ISSN 2278-3091
Volume 8, No.6, November – December 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse103862019.pdf
https://doi.org/10.30534/ijatcse/2019/103862019

An Extensive Study of Honeypot Technique

Ahood h. Althobaiti[1], Mohammed A. AlZain[1], Jehad Al-Amri[1], Mohammed Baz[1], Mehedi Masud
[1]College of Computers and Information Technology, {ahood.a1@tvtc.gov.sa, m.alzain@tu.edu.sa, j.alamri@tu.edu.sa, mo.baz@tu.edu.sa, mmasud@tu.edu.sa}

ABSTRACT

Honeypots have been utilized broadly for more than two decades. Notwithstanding, their improvement is infrequently went with a comprehension of how assailants can distinguish them. Further, our comprehension of successful avoidance methodologies that counteract the identification of honeypots is constrained. We present an arrangement of honeypot attributes just as honeypot discovery avoidance methodologies which limit the recognition paces of honeypots. We likewise give suggestions to future honeypot programming which is progressively versatile, secluded and consolidate a dynamic insight structure.

Key words : About four key words or phrases in alphabetical order, separated by commas.

1. INTRODUCTION

Honeypot is defined as cited in [1] is as follows: “A honeypot is a resource whose value is being in attacked or compromised. This means, that a honeypot is expected to get probed, attacked and potentially exploited. Honeypot do not fix anything. They provide us with additional, valuable information” [2] [43]. Honeynet a nectar net is definitely not a solitary framework, yet a system of honeypots frameworks intended to catch programmers inside exceptionally controlled and observed systems [2] [3] [44].Highlight a section that you want to designate with a certain style, then select the appropriate name on the style menu. The style will adjust your fonts and line spacing.

Honeypot is a security asset whose worth is being filtered, assaulted or caught [1]. Through this defining we can understand that, build a honeypot system’s aim is to let unauthorized users to detect and attack it. Honeypot itself does not fix any problems, it only provides additional, valuable information for us, and will not provide real valuable service to the outside world. What’s more, all attempts to access the honeypot is considered suspicious because of any attempt behavior which would connect honeypot can be considered a potential attacks, and the core value of the honeypot is to monitor, detect and analyze these attacks. Honeypot will not directly improve computer network security, but as an active defense technology it cannot be replaced by other security strategy[4].

According to the degree of interaction honeypot can be divided into low-interaction, medium-interaction and high-interaction honeypots [1].

2. HONEYPOT SYSTEMS

Honeypot frameworks are intended to draw in interlopers. These frameworks are utilized as a snare for unapproved correspondence in systems. Likewise, honeypot frameworks are utilized to find out about interloper conduct and interruption designs. With utilizing honeypot, after impedance, orchestrate chiefs or security specialists can pick how the aggressor prospered, divert coming about assaults, and see security vulnerabilities in the what's more, perceive security vulnerabilities in the system. Other than recognizing the various instruments used by programmers [5], honeypot innovation can likewise recognize the informal communities of gatecrashers by deciding the connections among interlopers [6].

There are a few kinds of honeypot frameworks dependent on the measure of cooperation. Honeypot is isolated into three social affairs, as low, focus and high-participation.

2.1 Low Interaction Honeypot

These kinds of honeypot are restricted in their level of communication. These frameworks really mimic administrations and working frameworks. In these frameworks, gatecrasher's exercises are constrained to the degree of imitating by the honeypots [5]. Low Interaction honeypot speak to a framework which reenacts explicit conventions of TCP/IP model. it's the principle bit of leeway of low cooperation honeypot [7]. Figure 1 displays low interaction honeypots network. As it seen in Figure 1 honeypots reenacts the administrations & working framework.

2.2 High Interaction Honeypot

In high-connection honeypots, it is needed to pull in the gatecrashers by getting the genuine administrations run.

What's more, outer projects are utilized to screen the gatecrasher exercises. In this cooperation honeypot regard to low and center honeypot as the gatecrasher in association

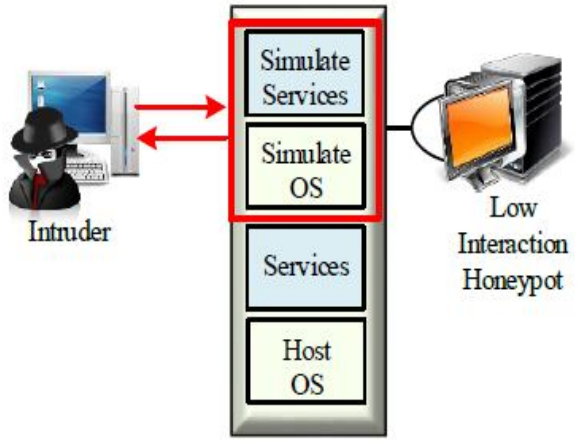

Figure 1: Low-Interaction Honeypots [6]

legitimately in the genuine framework to hold onto the honeypot hazard is unrivaled. To maintain a strategic distance from this issue on the firewalls a few safety measures can be taken. Other than the interloper is in correspondence with the framework legitimately can be assembled increasingly point by point data.

