Some Aspects of Intrusion Detection in IoE

Eugen Petac
Faculty of Mathematics and Computer Science
“Ovidius” University of Constanța, Romania
epetac@univ-ovidius.ro
Petruț Duma
Faculty of Electronics, Telecommunications and Information Technology
Technical University “Gh. Asachi”of Iaşi, Romania
pduma@etti.tuiasi.ro

Abstract

People, processes, pieces of information and things are now presented together in the new concept, called Internet of Everything (IoE). Information security must be carefully analyzed and reconsidered in order to face new challenges of the IoE . The first two parts of the article point out these issues. The third part of the paper highlights security attacks, security services and security mechanisms. A number of IoE solutions for Intrusion Detection Systems, in the context of using computational intelligence methods, are presented in part four. IoE virtual Honeypots solutions are identified in the last part of the paper.

Keywords: IoE, Information Security, Intrusion Detection System (IDS), Honeypot
J.E.L. Classification: L8, M1, M3.

1. Introduction

In August 1962, J.C.R. Licklider from MIT introduced the concept of “Galactic Network” [1], basically beginning to lay the foundation of the Internet as a global network communication. As a concept of global interconnection, the Internet of today is not much different. But technology has evolved very fast. Each decade has made its mark on the development of the Internet [2]. Today, with a penetration rate of approximately 40.4% of the world population [3], the key terms are “more data, more collaboration, and more complex systems of interactions" [4]. Cisco has defined a new concept called Internet of Everything (IoE) [5]. To start with, it refers to bringing people, processes, data and things together. There are obtained network connections which are more relevant and valuable than ever before. This is accomplished by transforming the pieces of information into actions that create new functionalities. IoE allows the creation of economic opportunities for individuals, companies and countries. Cyber attacks, emerging threats, and new vulnerabilities present new challenges for the IoE. Cybersmart, Cybersecurity, and Cybersafety are some of the strategies adopted by many countries in the education and research programs. It is important to be brought into attention for the economic and business environment to be an active partner in implementing IoE Security.

2. IoE Overview

IoE appears as a higher level of the Internet of Things (IoT), which corresponds to the networking of physical objects and the use of one of the existing communication technologies, with the purpose of creating greater utility value [6].

We refer to the IoE when adding superior capabilities to the IoT. These can include: the awareness of the context, an increase in the power of processing, independent energy supply and increasing of the recruitment and use of new types of information that are connected. IoE is heterogeneous, comprising both products and services vertical and horizontal - wired and wireless, indoor and outdoor pools, and is populated by a variety of products that fall within the range of simple devices to complex computing devices. All these capabilities are smart networks and services that are connected. The evolution of the Internet has been through four distinct phases, each characterized by a rapid growth of increasingly large business and, generally, of establishment: connectivity, network economy, collaborative experience, Internet of Everything (IoE). Services like the e-mail, web browsing, search content etc, are specific to the connectivity phase. E-commerce and supply chain digitization of the economy are characteristics of the second phase, the network economy, which has begun in the late 1990s. The collaborative experience with social media services, video, mobility and cloud computing completely transformed the world, starting with the year 2000. This is the IoE's stage of evolution of the Internet that connects people, processes, data and things. According to some studies [5],[7], it is expected that the number of connected devices and objects will exceed 50 billion by 2020. By 2022 the IoE can increase company profits by over 20%. Until 2018 data traffic in mobile networks will grow 11-fold to 190 exabytes an annual volume of 190 exabytes [8]. In the context to the increasing number of mobile connections to the Internet, mobile devices, but also to the number of connections and Machine-to-Machine (M2M), they will exceed the 10 billion by 2018 [8]. Cloud services are key to the IoE deployments. It is expected a significant increase in data traffic in the cloud, from 3.1 zettabytes in 2013 to 8.6 zettabytes 2018 [7], [8]. IoE becomes a network of networks where billion connections create unprecedented opportunities, but also new information security risks. Information to anyone, at any time and can be accessed from anywhere is what the people wanted all the time from the Internet. Software vulnerabilities, erroneous configuration, negligence regarding the handling of data are some of the causes that led to the problem of the Internet regulation. Four phases are defined [9] for the Internet regulation: *open Internet*, from the network's birth through about 2000; *access denied*, through about 2005; *access controlled*, through about (2010); and *access contested*, the actual phase.

3. Security Approaches

Information security is a broad concept that refers to the insurer of the integrity, of the confidentiality and availability of information, regardless of its form. Authentication, authorization and non-repudiation are closely related to the IoE entities (people, processes, things) that are using this information.

