# Privileged Account Management Approach for Preventing Insider Attacks

**Erhan Sindiren [1*] and Bünyamin Ciylan [2]**

[1*]Gazi University, Institute of Informatics, Department of Computer Forensics, Ankara 06680, Turkey
[2]Gazi University, Faculty of Technology, Computer Engineering, Ankara 06560, Turkey

**Summary**
The companies gradually increase their safety precautions towards protecting their information systems, but the attackers simultaneously explore many different methods for breaching or bypassing the safety precautions. In this cycle, the attacks to information systems are expected from outside, and the cyber security investments are made in this parallel. As a result of this, the companies are caught unprepared for these conscious or unconscious breaches. In order to achieve their goals in insider attacks, the attackers attempt to seize the privileged accounts, which have much more authorizations on the information systems than the normal accounts. The reason for targeting the privileged account is that these accounts have wide authorizations on the information systems. IT personnel are responsible for realizing and managing the cyber security precautions within the company. In general, the IT personnel do the same mistake by adopting the general approach; they expect the attacks from outsiders and ignore the insider threats. The most important one among these threats is the seizure of privileged accounts, which is used by the IT personnel every day, by the attackers. The measures to be taken for preventing the malicious use of privileged accounts and the approach to be adopted in order to increase awareness of IT personnel are discussed in this paper.

***Key words:***
*insider attacks, privileged account management, password security, risk management, digital identity management, access control*

## 1. Introduction

The information technologies play gradually more important role in lives of people, and it becomes irreplaceable for the humanity. The companies offering service in medicine, energy, finance, telecommunication, and similar industries use information technologies in order to increase the service standards. Thus, the companies closely follow the technological developments in order to offer the best service and to be able to compete against the other companies, as well as they might be the driving force of technological developments. Every new development in information technologies also brings new security problems together with it. The security problems that might occur in information technologies, which have a critical importance in lives of today's societies, might have destructive effects. In parallel with the traditional approach, the companies expect these security problems from the outside and they take their measures in this regard. But, the previous studies indicated that the threats do not only come from the outside but they might also come from inside the company [1-5]. In case of an insider attack, the security precautions that are capable of ensuring safety against the outsider attacks are less effective since the attackers have more information about the company than any outsider may have. Thus, because the attacker has more information about the system, the insider attacks are always more important [6, 7].

One of the methods to be used against the insider attacks that might occur in information systems of companies is to detect the misuse of privileged accounts of employees that have been authorized in parallel with their duties [8, 9]. Within this aspect, in order to better understand the importance of privileged accounts in preventing the insider attacks, it is important to define the insider attacks accurately. This definition should not be specific to the company but be specific to general and be inclusive, and then it can be easier to understand this problem.

Chinchan et al. defined the insider threat as the legal users maliciously using their systemic privileges in order to compromise or damage the valuable information [10]. Cappelli et al. defined the insider attack as the conscious and malicious abuse of authorizations by any partner, current or former employee, who have access to the information system or data of an company, in order to negatively affect the integrity, accessibility / availability, and/or confidentiality [11]. Greitzer et al. defined the insider attack as an individual's malicious use of an access authorization to an company's information systems, data or network for once or multiple times [12]. There are many similar definitions. But, the definition made by Bishop et al. is much more comprehensive. According to Bishop et al., the insider attacks are divided into two behaviors. The first one is the leakage of confidential information to the outside, and providing the unauthorized access to a resource or preventing the authorized access. At this point, the use of access authorization by an individual, who is

Manuscript received January 5, 2018
Manuscript revised January 20, 2018

authorized to access the data or resources, in order to provide information to third party/parties or to prevent the access of third party/parties having access authorization is explained. The second one is the use of legal access rights in order to perform an action that is against the company's security policy. In the second case, the access authorization is used in order to expand the privileges in the way breeching the security principles set for insider access [13]. The privileged accounts are the accounts that have the authorization of modifying/deleting/adding in directory service in order to maintain the management of IT infrastructure and components and are member to the group named "privileged accounts". These accounts, which are used by IT personnel and have certain privileges, have various authorizations, and they are one of the first values to be protected in IT infrastructure [14-16].

In surveys examining the cyber-attacks and breaches that the companies have been faced in recent years [17-19], it can be clearly seen that the insider threats significantly increased. In some of the studies [20-25], it was concluded that the malicious use of privileged accounts in insider attacks poses high level of risk and they would increase in further periods [26, 27].

In studies examining the reasons for insider attacks, it can be understood how dangerous the abuse of privileged accounts can be. For this reason, the privileged accounts should be monitored and audited, and they should not be left uncontrolled. The privileged accounts within the information systems are generally used by IT personnel. For this reason, the IT personnel should be trained continuously with programs consisting of theoretical and practical components and increasing the cyber-security awareness of IT personnel.

From this section, input the body of your manuscript according to the constitution that you had. For detailed information for authors, please refer to [1].

## 2. Related Works

The control and management of privileged accounts, which are one of the most important reasons for insider attacks in companies, is one of the most important IT problems to be taken into consideration. Regarding the solutions of this problem, many precautions and procedures have been suggested by the researchers. Although the objectives of these solutions offered by researchers are the same, they include different approaches.