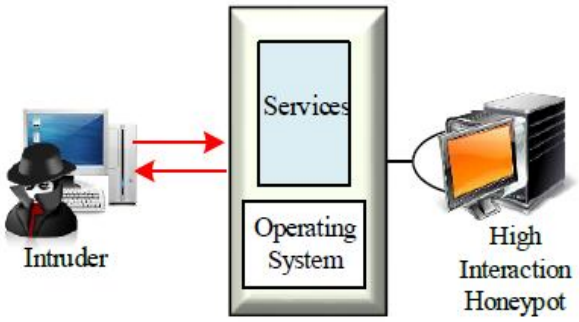

Figure 2: High-Interaction Honeypots [6]

High collaboration honeypot is all the more exorbitant & they need support all the more every now & again. Other than their points of interest they can be reason security vulnerabilities. The systems on which the high-association honeypots are utilized ought to be detached totally and all security safety measures additionally ought to be accepted generally as the interloper in collaboration with genuine framework can infiltrate to honeypot and seize the framework so new security dangers can be happened. As it displays in Figure 2 , high interaction honeypot is genuine PC frameworks with explicit genuine vulnerabilities [7] [6] [45].

3. HONEYPOTS COMMUNICAT WITH IPS/IDS

Honeypots framework for IDS and IPS frameworks is shown in Figure 3. The investigations in late writing show that the interruption discovery frameworks are us related to honeypot frameworks arrangement. Subsequently it very well may be recognized already obscure, new assaults.

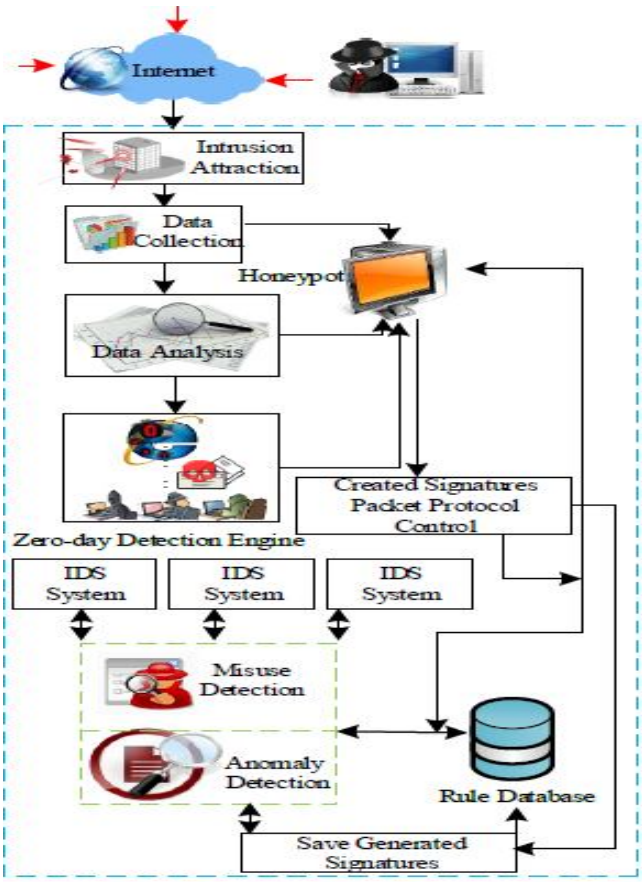

Figure 3: Honeypots with IDS/IPS [6]

Honeypot bring their quality from their vulnerable alternative [8]. To frame on their security defenselessness or mimic the security powerlessness reaction and furthermore both to stand out a hive honey bee to make nectar and as a snare stand out of the gatecrashers, give them to assault. Since they don't have genuine and noteworthy data on them they don't turn into a risk in genuine terms. Not at all like the other system and data security types of gear like interruption recognition frameworks and firewalls, honeypots are not utilized for a particular issue arrangement [9].

4. HONEYPOTS SIMPLE SCENARIO

In any occasion problematic, a honeypot is a preferred position that is used to perceive and check endeavors of unapproved utilize and access of system. It's worth is found in its exploitative state [10]. The longing was that attacked determination work together with the honeypots specialists revealing their whereabouts and objective., the data expanded through this strategy can use to uncover such vulnerabilities or help limit risk related with an assailant's specific ambush destinations, Antagonistic honeypots fuse honeypots including drive-by-download [11] [12]. Honeypot

is additionally utilized in organize domains that can't be commonly sufficiently checked by mastermind watching instruments. For example, when a delegate's framework get to affirmations are gained by a remote attacker (e.g., Secure Shell (SSH) accreditations), interference area structures that are routinely put near the edge switch of a framework can't inform security specialists about the exercises with respect to the aggressor. A honeypot, in any case, can exhibit the exchange off of the agent's record if the attacker tries to connect with it by methods for the specialist's workstation. A case of this is introduced on Figure 4 [13].

