A Method of Simplifying the Asset Dependency Cycle in Security Risk Analysis

Edri Yunizal¹, Judhi Santoso², Kridanto Surendro³
¹,²,³Program Studi Doktor Teknik Elektro dan Informatika, Institut Teknologi Bandung
¹Manajemen Informatika, IAIN Batusangkar

E-mail: ¹edriyunizal@iainbatusangkar.ac.id, ²judhi@informatika.org, ³surendro@gmail.com

Abstract. In recent years, one obstacle to information security risk analysis is the complexity of asset dependency. Developing research tends to produce models with great complexity and some that do not involve dependency cycles, make the model difficult to implement. This research developed the idea of compound nodes to produce a modular risk analysis that simplify the asset dependency cycle. This study uses the following assumptions: aimed at quantitative assessments, values based on likelihood, and based on graph basic models. The stages of the method consist of identification of cyclic in the initial model, reconstructing cyclic graph into acyclic graph, and reconstruction of cyclic sub graph into acyclic sub graph. Through an illustrative example, this research produces a method that helps facilitate understanding the complexity of asset dependencies in risk analysis.

1. Introduction

Large amounts of data on systems connected to the internet certainly need a protection mechanism. The method commonly used to obtain adequate protection is to carry out an information security risk analysis (ISRA), a process to identify and evaluate factors that can interfere with the success of the project or the achievement of objectives [1]. ISRA has an important role in the organization's ability to survive [1] – [3].

One of the main limitations of ISRA is asset dependency complexity [2]. The failure of one information asset in an organization can affect other assets and result in greater system failure. For example, a web has high security, but installed on a server with poor security. The calculation of web risk must also consider the condition of the server, because it is relevant. This makes the risk model assuming asset dependency stronger than not [4]. Unfortunately, traditional risk analysis only partially studied about it [5].

[5] – [15] is research that offers solutions to asset dependency constraints. Unfortunately, no one takes into account the asset dependency cycle. Cyclic dependence in risk analysis can originate from the process of collecting data [16] or requirements analysis [17]. Cyclic data collection may be due to weaknesses of the learning algorithm, with hidden variables. Example of a requirements analysis cycle is a client server application consisting of three components: database, application interface, and backup. Unauthorized access to the application interface will continue to allow unauthorized access to the backup. Unauthorized backup access will allow the attacker to obtain a password from the database, which again provides unauthorized access to the interface. The relationship between the database, application interface, and backup is a form of cycle.
Muller [17]–[19] attempted to solve the limitations of cyclic dependency by introducing the Dependency-Aware Root Cause (DARC) model in the Critical Infrastructure (CI) domain. Unfortunately, CI focuses on a series of important assets with a small size, while in other domains; the number of assets can be very large. In his own perspective, Muller showed that complexity is one of the future jobs. ISRA requires models that can take into account their cyclic dependencies, but in simpler complexity.

2. Related Works
The existence of asset dependencies in ISRA is generally new. Sendi et al. [2] in ISRA's taxonomy identified asset dependency as one of the fundamental problems that current risk tools and methods cannot address.

Suh and Han [6] initiated the asset dependency of ISRA. The model developed to determine the value of assets based on the relationship between the asset and the business function. Assets are valued based on the relationship with other assets that use maximum functions. Rahmad [8] added confidentiality and integrity in the form of threat scenarios corrected the weaknesses of [6], which only focused on availability.

Tatar & Karabacak [10] also observed the weaknesses in terms of availability in [6], and chose the hierarchical valuation of assets considering the CIA (confidentiality, integrity and availability) of these assets; this connectivity then presented in the form of associated tables. Breier [11] considered that the proposed asset dependency analysis [6] was too straightforward and could not describe it in detail because it based only on the maximum value of the related assets. Next, Breier presented the relationship between assets in the form of related graphs and provided asset values based on connection considerations, a risk matrix, physical connection patterns, and logic. The resulting value was combined with the initial value of the asset independently.

Alpcan & Bambos [5] examined the problem of interdependence in organizational risk based on three main factors of risk management: business units, threats/ vulnerabilities and humans. The proposed framework examined dependencies within and between business units, security/vulnerability threats and people using graph theory. Then, the model registered dynamic changes in the risk due to the interactions. Finally, they classified the risks in the organizations by using risk algorithms.

