presentation perimeter. As an example, the MZ is shown in Figure 8; while in Figure 9 a network schematic is used in which an overhead method is used for better visualization.

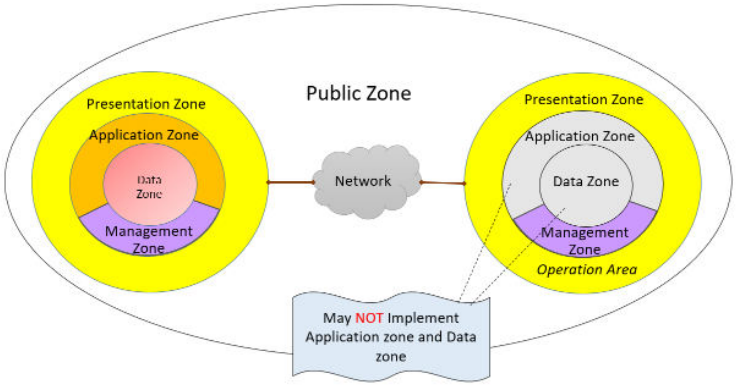

Figure 7. The public zone and network

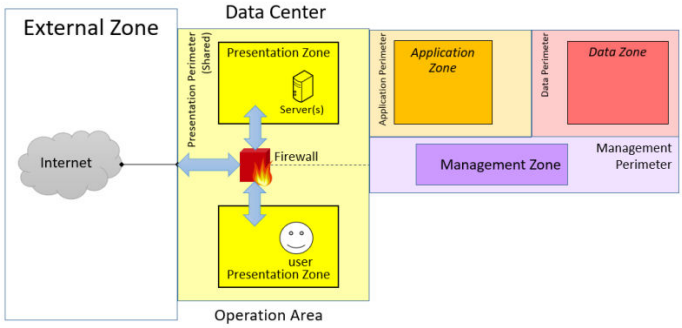

Figure 8. Suggested design for operation area collocated in the same building as the data center

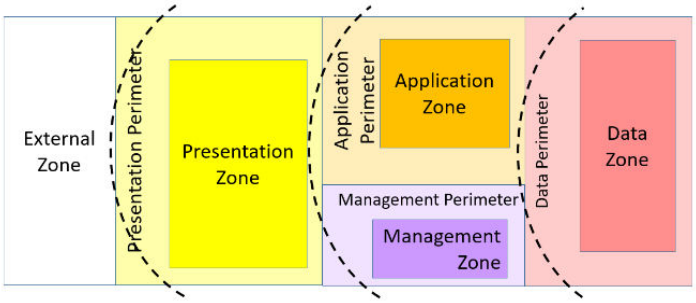

Figure 9. RBNNZA in a rectangular view

3.9. Zone types and aspects

Table 1 details the five main classification zone aspects used in the study.

Table 1. Five network zone classifications

Zones	Zone Description
External	The external network/Internet is a highly complex environment in which security measures must be implemented (Wall, 2013). However, the authors suggest that the Intranet and the operation zone as defined in ITSG-22 (Government of Canada, 2007) should be under security controls similar to the external zone.
Presentation	The presentation zone is a public zone used for web services, VPNs (virtual private networks), and DMZ (demilitarized zone) services.
Application	The application zone is used to install web services and internal application server services.
Data	The data zone is the primary storage area that can contain a network's database management systems data, file server data, user registration information (e.g. Lightweight Directory Access Protocol(LDAP) and Active Directory servers), and backup system data.
Management	This MZ is used to set up tools for managing computers and devices in other zones, such as the Syslog server, the computer management system, the security information, and event management (SIEM), the keyboard, video, and mouse (KVM) switch (Figure 10).

