IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 08, Issue 6 (June. 2018), ||V (VI) || PP 43-52

Network Segmentation strategies to articulate new method to Address Growing Information Security Concerns.

Dr.Ramesh K
Department of PG studies in Computer Science, Karnataka State Women's University, Vijayapur, India
Corresponding Author: Dr.Ramesh K

Abstract: This research paper proposes the concept of network segmentation as a practical advance to withstand information security deficiencies, concerned to Bring You Own Device (BYOD), Internet of Things (IoT).Cyber-attacks and regulatory accordance of Protection of Personal information. In view of which an idea of network segmentation is floated as a solution approach in terms of network architectures to improve information security and strengthen the cyber defence abilities. We have realised this architectural advance through sufficient use case designs. We have also adopted a decision support system with simulation modelling to evaluate the use cases that are proposed in this research paper.

Key words: *BYOD, IOT, Network Segmentation, Network Virtualization, Security Policies*

Date of Submission: 07-06-2018 Date of acceptance: 26-06-2018

I. INTRODUCTION

There is dire need to scrutinize, determine and place the network segmentation to improve current information security jurisdiction. Classical Network architectures basically emphasize on boundary allocated checks, While Network Segmentation endeavours a new aspect of improving information security controls based on crude network policies, adequate to recognize, define and control information progress between network components. Our paper examines the endorsement of network segmentation as a technology to address information privacy and data concerns, with respect to Bring Your Own Device (BYOD), Internet of Things (IoT) and Personal Information and Privacy regulations. This paper delegates an architectural framework in terms of network segmentation policies which is able to isolate an application, data streams and device connectivity based on the subtlety and seriousness of information and data.

All over the globe conventionally built Internet Protocol networks are still in extensive usage in many of the today's organizations. These conventional networks have become complex in last 22 years due to dramatically increase in interconnections number. Disruptions, namely Bring Your Own Device (BYOD), Virtualisation, Mobility and Software defined services have further increased the complexity of these networks. These difficulties made the network environments not to be fault tolerant with growing expenses concerned to management and the administration. Here concern is the complications of conventional networks with respect to the increasing probability of risk realisation. The focus here is to build fundamental basis to address business network infrastructure architectural concerns, if not defined it may further weakens, the essence on which the business depends. Hence to achieve business objectives, Network security has become key in propagating the risk factors , those which affecting the implementation of technology in achieving the business goals.At present networks are built conventionally on periphery based defence techniques, and security backing is affirmed over the network end to control the attacks, from piercing in to the network interiors.

Hence our idea is to analyse the present information security challenges, and recording the drawbacks that how traditional networking architectures are failing in handling the security concerns. A Survey is conducted to summarize the essence of Network-Segmentation as a framework which will be a basis to address security concerns related to BYOD, IoT, and Cyber regulations. We conducted a study with many IT experts and Information security engineers, to explore the risks and security concerns dealt with adoption of IoT, BYOD, and Data Privacy. The study defined the consent of stakeholders in bringing the feasibility of network segmentation, to solve many of the risks and security concerns of confidential data and network isolation in bringing down the risks associated with present security challenges.

Most of the information security engineers usually consider Network Segmentation is a better solution to address some of the basic security concerns those are required for current networks. Our paper aim is to create awareness and trigger the debate, on network segmentation adoption as a viable solution to address the risks associated with recent technology disruptions.

In this paper we have provided a procedure for LAN network architectures design that is able to cope with BYOD, IoT and Data Privacy, with the aid of network segmentation. This procedure design deals the busy traffics and also creates a method in depth to control information security challenges. The paper also contributes the design framework that explores the segmentation knowledge in terms of novel approach in placing the segmentation as a possible network architecture to bring basis for creating LAN environments capable of dealing with existing information security challenges.

II. PROPOSED NETWORK SEGMENTATION ARCHITECTURE

The trust[24] is the key factor, considered while designing a network security architecture in recent digital world scenario. The Organisations can win against half of the cybercrime battle by changing their existing trust models in to more zero trust approach. Due to the lack of trust[24] amongst senior management, the origination's information security strategies and policies are getting failed in many of the cases. Senior management some time become the catalyst to relax security controls for easier business interaction, to conform the security governance models without understanding the risks at their primary level. Thomson, K, von Solms, R, & Louw, L [1], emphasizes the need of adopting an environment by the senior management and executive committee to promote sincerity in ensuring information security practices otherwise cyber attacks will continue to increase, Hence Organisations need flexible and agile working environments without restrictions. The idea of network segmentation can contribute to solve many of these sufficient information security challenges. Figure 1, below shows a newer method of network designs, which is an abstract of architectural perspective, that a shows how a virtualisation and software defined networking can articulate the todys networks architectures.The proposed solution places an emphasis on agility with information security as a core outcome and is a direct result of our network segmentation approach.

