Designing a holistic end-to-end intelligent network analysis and security platform

M Alzahrani

Department of Information Technology, College of Computer Science & IT, Albaha University, Saudi Arabia
msawileh@bu.edu.sa

Abstract. Firewall protects a network from outside attacks, however, once an attack entering a network, it is difficult to detect. Recent significance accidents happened. i.e.: millions of Yahoo email account were stolen and crucial data from institutions are held for ransom. Within two year Yahoo’s system administrators were not aware that there are intruder inside the network. This happened due to the lack of intelligent tools to monitor user behaviour in internal network. This paper discusses a design of an intelligent anomaly/malware detection system with proper proactive actions. The aim is to equip the system administrator with a proper tool to battle the insider attackers. The proposed system adopts machine learning to analyse user’s behaviour through the runtime behaviour of each node in the network. The machine learning techniques include: deep learning, evolving machine learning perceptron, hybrid of Neural Network and Fuzzy, as well as predictive memory techniques. The proposed system is expanded to deal with larger network using agent techniques.

1. Introduction

Access control, firewalls and anti-virus software in information security have successfully helped us to stop people from doing wrong things in a computer network system. However, it still have limitation in providing insights into human behavior and advanced malware because the rules are set up statically in the traditional reliance. Thus, the rules are hard to update dynamically when needed due to the changes in the network. Security information and event management (SIEM), an approach to security management, provides us with a better insight into patterns of user behavior.

A technique called User Behavior Analytics has started to become particularly useful in giving solutions that have a level of flexible pattern recognition which rules are unsuitable, and which humans simply cannot achieve due to the excruciatingly large amount of data involved. The user behavior is considered a hard problem due to the fact that human behavior is erratic and hard to predict

A focus area of information security is cybercrime. It is difficult to prevent or fight this cybercrime due to the fact that attacks techniques are also getting sophisticated as more and more tools are available in the Internet that try to make the attacks very difficult if not impossible to detect. The attacker can launch the attacks form a different geographical location or continent or just from our next door neighbor. Government, businesses or even individuals may be targeted by this crime, regardless of size.

In fact System Administrators are often based only on ad hoc methods developed from years of experience in spotting and finding anomalous behaviors in their networks. Many commercial and open source tools have been developed to assist the System Administrators to guard their networks from the
attacks. Nevertheless, these tools are not dynamic to adapt any traffic changing that requires the System Administrators to redefine policies from time to time with the aim to trigger alerts. The accuracy of the detection depends on how good the description of the anomalous behavior.

2. Related Works

2.1. User behaviour analytics in traffic anomaly/malware detection
Detecting insider attacks against a network is really difficult due to the fact that the defense system may consider it was a normal activity. Works by Wang et al. [1] and W. Kim et al. [2] showed that emotions affected user superficial trust in new developed applications with either positive or negative emotion.

Sun et al. [3] found out “the effect of behavior” and presented “typical access uses of social web site”. The profile of user behavior is generated from user’s habit activity, and it has to be updated periodically to include the most recent changes. Yin et al. [4] described “a method for anomaly/intrusion detection on linear prediction and Markov chain model then are combined with signature verification to detect attacks more efficiently”. The introduced method is based on the temporal behavior of application, and used data from University of New Mexico. Qiao et al. [5] proposed “a behavior analysis-based learning framework”. A cluster-based outlier detection algorithm to detect anomalous data is introduced. The authors also described the set of factor of user behavior profile, program profile and system resource usage. “The proposed framework is sufficient to analyze behavior in host-based intrusion without explaining about how to capturing data in stream network and result of the alerts to be forwarded to response mechanism after identifying attack”. Lim & Jones [6], presented “taxonomy of anomaly detection techniques in network-based intrusion”. The authors confirmed the extent of the use of misuse-based detection system has become the dominant strategy for countermeasure from suspicious attacks and identified two approaches for building the behavior model; learning-based and specification-based models. Authors in [7] used fast-learning method with neural network based on pre-processed component. Prior to this work, Galassi et al. [8] through series of experiments investigated the possibility of automatically constructing a user profile from the logs users’ activities, and introduced a standard formalism for regular expressions adopted for describing episodes and profiles.

Work of [2], presented “user behavior in using social network”. The authors elaborated methods on how to attempt organizing the status, uses, and issues of social network into a comprehensive framework for the future of social networks/websites. The authors mapped the users’ (government, business and individual) behavior onto uses of social website. “A taxonomy of the most relevant users’ behavior features of current solutions” [9]. The behavior features and models were proposed to classify existing techniques. “Users’ behavior is very difficult to measure and is related with concepts such as social class, geographical culture, technical knowledge and many others” [10].