In their studies, Sarkar [28] and Padayachee [29] argue that it is necessary to provide the authorized personnel with minimum privileges regarding the access to information systems. In other words, these authors support that the assigned users should have only the authorization required for the task, in addition to the classification of tasks. Moreover, they also emphasize that the passwords to be used for privileged accounts should be created in accordance with certain standards. Baracaldo and Joshi have prepared technical templates representing the malicious use of privileges. By using the algorithm, which they have developed, bases on the authorization, roles, and policies, they have addressed the insider attacks by using these templates [30]. Regarding the access to an company's database, Chagarlamudi et al. have developed a model, in which the functions classified based on the tasks are fulfilled by authorized users via a graphical interface based on Petri net [31]. Colwill has suggested an approach, according to which the privileged account users authorized for access to valuable IT assets and data of a company are controlled, provided with only the necessary authorizations and continuously monitored. Moreover, he has emphasized the human factor (training and awareness) rather than the technological solutions [32]. Agrafiotis et al. have carried out a study on 120 insider attack cases and prepared a template for detecting the attacks. The attack template is based on analyzing the behaviors of privileged users, who have role-based profiles, and the abnormalities in their behaviors [33]. Bishop et al. have suggested the Attribute-Based Group Access Control (ABGAC) model that is based on dividing the IT resources into groups and defining the authorized user groups separately for each group of resources [34]. Wang et al. have developed a method that might be useful in estimation of potential insider attacks network- and host-based sensors before it occurs. This method includes the analysis of IT asset's security vulnerabilities and an identity validation process for the authorized privileged users [35]. Regarding the prevention of insider attacks, Nance et al. have suggested a model that is based on the graphical analysis of the interactions between the tasks, which have been divided into groups, in information systems and the users, who have been authorized for these tasks [36].

Given the studies on preventing or detecting the abuse of information systems during insider attacks by authorized users having privileged accounts, it can be seen that they are generally based on the technology. The number of studies including human-oriented approaches such as training the employees and increasing the awareness is limited. But, it is believed that it would be more effective to synchronously perform technology- and human-oriented approaches in struggling with and preventing the violations through privileged accounts in insider attacks.

## 3. The Approaches to the Insider Attacks Based on the Abuse of Privileged Accounts Results

The companies use many IT security systems in order to prevent the conscious and unconscious actions that might threaten the information systems from inside or outside. As a natural result of this, the companies increase their security precautions in parallel with the developing technology in order to protect their information systems and data, so they have to allocate gradually increasing budgets for this purpose [37]. In security of IT facing with different attack methods, different security vulnerabilities, and different actions on daily basis, the efforts are made in order to improve the actual precautions and measures, but the traditional IT security measures that should be taken in order to prevent the attacks are forgotten or neglected. As a result of this, the companies aiming to protect their information systems from the new possible attack type that might arise every day are observed to implement temporary solutions in order to save the day or they might prefer only the technology-based solutions [38, 39].

Considering the traditional IT security, the point coming to mind at first and considered as a vital security measure is the password security, because the first target of attackers in order to achieve their final objective is the passwords used in the system. In addition to the normal user accounts, there also are administrator accounts that belong to IT personnel and have privileged authorizations within the system. These accounts are generally used for the purposes such as maintenance, management and repair of information systems. The seizure of password of one of these accounts by the attackers might cause the seizure of entire system. These privileged accounts, which are the administrator accounts having privileged authorizations and used for administering the information system, are referred as Key to the Kingdom in some of the studies [40, 41].

The IT personnel having privileged accounts have the access authorization to databases, file servers, e-mail servers, and similar components of information system. For instance, an IT employer that have been assigned to a task on database might have access to all the components such as file servers, application servers, user information, e-mail servers, directory services, and etc. At first glance, this authorization might be seen normal since the ones having this privilege are IT personnel. But, it refers to the obvious infringement of confidentiality and integrity component of IT security (integrity, accessibility, and confidentiality). The confidentiality is defined as “keeping the sensitive information in secure and limiting them to the individuals and corporations considered appropriate” [42]. In other words, the confidentiality component refers to ensuring that the information can be accessed only by the allowed individuals and systems, as well as preventing the unauthorized access. The integrity is “to stay in a reliable, non-deteriorated or perfect condition” [42]. In other words, it is to ensure the information security in the way preventing the information from the modification or access by unauthorized individuals or systems. For this reason, the access of IT personnel having privileged accounts to the information systems other than they are responsible for should be prevented [43]. Controlling and managing the privileged accounts is not an additional security measure for the companies but is a necessity that should be prioritized. Using a strong password and renewing in short periods, the privileged accounts to the personnel assigned based on previously the defined tasks, and monitoring these processes would be useful in protecting the company from most of insider attacks [44-48].

## 4. Privileged Account Management Process

Protection from privileged account abuses of insiders or the other insider attack types requires specific solutions. But, given the cyber security solutions of companies, it can be seen that the majority of them focus on the outsider attacks [49]. The security solutions to be used for insider and outsider threats should not be considered separately but they should be integrated [50]. In order to prevent the insider threats, not only the technological solutions but also the human factor should be taken into consideration. It should never be forgotten that the chain is no stronger than its weakest link. The employees should be provided with cyber-security training on regular basis and the awareness should be increased. The achievements obtained from these trainings should be tested via social engineering tests. The current information security policies should be actively implemented in the company, and they should not be left on the paper [51].

