Secure Threat Information Exchange across the Internet of Things for Cyber Defense in a Fog Computing Environment

Mihai-Gabriel IONITA, Victor-Valeriu PATRICIU
Military Technical Academy, Bucharest, Romania
mihai_ionita01@hotmail.com, vip@mta.ro

Threat information exchange is a critical part of any security system. Decisions regarding security are taken with more confidence and with more results when the whole security context is known. The fog computing paradigm enhances the use cases of the already used cloud computing systems by bringing all the needed resources to the end-users towards the edge of the network. While fog decentralizes the cloud, it is very important to correlate security events which happen in branch offices around the globe for correct and timely decisions. In this article, we propose an infrastructure based on custom locally installed OSSEC agents which communicate with a central AlienVault deployment for event correlation. The agents are based on a neural network which takes actions based on risk assessment inspired by the human immune system. All of the threat information is defined by STIX expressions and a TAXII server can share this information with foreign organizations. The proposed implementation can successfully be implemented in an IoT scenario, with added security for the "brownfiled" devices.

Keywords: *Cyber Defense, Neural Networks, Intelligent Threat Exchange, Internet of Things, Fog Computing.*

1 Introduction

The paper tackles one of the most important fields of cyber security. The following analysis concerns threat information exchange. Without information exchange a cyber-security system's functionality is severely hampered. An event might not trigger a specific danger threshold if attacks are stealthy and targeted. But the same attack, if information is gathered and correlated from different sources around an organization's network, might hit that specific threshold and also hit an alarm point which will be much more visible to a human operator. In different studies similar to [1] it is demonstrated that a single event can make the difference from an incident which is categorized as important and treated in a timely manner, to an incident that is categorized as usual activity and left uninvestigated. Information regarding cyber threats, when exchanged between entities involved in the same field of action, permits transforming information into intelligence. The topic discussed in the present paper is focused on intelligent threat exchange, which makes different checks and decisions before sending a series of information in a secure manner. Any attack detail can be used by a third party for exploiting different vulnerable resources from the protected organization. Another thorny problem of the current cyber security state is that of standardizing the way security incident information is normalized and packed for transport. This latter problem is also discussed in the current article.

In close correlation with information sharing and the standardization problem lies that of the ever changing cyber-security context. Where huge, cloud based, software code development and sharing platforms are under Denial of Service attacks from state entities. Security for the future of the internet has to be taken very seriously. The Internet of Things brings huge changes to the way security is planned and done. This article delves into the fog computing paradigm analyzing it and proposing different ways to secure end devices which, in the end, will be connected to the network. It also upgrades a currently implemented system for its integration with the fog computing paradigm. This system is based on an evolved micro distributed Security, Incident and Event Management (SIEM)-like architecture which bases its intelligence on a neural network, for collecting, analyzing and sharing threat information.

DOI: 10.12948/issn14531305/20.3.2016.02

2 Information Exchange Perspectives in the Present

In today's current cyber security world evaluating incidents without knowing what happens to adjacent network segments, neighboring countries or without having full visibility in your organization is unimaginable and a sure way toward failure. There have been different initiatives in this field but there is a huge problem which keeps the domain from evolving. This is the standardization of event information definition and the standardization of message format used for exchanging information regarding different cyber security events.

The organization which invests large amounts of money in any important initiative is the Department of Homeland Security (DHS) of the United States of America (USA). The interest of the DHS is to keep the pole position in this field which is of huge interest to the civil, governmental and military institutions of the USA. Cyber threat exchange through a standardized, reliable, tested and nonetheless secure protocol is of utmost importance. The USA have a large base of security information collectors, which are geographically distributed and are administered by different entities which sometimes may not be willing to share or give away all their collected security incident information to other entities from other fields of activity. As an example, maybe the public sector would be reluctant to share information with the governmental entities which are involved in intelligence collection activities. In the same direction, it may be possible that militarized structures would not want to give away attack information to civil organizations from the governmental hierarchy.

In this respect, there is high interest for selective security information sharing based on preset relationships with other organizations. But another problem consists of a drawback and this is the fact that log information has to be standardized when shared, otherwise computational resources and time will be lost for interpreting, integrating and correlating the received information into an organization's own database. This will of course, lead to delays in cross correlation of events and decision taking when quick action is needed.

2.1 Protocols for the Common Definition of Cyber Threat Information, Incidents and Indicators of Compromise (IOC)

As stated above, the DHS, one of the most active sponsors of the standardization initiatives has pushed through MITRE the Common Vulnerabilities and Exposures (CVE) standard which was adopted by more than 75 vendors and quickly developed into the de facto standard for defining vulnerabilities. Since then it is used for comparing different vulnerabilities from different vendors. And it is really helpful in comparing the severity of different exposures.