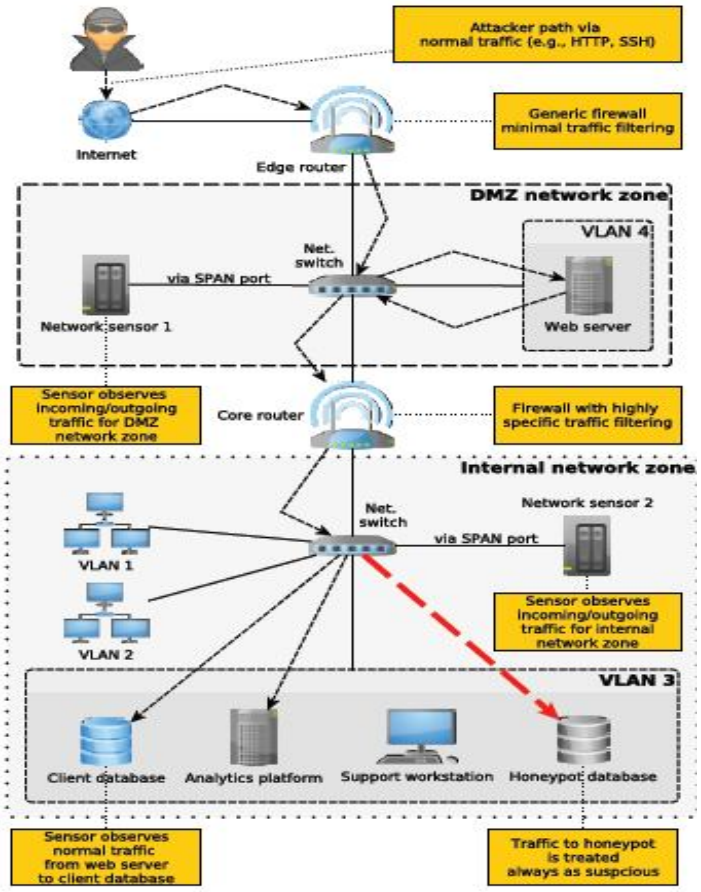

Figure 4: A honeypot situation on a system [6]

5. HONEYPOT CHARACTERISTICS

Different kinds of honeypots have been produced for an assorted arrangement of utilizations. Some are increasingly nonexclusive though some are exceptionally explicit attributes, for example, the capacity to imitate a specific system encryption[14] [15] :

1) Objective: There are two primary categories for honeypots:

Production and research [16] Research honeypot is utilized to produce danger knowledge about assailants. They are frequently put in a system's interestingly; creation honeypots are regularly put close to security resources to fill in as pointers of compromise (IOC) for inner just as outer dangers. Basically, the usefulness of these honeypots are for alarming safeguards of an assault, and just restricted insight is accumulated about the assailant (in sharp appear differently in relation to look into honeypots). The most punctual antecedent of generation honeypot are checked darkness (the unused IP address area in a nearby system)[17].

2) Loyalty: Honeypot can be portrayed dependent on the degree of communication that they permit among them and the assailant. Low association honeypots take into consideration communications with them just for a brief timeframe.

3) Implementation: A honeypots usage includes the utilization of programming, equipment or cross breed. Equipment honeypots can change from normal PCs to particular Supervisory Control and Data [18] .

4) Scalability: Versatility insinuates the limit of a honeypot or parts thereof corresponding. This trademark ends up being particularly noteworthy with the ascent of botnets similarly as the general addition in the amount of cyberattacks and state performers that hope to attack affiliations [19] [20]. Different honeypots created have concentrated on dealing with a huge number of simultaneous associations [13, 21].

6. HONEY POT AS A SERVICE

Honeypot is a counterfeit system that achieve the same task like the real one inside the production system but honey pot has no production value so even if it is compromised by the attacker the real infrastructure is not affected in any way to be an original valuable data to an attacker because it creates an emulated environment which consists of fake file system, fake services. Honey Pots can gather smaller, prominent-value, datasets because they log illicit activity only and they do not need acknowledged attack signatures, unlike IDS. A legitimate cloud user may want to learn more about attacker’s profile, attacker’s interest in his resource. A cloud [22, 23] user may want to collect suspicious activity [24, 25] related to his system on cloud [26] or his system image. A cloud user may want to detect intruder’s technique to intrude and may want to determine vulnerabilities in the real system. Cloud users may want a security service that can keep the track of the illegitimate access and login attempts to his system inside cloud [27, 28] and can maintain detailed interaction logs after successful illegal penetration into his system [29-31]. A cloud client may need a checking arrangement which can screen criminal behavior and early caution about its essence and this should be possible by a cloud nectar pot (see Figure 5). Either client himself can execute nectar pot in cloud condition that can verify client's genuine example. Or on the other hand generally specialist co-ops can furnish with the nectar pot administration to the cloud clients. In the latter case client should buy the nectar pot occasion from the cloud nectar pot specialist co-op and client need not to stress over the area , engineering and arrangement of the nectar pot for this

situation he should simply recognize the requirement for the nectar pot and buy an occurrence to verify his own framework from the vindictive activity [32].

Later on this detailed log and profile can be analyzed by the user, cloud security analyst, forensic department to gain more knowledge about attacker's capabilities, behavior, attacking pattern and techniques [33].

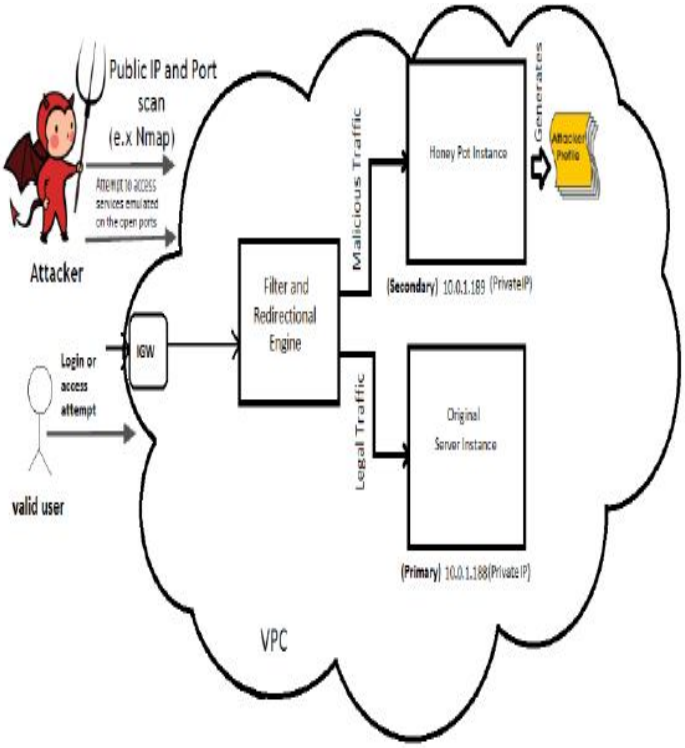

Figure 5: Honey Pot as a service in cloud [33]