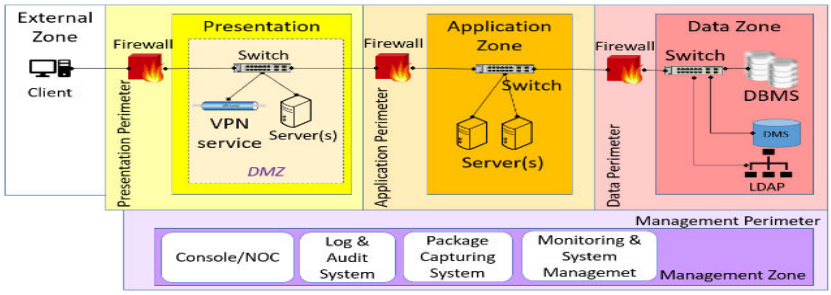

Figure 10. Network diagram view sample (The authors)

3.10. Disaster recovery data center

In consideration of a disaster recovery data center, the authors added the following additional design rule:

Rule H implementations should only allow different data centers to connect at the same layer/level of zone security.

Thus, the primary data center (PDC) and the disaster recovery data center (DRDC) can have similar architectures (ring-based network architecture of three-layers) allowing for a direct connection between the two data centers' data zones. Hence, generic replication solutions could be implemented for this architecture.

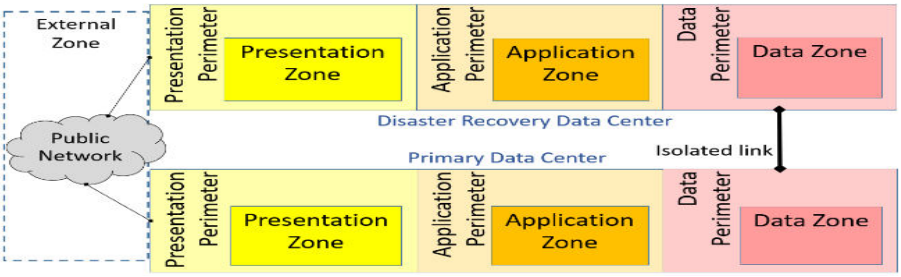

Figure 11. Proposed DRDC diagram (The authors)

3.11. The attack hop rule

In consideration of the need for highly secure zone crossings, the authors added the following additional design rule:

Rule I implementations suggest that the number of attack hops in the attack tree cannot be lower than the number of rings (Schneier, 1999).

Therefore, after a review of Figures 3 – 11, it is suggested that all designs must have a minimum of three attack hops, with Figure 12's conceptual model showing this.

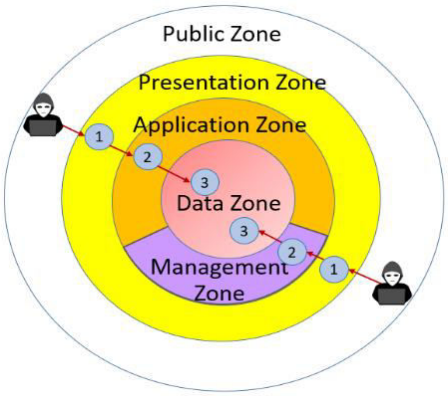

Figure 12. Conceptual Model of proposed attack hops (The authors)

3.12. Empty data zones

Usually, hackers target a network's organizational data as a primary target, which led to the authors proposing Rule B which suggests that data storage is restricted to the highest security zone. Additional security provisions the authors suggest are:

Critical data should not be placed in a presentation or application zone, with the MZ only allowed to contain configuration and login parameters. Furthermore, other security weaknesses with organizations should also be considered. These include:

Public websites often store their user information and passwords in the presentation zone, which violates the authors' Rule B which assures that the data flows only from an adjacent zone which ensures a higher safeguard for data assets.

Prohibiting data storage in the presentation zone requires an upgrade of the web-based software architecture, such as the proposed N-Tier architecture. In addition to using an N-Tier architecture, security can be enhanced by constraining how web-based applications store their files (e.g. not on the webserver). Even though a successful attack on the MZ (thru PZ->MZ) is undertaken, if Rule 1 is implemented, it will still require another zone hop to reach a data zone (three hops total).

3.13. Equipment and software mix

Various authors and reports have stated the need that to ensure maximum network security equipment from multiple vendors (eg. layer 3/4 firewalls or IPS/IDS security software) should be used which serve the same functional purpose (Buecker et al., 2011, 2014; Schneier, 1999; Taylor, 2018). Also, it is suggested that different network protocols be used for each hop, with examples including HTTPS, Web Services, and DBMS protocols for one access session (Figure 4). This increases the attack time and cost to a potential security threat.

