Proc. of The Third Intl. Conf. on Advances in Computing, Electronics and Communication - ACEC 2015
Copyright © Institute of Research Engineers and Doctors, USA .All rights reserved.
ISBN: 978-1-63248-064-4 doi: 10.15224/ 978-1-63248-064-4-07

An Extended Human Threats Taxonomy To Identify Information Security Breaches

İhsan Ömür Bucak

***Abstract*— Many Information Security (IS) researchers emphasize the importance of human factor within information security. The main problem is that the ones responsible for information security do not take the thoughts, feelings and behavior of employees into account. It is common for organization management and people responsible for security not to listen to employees but mainly deal with commanding them. Unintelligent countermeasures may result in employees behaving in a way that would negatively affect security, because security solutions are developed to attempt to protect information, but the human factor is often left without attention. Taxonomy is an important milestone for this work because it will enhance the ability to examine the problem in a more systematic way and will eventually contribute to the establishment of a behavior-based intrusion detection model. The taxonomy work here covers a more recent and up-to-date taxonomy effort with increased dimensions and features. None of the previous taxonomies are directly related with the detection of human threats. By doing so, we create chances to measure the detection rate of attack types.**

Keywords—information security; taxonomy; intrusion detection systems; human factors

I. Introduction

Many Information Security (IS) researchers emphasize the importance of human factor within information security [1-3]. Gardner states that a human is not used to thinking that his feelings are a source of his conscious decisions, but many researchers prove that human behavior is affected by cognition and affect [4]. But the human brain is designed with blind spots, not only optical, but also psychological [5]. Even those who have knowledge and skills have blind spots and make errors all the time [3]. An employee can contribute to the security related actions every day, and his/her view on information security is built on organizational, technological and individual factors [6]. Information security usually has a lot of tradeoffs and mainly it affects functionality – employees have various limitations to perform their duties.

The main problem is that the ones responsible for information security do not take the thoughts, feelings and behavior of employees into account. Reference [7] even states that it is common for organization management and people responsible for security not to listen to employees but mainly deal with commanding them. Reference [3] notices the important characteristics of information security practice within organization – it arouses emotions, sometimes even significant negative emotions. Unintelligent countermeasures may result in employees behaving in a way that would negatively affect security, because security solutions are developed to attempt to protect information, but the human factor is often left without attention [8].

II. Intrusion Detection Systems

Intrusion Detection Systems (IDSs) are monitoring systems which are used to detect intrusions on a computer or a network. Intrusions are unauthorized and anomalous activities which were defined as "a sequence of related actions performed by a malicious adversary that results in the compromise of a target system" in [9]. An intrusion detection system is an indispensable tool for network administrators because, without such a device, it would be impossible to analyze the huge amount of packets traversing current networks every second. After more than thirty years of intensive research on intrusion detection systems, the field is still open to further investigations especially regarding the accuracy of the detection. Moreover, variants of known attacks as well as new attacks can often go through the system without being detected.

According to [10], a good intrusion detection system detects a wide variety of intrusions, in a timely fashion, and presents analysis results as simply and accurately as possible, using any combination of anomaly detection, misuse modeling, or signature detection to identify threats. Anomaly detection works by assuming that attacks look out of the ordinary. Before we can find an anomaly, we need to map out what is normal, and using thresholds look for traffic that is out of these bounds. Misuse modeling looks for specific commands or actions that lead to a known misuse or abuse of otherwise appropriate system states. Signature detection involves recognizing patterns of known code states that can put the system in an undesirable state when executed.

Intrusion Detection Systems (IDSs) and behavior classification have come a long way since the inception of digital forensic auditing. IDSs cannot detect all types of intrusions, as attack permutations are constantly being generated. Attack types can have many permutations, and static signatures do not always work. The alternative to signature detection, namely threshold establishment and monitoring, is used to detect the unknown. A number of machine learning algorithms can be used to effect the classification of normal and malicious network traffic, enhancing an IDS to be able to generalize network traffic into "good" and "bad", thereby avoiding the necessity to use exact string matches [11].

