Comparative study of visualization for network situational assessment using HPPAL approach

Yashi Sharma
Dept.of CSE
SVITS
Indore, India

Rupali Bhartiya
Dept.of CSE
SVITS
Indore, India

Akhilesh Sharma
Dept.of CSE
SVITS
Indore, India

ABSTRACT
It additionally makes the representation of assault conditions by making the diagrams and plots which enormously enhances the rate and the quality measures of persons or machines choice making. This work is using so as to go to distinguish the real system status different measurements of the premise of which precise choices can be made. Basically the work is utilizing four classifications of measurements such as defined as the skill to effectively determine an overall computer network status based on relationships between security measures in multiple dimensions. In present era pc system is taken as a core component of various technology supported area such as banking sector, emergency systems, crisis framework etc [1]. This document presents some of the requirement associated with the visualization for network situational assessment. In this paper we introduce a novel network situational awareness tool that perceive network security situation comprehensively. Visualization is one of the best mean for a system to present its result to the end user and through maps and data plots humans can easily understand the whole process and improve their decision making. Our current focus is on subjective area rather than objective study of network security. To understand and measure the overall security of a network, one must first understand the vulnerabilities from multiple views and how they can combine to construct an attack [2].

General Terms
Networks – Network Performance modeling.

Network –Network Performance investigation.

Keywords
Vulnerability Measurement, Forecasting, Transformation, path

1. INTRODUCTION
An Internet assaults are developing at a disturbing rate, turning out to be more intense and complex with time. These assaults posture genuine security danger to big business systems, business sites and to the a large number of home web clients. As indicated by the Worldwide Infrastructure Security Report, a review of 70 of the greatest net administrators in North America, South America, Europe and Asia found that vindictive assaults were rising pointedly and that the individual assaults were developing all the more capable and refined [3].

There are a lot of programmed interruption recognition advances accessible; however they have some natural shortcomings. Inconsistency location based interruption recognition frameworks regularly produce a colossal number of false cautions which overpower security engineers. Known assault marks based interruption discovery frameworks do not have the capacity to identify new or obscure assaults. Hence, programmed interruption location frameworks alone are not adequate for system security and security architects are expected to adapt up to pernicious assailants [4].

Engineer Disclosure is the way toward discovering designs in a few information and Searching is the way toward figuring out whether a specific example exists in an information set. Examples are essentially spatial and transient structures in the information or connection in the fields of the information. In system movement, nearness of examples in the information shows some assault. Computerized disclosure of examples is not advanced and sufficiently vigorous in the system security domain, attributable to the developing many-sided quality of web assaults. Along these lines, however the errand of Searching is effective and quick on machines; Discovery is still an extremely human situated assignment. The human eye has been often upheld as a definitive information mining instrument and can perceive and construe designs from visual information instinctively. Human security designers can look through the information to make marks for new assaults and representation has regularly helped security examiners in this undertaking of their

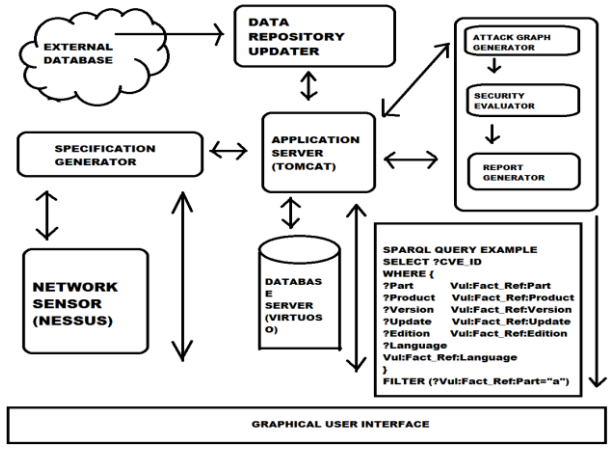


Fig. 1. Network infrastructure

System information perception has effectively empowered security experts to comprehend the way of movement present in a system, to recognize surprisingly high activity and track down focuses in the system that make such a major activity. System activity perception likewise once in a while helps experts to identify web assaults like dissent of administration assaults and impacts of worms. In any case, extricating muddled examples from a lot of time-changing information is dull for people as their ability to understand a lot of information is constrained. Customary system movement

perception frameworks give a simple level of visual presentation of results and depend for the most part on human ability for discovering irregularities in activity. In this manner, they can be utilized for identifying just vast scale web assaults and can't help the disclosure of unpretentious and more advanced assault patterns [6].

