Insider Threats in Air-Gapped Networks: A Security Perspective

Ashwini Kumar Verma
Department of CSE
University School of ICT
Gautam Buddha University, Greater Noida, India

Sanjay Kumar Sharma
Department of CSE
University School of ICT
Gautam Buddha University, Greater Noida, India

ABSTRACT
Mitigating the risks posed by insiders with legitimate access is a complex challenge in the field of cybersecurity. Even with cutting-edge security policies in place, malevolent insiders remain a significant threat to businesses due to their comprehensive awareness of organizational assets and processes, which may include exploitable vulnerabilities. This threat is particularly concerning for air-gapped networks, which are frequently utilized by security-sensitive entities such as the military, critical infrastructure, finance, and research and development institutions. While these networks are difficult to hack from the outside, they are highly susceptible to insider attacks. While there are existing insider danger taxonomies for general computer networks, they do not account for the unique risks associated with malicious insider in air-gapped networks. As a result, authors have developed a new taxonomy that focuses on the actions taken by trusted individuals. Our research involved identifying the shortcomings of current taxonomies and mapping real-world instances of insider threats to our proposed taxonomy. Our findings suggest that successful exploits in air-gapped networks require both physical and cyber-world components.

General Terms
Computer Science, Network Security, Isolated Networks

Keywords
Air-gapped Network, Cyber Security, Insider Attack.

1. INTRODUCTION
Modern enterprises are confronted with significant cyber security expostulations due to their growing dependence on cyber connectivity. While traditional cybersecurity efforts have been primarily focused on external threats, recent security incidents involving trusted insiders like Edward Snowden and Robert Hanssen have created new obstacles for identifying potential insider threats [1]. As a result, insider threat detection has become one of the most challenging cybersecurity concerns for businesses and government agencies alike.

Air-gapped networks are commonly utilized by security-focused enterprises [2]. Security measures such as Firewalls, IDS/IPS, and SIEM systems are typically deployed to secure these isolated networks. However, these measures primarily target external risks and are not elevated to protect against insider attacks. Insiders are considered the primary threat to air-gapped networks due to their elevated level of access to IT infrastructures [3]. In spite of the implementation of security measures, a resolute insider may only need a single chance to introduce a zero-day malware or extract confidential information. [4]. Notorious instances of insider threats include the Stuxnet and Agent.btz viruses [2].

Studies conducted on insider attacks [5], [6], [7] reveal theoretical constraints in comprehending the issue, as well as practical challenges in identifying and implementing effective responses. Moreover, most existing literature primarily focuses on insider threats within firms that utilize conventional computer networks with internet access. However, it is essential to give specific consideration to insider threats within air-gapped networks, both in theory and practice.

The definition of the term "insider" has varied across different research studies. Some have adopted a limited perspective, defining insiders as those who have physical or logical access to any resource from a cyber standpoint. In contrast, others have adopted a more comprehensive approach, taking into account cultural, organizational and societal factors as well. Few definitions explore the degree of insiderness, which signifies the magnitude of an individual's access to a resource. As a result of their diverse application across various fields by scholars and practitioners, these terms are currently vaguely defined [8].

An employee who is considered trustworthy (an insider) within the organization carries out or neglects to perform an action (intentionally or unintentionally) that harms any asset / capacity and has negative effects for the enterprise. In different contexts, the word "closed network" might signify different things. A closed network is defined as "any organization's computer network that is isolated (air-gapped) from any public network for both inbound and outgoing traffic."

Enterprises that prioritize security often opt for air-gapped computer networks. While businesses with internet access are exposed to diverse attacks such as malware, phishing, SQL injection, zero-day exploits and DoS, using anti-malware software with auto-update features and implementing the latest security updates and malware definitions across all computer nodes can help manage the risks. However, air-gapped networks present a challenge in maintaining consistent security posture due to the difficulty of applying security patches and malware definitions to all machines.