The accurate implementation of the components of privileged account management process (Fig. 1) will increase the robustness of company against the insider threats. This process will minimize the level of threat but not eliminate it completely. But, it will enable the company to detect the ones responsible for the breaches.

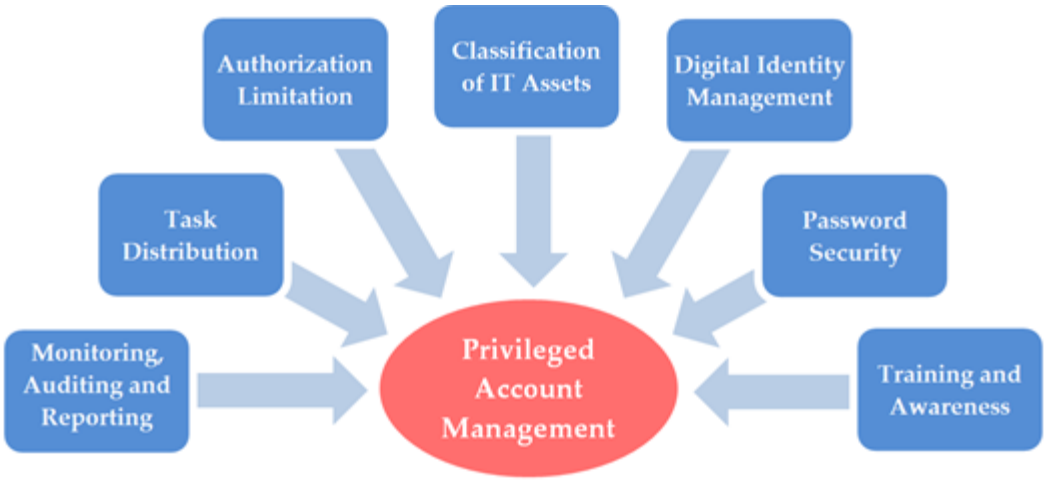


Fig. 1 The components of privileged account management process

### 4.1 Task Distribution and Authorization Limitation

A single IT employee cannot be responsible for all the components of IT infrastructure of a company, which have a large IT infrastructure. For this reason, the appropriate task distribution should be ensured for IT personnel in companies. But, the privileged accounts of IT personnel also should be included in this task distribution. Otherwise, an IT employee that is responsible for web servers may access to file servers, FTP servers, database servers, log servers, and most importantly to directory service servers by using the privileged account. He/she can modify these systems in an unauthorized manner and without being assigned by the management. For this reason, the accurate task distribution should be made not only for the ordinary staff but also for IT personnel [38, 52-55].

In cases that the assignments pass beyond the limit that a user can handle, the methods that might cause the problems in IT security (all of the passwords might be same or easy-to-find, the passwords might be noted on somewhere that can be easily found, and etc.) are more likely to be used. The identity management process is implemented in order to prevent such security problems or leave and change of job for various reasons to reorganize the access rights in issues [56].

The use of privileged accounts by IT personnel without any limitation might cause IT security problems within the company. For this reason, the access of IT personnel to the information systems other than those they are responsible for should be prevented [43]. The access rights in the information systems should be organized based on the assignments, and the IT personnel should be subjected to identity validation based on their tasks.

### 4.2 Classification of IT Assets

In order to organize the access rights of privileged account users upon the task distribution, the IT assets should be classified into certain groups. The illegal access to IT assets, which are under responsibility of other departments, by the other users with legal authorizations might cause hard-to-detect security breaches within the company. For this reason, the IT assets should be grouped based on the task distribution [34]. But, the classification of IT assets should not be left on the paper. The classification should be maintained technically by using hardware and/or software security solutions via access control lists (based on port, IP, and user). The privileged access rights should be assigned based on according to task distribution and IT assets classification.

### 4.3 Digital Identity Management

In last decade, the companies having large IT infrastructure pay significant importance to identity management in order to reduce the work load of IT personnel, decrease the digital identity management costs, prevent the risks that might threaten the security, and include the identity management process into workflows [56].

The identity management process is performed in order to ensure the access of users having digital identity to the allowed sources within their authorization limitations, prevent the access to resources that they are out of their authorization limitations, control the authorized and unauthorized access, and most importantly determine and classify the authorizations of users [57, 58]. These operations are an important part of IT security. While

putting the identity management process into practice, the following points should be taken into consideration;

- The procedure of adding and deleting the digital identities from Identity Management Process should be determined,
- Each of the digital identities should be unique in order to detect the person(s) that is(are) responsible for the consequences of negative scenarios,
- An approval mechanism process should be implemented for each staff before granting required rights and authorizations to access IT infrastructure
- The access rights given to personnel should be in compliance with general and enterprise security policies, as well as the principle of "task distribution",
- The personnel, who have been authorized for access to IT infrastructure, should be given written/verbal (preferably in written format) information about the access rights, which they have, and the security limitations,
- Regardless of the reason, the digital identity information of employer, the position of whom has been changed or who has been discharged from the company, should be updated and his/her authorizations should be synchronized.