III. Classifying Intrusion Incidents

Upon looking through the literature, taxonomy work in this paper has aimed to acquire the strengths of the taxonomies in [12] and [13] as they differ considerably from the others. Reference [12] surveys the extrinsic and intrinsic motivations that influence the propensity toward a compliant information security behavior. It also indicates that the

İhsan Ömür Bucak , Assoc. Prof.
Melikşah University
Kayseri, Turkey

compliant information security behavior refers to the set of core information security activities that have to be adhered to by end-users to maintain information security as defined by information security policies. In addition, the compliance mindset also subscribes to what might be called a deterrence theory of motivation, which employs mandates, procedural controls and threats of punishment to manage and motivate people.

One of the most referred taxonomy was published in [13] which defines behavioral information security as the human actions that influence the availability, confidentiality, and integrity of information systems. Reference [13] uses social, organizational, and behavioral theories and approaches, and conducts a series of empirical investigations in developing taxonomy of security behaviors and identifying the motivational predictors of such behaviors. However, the taxonomy in [12] has been found very theoretical mostly related with motivation but it was advanced. On the other hand, the taxonomy in [13] was very practical but it was basic. At this point a practical and advanced taxonomy study that can combine their main strengths came forward as a result. The taxonomy in [13] has also been found very useful and improvable. Firstly we thought about adding impact level as the third dimension because the impact level is related with the risk of the behavior. If one can define the risk of a behavior, one can take precautions to reduce or avoid it and if the risk is low or the cost of treatment is not cost-effective for the organization, it can be ignored [14]. We get the impact levels from National Vulnerability Database (NVD) [15], Common Vulnerability Scoring System (CVSS) [16], and Common Vulnerabilities and Exposures (CVE) [17].

Upon adding the impact level we obtained a three level taxonomy as shown in Table I and we know the risk level of the behavior so that we can accept it or ignore it but how can we detect it? Another dimensional need came out with the motivation of this question. None of the previously mentioned taxonomies are oriented towards detection of insider misuse, in terms of considering how we would approach the task of monitoring activities to determine where problems may be apparent.

In determining a means to link classification to the method of detection, it is considered appropriate to classify human behavior as based on the level of the system at which they might be detected. The basis for this is that different types of behaviors manifest themselves at varying layers of the system. With this form of classification in mind, the concept can be illustrated using a variety of recognized insider activities, and then considering the different layers at which they may be detected. The classification is presented in Table II, and then examples of the incidents concerned are considered in the sub-sections that follow. These consider what could be monitored, and how this could be used to detect, control and restrict misuse-related behavior.

There are a large variety of different attack types [18]. An attacker may attempt to guess a user's password. Attackers may also monitor the network to obtain the information they require to launch an attack. Sometimes attackers try to put unauthorized programs onto computers that they have access to. Sometimes they may steal information or corrupt information. They may also try to perform a denial of service attack. A good taxonomy makes it possible to classify individual attacks into groups sharing common properties [19]. One widely used taxonomy divides attacks into four classes [20]: Probes, Denial of Service (DoS), User to Root (U2R) and Remote to Local (R2L).

Threat type is important; because if we want to manage the threats we need to be able to detect them, so we add threat type attribute in our taxonomy and we get five-dimensional Human Threats Taxonomy as shown in Table III.

IV. Conclusions

In the last section, we classified human threats and to prevent those threats, we need to detect them. There are many approaches which use data mining algorithms to detect insider attacks. Network based detection is one of the mechanism to accurately distinguish insider behavior from the normal behavior. Anomaly detection has attracted the attention of many researchers to overcome the weakness of signature-based IDSs in detecting novel attacks [21]. However, when we look at the state of the detection solutions and commercial tools, there is little evidence of using the anomaly detection approach, and people still think that it is an immature technology. We believe that if we productively apply machine learning while narrowing the large variety of algorithms, we can get high detection rate, low false alarm rate and better time cost in anomaly detection. In order to accomplish this goal, a suitable experimental methodology can be designed with the following properties in mind:

- Algorithms should be selected from a variety of statistical models in the machine learning area, so proper representations of the fundamental options are tested.
- The dataset against which the algorithms are tested should be a realistic representation of both normal and abnormal traffic, including zero-day attack instances.