Air-gapped networks are commonly used to protect against external attacks. By isolating the network from the internet, vulnerable systems become less exposed to external attacks. Though, cyber attacks such as Stuxnet have shown that focused attacks on isolated facilities are real and dangerous risks. These occurrences demonstrate that air-gapped networks may be breached, and there has been a growing interest in exfiltrating sensitive information from networks using concealed cross network attacks [9], [10]. In these situations, the primary attack vector is a trusted insider with legitimate access to the secured computer facilities, such as an employee, contractor, or supplier.

2. ASSESSMENT OF CURRENT INSIDER THREATS

In this section, authors will analyze the limitations of existing insider threat categories for use in air-gapped networks and highlight their possible drawbacks. The shortcomings of previous research have not been systematically explored, which authors will utilize to propose a new insider threat taxonomy.

The RAND Corporation has developed a classification system for unusual insider conduct [11] intended for the intelligence community, which offers indicators for identifying possible insider attacks. They suggest that a malevolent insider must carry out a sequence of actions that can be monitored using both non-cyber and cyber metrics. In a study by Igure et al., several classifications for cyber-attacks and system vulnerabilities created from 1974 to 2006 were reviewed. It was found that all classifications share 4 dimensions: target, source, impact, and vulnerability. Additionally, the study determined that a security assessment taxonomy should be hierarchical and specific to a particular domain [12].

A study by the CERT Insider Threat Team [13], [14] explores unintentional insider threat (UIT), which happens when corporate information is accidentally compromised. They drafted a layered classification consisting of 4 elements: (i) role of user, (ii) cause, (iii) data delivery mechanism, (iv) industry. The classification focuses on both technical and non-technical aspects of the insider attack, including human factors, risk management, and psychosocial factors.

In four separate real-world threat situations, a framework for defining insiders and their behaviours was implemented [15]. The framework presented by the authors covers the roles of the company, individual, IT systems, and environment, which includes incidents such as HDD removal, increase in email replies and purloined intellectual property. The authors suggest that this paradigm may be used to analyze the problem of insider threat from four distinct viewpoints. The author Magklaras et al. projected a tiered categorization of insider IT system abuse that focuses on the human aspect. The categories include System Role, Misuse Reason, and System Consequences, and they are utilized to develop an Insider Threat Prediction Tool [16].

Mundie et al. and Homoliak et al. 2019 provides a thorough examination of Insider Attack categories and protection strategies. The authors did an excellent job categorising threats and defensive solutions from earlier research and produced a structured category that combined several previous taxonomies utilising the 5W1H information collecting technique. Initially, writers assigned several classifications to 5W1H questions and included a few sub-classifications to bolster their structural category [17], [18].

Authors construct a new categorization of insider attacks based on the recognised inadequacies of existing classifications, covering thorough coverage of the subject from several angles.

3. PROPOSED CATEGORY OF INSIDER ATTACKS

The primary difference between an air-gapped network and a regular computer network used by sensitive organizations is that the first one is not directly connected to external networks, making it less exposed to external threats. Additionally, data exfiltration and malware infiltration on an air-gapped network would typically require the involvement of authorized users, resulting in limited channels for such attacks. Due to their isolation, it is difficult for network admin to keep air-gapped networks updated with the latest patches and security measures, which makes them more susceptible to newly identified attacks by security researchers. Nonetheless, another aspects of security, including organizational aspects, cyber aspects, psychological aspects, and social aspects, would be similar for both categories of networks.

Multiple parameters may have an unfavourable impact on the organisation. These threats can emerge in a variety of domains, including physical, cyber, individual, and organisational. Table 1 provides a comparison of several Insider attacks variables for public and air-gapped networks. Table 1 illustrates that the majority of insider risks perceived in public and air-gapped networks are similar, with the primary difference being their susceptibility to outside exposure. The factor that sets apart these two types of networks in terms of insider threats is the physical closeness of the perpetrator to their target.