## 4.4 Password Security

The password is the series of characters that the user utilizes in login in a computer, and accessing to files, programs, and other resources. The passwords are used for ensuring that the users do not access to a computer unless they are authorized [59, 60]. By its nature, the password is the personal information. This means that users having this information are authorized to access the password-protected values. In other words, the password to be used in accessing the valuable assets is used in the way determined by the user, unless a measure is taken contrariwise. In this case, we protect our assets as much as the sensitivity shown by the person we trust to deliver our valuable assets. But, as in any domain involving human factor, this also is open for the errors [61]. The passwords constitute the final protection line in protecting the information stored in a computer or an information system and to prevent the unauthorized access to the resources. In some cases, despite all the measures taken, they are the real protection instrument [62].

A strong password can be defined as the series of characters that are not easy-to-estimate or cannot be seized by trial and error easily [63]. The first step of creating a strong and robust password is to increase the length of password, i.e. the number of characters in this series. It can be stated that the passwords that are created in parallel with this approach are stronger when compared to those consisting of fewer characters. Increasing number of characters is one of the most important factors increasing the entropy value, and it is considered as one of the methods used in order to create a strong password [64]. But, higher number of characters used in a password is not the single standard in creating a strong password. The more the numbers, lowercases, uppercases, and special characters are used in password and the higher the character diversity is, the further the entropy value increases [65].

Besides the mistakes made while creating the password, also the mistakes are made in using the passwords. The users generally make a habit of this sort of mistakes [65]. When one of a password of a social network account, an online banking account, a cloud storage account, or a business user account etc. is seized, the user's other accounts become under the risk. Because, the password creation behavior of user is learnt by the attackers. For this reason, in operating systems, social networks, and online banking applications, some further precautions (password length, character diversity, prevention of the use of name and date of birth, forcing user to change the password on a regular basis, character diversity, prevention of the use of name or date of birth, forcing the user to change the password on a regular basis, prevention of the use of previous passwords, and etc.) are taken in order to strengthen the password [66]. But, even these measures might not motivate users to correct their passwords, and these users continue to repeat the errors, some of which are presented in Table 1 [61, 67].

Table 1: Samples of password usage errors

| ***Type of action*** |
|---|
| Use of passwords used at special life (online banking passwords, social network passwords, and etc.) in business |
| Use of habits that can be easily found via social networks such as date of birth, names of family members, hobbies, and sport teams in passwords |
| Constituting a new password by changing only single letter, number or character of older password |
| The use of default passwords in computer without changing them |
| Keeping the documents, which include the password information, in computer |
| Keeping the documents, which include the password information, nearby computer |
| Sharing the passwords with colleagues |
| Using the same password in different accounts by interchanging |

A strong password should be created in the way including no meaning, consisting of random characters, and having enough length. The following criteria are the basic criteria regarding a strong password [65, 68]:

- Since it is easier to seize the passwords consisting of fewer characters when compared to those consisting of

higher number of characters, the passwords should be longer,
- The password should include uppercase, lowercase, number, and special characters. The consequent or repetitive combinations (such as "12345678," "55555555," or "abcdefg" and etc.) or the letters located adjacent to each other in keyboard should not be used,
- It should be easily remembered by the user but hard-to-estimate by the others.
- It should not include the names and/or date of birth of relatives,
- It should not be a word that has a meaning (even in a foreign language) such as password or is written in different order (reverse) such as drowssap or contraseña,
- It should be easily remembered. A strong password should not be created in the way decreasing the remember ability or the password should not be remembered by looking at a note every time. The easy-to-remember passwords with mnemonic statements should be preferred,
- It should not be shared by any member of company, regardless of their position within the company,
- It should be changed regularly. The period of changing should be shortened depending on the importance of subject protected by the password,
- It should not be used in public or unknown computer,
- It should not be sent via e-mail.

The password attacks are the attempts to illegally seizure the passwords of accounts, which are used on information systems, by the attackers [69]. It might vary depending on the methods, instruments and target system structure [70]. The passwords that have been seized by the attackers are used by the attackers in order to damage the system or achieve the valuable data by seizing the information system. In order for the attackers to achieve their goals, the seized accounts must have the required authorizations on the target system. In cases, in which the password of an unauthorized account has been seized, the attackers attempt to achieve their goals by using method called privilege escalation [71, 72].

### 4.5 Training and Awareness

The main objectives of information security training and awareness are to decrease the risk of misuse of technology and human errors that might arise from the lack of knowledge, and to inform the individuals about the information security threats and problems. In order to protect the fundamental characteristics of information security, it is not enough to take only technological measures. An ideal security approach should involve technological solutions and human factor together. The idea that the problems regarding the information security can be solved only by using technological methods causes the human factor to be neglected. The information security breaches might be based on software or hardware, as well as they might arise in relation with human factor. For an attacker that can pass beyond the human factor, it is much easier to overcome the technological cyber-security solutions. Because, even if all the technological regulations and security problems are developed and determined, the users having lack of awareness would disable these technical solutions [73]. The individual does not want to protect any component that is not valuable to him/her. For this reason, one of the most important components of the information security is undoubtedly the training and awareness [74].