Figure 6 depicts different access scenarios as 1,2,3 and 4. Let us consider these scenarios one by one. In case 1 real user try to access the real system by using system's public IP and authentication details since the configured security group of the real system opens port 22 for SSH service from My IP (i.e. the IP of the admin's system using which user/admin can log into system or access the system this My IP value is entered by the user/admin during the configuration of the security group) and filtration and redirection engine consists of details valid user IP for this real system to log in or access it so it simply redirects the request to the real system and this valid user successfully login to the system. In case 2 attacker who somehow managed to obtain or crack the user details and authentication details [34] (password/key) tries to login /access the real system but since attacker's IP is different and not known to the FRE also not configured in security group details of the real system for the SSH service so FRE simply redirects this request to the corresponding honey pot instance which is activated/purchased/set-up for this real system and attacker is now logged into honey pot instance. Even if attacker tries to nmap or scan IP range of cloud (as shown in case 3) then he may notice honey pot instance IP host is up and may try to access or login to this open host using its open ports in this case also he login/access to the honey pot instance which is intentionally made available or open as well as services on it are also open and ssh service is open from anywhere that is from internet. These ports are open in the security group configuration of the honey pot instance. Both in case 2 and 3 attacker accesses or interact with honey pot so honey pot instance generates short file about attacker's necessary details in order to alert the real user instantly as soon as the attack is detected on honey pot instance and sends this file information as a notification to the real user as shown in figure 6.

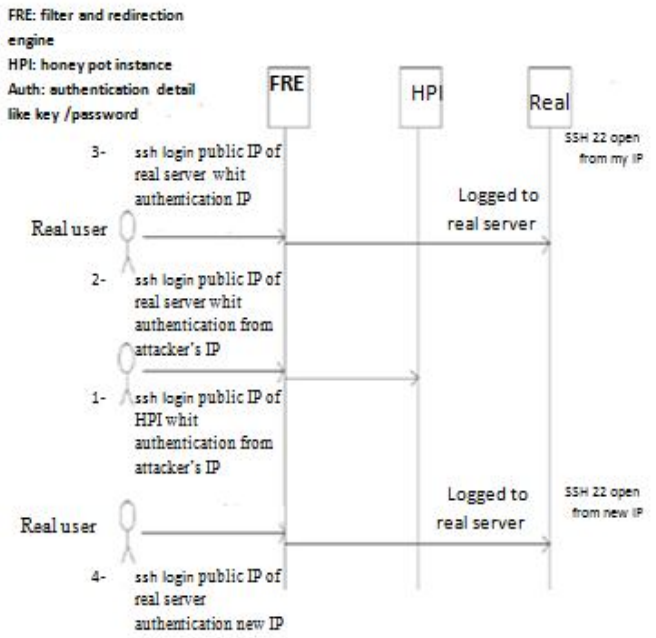

Figure 6: Different Access Scenarios[33]

Later on this user can see detailed logs or attacker's detailed profiles whenever he wants. In case 4 if real user changes his network then his system's IP through which he logs in or accesses the real server on cloud also changes so in order to successfully login to the real server (or system on cloud) he must change the security group settings and change old My IP value to this new IP value otherwise he won't be able to successfully login/access the server via this changed IP. Also this changed IP must be reflected in the corresponding entry for the real system inside the Filter and redirection engine (FRE) otherwise if this changed IP is unknown to FRE then every time when user would try to log in or access the real server (via the changed IP) then this user would be redirected to the honey pot instance and won't be able to access the real server [33] [35] on the captor, which immensely limits the believability of improving the first class data get (show the accompanying event 1). Take the ishing trap as an allegory of honeypot:

Event 1: the catch with bait can get guiltless and eager ish (as substance kids), anyway possibly will disregard to get perplexing ish (as moved software engineers);

Event 2: discrete the draw from the catch, & put it into a network, which will be progressively in secret, and besides will have higher ish get deficiency. At the point when the honeypot establishment is isolated, the plan consistently needs an orchestrator to engage them to work together.

7. HONEYPOT BASED ON CATEGORIES

7.1 Research Honeypot

This is the honeypot which is constrained by experts and is use to verify data of the software engineer society. these are constrained by a volunteer, non - advantage examine affiliation or an enlightening establishment to aggregate information about the points of view and methodologies of the dark that gathering concentrating on different frameworks. These honeypots don't build the estimation of a specific affiliation. Or maybe, they are used to investigate the threats affiliation stand up to and to make sense of how to all the more likely secure against those risks. This information is then used to verify against those threats. examine honeypot is complicated to send and keep up, get wide information and are used essentially by research, military or government affiliations.