Table 1. Comparison of insider threats

Domain	Insider Attack	Public Network	Air-gapped Network
Physical	Unauthorized access	Same in both networks	
	Destruction	Same in both networks	
Cyber	Remote Hack	High	Low
	Disclosure	High	Low
	Destruction	Same in both networks	
Individual	Psychological	Same in both networks	
	Social	Same in both networks	
	Environmental	Same in both networks	
	Technical Skills	Same in both networks	
	Knowledge	Same in both networks	
	Access	Same in both networks	
Organization	Policies/ Procedures	Same in both networks	
	Environment	Same in both networks	

By expanding our analysis of insider attack, our categorization now encompasses four new aspects as depicted in figure 1:

1. The identity of the enterprise's personnel involved.

2. The actions or inactions of personnel.

3. The enterprise's assets involved in the attack.

4. The potential consequences for the enterprise as a result.

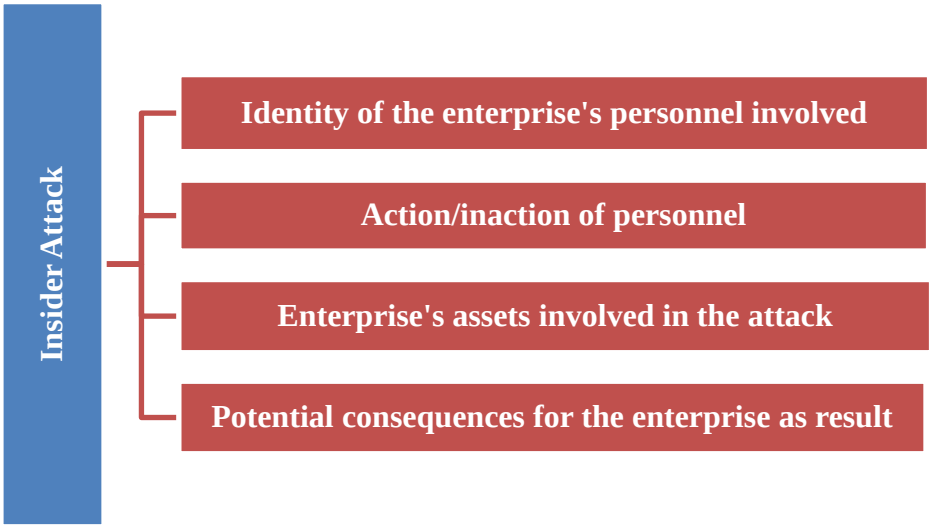

Fig 1: New categorization of insider attack in air-gapped network

3.1 The identity of the enterprise's personnel involved

In an enterprise, the personnel comprises of employees who are entrusted with access to specific assets in order to perform their job duties. An individual's job within an organization is defined by a combination of their access privileges, knowledge of organizational assets, rules and procedures, as well as their skill level. Role-based access control mechanisms are commonly employed to determine user access based on the principle of need-to-know, which is an effective approach. By classifying users based on their roles, an enterprise can gain a better understanding of insider threats and develop appropriate security measures to counter them.

The personality traits of personnel comprise social and psychological elements that can prompt them to engage in unwelcome behaviors. Psychological variables are considered relatively fixed aspects of an individual's personality, while social influences are more temporary and subject to change over time. Factors such as physical, mental health, and age as well as financial and domestic circumstances, can have both positive and negative effects on the personality of personnel.

For an individual to commit a criminal act, they must also possess a motivation to do so. This motivation may stem from social or environmental factors such as feelings of injustice, insult, stress, unhappiness, or other causes that can provide a significant impetus for an otherwise trustworthy individual to engage in inadvertent threatening behavior.

3.2 The actions or inactions of personnel

The authorised individual's action or inaction is the most crucial factor in the suggested categorization. Air-gapped computer networks are highly vulnerable to malicious actions by trusted insiders. This is because the absence of external connections protects the network from external threats, but any internal breach can have severe consequences. Whether intentional or unintentional, any unpleasant behavior by individuals, including those who are complacent or lazy, can potentially compromise the security of these networks. Some examples of physical security breaches that can pose a danger to air-gapped networks include hardware movement, vendor visits to critical locations, and so on. Therefore, it is crucial to remain vigilant and implement robust security measures to prevent any unauthorized access or malicious activity within the network.