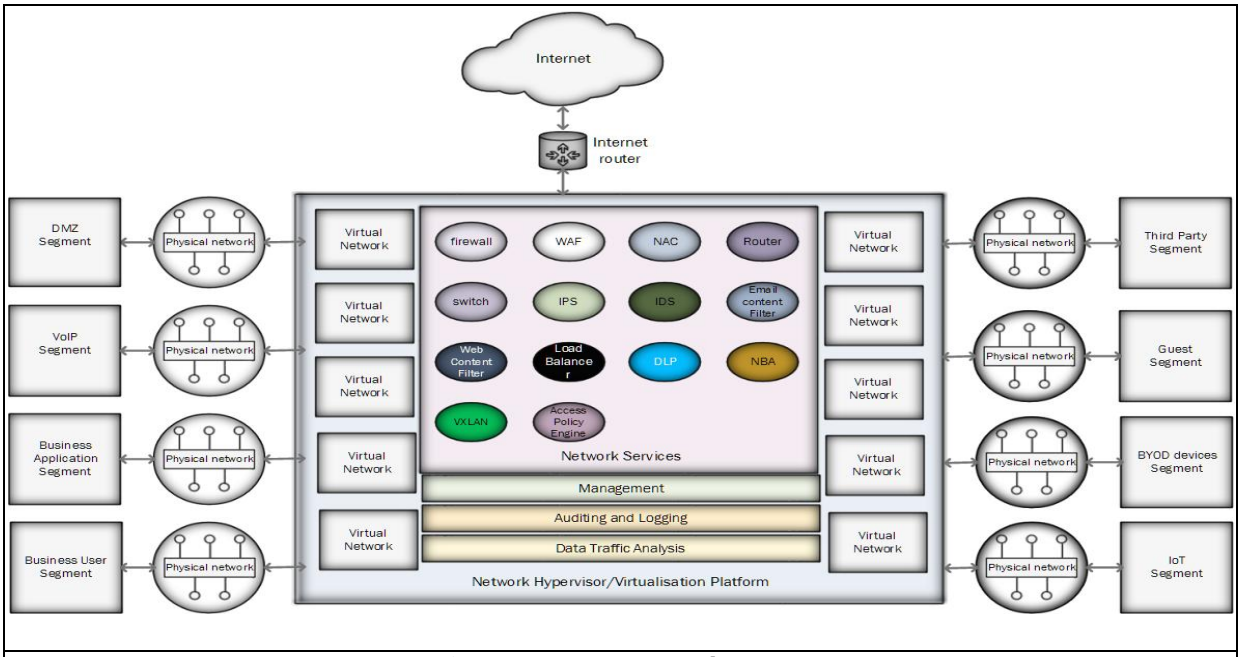


Figure 1 : Secure Network Design

Design Approach Principle

The design principle here adopted is based on user applications, network flows and trusted/ untrusted devices. All the traffic flows in the network is presumed to be untrusted in the designed model, and is subjected to information security scrutiny to find out whether malicious activities are restricted from generation during the data flow all over the network. This requires a support from Senior management and executives of organisations and is critical for the feasibility of such an approach. Network security design needs an endorsement of a Zero Trust approach which would be the fundamental change effective on core business functions within an organisation. Our approach i.e zero trust is a foundation to balance the judicial and regulatory standards within which different businesses operate.

The zero trust model was first described by Kindervag, J[2], the objective was to target the internal security controls that are able to detect, restrict and alert malicious activity that is trying to pierce the internal

network. This approach was to narrow, device-to-device, user-to-user and application-to-application access, and to reduce the risk of malware spreading and also to reduce the impact and scope of an infection dramatically.

Information security policies adopted

The framework of architectural design furnishes the details of information security policies aggregations which are devised to boost the overall network security aspects. Aggregation of network based services may be incorporated into the executive layer with the aid of network virtualisation. Complete network security aspects can be served by these combined Services based on the requirements for the Virtual network. E.g. A DMZ network hosting web servers could incorporate routing, switching services and firewall, where as an IPS and potential Web Application Firewall (WAF),A guest virtual segment can incorporate services such as switching, firewalling and a web content filtering. TheVirtual Machine contains all these security services integrated with each other. An optimised and efficient design for a particular requirement can be achieved from the interleaved network services which are the building blocks in this proposed architecture. Network Virtualisation includes Firewall, Network access control (NAC), Routing and switching services, Virtual extensible LAN (VXLAN) capabilities, Intrusion Detection Systems (IDS) and Intrusion prevention Systems (IPS),Network Load Balancer(NLB) and Data loss prevention Capabilities as a network Services.

Network Service Description

The Design approach mentioned in this paper procures the information security[10] policies to be generated at various levels and aggregates the devices as well as network services. This approach makes the network capability ensures the flowing network traffic is validated and authorised, conforming to the zero trust approach and integrates aggressively across various information security regulations. Figure 2.shown below furnishes the hierarchy of information security policies which are described based on the architectural design.