3.14. Backup solutions

Another critical element within the network architecture is the ability to provide an effective and secure means for data backup. It is also suggested that the data-backup architecture (DBA) comply with Rule A that suggests that DBAs must be provided only within the data zone. This allows for the ability to recover using the MZ tools to reinstall and reconfigure successfully. Furthermore, the authors suggest the following DBA protocols:

Off-site backup should be used in which data from the PDC to the DRDC is done as well as to a separate data backup center if required (Figure 13).

Backup protection systems and data are also potential targets to attackers. Therefore, a backup system should be installed in the data zone where data protection is maximized.

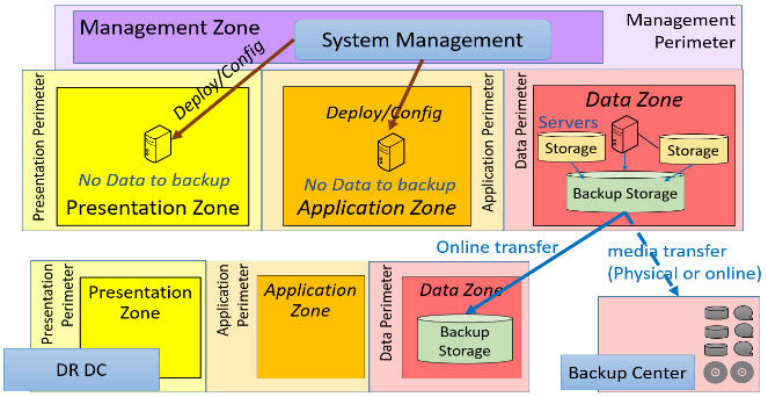

Figure 13. Proposed data backup migration diagram

3.15. Network Operations Center (NOC)

Personnel who have access to the physical network are also potential security threats, as are individuals who have been granted system administrator' privileges. Therefore consideration needs to be given to the NOC's physical security control plan. Common tools for this now include CCTV monitoring and biometric entry controls. It is also sometimes necessary to limit network access only through physical access from a NOC facility (no remote management).

Also, to even further minimize risks from NOC staff threats, the authors suggest methods in which data leaks are mitigated. Potential solutions include disallowing removable storage devices such as thumb drives, prohibiting the use of wireless networks inside the NOC, and also forbidding any unauthorized equipment to be used within NOC. Finally, having physical security of all personnel who enter and exit the NOC is suggested when the security importance warrants it.

4. Verification Tools

4.1 Attack path analysis

As has been suggested, multiple hops are an effective method for better assuring the integrity of a network's data zone, especially in a ZDA vulnerability attack. Various authors and organizations have suggested also data flow diagrams been used when analyzing the threat to the network's architecture (Open Web Application Security Project [OWASP], 2020; ThreatModeler, 2019). Therefore, the authors present Figure 14 in which a threat hop analysis using a tree concept is shown. Moreover, the study's analysis takes into consideration attack complexity, hacker attack cost, and their requirement for specialized software and hardware tools. However, we conclude that the overall security level depends on the path with the least resistance (total hops).

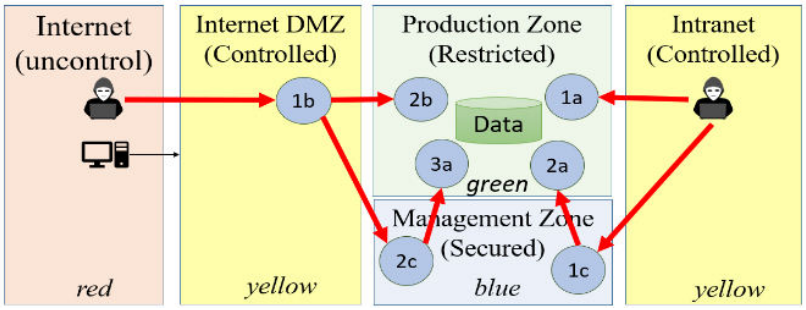

Figure 14. Architecture path of least resistance (The authors)

