Insider threats, are they real bluster?

Mohannad Alhanahnah
School of Computing, Telecommunications and Networks,
Faculty of Computing, Engineering and the Built Environment,
Birmingham City University
Email: Mohannad.alhanahnah@mail.bcu.ac.uk

Abstract: *Authorized users pose high risk and destructive consequences in comparison with external attacks, because they are trusted, possess knowledge and access. Nevertheless, companies underestimate this risk, and concentrate on the mitigation of external attacks. Recently, companies have begun reviewing their internal security policies and operations, due to the revelation of Snowden's incident. In fact, addressing this intricate problem is a challenging mission, because of the bewildering diversity of this research problem. Therefore, for reducing the complicity and providing an overarching description, this article aims to illustrate the definition of insider threats, and explains different types of insider attacks. It also appraises several of the proposed methods of detection and prediction in the surveyed literature.*

Keywords: insider threats, malicious insider, unintentional insider, detection, prediction

Introduction

Misusing or abusing company assets by individuals, who possess permissions and have knowledge about company internal systems, has significantly increased in recent times (Legg et al., 2013), therefore this issue is considered the second greatest cybersecurity threat (Greitzer et al., 2009). These threats have serious consequences, and some have become more intelligent and sophisticated (Legg et al., 2013). However, the main concern of the vast majority of companies and organizations is to protect themselves from external attacks, and they are largely either overlooking or oversimplifying potential internal threats, thus they do not plant countermeasures that can reduce these threats perpetrated by insiders (Grant, 2009). Consequently, traditional protection solutions for external attacks are unable to detect insider threats.

What are insiders and insider threats?

The term 'insiders' is broad, could cover a spectrum of users, and has no evident definition. But according to several authors (Ophoff et al., 2014; Hunker & Probst, 2011; Costa et al., 2005; Chinchani et al., 2005), insiders are legitimate users, familiar with internal systems and could be aware of organization's security countermeasures. Hamin (2000) and Silowash (2012) also consider employees, contractors, vendors and consultants as insiders. Greitzer (2014) and Colwill (2009) divide insiders into two categories: malicious (intentional) insiders and unintentional insiders. Ophoff *et al*. (2014) add a third category, 'motives', to the previous categories, for describing behaviors that could be considered abnormal, but do not lead to security incidents. Furthermore, Sarkar (2010) extends the definition of insiders to encompass spouses, relatives and clients of employees.

In fact, classifying insiders is a controversial issue, and there is no agreement about it. In addition to the previous categories, Catrantzos (2009) classifies insiders in three types, 1) Hostile or malicious insider 2) Infiltrator and 3) Recruited asset, and Anderson *et al*. (2007) have other classifications for insiders: 1) masqueraders 2) legitimate users and 3) clandestine users. However, all these types fall under the category of malicious insiders, simply because they have the intention to cause harm. Silowash *et al*. (2012) consider malicious insiders to be any current or previous employee, contractor, or partner who has/had an authorized access and intentionally carried out actions harming the confidentiality, integrity or availability of the organization's assets. On the other hand, the same team defines unintentional insiders in the same as with malicious insiders, except they do not have malicious intent to harm the organization, and do not understand that their accidental actions could have a negative impact on the organization's systems (CERT Insider Threat Team 2013).

Similarly, there are several perceptions for the definition of 'insider threats'. Obviously, there should be a direct relationship between the definition of insider threats and insiders, therefore, simply insider threats could be considered as harmful acts committed by insiders, regardless of their intentions. In general, the definition of insider threats revolves around misusing, abusing or violating security policies by legitimate users, who have or had authorized access (Ophoff et al., 2014; Silowash et al., 2012). However, there is much debate whether to consider unintentional acts under the umbrella of insider threats (Reidy, 2013; Schultz, 2002), especially actions performed in response to external attacks (social engineering, phishing or spear phishing) (Greitzer et al., 2014), because the ultimate beneficiary is the external hacker rather than the insider. Also, according to (Juels & Yen, 2012), social engineering is techniques utilized by Advanced Persistent Threat (APT) actors to steal users' credentials without their knowledge, in order to accomplish their external attack.

