Journal of Applied Science and Agriculture, 9(4) April 2014, Pages: 1552-1558

AENSI Journals

Journal of Applied Science and Agriculture

ISSN 1816-9112

Journal home page: www.aensiweb.com/jasa/index.html

A Correlation Method for Identifying Slow Attacks

[1]Shima Amiri and [2]Zhina Zamani

Department of Computer, Islamic Azad University, Ilam branch, Ilam, Iran.

ARTICLE INFO

Article history:
Received 20 January 2014
Received in revised form 16 15 April 2014
Accepted 25 April November 2014
Available online 5 May 2014

Keywords:
Network Security Intrusion Detection False and True Positive and Negative alerts

ABSTRACT

Currently, managing raw alerts generated by different sensors with various capabilities, placed in different locations of intrusion detection systems has become an important issue. All intrusion detection systems are able to generate alerts in case of an intrusion; however these systems are not able to manage and analyze the generated alerts themselves due to the large number of generated alerts and also false positives. There has been many methods to eliminate this weakness one of which is alert correlation. Using alert correlation methods, we can fully manage alerts generated by intrusion detection systems. Moreover we can ignore false alerts to some extent, reduce generated alerts and facilitate their analysis. In order to focus on security requirements of organizations, it is recommended to use alert correlation coupled with a knowledge database and event log analysis system in a security operations center. We can simply define alert correlation as the process of correlating different alerts. Generally we can say that alert correlation facilitates management, investigation and analysis of different security alerts generated by various systems. It connects different alerts and also reduces the number of raw alerts.

To Cite This Article: Shima Amiri and Zhina Zamani., A Correlation Method for Identifying Slow Attacks. ***J. Appl. Sci. & Agric.,*** *9(4): 1552-1558, 2014*

INTRODUCTION

Increasingly expansion of computer networks and their users has made security provision one of the open academic and commercial subjects studied by many researchers around the world. As computer networks expand, destructive attacks are also increased in these networks, such that we observe a many new attacks around us every day. Many devices are used in the context of networks to provide security. These devices include intrusion detection system, intrusion prevention systems, firewalls, etc.

With taking into account the expansion of current networks and the fact that sensors of the intrusion detection systems may be installed in different locations of the network, a great number of alerts are generated by these devices. Moreover since intrusion detection networks may not be fully accurate, it is possible that false alerts are generated. There are different types of false alerts which will be described in the following sections. Therefore, due the great number of alerts generated by these systems and the possibility of false alerts among true ones, users are not capable of correctly managing and investigating these alerts. Several methods have been proposed to solve this problem which all has some advantages and drawbacks; however one of these methods which is almost the best solution, is alert correlation. Alert correlation refers to correlating different or sometimes similar alerts generated by different intrusion systems of a network. In other words some low-level alerts are synthesized to create a high-level alert. This reduces the number of alerts to investigate in comparison to the initial number. Another advantage is that while correlating alerts, false alerts can be identified and eliminated during this stage. Another advantage is that a new alert is generated by synthesizing low-level alerts which is more comprehensive, applicable and in a higher level of abstraction for network security managers. Moreover generated alerts after correlation can be prioritized by the attack and generated alerts which make managers react more properly to attacks and also recover from damages cause by it. Due to the great importance of alert correlation, we focus the rest of this article on alert correlation. This study is a survey about alert correlation and presents no novel ideas.

We intent to concentrate on intrusion detection system whose primary task is to timely detect an intrusion in the network.

Current Architectures:

This section introduces four of the current existing architectures in the logic level for alert correlation systems.

Corresponding Author: Shima Amiri, Department of computer, Islamic azad university, Ilam branch, Ilam, Iran.

