Detection and Control of Malicious activity and Digital Forensic in BYOD

Md Iman Ali, Sukhkirandeep Kaur

Abstract: Enterprises are focusing greatly on Bring your own Device strategy since 2009 when Intel Adopted Bring your Own Device phenomena for the employees and later on this became more popular. Since 2012 exponential growth of BYOD services in the corporate environment also observed for providing an alternate method of working environment using employee personal device, however due to increased security threats and malicious activities occurring in BYOD environment most of the corporate are facing major challenges in enabling BYOD program. Increased Cyber-attack fragmenting the business ecosystem and cyber security becomes business survival factor. Increased amount of cyber attack in BYOD environment has created a major road block in adoption of BYOD. Existing security models of BYOD implementation, tools and techniques does not match the pace of security landscape at which cyber threats are growing. Moreover existing detection and control techniques of malicious activities in BYOD environment are not sufficient for cyber forensic investigation post an attack. By creating a secured model of BYOD environment security risk can be reduced. During this research Two different approach was followed to mitigate these risks. First approach was reverse adoption of encryption technique used to protect corporate network from BYOD environment. In 2nd approach malicious activity detection and protection mechanism explored with cyber forensic readiness in BYOD environment. Significant positive result observed to protect the corporate network infrastructure from untrusted BYOD traffic using GetVpn in cluster deployment. 2nd phase of this research has resultant to build digital forensic readiness BYOD model. Building a cyber secured model of BYOD cluster deployment ecosystem has contributed to reduce the risk of cyber threat. And detection of malicious activities has contributed in building a cyber forensic BYOD infrastructure to provide cyber confidence BYOD services.

Keywords: Cyber Security, Digital Forensic, BYOD, Encryption.

1. INTRODUCTION

Bring your own device (BYOD) is connecting non trusted external devices in Corporate network infrastructure. Creating alternate method of working model to increase employee productivity and employee satisfaction strategy project running almost majority of the organization. Predicted adoption of BYOD services by 2022[1] are expected to increased by 75% as per the study conducted by Gartner from 35% in 2018 which is almost double of the growth. By 2021[2] maximum organizations are expected to use IoT, 94% of the organization will adopt IoT as per Microsoft report. This pace of growth are also reason for increasing the cyber security risk and data leakage incident. Unmanaged devices might not be following the standard security practice, may not follow line of defense against malicious content[3]. Risk of malicious activities are also increased in BYOD environment as the devices increased. A Study concluded 62% of digital incidents are triggered by inside users either by intention or by unintentional [4]. Md Securing BYOD infrastructure by using multiple tools and technique always been explored but due to increased amount of threat landscape and advancement of threat tools and techniques always there is a need of advancement of further research.

1.1 PREVIOUS STUDY:
1.1A CERTIFICATE BASED SECURED AUTHENTICATION MODEL: Certificate based Hybrid authentication model with 3 tier captcha collective model of authentication was one of the successful model[5]. Secured authentication model of framework was explored for secured authentication and onboarding of BYOD internal users[6]. Also dual factor authentication method has been analyzed for secure communication. using SceTher Tool and computerized dual factor authentication mechanism is tested for automatic verification tool with secured approach in IoT[7]. Secured model of authentication with 802.1x authentication was explored implementing network security control[8].

1.1B BYOD ENCRYPTION SECURITY MODEL: Encryption technology is used to encrypt corporate data in mobile devices[9]. Encryption/cryptographic method of network security is an option in a recent research in 2019 explored end to end encryption is secured model [10]. Denial-of-Service Attack (DDoS) attack in remote access connection and network traffic gets congested remote site traffic authentication traversing is a challenge[11] and explored IDS/IPS are essential components studied.

1.1C BYOD BLOCK CHAIN AUTHENTICATION: Advance level BYOD block chain technique authentication with self service portal was explored where authentication process reduce the risk of data leakage and threat due to unauthorized access and thus secured the core network infrastructure from attack[12]. Multi factor block chain secured model of block chain cryptographic authentication model was explored for building enhanced secured BYOD environment[13].