2.2. Deep Learning
The existing network policies are not adequate to adapt to the continually changing network conditions arising from the explosive traffic growth. Thus, there is a need to rethink how the network traffic control can be improved. The incorporating intelligence into network traffic control systems can play a significant role in guaranteeing security and Quality of Service (QoS) in Internet Protocol (IP)-based networks [11]. Over the past few decades, machine learning (ML) has been exploited to intelligently dictate traffic control in wired/wireless networks [12-14]. Authors in [15] mentioned: “Since the early excitement stirred by machine intelligence in the 1950s, smaller subsets of machine intelligence have been impacting a myriad of applications over the last three decades”. Recently, an even smaller subset of Machine Intelligence and ML techniques, known as deep learning, has emerged with the potential of creating even larger disruptions [16-18].
2.3. Automatic run-time extraction of network protocol specification

A network protocol is a set of rules that describe the messages format and the way they are exchanged (i.e., the protocol state-machine) between two or more network devices. The process of analyzing and discovering Application-level specification of unknown/proprietary network protocols is known as reverse engineering.

Security applications require knowledge on protocol specification. For example a network management software depends on the knowledge to correctly recognize and classify monitored network traffic; penetration testing that generates network inputs to an application to uncover potential vulnerabilities can take advantage of such knowledge to improve the testing process by generating “malicious” inputs more efficiently; a network-based intrusion prevention and detection applications require the knowledge to perform deep packet inspection. The standard protocols specification such as SMTP and HTTP, can be obtained easily because they are available openly. However, for a proprietary protocols such as SMB or Skype, the specification has to be re-engineered. Unfortunately, the manual application of reverse engineering is a time-consuming, tedious, and error-prone task due to the following problems: (1) A message field may not be static; (2) A single protocol message may contain a large number of fields; and (3) complicated relationships (e.g., sequential, parallel, and hierarchical) or dependencies among the fields may exist. This work consider a number of real-world protocols and server applications such as HTTP and SMTP.

2.4. Runtime behaviour Analytics

Traffic classification/intrusion detection system requires specific logics to describe attack signatures, and specific model-checking algorithms. Compared to standard misuse detection tools, a temporal logic allows one to describe behavior involving several events over time: standard misuse detection tools (e.g., anti-virus software or simple network intrusion detection systems) match a library of patterns against single events, and emit an alert once single so-called dangerous events occur. These days, more attacks involving complex, correlated sequences of events, which are usually individually kind.

Instamon is equipped by future traffic classification and intrusion detection tools which capable of analyzing and correlating events over time, in real time. Its purpose is to detect, report, and take countermeasures against intruders. The core of the engine is based on a defined language and algorithm. There are many other formalisms attempting to detect complex intrusion detection scenarios, using means as diverse as Petri nets, parsing schemata, continuous data streams, etc.

2.5. Sequential Hierarchical Superset (SHS) Neocortex Memory System

As described earlier, human neocortex memory system forms the basis of intelligence, perception, creativity, and even consciousness. Our brain learns and understands knowledge by utilizing its neocortex. As described in the memory prediction framework theory [19], neocortex stores sequences of data in a hierarchy. It also recalls data auto-associatively in a form of prediction and match it with the actual input data.

It is constructed of 6 layers of cortical sheet. In the lower hierarchy, the stored data will be more specific features/details and fast changing. So it can be said that long term memory is stored in the top layer and short term memory is stored in the bottom layer [20].

3. The proposed design and discussion

The open-ended challenge in securing enterprise network are the driver to many innovative network monitoring and security solutions. High speed data capture, real-time analysis, exponential growth of captured data size, and complex data are among the common problems in existing network monitoring and security solutions. This paper presents a high-level proposal to extend the existing work on network monitoring platform and develops a holistic end-to-end intelligent network analysis and security cloud platform not only leveraging pfSense, a wildly adapted, robust, and proven open source
security library for traffic data analysis and protection, but also adopting as well as proposing various machine learning techniques for intelligent data representation and security analysis. Figure 1 depicts the high-level design of the proposed system named as *Instamon*.

![High level architecture of InstaMon cloud.](image)

The main idea is to have cloud-based network monitoring platform where organization can monitor their network with multiple segments or locations from anywhere anytime through desktop, mobile apps, or web browser. As a passive monitoring solution, the InstaMon agent will sit at the network edge and work together with the adapted pfSense module to collect and analyse network traffic. The proposed InstaMon cloud is designed to be modular to allow organizations to subscribe or active only certain type of information that they intend to monitor such as the commonly monitored network usage statistics, web usage, server health monitoring, etc. as well as the analytics and intelligent monitoring modules.

### 3.1. The backend engine

At the back of InstaMon cloud lies the backend analytics module which regularly pulls data from various tables in the databases for certain analytics as well as intelligent analysis. This backend analytics module will adopt extensible design to allow new analytics plugin or new intelligent analysis plugin be added in the future. On the other hand, the data source will receive compact data from multiple monitoring points where InstaMon agent is installed. These compact data will not be as detailed as the raw data but instead will have different compact structures according to the purpose of the data source collected at various network points. Figure 2 shows the design of the backend analytics module with proposed initial default plugins.