According to Hunker & Probst (2011) and Bellovin (2008), types of insider attacks are:

Misuse of access: the most difficult to detect and prevent, because the insider already maintains authorized access.

Bypassing defenses: insider by default is in an advantage position to bypass security protection mechanisms (firewall and IPS/IDS) that are planted by the company, so technical factors alone are insufficient to protect from insiders.

Access-control failure: flaws in the access-control mechanisms resulting from misconfiguration of the system or bugs in the access-control system. Thus, as with misuse, it is difficult to detect abnormal behaviors.

Silowash *et al*. (2012) analyzed 371 insider incidents, thence classified malicious insider activity to the following categories:

IT sabotage (Bishop et al., 2014): insider aims to harm an organization or an individual by utilizing IT resources.

Theft of Intellectual Property (IP): called data exfiltration in (Bishop et al., 2014), where the insider steals IP documents, and sensitive information.

Fraud: unauthorized modification, addition or deletion performed by the insider, where the financial gain is the motivation for committing this attack, thus financial institutions are the main sector which suffers from this issue.

Miscellaneous: an insider's activity does not fall under any of the previous classes.

In addition to that, there are insider attacks cases could fall under more than one class, as illustrated in figure 1, which shows the total number of the analyzed cases, excluding the 22 miscellaneous cases. Five incidents are shared between fraud and IT sabotage; also there is an overlapping in seven cases between fraud and IP theft.

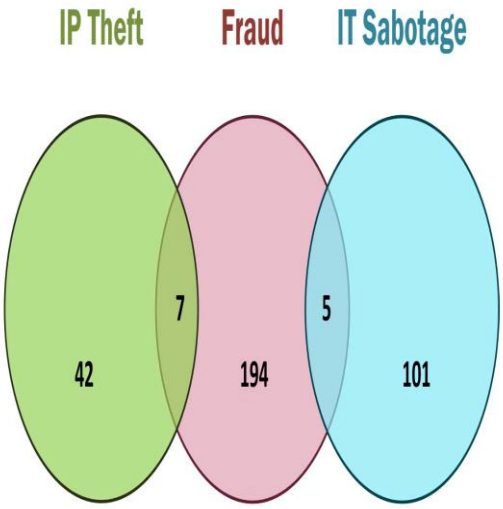

Figure 1 Classes of insider activities and number of incidents in each category (Silowash et al., 2012)

Consequences of insider threats

Although the phenomenon of insider threats is not a new issue (Legg et al., 2013), and has been discussed for more than a decade; and figure 2 depicts the yearly distribution of publications in this area. But the proposed solutions for mitigating insider threats are still emerging, as will be discussed below. A recent case (BBC, 2013) brought the attention of organizations and governments to the necessity of developing security controls, which can alleviate or prevent the damage of internal incidents. This was the leak of numerous classified US government documents were been by Edward Snowden, a US NSA contractor. However, it is arguable whether Snowden should be considered as a whistle-blower or a traitor. Whatever his motivation, he leaked crucial information without permission.

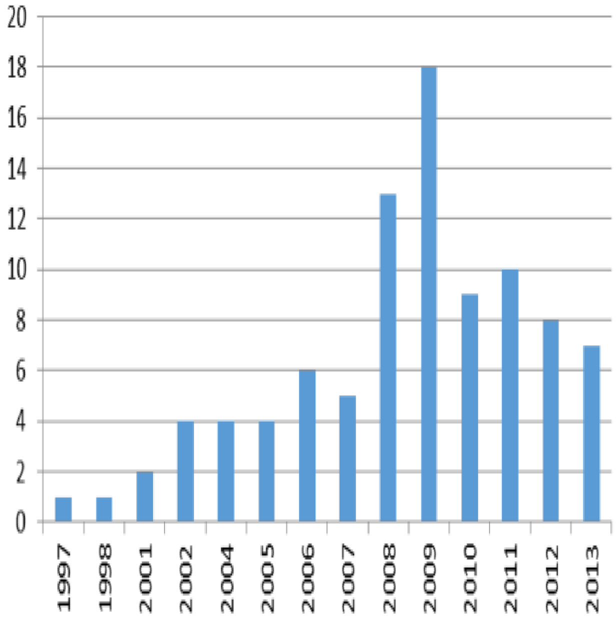

Figure 2 Distribution of articles from top ranked journals by year (Ophoff et al., 2014)