7.2 Production Honeypots

This is the Honeypot controlled by the endeavors as a bit of framework security spine. This Honeypot work as early forewarning network. The goals of these Honeypot is to diminish the risks in adventures. It's gives the data to the manger about the attack already the genuine assault [7]. This is definitely not hard to use, get simply limited information, and are used on a very basic level by associations or undertakings; Production Honeypots are put inside the age arrange with other age servers by a relationship to improve their by and large state of security. Ordinarily, age Honeypots are low coordinated effort Honeypots, which are less requesting to send. They give less information about the attacks or aggressors than examine honeypot do. The inspiration driving an age honeypot is to assist moderate with hazarding in an association. The honeypot improves the wellbeing endeavors of an affiliation [3].

8. HONEYPOT CREATIONS ALGORITHM

Nectar gen: Generate High Quality Artificial Profiles that observe Association Rules mined from the slithered information. Profile Gen: A Method for Automated Generation of profiles for professional social network[36] [37, 38]. Virus Total: Scanned each Email using “Virus-Total” to find malware & spam. DCG(Discounted Cumulative Gain) : We utilized DCG Measure so as to quantify the viability of our system likewise in recognizing suspicious email got [35].

8.1 Keen Honeypot based E-Commerce Security Model

HONEYPOT the Keen-Honeypot expanded its capacity from straightforward following administrations to cutting edge basic leadership administrations. Customary Honeypot play out a government agent over aggressor's conduct and Intrusion exercises though Keen-Honeypot coordinated with Data Mining administrations to perform information building on caught information. Table 1 gives the understanding perspective about variety among the two Honeypots.

The proposed layered design needs an entwining between Honeypot framework and Data Mining framework [39].

Table 1: Difference between keen honeypot and honeypot[39]

Keen honey pot	Hone pot
Tracks behavior of attackers	Tracks behavior of attackers
Collect information about Log details Credential breached Security breach activities Intruder activities Hackers behavior	Collect information about Log details Credential breached Security breach activities Intruder activities Hackers behavior
Automatic analysis with data mining tools	Manual analysis intrusion statistics
Policy adjustments using decision support system	Manual adjustments of policies
More refined knowledge extraction using knowledge engineering techniques	Highly qualified professionals need to perform analysis on the site
Maintains trends of data about attacks in pre-processed format	Maintains only limited period of data in raw format only
Design time complexity is high but durability and performance is versatile	Design time complexity is low but performance is low Durability is inconsistent
High research activities with machine learning tools	Medium research activities with in- built static modules
learning tools	static modules

9. A HONEYPOT SYSTEM FOR WEARABLE NETWORKS

WEARABLE HONEYPOTS Figure 7 display the present architecture of wearable honeypot network. It comprises of 2 classes of elements: (1) the base location & (2) a few bait hubs. The fake hubs are uncommonly assigned hubs in the system whose lone errand is to be a piece of the honeypot framework. These are unique in relation to the remainder of the hubs in the BAN that really screen the client' wellbeing. We call these client wellbeing checking hubs as authentic hubs. To streamline the discourse, we will concentrate on a honeypot with one bait hub. The thought can be effectively reached out to various distraction hubs. Basically the base station advises the fake hub to send it (the base location) counterfeit sensor information as though the distraction hub were a real hub in the BAN. The base station definitely realizes what information will be sent and subsequently when it gets the phony information from the bait hubs, verifies whether they got information is same as what it anticipates. Any error is recognized as an endeavored trade off stacked information

that catches action changes, for example, sitting to standing, remaining to strolling and so forth. These give a few seconds of practical progress. Given that the hubs in a BAN have restricted stockpiling capacities we don't be able to store enormous amounts of accelerometer information. Subsequently, our pre-stacked accelerometer esteems may rehash sooner or later, which may bring about the information being recognized as phony by the foe who is listening in. Our way to deal with tending to this issue is to include a limited quantity of variable arbitrary commotion to the genuine accelerometer information before it is sent. For this they actualized a PRNG at both the base location and the fake hubs. The seed for the PRNG are sent as a feature of the coordination message. In this manner for any Acceleration information sent by the hub an exceptionally specific estimation of commotion (or counterbalance) is additionally affixed to the worth, the two of which are known to the base location. For this work they used Tiny MT PRNG [5]. They utilized Tiny MT in light of the fact that it is explicitly advanced for low capability gadgets, for example, detecting stages. Further, it has a time of 2127, and the coasting point numbers depend on equitably appropriated 32 piece whole numbers. In our usage TinyMT restores a skimming point r with the end goal that 0 _ r < 1. Given ascertain the counterbalance that we need to addition the Acceleration information. Here, sexually transmitted disease is the standard deviation of the Acceleration data. As our accelerometer information is in 3 tomahawks, the worth n is determined multiple times, once for every pivot. The estimation of n will be diverse for every pivot as the sexually transmitted disease esteem for the accelerometer information in every hub would be extraordinary. Figure 8 shows a model accelerometer information for strolling (spoke to as the size of the x, y, and z pivot Acceleration data) and the resultant random information (i.e., with counterbalance). It tends to be seen that randomized information doesn't rehash and remains in go inside the genuine action [40].