![Backend analytics engine design.](image)
3.2. *Human brain’s neocortex inspired invariant hierarchical memory model*

There will be 3 machine learnings as well as brain inspired engine used to support the analytics and intelligent monitoring module. The first one will be a collection of various neural network tools and pre-trained neural network model, which will be used to run deep learning analysis of user traffic behavior and predict future trends. Depending on the configuration, some output of this analysis would be list of unusual user activities, user upload/download pattern, user web usage pattern, etc. The second engine is an adaptation of the existing traffic profiling engine implemented using evolving connectionist technique enabling a real-time traffic anomaly detection at InstaMon agent by pulling the appropriate daily profile. This work also develops alerting archive module to give network administrator the power to manually adjust how the profile would evolve over previous anomalous activities detected.

Lastly, this work includes an implementation of human brain’s neocortex inspired invariant hierarchical memory model as a powerful tool to learn network traffic data from as low as every byte inside a network packet hierarchically into high level network traffic pattern. This brain model will be exported into InstaMon agent and be used for various monitoring activities from as low as packet decoding process and creating compact format of traffic data to be passed back to InstaMon cloud data source. Combined with the traffic profile, the brain model will also be used to perform forensic analysis at a later stage inspecting traffic from 5 minutes interval to hourly, daily, and monthly.

Figure 3 depicts the idea of multi-segment monitoring architecture of InstaMon cloud solution. The idea is to adapt pfSense to act as border control firewall that regulates internet traffic and as high speed capturing and analysis box. This pfSense based capturing and analysis box will tap on the edge of every network segment will periodically pass both collected packets and statistical analysis data to InstaMon agent. InstaMon agent will perform real-time traffic analysis and use various profiles, rules and engines from the backend analytics created to detect anomalous traffic, abnormal user usage behavior, as well as matching the traffic prediction trend with the actual traffic.

![Figure 3. The architecture of multi-segment monitoring.](image)

3.3. *The proposed Sequential Hierarchical Superset (SHS) model*

The biggest problem lies in the fact that neural networks have little similarity with the actual processes in the brain other than both being constructed of many interconnected units. To address this issue, a
more biologically plausible model is needed that reflects the actual human intelligence. In fact, it is a need to first understand how intelligence developed in human brain from neuroscience perspective.

Our knowledge on the detailed biological process of the human gene interaction, human brain evolution, and other biological processes is still in its infancy. But two recent important discoveries in neuroscience have shed some lights on different perspectives on modeling the brain. The first one is the fact that the evolution of human brain structure is significantly affected by its genome structure and the second one is a theory called memory-prediction framework which explains the high-level architecture of the human neocortex and how it works. The memory-prediction framework states that human’s neocortex memory system forms the basis of intelligence.

The task of network forensic requires human intelligence to analyze and understand what is happening to the network. The Sequential Hierarchical Superset (SHS) model have the advantage of being able to process data in high speed and able to perform basic analysis on the data in real-time fashion. The proposed approach of Sequential Hierarchical Superset (SHS) implementation is translating the biological model of neocortex memory system into a simple working model based on the memory prediction framework [20] and with their smaller part in distributed neuro-gen adaptive engine [21][22][23]. Figure 4 shows the framework, adopted from [20].

4. Initial implementation & results
The first phase of the implementation is undergoing. The system is developed using Java programming under Eclipse technology platform. The typical implementation of the proposed system in an enterprise system is shown in Figure 5. Some intelligent features are shown in Figure 6, Figure 7 and Figure 8.

The preliminary results from experiments show a promising performance of SHS in terms of the way it manages and relates information about the network. The results were analyzed after running the experiment for around one month. The first and second week can be considered as the SHS learning period. Figure 8 shows the number of sets inside SHS memory after 1 month of experiment.
Figure 6. Screenshot of the intelligent features (rules creation).

Figure 7. Clustering of network traffic to detect anomaly.

Figure 8. The SHS memory structure after 1 month of running.
5. Conclusion
In conclusion, it is believed the proposed InstaMon cloud solution could provide holistic end-to-end network monitoring and protection to assist network administrator to manage and protect their organization’s network.