We have classified the human behaviors and defined the attack types of the behaviors in order to define the risk and measure the detection rate of those threats individually. Detection rate is an important factor in determining the risk. None of the previous taxonomies are directly related with the detection of human threats. By doing so, we create chances to measure the detection rate of attack types. We introduced a most up-to-date taxonomy which aims to encompass today's human threat factors associated to legitimate user actions. We described the impact level of attacks and also described the attack types. We added these attributes because they are significantly related with anomaly detection. We gave examples about the human threats. The taxonomy is tailored to the needs of automated human threat prediction. The establishment of this classification scheme paves the way for the construction of a suitable behavior-based intrusion detection system. Taxonomy is an important milestone for this work because it will enhance the ability to examine the problem in a more systematic way and will eventually contribute to the establishment of behavior-based intrusion detection systems. In our human threats taxonomy, we divided attacks into four

Proc. of The Third Intl. Conf. on Advances in Computing, Electronics and Communication - ACEC 2015
Copyright © Institute of Research Engineers and Doctors, USA .All rights reserved.
ISBN: 978-1-63248-064-4 doi: 10.15224/ 978-1-63248-064-4-07

classes: Probe, User to Root, Remote to Local, and Denial of Service attacks. The objective is to find the machine learning algorithm that can detect the anomalies with the highest accuracy. Therefore, by running the algorithm with the highest accuracy, we can measure the detection performance of attacks by types which we have defined in our taxonomy work.

References

[1] J. Colley, The information security professional is more than 'a necessary evil', 2007.

[2] B. Schneier, "The psychology of security", Progress in Cryptology – AFRICACRYPT, Vol. 5023, pp. 50-79, 2008.

[3] A. Mcllwraith, Information security and employee behavior: how to reduce risk through employee education, training and awareness, Gower, Hampshire, 2006.

[4] D. Gardner, The Science of Fear, Dutton, New York, 2008.

[5] C. Tavris and E. Aronson, Mistakes were made (but not by me), Harcourt, Florida, 2007.

[6] E. Albrechtsen, A qualitative study of users' view on information security, 2007.

[7] M. E. Kabay, Using social psychology to implement security policies, 2002.

[8] K. L. Thomson, R. Solms, and L. Louw, Cultivating an organizational information, 2006.

[9] C. Kruegel, F. Valeur, and G. Vigna, "Intrusion Detection and Correlation: Challenges and Solutions", Advances in Information Security, Vol. 14, Springer-Verlag, 2005.

[10] M. Bishop, Introduction to Computer Security, Addison Wesley, Boston, 2005.

[11] I. Chairunnisa, Lukas, and H. D. Widiputra, "Clustering based intrusion detection for network profiling using k-means, ecm and k-nearest neighbor algorithms" Konferensi Nasional Sistem dan Informatika, pp. 247-251, Bali, 2009.

[12] K. Padayachee, "Taxonomy of compliant information security behavior", Computers and Security, Vol. 35, No. 5, pp. 673-680, 2012.

[13] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors", Computers and Security, Vol. 24, No. 2, pp. 124-133, 2005.

[14] ISO, ISO/IEC 17799 Information Technology, Security Techniques, Code of practice for information security management, 2005, retrieved on October 10th, 2013.

[15] NVD, National Vulnerability Database, November 2013, URL http://nvd.nist.gov, Accessed in January 20th, 2014.

[16] CVSS, Common Vulnerability Scoring System, November 2013, URL http://www.first.org/cvss, Accessed in January 20th, 2014.

[17] CVE, Common Vulnerabilities and Exposures, November 2013, URL http://cve.mitre.org, Accessed in January 20th, 2014.

[18] Fyodor, Fyodor's Exploit World, September 2013, http://insecure.org/sploits.html, Accessed in December 15th, 2013.