Another initiative the MITRE organization is pursuing for standardization is the Structured Threat Information eXpression (STIX) which is "a collaborative community-driven effort to define and develop a standardized language to represent structured cyber threat information. The STIX Language intends to convey the full range of potential cyber threat information and strives to be fully expressive, flexible, extensible, automatable and as human-readable as possible.[2]" The following Figure 1 depicts STIX's use cases with approaches for inter-organizational sharing, as well as sharing events outside an organization, with the interested community, for example. This example can be easily used inside an organization which is specialized in analyzing malware. When investigating a piece of code they would have specific information sharing needs, concerning only the team members designated for solving that task. After the analysis is complete, they may be willing to share some parts of the results with other similar organizations for threat sharing or collaboration on the matter. In the end, when the investigation is complete, the organization could decide to post an article about the malware's analysis and a few samples for the public community to realize what they are up against.

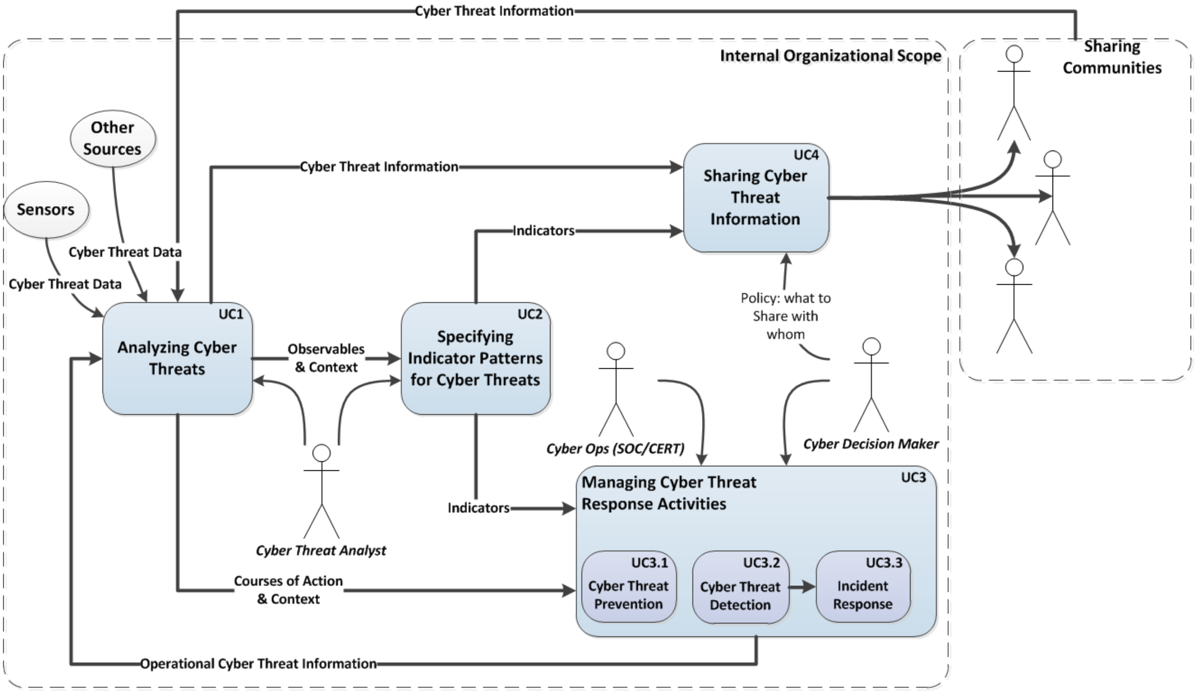

Fig. 1. Various STIX use cases [2]

2.2 Protocols for Securely Exchanging Cyber Incidents and Security Information

As in the previous section, MITRE is also working on standardizing the Trusted Automated eXchange of Indicator Information (TAXII), alongside STIX. "TAXII defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries. TAXII, through its member specifications, defines concepts, protocols, and message exchanges to exchange cyber threat information for the detection, prevention, and mitigation of cyber threats. TAXII is not a specific information sharing initiative or application and does not attempt to define trust agreements, governance, or other non-technical aspects of cyber threat information sharing. Instead, TAXII empowers organizations to achieve improved situational awareness about emerging threats and enables organizations to easily share the information they choose with the partners they choose.[3]"

This protocol is a flexible one, as it supports the major models for exchanging information in a graph architecture:

- Source-subscriber – one way transfer from the source to the subscriber, used in public/private bulletins, alerts or warning; as depicted in Figure 2.
- Peer-to-peer – both push and pull methodology for secret sharing, usually used in collaboration on different attacks. It allows the entities to establish different trust relationships directly with its partners by exchanging only the needed information. The model is illustrated in Figure 3.
- Hub-and-spoke – similar to the previous model, but here the dissemination of information happens through a central entity, the hub. Here different checking and vetting operations can be done on the information received from the spokes, before sending it to the other spokes, as shown in Fig. **4**.

Another strong initiative in this domain is that of NATO countries. They have come up with different frameworks for exchanging threat data in a secure manner.