In a cluster deployment of BYOD environment pre-authentication traffic traverse through corporate MPLS network where corporate network and BYOD network converge to reach the destination for authentication server. In this scenario there is a major risk of security breach. First objective of this research is to secure the corporate network from BYOD traffic while traversing through same corporate network using reverse adoption of BYOD traffic encryption. In our 2nd approach post authentication of BYOD users detection of malicious activities are examined and control mechanism is explored.

Second objective of the research is to detect the malicious activities and enable a control mechanism to protect the
Detection and Control of Malicious activity and Digital Forensic in BYOD

BYOD infrastructure and corporate network.

II. DESIGN AND IMPLEMENTATION METHODOLOGY

During the research we have explored 2 different approach for securing Network and malicious activity detection for forensic investigation.

In first approach corporate network infrastructure is protect from BYOD untrusted network.

2nd approach was taken for detection of malicious activities and protection mechanism was analyzed.

2.1 BYOD AUTHENTICATION TRAFFIC ENCRYPTION TO REDUCE CYBER RISK

Traffic encryption [14] was used as first level of mitigation[15] to reduce cyber threat risk. Authentication traffic from branch location to central location is encrypted using Get VPN to secured the communication between branch untrusted BYOD traffic to central location authentication destination. Get VPN was used to secure the traffic over MPLS [16] which encrypt the communication and protect the internal network from threat[17] to reduce the attack from BYOD users.

![Image: BYOD Authentication untrusted traffic over MPLS using Getvpn.](image)

Figure 1: BYOD Authentication untrusted traffic over MPLS using Getvpn.

Additional components used for this testing for authentication traffic between branch location to central location.

Table 1: components for BYOD traffic

| Sl.no | Components         | Purpose                                      |
|-------|--------------------|----------------------------------------------|
| 1     | MPLS connectivity  | Authentication traffic flow between branch and central location. |
| 2     | Internet link      | Local exit for BYOD internet traffic.         |

IP address used during the test for pr-auth and post auth traffic[6] as per solution of “BYOD Secured Framework”

Table 2: IP address schema

| Sl No | Pre-auth subnet   | Post-Auth subnet | Note                                    |
|-------|-------------------|------------------|-----------------------------------------|
| 1     | 192.168.x.x/16    | 172.28.x.x/16    | Segmented IP address used for major subnet |

Initial authentication traffic was routed from Branch location to Central location encrypted using Getvpn. Implementation of getvpn was done as per standard guideline[16]. Encryption acl configured on Getvpn Key server as below.

Table 2.1: Encryption policy on Key server

| Group Name: BYOD-Test | Configured ACL: | KEK POLICY (transport type : Unicast) spi : 0xC68CC7816905D0DA41A7DF6A218D6A0A              |
|-----------------------|-----------------|-------------------------------------------------|
|                       | access-list LAN deny udp any port = 848               |
|                       | access-list LAN deny udp any port = 848 any          |
|                       | access-list LAN deny tcp any port = 179              |
|                       | access-list LAN deny tcp any port = 179 any          |
|                       | access-list LAN permit ip 192.168.0.0 0.0.255.255     |
|                       | 192.168.0.0 0.0.0.255.255                            |

In the policy 192.168.x.x network is encrypted for traversing through corporate MPLS network along with corporate trusted IP segment. Policy configured on Key server for encryption of BYOD traffic over MPLS for Group member.