In some of the studies on reasons of information security threats, it can be seen that these threats more frequently originate from unaware or ill-minded personnel having authorization to enter or access to the company when compared to hackers, malwares and malicious hardware. For this reason, the personnel selection, training, information storage policies, and the persons having conscious and compliant character may have significant contribution to the security [75]. In a study carried out on the potential attacks to enterprise information systems, two attacks performed by an insider and by a malware were compared, and it was determined that the insider cause higher level of damage [76].

The social engineering is defined as the process of capturing the confidential information or unauthorized access to the systems by tricking the users. The single known protection method against the social engineering is the efficient information security awareness [77]. Thanks to these trainings, it can be ensured that the users' knowledge and awareness about the social engineering attacks will be increased and such attacks can be prevented [78].

In the holistic approach regarding the enterprise information security, the human aspect is a factor that should never be neglected [79]. The objective of information security trainings and awareness is to draw the attention of users to the security of information systems. In other words, it is to inform the employers and users about the information security and its importance.

### 4.6 Monitoring, Auditing and Reporting

Within the scope of struggle with insider threat and especially in preventing the abuse of privileged accounts, the behaviors of users in information systems should be monitored, audited, and reported. Moreover, the monitoring, auditing, and reporting should be used in order to reveal if all of the technological solutions and procedures realized by the company regarding the

information security are put into practice accurately by the employers [32]. These three arguments are important for the company in terms of risk management and compliance to security standards and policies [80].

Especially the insiders having privileged accounts should be considered as the most important threat since they know the fundamentals of basic operation of company and information system. They may hide themselves by concealing their attacks to information systems under the cover of their legal duties. It is more likely for an insider, who have the privileged account and the trust of company, to infiltrate into the information system and to hand the critical information over to third parties [81]. For this reason, the activities of privileged account users within the information system should be closely monitored by establishing a technical infrastructure. The reports must be inspected at certain intervals so that a behavior that does not carry an attack symptom at first sight but may constitute an unobtrusive piece of an attack can be detected.

## 5. Solution Suggestions

In order to prevent the breaches arising from privileged accounts in insider attacks, the companies should develop a security procedure based on the subjects discussed above. The procedure that will be developed should;

- Block the access of IT personnel to the resources, for which they are not authorized and which are out of their responsibility,
- Clearly determine the limits of IT personnel's responsibilities,
- Train IT personnel to increase the awareness and knowledge about IT security,
- Prevent the arbitrary operations performed by IT personnel,
- Prevent the access of evil-minded individuals to the resources, for which they are not authorized,
- Keep the log records that will facilitate monitoring the activities of IT personnel,
- Increase the resistance of company to the password attacks to be performed by attackers on the information system,
- Directly involve the executives into the IT security process.

The mechanism to be established within the scope of procedures should be integrated with information systems of company. This mechanism should be placed between the valuable IT resources and IT personnel as an additional security layer in access to servers and computers within the IT infrastructure of company (Fig. 2)


Fig.2. Position of privileged account management and control mechanism in an IT infrastructure

## 6. Conclusion

The companies make investment to the state-of-art security software and hardware solutions in order to protect their valuable data. But, in case of the seizure of privileged accounts by using human-oriented attack methods such as social engineering, even the latest technological security solutions might be useless. The seized privileged accounts might cause the infiltration to the information system of company including the most critical and sensitive data. This situation may cause various destructive effects on the company such as damage the company's reputation. For this reason, the companies should re-evaluate the number of privileged accounts and create the privileged accounts at adequate number and with required authorizations. The authorizations of all other accounts should be limited in parallel with the "need-to-know" principle. Thus, even in case of the worst scenario, the potential consequences will be limited to the authorization of relevant account.

Within this context, the approach presented in this paper aims to increase the robustness of information system against the insider attacks, as well improving the information system security. Moreover, it should not be expected to solve all IT security problems. The emphasized approach aims to take the privileged accounts having various rights, allowances, and privileges under

control. Furthermore, it is also aimed to determine the passwords of privileged accounts in parallel with fundamental IT security principles and to create passwords that are more robust to password attacks.

By means of this approach, it was aimed to clearly determine the duties and responsibilities of IT personnel within the company. Thus, this may be possible to equally distribute the workload of IT personnel and to clearly determine their roles in information system. Task distribution of IT personnel may prevent the authorization conflicts by rearranging the responsibilities regarding the data, resources, and services in information systems.

This approach will increase the awareness of IT personnel, who have insufficient knowledge about the IT security and insider threats, and enable the executives to understand the importance of this subject. The realization of suggested approach will increase the robustness of company regarding this issue by preventing the abuse of privileged accounts in insider threats. This approach will not only take the privileged accounts under control, but it will also remarkably contribute to the prevention of data breaches. The security of information systems, which gain robustness against the conscious or unconscious intervention, will significantly increase.