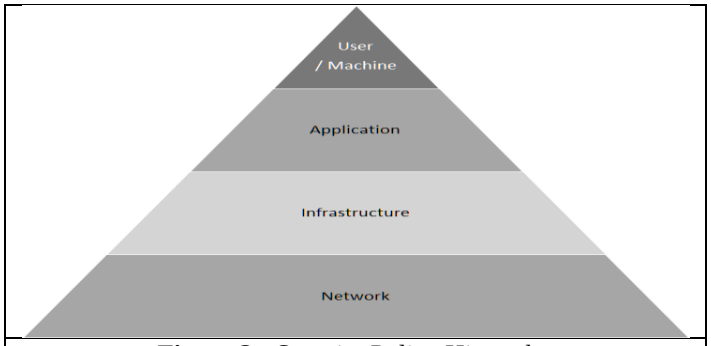


Figure 2 : Security Policy Hierarchy

This security policy hierarchy is referred and altered on basis of Miller, L, & Soto, J, [3]. There are only 3 lower hierarchies we are proposing a fourth layer user/machine device based authentication in this research paper. Information security regulations are defined here to address network and infrastructure controls as well as application and user/machine rules. The security policy hierarchy is expressed in terms of user machine devices, applications, Network rules and Infrastructure.

Secure Network Design strategies

The Intellectual network architecture shown in Figure 1. Proposes a basis to address the challenges of present information and cyber security concerns [11][13].This architecture is designed in such a way that its roots are rooted deeply in network segmentation strategies and virtualisation such that incoming traffic is treated as untrusted until a process tests it for verification and authorisation based on relevant security policies described below.

Management: To design an effective network security capability which can deal an existing and future cyber threats are found in integration and analytics. The effective centralised virtual networks and management potentials to manage the relevant network services configured within a virtual network are provided by the management layer to ensure the centralised administration of network services.

Auditing : Auditing and logging capabilities are added to management layer to allow a complete adaptable configuration potential to restrict the errors and promote consistency to ensure consistent zero trust model amongst all services. Within a virtual network segment, and also across network services throughout the virtual stack and other virtual segments, It is necessary to ensure accurate occurring of auditing and logging of network services, to ensure an integration of exceptional cyber defence strategy compared to present defences. The

network management will get grow when they trigger the defensive actions across a majority of network services to learn and move onto the dedicated network defence.

Analysis: The Traffic Analysis competence gets the real time network security[12] analytics to the malicious actions. To bring consistency and uniformity in logging capabilities across the majority of network services, analysis tools can be used to gain better insight into the security modes of the network. If these tools are combined with network base line analysis directions to detect anomalies in the network, so that security efforts can be focused on to reduction of network irregularities by false positives and negatives. With these analysis tools Security engineers can find the suspicious network behaviour related to a cyber-attack by recognising network traffic packets, patterns and alerts with the virtualisation of network services, centralised management, auditing, alerting and with analytic tools, so that interaction of security development is improved and unwanted network traffic is detected faster using these analytical potentials. Hence the Segmentation strategies suppress threats faster and place the limit on target area of a cyber-attack.

III. IMPLEMENTATION (REALIZATION)

ANALYSIS OF DESIGN

Network Segmentation strategies contributes a modern network designs established upon virtualisation to deliver an integrated security potential aggressively powered of controlling network traffic within a Local Area Network to achieve feasible solution. These strategies are built over a sufficient evidences of intensity and frequency of breaches available at present scenario. Segmenting networks can be a logical strategy which is capable of addressing security concerns not troubling business in current times.

Proposed Use Cases

The Proposed Designs are examined on the basis of security policy hierarchy Figure 2. Which incorporates segmentation strategies and design. We have tested the security challenges against the model using decision support system.

3.1 Bring your Own Device and Guest Access

Classic BYOD [7] and Guest networks are usually built under the subset of the existing business network, also shares the equipments such as Wi-Fi controllers, Firewalls[14] and Content Filters. Hence this pushes BYOD itself in to the complications of dividing the business resources with guest access. To overcome this there is a need to build separate networks to provision the BYOD [8] and Guest access, are shown in figure 3(a) and 3(b).The complexity of BYOD [8] and Guest access increased due to added purchases of hardware and software.