Table 3: Getvpn GDOI security policy

| Key Server Policy: | For group GETVPN-Test (handle: 2147483650) server 10.1.1.1 (handle: 2147483650): |
|--------------------|---------------------------------------------------------------------------------|
| # of teks : 1     | Seq num : 6                                                                      |
| KEK POLICY (transport type : Unicast) spi : 0x80B694D2                         |
| management alg : disabled encrypt alg : 3DES                                    |
| crypto iv length  : 8 key size : 24                                            |
| orig life(sec)     : 86400 remaining life(sec) : 66918                         |
| sig hash algorithm : enabled sig key length : 294                              |
| sig size           : 256                                                         |
| sig key name       : HO-KS-KEY                                                    |
| TEK POLICY (encaps : ENCAPS_TUNNEL) spi : 0x80B694D2                            |
| access-list        : BYOD                                                        |
| transform          : esp-aes esp-sha-hmac                                        |
| alg key size       : 16                                                          |
| sig key size       : 20                                                          |
| orig life(sec)     : 3600 remaining life(sec) : 2624                            |
| tek life(sec)      : 3600                                                        |
| elapsed time(sec)  : 976                                                          |
| override life (sec): 0                                                           |
| antireplay window size: 64                                                        |

For group GETVPN-Test (handle: 2147483650) server 10.1.1.2 (handle: 2147483651):

As shown above BYOD traffic is encrypted and encapsulated with TEK Policy. During the research BYOD environment was setup using multiple hardware/equipment. Design of BYOD with Getvpn for Guest traffic simulated in this research was as show below.
Detection and Control of Malicious activity and Digital Forensic in BYOD

After implementation observed enforced encryption policy for BYOD traffic on GM

Table 5.2: enforced policy of getvpn on GM

| GETvpn-GM | show crypto ipsec sa
|------------|--------------------------
| interface: GigabitEthernet0/0/0
| Crypto map tag: GetVPN-Test, local addr 172.1.1.1
| protected vrf: (none)
| local ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
| remote ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
| Group: GETVPN
| current_peer 0.0.0.0 port 848
| PERMIT, flags={}

During this research Getvpn infrastructure was used using 2 remote branch and 1 data center central. Key server was placed in same network for security policy management. AAA server was placed in central site. Authentication server was used as Identity service Engine. External firewall was used during the test as Checkpoint firewall.

III. RESULT AND ANALYSIS

3.1 PROTECTING CORPORATE NETWORK FROM BYOD UNTRUSTED AUTHENTICATION TRAFFIC

In this research protection of the network has been explored using GetVPN. As shown in fig-2 BYOD authentication traffic traversing from branch network to Data center over corporate MPLS network where AAA server placed are encrypted and segregated. Below result shows the encryption.

Encryption acl received on Getvpn GM as below

Table 5.1: Enforced policy ACL on GM (Figure 1 GM)

| GETvpn-GM | show crypto gdoi gm acl
|------------|--------------------------
| Group Name: GETVPN
| ACL Downloaded From KS 10.1.1.2:
| access-list deny udp any any port = 848
| access-list deny udp any any port = 848 any
| access-list deny tcp any any port = 179
| access-list deny tcp any any port = 179 any
| access-list permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

After traversing the network authentication traffic has reached corporate data center firewall where central authentication server is placed.
Detection and Control of Malicious activity and Digital Forensic in BYOD

Below record was captured during the research where authentication traffic on port 8443 reflects during onboarding of BYOD users

Figure 3: Pre-auth traffic logs towards AAA from Firewall logs (Fig-2, index 2-Firewall)

Table 6: BYOD onboarding Traffic logs from Firewall (Figure 2, Index 2 Firewall)