Furthermore, insider activities might emerge as one of three main behaviours: abusing allowed access to corporate assets, circumventing established security measures, and, most importantly, violating the organisational security policy. Typically, any perilous conduct should contravene the established security protocols of an organization, otherwise, the policy itself could become a threat. Insufficient, inadequate, or ambiguous security regulations would not act as a deterrent to potential wrongdoers. Implementing appropriate tools, techniques, and processes for policy enforcement presents another challenge. However, instilling trust in policy enforcement can be achieved through measures such as mandatory leave, job rotation, frequent audits, and contingency drills, which can discourage and delay any unwarranted actions.

Looking at it from the perspective of an organization, any action taken must appear in either the cyber or physical realm and involve either ingress or egress in context to air-gapped networks. Since accessing air-gapped computer networks necessitates physical access, the authorized personnel must perform some activity within a specific timeframe and location by utilizing their access to organizational resources. Actions can also be classified according to their time of execution, location, and different dependencies on the host and network. In the case of physically sabotaging IT assets, the perpetrator would necessitate physical access and ample time to execute the destructive activity. Additionally, various logical and physical constraints, such as prime hours and colleagues, may curtail the offender's actions.

3.3 Asset of the enterprise

The third categorization component is the entrepreneurial firm, which can either be the object of the threatening activity or used to carry it out. An effective attack would need a sequence of failures or bypasses of other, less critical security measures, which could result in the destruction of essential enterprise assets. These assets could be physical or virtual and may include vulnerabilities that are time-sensitive, either in terms of

technology or procedures that can be exploited. Threatening activities may also harm digital assets, such as trust and reputation. Additionally, the location of the asset can serve as a categorization factor for insider threats in air-gapped networks since it affects accessibility for individuals within the enterprise.

3.4 Consequences for the enterprise

The fourth component in the internal threat categorization is the ramifications for the enterprise if such dangerous behaviours are carried out effectively. Through unauthorised disclosure, alteration, and destruction / denial of vital business services, It could potentially jeopardize the confidentiality, integrity, or availability of enterprise assets. Such implications might be further characterised as low, medium, or high severity to organizational processes.

Air-gapped networks are often employed in sensitive facilities, such as SCADA systems in critical infrastructure, making even a small compromise have a significant impact on the agency's capabilities (as was the case with Stuxnet). Additionally, the magnitude of the damage triggered by an action could have a global or local impact on the organization's capabilities and mission. A malevolent act of the largest magnitude and worldwide impact will have serious consequences for the company. As a result, adequate mitigation for such severe repercussions should be prioritised.

The suggested categorization offers a comprehensive understanding of the Insider Attack issue, particularly in the context of physically disconnected networks. It aims to record the “Who, What, When, Where, Why, and How” of each cybersecurity event, which were not previously included in other categorization schemes. Homoliak et al. 2019 has proposed a categorization that combines prior categories with additional classifications [18], but their study neglects to consider system’s security gaps that manipulated to achieve the breach, as well as the asset, action, and position of the attacker. In the case of air-gapped networks, the position of these components is significant.

4. APPLICATION OF SUGGESTED CATEGORIES

In this section, authors establish how our proposed categorization can be applied to real-world instances of insider threats in air-gapped networks.

4.1 Dissatisfied program writer initiating system sabotage

A government body contracted a system developer to create a safety-related system. When severe difficulties with the programme were discovered, the employee was ordered to document the source code in order to have centralised control over the development. In fear of project outsourcing, salary reductions, and demotion, the employee hid the codebase to impede the transfer of the project. Despite filing a grievance that was dismissed, the individual still quit as a result. He removed the source code when returning the official laptop, stating it was regular wiping process. It was later discovered that he/she had erased the final copy of the codebase and transferred it to portable storage. The organization was unable to do any system maintenance due to a lack of source code. The investigators later discovered the protected source code at his residence.