There has been little work on upgrading perception to empower security investigators to find non-minor examples in system movement logs. Ebb and flow system movement perception devices do not have the key usefulness of looking and envisioning spatial and fleeting examples in system activity information. The examples bolstered by the majority of the present perception instruments are confined to speak to imperatives on the IP addresses, ports, conventions and different qualities of a solitary record/stream. The dialect/organize that the example is spoken as far as possible the sorts of examples that can be found. One can't determine, the more broad class of examples that can encode "who converses with whom in what request" data. Improving these instruments with the non specific example investigation ability makes them all the more for all intents and purposes utilized by system managers.

2. RELATED WORK

The instrument VisFlowConnect-IP in [7] pictures IP framework movement stream to give a general point of view of the entire framework, which licenses framework inspectors to apparently overview the accessibility of limitless and complex frameworks.

The SiLK device in [8] gives framework stream records to network examiners to fathom request and gather both later and chronicled framework action data. Using these instruments, framework examiners can have bits of learning into various parts of framework practices. Regardless, these present instruments focus on getting and looking at framework stream information. They don’t have the limit of separating and looking over other security related information, for instance, vulnerabilities and perils.

There is another example of investigation in ambush showing, which is to join strike outline models and organization dependence models. In their substance, ambush charts address possible assailant exercises in the light of current structure course of action. Meanwhile, they don't address organization conditions and their fundamental affiliation necessities. N. Kheir et al. [9] propose to increase the use of CVSS estimations in the association of intrusion response, by supplying this metric with component information about structure setup and organization conditions sorted out within dependence charts. The dependence chart is further used to survey the general impact of an ambush, along these lines supplanting the easygoing environmental parameters in the CVSS vector. Regardless, the issue with this approach is that it doesn't diagram models.

In attacks are depicted and showed in a composed and reusable tree-based structure. In a strange state figured model of attack checking the intruder's point (ambush system) is shown. The paper chooses intrusion desire as the goal tree. A conclusive goal of interference thinks about to the root center point. Lower level center points address choices or asked for sub-goals in finishing the upper center point/objective. The sensible forms are used for representation of transient courses of action of interference points. The complete work using the asserted tree-based philosophy is proposed in [10]. This paper depicts suggests for reporting ambushes in a sort of attack trees.

3. PERFORMANCE COMPARISION

Situational awareness technique is used to measure the behaviors of various networked components which create a boundary between the actual working and desired operations. If the working is deviated from the desired then it is assumed that some unwanted operations are performed on them by which attack probability and occurrence is confirmed. So an attack removal strategy is applied in near future on these resources. The system should have the ability to handle the data coming from different resources and makes certain process of transforming these records to desired format for pattern matching. It is having a wide variety of devices generating logs such as network configuration, vulnerabilities, system logs, network security device alerts, network traffic and so many others. Later on these records are processed and analyzed to forecast the attack vulnerability. There are a number of system tools currently used in the field of network security situation awareness, such as NVisionIP and VisFlowConnect-IP.

4. PROBLEM DOMAIN AND SOLUTION DOMAIN

The Network security situational mindfulness is an information examination based methodology requires an enormous handling of data. It changes as indicated by various gadgets, their changes and reconciliations in the system. The point is to build the information accessibility by making the framework more strong and dependable. In such situations, data handling depends on a combination of system variables and parameters which is utilized to make the preventive appraisal of the circumstance [11]. The point is to recognize the surprising examples and from this anticipate the future impacts of the assaults on said gadgets. In the wake of concentrating on the different existing methodologies in the distinctive territories of the system utilized for expectations and anticipating, this work had distinguished that expert needs to know the examples in a confined way and the identification is completely in view of coherent capacities of few of those. Along these lines, some mechanization is required for better comprehension of vulnerabilities and impacts of assaults. Here are the some recognized issues in existing methodologies for determining the issues of powerlessness investigation.

The example to be scanned for in the system activity diagram can be indicated as a sub graph in the DOT position. For instance, to look for a disavowal of administration assault design, one can determine a diagram where there are various hubs assaulting (sending bundles to) a solitary casualty hub around the same time. It shows such a DOT chart. Take note of how one can determine different characteristics in this detail. In the event that a hub or edge property coordinating is enacted, the predefined properties are coordinated while discovering designs in the info chart. Empowering trait coordinating gives a considerable measure of adaptability in making designs. Traits can be made out of the accompanying sorts: string, position arranges (pair of comma isolated genuine number. Security is the method for accomplishing classification and protection with powerful information transmission and accessibility. For viable correspondence over the system, it could be dealt with as basic element and must be observed constantly. The system is a major workplace produced using an accumulation of different gadgets, conventions, servers and host parallel creating a great many records for every unit time. Handling of such enormous measure of information is a muddled dled assignment and requires more endeavors as far as time and cost. Hence, this paper gives an option method for

taking care of security by powerlessness evaluation. As per the methodology, system parts are dissected on their past exercises and changes obliged. These components ought to be allowed or rejected in like manner to their likelihood of assault helpless qualities called as appraisal qualities.