In the security sense it is discussed attacks, mechanisms and services [10], [11]. Any action that compromises the security of information represents a security attack. This action can be passive (a release of message contents or traffic analysis) or active (Masquerade, Replay, Modification of message contents, Denial of Service - DoS, Distributed Denial of Service - DDoS). A security mechanism is designed to detect, prevent, or recover from a security attack. Encipherment, digital signature, access control, data integrity, authentication exchange, traffic padding, routing control, notarization are some of the main security mechanisms that provide adequate security. Security service enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms. The main security services are: data confidentiality (connection, connectionless, selective field, traffic flow), authentication (peer entity, data origin), data integrity, non-repudiation (with proof of origin/ delivery), access control, availability.

An intrusion is defined as a set of unauthorized activities attempting to compromise integrity (the attacker can modify the system state and alter the data without proper authorization from the owner), confidentiality (the attacker gains access to confidential and otherwise inaccessible data) or availability (the system is either shut down by the attacker or a resource made unavailable to general users). One can reach the critical situation in which the attacker gains full control of the system and can alter the access privileges of the system, with a potential risk of compromising overall system resources.

Intrusion Detection corresponds to a set of techniques and methods used to detect suspicious activities at both the host (Host Based Intrusion Detection - HIDS) and/or the network level (Network Based Intrusion Detection - NIDS). It is very important the analysis of the suspicious activities in order to detect the possible incidents of imminent threats of violation of security policies, acceptable use policies, or standard security practices. The detection of any intrusion and the attempt to remove a possible incident allows the intrusion prevention. Intrusion Detection Prevention Systems (IDPS) encompasses both the detection and the intrusion prevention aspects. Referring to the IoE, few of the main purposes for which the IDPs sites should be considered are:

- The identification of possible incidents, recording information about them, trying to remove the incident and reporting it to the security administrators.
- The identification of issues regarding security policies, documenting the existing threats and deter individuals to violate the security policies.

4. Related Work

Intrusion detection methods are relatively new. These involve gathering information about known attack types and detection of any attempts to compromise a network or, in particular, attack one specific entities in the network. Detection of intrusion depends on the understanding of the security administrator of how the attack works. The information collected can be used to strengthen the strategic security of a network or other legal purposes.

In terms of techniques used, an IDS can be passive (detects a potential security breach, records information and alerts the administrator) or active (suspicious activity responds by terminating the connection or blocking network traffic from suspected malicious source). On the other hand, the IDS may be based on anomalies (Anomaly Based IDS – ABIDS) or signature/rule based (Signature Based IDS - SBIDS) or hybrid.

An ABIDS establishes a baseline of performance-based on assessments of normal network traffic. The IDS will report current network traffic from the baseline established to assess whether or not fall into the normal range. A fully taxonomy of ABIDS [12] contains a series of Techniques used to detect intrusion, with a number of remarks about the advantages and disadvantages: Statistical anomaly (Operational Model or Threshold Metric, Markov Process Model or Marker Model, Statistical Moments or Mean and Standard Deviation Model, Multivariate Model, Time Series Mode), Data mining based approach (Clustering, Association rule discovery, Classification), Knowledge based detection (State Transition Analysis, Expert Systems), Signature Analysis, Petri Nets), Machine learning (Bayesian Approach, Neural Networks, Fuzzy Logic, Genetic Algorithms, Support vector machines). To this it is added ABIDS based on new technologies such as: Evolutionary Computation [13], DNA Computing [14], Membrane Computing [15], Quantum Computing [16], Swarm Computing [17].

A SBIDS examines the network traffic looking for preconfigured attack patterns and predetermined known signatures (e.g., nature of data packets, failed attempt to run an application, failed logins, file and folder access etc.). A collection of such signatures must be updated constantly. A SBIDS has the following advantages: simple to implement, lightweight, low false positive rate, high true positive rate for known attacks. The disadvantages of SBIDS are: signature database must be continually updated and maintained, may fail to identify a unique attacks and low detection rate for zero day attacks [18]. There are a number of solutions based on Snort [19],Aho-Corasick Algorithm [20], Boyer-Moore Algorithm [21].