Investigation: The insider felt uneasy and bereaved as a result of the outsourcing and potential wage cut. Because he was adept and had total authority over the source code, prior to termination, the individual replicated codebase and erase it from the office terminal. This activity raised concerns for the company's availability.

4.2 Dissatisfied network admin causing network outage

A government organization’s IT department recruited a network administrator who was the sole individual possessing comprehensive knowledge and the admin password for the network he had constructed. He refused to allow any new administrator in order to maintain control of the network. He was punished and moved to another project due to poor performance and threatening conduct with coworkers. Because the insider refused to provide up network credentials, he was fired and jailed. As the passwords were unavailable, network access was blocked for a period of weeks. Later on, coworkers discovered rogue access points that had been placed in concealed locations and were configured to cause system failure upon password-less reset attempts. Finally, during a meeting, the criminal provided the genuine password to a government official while claiming that his activities were security best practises.

Investigation: When new administrators arrived, the insider felt bereaved and unjustly. He was dismissed as a result of his hostile work environment conduct. Due to the inaccessibility of network passwords, his talents and privileges to the whole network kept the company in a state of denial for weeks on end.

4.3 Harassed executive causing data loss

The insider was employed as a director by a government agency. The insider found himself in a tough predicament as a result of his ongoing battle with another official. While at work, the insider began destroying official HR doc’s. The following day, a coworker reported the deletion of e-mails from the individual's computer and the destruction of documents from the previous day. Approximately two weeks later, the insider began deleting official e-mails and spreadsheets. The insider was immediately terminated from their position, but no charges were filed against them.

Investigation: The insider found themselves in an uncomfortable situation due to a dispute with another official. As a sort of retaliation, the insider began destroying everything within his reach, both physically and electronically.

4.4 Assistant causing IP data theft

A beverage manufacturing business employed an insider as an executive administrative assistant. He or she got access to confidential information such as product samples and private papers as an executive assistant. Physical security cameras caught her taking company secrets and product samples from her backpack. The insider stole physical documents and made duplicates, as well as printing a sensitive e-mail from their executive regarding classified projects. They were supported by two outside co-conspirators who promised to sell the organization's trade secrets to a rival. A replica of the confidential e-mail was sent, along with supplementary information and the co-conspirators' bank account details.

Investigation: Our proposed categorization has been successfully applied to four genuine insider vulnerabilities in air-gapped networks. These examples demonstrate how our categorization can effectively define the problem of insider threats in this type of environment. By addressing the Who, What, When, Where, Why, and How of insider attacks, our categorization can aid in the selection of appropriate

countermeasures, including procedures, policies, tools, and techniques to implement robust security measures.

While existing insider attack categorizations are suitable for public networks, our approach is specifically tailored to air-gapped networks, which have limited outside exposure and only trusted insiders can carry out harmful acts. Our categorization places significant concentration on position in three of the four dimensions, making it a comprehensive and useful tool for addressing insider threats in air-gapped networks.

5. CONCLUSION

Insider threat scenarios span various domains, including organizational culture, behavioral sciences, and cybersecurity. Research shows that in most cases, warning signs of insider misconduct could have been detected through social and behavioral indicators, which could have been addressed to prevent the incident. However, the lack of accurate data remains the biggest challenge in insider threat research. Organizations either have limited knowledge of insider abuse or are hesitant to disclose information due to the risk of reputation and financial loss.

This paper focuses on describing insider attacks in air-gapped networks. Authors analyze different insider threat categories, identify their limitations in the context of air-gapped networks, and propose a new categorization specifically for insider threats in such networks. A then map our new categorization to real-world examples to demonstrate its effectiveness in characterizing risks and enabling organizations to choose appropriate security measures and strategies.