## References


[1] Bishop, M.: 'The insider problem revisited'. Proc. New security paradigms, Lake Arrowhead, CA, USA, September 2005, pp. 75-76

[2] Brackney, R. C., Anderson, R. H.: 'Understanding the Insider Threat'. Proc. RAND Corporation Conference, Santa Monica, CA, USA, March 2004, pp. 11-32

[3] Keeney, M., Kowalski, E., Cappelli, D. et al., ' Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors' 2005), pp. 1-45

[4] Martinez-Moyano, I. J., Rich, E., Conrad, S. et al.: 'A behavioral theory of insider-threat risks', ACM Transactions on Modeling and Computer Simulation, 2008, 18, (2), pp. 1-27

[5] Kandias, M., Stavrou, V., Bozovic, N. et al.: 'Proactive insider threat detection through social media: the YouTube case'. Proc. 12th ACM Workshop on privacy in the electronic society, Berlin, Germany, November 2013, pp. 261-266

[6] Liu, D., Wang, X., Camp, J.: 'Game-theoretic modeling and analysis of insider threats', International Journal of Critical Infrastructure Protection, 2008, 1, pp. 75-80

[7] Jang-Jaccard, J., Nepal, S.: 'A survey of emerging threats in cybersecurity', Journal of Computer and System Sciences, 2014, 80, (5), pp. 973-993

[8] Magklaras, G. B., Furnell, S. M.: 'Insider Threat Prediction Tool: Evaluating the probability of IT misuse', Computers & Security, 2001, 21, (1), pp. 62-73

[9] Humphreys, E.: 'Information security management standards: Compliance, governance and risk management', Information Security Technical Report, 2008, 13, (4), pp. 247-255

[10] Chinchani, R., Iyer, A., Ngo, H. Q. et al.: 'Towards a Theory of Insider Threat Assessment'. Proc. Int. Conf. Dependable Systems and Networks (DSN'05), Yokohama, Japan, June 2005, pp. 108-117

[11] Cappelli, D. M., Moore, A. P., Trzeciak, R. F.: 'The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)' (Pearson Education, Westport, MA, USA, 2012) p. 23

[12] Greitzer, F. L., Moore, A. P., Cappelli, D. M. et al.: 'Combating the Insider Cyber Threat', IEEE Security & Privacy Magazine, 2008, 6, (1), pp. 61-64

[13] Bishop, M., Gates, C.: 'Defining the insider threat'. Proc. 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead, Oak Ridge, TN, USA, 12 - 14 May 2008, pp. 1-3

[14] Huey, P. Oracle Database Security Guide [Online]. Available: http://www.webcitation.org/6otEQCDt2

[15] El Maliki, T., Seigneur, J.-M.: 'A Survey of User-centric Identity Management Technologies'. Proc. Int. Conf. Emerging Security Information, Systems, and Technologies (SECUREWARE 2007), Valencia, Spain, October 2007, pp. 12-17

[16] De Capitani di Vimercati, S., Paraboschi, S., Samarati, P.: 'Access control: principles and solutions', Software: Practice and Experience, 2003, 33, (5), pp. 397-421

[17] Symantec, '2016 Internet Security Threat Report' (Symantec, 2016), p. 53

[18] Ponemon, '2016 Cost of Data Breach Study: Global Analysis' (IBM, 2016), p. 2

[19] IBM, 'X-Force Threat Intelligence Index' (IBM, 2017), p. 19

[20] Vormetric, '2016 Vormetric Data Threat Report' (Vormetric, 2016), p. 11

[21] AlienVault, 'Analyst Report:Insider Threat Report' (AlienVault, 2016), pp. 4-7

[22] Haystax, 'Insider Attacks Industry Survey' (Haystax, 2017), p. 14

[23] Cser, A., Balaouras, S., Koetzle, L. et al., 'The Forrester Wave: Privileged Identity Management' (Forrester, 2016), p. 2

[24] Verizon, 'Data Breach Investigations Report' (Verizon, 2017), p. 48

[25] Ponemon, 'Privileged User Abuse & The Insider Threat Report' (Raytheon Company, 2014), p. 7

[26] Pilling, R.: 'Global threats, cyber-security nightmares and how to protect against them', Computer Fraud & Security, 2013, 2013, (9), pp. 14-18

[27] Claycomb, W. R., Huth, C. L., Flynn, L. et al.: 'Chronological Examination of Insider Threat Sabotage: Preliminary Observations', Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 2012, 3, (4), pp. 4-20

[28] Roy Sarkar, K.: 'Assessing insider threats to information security using technical, behavioural and organisational measures', Information Security Technical Report, 2010, 15, (3), pp. 112-133