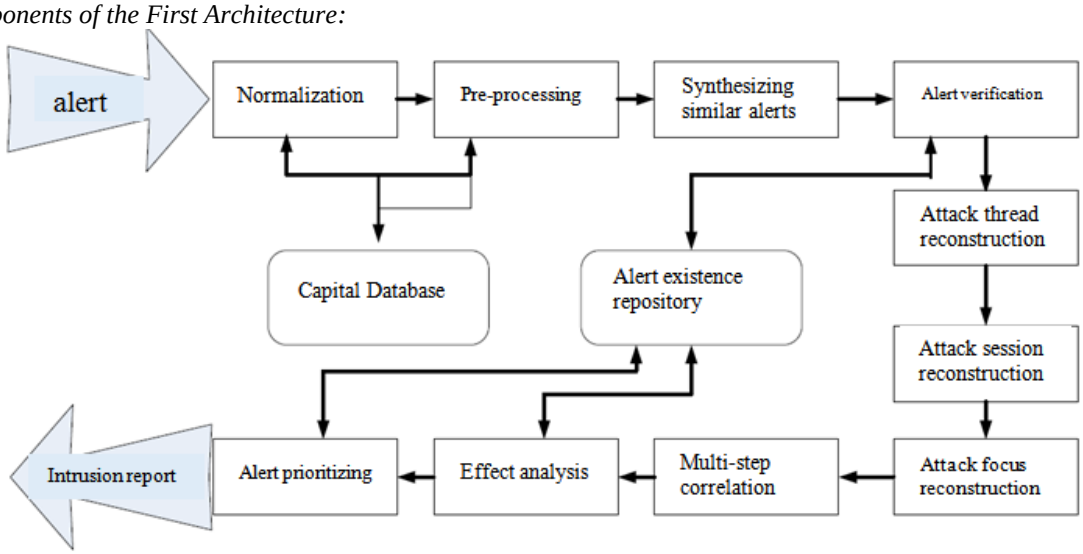
Journal of Applied Science and Agriculture, 9(4) April 2014, Pages: 1552-1558

First Architecture (Integrated Method to Correlation)

The First Architecture:

includes ten components: normalizing, pre-processing, synthecizing similar alerts, verifying alerts, creating attack threads, creating attack sessions, attack focus reconstruction, multi-step correlation, effect evaluation and alert prioritizing.

Components of the First Architecture:



The Second Architecture:

includes two components: normalizing and synthesizing the events and alerts. This was mostly an experimental architecture and it is only used to test new methods.

Components of the Second Architecture:

The Third Architecture:

includes three components: normalizing, synthesizing alerts and events, creating views. This architecture is rather experimental than practical and it mostly used to test new innovating methods.

Creating Views:

One of the important activities of correlation systems is creating major views for alerts. These views can be defined based on different analysis requirements with different objectives. Examples of this group of activities include:

Creating Attack Threads:

100 correlating alerts with the same attacker and victim and occurring close to each other. This was also explained in the first architecture.

Security Events Report:

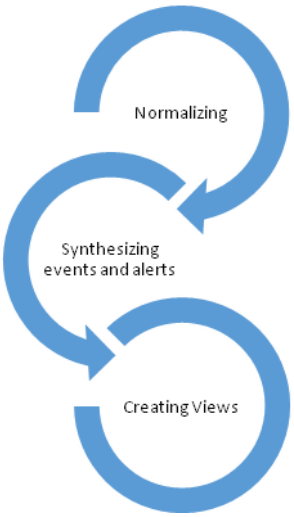
grouping alerts with same attackers, victims and attack types, occurring in short time intervals.

Journal of Applied Science and Agriculture, 9(4) April 2014, Pages: 1552-1558

Various Attack Graph Visualization Tools:

this group of methods, first connects events based on perquisite relationships as a graph and then simplifying the graph for observation and analysis using different methods.