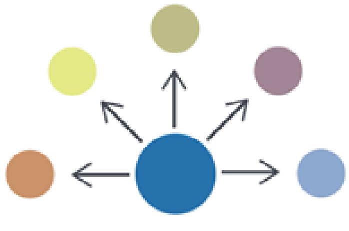

Fig. 2. Source-Subscriber model [2]

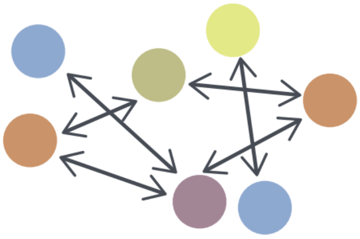

Fig. 3. Peer-to-peer model [2]

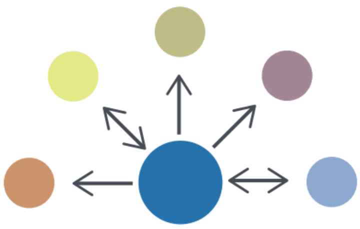

Fig. 4. Hub-and-spoke model [2]

The Cyber Defense Data Exchange and Collaboration Infrastructure (CDXI) [4] is one of the proposals which can be used on international level for cooperation. In a similar manner the Internet Engineering Task Force (IETF) has a set of standards for cooperation: Real-time Inter-network Defense (RID) and the Incident Object Description Exchange Format (IODEF), as further described in our article [5]. CDXI is one of the better documented proposals for an information sharing architecture for NATO partner countries. Its author, in [4] outlines the major problems of this domain:

"-there are no mechanisms available for automating large-scale information sharing" These are a must have in the context of the proposed architecture.

"-many different sources of data containing inconsistent and in some cases erroneous data exist." For a system that processes thousands of data streams, any delay can be considered catastrophic.

"-incompatible semantics using the same or similar words are used in different data sources covering the same topics." This only increases a repository size without adding any value and making it harder for a clustering algorithm to provide correct results. Once again, in this context it is very important to have a clear algorithm of Quality Assurance over data received from partners

3 Attacks are Evolving and Adequate Measures have to be taken

The massive Distributed Denial of Service (DDoS) which hit Github in 2015 was apparently directed against the github.com projects "GreatFire" and "CN-NYTimes" [6] which are preoccupied with circumventing China's Great Firewall (GFW) and preventing censorship for assuring freedom of speech. The "GreatFire" project is a Google mirror which makes Google searches available where they would be usually blocked. The latter project is in charge of hosting local NYTimes mirrors for Chinese citizens to read, without being forbidden the access to freely available information. Even a DNS poisoning attack in China can have a horrific effect for a usual, small enterprise target. As was the case with the server in [7] which was attacked by a huge number of IP addresses from China and later, after the DNS poisoning was stopped, he was still targeted by usual BitTorrent clients which saw the IP alive again. The phases such an attack follows are illustrated in the bellow Figure 5. Such rapid shifts in attack patterns can easily affect the balance of the internet. And there isn't much to do against them, except seek the Internet Service Provider's (ISP) assistance, which is the only one that can help with black-hole routing techniques, or offloading attack traffic to other resources or entities specialized for this type of traffic volume.

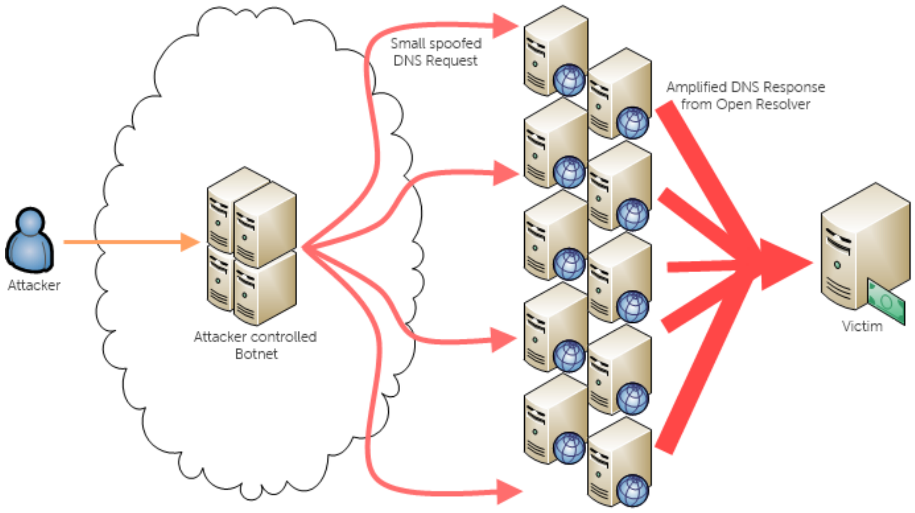

Fig. 5. The anatomy of a DNS amplification attack **[8]**

3.1 The Internet of Things

The Internet of Things (IoT) paradigm is greatly changing the way security is thought of and implemented. If the DDoS attack described in the above section is such a serious problem, what can be thought of the moment when almost every device will be directly connected to the internet with an IP address? The sixth version of the IP protocol (IPv6) is clearly the enabler here, as the address space for IPv4 is getting insufficient. As the authors wrote in [9], the security of the IoT is critical for a healthy evolution of the internet. On the same note, if these proposals are not respected, as we expressed our fears in [10], the scenario of a million A/C units from China attacking by DDoS a server in Europe could be a sad reality. Again, for preventing such events, the security has to be implemented in newly designed devices and manufacturers have to spend more money on testing for security flaws. For the so called “Brown Field” devices, as depicted in Figure 6, which will be adapted for the IoT era, their security has to also be adapted if we want a secure environment.