[29] Padayachee, K.: 'An assessment of opportunity-reducing techniques in information security: An insider threat perspective', Decision Support Systems, 2016, 92, pp. 47-56
[30] Baracaldo, N., Joshi, J.: 'An adaptive risk management and access control framework to mitigate insider threats', Computers & Security, 2013, 39, pp. 237-254
[31] Chagarlamudi, M., Panda, B., Hu, Y.: 'Insider Threat in Database Systems: Preventing Malicious Users' Activities in Databases'. Proc. Sixth Int. Conf. Information Technology: New Generations, Las Vegas, NV, USA, April 2009, pp. 1616-1620
[32] Colwill, C.: 'Human factors in information security: The insider threat – Who can you trust these days?', Information Security Technical Report, 2009, 14, (4), pp. 186-196
[33] Agrafiotis, I., Nurse, J. R. C., Buckley, O. et al.: 'Identifying attack patterns for insider threat detection', Computer Fraud & Security, 2015, 2015, (7), pp. 9-17
[34] Bishop, M., Gates, C., Frincke, D. et al.: 'AZALIA: an A to Z assessment of the likelihood of insider attack'. Proc. IEEE Conference on Technologies for Homeland Security, Boston, MA, USA, May 2009, pp. 385-392
[35] Wang, Y. L., Yang, S. C.: 'A Method of Evaluation for Insider Threat'. Proc. Int. Symposium on Computer, Consumer and Control, Taichung, Taiwan, June 2014, pp. 438-441
[36] Nance, K., Marty, R.: 'Identifying and Visualizing the Malicious Insider Threat Using Bipartite Graphs'. Proc. 44th Hawaii Int. Conf. System Sciences, Kauai, HI, USA, January 2011, pp. 1-9
[37] Morgan, S., 'CyberSecurity Market Report', Cybersecurity Ventures, https://cybersecurityventures.com/cybersecurity-market-report/, accessed November 2017
[38] Hu, Q., Xu, Z., Dinev, T. et al.: 'Does deterrence work in reducing information security policy abuse by employees?', Commun. ACM, 2011, 54, (6), pp. 54-60
[39] Sladic, G., Milosavljevic, B., Konjovic, Z.: 'Context-sensitive access control model for business processes', Computer Science and Information Systems, 2013, 10, (3), pp. 939-972
[40] De Clercq, J., Grillenmeier, G.: 'Single Sign-On', in 'Microsoft Windows Security Fundamentals', (Digital Press, Burlington, NJ, USA, 2007), pp. 533-579
[41] Jensen, G., 'Managing the Keys to the Kingdom - Privileged/Shared Accounts', Oracle, https://blogs.oracle.com/cloudsecurity/managing-the-keys-to-the-kingdom-privilegedshared-accounts-simeio-solutions, accessed November 2017
[42] Slade, R.: 'Dictionary of Information Security' (Elsevier Science, Rockland, MA,USA, 2006) pp. 43,101
[43] A. Younis, Y., Kifayat, K., Merabti, M.: 'An access control model for cloud computing', Journal of Information Security and Applications, 2014, 19, (1), pp. 45-60
[44] Stoneburner, G., Goguen, A., Feringa, A., 'Risk Management Guide for Information Technology Systems' 2012)
[45] Moses, S., Rowe, D. C., Cunha, S. A.: 'Addressing the Inadequacies of Role Based Access Control (RBAC) Models for Highly Privileged Administrators: Introducing the SNAP Principle for Mitigating Privileged Account Breaches', International Journal of Intelligent Computing Research, 2015, 6, (3), pp. 583-591
[46] Indu, I., Anand, P. M. R.: 'Identity and access management for cloud web services'. Proc. IEEE Recent Advances in Intelligent Computational Systems (RAICS), Trivandrum, India, December 2015, pp. 406-410
[47] Grafton, J.: 'Avoiding the five pitfalls of privileged accounts', Network Security, 2013, 2013, (5), pp. 12-14
[48] Gaw, S., Felten, E. W.: 'Password management strategies for online accounts'. Proc. second symposium on Usable privacy and security, Pittsburgh, PA, USA, July 2006, pp. 44-55
[49] Jouini, M., Rabai, L. B. A., Aissa, A. B.: 'Classification of Security Threats in Information Systems', Procedia Computer Science, 2014, 32, pp. 489-496
[50] Jones, A., Colwill, C.: 'Dealing with the Malicious Insider'. Proc. 9th Australian Information and Warfare Security Conference, Perth, Western Australia, 1-3 December 2006, pp. 1-14
[51] Kavanagh, J., 'Security special report: The internal threat', ComputerWeekly, http://www.computerweekly.com/feature/Security-special-report-The-internal-threat, accessed November 2017
[52] Sandhu, R. S., Coyne, E. J., Feinstein, H. L. et al.: 'Role-based access control models', Computer, 1996, 29, (2), pp. 38-47
[53] Tep, K. S., Martini, B., Hunt, R. et al.: 'A Taxonomy of Cloud Attack Consequences and Mitigation Strategies: The Role of Access Control and Privileged Access Management'. Proc. IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, August 2015, pp. 1073-1080
[54] Vroom, C., von Solms, R.: 'Towards information security behavioural compliance', Computers & Security, 2004, 23, (3), pp. 191-198
[55] Buszta, K.: 'Security management', in Tipton, H. F., Krause, M., (Eds.): 'Information Security Management Handbook', (Taylor & Francis, Boca Raton, FL,USA, 2007, 6th edn.), pp. 155-164
[56] Laurent, M., Denouël, J., Levallois-Barth, C. et al.: 'Digital Identity', in Laurent, M., Bouzefrane, S., (Eds.): 'Digital Identity Management', (Elsevier, London, UK, 2015, 1st edn.), pp. 33-40
[57] Ayed, G. B., Ghernaouti-Helie, S.: 'Digital Identity Management within Networked Information Systems: From Vertical Silos View into Horizontal User-Supremacy Processes Management'. Proc. 14th Int. Conf. Network-Based Information Systems, Tirana, Albania, September 2011, pp. 98-103
[58] Wood, P.: 'Implementing identity management security - an ethical hacker's view', Network Security, 2005, 2005, (9), pp. 12-15
[59] Bonneau, J.: 'The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords'. Proc. IEEE Symposium on Security and Privacy, San Francisco, CA, USA, May 2012, pp. 538-552
[60] Morris, R., Thompson, K.: 'Password security: a case history', Commun. ACM, 1979, 22, (11), pp. 594-597
[61] Hayashi, E., Hong, J.: 'A diary study of password usage in daily life'. Proc. SIGCHI Conference on Human Factors in