Insider threats are less prevalent compared to external attacks, but their potential results could be more harmful. Various cases show clearly the severity of insider threat towards the national security of the US, with the example of Edward Snowden, and Robert Hanssen, a US FBI agent, who had stolen confidential information and sold it to Russian agencies (BBC 2013; FBI 2001). Despite that, the majority of Chief Security Officers (CSOs) focus only on employing technologies to protect from external threats, and do not implement necessary countermeasures against insiders (Grant, 2009). This fact can be clearly deduced through the scarcity in the policies, procedures and mitigation solutions that control employees' bad behavior. The following statistics about UK companies demonstrate that negligence: "84% do not scan outgoing email for confidential data, 52% do not carry out any formal security risk assessment, 78% of companies had computers with unencrypted hard discs stolen and 67% do nothing to prevent confidential data leaving on USB sticks" (BERR, 2008). Therefore, numerous companies are prone to insider threats, because of the growth of contracts with third-parties, and the rapid expansion of outsourcing.

The consequences of insider threats are unlimited, and could be tangible or intangible, but they could be generalized (Ophoff et al., 2014) to financial loss and damage of reputation:

Financial loss: Cappelli et al. (2004) describe 15 financial loss cases between 1996 and 2002 in the financial sector. They also mention that the financial gain is the most prevalent motive throughout the 26 incidents examined, and show that preforming internal fraud activities does not require high technical skills.

Damage of reputation: there are other impacts, such as business disruption and customer loss, but they could fall under category of financial loss. However, undoubtedly any publicly disclosed insider threat incident could indirectly lead to damage of reputation, thus loss of reputation would be considered the ultimate result of any insider attack if publicly disclosed.

In addition to the lower prevalence, Cole & NetIQ (2006) give other reasons behind ignoring insider threats: 1) they are easy to be denied, 2) protecting public reputability, 3) and lack of evidence of the occurrence of internal incidents. Because of the fear of gaining a bad reputation, organizations do not announce any information about insider incidents. Indeed, lack of real cases and disclosed incidents are significant issues from which researchers suffer, and this is an obstacle against enhancing threat assessment efforts.

Of the respondents to the 2014 US State of Cybercrime Survey, 32% stated that the impact of insider crimes is more costly and damaging than external attacks (PwC, 2014). This report also mentions that not only the current employees are the source of insider threats, thus companies should monitor all internal privileged users such as former employees, contractors, customers and business partners. This is because the percentage of the insider incidents committed by current contractors and former contractors in 2014 increased to 18% and 15%, respectively, from 16% and 13% in 2013.

Mitigation solutions and frameworks

Overview

At this point, the diversity of insiders and consequences have been discussed, and the differences between malicious activities has been described, whereas accomplishing some threats need high technical skills, i.e. fraud, but performing other attacks does not require technical knowledge i.e. sabotage. Also, some research addresses only UIT (CERT Insider Threat Team, 2013), where others focus on malicious insider threats (Legg et al., 2013; Eberle & Holder, 2009), and another group of research focuses on figuring out one of insider activities, as mitigation solution from internal frauds (Cappelli et al., 2004), sabotage or data exfiltration (Hexis Cyber Solutions, 2014). Therefore, there are many mitigation solutions; ranging from general best practices and guidelines, such as separation of duties, security audit and awareness training, to pure mitigation frameworks.