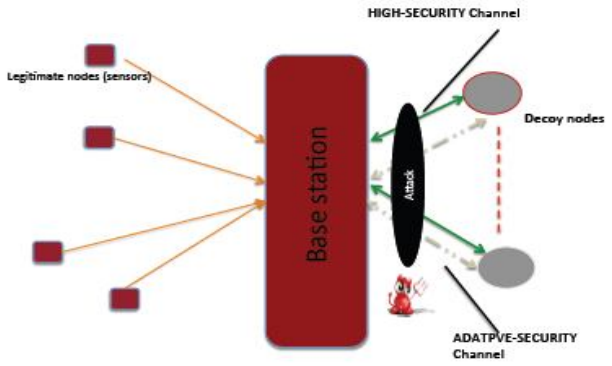

Figure 7: Wearable Honeypot System[3]

9.1 Honeypot Related Tools

The accompanying instruments expand the usefulness of honeypots or are intended to be utilized all the while with honeypots, for instance by making overseeing assignments simpler or identification executables naturally. Snare n-Switch The accompanying instruments expand the usefulness of honeypots or are intended to be utilized all the while with honeypots, for instance by making overseeing assignments simpler or identification executables naturally. Snare n-Switch The accompanying instruments expand the usefulness of honeypots or are intended to be utilized all the while with honeypots, for instance by making overseeing assignments simpler or identification executables naturally. Snare n-Switch The accompanying instruments expand the usefulness of honeypots or are intended to be utilized all the while with honeypots, for instance by making overseeing assignments simpler or identification executables naturally. Snare n-Switch [40]. was not a honeypot innovation in that capacity which just imitated FTP and HTTP administrations [42].

SCADA Honeypots "Supervisory Control and Data Acquisition (SCADA)"

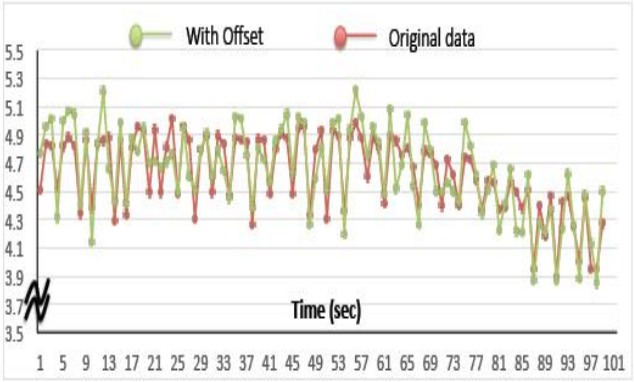

Figure 8: Honeypot Messages [41]

The writing specifies just scarcely any honeypots structured particularly for SCADA frameworks. Every one of them has a place with one of the two conventional honeypot classes [7]low-cooperation or high-connection. A high-connection honeypot for the most part utilizes a genuine asset and let an assailant to communicate with it, for example sign into the working framework. A low-cooperation honeypot works by imitating an asset or some piece of it making an assailant persuaded that he connects with the genuine asset. From one perspective the high interaction honeypot can initiate and along these lines identify any sort of assault against the specific asset while the productivity of the low-connection honeypot is constrained by the exactness of the imitating. Then again the low interaction honeypot is normally simpler to send and keep up and includes a lower danger of the honeypot to become traded off. One of the principal activities concerning SCADA honeypots is the SCADA Honeynet Project [8] that was begun in 2004. It means to make a SCADA honeypot dependent on the low interaction honeypot Honeyd. Honeyd reenacts various system conventions, for example, HTTP, SMTP and FTP however it very well may be reached out to recreate other system conventions utilizing basic contents. The designers of the SCADA Honeynet Project make various contents imitating a PLC gadget with

HTTP, FTP, Telnet and Modbus administrations. They additionally execute a Java applet that shows the status of a SCADA gadget. The venture being at the confirmation of idea arrange has not been created since 2005. In light of the SCADA Honeynet Project, Digital Bond [10].builds up a low-communication SCADA honeypot that imitates a prominent PLC gadget with SNMP and all administrations gave by the SCADA Honeynet Project honeypot. In addition, Digital Bond proposes a security component called SCADA Honeywall. It utilizes IDS with unique SCADA marks to identify known assaults and can prevent the outbound traffic from the undermined honeypots. The SCADA Honeywall can be set before either a low-communication honeypot like the one gave by Digital Bond or a high-cooperation honeypot utilizing for example a genuine PLC. Two diverse honeypot frameworks that have been utilized to gather measurable information about the SCADA cyberattacks are portrayed in [11] .One framework is a high-communication honeypot that uses a genuine PLC gadget and a physical server. The PLC imitates a temperature controller in a processing plant and has temperature, fan speed and light settings that can be adjusted. The physical server that is associated with the PLC works as a HMI and theoretically alters the PLC settings. The subsequent framework is a low-communication honeypot acknowledged on the Amazon EC2 cloud Web administration. One Amazon EC2 occasion is arranged as a Web page imitating the interface of a water pressure station. The Amazon EC2 occurrence associated with the first recreates PLC with DNP3 and Modbus administrations. Another low-cooperation SCADA honeypot copying PLC is displayed in [6]. It actualizes three correspondence conventions: Modbus, FTP and SNMP. In addition, it has an extraordinary module for recognizing testing action at the rest of the TCP ports. The honeypot likewise gives extra highlights, for example, sifting and collecting the security occasions. One of the most recent SCADA honeypots is Conpot [12] on which work started in 2013. Conpot is a low-association honeypot that at the default setup copies Siemens SIMATIC S7-200 PLC. It gives an execution of Modbus and SNMP. The reaction times of copied administrations can be misleadingly deferred to copy the conduct of a framework under consistent burden. Conpot can be conveyed with a custom HMI. It is an open source programming that can be effectively stretched out to copy increasingly complex SCADA frameworks. The task is effectively created under the support of the Honeynet Project. Toward the end, it ought to be noticed that adjacent to the previously mentioned run of the mill SCADA honeypots there are other increasingly broad honeypot arrangements that might be utilized to ensure SCADA frameworks. For instance, GhostUSB [13]is a low interaction honeypot that imitates a USB stockpiling gadget. In spite of the fact that it doesn't concentrate on the SCADA organize conventions it very well may be utilized in the SCADA framework to identify malware that proliferates through USB gadgets, for example Stuxnet. Finishing up, the SCADA honeypots known in the writing permit observing traffic associated with a HMI and average PLC gadgets. They center around the customary SCADA correspondence conventions, for example, Modbus, SNMP, FTP and HTTP. Considering that these conventions are excluded from the IEC 61850 standard none of the current SCADA honeypots is reasonable for present day SASs consistent with this standard [41].