Computing Systems, Vancouver, BC, Canada, May 2011, pp. 2627-2630
[62] Kraus, R., Barber, B., Borkin, M. et al.: 'Windows Operating System – Password Attacks', in 'Seven Deadliest Microsoft Attacks', (Syngress, Burlington, MA, USA, 2010), pp. 1-23
[63] Zhang, L., McDowell, W. C.: 'Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords', Journal of Internet Commerce, 2009, 8, (3-4), pp. 180-197
[64] Shay, R., Komanduri, S., Kelley, P. G. et al.: 'Encountering stronger password requirements: user attitudes and behaviors'. Proc. Sixth Symposium on Usable Privacy and Security, Redmond, WA, USA, July 2010, pp. 1-20
[65] Yan, J., Blackwell, A., Anderson, R. et al.: 'Password memorability and security: empirical results', IEEE Security & Privacy Magazine, 2004, 2, (5), pp. 25-31
[66] Inglesant, P. G., Sasse, M. A.: 'The true cost of unusable password policies: password use in the wild'. Proc. SIGCHI Conf. Human Factors in Computing Systems, Atlanta, GA, USA, April 2010, pp. 383-392
[67] Gehringer, E. F.: 'Choosing passwords: security and human factors'. Proc. Int. Symposium Technology and Society (ISTAS'02), Raleigh, NC, USA, June 2002, pp. 369-373
[68] Kuo, C., Romanosky, S., Cranor, L. F.: 'Human selection of mnemonic phrase-based passwords'. Proc. Second symposium on Usable privacy and security, Pittsburgh, PA, USA, July 2006, pp. 67-78
[69] Hansman, S., Hunt, R.: 'A taxonomy of network and computer attacks', Comput. Secur., 2005, 24, (1), pp. 31-43
[70] Hoque, N., Bhuyan, M. H., Baishya, R. C. et al.: 'Network attacks: Taxonomy, tools and systems', Journal of Network and Computer Applications, 2014, 40, pp. 307-324
[71] Adams, A., Sasse, M. A.: 'Users are not the enemy', Commun. ACM, 1999, 42, (12), pp. 40-46
[72] Wilhelm, T.: 'Professional Penetration Testing: Creating and Operating a Formal Hacking Lab' (Syngress, Burlington, MA, USA, 2009) pp. 339-391
[73] Shaw, R. S., Chen, C. C., Harris, A. L. et al.: 'The impact of information richness on information security awareness training effectiveness', Comput. Educ., 2009, 52, (1), pp. 92-100
[74] Gönen, S., Ulus, H. İ., Yilmaz, E. N.: 'An Examination upon the Crimes Committed on Informatics', International Journal of Informatics Technologies (IJIT), 2016, 9, (3), pp. 229-236
[75] Shropshire, J., Warkentin, M., Sharma, S.: 'Personality, attitudes, and intentions: Predicting initial adoption of information security behavior', Computers & Security, 2015, 49, pp. 177-191
[76] Leitner, M., Rinderle-Ma, S.: 'A systematic review on security in Process-Aware Information Systems - Constitution, challenges, and future directions', Inf. Softw. Technol., 2014, 56, (3), pp. 273-293
[77] Gardner, B.: 'What Is a Security Awareness Program?', in Gardner, B., Thomas, V., (Eds.): 'Building an Information Security Awareness Program', (Syngress, Boston, MA,USA, 2014, 1st edn.), pp. 1-8
[78] Arachchilage, N. A. G., Love, S.: 'Security awareness of computer users: A phishing threat avoidance perspective', Comput. Hum. Behav., 2014, 38, pp. 304-312
[79] Rocha Flores, W., Antonsen, E., Ekstedt, M.: 'Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture', Computers & Security, 2014, 43, pp. 90-110
[80] Sharma, A., Sharma, S., Dave, M.: 'Identity and access management- a comprehensive study'. Proc. Int. Conf. Green Computing and Internet of Things (ICGCIoT), Noida, India, October 2015, pp. 1481-1485
[81] Nguyen, N., Reiher, P., Kuenning, G. H.: 'Detecting insider threats by monitoring system call activity'. Proc. IEEE Systems, Man and Cybernetics Society Information Assurance Workshop, West Point, NY, USA, June 2003, pp. 45-52