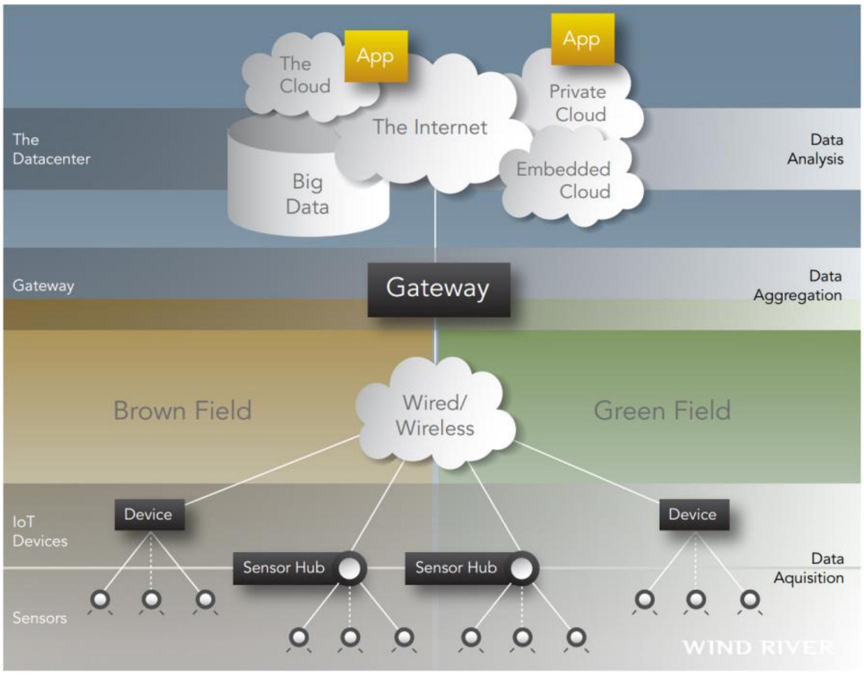

Fig. 6. A generic IoT topology **[9]**

DOI: 10.12948/issn14531305/20.3.2016.02

Unfortunately Crime as a Service (CaaS) is on the rise [11] and it will be of great interest to the authorities in the fore coming period when more and more devices will be directly connected and they will be remotely administered. The IoT paradigm also poses problem for existing administrative platforms which employ Machine to Machine (M2M) communication mechanisms. An increase in load may strain the protocols or security flaws may appear. Like any new concept which is implemented at such a large scale, it is impossible to correctly predict all the implications or foresee all the turning points. Thus, security updates have to be remotely pushed to any modern connected equipment. This is where Mobile Device Management (MDM) platforms will see an increase in popularity, and will be extended from administering smartphones, tablets and laptops, to smart-wearables, automotive components and house-hold items which will possess the intelligence and the connectivity to be remotely administered. In such a connected world the task for administering all the network equipment will be a hassle. Again, the stress on communication infrastructures will increase exponentially. And their criticality will be maximized. Administering security events will get to a whole new level, as the number of connected device grows, and any household will look like a small datacenter. Attacks will be much more easily planned with only a block of houses. Hiding attack traffic in the usual traffic, as its flow increases, will get easier. Storage capacity and speed requirements will skyrocket. Like it was said earlier, the number of security incidents will rise significantly and the need for threat information sharing will become critically needed. Without sharing threat information useful in correlating apparently disparate security incidents, large hacking campaigns will get unnoticed. Again, large amounts of stress will be put on human operators, which monitor these SIEM systems. The need for automated response and visual analytics will be essential for a healthy system or network.

Cognitive representation of events should be of prime importance for Chief Security Officers (CSO) who are going to catch the change in approach for security. Where the sheer number of events will be overwhelming even for a well-organized team of experts. Even in the present day, the number of security incidents can be overwhelming for some SIEM analysts in some larger enterprises. So the expansion of connected and monitored devices can only worsen the problem. The IoT adoption, even if sustained by different vendors and the developer community, has to be taken with great care as it will bring a major shift in perspective.

3.2 Fog Computing

Fog computing can be seen as the newest advance of virtualization. The fog computing concept took birth from the main need of reducing latency in the IoT world. It is conceived by Cisco [12] and is nothing else but an extension of the Cloud paradigm. They also use marketing terms as the “Internet of Everything (IoE)” which describes that in a not so distant future, all our devices will be connected. They even state in [12] that we are “returning” to the mainframe era of the 1950’s where people would use “dumb terminals” to access data stored on a huge computer called a mainframe. Those days are gone and now we use “thin clients” to connect to file servers or the cloud for accessing stored data in a virtualized environment, totally transparent for the user. Of course now there are other demands, data is diverse and its presentation to the user is totally different.

Returning to the motivation of the rebirth of this old model under the form of fog computing is given by the need to quickly access data, get commands or information from a computing node which is in close proximity. As depicted in Figure 7 below, it is important to bring the data and the processing power close to where the “things” needing it are. This can be seen as a good initiative both from a latency perspective as well as a security view. Nonetheless, storage of personal information is another problem of the cloud computing environment. Which was one of the problematic

DOI: 10.12948/issn14531305/20.3.2016.02

subjects in its adoption. Now, the fog computing component resolves this problem as personal information can be stored on a device as a set-top-box or a wireless access point near the client. This personal information can be accessed from any device in the household without privacy problems which appear in the cloud paradigm, where the discussion is open to who has access to personal data.