For example, we consider the attack path as follows:

Route 1) 1a

Route 2) 1b -> 2b

Route 3) 1c -> 2a

Route 4) 1b -> 2c -> 3a

Here, the least number of attack hops is undertaken through Route 1's attach from the Internet. Another example of an attack hop analysis is to take into consideration the use of virtual machines (VMs) in different zones as shown in Figure 15. In this case, due to multiple VMs sharing the same physical machine case, it becomes easy to see how the number of attack hops can easily drop to only one or two.

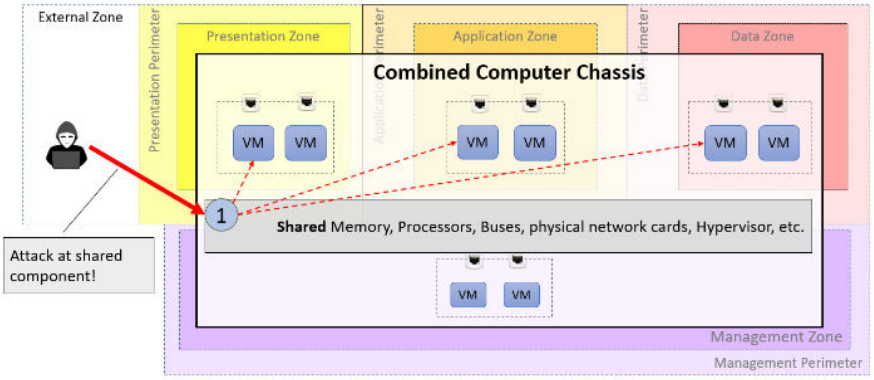

Figure 15. Attack hops analysis on network VMs

4.2. Zone security requirements.

ITSG-22 (Government of Canada, 2007) guidelines suggest that a zone's perimeter is the most effective location for security tool implementations. However, advanced security requirements require greater amounts of support expertise and are also associated with higher acquisition and operations costs.

5. Pilot Study Prototype Results

5.1. Evaluation by comparison

From the literature and theory, the researchers identified and adopted three network security architectures for the study. We shall label them Architecture A (single network zone layer) and Architecture B (two nested zone layers) (Buecker et al., 2011; 2014; Government of Canada, 2007), and the ring-based nested network zone which we have labeled Architecture C.

5.2. Sensitivity to the Zero-Day Attack (ZDA)

For purposes of defining the ZDA sensitivity of a network zone (S_z), we assumed that the probability of the given network zone open to ZDA vulnerability is a value from 0 to 1. Therefore, we can write this formula:

S_z(Architecture A)= $\frac{1}{n}$; where n >=1 [1]

In the case of Architecture B's two nested zone layers, we could simplify the analysis by letting S_z for all zones = $\frac{1}{n}$ (the same way as the big-O analysis method). Because the zones are nested, the probability of two nested zones is:

S_z(Architecture B) = $\frac{1}{n} \cdot \frac{1}{n} = \frac{1}{n^2}$ [2]

In case of the Architecture C, the three layers nested zones, we also get:

S_z (Architecture C) = $\frac{1}{n^3}$ [3]

5.3. Implementation cost

Let us define $I_Z$as the implementation cost of a zone (excluding the zone perimeter), and I_p is the implementation cost of a zone perimeter. Again, to simplify the analysis method, we assume that I_z and I_p for all zone types are not much different.

Therefore, the total implementation cost for each zone is:

The total implementation cost (I) is $I_z + I_p$ for each zone. [4]

And if we assume that I_z of architecture (A, B, and C) should not be much different, we could say that:

$I = I_z(\text{all zones}) + y\ I_p$ [5]

Where I am the overall investment, I_z (all zones) is I_z of all zones, I_p is the typical implementation cost of zone perimeter and y is the number of layers. Here, the management zone is a common cost of architecture A, B, and C, so, we could remove it from this comparative analysis.