[19] S. Mukkamala, A. Sung, and A. Abraham, "Intrusion detection using ensemble of soft computing and hard computing paradigms", Journal of Network and Computer Applications, Vol. 28, pp. 167-182, 2005.

[20] K. Kendall, A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems, Master's Thesis, MIT, 1999.

[21] A. A. Ghorbani, W. Lu, and M. Tavallaee, Network Intrusion Detection and Prevention: Concepts and Techniques, Springer, New York, 2010.

About Author:

BS and MS, Istanbul Technical University, PhD, Oakland University, Michigan, 2000. Research strength mainly lies on Computational Biology, Modeling and simulation, Artificial Intelligence (Pattern Recognition, Machine Learning, Computer Vision, and Artificial Neural Networks, Nonlinear Learning Theory and Reinforcement learning and its variants), and Control Systems (Hybrid Electric Vehicles and Energy Management Strategies).

TABLE I. 3-D HUMAN THREATS TAXONOMY

Expertise	**Intention**	**Impact Level**	**Title**	**Description**	**Example**
High	Malicious	High	Intentional destruction	Behavior requires technical expertise together with a strong intention to do harm to the organization’s IT and resources and has high impact level.	Employee breaks into an employer’s protected files in order to steal a trade secret.
High	Malicious	Medium	Man in the middle	Behavior requires technical expertise and includes intention to do harm through annoyance, harassment, rule breaking, etc. and has medium impact level.	Employee stands in the middle of a communication between two hosts. By poisoning the ARP table of one of the two hosts taking part in the communication, the attacker can redirect the traffic to his computer first and then forward it to the intended destination after having read the content of the message.
Low	Malicious	High	Resource exhaustion	Behavior requires minimal technical expertise but nonetheless includes intention to do harm through annoyance, harassment, rule breaking, etc. and has high impact level.	Employee sends large ping packets to a computer or a server, resource exhaustion occurs when the server or the computer receives more queries than it can process. In that case, legitimate users will not be able to access this resource during the time of the attack or even afterwards if the server crashes.
Low	Malicious	Medium	Steeling Privilege	Behavior requires technical expertise and includes intention to do harm through annoyance, harassment, rule breaking, etc. has medium impact level.	Getting an employee's user name and password who has no restricted internet access and using it.
High	Neutral	High	Dangerous tinkering	Behavior requires technical expertise but no clear intention to do harm to the organization’s IT and resources, has high impact level.	Employee configures a wireless gateway that inadvertently allows wireless access to the company’s network by attackers who scan wireless networks and access them for stealing secrets.
High	Neutral	Medium	Accidentally Allowing	Behavior requires technical expertise but no clear intention to do harm to the organization’s IT and resources, has medium impact level.	Employee configures the firewall that inadvertently allows employees use probing services which attackers use for attacking.
Low	Neutral	High	Naive mistakes	Behavior requires minimal technical expertise and no clear intention to do harm to the organization’s information technology and resources and has high impact level.	Choosing a bad password such as ‘‘password.’’ An employee can use his/her colleague's account for accessing private or protected files.
Low	Neutral	Medium	Personal usage	Behavior requires minimal technical expertise and no clear intention to do harm to the organization’s information technology and resources and has medium impact level.	Employee gets root privilege and stores personal large size data on a company server and shares it on the internet.
High	Beneficial	High	Aware assurance	Behavior requires technical expertise together with a strong intention to do good by preserving and protecting the organization’s information technology and resources against high level breaches.	Recognizing the presence of a backdoor program through careful observation of own PC.
High	Beneficial	Medium	Paying attention	Behavior requires technical expertise together with a strong intention to do good by preserving and protecting the organization’s information technology and resources against medium level breaches.	Employee recognizes an abnormal usage or services on a computer or a server and recognize that somebody obtained administrator rights on the attacked computer in order to have full control of it.
Low	Beneficial	High	Basic hygiene	Behavior requires no technical expertise but includes clear intention to preserve and protect the organization’s IT and resources against high level breaches.	A trained and aware employee resists an attempt at social engineering by refusing to reveal her password to a caller claiming to be from computer services.
Low	Beneficial	Medium	Awareness	Behavior requires no technical expertise but includes clear intention to preserve and protect the organization’s IT and resources against medium level breaches.	Reporting a suspicious e-mail which wants to click the link and enter the personal info and also not clicking the link or entering personal info.