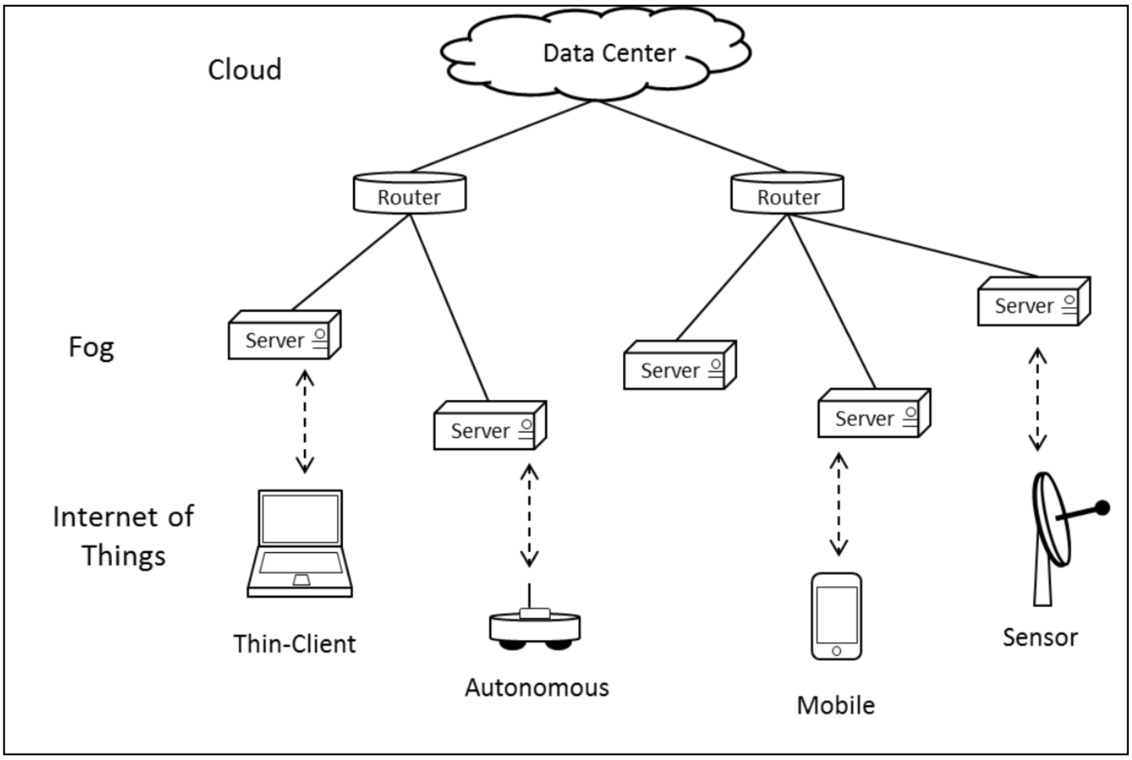

Fig. 7. Generic Fog Computing architecture **[13]**

The storage of data and deployment of applications can be done on a device under the ownership of the user, such as a networking device (router, switch access point), a set-top-box, an IP camera, or why not in the future, larger house hold items like a smart TV, a refrigerator etc. This service, as explained by the authors in [14] is very useful from a commercial point of view because it can be used as a replacement for the current "pay-as-you-go" solutions for distributing videos and other video-on-demand content. Another strong point of this approach is from the perspective of latency, real time load balancing and geographically distributed fail-over redundancy.

Another very important feature, which such a fog controller has, is great insight into the network it controls. And it can act as a localized sensor, which is geographically aware, for a security system or even as an Intrusion Detection System (IDS). If the fog controller is running on a network equipment, this one can be upgraded with a security appliance and turned into a web proxy with filtering capabilities and a sensor for an upgraded Security Incident and Event Management (SIEM) system, like the one we developed and presented in [15].

If talking only about architectural ties, then the fog computing (FC) paradigm is very similar to that of Software Defined Networking (SDN). The central authority of the FC paradigm sends commands to the fog controllers which are distant and located close to the end user. In a similar manner, the SDN controller updates flow tables in its flow compatible switches, which are usually closer to the client. This analogy makes combinations possible, like integrating fog computing into geographically distributed SDN networks. Where real-time load balancing, which is one of the starting points of fog computing creation, can be adopted in the construction of SDN networks.

DOI: 10.12948/issn14531305/20.3.2016.02

4 Security Concerns Regarding the Future of the Internet

The Internet is going towards new phases which nobody can predict if they will prove secure enough in the world we are living now. The research community is stronger than ever. Based on the current technological advancements, distributed research and collaboration is easier than ever. This is why the future of the Internet is so hard to foresee. On the other hand an implementation's security is quickly proven as vulnerable if it is posted online. The security community is very strong, the learning curve for attacking online resources is getting lighter and more script-kiddies are riding attack waves against medium to large enterprise infra-structures. Denial of Service (DoS) is less present than its bigger brother, the distributed kind of DoS. These are even more powerful in the last days when different amplification techniques are publicly available. To their aid come different global search engines like Shodan which indexes weak servers that can be exploited easily. Something similar happened with the Spamhouse attack [16] where Domain Name Service (DNS) amplification techniques were used for reaching a staggering 300Gbps attack.