| Id:                     | 0abca241-0100-00c0-5db2-92bf0037002c |
| Marker:                 | @A@@B@1571941803@C@3224900            |
| Log Server Origin:     | 10.5.5.5                              |
| Time:                   | 2019-10-25T06:14:23Z                  |
| Interface Direction:   | outbound                              |
| Interface Name:        | eth3                                  |
| Connection Direction:  | Internal                               |
| Id Generated By Indexer: | false                         |
| First:                  | true                                  |
| Sequencenum:           | 110                                   |
| Service ID:            | tcp8443                               |
| Source:                | 192.168.112.129                       |
| Source Port:           | 33541                                 |
| Destination:           | 192.168.106.19                        |
| Destination Port:      | 8443                                  |
| IP Protocol:           | 6                                     |
| Context Num:           | 1                                     |
| Action:                | Accept                                |
| Type:                  | Connection                            |
| Policy Name:           | Standard                              |
| Policy Management:     | ResearchMGMT                          |
| Db Tag:                | [F49A528D-FD8D-9749-806A-501AA6B55588] |
| Policy Date:           | 2019-10-18T10:12:30Z                  |
| Blade:                 | Firewall                              |
| Origin:                | ResearchFirewall                      |
| Service:               | TCP/8443                              |
| Product Family:        | Access                                |
| Logid:                 | 0                                     |
| Access Rule Name:      | CNA                                   |
| Access Rule Number:    | 53                                    |
| Policy Rule UID:       | 18547ecc-3565-41ed-b234-97381e3c9a52   |
| Layer Name:            | Network                               |
| Interface:             | eth3                                  |

Table 7: Traffic snip details

| Sl No | Source          | Destination          | Attack type |
|-------|-----------------|----------------------|-------------|
| 1.    | External        | BYOD Infrastructure  | Critical    |
| 2.    | Internal        | External network     | Critical    |

3.2 DETECT AND CONTROL CRITICAL ATTACK IN BYOD AND FORENSIC ANALYSIS

In this research we have done in-depth analysis of BYOD security infrastructure. During the traffic analysis of critical attack in nature was detected using wireshark. In this phase we captured 2 different critical categories of traffic as (a) Attack from External source to BYOD infrastructure (Internal) and again (b) attack traffic from Internal to External

Traffic captured as below

Table 7: Traffic snip details

3.2.A ATTACK FROM EXTERNAL TO INTERNAL

Here traffic is captured on Internal router shown in fig-3 (index 11). We snipped the traffic logs from router LAN side interface to detect traffic. Critical attack category traffic has been detected. Malicious activity was captured using wireshark [18] logs and analyzed. Multiple packets are captured and filtered out a particular packet from wireshark. Traffic source from 129.211.113.210 which is an attack source IP in this case and the destination is 61.246.179.210. This packet is captured and the same is detected on figure 2 (index 2-external interface). The packet is http port 80 traffic. Packet captured are shown in below figure 4. Http header is checked of this packet and later same packet is analyzed on Checkpoint firewall.

Figure 4: Packet captured using wireshark.(Interface of Fig2,Index 2)

The same packet when we checked on IPS blade of checkpoint firewall of the architecture shown in figure 2 (index 2). We have found the malicious traffic which critical attack in nature.
The category of attack is SQL Servers SQL Injection Evasion Techniques - ver 2[19] which was targeted to use commands on SQL servers by remote attackers by getting access. Forensic module details are also captured on checkpoint firewall which has detected the resource details targeted to access. Later this particular attack is blocked and evidence for this malicious activity was preserved on smart management server for further investigation as well without breaking chain of custody.

3.2.B ATTACK FROM INTERNAL TO EXTERNAL

As most of the time trusted users insiders are more vulnerable and 62% attack are from insiders[4]. So in this research internal traffic threat was analyzed and find evidence of the malicious activity. Same type of packet captured was conducted to find malicious traffic. This time packet was capture on internal interface of the firewall(Figure 2, 2) and filtered out a packet and analyzed in wireshark logs as shown below. This time return traffic was captured and investigated.

3.2.C APPLICATION LAYER MALICIOUS ACTIVITY FORENSIC

Application layer threat was analyzed and captured on ingress interface of the firewall shown in fig 3 (index 8) and below was the result traffic sourcing from one of the BYOD user having IP address of 172.28.35.205 to the destination 203.107.1.34.