Moreover, some research considers only psychological traits for developing mitigation solutions (Laskey et al., 2004; Axelrad et al., 2013), while others take into account technical factors (Spitzner, 2003), and some combine both techniques (Nkosi et al., 2013). In general, mitigation solutions from insider threats could be divided into two categories: detection models (Parveen et al., 2011; Buford et al., 2008) and proactive or prediction models (Kandias et al., 2010; Schultz, 2002; Axelrad et al., 2013). These categories are discussed in the two sections that follow.

Detection solutions

(Eberle & Holder, 2009) introduced a detection model by utilizing Graph-Based Anomaly Detection (GBAD) approaches. The GBAD system has the ability to uncover modifications, insertions, and deletions. They used Minimum Description Length (MDL) and inexact matching algorithm to uncover modifications. The insertion algorithm (GBAD-Probability) uses probability and MDL. Finally, Maximum Partial Substructure (MPS) and MDL have been utilized for anomalous graph deletions. In order to prove the solution, the authors built an simple email dataset, simulated insiders' behaviour, and the algorithm successfully discovered several anomalies in the email traffic. On the other hand, this model does not consider or make any correlation with other aspects. The process of defining normal behaviour is not clearified, is it only based on user's behaviour or the business model of the company.

Other proposed models are similar to (Eberle & Holder, 2009), they employed one or several machine learning techniques to detect insiders. For instance (Parveen et al., 2011) used unsupervised machine learning techniques, and do not recommend utilizing supervised machine learning algorithms, because they are time-consuming, expensive and require large amounts of well-balanced training data to be effective.

Also, (Nkosi et al., 2013) introduced a model for detecting malicious insiders in Software as a Service (SaaS) cloud environments. This model utilizes data mining techniques. Indeed, it uses the PrefixSpan algorithm for generating a normal pattern (profile) for each employee, and then it can detect any deviation from the norm. Interestingly, the initial phases of the model cover non-technical aspects. The non-technical criteria are performed in cooperation with the HR department, it encompasses firstly, pre-employment background checking, which could include checking credit reports, criminal records, school and medical reports, and secondly, preparing policies and procedures specify access and usage of company resources. Furthermore, several tests have been executed to evaluate the model sensitivity and its precision, and discover possible ways to decrease the false positive/false negative rates.

Predictive solutions

(Legg et al., 2013) introduced a reasoning model which can assist analysts to discover potential insiders. This model relies on technology, sociology and psychology factors for drawing hypotheses regarding potential insider threats, by creating a profile for every user, monitoring his or her behavior and correlating this behavior with logs from other sources, such as technology and physical i.e. CCTV. Since the proposed model relies on several factors, correlates between them, and keeps users' profiles updated, this would improve the accuracy of the hypotheses (predicting whether the behavior is abnormal). However, the technologies that will be used to implement the solution have not been clarified, and this model has not been evaluated, hence its efficiency and accuracy are questionable.

Another prediction model is proposed by (Kandias et al., 2010). It uses technical factors i.e. real-time monitoring in conjunction with psychological factors; therefore, two profiles are created for each employee: IT usage profile and psychological profile. However, there is blurring in the scoring system of the decision engine, which could not yield precise predictions, for instance a user sophistication formula has not been built on well-established information about a user's usage and skills, especially the calculation of the resources consumption in the user's machine, which is based on RAM, CPU and running applications. This model can be defeated easily by performing the attack gradually, rather than a one shot attack. Furthermore, as with the previous prediction model, this model has neither been implemented nor evaluated, and these tasks are mentioned as a future work.

Conclusion

As insider threats are a broad issue, therefore mitigation solutions also vary. Indeed, organizations should seriously seek more tailored strategy and mitigation approaches for protecting their business. This requires substantial efforts for investigating the challenging research topic, because there is no single agreed definition and categorization of insider threats. In addition, indications of insiders are unlimited, and there is no conclusive agreement among them, for example many frameworks consider disgruntled employees as a useful indication for detecting potential abnormal activities, but they have not specified how to measure this metric accurately. Although the majority of the research emphasizes the importance of collecting logs and make a correlation among them, when it comes to specify log sources, there is a noticeable absence of specifying types of logs that should be collected, either network, operating system or access logs, and their criticality.