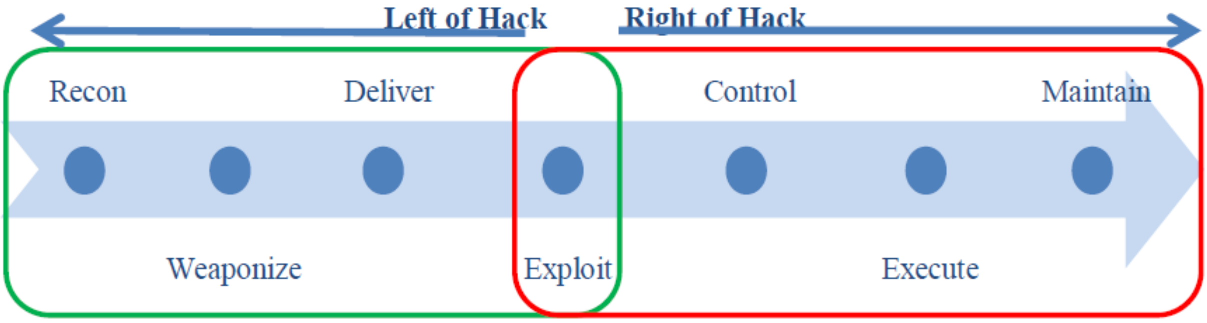

Fig. 8. The phases of exploiting a vulnerability **[2]**

For a successful (Advanced Persistent Threat) APT-less environment, attacks have to be detected during the reconnaissance phase, the “Recon” step depicted in the above Fig. 8. The attack can be stopped if it is detected all the way from the recon to the delivery step. Any exploit package should be stopped entering the organization until the exploit step, otherwise the only things protecting us are the host installed security applications such as classical antivirus solutions, which will surely be unavailable on an IoT device. Moreover, even if they would be installed, they could be unaware of a 0-day exploit.

Our agents, based on the artificial neural network are especially designed to detect APT attacks. Even if an APT is deployed on the monitored systems, it should be detected when it tries to make lateral movements, for additional discovery or for replicating on other systems.

APT lateral movement is the moment these pieces of malware are the most vulnerable to detection. Otherwise, during the other phases of the attack they are usually highly packed or lying dormant until specific actions are taken by the user.

In a fog computing environment, local, concentrated, DoS attacks will be very used, because there is no need for large bandwidths. A 5 GB/s attack is more than necessary to take out a usual home user or small enterprise. Also, like presented by Dr. Jordan in his research paper [13], reliance on distributed images for booting from the network could prove to be a thorny problem because of runtime errors or maliciously replacing them with “tainted” ones. Booting unsigned images, without verifying them could lead to starting attacks against other similar infrastructures without even knowing it. Zombies are the reason CaaS is so successful. Botnets are created from infected computers which later launch attacks to the bot herder's victim, without the actual user of the zombie pc even suspecting something. Weak authentication could lead

DOI: 10.12948/issn14531305/20.3.2016.02

again to brute force attacks, in which the attacker tries to generate all the possible combinations for guessing a password. In such a distributed environment, weak authentication could also pose problems when dealing with authenticating entities higher on the hierarchical chain. Failure of authenticating the master node in an SDN environment leaves the gate open for DoS or attacking other systems. The problem is similar in a fog computing setup, if we take into account the downloading Operating System (OS) applications from special repositories. Man-in-the-middle (MitM) attacks can be common in a geographically distributed network if correct cryptography is not used.