Components of the Third Architecture:

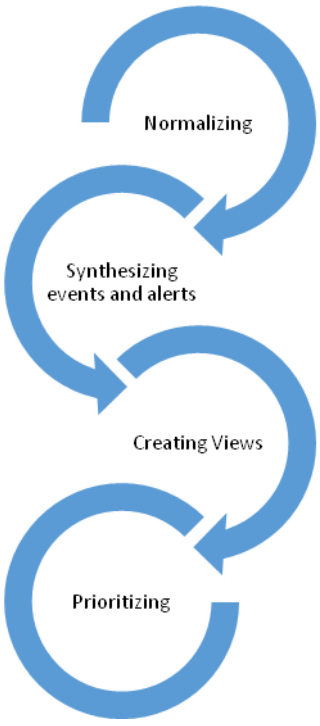


The Fourth Architecture:

which is more complete than the two previous architecures and less complete than the first. It includes five components: normalizing, synthesizing alerts, synthesizing events, creating views and prioritizing.

This architecture is both practical and experimental

Components of the Fourth Architecture:



Alert Correlation in Intrusion Detection Systems:

Journal of Applied Science and Agriculture, 9(4) April 2014, Pages: 1552-1558

Alert correlation is a process for analyzing and correlating security signs and alerts to aggregate the information of the network and hosts. Different techniques have been proposed in recent years for sign correlation and attack scenario analysis which can be generally categorized in three groups:

Correlation based on statistical similarity between signs attributes.

Correlation based on comparing complete pre-defined attack scenarios.

Correlation based on attack consequences and perquisites.

(Valdes and Skinner, 2001) use a statistical approach for correlating signs by comparing their similarities. (Shopens, 2002) use classification techniques based on attribute similarities. (Debar and Vespey, 2001) propose conceptual hierarchical classification techniques for correlation. Complete scenario of attacks provide useful information for sign analysis. This data is aggregated from the knowledge of researchers. LAMBDA (Copens et al, 2000) and STATL (Ecman et al, 2002) are standard languages for specifying the stages of attacks. However their significant problem is that they are unable to identify new attacks.

Another approach, correlation based on perquisites and consequences of attacks is used to eliminate the constraints of the above method. In other words, instead of using pre-defined complete attack scenarios, perquisites and consequences of each attack is specified before correlation. The correlation engine operates through comparing the consequences of the previous and perquisites of the future attacks.

Correlation:

The goal of alert correlation is finding logical relationships between alerts to reconstruct an attack scenario. This sub-process of correlation is also called creating attack scenarios or mining attack scenarios. The research in the context of correlation is categorized as follows (Elmemory and Zhang, 2007):

Similarity based Correlation: alerts are classified based on their attribute similarities.

Attack scenario recognition correlation: logical relationships between alerts relies on creating attack scenarios. In other words, two alerts are correlated if it is possible to create a new attack scenario by synthesizing them.

Statistical Correlation: methods using statistical correlation, correlate alerts if they are statistically dependent.

Time Correlation: two alerts are correlated based on time relationships between them.

We must node that three of the aforementioned methods are more popular and most researches only mention these three.

Similarity based Correlation:

The similarity based methods, also known as probabilistic method, classifies alerts based on their attribute similarities. A mathematical framework is proposed which can be used to match very similar alerts (not necessarily the same). The minimum similarity degree required to correlate two alerts can be configured by a corresponding variable. The similarity based correlation tries to correlate alerts based on common attributes, their similarities and using a configurable a general total expected similarity parameter. 116 hyper-alerts are generated from each set of correlated alerts.

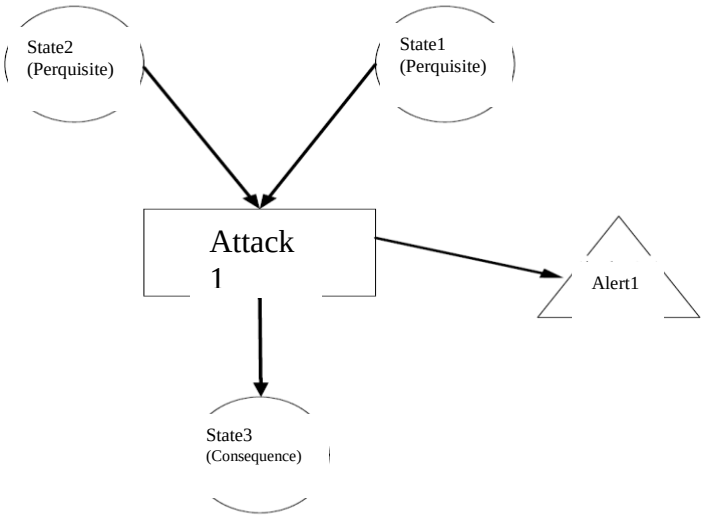
Scenario based Correlation:

One of the correlation methods is scenario recognition. This methods describes an attack scenario and recognizes it while execution. Most of the related research use visual models or learning methods to specify attack scenario. CAML, ADELE, STATL and LAMBADA are instances of detection and correlation languages used for describing attack.

Statistical Correlation:

Statistical correlation is complement to correlation using a knowledge database. Kane uses Bayesian networks to model casual relationships between alerts. This model represents alerts by nodes and relationships by edges. The goal of this model is to specify the types of alerts which are the cause of alert A and expressing the conditional probability in case its parents (causes) occur. They have proposed a simple algorithm based on mutual information of 128 alerts to create a Bayesian network structure (casual relationships between alerts). This research uses a casual network as a tool of expressing casual relationships and probabilistic dependencies. The casual network is a directed acyclic graph in which each node represents a random variable containing a set of possible states. Edges represents probabilistic (casual) dependencies between variable.

Journal of Applied Science and Agriculture, 9(4) April 2014, Pages: 1552-1558



The placement and connections of status nodes, the attack and the alert have different effects on the attack as different perquisites. Attacks are also different regarding their success rate. The probability of recognizing attacks is also different regarding the operational domain and the recognition by different intrusion detection systems. This can be applied to the correlation process by the knowledge of security analyzers about attacks and alerts. This knowledge is expressed through specifying the perquisite probabilities of the parent nodes and the conditional probabilities of other nodes.

Time Correlation:

Lee and Kane have proposed a method in which casual relationships between alerts are analyzed using Granger casual test (GCT). This test is a statistical analysis methods based on time sequences which enables determining the correlation between a time sequence variable (X) and another time sequence variable (Y) using statistical hypothesis test. In order to analyze time sequences in alert correlation, time sequence variables are modeled for all hyper-alerts based on the number of alerts in the unit of time and then GCT is performed.

GCT determines whether X has significant information about Y. if it does, alert type X can be the cause of alert type Y.

The main notion of GCT is approximating the value of Y using two models:

Autoregressive (AR). The value of Y is approximated by its previous values.

Auto regressive mobile average (ARMA). The value of Y at time t is approximates by its previous values and previous values of X.

Comparison of Alert Correlation Methods

Feature	Similarity based	Scenario based	Statistical based
The ability to synthesize received alert from various sources	Simple	Based on existing knowledge	No
Requiring pre-existing knowledge	Alert comparison functions	Alert/scenario definitions	No
The ability to identify false alerts	Only in case of overlapping different alert sources	Yes	Speculates
Identifying multi-stage attacks	Hardly	Yes	Speculates
The ability to operate under unknown (new) conditions	Yes	No	If learning is possible
Expected error rate	Average	Low	High
Usable alone for the entire process	Suitable	Suitable	Unsuitable

As we can see in the table above, none of the methods can be used alone for alert correlation; since each has some weaknesses and none can alone satisfy the needs of the correlation process. They are usually applied combined.

At the final section of this research, we have introduced different existing architectures for alert correlation and their components. As it was mentioned, there are different architectures for alert correlation which all have advantages and drawbacks. Other architectures are mostly used in commercial products and they are not accessible to public. After selecting a suitable architecture, a correlation method should be selected which is a difficult task due to the existence of various correlation methods. As it was mentioned each methods has its advantages and drawback. Today an individual product rarely and in special cases use only one method and mostly a combination of them is applied. Therefore we can conclude that none of the aforementioned methods are sufficient alone.

