

# Towards a Social Network Approach for Monitoring Insider Threats to Information Security

Anand Natarajan and Liaquat Hossain

School of Information Studies, Syracuse University  
4-108 Center for Science and Technology, Syracuse, New York 13244-4100  
{anataraj, lhossain}@syr.edu

**Abstract.** Monitoring threats to information security is increasingly becoming important to protecting secured organizational documents. There is increasing number of threats to information security, which originates from the internal users of the system. Insider is defined as a trusted person and has access to classified documents. Our focus here is on understanding mechanisms for monitoring insiders working with the intelligence community. The analyst working with the intelligence community usually works on a TOI (Topic of Interest) and AOI (Area of Interest) so that they can develop a report about a very specific question. How do we ensure that these analysts do not perform malicious act during their course of collection, analysis and report generation for a given task? We suggest the need for social network monitoring of these analysts, which would help decreasing the threats of malicious intent of the insider. In this paper, we first provide a logical representation of analyst workflow model. Secondly, we describe the use of social network approach in general and suggest its application to monitoring insider threats. Thirdly, we provide an analysis of the properties and characteristics of social network analysis as they relate to monitoring insider threats for the intelligence community<sup>1</sup>.

## 1 Insiders Threats to Information Security

An insider is an individual within the organization who is empowered to fulfill certain job functions. The empowerment of the individual depends on the context as well as the time duration of the job requirement. For example, a financial broker working in the stock market industry might have access to certain financial information of his or her customer as long as the customer has business transactions with the broker. An insider for this study is defined as someone who has been (explicitly or implicitly) granted privileges authorizing use of a particular system or facility [1].

It is important to acknowledge that there is an increasing abuse of responsibilities and power for malicious use by insiders. Cases of moles within the Intelligence Community (IC), insider trading in financial stock markets, bank fraud by employees are some of the common insider threats facing current organizations. Unfortunately, there are no fully developed technologies or mechanisms for detecting or preventing insider threats to occur. The subtle nature of these threats and the innumerable ways by which these threats can happen makes it extremely difficult to detect or prevent these

---

<sup>1</sup> This work was supported by Advanced Research & Development Activity (ARDA's) Information Assurance for the Intelligence Community (IAIC) program.

insider threats. Therefore, it is increasingly important for developing effective strategies and methods to detect and prevent these insider threats.

In this conceptual paper, we focus our effort on monitoring insider threats to information security for the intelligence community. First, we provide a general overview of the insider threats within the intelligence community using an analyst workflow model that focuses on social interactions. Secondly, we provide a description of background and techniques of social network analysis and suggest its application to monitoring insider threats for the intelligence community. Lastly, we suggest a social network approach as they relate to monitoring the insider threats for the IC.

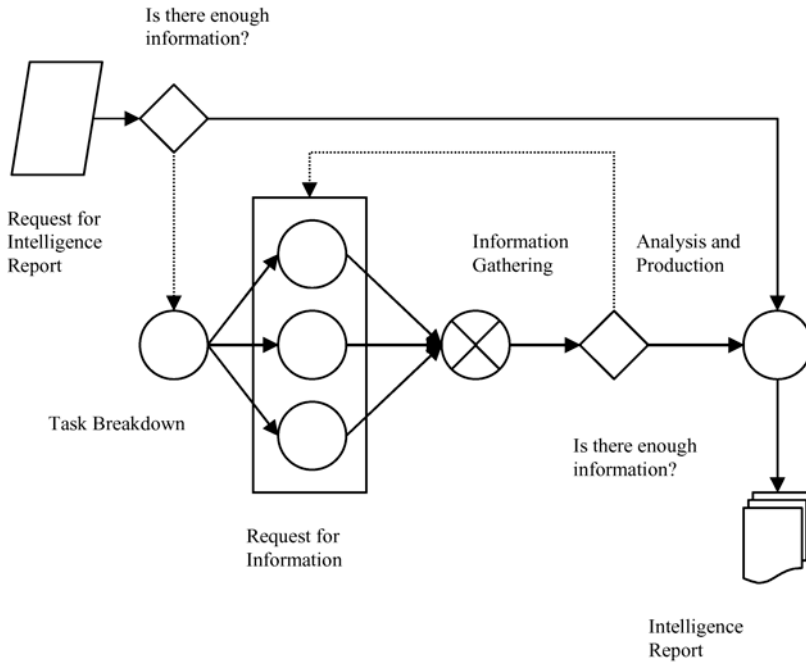
## 2 Insider Threats in the Intelligence Community