5 The Proposed Implementation

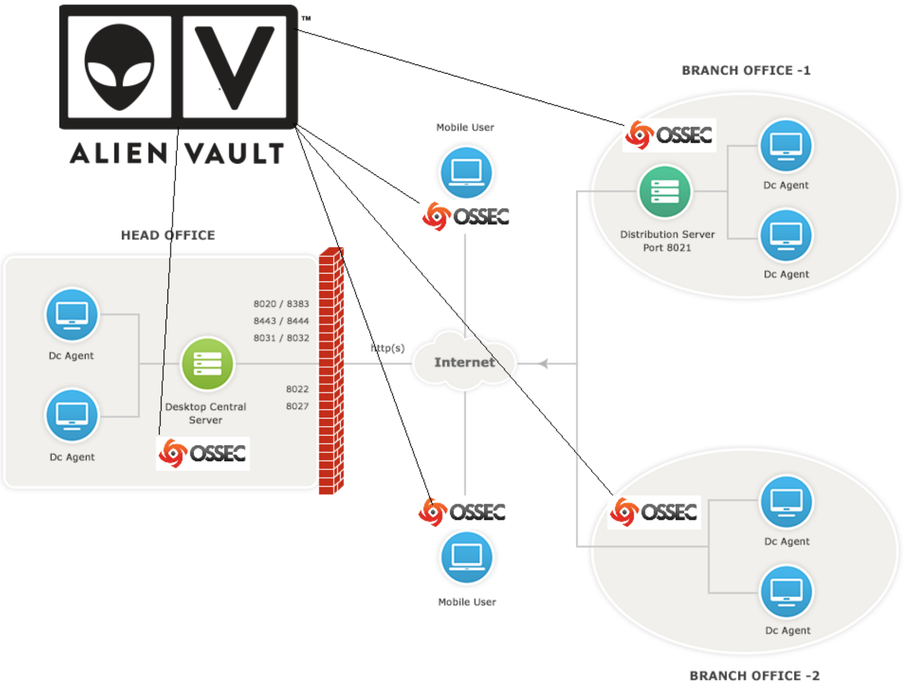

Fig. 9. The proposed implementation

The above depicted system, in Fig. 9 is the one used for information sharing. The above design illustrates a typical distributed system with a head office and multiple branch offices. All of these systems have installed and running a custom version of the popular Host Intrusion Detection System (HIDS) OSSEC. These act as micro Security Incident and Event Management (SIEM) in their environment. They collect logs from the systems they reside upon and exchange information with other similar agents in their branch. If instructed from the headquarters, full blown SIEM can exchange information between branches if the situation calls for quick action in a specific area. But usually they only exchange events inside the same branch because they only have pre-set a specific key, defined per branch. Those of the other branch agents are deployed from the central authority depicted as alienvault in the above Fig. 9, when needed.

Our proposed implementation uses STIX expressions for defining threat and attack information which are collected from the branch agents and imported into alienvault's Open Threat Exchange (OTX) feed for actionable correlations. If needed, the central authority has a functional TAXII server which can be used for communicating with other entities outside of the organization.

The custom OSSEC agents are based upon a neural network, better described in our article [15].

DOI: 10.12948/issn14531305/20.3.2016.02

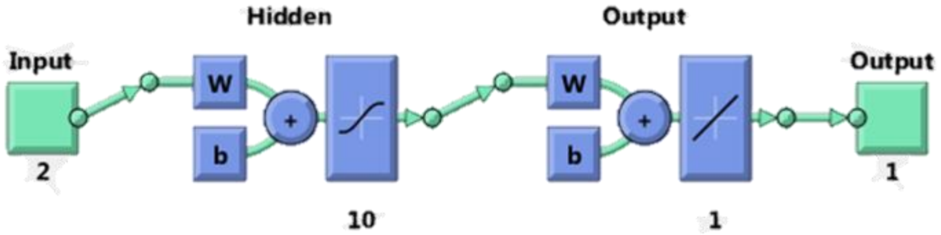

Fig. 10. The proposed architecture based on Feed Forward Backward Propagating Neural Network

As depicted in Fig. 10, "the proposed architecture implies a Feed-Forward Backward-Propagating neural network based on two input layers, ten hidden layers and one output layer. The training was done using 1000 input values and 1000 output values captured from a network of sensors formed by local agents, based on the processed security events. The training was done using the Levenberg-Marquardt method. Performance was calculated using the Mean Square Error approach. [15]".

As further explained in [10], our older article, we use the same experimental criteria for defining risk assessment metrics, as described below, in Table 1.

Table 1. Risk calculated for different types of attacks

Asset	**Determined risk using Neural Net**	**Probability**	**Harm**	**Calculated Risk**
Network info	0.0026	5	0	Null – 0
User accounts	12.0014	3	4	High – 12
System integrity	12.0013	4	3	HIGH – 12
Data exfiltration	12.0009	2	6	HIGH – 12
System availability	15.0007	3	5	HIGH - 15

The results in "Table 1" are obtained after comparing the output of the neural network to the calculated result of the following formula:

$$\text{Risk} = (\text{Probability x Harm})^{(\text{Distress\_ signal} + 1)}$$

6 Conclusions and Future Research

As stated above, threat exchange information is crucial for the development of the cyber security field. The detection of current, sophisticated, cyber-attacks is impossible without proper sharing of an organization's current attack information. If this information is introduced as input in our neural network, different correlations can be made which could detect sophisticated orchestrated attacks like APT campaigns which could go undetected if callbacks to C&C (Command and Control) servers are not registered. The key aspect and the "take away" idea of this paper is that without standardizing and normalizing events, all this collaboration would be impossible between organizations which have heterogeneous communication infrastructures.

The above proposed implementation fits very well in the fog computing design as a fog controller. This compute node which resides on the edge of the network is capable of inspecting all the network traffic which comes into its protected network as it is also able to inspect all the outbound traffic. The outbound traffic is specifically interesting because here callbacks to remote C&C servers can be investigated. Placed like this, the system is truly capable of protecting critical infrastructures from malware, APT threats and cyber espionage campaigns.

DOI: 10.12948/issn14531305/20.3.2016.02

In our opinion, in the adoption process of IoT the fog paradigm will be actively implemented because of the benefits described in the dedicated section. From these we underline: added privacy, increased bandwidth and reduced costs when it comes to bandwidth expenditures and leased lines.