Journal of Applied Science and Agriculture, 9(4) April 2014, Pages: 1552-1558

The Problem:

We can generally say that security event and alert management is currently facing security managers with many challenges due to different security devices, the high speed of alert generation by these devices and also the variety, extension of alerts and also the existence of false alerts. Some of these challenges are:

The large amount of generated alerts by different security systems.

Different and multi-layer security solutions like firewalls, intrusion detection systems, intrusion prevention systems, Antiviruses, etc. all of which generate events in different formats and each follow different tasks.

Inexistence of specific and recorded measures for risk management and the significance of each alert. Increasingly extension of security attacks and creation of new attacks. Inability to analyze related and multi-step attacks that each step is recognized by one system. In order to eliminate these issues and focus on security requirements of the organizations, alert correlation with knowledge databases and event recording systems are recommended in a security operations center. However we can simply define alert correlation as the task of correlating different alerts. In fact, alert correlation connects events in a way that new meanings are created from them. Sometimes the amount of alerts is so high that human personnel are not capable of managing, analyzing and responding to those alert and also alerts are low-level. Thus alert correlation reduces the number of alerts generating higher level and more abstract alerts and their making management and analysis simple for human personnel. Another task of alert correlation is to transform raw received alerts into a common format.

We can generally say that alert correlation facilitates management, investigation and analysis of different security alerts generated by different systems, also connects alerts and reduces the number of raw alerts.

Related Work:

The first related article was published in 1990s. After that article, this subject was investigated by the researchers and started its evolution process. At first, existing alert correlation architectures were discussed and different correlation methods were then proposed. This study introduced different existing architectures containing different components each following a particular task. Each of these architectures have their own characteristics, advantages and drawbacks. As correlation architectures, there are different correlation methods. However none of those methods scientifically satisfy all requirements and each had their own advantages and drawbacks. Composite methods were also presented which used a combination of correlation methods. Statistical methods were not significantly applied among the correlation methods presented, they were limited to a specific domain and never applicable independently. In fact it can be used alone but it would never have the required performance. Similarity based methods solve the problems of statistical methods to some extent. However they possessed the same amount of problems. For instance in order to properly apply these methods, they should contain all attack patterns, so that based on the algorithm used, they can examine the similarity between the real attacks, the attacks they include and generate an alert.

Moreover, these methods were not able to discover the relationship between different attacks. These methods were also not applicable independently. Methods based on knowledge databases, to some extent, solved the problems above; however they also had some problems, one of which was the large size of the knowledge database they used. Therefore we can generally say that correlation methods are not usable alone and they should be essentially applied combined. Currently commercial systems usually use knowledge based correlation coupled with similarity based methods to some extent.

REFERENCES

Scarfone, K. and P. Mell, 2007. Guide to intrusion detection and prevention systems (idps), NIST Special Publication, 800: 94.

Barbar´a, D., J. Cuotuo, S. Jajodiaand N. Wu. ADAM, 2001. A testbed for exploring the use of data mining in intrusion detection. ACM SIGMOD Record, 30(4): 15-24.

Vigna, G. and R.A. Kemmerer. NetSTAT, 1999.A network-based intrusion detection system. Journal of Computer Security, 7(1): 37–71.,

Kummar, S. and E.H. Spafford, 1995. A software architecture to support misuse intrusion detection. In Proceedings of the 18th National Information Systems Security Conference, pp: 194-204.

Valeur, F., G. Vigna, C. Kruegel, and R.a. Kemmerer, 2004. Comprehensive approach to intrusion detection alert correlation, IEEE Transactions on Dependable and Secure Computing, 1(3)169-146.

Al-mamory, S.O. and H.L.I. Zhang, 2007. A Survey on IDS Alerts Processing Techniques, pp: 69-78.