Intelligence community spans across multiple organizations like the CIA, FBI, NSA, etc. The functioning of these organizations is largely dependent on highly critical information. The reliability and the security of this information are important for the operations and the success of these organizations. The NSTISSC (currently CNSS) report on insider threat [2], suggests an increasing number of insider malicious behavior, which poses threats to the national security. However, the measures proposed in these studies largely focus on securing insider's use (or abuse) of information systems within the community. However, securing the information systems alone does not eliminate the risk of insider threats. Malicious behavior of "logical outsiders" [1], where people from outside can obtain secure information through social contacts (friendship, kinship relations), can be equally threatening. In this paper, we propose that monitoring and profiling the social behavior of insiders within the community would help us better manage the threats to the community from the insiders.

One of the critical operations of the analysts within the IC is the production of intelligence reports, which contains critical and classified information. The process of information collection for producing intelligence reports involves the collaboration of various socio-technical entities to accomplish specific tasks. The various social and technical entities involved in the intelligence reports production process are the agents, roles and the resources within the various organizations. The general logical workflow model of the process of production of intelligence report by analysts within the US Intelligence Community is shown in the figure below. This workflow model is a result of observations and discussion at the workshop to develop workflow scenarios of analysts. This validated model is a very general description of the operations of analysts. The process flow model suggests that production of report involves several steps: (i) task assignment, (ii) collection assignment, (iii) analysis and production, and (iv) dissemination of the reports.

At each stage of the process, various roles are required to accomplish specific tasks (such as SME, linguist). These roles interact with each other and with other technical resources (such as UN Database, OTA Database) for collecting information required for analysis. Figure 2 represents the social interactions of analysts with other actors and resources in the production of the intelligence reports. As mentioned above, it requires the cooperation and coordination of various social and technical entities within the community. The request for report is in the form of a "Question". Within the context of this "question", various analysts (A) are assigned (or enrolled) into various roles (R). These roles interact with each other and with resources (information systems) within and across the various organizations in the community. These interac-

tions of insiders seeking intelligence information serve as source to model their social behavior.

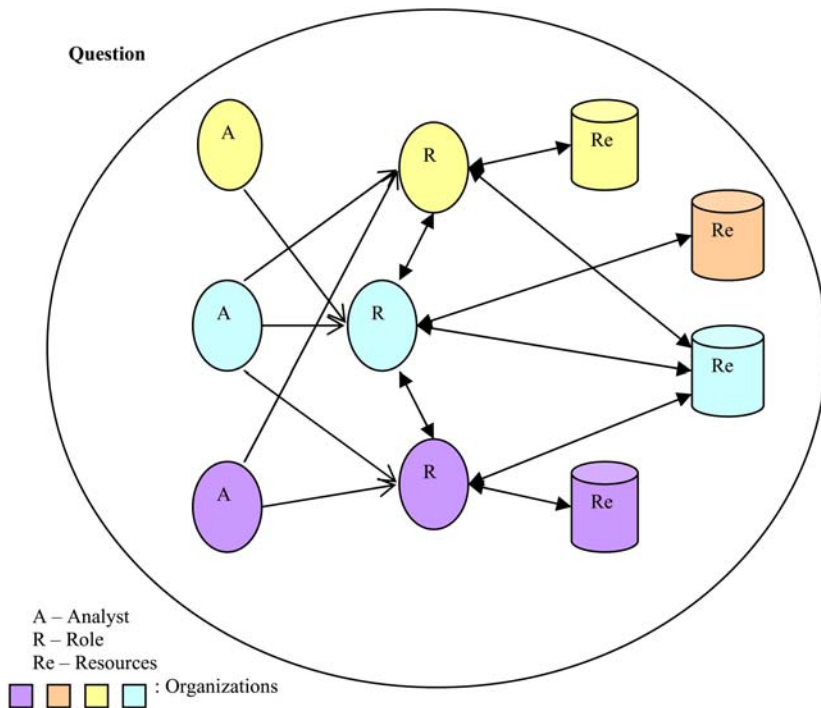


**Fig. 1.** A general Logical Representation of Intelligence Analyst Workflow

Instances of malicious behavior by insiders include collection of information about topics that are not of interest, disseminating information to unauthorized individuals, and accessing information sources that are not relevant to current task that is assigned to the analyst. Information about the activities of analysts could be collected and compared (peer comparison) with other analysts working on similar problem to identify malicious behavior. The obtained social behavior can also be compared to an expected behavior to measure deviations from normal activities. Social Network Analysis serves as a powerful tool to perform this analysis.