For extending this implementation we are currently working on spreading this application in the "complicated" world of the Internet of Things with a custom built malware analysis platform especially designed for detecting APT attacks.

References

[1] S. Gupta, "Logging and Monitoring to Detect Network Intrusions and Compliance Violations in the Environment," *SANS Institute InfoSec Reading Room*, 07-Apr-2012. [Online]. Available: https://www.sans.org/reading-room/whitepapers/logging/logging-monitoring-detect-network-intrusions-compliance-violations-environment-33985. [Accessed: 27-May-2016].

[2] S. Barnum, "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX^{TM})," 20-Feb-2014.

[3] MITRE, "Trusted Automated eXchange of Indicator Information - TAXII: Enabling Cyber Threat Information Exchange." [Online]. Available: https://makingsecuritymeasurable.mitre.org/docs/taxii-intro-handout.pdf. [Accessed: 27-May-2016].

[4] L. Dandurand and O. S. Serrano, "Towards improved cyber security information sharing," in *5th International Conference on Cyber Conflict (CyCon), 2013*, 2013, pp. 1–16.

[5] M. G. Ionita and V. V. Patriciu, "Autoimmune Cyber Retaliation Supported by Visual Analytics," *J. Mob. Embed. Distrib. Syst.*, vol. 6, no. 3, pp. 112–121, Sep. 2014.

[6] E. Hjelmvik, "China's Man-on-the-Side Attack on GitHub," *NETRESEC Blog*, 31-Mar-2015. [Online]. Available: http://www.netresec.com/?page=Blog&month=2015-03&post=China%27s-Man-on-the-Side-Attack-on-GitHub. [Accessed: 27-May-2016].

[7] C. Hockenberry, "Fear China," *furbo.org*, 22-Jan-2015. [Online]. Available: http://furbo.org/2015/01/22/fear-china/. [Accessed: 27-May-2016].

[8] EVIL SECURITY, "DRDoS – Denial of Service on Steroids," *Evil Security*, 05-Apr-2015. [Online]. Available: http://www.evilsec.net/2015/04/drdos-denial-of-service-on-steroids/. [Accessed: 30-May-2016].

[9] M. Talwar, "Security Issues in Internet of Things," *Int. J. Emerg. Technol.*, vol. 6, no. 2, p. 364, 2015.

[10] P. V.-V. Ionita Mihai-Gabriel, "Achieving DDoS resiliency in a software defined network by intelligent risk assessment based on neural networks and danger theory," presented at the IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI), 2014, 2014.

[11] O. SCOTT-COWLEY, "The Rise of Cybercrime-as-a-Service," *MimeCast*, 23-Jul-2015. [Online]. Available: https://www.mimecast.com/blog/2015/07/the-rise-of-cybercrime-as-a-service/. [Accessed: 27-May-2016].

[12] Cisco, "Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are," *Cisco*, Apr-2015. .

[13] J. Shropshire, "Extending the Cloud with Fog: Security Challenges & Opportunities," 2014.

[14] I. Stojmenovic and S. Wen, "The Fog Computing Paradigm: Scenarios and Security Issues," 2014, pp. 1–8.

[15] M. G. Ionita and V. V. Patriciu, "Biologically inspired risk assessment in cyber security using neural networks," in *2014 10th International Conference on Communications (COMM)*, 2014, pp. 1–4.

[16] A. Balapure, "DDoS Attack on Spamhaus – An insight," *InfoSec Resources*, 15-

Apr-2013. [Online]. Available: http://resources.infosecinstitute.com/ddos-attack-on-spamhaus/. [Accessed: 27-May-2016].

Mihai-Gabriel IONIȚĂ has graduated the Military Technical Academy's Computer Science faculty in 2011. He holds a Master's Degree in Computer Science from 2013. And starting with the same year he is a PhD student in the Computer Sciences and Information Technology Doctoral School of the same university. He is passionate of all aspects regarding Cyber Security with emphasis on Artificial Intelligence, Malware Analysis and Cryptography. He is the author of 13 indexed research papers in the field of artificial intelligence and malware analysis.

Victor-Valeriu PATRICIU is an alumni of the Politehnica University of Timisoara, Computer Engineering Department, class of 1975. Mr. Victor-Valeriu PATRICIU obtained his Magna cum laude PhD in 1993 at Politehnica University of Bucharest, Computer Engineering Department, thesis: "Security of Distributed Systems and Computer Networks; A Software Toolkit for Generating Cryptographic Services for Networks and Distributed Systems". Mr. Victor-Valeriu PATRICIU started his university career in 1979 in the Computer Engineering Department from Military Technical Academy, first as teaching assistant between 1979 and 1985 then as associate professor from 1985 to 1995. Since 1997 to current he works as professor at the same university. Mr. Victor-Valeriu PATRICIU was a PhD adviser from 1997 in Military Technical Academy Doctoral School of Electronic, Informatics and Communication Systems for Defense and Security, in Computer Science & Information Technology domain. He is the official doctoral supervisor (Ph.D.) for students in Computer Science & Engineering.

DOI: 10.12948/issn14531305/20.3.2016.02