References
[1] Wang, C.Y., Chou, S.-cho T. & Chang, H.-ching, 2009. Emotion and motivation: understanding user behavior of web 2.0 application, IEEE Computer Society Seventh Annual Communications Networks and Services Research Conference, pp.1341-1346.
[2] Kim, W., Jeong, O.K. & Lee, S.W., 2010. On social Web sites. Journal of Information Systems, 35, pp.215-236.
[3] Sun, Y. et al., 2010. Hybrid Regular Expression Matching for Deep Packet Inspection on Multi-Core Architecture. IEEE Proceeding Computer Communications and Networks (ICCCN), pp.1-7.
[4] Yin, Q. et al., 2004. Based on Behavioral Method Based on Behavioral Model. AnalysisIEEE Proceeding of the 5th World Congress on Intelligent Control and Automation, pp.4370-4374.
[5] Qiao, H. et al., 2007. Behavior Analysis-Based Learning Framework for Host Level Intrusion Detection. Proceedings of the 14th Annual IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS’07).
[6] Lim, S.Y. & Jones, A., 2008. Network Anomaly Detection System : The State of Art of Network Behaviour Analysis British Telecommunications plc , Security Research Centre , Ipswich , United Kingdom. International Conference on Convergence and Hybrid Information Technology 2008, pp.459-465.
[7] Koch, R., 2009. Changing Network Behavior. 2009 Third International Conference on Network and System Security, pp.60-66.
[8] Galassi, U., Giordana, A. & Mendola, D., 2005. Learning User Profile from Traces. 2005 Symposium on Applications and the Internet Workshops (SAINT 2005 Workshops), pp.166-169. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1620003.
[9] Oh, S.H. & Lee, W.K., 2003. An anomaly intrusion detection method by clustering normal user behavior. Computers & Security, 22(7), pp.596-612.
[10] Pais, I. & Almeida, M., 2009. End User Behavior and Performance Feedback for Service Analysis. Intelligence in Next Generation Networks, 2009. ICIN 2009, pp.1-6.
[11] Barabas M, Boanea G, and Dobrota V, 2011. Multipath routing management using neural networks-based traffic prediction, in The 3rd International Conference on Emerging Network Intelligence, Lisbon, Portugal, Nov. 2011.
[12] Zhang, J. et al., 2009. A Distributed IPS Model Based On Neighbor Distance 1. IEEE Proceeding Ubiquitous, Autonomic and Trusted Computing, (09), pp.465-469.
[13] Ali M.K.M. and Kamoun F, 1993. Neural networks for shortest path computation and routing in computer networks, IEEE Transactions on Neural Networks, vol. 4, no. 6, pp. 941–954, Nov. 1993.
[14] Boanea G, Barabas M, Rus A.B., Dobrota V, and Domingo-Pascual J, 2011, Performance evaluation of a situation aware multipath routing solution, in 2011 RoEduNet International Conference 10th Edition: Networking in Education and Research, Iasi, Romania, Jun. 2011, pp. 1–6.
[15] Fadlullah Z, Tang F, Mao B, Kato N, Akashi O, Inoue T, Mizutani K, 2017. State-of-the-Art deep learning: evolving machine intelligence toward tomorrow's intelligent network traffic control systems, IEEE Communications Surveys & Tutorials. 2017, Issue: 99, DOI: 10.1109/COMST.2017.2707140
[16] Liu, F., Findlay, R. D. and Song, Q., “A Neural Network Based Electrical Loss Prediction of Bare Overhead ACSR Conductors” Proceeding of the First International Conference on Innovative Computing, Information and Control - Volume II (ICICIC'06), IEEE Press, 2006,
pp. 392-395.

[17] Gwon Y. L and Kung H. T, 2014, Inferring origin flow patterns in wi-fi with deep learning,” in Proceedings of the 11th International Conference on Autonomic Computing (ICAC ’14), pp. 18-20, Philadelphia, PA, USA, Jun. 2014.

[18] Ngia J, Khosla A, Kim M, Nam J, Lee H, and Ng A.Y ,“Multimodal Deep Learning,” in International Conference on Machine Learning (ICML), Bellevue, USA, Jun. 2011.

[19] Hawkins, J., and Blakeslee, S., “On Intelligence”, Owl Book, New York, 2005.

[20] Pasha M.F, Budiarto R, Ramadass S, and Syukur M, 2008. A sequential hierarchical superset implementation of neocortex memory system and its case study of automated network forensic analysis, Proc. of Int. Conf. on Artificial Intelligence 2008, Las Vegas, 14-16 July 2008, pp. 490-495.

[21] Rahmat R, Pasha M F, Syukur M, Budiarto R 2015 A gene-regulated nested neural network International Arab Journal of Information Technology 12 pp. 532–539

[22] Pasha M F, Rahmat R F, Budiarto R, and Syukur M 2010 A distributed autonomous neuro-gen learning engine and its application to the lattice analysis of cubic structure identification problem International Journal of Innovative Computing, Information and Control 6 pp. 1005–1022

[23] Hasibuan Z A, Rahmat R F, Pasha M F and Budiarto R 2009 Adaptive Nested Neural Network (ANNN) based on Human Gene Regulatory Network (GRN) for Gene Knowledge Discovery Engine IJCSNS International Journal of Computer Science and Network Security 9 pp. 43–54