### 3 Social Network Analysis: Background and Techniques

Network data consists of a square array of measurements (in most cases), with both the rows and columns having the same cases (or actors, subjects). Network data focuses on the actors and their attributes. Thus the analysis is on the relationship among the actors rather than the attributes of the actors by itself. The two major emphases on network analysis include, seeing how actors are embedded within the overall network structure, and seeing how the whole pattern of individual choices gives rise to more holistic patterns. One major difference between the conventional data analysis is that the samples in network analysis are not independent. [1]



**Fig. 2.** Network Representation of interactions of analysts in IC

The various strategies to perform social network analysis include analysis of the complete network or partial network or egocentric network. The critical element in social network analysis is to specify the type of relationship (ties) that determines the association between the actors. There may be several relations between a given set of actors, but typically the researcher specifies one of few types. Binary, nominal or ordinal measure could then be used for measuring the relationships. The types of analysis include descriptive analysis (median tie strength of actor, mean density of network, degree of similarity among actors, finding patterns in the network) and interpretive analysis (includes stability, reproducibility or generalizability of result in single sample).

### 3.1 Analyzing Data in Graphs and Matrix

Social scientists use mathematical concepts from “matrix algebra” and “graph theory” to create “sociograms”. A dataset in the form of a matrix can be used to measure the degree of symmetry in the pattern of relations among the actors. Correlations between matrices say how similar they are and regression is used to predict the scores of a matrix using another [3]. For example, we might be able to analyze if the kinship predicts the strength of friendship. The paths between the nodes are used in calculating the number and length of pathways among actors, which is critical to notions of power, centrality, and the formation of groups and substructures. Granovetter [4] used

network concepts like the “strength of weak ties” to analyze the opportunities and constraints for individuals. Burt [5] used the theory of “structural holes” to measure “social capital” of managers.

### 3.2 Properties of Networks and Actors

Difference in how the individuals are connected within the network can be very important in understanding their attributes and behaviors. It is important to go beyond the simple calculations of density of the network and the individuals. The ideas of distance between the actors and the connectedness help in understanding the “opportunities” and “constraints” faced by individuals within the social groups. One important constraint is that a single example (or representation of a relationship) of the graph cannot and usually does not capture all of the possibilities (other possible ties) [1]. Two important social attributes of actors lie in the connection (the relationship) and the number of connections between actors (path).

**3.2.1 Connections.** In a network, the number of actors, the number of possible connections and the actual connections that is present provides valuable information about the population, like the “moral density” and the “complexity” of the social organization. The number and the kinds of ties that individuals have help determining how much embedded they are within the social structure, the opportunities and constraints towards their behavior, and the influence and the power that they have. Dyadic analysis of the directed data can tell us about the stability of the social network. It is perceived that a network with predominance of null or reciprocated ties maybe more stable than asymmetric connections. Triadic analysis could be performed to analyze the transitivity of the actors within the network that contributes to their equilibrium.

- a) *Size, density and degree:* The size of the network is calculated by counting the number of nodes. The density of the network is the proportion of all ties that could be present that actually are. In a binary network, the mean gives the percentage of all possible ties. The standard deviation gives an idea of how different the ties are. Calculating the *out-degree* of each row (“source”) describes the role of that actor as source within the network. The variance of each row tells us how predictable the behavior of the actor is. Similarly, for *in-degree*, we can calculate the mean, SD and variance that provides information about the power of individuals or how much of information overload they manage.
- b) *Reachability:* An actor is said to be reachable if he can be tracked through a set of connections regardless of the number of actors between them. Calculating reachability can identify formation of sub-groups.
- c) *Reciprocity and Transitivity:* Dyadic and Triadic relationships are used to calculate reciprocity and transitivity. By identifying the number of “In ties”, “Out ties”, “No ties”, “Reciprocated ties”, and the “Neighborhood size” of each actor, we can analyze the social roles of the actors within the network.