TABLE II. 4-D HUMAN THREATS TAXONOMY

Expertise	Intention	Impact Level	Threat Layer	Title	Description	Example
High	Malicious	High	OS	Intentional destruction	Behavior requires technical expertise together with a strong intention to do harm to the organization's IT and resources and has high impact level.	Employee breaks into an employer's protected files in order to steal a trade secret.
High	Malicious	Medium	Network	Man in the middle	Behavior requires technical expertise and includes intention to do harm through annoyance, harassment, rule breaking, etc. and has medium impact level.	Employee stands in the middle of a communication between two hosts. By poisoning the ARP table of one of the two hosts taking part in the communication, the attacker can redirect the traffic to his computer first and then forward it to the intended destination after having read the content of the message.
Low	Malicious	High	Network	Resource exhaustion	Behavior requires minimal technical expertise but nonetheless includes intention to do harm through annoyance, harassment, rule breaking, etc. and has high impact level.	Employee sends large ping packets to a computer or a server, resource exhaustion occurs when the server or the computer receives more queries than it can process. In that case, legitimate users will not be able to access this resource during the time of the attack or even afterwards if the server crashes.
Low	Malicious	Medium	OS	Steeling Privilege	Behavior requires technical expertise and includes intention to do harm through annoyance, harassment, rule breaking, etc. has medium impact level.	Getting an employee's user name and password who has no restricted internet access and using it.
High	Neutral	High	Network	Dangerous tinkering	Behavior requires technical expertise but no clear intention to do harm to the organization's IT and resources, has high impact level.	Employee configures a wireless gateway that inadvertently allows wireless access to the company's network by attackers who scan wireless networks and access them for stealing secrets.
High	Neutral	Medium	Network	Accidentally Allowing	Behavior requires technical expertise but no clear intention to do harm to the organization's IT and resources, has medium impact level.	Employee configures the firewall that inadvertently allows employees use probing services which attackers use for attacking.
Low	Neutral	High	OS	Naive mistakes	Behavior requires minimal technical expertise and no clear intention to do harm to the organization's information technology and resources and has high impact level.	Choosing a bad password such as ''password.'' An employee can use his/her colleague's account for accessing private or protected files.
Low	Neutral	Medium	OS	Personal usage	Behavior requires minimal technical expertise and no clear intention to do harm to the organization's information technology and resources and has medium impact level.	Employee gets root privilege and stores personal large size data on a company server and shares it on the internet.
High	Beneficial	High	OS	Aware assurance	Behavior requires technical expertise together with a strong intention to do good by preserving and protecting the organization's information technology and resources against high level breaches.	Recognizing the presence of a backdoor program through careful observation of own PC.
High	Beneficial	Medium	Network	Paying attention	Behavior requires technical expertise together with a strong intention to do good by preserving and protecting the organization's information technology and resources against medium level breaches.	Employee recognizes an abnormal usage or services on a computer or a server and recognize that somebody obtained administrator rights on the attacked computer in order to have full control of it.
Low	Beneficial	High	OS	Basic hygiene	Behavior requires no technical expertise but includes clear intention to preserve and protect the organization's IT and resources against high level breaches.	A trained and aware employee resists an attempt at social engineering by refusing to reveal her password to a caller claiming to be from computer services.
Low	Beneficial	Medium	Network	Awareness	Behavior requires no technical expertise but includes clear intention to preserve and protect the organization's IT and resources against medium level breaches.	Reporting a suspicious e-mail which wants to click the link and enter the personal info and also not clicking the link or entering personal info.