10. CONCLUSION

In this paper, we have introduced a system for identifying new assaults in low-collaboration honeypot traffic. The proposed recognition technique is performed in two stages. Right off the bat, traffic streams are assembled dependent on IP locations and afterward PCA profile of honeypot traffic is manufactured. Also, new traffic vectors are anticipated onto the leftover space of the PCA assault model and the square expectation mistake (SPE) measurement is utilized to hail new attacks dependent on their enormous deviations from the assault model. The adequacy of the proposed procedure is demonstrated through the investigation of genuine traffic information from the Leurré.com venture and is approved using engineered assault information. Our assessment results show that our procedure is fit for recognizing various sorts of assaults with no earlier information on these assaults and the system has low computational necessity that makes it appropriate for online discovery frameworks. Future work incorporates computerizing the extraction of the identification parameters and improving the model capacity to adjust after some time to changes in the relationship structure. Another zone for development is to create assault classification models to help in finding the real class of the identified assaults naturally, which would facilitate the understandings.

REFERENCES

1. Spitzner, L., Honeypot-Definition sand value of honeypots. 2000.
2. Widodo, T., E.A. Muhsina, and B. Sugiantoro, Honeypot Log Analysis as a Network Security Support. IJID (International Journal on Informatics for Development), 2019. 2(1): p. 8-12.
3. Jafirkhan, M.A.M. and S. Mahadik, Data Security using Honeypot System. 2018.
4. Yao, J. and J. Chen. The Design of Website Security Defense System Based on Honeypot Technology. in 2016 2nd Workshop on Advanced Research and Technology in Industry Applications (WARTIA-16). 2016: Atlantis Press. https://doi.org/10.2991/wartia-16.2016.305
5. Chawda, K. and A.D. Patel. Dynamic & hybrid honeypot model for scalable network monitoring. in International conference on information communication and embedded systems (ICICES2014). 2014: IEEE. https://doi.org/10.1109/ICICES.2014.7033844
6. Baykara, M. and R. Daş, A survey on potential applications of honeypot technology in intrusion detection systems. International Journal of Computer Networks and Applications (IJCNA), 2015. 2(5): p. 203-208.