Architecture A's implementation cost is I_z (all zones) + I_p [6]

Architecture B's implementation cost is I_z (all zones) + 2 I_p [7]

Architecture C's implementation cost is I_z (all zones) + 3 I_p [8]

5.4. Operational Cost

Using the same method for calculating the implementation cost, we could infer that:

Architecture A's operational cost is O_z (all zones) + O_p [9]

Architecture B's operational cost is O_z (all zones) + 2 O_p [10]

Architecture C's operational cost is O_z (all zones) + 3 O_p [11]

5.5. Latency Time

First Paragraph: use this for the first paragraph in a section.

For the latency time analysis, we borrowed the methods previously used for the implementation cost and the operation cost analysis. Hence, we infer that:

Architecture A's latency time is L_z (all zones) + L_p, [12]

Architecture B's latency time is L_z (all zones) + 2 L_p [13]

Architecture C's latency time is L_z (all zones) + 3 L_p. [14]

Figure 16 also shows the latency time impact on the proposed architecture, which has a relatively small impact on the baseline latency time.

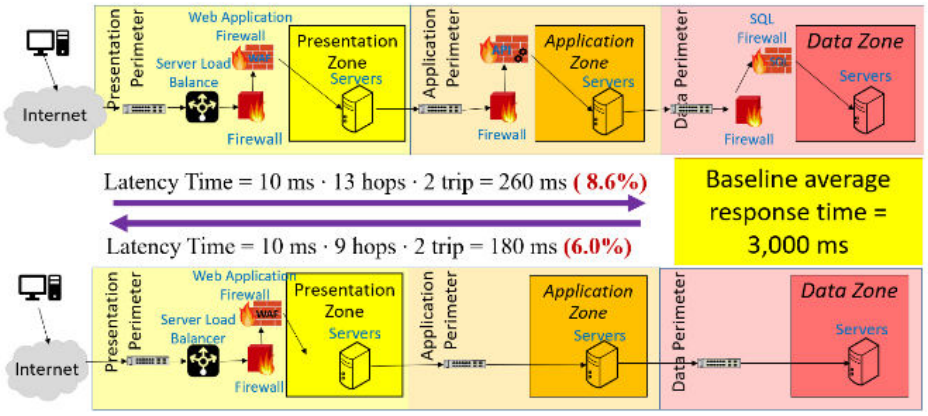

Figure 16. Network security architecture latency time analysis (The authors)

Table 2 and Figure 17 show the correlation between the attributes and the number of layers, which assumes a zero-day attack (ZDA) vulnerability probability (S_z), which is equal to 0.5. In other words, each zone has a 50% chance of having a ZDA. Here, the I_p, O_p, and L_p values are represented by the same line since their growth rates are in the same direction. While the data shows that even though the vulnerability rapidly drops when using three layers of architecture, the costs and latency linearly increase. Therefore, the results suggest that there are trade-offs decisions when considering the need for improved security compared to the higher associated cost and slower network latency.

Table 2. Security evaluation attribute comparison

Architecture	A	B	C
Number of Attack Hops	1	2	3
Sensitivity to Zero-Day Attack (S_z), n >= 1	$\frac{1}{n}$	$\frac{1}{n^2}$	$\frac{1}{n^3}$
Additional Implementation Cost from Architecture A	-	I_p	2 I_p
Additional Operation Cost from Architecture A	-	O_p	2 O_p
Additional Network Latency Time from Architecture A	-	L_p	2 L_p

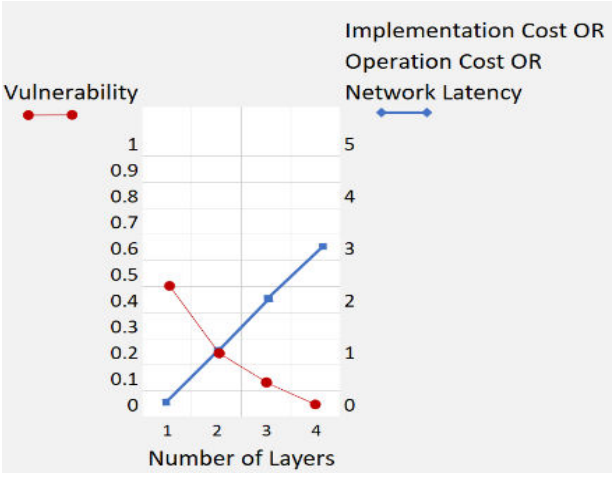

Figure 17. Comparison of evaluation attributes (The authors)