6. REFERENCES

[1] Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., and Osula, A. M. 2015. Insider threat detection study. NATO CCD COE, Tallinn.

[2] Guri, M., and Elovici, Y. 2018. Bridgeware: The air-gap malware. Communications of the ACM, 61(4), 74-82. DOI:10.1145/3177230.

[3] Choo, K. K. R., Smith, R. G., McCusker, R., and Choo, K. K. R. 2007. Future directions in technology-enabled crime: 2007-09. Canberra: Australian Institute of Criminology.

[4] Choo, K. K. R., and Smith, R. G. 2008. Criminal exploitation of online systems by organised crime groups. Asian journal of criminology, 3, 37-59. DOI: 10.1007/s11417-007-9035-y.

[5] Al-Mhiqani, M. N., Ahmad, R., Zainal Abidin, Z., Yassin, W., Hassan, A., Abdulkareem, K. H., and Yunos, Z. 2020. A review of insider threat detection: classification, machine learning techniques, datasets, open challenges, and recommendations. Applied Sciences, 10(15), 5208. DOI: 10.3390/app10155208.

[6] Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., and Burnap, P. 2020. Impact and key challenges of insider threats on organizations and critical businesses. Electronics, 9(9), 1460. DOI: 10.3390/electronics9091460.

[7] Alsowail, R. A., and Al-Shehari, T. 2020. Empirical detection techniques of insider threat incidents. IEEE Access, 8, 78385-78402. DOI: 10.1109/ACCESS.2020.2989739.

[8] Hunker, J., and Probst, C. W. 2011. Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 2(1), 4 27.

[9] Guri, M., Kachlon, A., Hasson, O., Kedma, G., Mirsky, Y., and Elovici, Y. 2015. Gsmem: Data exfiltration from air-gapped computers over {GSM} frequencies. In 24th {USENIX} Security Symposium ({USENIX} Security 15) (pp. 849-864).

[10] Zhou, Z., Zhang, W., and Yu, N. 2018. IREXF: data exfiltration from air-gapped networks by infrared remote control signals. arXiv preprint arXiv:1801.03218. DOI: 10.48550/arXiv.1801.03218.

[11] Brackney, R. C., and Anderson, R. H. 2004. Understanding the insider threat. Proceedings of a March 2004 workshop. RAND CORP SANTA MONICA CA.

[12] Igure, V. M., and Williams, R. D. 2008. Taxonomies of attacks and vulnerabilities in computer systems. IEEE Communications Surveys & Tutorials, 10(1), 6-19. DOI: 10.1109/COMST. 2008.4483667.

[13] Alhanahnah, M. J., Jhumka, A., and Alouneh, S. 2016. A multidimension taxonomy of insider threats in cloud computing. The Computer Journal, 59(11), 1612-1622. DOI: 10.1093/comjnl/bxw020.

[14] Team, C. I. T. 2013. Unintentional insider threats: A foundational study. cahier de recherche CMU/SEI-2013-TN-022, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 18. DOI: 10.1184/R1/6585575.v1.

[15] Magklaras, G. B., and Furnell, S. M. 2001. Insider threat prediction tool: Evaluating the probability of IT misuse. Computers & security, 21(1), 62-73. DOI: 10.1016/S0167-4048(02)00109-8.

[16] Predd, J., Pfleeger, S. L., Hunker, J., and Bulford, C. 2008. Insiders behaving badly. IEEE Security & Privacy, 6(4), 66-70. DOI: 10.1109/MSP.2008.87.

[17] Mundie, D. A., Perl, S., and Huth, C. L. 2013. Toward an ontology for insider threat research: Varieties of insider threat definitions. In 2013 third workshop on socio-technical aspects in security and trust (pp. 26-36). IEEE. DOI: 10.1109/STAST.2013.14.

[18] Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., and Ochoa, M. 2019. Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. ACM Computing Surveys (CSUR), 52(2), 1-40. DOI: 10.1145/3303771.