Thus, the literature survey shows many gaps. Nevertheless, all the proposed models that have been evaluated suffer from lack of accuracy (false positive/false negative rates); this pitfall comes from not clearly specifying taxonomies of insider threats, and describing the employed approaches and techniques for carrying out the abnormal activities, and the shortcoming appointing the appropriate observables which could lead towards drawing accurate decisions.

References

Anderson, G.F., Selby, D.A. & Ramsey, M., 2007. Insider attack and real-time data mining of user behavior. *IBM Journal of Research and Development*, 51(3.4), pp.465–475.

Axelrad, E.T., Sticha, P.J. & Brdiczka, O., 2013. A Bayesian Network Model for Predicting Insider Threats. In *2013 IEEE Security and Privacy Workshops*. IEEE, pp. 82–89.

BBC, 2013. BBC News - Profile: Edward Snowden. Available at: http://www.bbc.co.uk/news/world-us-canada-22837100 [Accessed November 15, 2014].

Bellovin, S.M., 2008. The Insider Attack Problem Nature and Scope. In S. J. Stolfo et al., eds. *In Insider Attack and Cyber Security*. Advances in Information Security. Boston, MA: Springer US, pp. 1–4.

BERR, 2008. *Information Security Breaches Survey 2008*, Available at: http://www.eurim.org.uk/activities/ig/voi/DBERR.pdf [Accessed December 20, 2014].

Bishop, M., Conboy, H.M., Huong Phan, Simidchieva, B.I., Avrunin, G.S., Clarke, L.A., Osterweil, L.J. & Peisert, S., 2014. Insider Threat Identification by Process Analysis. In *2014 IEEE Security and Privacy Workshops*. San Jose, CA: IEEE, pp. 251–264.

Buford, J.F., Jakobson, G. & Corp, A., 2008. Insider Threat Detection Using Situation-Aware MAS. In *2008 11th International Conference on Information Fusion*. Cologne: IEEE, pp. 1 – 8.

Cappelli, D., Moore, A.P., Randazzo, M.R., Keeney, M. & Kowalski, E., 2004. *Insider Threat Study : Illicit Cyber Activity in the Banking and Finance Sector*, Available at: http://resources.sei.cmu.edu/asset_files/SpecialReport/2004_003_001_50299.pdf.

Catrantzos, N., 2009. *No Dark Corners: Defending Against Insider Threats to Critical Infrastructure*. Monterey, CA, USA: Naval Postgraduate School.

CERT Insider Threat Team, 2013. *Unintentional Insider Threats : A Foundational Study*, Available at: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=58744 [Accessed December 20, 2014].

Chinchani, R., Iyer, A., Ngo, Hu.Q. & Upadhyaya, S., 2005. Towards a Theory of Insider Threat Assessment. In *2005 International Conference on Dependable Systems and Networks (DSN’05)*. Washington, DC, USA: IEEE, pp. 108–117.

Cole, E. & NetIQ, 2006. *Addressing the Insider Threat with NetIQ Operational Change Control Solutions*, Available at: http://www.bitpipe.com/detail/RES/1155054635_181.html [Accessed January 25, 2015].

Colwill, C., 2009. Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report*, 14(4), pp.186–196.

Costa, P.C.G., Laskey, K.B., Revankar, M., Mirza, S., Alghamdi, G., Barbará, D., Shackelford, T. & Wright, E.J., 2005. DTB Project : A Behavioral Model for Detecting Insider Threats. In *International Conference on*

Intelligence Analysis. McLean, VA: MITRE Corporation.

Eberle, W. & Holder, L., 2009. Insider Threat Detection Using Graph-Based Approaches. In *2009 Cybersecurity Applications & Technology Conference for Homeland Security*. New York, NY, USA: IEEE, pp. 237–241.

Grant, I., 2009. Insiders cause most IT security breaches, study reveals. Available at: http://www.computerweekly.com/news/1280090551/Insiders-cause-most-IT-security-breaches-study-reveals [Accessed November 17, 2014].