Same packet was analyzed on the checkpoint firewall and found this was a serious malware category malicious activity. The forensic threat emulation was enabled on checkpoint firewall to detect the malicious activity and forensic logs was seen on this blade. Below result was found which again blocked using application control blade. As seen traffic sourcing from 172.28.35.205 destined to 203.107.1.34.
Detection and Control of Malicious activity and Digital Forensic in BYOD

IV. DISCUSSION

First objective of this study was to minimize the security risk in Cluster deployment of BYOD infrastructure using encryption method. In this study we have explored encryption mechanism adoption for BYOD traffic. While BYOD is deployed in cluster where authentication server is central and authentication traffic is coming from remote branch to central data center, BYOD traffic is traversing with corporate network. Organization MPLS network carrying traffic for both the network where risk is more. Second objective of this research was detection of malicious activity, then protect and explored the Forensic investigation of BYOD malicious traffic. Detection of Cyber attack in the BYOD environment is most critical task. Study on BYOD security risk in Airport Security which is a major risk of the country[21] due to BYOD. Also another study says BYOD might become “Bring your own danger”[22] if control security is not implemented and if not prepared for forensic investigation after an attack, so this study has a significant result of detecting malicious activity using application layer of detection mechanism.

4.1 CONTRIBUTION

Contribution of this research in BYOD infrastructure is securing corporate network from BYOD untrusted authentication traffic using reverse adoption of encryption mechanism for BYOD traffic not corporate MPLS. This method segregate traffic between corporate network and BYOD network from Branch to Data center. As a result security risk gets reduced. 2nd contribution of this research is to detect and protect malicious activities in BYOD infrastructure and forensic investigation using threat emulation.

4.2 FUTURE RESEARCH

Future research in this direction is to explore advance forensic investigation model inline with corporate Cyber Law. Detection of cyber attack in BYOD infrastructure forensic investigation model is on demand in the study, which can be further explored in details.

V. CONCLUSION

A secured authentication model is required to protect corporate network infrastructure and reduce cyber risk due to adoption of BYOD. In this paper we have presented a model of reverse adoption of encryption technique of BYOD traffic while traversing through corporate MPLS network. Segregated the corporate network from BYOD traffic using a reverse adoption of encryption mechanism. This makes the BYOD authentication traffic securely reaching the central AAA server without touching corporate network. Security risk is reduced using this encryption method and corporate network becomes risk free and provide Cyber secured BYOD environment.

Second part of the research has explored the detection of malicious activities and protect the BYOD infrastructure. 2nd part of the research has contributed to build digital forensic readiness BYOD infrastructure to conduct investigation post attack.

ACKNOWLEDGEMENT

The research, hypothesis, assessments and analysis articulated in this paper are those of the authors alone and not the organization with whom the authors are associated.