Faculty, T.A. and I.P. Fulfillment, 2005. A Probabilistic-Based Framework for INFOSEC Alert Correlation Xinzhou Qin A Probabilistic-Based Framework for INFOSEC Alert Correlaon,"no. August.,

Cuppens, F. and R. Ortalo, 2000. LAMBDA: A language to model a database for detection of attacks. In Proc. Of Recent Advances in Intrusion Detection (RAID 2000), 197-216, September.

Dain, O., and R.K. Cunningham, 2001. Fusing a heterogeneous alert stream into scenarios. In In Proceedings of the 2001 ACM workshop on Data Mining for Security Applications, pp: 1-13.

Karim Tabia, Salem Benferhat, Philippe Leray, Ludovic M´e, 2011. Combining AI-based approaches for exploiting security operators' knowledge and preferences, Security and Artificial Intelligence (SecArt,(Barcelona:Spain.

Peng Ning, Yun Cui, Douglas S. Reeves., 2002, Consrtcting attack scenarios through correlation of intrusion alerts,CCs-02 Proceedings of the 9□□ ACM conference on Computer and communications security, pp: 245-254.

Z.-tang Li, J. Lei, L. Wang, and D. Li, 2007. A Data Mining Approach to Generating Network Attack Graph for Intrusion Prediction,Fourth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2007), no. Fskd, pp: 307-311.

A.-fang Zhang, Z.-tang Li, D. Li, and L. Wang, 2007. Discovering Novel Multistage Attack Patterns in Alert Streams," 2007 Internaonal Conference on Networking, Architecture, and Storage (NAS 2007, (no. Nas, pp: 115-121.

Paul Ammann, D., Wijesekra, S. Kaushik, 2002. Scalable, graph-based network vulnerability analysis,CCs-02Proceedings of the 9th ACM conference on Computer and communications security, pp: 217-224.

Oh, W., K. Leeb, 2004. Causal relationship between energy consumption and GDP revisited: the case of Korea 1970-1999, 26(1): 51-59.

Ma, J., Z.-tang Li, and W.-ming Li, 2008. Real-Time Alert Stream Clustering and Correlation for Discovering Attack Strategies, 2008 Fih Internaonal Conference on Fuzzy Systems and Knowledge Discovery, pp: 379-384.

Li, Z., A. Zhang, J. Lei, and L. Wang, 2007. Real-Time Correlation of Network Security Alerts, IEEE International Conference on e-Business Engineering (ICEBE'07), pp: 73-80.

Agrawal, R. and R. Srikant, 2004. Mining sequential patterns, Proceedings of the Eleventh International Conference on Data Engineering, pp: 3-14.

Templeton, S.J. and K. Levitt, 2000, A requires/provides model for computer attacks, Proceedings of the 2000workshop on New security paradigms - NSPW '00, pp: 31-38.

Ning, P., Y. Cui, D.S. Reeves and D. Xu, 2004. Techniques and tools for analyzing intrusion alerts, ACM Transactions on Information and System Security, 7(2): 274-318.

Sannella, M.J., 1994. Constraint Satisfaction and Debugging for Interactive User Interfaces, Ph.D. Thesis, University of Washington, Seattle, WA.

Zachman, J.A., 1987. A Framework for Information Systems Architecture, IBM Systems Journal, Vol. 26, No. 3.,

Sisalem, D., J. Floroiu, J. Kuthan, U. Abend, H. Schulzrinne, 2009. SIP Security, John Wiley and Sons Publicaiton.

Frédéric Cuppens Alexandre Miège., 2002. Alert Correlation in a Cooperative Intrusion Detection Framework ,IEEE Symposium on Security and Privacy, pp: 202.

Eckmann, S.T., G. Vigna and R.A. Kemmerer, 2002, STATL: An Attack Language for State-based Intrusion Detection.Journal of Computer Security, 10(1/2): 71-104.

Ning, P., Y. Cui, D.S. Reeves and D. Xu, 2004. Tools and techniques for analyzing intrusion alerts.ACM Transactions on Information and System Security, 7(2): 273-318.