Khanmohammadi & Houmb [13] introduced a new concept in risk assessment focusing on business objectives, ignoring the assets and process which supporting it. The process identified and assessed the risks at the business process level. The risk was also grouped based on the critical level, role and level of importance of the organization as a whole. Schmidt & Albayrak [14] have developed a quantitative framework for risk assessment vertically and horizontally. Horizontal connectivity is between assets, while vertical connectivity brings connectivity into three levels: process, service, and application. At the application level, the hardware gives virtual asset values. Hierarchical virtual asset values is combined with district time algorithms to obtain risk values. This approach evaluates business processes and thanks to infrastructure dependencies, these values are broken down into each component of the computer system.

Lololei et al [15] divided the values of the assets on independent and dependent values. Independent values obtained from two parameters: cost (initial costs, maintenance costs, replacement costs), and the level of importance of the asset in the business process. The dependence value of the asset dependency presented in the form of CIA parameters, focused on availability. Level of dependency classified as partial or total, as indicated by the dependency percentage.

Muller [19] has created a DARC model, a quantitative research that offers convenience because the organization only needs to determine the value of assets ranked as root and attribute the probability of dependence. This search has improved by positioning the assets in layers by himself [18].

Based on the basic description of several previous studies. The theoretically elaborated models can overcome the limits of asset dependence. However, in practice, Rahmad [7]–[9] must use a very large list of threat scenarios [19]. Breier's research [11] showed the connectivity of 10 assets in a building, it will be very difficult to apply it to the real world with all assets. Similarly, with the development of
Muller [19], the connectivity of each asset will be determined in a special graph that makes the mapping very complex, and will be difficult for organization to implement. Muller stated that the fact that graphics dependencies can be large is a problem that must be solved [19]. This clearly shown in [19] of how to apply the proposed DARC model in the real world (Figure 6). This shows how the loss of readability of the graph. Even for the supply chain sector, the development of initial risk has a very large graph, see [20].

The second obstacle is the coverage of the types of risk. The investigation conducted by Loloei and Shahriari [15], Suh and Han [6] is example that admitted only the assets availability risk. The dimensions of the information security objectives only transmitted as separate values sometimes used as the average for each asset, such as research [6]–[9].

Qualitative approaches are indeed more widely used in the field of information security [3]. Indeed, this approach presents the subjectivity of the evaluator [2] which further contributes to the creation of weaknesses in expert dependence.

Ouyang told CI that one of the recommended and advanced methods for overcoming dependencies is high level architecture (HLA). HLA uses the concept of modularization to overcome difficulties in the legibility of the risk analysis model that takes into account asset dependencies [21]. With the similarity of the existing parameters, IS can take advantage of these developments, just like Muller [19], who has developed several CI studies for IS.

Differences in modelling and simulation approaches sometimes lead to conflict, so an integrated approach is needed to differentiate each responsibility into a uniform framework [22]. Modularization of Eusgeld's risk analysis at the highest level of the system of system (SoS), which in turn consists of several subsystems at the critical infrastructure level, and with the lowest, is at the system level. Unfortunately, this remains at the conceptual level with several challenges in its application [22]. Which later became the basis of this article.

Figure 1. Study of literature

To apply the Eusgeld conceptual model [21] in the risk analysis, the approach with fault tree analysis (FTA), event tree analysis (ETA) and the attack tree cannot be used because it does not support cycle dependencies. The only possible approach is to use the attack graph. A dependency model involving dependency cycles is the connectivity model of the Omer & Schill’s [23]. In their study, the cycle was correlated with dependencies for the case of web services.
Based on the study of the literature (Figure 1), this paper proposed a model of risk analysis based on dependence. The idea came from the development of the dependence of the IS risk analysis [5]–[9], [13]–[15], [15] resulting from the Sendi’s taxonomy [2]. Based on the faster development of CI, the adaptation of the conceptual model developed by the literature [21], [22], [24], [25]. In the final stage, the conceptual model was applied in the operational model using a combination of Muller risk analysis proposals [17]–[19] followed by a compound node proposed by Omer and Schill [23].