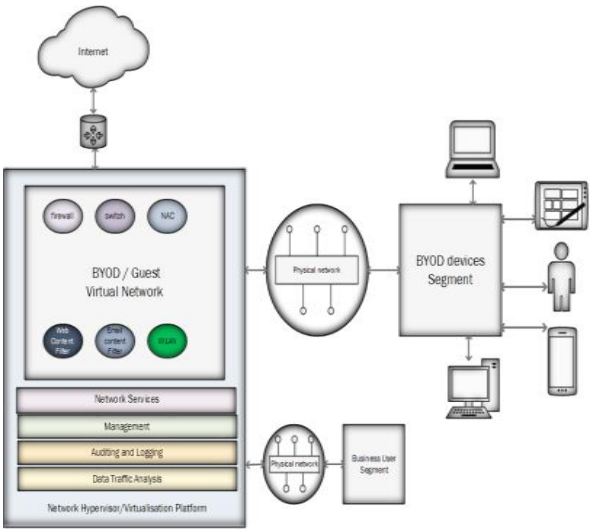


Figure 3(a) Use Case for BYOD segmentation

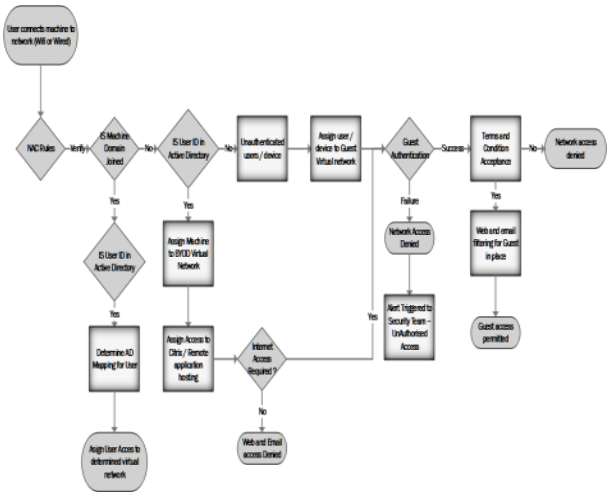


Figure 3(b) BYOD Decision Diagram for Application / Data Segmentation

Figure 3(a). describes an architectural design contributed to satisfy the BYOD and Guest access based on the proposed virtual architecture depicted in figure 1. This proposed Virtual network layout furnishes the applicable services for Guest / BYOD access to the network. This architecture allows Guest users only to access the internet, but not any other services on the network. Using this proposed virtual architecture BYOD user's

untrusted devices can connect to the network to access genuine business services. But this cannot be the same for Zero Trust model, creates security concerned problems therefore organisations must implement the stringent segmentation policies. The decision diagram depicted in Figure 3(b) examines the nodes plugged to the network to indicate whether these devises are guest devices or BYOD's. Based on this description the network service (NAC virtual service) is able to cater the concerned authorisations to permit or deny access to corporate resources.

The proposed Segmentation doesn't require an additional security infrastructure to disconnect the Guest network completely from the rest of the network. The virtual segment provisioned in the architecture for Guest and BYOD access permits the required enough network services to cater the risks and concerns of untrusted devices. The proposed use case provisions enough controls to deal the risks of BYOD and Guest devices over the network, endorsing the model of zero-trust.

Network segmentation [21] architecture proposed here ensures the data and application privacy through, the legitimate segmentation and network controls applied to complete LAN network communications. The proposed segmentation in this paper restricted to only permitted communications to access network services, applications and information that they are authorised to auditing/logging provisions. The core of virtual network hypervisor has got both monitoring and traffic analysis services and provides the required data to identify, if any of the unwanted traffic flows reoccurring (i.e. traffic jump attempts from one segment to another). Our segmentation layout is equipped with sufficient rules that can structured to detect such traffic inconsistencies and triggers the applicable network segmentation policy, which lockdowns quickly to isolate any malicious traffic.

3.2 Internet of Things (IoT)

Figure 4(a), represents our effective IoT[15] network architecture design that is composed of diverse IoT endpoints (sensors, devices, appliances) lead by an IoT aggregator, for the accretion of IoT Data that can be fed into a data warehouse or a database for further analytics and finally presents an application web server as an end user application.

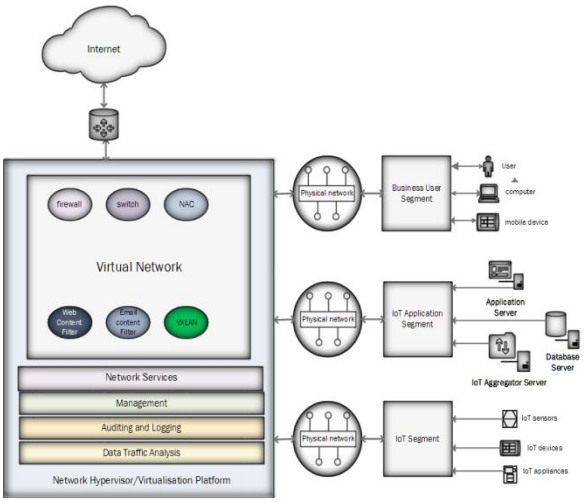


Figure 4(a) Use Case for IOT segmentation

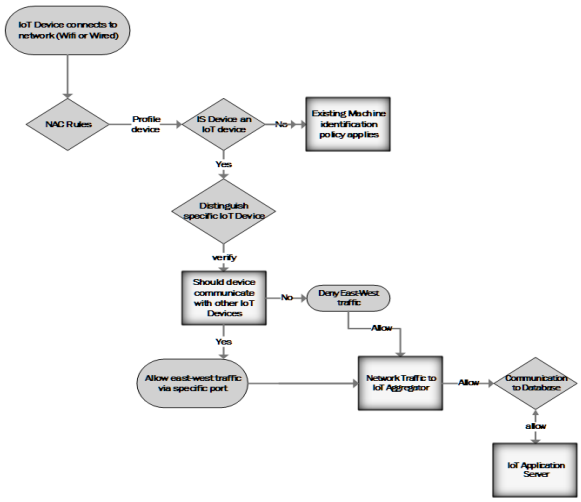


Figure 4(b) IOT Decision Diagram

We have provided here a simple essence of a security segmentation model for IoT, which is a simplified approach that provisions the IoT devices distribution across the network and varying endpoints. The architecture identifies IoT devices based on NAC features to deploy the segmentation policies to confine the devices belonging to IoT virtual network segment. NAC policy engines are applied to depict the rule sets to regulate the devices so that an appropriate IoT guidelines shall be enforced. Often we find many situations where IoT devices share communication with each other, Specifically NAC polices are required for this kind of instance, to control East-West movement and isolate IoT devices segment. Using the NAC rule sets, the NAC service can be virtualised on any of the virtual network segment to create the capability to recognise and figure out IoT devices subsequently. Figure 4(b),shows admissible network segment profiling process in sequenced steps where an IoT device is, recognised and authorized. This approach of segmentation improves the security aspects at a basic level for an IoT devices over the network. The Elkhodr, M, Shahrestani, S, & Cheung, H (2016), research paper suggests a robust middleware platform,is much effective and required to ensure the data communication with a less budget and low power IoT devices to undergo crude data security controls. Such middleware solutions are compatible for the IoT, but needs more complex NAC and firewall regulations. In