6. Conclusion

From the initially proposed network security architecture design framework based on ring-based nested network zones, the authors took a defense-in-depth strategy to develop and support a real-world data center's requirements. Additional aspects also included data center conditions, the disaster recovery data center, and the off-site backup design. The authors also offer options and criteria for advanced security attributes allowing for customization in different contexts. Multiple diagram views were used to help readers visualize and simplify the design process along with the evaluation method. Finally, the advantages and disadvantages of the proposed ring-based nested network zones architecture making it easier to decide whether or not the architecture is the right choice for your organization's network security needs.

References

Altvater, A. (2016, May 19). What is N-Tier Architecture? How it works, examples, tutorials, and more. https://stackify.com/n-tier-architecture/

Bavati, I. (2020, June 22). A zero-day guide for 2020: Recent attacks and advanced preventive techniques. *Malwarebytes Labs*.https://tinyurl.com/dp6w857k

Bernstein, C. (2020, April). Presidential Policy Directive 21 (PPD-21). https://tinyurl.com/44d5fmru

Bhirud, S. G., & Katkar, V. (2010). A novel architecture for intrusion-tolerant distributed intrusion detection system using packet filter firewall and state transition tables. *International Journal of Computer Applications, 8*(11), 29 – 32. https://doi.org/10.5120/1248-1631

Bolanio, J. B., Paredes, R. K., Yoldan, A. L., & Acapulco II, R. E. (2021). Network Security Policy for Higher Education Institutions based on ISO Standards. *Mediterranean Journal of Basic and Applied Sciences, 5*(1), 1 – 17.https://doi.org/10.46382/mjbas.2021.5101

Buecker, A., Browne, K., Foss, L., Jacobs, J., Jeremic, V., Lorenz, C., et al. (2011).*IBM Security Solutions Architecture for Network, Server, and Endpoint. IBM Redbooks publication.* https://tinyurl.com/34tjshb9

Buecker, A., Arunkumar, S., Blackshaw, B., Borrett, M., Brittenham, P., Flegr, J., et al. (2014). *Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security.* IBM Redbooks publication. https://tinyurl.com/47uds2hv

Chaisuriya, S., Keretho, S., Sanguanpong, S., & Praneetpolgrang, P. (2018). A security architecture framework for critical infrastructure with ring-based nested network zones. *2018 10th International Conference on Knowledge and Smart Technology (KST),* Chiang Mai, Thailand (pp. 248-253). https://doi.org/10.1109/KST.2018.8426099

Compliance Council. (2020). *ISO 27001 vs NIST Cybersecurity Framework*. https://tinyurl.com/

Cybersecurity and Infrastructure Security Agency [CISA] Act of 2018. (2018, November 16). https://www.cisa.gov/critical-infrastructure-sectors

Department of Defense. (1985, December). Department of Defense trusted computer system evaluation criteria - DoD 5200.28-STD. https://tinyurl.com/23mcd6dz

European Court of Auditors. (2019, March). Challenges to effective EU cybersecurity policy. https://tinyurl.com/36dfastz

Felderer, M., & Fourneret, E. (2015). A systematic classification of security regression testingapproaches. *International Journal on Software Tools for Technology Transfer, 17*(3), 305 – 319. https://doi.org/10.1007/s10009-015-0365-2

Government of Canada. (2007, June). Baseline security requirements for network security zones in the Government of Canada (ITSG-22). https://tinyurl.com/4br6zczs

Government of Canada. (2009, May). Information technology security guideline (ITSG-38) network security zoning (Design considerations for placement of services within zones)

Government of Canada. (2013, February 18). Operational security standard on physical security. Treasury Board of Canada Secretariat. https://tinyurl.com/y5dejbsz