7. Malanik, D. and L. Kouril. Honeypot as the Intruder Detection System. in Proceedings of the 17th WSEAS International Conference on Computer, Kos (GR). 2013.
8. KARTAL, M., Ş. SAĞIROĞLU, and H.İ. BÜLBÜL, IPV6'da GüvenlikAçıklarınaGenelBirBakış. Politeknik Dergisi, 2013. 16(3): p. 119-127.
9. Gökırmak, Y., et al., IPv6 Balküpü Tasarımı. Tübitak Ulakbim, Ankara, 2011.
10. McGrew, R. Experiences with honeypot systems: Development, deployment, and analysis. in Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06). 2006: IEEE. https://doi.org/10.1109/HICSS.2006.172
11. Endicott-Popovsky, B., et al. Use of deception to improve client honeypot detection of drive-by-download attacks. in International Conference on Foundations of Augmented Cognition. 2009: Springer. https://doi.org/10.1007/978-3-642-02812-0_17
12. Zou, C.C. and R. Cunningham. Honeypot-aware advanced botnet construction and maintenance. in International Conference on Dependable Systems and Networks (DSN'06). 2006: IEEE.
13. Tsikerdekis, M., et al. Approaches for Preventing Honeypot Detection and Compromise. in 2018 Global Information Infrastructure and Networking Symposium (GIIS). 2018: IEEE.
14. Faragallah, O.S., et al., Block-based optical color image encryption based on double random phase encoding. IEEE Access, 2018. 7: p. 4184-4194.
15. AlZain, M.A. and J.F. Al-Amri, Application of Data Steganographic Method in Video Sequences Using Histogram Shifting in the Discrete Wavelet Transform. International Journal of Applied Engineering Research, 2018. 13(8): p. 6380-6387.
16. Mairh, A., et al. Honeypot in network security: a survey. in Proceedings of the 2011 international conference on communication, computing & security. 2011: ACM.
17. Sanders, C. and J. Smith, Applied network security monitoring: collection, detection, and analysis. 2013: Elsevier.
18. Abbasi, F.H. and R. Harris. Experiences with a generation iii virtual honeynet. in 2009 Australasian Telecommunication Networks and Applications Conference (ATNAC). 2009: IEEE. https://doi.org/10.1109/ATNAC.2009.5464785
19. Fan, W., et al., Enabling an anatomic view to investigate honeypot systems: A survey. IEEE Systems Journal, 2017. 12(4): p. 3906-3919. https://doi.org/10.1109/JSYST.2017.2762161
20. Al-Hakbani, M.M. and M.H. Dahshan. Avoiding honeypot detection in peer-to-peer botnets. in 2015 IEEE International Conference on Engineering and Technology (ICETECH). 2015: IEEE. https://doi.org/10.1109/ICETECH.2015.7275017
21. Fan, W. and D. Fernández. A novel SDN based stealthy TCP connection handover mechanism for hybrid honeypot systems. in 2017 IEEE Conference on Network Softwarization (NetSoft). 2017: IEEE.
22. Alzain, M.A. and E. Pardede. Using multi shares for ensuring privacy in database-as-a-service. in 2011 44th Hawaii International Conference on System Sciences. 2011: IEEE. https://doi.org/10.1109/HICSS.2011.478
23. AlZain, M.A., B. Soh, and E. Pardede. Mcdb: using multi-clouds to ensure security in cloud computing. in 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing. 2011: IEEE.
24. AlZain, M.A., B. Soh, and E. Pardede, A new model to ensure security in cloud computing services. Journal of Service Science Research, 2012. 4(1): p. 49-70. https://doi.org/10.1007/s12927-012-0002-5
25. AlZain, M.A., B. Soh, and E. Pardede. A new approach using redundancy technique to improve security in cloud computing. in Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec). 2012: IEEE.
26. AlZain, M.A., et al. Cloud computing security: from single to multi-clouds. in 2012 45th Hawaii International Conference on System Sciences. 2012: IEEE.
27. AlZain, M.A., et al., Byzantine Fault-Tolerant Architecture in Cloud Data Management. International Journal of Knowledge Society Research (IJKSR), 2016. 7(3): p. 86-98. https://doi.org/10.4018/IJKSR.2016070106
28. AlZain, M.A., et al., Managing Multi-Cloud Data Dependability Faults, in Knowledge-Intensive Economies and Opportunities for Social, Organizational, and Technological Growth. 2019, IGI Global. p. 207-221.
29. AlZain, M.A., B. Soh, and E. Pardede. A byzantine fault tolerance model for a multi-cloud computing. in 2013 IEEE 16Th International Conference On Computational Science And Engineering. 2013: IEEE.
30. AlZain, M.A., B. Soh, and E. Pardede, A survey on data security issues in cloud computing: From single to multi-clouds. Journal of Software, 2013. 8(5): p. 1068-1078. https://doi.org/10.4304/jsw.8.5.1068-1078
31. AlZain, M.A., Data security, data management and performance evaluation in a multi-cloud computing model. 2014.
32. Khan, N.F. and M. Mohan, Cloud security using self-acting spontaneous honeypots. International Journal of Engineering and Technology, 2018. 7: p. 243-247.
33. Khan, N.F. and M.M. Mohan, HONEY POT AS A SERVICE IN CLOUD. International Journal of Pure and Applied Mathematics, 2018. 118(20): p. 2883-2888.
34. Sodhi, G.K., et al., Preserving Authenticity and Integrity of Distributed Networks through Novel Message Authentication Code. Indonesian Journal of Electrical Engineering and Computer Science, 2018. 12(3): p. 1297-1304.
35. Shrutika, L., et al., Analyzing & Detecting Cyber Attacks using Honeypot. International Journal of Engineering Science, 2019. 21761.

36. Samra, H.E., et al., A Conceptual Model for Cloud-Based E-Training in Nursing Education, in Knowledge-Intensive Economies and Opportunities for Social, Organizational, and Technological Growth. 2019, IGI Global. p. 295-310. https://doi.org/10.4018/978-1-5225-7347-0.ch015
37. Alsaif, S.A., et al., From Learning Management Systems to a Social Learning Environment: A Comparative Review and the Implications. International Journal of Smart Education and Urban Society (IJSEUS), 2019. 10(1): p. 1-18.
38. Samra, H., et al., Utilisation of hospital information systems for medical research in Saudi Arabia: A mixed-method exploration of the views of healthcare and IT professionals involved in hospital database management systems. Health Information Management Journal, 2019: p. 1833358319847120.
39. Krishna, B.R. and B. Sushma, Keen Honeypot based E-Commerce Security Model. 2017.
40. Leonard, A., et al. A honeypot system for wearable networks. in 2016 IEEE 37th Sarnoff Symposium. 2016: IEEE. https://doi.org/10.1109/SARNOF.2016.7846755
41. Kołtyś, K. and R. Gajewski, Shape: A honeypot for electric power substation. Journal of Telecommunications and Information Technology, 2015(4): p. 37--43.
42. Nawrocki, M., et al., A survey on honeypot software and data analysis. arXiv preprint arXiv:1608.06249, 2016.
43. Irma T. Plata, Edward B. Panganiban and Bryan B. BartolomeA Security Approach for File Management System using Data Encryption Standard (DES) algorithm, International Journal of Advanced Trends in Computer Science and Engineering, Vol 8, No. 5, 2019 https://doi.org/10.30534/ijatcse/2019/30852019
44. Intisar Shadeed Al-Mejibli and Nawaf Rasheed Alharbe, A Fuzzy Analytic Hierarchy Process for Security Risk Assessment of Web based Hospital Management System, International Journal of Advanced Trends in Computer Science and Engineering, Vol 8, No. 5, 2019 https://doi.org/10.30534/ijatcse/2019/92852019
45. Abdelrahman ElSharif Karrar and Mohamed Fadl Idris Fadl, Security Protocol for Data Transmission in Cloud Computing, International Journal of Advanced Trends in Computer Science and Engineering, Vol 7, No. 1, 2018 https://doi.org/10.30534/ijatcse/2018/01712018