parallel the need for data figuring on network services can be certified to maximize the crude data privacy controls proposed by Elkhodr, M, Shahrestani, S, & Cheung, H (2016).

3.3 Cyber Security: APT.

Network segmentation policies must deal effectively the sophistication of evolving threats, and must be productive to automate responses to network traffic with real-time efficiencies. In Figure 5(a) we have described the segmentation polices that is capable to cancel the connection from the potentially infected host, trying an attempt to meet an investigation work ,so that it can penetrate into more and more machines, for example a HR segment trying to continuously connect to other HR machines in that particular segment. Hence real-time decision making ensures proliferation in the whole network tried by the APT's are immediately controlled.

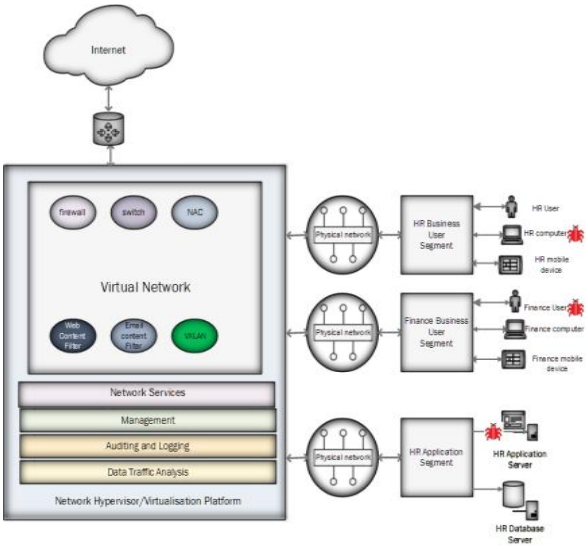


Figure 5(a) Use Case for Cyber Security segmentation

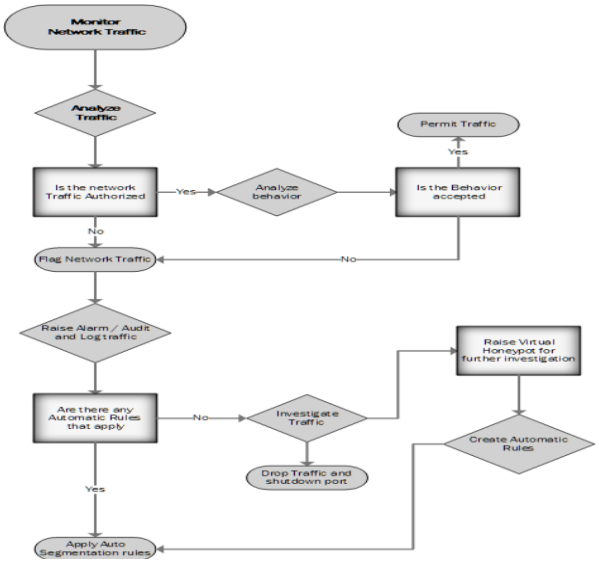


Figure 5(b) Cyber Security Decision Diagram

Figure 5(b), describes a decision diagram that depends on virtual network services[16] such as IPS, firewalls, NAC etc., Our proposed use case also has got the capability of auditing, logging and monitoring abilities those are part of the virtual network. Here it analyses for any potential damaging threats making their moves in a perticular traffic movement, For illustration a potential infected host in the finance network segment attempting to perform port scans on other network segments, such as the HR segment, which is treated as profoundly suspicious behaviour, our proposed policies for network segmentation are capable of cancelling the host connection, or it can also able to isolate a particular machine to conduct further investigations. The key proposals such as flexibility and efficiency deal mercilessly with malicious network traffic,with real-time changes within the network virtualisation stack is highlight of our proposal in this paper. It also includes a further scheme that highlights odd network traffic, for instance an HR computer trying to access the HR application at on odd hour that is not in conformance with the monitored pattern. An HR desktop tries to access the HR application at odd hour, our proposed segmentation policies will detect this traffic / behaviour anomaly and initiates appropriate action. Hence we can say that an effective segmentation network security analysis derives the advantage of clear gauge and based on guidelines of existing network traffic flows as well as server / application performances. The criterions could also be applied to odd HR application performances or network traffic that exists outside of the observed patterns, to identify malicious activity and a potential compromise.