Different types of IDS or combinations of them, may (or may not) be appropriate to protect the resources of IoE entities, depending on the security policy adopted. It is very important to take into account a number of factors that may limit the capabilities of an IDS. These include: failure to update signatures - a collection of signatures that is not updated can leave the IDS vulnerable to attack strategies; a small number of attacks – the real attacks can be so far below the rate of false alarms that are usually ignored by the IDS; very high rate of false alarms due to erroneous packets generated by the malfunction of software, altered DNS data and lost local packets. In addition, the attacker has access to a number of techniques to avoid the IDS's: DoS/DDoS attacks on IDS - it consumes the resources and generates a large number of false alarms and are able to hide real attack; traffic insertion in IDS - an attacker can send packets that will reach not only the target IDS station resulting in a series of false alarms; protocol violations – deliberate violations of TCP or IP so that the target station will handle different packages than the IDS; overlapping fragments - technique that involves creating TCP packets with sequence numbers that are overlapping; fragmentation and sending of small packets - a basic technique which involves the fragmentation of information into multiple smaller packages makes it impossible to reconstruct the IDS session.

Intrusion Detection depends on the understanding of how the attack works by both administrators in security, in general, and by an information security culture [22], [23]. This way, the IOE brings together people, processes, and things.

5. Honeypot as IoE Security Solution

The Honeypot (HYP) is a flexible, software and/or hardware, used for detecting or rejecting the unauthorized use of a system attempts, recording instruments used by attackers. When the HYP detects an intruder, it seems to be part of a defenceless components of the system (though isolated and protected), that contains both useful files and pieces of information that allow access to other networks. Once the intruder process enters the system, the IDS records information about it. For the regular users, the HYP does not have any value while interaction with it is an unauthorized activity. The HYP only collects information when an entity is interacting with it, having the specific nature of the trap. Data generated are fewer, and thus easier to analyse. Since interacting only with unauthorized activities, suitable for attack attempts, the number of false alarms is small. It should be pointed out that there are some drawbacks to be considered: introducing of a significant risk factor in the system as a result of exposure to potential attacks; specializing in a particular type of interaction, such as http, smtp or ftp services; because they have a common behaviour, there is a risk for the HYPs to be easily detected.

- With low interaction: emulate network services or components of an operating system; they are easy to install, more secure, but collect less information.
- With enhanced interaction: simulate all aspects of an operating system; they can be fully compromised, allowing other attacks; collect large amounts of information.

For the IoE, HYPs can successfully contribute to improving the security eof the entities. Through HYPs attack tools and methods, as well as methods of communication, organization and motivations of attackers can be determined. Our experiments have shown the benefit of virtual HYP solutions: HoneyDrive [24], Dionaea [25], Kippo SSH [26], SHIVA (Spam Honeypot with Intelligent Virtual Analyzer) [27].

6. Conclusions

The Connectivity and advanced intelligent interaction between people, devices, systems and services, this is what IoE is ready to offer. The interconnection will require new strategies in all areas and will allow the development of complex applications. In such a context, the entire vision on information security will change. Of course, there will be different running costs. In Europe the information security budget has increased in 2014 compared to 2013 from 3.0 million $ to 3.4 million $, and in the US from 4.5 million to $ 4.6 million $ [28]. Security policies and processes will be part of the core of the IoE Security. Security based on identity is the favorable solution for the IoE în connection to security based on perimeter. Intrusion detection requires finding new solutions based on computational intelligence and virtualization. Among other things, IoE includes: permanent identification of possible weaknesses, constant review of the security policies and a continuous process of security education.

7. References

[1] Leiner, B.M., Cerf,V.G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C., Postel, J., Roberts, L. G., Wolff, S., “Brief History of the Internet”, 15 Oct 2012, retrieved from http://www.internetsociety.org/, 2015.

[2] Cohen-Almagor, R.,, “Internet History”, *International Journal of Technoethics*, 2(2), 45-64, April-June 2011, retrieved from http://www.hull.ac.uk/rca/docs/articles/,2015.

[3] ITU, *Manual for Measuring ICT Access and Use by Households and Individuals* 2014,

retrieved from http://www.itu.int/pub/D-IND-ITCMEAS-2014, 2015.

[4] NSF, "Research on Today's Internet", retrieved from http://www.nsf.gov/about/ history/ nsf0050/pdf/internet.pdf, 2015.

[5] Bradley, J., Reberger, C., Dixit, A., Gupta, V., "Internet of Everything: A $4.6 Trillion Public-Sector Opportunity", retrieved from http://ioeassessment.cisco.com/learn, 2015.

[6] Höller, J., Tsiatsis, V., Mulligan, C., Karnouskos, S., Avesand, S., Boyle, D., "From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence", Elsevier, 2014.