Greitzer, F.L., Paulson, P.R., Kangas, L.J., Franklin, L.R., Edgar, T.W. & Frincke, D.A., 2009. *Predictive Modeling for Insider Threat Mitigation*, Available at: https://www.pnl.gov/cogInformatics/media/pdf/TR-PACMAN-65204.pdf [Accessed March 2, 2015].

Greitzer, F.L., Strozer, J.R., Cohen, S., Moore, A.P., Mundie, D. & Cowley, J., 2014. Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. In *2014 IEEE Security and Privacy Workshops*. San Jose, CA: IEEE, pp. 236–250.

Hamin, Z., 2000. Insider Cyber-threats: Problems and Perspectives. *International Review of Law, Computers & Technology*, 14(1), pp.105–113.

Hexis Cyber Solutions, 2014. *Using HawkEye AP 6 . 0 for Detecting Insider Threats*, Available at: http://i.crn.com/custom/Hexis_HawkEye_AP_InsiderThreat_WP.pdf [Accessed December 11, 2015].

Hunker, J. & Probst, C.W., 2011. Insiders and insider threats An overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, 2(1), pp.4–27.

Juels, A. & Yen, T.-F., 2012. Sherlock Holmes and The Case of the Advanced Persistent Threat. In *5th USENIX conference on Large-Scale Exploits and Emergent Threats (LEET'12)*. Berkeley, CA, USA: USENIX Association.

Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M. & Gritzalis, D., 2010. An Insider Threat Prediction Model. In *Trust, Privacy and Security in Digital Business*. Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 26–37.

Laskey, K., Alghamdi, G., Wang, X., Barbará, D., Shackelford, T., Wright, E. & Fitzgerald, J., 2004. Detecting Threatening Behavior Using Bayesian Networks. In *Proceedings of the Conference on Behavioral Representation in Modeling and Simulation*.

Legg, P., Moffat, N., Nurse, J., Happa, J., Agrafiotis, I., Goldsmith, M. & Creese, S., 2013. Towards a conceptual model and reasoning structure for insider threat detection. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 4(4), pp.20–37.

Nkosi, L., Tarwireyi, P. & Adigun, M.O., 2013. Insider threat detection model for the cloud. In *2013 Information Security for South Africa*. Johannesburg: IEEE, pp. 1–8.

Ophoff, J., Jensen, A., Sanderson-Smith, J., Porter, M. & Johnston, K., 2014. A Descriptive Literature Review and Classification of Insider Threat Research. In *Proceedings of Informing Science & IT Education Conference (InSITE)*. pp. 211–223.

Parveen, P., Evans, J., Thuraisingham, B., Hamlen, K.W. & Khan, L., 2011. Insider Threat Detection Using Stream Mining and Graph Mining. In *2011 IEEE Third Int'l Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third Int'l Conference on Social Computing*. Boston, MA: IEEE, pp. 1102–1110.

PwC, 2014. *Managing cyber risks in an interconnected world*, Available at: http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml [Accessed November 16, 2014].

Reidy, P., 2013. Combating the Insider Threat at the FBI: Real World Lessons Learned. *Black Hat USA 2013*. Available at: https://media.blackhat.com/us-13/US-13-Reidy-Combating-the-Insider-Threat-At-The-FBI-Slides.pdf [Accessed November 17, 2014].

Roy Sarkar, K., 2010. Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report*, 15(3), pp.112–133.

Schultz, E.E., 2002. A framework for understanding and predicting insider attacks. *Computers and Security*, 21(6), pp.526–531.

Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T. & Flynn, L., 2012. *Common Sense Guide to Mitigating Insider Threats*, Software Engineering Institute. Available at: http://www.sei.cmu.edu/reports/12tr012.pdf [Accessed October 20, 2014].

Spitzner, L., 2003. Honeypots: catching the insider threat. In *19th Annual Computer Security Applications Conference, 2003. Proceedings.* Washington, DC, USA: IEEE, pp. 170–179.