IV. SETTING NETWORK ENVIRONMENT PARAMETERS BASED ON ARTEFACTS AND HYPOTHESIS

We have used the decision system mentioned in [4] hypothetically to artefact that lays down a model with an architectural approach in segmenting the networks to solve the extensive risks occurring within BYOD and IoT devices being seen on internal networks. A software service requires specification of multiple rate parameters including (i) vulnerability arrival rate (Δ_{vuln}^{-1}) (ii) patch arrival rate $(\Delta_{patc\ h}^{-1})$, (iii) exploit development rate (Δ_{dev}^{-1}), and (iv) exploit occurrence rate $(\Delta_{exploit}^{-1})$ Additionally, each enclave requires

specification of the enclave cleansing rate ($\Delta_{cleanse}^{-1}$). Here, the goal of cleanse is to characterize a representative service. Here we e utilize all the assumptions hypothetical used in [4] .
These studies define a vulnerability lifecycle that captures the state of a vulnerability over time. We use this to characterize vulnerability phases including vulnerability disclosure (when the vulnerability becomes known), exploit development (when an exploit for the vulnerability is developed), exploit deployment (when the exploit is used), and patching (when a patch for the vulnerability becomes available). We demonstrate the system via a network environment under an evolving information flow and a cyber threat. The aim is to use the system to improve an initial segmentation architecture as

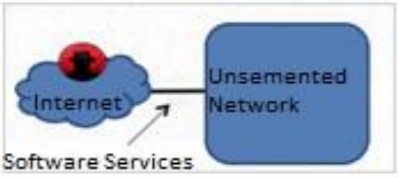


Figure 6 Initial segmentation architecture

acceptable level of risk and to adapt that architecture, if necessary, when the threat changes.
Fig. 6 shows the initial architecture, which represents an unsegmented network that is a network with only a single enclave such that all network devices can communicate directly with all other network devices. In this single enclave network direct communications are allowed from enclave to the Internet where cyber attackers preside. Communications from the network to the Internet are made through software services (applications).

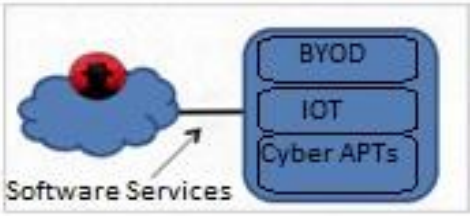


Figure 7: segmented architecture envelopes

Figure 7 shows the network environment as is specified by parameters described in Section 3. Figure 7 is used to leverage real vulnerability, patch, and exploit data to characterize a representative software service and its associated expected rates of vulnerability arrival, patching, and exploit development using the process given in [4]. Below is a summary of this process.

Figure 8.Time dependencies between vulnerability lifecycle phases

Figure 8 shows time dependencies between these phases. From the figure, vulnerability disclosure kicks off two processes in parallel: exploit development and patch arrival. Once an exploit has been developed for the vulnerability (and before a patch has arrived), exploits that may result in compromises can now occur for that service. Patching ends the lifecycle by rendering its exploit(s) ineffective. We use data collected with respect to these phases to compute rates for a representative service.

Δ_{vuln}^{-1} :This term is to characterize the vulnerability arrival rate of a representative service there is need of averaging the most common services given in [5] is as shown below

$$\Delta_{vuln}^{-1} = \frac{\sum_{i \in N} \frac{V_i}{T}}{|N|} \quad (1)$$

where i represents the most vulnerable application [4]. Vi is the weighted sum of vulnerabilities for application i over time period T where weights are given by each vulnerability's severity score . N is a set containing the most vulnerable applications [5] which collects vulnerability data and groups them based on the applications. Note that Eq. 1 considers the set of all known vulnerabilities for a given software service s over a given time period, T Δ_{patch}^{-1}: analyzes data on vulnerabilities patch and derives vulnerability discovery dates and patch availability dates from public sources. We fit their results to a Poisson distribution and then compute a weighted average of these fitted results.

Δ_{dev}^{-1}: executes a similar process to derive exploit availability (exploit development) dates. This yields exploit development rates ranging from ≈ 8 days before disclosure to ≈ 2 days after disclosure. Additionally, [4] reports that for ≈ 90% of vulnerabilities collected, exploits are available within 10 days of their corresponding disclosure dates. We investigate three settings of this parameter that characterize three increasing attacker threat levels.

$\Delta_{exploit}^{-1}$: Incident reports are generally difficult to come by because organizations do not like to share data on detected compromise events within their networks. As such we investigate three settings of this parameter that characterize varying levels of attacker aggressiveness.