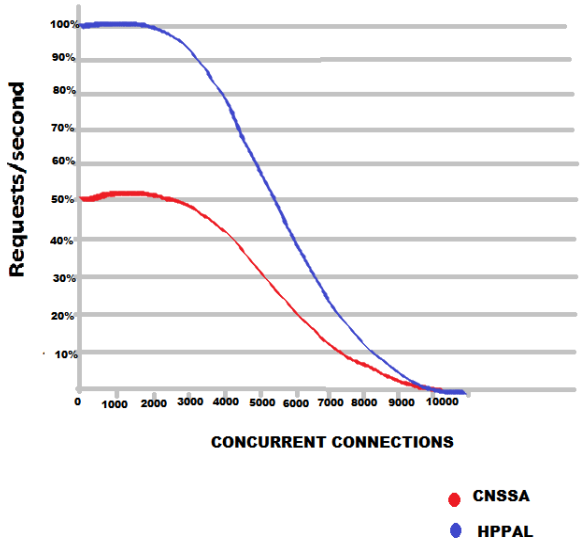
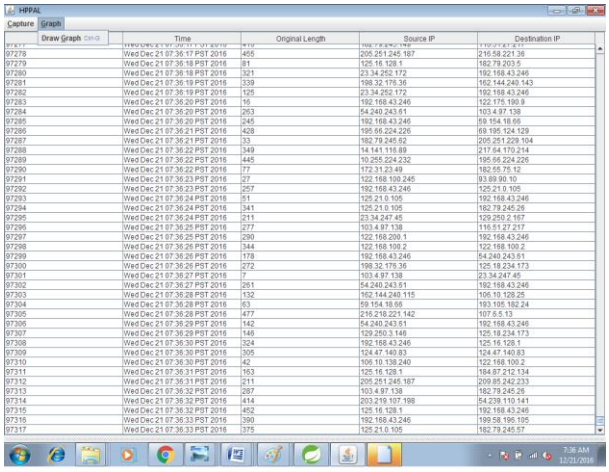


Fig 2: Accuracy analysis

5. RESULT ANALYSIS

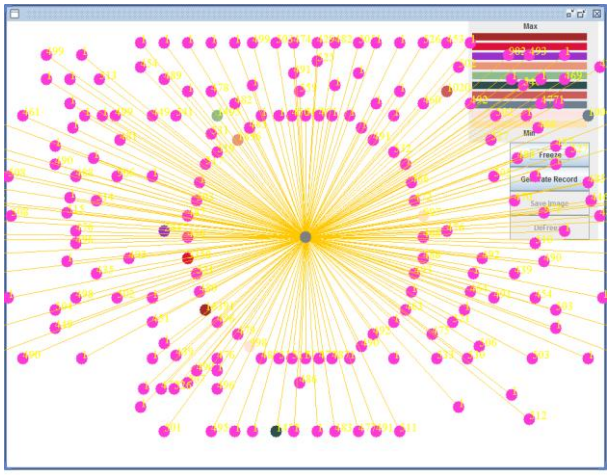
5.1 Log table

This table gives the standardized way to deal with information enter in the method with data about time, SourceIP, DestinationIP ,Server data this field goes under this table method.



5.2 Node subtle element diagram

This figure demonstrates points of interest of various hubs in a ring, it gives data on IP Address from where it originated, it similarly gives data about the packet size and on which gathering it is based.



6. BENEFIT OF THE PROJECT

This issues and ideas that stay unaddressed can be performed later on. This framework can further be reached out to actualize continuously arranges where it needs to manage the undesirable assaults. It is judged by the methodology which can be added to correct.

- Better Security analysis process.
- Easy adaptation of network configuration and security guidelines.
- Attacker activities and purpose analysis.
- Information grouping for network situation-awareness.
- Achieving self-awareness for network policy.
- Active and passive attack detection.
- Transmission intrusion detection.
- Deep Packet Inspection.

7. CONCLUSION

In this paper, we created strategies to extricate valuable data about the system circumstance from alarming, while the majority of existing frameworks simply concentrate on net stream information. We proposed a way to deal with consequently relate the cautions to produce a straightforward assault diagram based upon time and space confinement. The chart administrates to comprehend the assault steps just. This methodology can find new ready relations and it doesn't rely on upon foundation learning. The reenactments demonstrated that with the proposed techniques framework can proficiently investigate expansive sum cautions and spare heads' opportunity and vitality also. We have exhibited a system movement investigation framework that backings chart design coordinating and perception. Graphical dialect is an exceptionally natural, adaptable and general example detail arranges that catches worldly and spatial occasions in system movement. By assembling visual bits of data passed on by littler examples, security examiners can find more intricate and modern assault designs.