Heilmann, J. (2010). *Application Security Review Criteria for DevSecOps Processes*. (Masters thesis, Lulea University of Technology]. Sweden. https://tinyurl.com/y3uynzea

International Organization for Standardization (2012). ISO/IEC 27033-2:2012: Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security. https://www.iso.org/standard/51581.html

International Organization for Standardization (2013). ISO/IEC 27002:2013 Information technology – Security techniques –Code of practice for information security controls, Geneva, Switzerland, October 2013

International Organization for Standardization (2014). ISO/IEC 27033-4:2014 Information technology – Security techniques – Network security – Part 4: Securing communications between networks using security gateways, Geneva, Switzerland

International Organization for Standardization. (2015). ISO/IEC 27033-1. Information technology – Security techniques - Network security - Part 1: Overview and concepts, August 15, 2015.

Kääriäinen, K. (2019). *Improving security in software development process: Case Tieto AS*. [Masters thesis, South-Eastern Finland University of Applied Sciences]. Finland. https://tinyurl.com/4bvchwuj

Lepofsky, R. (2014). ISO/IEC 17799:2005 and the ISO/IEC 27000:2014 Series. In *The Manager's Guide to Web Application Security*, (pp.161 – 163). Apress. https://doi.org/10.1007/978-1-4842-0148-0_12

LogiReport. (2020). 3-Tier Architecture: A complete overview - What is a 3-Tier Architecture? https://tinyurl.com/dkuvb4d2

Mansfield-Devine, S. (2018). DevOps: finding room for security. *Network Security, 2018*(7), 15 – 20. https://doi.org/10.1016/s1353-4858(18)30070-9

McGraw, G. (2004). Software security. Security & Privacy. *IEEE Security & Privacy Magazine, 2*(2), 80 – 83. https://doi.org/10.1109/msecp.2004.1281254

McGraw, G., Migues, S., & West, J. (2017). *Building Security in Maturity Model (BSIMM9).* Academic Press.

Moschovitis, C. (2021). A Cybersecurity Primer. In *Privacy, Regulations, and Cybersecurity: The Essential Business Guide*. (pp. 181 – 204). John Wiley & Sons. https://doi.org/10.1002/9781119660156.ch11

National Security Agency. (2010, March). Defense in depth a practical strategy for achieving information assurance. https://tinyurl.com/3feb3v7r

Open Web Application Security Project (OWASP). (2017). OWASP Top 10 –2017: The ten most critical web application security risks. https://tinyurl.com/mnc5n7je

Open Web Application Security Project (OWASP) (2020). OWASP SAMM v2.0 – Core Model Document. https://tinyurl.com/3trwshac

Publico, R. (2017, March 1). What is a man-in-the-middle attack and how can you prevent it? GlobalSign. https://tinyurl.com/exez5zrw

Rohr, M. (2019, July 23). Impressions of OWASP SAMM 2 Beta. [Personal Blog]. https://tinyurl.com/22zv6x2v

Schneier, B. (1999). Attack Trees. Dr. Dobb's Journal. https://tinyurl.com/y59bmkvt

Swathy-Akshaya, M., & Padmavathi, G. (2019). A study on zero-day attacks. *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM),* Amity University Rajasthan, Jaipur - India, February 26-28, 2019. http://dx.doi.org/10.2139/ssrn.3358233

Taylor, S. (2018). Protecting embedded systems from zero-day attacks. *Proceedings of NAECON 2018 - IEEE National Aerospace and Electronics Conference*. https://doi.org/10.1109/naecon.2018.8556791

ThreatModeler. (2019, August 12). Process flow vs. data flow diagrams for threat modeling. https://tinyurl.com/tdetc

Turton, W., & Robertson, W. (2021, March 7). Microsoft attack blamed on China morphs into global crisis. *Bloomberg*.https://tinyurl.com/va9m843v

Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal, 26*(2), 107 - 124. https://doi.org/10.1057/sj.2012.1

Watts, S. (2017, July 26). N-Tier Architecture: Tier 2, Tier 3, and multi-tier explained. [Personal blog]. https://tinyurl.com/3pm4hubx