Table 1

Network Environment Parameter Settings

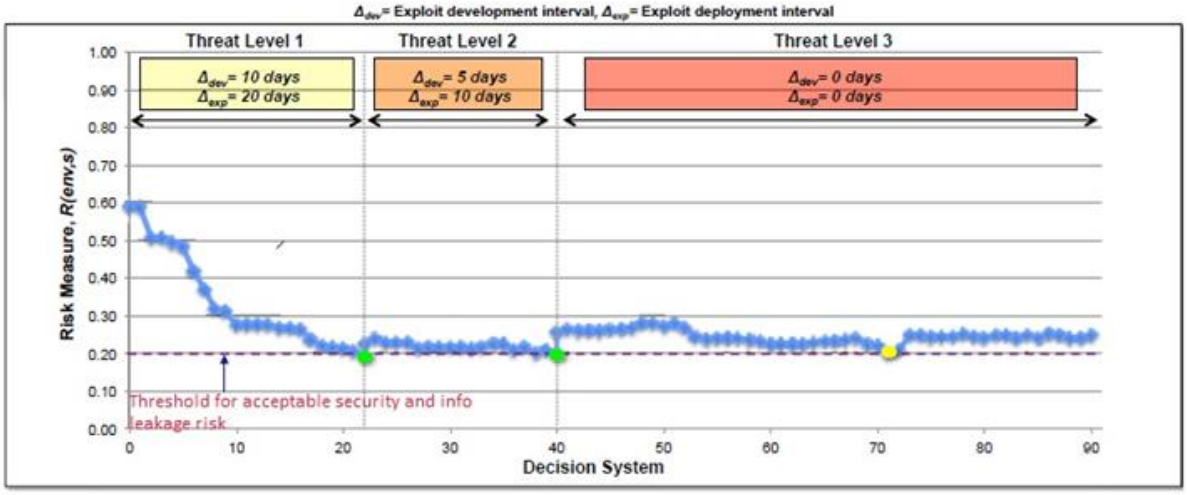
Δ_{vuln}^{-1}	Vulnerability Arrival Rate	1 every 65 days
Δ_{patch}^{-1}	Patch Rate	1 every 25 days
Δ_{dev}^{-1}	Exploit Development Rate	1 every 10, 5, or 0 days
$\Delta_{exploit}^{-1}$	Exploit Deployment Rate	1 every 20, 5, or 0 days
Δ_{clean}^{-1}	Enclave Cleanse Rate	1 every 4 years

The settings for network environment parameters are given in Table I. The expected rate of enclave cleansing (last row of the table) is set via an observation given in [6] which documents an advanced attacker who was able to persist in a victim's network. For parameters exploit development and exploit deployment (rows exploit 3 and 4 in the table, respectively), we use three different settings to characterize three threat levels ranging from lower to higher threat. The highest threat level (Δ_{dev}^{-1} = 1 every 0 days and $\Delta_{exploit}^{-1}$ = 1 every 0 days) represents an attacker who exploit effectively can exploit a vulnerability as soon as it arrives.

V. RESULTS AND EVALUATION

The use cases described in section 3, benchmarks a consistent approach that segments the networks ,a consistent method that designs the information security regulations and alerts for implementing secured data parallelisation and gathering of solvable use cases. The artefact demonstrates a model and our architectural approach segments the networks in order to address the frequent risks associated with BYOD and IoT devices those visit internal networks. Our architectural design provides also a method to separate business applications depending on network communications. The risk of a data breach can be reduced by a emphasized core competence combined response leakage solutions to build further required data loss. The architectural design model signifies also, how a zero-day and new malware burdens can be notified within the segmented network by monitoring the behaviour of network patterns and addressing any anomalies that may surface. The proposed segmenting Automation policies definitely develops the immunity capabilities ,those make the network to emerge more aggressively, running and quick approach to deal cyber threats. The results we have provided here are all based on the hypothetical as mentioned in [4] .Fig. 9 gives the results for our experiments over the three threat environments. In the figure, the vertical axis is the risk measure and the horizontal axis is the system iteration number. The experiment starts with the lowest threat level (shown as Threat Level 1 in yellow) and progresses to the higher threat levels (shown as Threat Level 2 in orange and Threat Level 3 in red). The purple dotted line represents the threshold for acceptable risk. From Fig. 9 the initial architecture is evaluated with respect to the first threat environment (Threat Level 1) and, at each successive iteration, the proposed architectures with progressively lower risk. With iterations that meets the risk threshold (denoted by the green dot to the left of the plot). Then the threat environment shifts to Threat Level 2 and Finally, the threat

environment shifts again to the highest threat level, Threat Level 3, and the system re-evaluates the architecture. As the architecture no longer satisfies the threshold, the search process is repeated.



VI. CONCLUSION

This paper proposes network segmentation architectures in the form of use cases that are optimized for security and information loss. Here we employed artefact based hypothetical results that shows the combination of computational intelligence with simulation modelling to construct and evaluate the architectures, and adapt to changing threat levels. Results highlight the system's ability to segmentation architectures to meet an acceptable threshold of risk for a given threat environment and adapt to changing threat levels by the network. This work addresses the need for systems that leverage the architectures to generate optimal/near-optimal cyber security decisions and reduce the information loss in real time. Future work is focused on synthesis, automation and composition of segmentation policies. Network security can be achieved by network segmentation controls that are extended to accommodate productive and competent cyber security potentials. The final realisation of virtual security is to lend an upper hand to businesses so that cyber criminality lies on the future advances of open standards across the ICT infrastructure spectrum. The higher maturity in network virtualisation and security policy interrogation is defined by efficiency in security operations and conformance to relevant regulations and Effective security controls.

REFERENCES

[1]. KL Thomson, R von Solms, L Louw. Computer Fraud & Security 2006 (10), 7-11, 2006. 135, 2006. "A business approach to effective information technology risk analysis and management". S Halliday, K Badenhorst, R Von Solms. Information Management & Computer.