8. AKNOWLEDGEMENT

This research work is recommended from the SVITS as to improve the current techniques in network security using this method. Thus, the authors also wish to acknowledge institute administration for their support & motivation during this research..They additionally like to offer gratitude to Mrs.

Rupali Bhartiya and Mr. Akhilesh sharma for support in regards to the situational mindfulness framework & for creating the methodology adjusted for this paper.

9. REFERENCES

[1] Rongrong Xi, Shuyuan Jin, Xiaochun Yun and Yongzheng Zhang, "CNSSA: A Comprehensive Network Security Situation Awareness System", in International Joint Conference of IEEE TrustCom, ISSN: 978-0-7695-4600-1/11, doi: 10.1109/TrustCom.2011.62, 2014.

[2] William Streilein, Kendra Kratkiewicz, Michael Sikorski, Keith Piwowarski, Seth Webster, "PANEMOTO: Network Visualization of Security Situational Awareness through Passive Analysis ", in Workshop on Information Assurance United States Military Academy, Proceedings of the IEEE, 2007.

[3] Rongzhen FAN, Mingkuai ZHOU, "Network Security Awareness and Tracking Method by GT", in Journal of Computational Information Systems, Binary Information Press, ISSN: 1043-1050, Vol. 9: Issue 3, 2013.

[4] Igor Kotenko and Andrew Chechulim, "Attack Modelling and Security Evaluation in SIEM System", in International Transaction of System Science and Application, SIWN Press,, ISSN:2051-5642, Vol. 8, Dec 2012.

[5] Bon K. Sy, "Integrating intrusion alert information to aid forensic explanation: An analytical intrusion detection framework for distributive IDS", in Elsevier Journal of Information Fusion, ISSN: 1566-2535, doi:10.1016/j.inffus.2009.01.001, 2009.

[6] Timothy Shimeall, Sidney Faber, Markus DeShon and Andrew Kompanek, "Using SiLK for Network Traffic Analysis", in CERT R Network Situational Awareness Group, Carnegie Mellon University. September 2010.

[7] William Yurcik, "Visualizing NetFlows for Security at Line Speed: The SIFT Tool Suite", in 19th Large Installation System Administration Conference (LISA '05), 2005.

[8] Xiaoxin Yin, William Yurcik and Michael Treaster, "VisFlowConnect: NetFlow Visualizations of Link Relationships for Security Situational Awareness", in ACM, doi: 1-58113-974-8/04/0010, Oct 2004.

[9] Xiaoxin Yin, William Yurcik and Adam Slagell, "The Design of VisFlowConnect-IP: a Link Analysis System for IP Security", in National Center for Advanced Secure Systems Research (NCASSR), 2010.

[10] Ji-Bao Lai, Hui-Qiang Wang, Xiao-Wu Liu and Ying Liang, "WNN-Based Network Security Situation Quantitative Prediction Method and Its Optimization", in Journal of computer science and technology, Vol. 23, Issue 3, ISSN: 0222:0230, Mar 2008.

[11] SunJun Liu, Le Yu and Jin Yang, "Research on Network Security Situation Awareness Technology based on AIS", in International Journal of Knowledge and Language Processing, ISSN: 2191-2734, Volume 2, Number 2, April 2011.

[12] L Wang, S Noel, S Jajodia, Minimum-cost network hardening using attack graphs, Computer Communications, Vol. 29, 2006.

[13] L Wang, T Islam, T Long, A. Singhal, S. Jajodia, An attack graph-based probabilistic security metric, Proc. of the 22nd annual IFIP WG 11.3 working conference on Data and Applications Security. Springer-Verlag Berlin, pp. 283-296.

[14] L Williams, GARNET: A Graphical Attack Graph and Reachability Network Evaluation Tool, Proc. of the 5th international workshop on Visualization for Computer Security, Springer- Verlag Berlin, 2008.

[15] M M Gamal, D Hasan, A F Hegazy, A Security Analysis Framework Powered by an Expert System, International Journal of Computer Science and Security. Vol. 4, No. 6, 2011, pp. 505–526.

[16] M McQueen, T McQueen, W Boyer, M Chaffin, Empirical estimates and observations of 0-day vulnerabilities, Hawaii International Conference on System Sciences, 2009.

[17] M Y Huang, T M Wicks, A Large-scale Distributed Intrusion Detection Framework Based on Attack Strategy Analysis, Computer Networks, Vol. 31, NewYork, NY, USA, 1999, pp. 2465-2475.