[7] Bradley, J., Barbier, J., Handler, D., "Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion", retrieved from http://www.cisco.com/web/ about/ac79/docs/innov/, 2015.

[8] Cisco, "Cisco Visual Networking Index: Forecast and Methodology, 2013–2018", retrieved from http://newsroom.cisco.com/ release/1426270, 2015.

[9] Palfrey, J. G., "Four Phases of Internet Regulation", *Social Research*, Vol. 77, No. 3, Fall 2010, Berkman Center Research Publication No. 2010-9, retrieved from http://ssrn.com/abstract=1658191, 2015.

[10] Stallings, W., *Cryptography and Network Security: Principles and Practice*, 6th Edition, Prentice Hall, 2013.

[11] Stallings, W., *Network security essentials: applications and standards*, Prentice Hall, 2007.

[12] Gyanchandani, M., Rana, J. L., Yadav, R. N., "Taxonomy of Anomaly Based Intrusion Detection System: A Review", *International Journal of Scientific and Research Publications*, Vol. 2, Issue 12, December 2012, retrieved from http://www.ijsrp.org/ research-paper-1212/ijsrp-p1232.pdf, 2015.

[13] Sen, S., *Evolutionary Computation Techniques for Intrusion Detection in Mobile Ad Hoc Networks*, PhD Thesis, University of York, United Kingdom, 2010, retrieved from https://www.cs.york.ac.uk/nature/group/these s/SevilSen.pdf , 2015.

[14] Mahdy, R., Saeb, M., "Design and Implementation of an Anomaly-based Network Intrusion Detection System Utilizing the DNA Model", *Proceeding of the 9th WSEAS Int. Conference on Data Networks, Communications, Computers*, Trinidad and Tobago, November 5-7, 2007, retrieved from http://www.wseas.us/e-library/conferences/2007trinidad/, 2015.

[15] Rufai, I. K., Muniyandi, R. C., Othman, Z. A., "Improving Bee Algorithm Based Feature Selection in Intrusion Detection System Using Membrane Computing", *Journal of Networks*, Vol. 9, No. 3, March 2014, retrieved from http://www.academypublisher .com/jnw/vol09/no03, 2015.

[16] Omar S. Soliman, S.O., Rassem, R., "A Network Intrusions Detection System based on a Quantum Bio Inspired Algorithm", *International Journal of Engineering Trends and Technology* (IJETT) – Vol. 10 No.8, Apr 2014, retrieved from http://arxiv.org/ftp/ arxiv/papers/1405/, 2015.

[17] Satpute, K., Agrawal, S., Agrawal, J., Sharma, S., "A survey on anomaly detection in network intrusion detection system using particle swarm optimization based machine learning techniques", In *Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications* (FICTA), pp.441–452. Springer, 2013.

[18] Bilge, L., Dumitras, T., "Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World", In *ACM Conference on Computer and Communications Security*, Raleigh, NC, October 2012.

[19] Snort - Open source network intrusion prevention system, retrieved from https://www.snort.org/, 2015.

[20] Marc Norton, M., "Optimizing Pattern Matching for Intrusion Detection", retrieved from http://citeseerx.ist.psu.edu/, 2015.

[21] Xiong, Z., "A Composite Boyer-Moore Algorithm for the String Matching Problem", In *Parallel and Distributed Computing, Applications and Technologies* (PDCAT), 2010 Int.Conf. , pp.492-496, 8-11 Dec. 2010.

[22] Niekerk,J.,F.,V., Solms,V., R., "Information security culture: A management perspective", In Computers & Security, Vol. 29, Issue 4, June 2010, pp. 476–486, retrieved from http://www.sciencedirect.com/, 2015.

[23] Olivos, O., "Creating a Security Culture Development Plan and a Case Study", *Proceedings of the Sixth International Symposium on Human Aspects of Information Security & Assurance* (HAISA 2012), Crete, Greece, June 6-8, 2012.

[24] HoneyDrive, retrieved from https://www. honeynet.org/node/1177, 2015.

[25] Dionaea retrieved from http://dionaea. carnivore.it/, 2015.

[26] Kippo SSH, retrieved from https://code. google.com/p/kippo/, 2015.

[27] SHIVA, retrieved from https://www. honeynet.org/node/1078, 2015.

[28] "Global State of Information Security Survey 2015", *PwC Report*, retrieved from http://www.pwc.com, 2015.