[2]. November 5, 2010"Build Security Into Your Network's DNA: The Zero Trust Network Architecture "by John Kindervag with Stephanie Balaouras and Lindsey Coit

[3]. J Am Med Dir Assoc. 2015 Aug 1;16(8):682-9. doi: 10.1016/j.jamda.2015.03.010. Epub 2015 Apr 11.Associations Between Ankle-Brachial Index and Cognitive Function: Results From the Lifestyle Interventions and Independence for Elders Trial.Espeland MA1, Newman AB2, Sink K3, Gill TM4, King AC5, Miller ME6, Guralnik J7, Katula J8, Church T9, Manini T10, Reid KF11, McDermott MM12; LIFE Study Group.

[4]. A Nature-inspired Decision System for Secure Cyber Network Architecture Neal Wagner, Cem S¸. Sahin¸, Jaime Pena, and William W. Streilein MIT Lincoln Laboratory Lexington, MA, USA

[5]. S. Frei et al., Modeling the Security Ecosystem - The Dynamics of (In)Security. Boston, MA: Springer US, 2010, pp. 79–106.

[6]. (2013) Apt1: Exposing one of china's cyber espionage units. [Online].Available: http://intelreport.mandiant.com/.

[7]. Strom, D 2015, 'NEW RULES FOR SECURING YOUR VIRTUAL INFRASTRUCTURE', Information Security, 17, 10, pp. 9-14, Computers & Applied Sciences Complete, viewed 15 March 2016.

[8]. Chang, J, Ho, P, & Chang, T 2014, 'Securing bYOD', IT Professional, 16, 5, p. 9-11, viewed 9 May 2016.

[9]. Furbush, James (2012),' BYOD strains corporate wireless network bandwidth" Available at http://searchmobilecomputing.techtarget.com/news/2240118466/BYOD-strains-corporate- wireless-network-bandwidth, Accessed 9 May 2016.
[10]. Kiravuo, T, Sarela, M, & Manner, J 2013, 'A Survey of Ethernet LAN Security', IEEE Communications Surveys And Tutorials, viewed 20 June 2016.
[11]. Khoussainov, R, & Patel, A 2000, 'LAN security: problems and solutions for Ethernet networks', Computer Standards & Interfaces, 22, pp. 191-202, viewed 20 June 2016.
[12]. Seabrook, J 2013, 'Network Insecurity', New Yorker, 89, 14, pp. 64-70, viewed 26 June 2016.
[13]. Markowsky, G. and Markowsky, L., 2011. Using the castle metaphor to communicate basic concepts in cybersecurity education. In Proc. SAM (Vol. 11, pp. 507-511), viewed 26 June 2016
[14]. Sheldon, T (2001), 'Firewall', available at http://www.linktionary.com/f/firewall.html, accessed 28 June 2016.
[15]. Thierer, AD 2015, 'THE INTERNET OF THINGS AND WEARABLE TECHNOLOGY: ADDRESSING PRIVACY AND SECURITY CONCERNS WITHOUT DERAILING INNOVATION', Richmond Journal Of Law & Technology, 21, 2, pp. 1-118, Index to Legal Periodicals & Books Full Text (H.W. Wilson), viewed 4 July 2016.
[16]. Turull, D, & KTH, S 2016, 'Network virtualization as enabler for cloud networking', Triatic, SwePub, viewed 15 September 2016.
[17]. Smith, MS 2015, 'Protecting Privacy in an IoT-Connected World', Information Management Journal, 49, 6, pp. 36-39, viewed 21 September 2016.
[18]. Elkhodr, M, Shahrestani, S, & Cheung, H 2016, 'A Middleware for the Internet of Things', arXiv, EBSCOhost, viewed 21 September 2016.
[19]. Turull, D, & KTH, S 2016, 'Network virtualization as enabler for cloud networking', Triatic, SwePub, viewed 15 September 2016.
[20]. Kuliesius, F, & Dangovas, V 2016, 'SDN enhanced campus network authentication and access control system', International Conference On Ubiquitous And Future Networks, ICUFN, 2016- August, ICUFN 2016 - 8th International Conference on Ubiquitous and Future Networks, p. 894- 899, viewed 8 September 2016.
[21]. Mijumbi, R, Serrat, J, Gorricho, J, Bouten, N, De Turck, F, & Boutaba, R 2016, 'Network function virtualization: State-of-the-art and research challenges', IEEE Communications Surveys And Tutorials, 18, 1, p. 236-262, viewed 15 September 2016.
[22]. Data Centre security design guide by Mike storm
[23]. IEEE 802.1Q-2011, 1.4 VLAN aims and benefits
[24]. Robson de Oliveira Albuquerque,Luis Javier García Villalba,Ana Lucila Sandoval Orozco, Fábio Buiati,and Tai-Hoon Kim "A Layered Trust Information Security Architecture" Published online 2014 Dec doi: 10.3390/s141222754 in MDPI.

Dr.Ramesh K "Network Segmentation strategies to articulate new method to Address Growing Information Security Concerns.. IOSR Journal of Engineering (IOSRJEN), vol. 08, no. 6, 2018, pp. 43-52.