**3.2.2 Distance.** The distance among the actors is an important macro-characteristic of the network as a whole. In a simple graph, a *walk* is a general connection between two

people, a sequence of actors and relations that begins and ends with actors. *Geodesic distances* (the shortest walk between two nodes) are used to measure how accessible the actors are within the network. It helps to assess the nature of the network, like the ease of information flow. *Eccentricity* is the measure of how far an actor is from the furthest other. Row-wise and column-wise measures of the mean and standard deviation of the eccentricity would give us an idea about how “far” an actor is from each other and how far each actor is from each other who might be trying to influence them. The *diameter of a network* is the largest geodesic distance in the network. It can be used to calculate the upper bound of the lengths of connections that we want to study.

#### 4 A Case for Application of SNA for Monitoring Insider Threats

Network analysis is a powerful tool for modeling and analyzing the behavior and intentions of actors within any social network. Modeling expected behavior and comparing it with the actual behavior will produce variances in the output that predicts and detects malicious intent and behavior. For example, the calculation of in-degree for an information collector is an indicator of the high information that he has requested. An analyst performing the role of information collection is “expected” to have a high density of in-degree. The density can be peer evaluated and the variance will predict the nature of the analyst’s behavior or intentions. On the other hand, an analyst performing the role of “analysis” of the collected information should have a lesser density of in-degree.

Similarly, the nature of the connections between the analysts could be determined by the analysis of transitivity and reciprocity attributes present in the relationship within the social network. Analysts working in groups (informal) due to their past association (friendship) can be determined by transitive and reciprocity analysis of their interactions. The network distance between various actors within the social network is an estimation of the power wielded by these actors due to their position within the social structure [6]. Every analyst within the organization can use this to perform an impact analysis of malicious behavior. Contingency plans can be developed to mitigate and minimize the impact of such malicious activities.

As seen above, social network analysis could be used as a powerful tool for modeling and analyzing the behavior and intentions of actors, especially analysts working within the intelligence community. These examples provided represent only a small percentage of the immense potential of the use of social network analysis. There are several other properties and methods in social network analysis that help identify social characteristics or attributes of individuals and groups such as power, creation of social roles and comparing structural equivalence of network relations. Further research needs to be done to realize the complete potential of this powerful tool. Currently, the authors are involved in the experiments that involve the use of social network analysis for modeling the behavior of analysts within the intelligence community. The use of social network analysis could be the move towards the solution for monitoring and detecting the threats posed by the malicious intentions and behaviors of the insiders.

## 5 Conclusions

We provided a logical representation of analyst workflow model for developing an understanding of how intelligence analyst progress from task assignment to completion of the report. We further discussed social network approach in general and concluded that it is a useful paradigm for monitoring insider threats and in particular for the Intelligence Community.

Implications of future research will include the development of specific strategies in social network analysis to model the behavior of analysts. The authors, along with other researchers, are currently involved in research to design and develop a working model that incorporates the capabilities of social network analysis, along with other techniques, for monitoring insider threats.

The social network approach towards monitoring threats can be applied in other industries that face similar risks from insiders. We conclude by saying that social network approach is a very useful approach for modeling and analyzing the hidden behavioral characteristics of actors within social groups.

## References

1. Neumann, P. (1999). Risks of Insiders. *Communications of the ACM*, Vol. 42(12), pp. 160.
2. NSTISSC (July, 1999). The Insider Threat to US Government Information Systems. Retrieved on Feb 01, 2004.  
URL: [http://www.nstissc.gov/Assets/pdf/NSTISSAM\\_INFOSEC1-99.pdf](http://www.nstissc.gov/Assets/pdf/NSTISSAM_INFOSEC1-99.pdf)
3. Hanneman, R. A. (2001). *Introduction to Social Network Method*. Retrieved on Jan 28, 2004. URL: <http://faculty.ucr.edu/~hanneman/SOC157/NETTEXT.PDF>
4. Granovetter, M. (1973). The Strength of Weak Ties. *The American Journal of Sociology*, 78(6), 1360 – 1380.
5. Burt, R. S. (1997). The contingent value of social capital. *Administrative Science Quarterly*, 42(2), 339 – 365.
6. Wellman, B. (1983). Network Analysis: Some Basic principles. *Sociological Theory*, Vol. 1, pp. 155 – 200.