Proc. of The Third Intl. Conf. on Advances in Computing, Electronics and Communication - ACEC 2015
Copyright © Institute of Research Engineers and Doctors, USA .All rights reserved.
ISBN: 978-1-63248-064-4 doi: 10.15224/ 978-1-63248-064-4-07

TABLE III. 5-D HUMAN THREATS TAXONOMY

Expertise	**Intention**	**Impact Level**	**Threat Layer**	**Attack Type**	**Title**	**Description**	**Example**
High	Malicious	High	OS	User to Root (U2R)	Intentional destruction	Behavior requires technical expertise together with a strong intention to do harm to the organization’s IT and resources and has high impact level.	Employee breaks into an employer’s protected files in order to steal a trade secret.
High	Malicious	Medium	Network	Denial of Service (DoS)	Man in the middle	Behavior requires technical expertise and includes intention to do harm through annoyance, harassment, rule breaking, etc. and has medium impact level.	Employee stands in the middle of a communication between two hosts. By poisoning the ARP table of one of the two hosts taking part in the communication, the attacker can redirect the traffic to his computer first and then forward it to the intended destination after having read the content of the message.
Low	Malicious	High	Network	Denial of Service (DoS)	Resource exhaustion	Behavior requires minimal technical expertise but nonetheless includes intention to do harm through annoyance, harassment, rule breaking, etc. and has high impact level.	Employee sends large ping packets to a computer or a server, resource exhaustion occurs when the server or the computer receives more queries than it can process. In that case, legitimate users will not be able to access this resource during the time of the attack or even afterwards if the server crashes.
Low	Malicious	Medium	OS	Remote to Local (R2L)	Steeling Privilege	Behavior requires technical expertise and includes intention to do harm through annoyance, harassment, rule breaking, etc. has medium impact level.	Getting an employee's user name and password who has no restricted internet access and using it.
High	Neutral	High	Network	Probe	Dangerous tinkering	Behavior requires technical expertise but no clear intention to do harm to the organization’s IT and resources, has high impact level.	Employee configures a wireless gateway that inadvertently allows wireless access to the company’s network by attackers who scan wireless networks and access them for stealing secrets.
High	Neutral	Medium	Network	Probe	Accidentally Allowing	Behavior requires technical expertise but no clear intention to do harm to the organization’s IT and resources, has medium impact level.	Employee configures the firewall that inadvertently allows employees use probing services which attackers use for attacking.
Low	Neutral	High	OS	User to Root (U2R)	Naive mistakes	Behavior requires minimal technical expertise and no clear intention to do harm to the organization’s information technology and resources and has high impact level.	Choosing a bad password such as ‘‘password.’’ An employee can use his/her colleague's account for accessing private or protected files.
Low	Neutral	Medium	OS	User to Root (U2R)	Personal usage	Behavior requires minimal technical expertise and no clear intention to do harm to the organization’s information technology and resources and has medium impact level.	Employee gets root privilege and stores personal large size data on a company server and shares it on the internet.
High	Beneficial	High	OS	Remote to Local (R2L)	Aware assurance	Behavior requires technical expertise together with a strong intention to do good by preserving and protecting the organization’s information technology and resources against high level breaches.	Recognizing the presence of a backdoor program through careful observation of own PC.
High	Beneficial	Medium	Network	User to Root (U2R)	Paying attention	Behavior requires technical expertise together with a strong intention to do good by preserving and protecting the organization’s information technology and resources against medium level breaches.	Employee recognizes an abnormal usage or services on a computer or a server and recognize that somebody obtained administrator rights on the attacked computer in order to have full control of it.
Low	Beneficial	High	OS	Remote to Local (R2L)	Basic hygiene	Behavior requires no technical expertise but includes clear intention to preserve and protect the organization’s IT and resources against high level breaches.	A trained and aware employee resists an attempt at social engineering by refusing to reveal her password to a caller claiming to be from computer services.
Low	Beneficial	Medium	Network	Remote to Local (R2L)	Awareness	Behavior requires no technical expertise but includes clear intention to preserve and protect the organization’s IT and resources against medium level breaches.	Reporting a suspicious e-mail which wants to click the link and enter the personal info and also not clicking the link or entering personal info.