REFERENCES

1. H. Shetty, L. Unid-Farboud, and P. Arriandiaga, “Competitive Landscape: Managed Mobility Services,” p. 20.
2. “94% enterprises will use IoT by end 2021: Microsoft report,” https://www.livemint.com/.
3. Available: https://www.livemint.com/technology/tech-news/94-enterprises-will-use-iot-by-end-2021-microsoft-report-1565165449842.html. [Accessed: 08-Aug-2019.]
4. B. Tokuyoshi, "The security implications of BYOD," Network Security, vol. 2013, no. 4, pp. 12–13, Apr. 2013.
5. J. Collie, “A Strategic Model for Forensic Readiness,” Athens Journal of Sciences, vol. 5, no. 2, pp. 167–182, Jun. 2018.
6. U. Raj, “Certificate based hybrid authentication for Bring Your Own Device (BYOD) in Wi-Fi enabled Environment,” vol. 13, no. 12, p. 7, 2015.
7. "BYOD Secured Solution Framework," International Journal of Engineering and Advanced Technology, vol. 8, no. 6, pp. 1602–1606, Aug. 2019.
8. "International Journal of Scientific Research in Computer Science, Engineering and Information Technology," p. 7, 2018.
9. K. Allhardt and W. Shawkat, “Implement network security control solutions in BYOD environment,” in 2013 IEEE International Conference on Control System, Computing and Engineering, Penang, Malaysia, 2013, pp. 7–11.
10. P. K. Gajar, A. Ghosh, and S. Rai, “BRING YOUR OWN DEVICE (BYOD): SECURITY RISKS AND MITIGATING STRATEGIES,” p. 9, 2010.
11. K. Joshi, M. Pathak, S. Jose, S. Dahiya, and S. Jose, “"71) Applicant: Gigannon Inc., Santa Clara, CA (US),” p. 18.
12. M. Mahinderjit Singh, S. Sinjag, O. Ying San, N. H. A. Hassan Malim, and A. R. Mohd Shariff, “Security Attacks Taxonomy on Bring Your Own Devices (BYOD) Model,” International Journal of Mobile Network Communications & Telematics, vol. 4, no. 5, pp. 1–17, Oct. 2014.
13. F. Jamal, M. T. Abdullah, A. Abdullah, and Z. M. Hanapi, “BYOD Authentication Process (BAP) Using Blockchain Technology,” Control Systems, vol. 10, no. 11, p. 8, 2018.
14. F. Jamal, M. T. Abdullah, A. Abdullah, and Z. M. Hanapi, “Enhanced Bring Your Own Device (BYOD) Environment Security based on Blockchain Technology,” International Journal of Engineering, p. 6.
15. M. Ratchford, P. Wang, and R. O. Sheit, “BYOD Security Risks and Mitigations,” in Information Technology - New Generations, vol. 558, S. Latifi, Ed. Cham: Springer International Publishing, 2018, pp. 193–197.
16. M. P. Souppaya and K. A. Scarfone, “Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security,” National Institute of Standards and Technology, NIST SP 800-46R2, Jul. 2016.
17. “Cisco SAFE Reference Guide,” p. 354.
18. “Wireshark · Go Deep.” [Online]. Available: https://www.wireshark.org/. [Accessed: 06-Oct-2019].

19. “Search: SQL Servers SQL Injection Evasion Techniques - ver 2 | Check Point ThreatPoint.” [Online]. Available: https://threatpoint.checkpoint.com/ThreatPortal/search?pattern=SQL-\%20Servers\%20SQL\%20Injection\%20Evasion\%20Techniques\%20-%20Ver\%202&type=all&page=0&utm_source=cp_logs. [Accessed: 19-Oct-2019].

20. “Search: Unzip Extra Field Uncompressed Size Buffer Overflow | Check Point ThreatPoint.” [Online]. Available: https://threatpoint.checkpoint.com/ThreatPortal/search?pattern=Unzip-%20Extra%20Field%20Uncompressed%20Size%20Buffer%20Overflow&type=all&page=0&utm_source=cp_logs. [Accessed: 19-Oct-2019].

21. G. Suciu, A. Scheianu, I. Petre, L. Chiva, and C. S. Bosoc, “Cybersecurity Threats Analysis for Airports,” in New Knowledge in Information Systems and Technologies, vol. 931, A. Rocha, H. Adeli, L. P. Reis, and S. Costanzo, Eds. Cham: Springer International Publishing, 2019, pp. 252–262.

22. P. Beckett, “BYOD – popular and problematic,” Network Security, vol. 2014, no. 9, pp. 7–9, Sep. 2014.

AUTHORS PROFILE

Md Iman Ali is a Research scholar, in the department of computer application at Lovely Professional University, Punjab, India. He has completed MCA and DOEACC “A” level. As a professional certification he is CCIE Lab certified. He is working as an Associate Director, Technology, KPMG India. His research interest area include BYOD secured solutions, Digital Forensic, Cyber Forensic, Cyber security, SD-WAN Security, Cloud Security and Smart city Cyber Forensic.

Dr. SukhKirandeep Kaur, is an assistant professor in Department of Computer Science and Engineering, Lovely Professional University, Phagwara. She received her PhD from National Institute of Technology, Srinagar. She has authored over 10 papers in international journals and conferences. Her research interest includes Wireless Sensor Networks, Internet of Things and Artificial Intelligence, Cyber Security, Cyber Forensic, BYOD.