3. Methods

3.1. Assumption

3.1.1. Quantitative. The emphasis on the conceptual model makes HLA a challenge in terms of application. However, the idea of combining several models at the same time will be very difficult to be applied in a qualitative research that emphasizes the subjectivity and experience of the evaluation team. This makes it difficult to give an overview of the risks involved. Only quantitative research makes it possible to observe all the risk scenarios and compare them to each other [17].

3.1.2. Likelihood. The risk calculated based on a combination of threat probability estimates for each asset and the impact that affects the assets successfully [26]. The non-consideration vulnerability used Fenz's statement in [9]: the node's probability of exploiting a vulnerability due to the actual threat is only an intermediate node to facilitate the mapping of the threat. After all, the targeted steps are risk analysis, to demonstrate why risk management needs to be implemented [1], which requires simplicity in the components used. Because risk defined as a product of probability and non-compliance, preventive safety measures aim to reduce the likelihood, while mitigation measures applied to reduce the consequences [27]. The first priority is of course to reduce the likelihood.

The likelihood connection expressed in the formula [26]: Risk (Threat, Asset) = Likelihood (Threat) \(\otimes\) Impact (Threat, Asset)

3.1.3. Graph based model. This research adapted the model from [17], because it has considered cyclic in information security. In [17], where for V set as a security incident, statement \(V \subseteq A \times S\) can be used, A is the set of all the assets and S is the set of security properties. These security properties known as Security Triads: Confidentiality, Integrity, and Availability (CIA) [17], so S consists of \{C, I, A\}. Asset confidentiality written as \(a.s\) instead of \((\alpha, \beta) \in A \times S\). So that the hard disk (HDD) availability can be written HDD.A. If incident a have impact on incident b, it can be written \(a \rightarrow b\) instead of \((\alpha, \beta)\), so that if hard disk availability affects data availability, it can be written HDD.A \(\rightarrow\) DATA.A.

3.2. Construction

Based on the previous assumptions, the simplification process consisted of the following steps:

1. Identification and extraction of cyclic sub graphs.
   Cyclic identification and extraction process used Tarjan algorithm [28], as done by [23] to test the measurement of cyclic dependence on web services. Tarjan’s algorithm has the ability to identify elementary circuit, an elementary path (a path contains no node twice) with the exception that its first and last node are identical. Tarjan algorithm requires initial graph (G1) as basic input. Tarjan algorithm uses G1 to identify cyclic sub graphs, and then extracts them into array of cyclic sub graph (G2)

2. Reconstruct initial cyclic graph into acyclic graph.
   The next step is to transform each G2 elements in G1 into a compound node. In the process of transformation, there is a change in the situation at the incoming and outgoing edges. Edges connected to the compound node replaces all the edges connected to the G2 element. The incoming edge of the compound node is from the incoming edge of the G2 elements, the same thing applies to the outgoing edge. So that it can be interpreted that every node that depends on
the G2 elements will depend on the compound node that replaces it. This also applies vice versa; the compound node generated during the reconstruction will remain dependent on the dependent G2 elements.

3. Reconstruct cyclic sub graph into acyclic ones.

Based on the model definition [17], node execution was not performed several times, only once in one experiment. Therefore, every G2 element structure must be acyclic. Restructuring process used Wang algorithm [29]. The use of Wang's algorithm is for cyclic restructuring. This algorithm used the Bayesian Network (BN) due to the acyclic requirements. Based on Wang's algorithm, a node that is not an entry point of a cycle will be more efficient to calculate the cumulative score without considering the cycle. For each node in the cycle that has only one incoming edge, the cumulative score can be calculated (after the calculation of the point entry is complete) as the node is not in the cycle.

The results of the reconstructions of the cyclic G2 elements are stored in acyclic G4 elements (also in array).

![Figure 2. G1 Initial Graph](image)

3.3. Illustration

A data security case study of a client-server application will demonstrate the implementation capabilities of the proposed method.

In the client-server application, a data center requires availability of routers and servers. Server availability requires the availability of the database. Database availability requires the availability of internal data A and transaction data A. For security, database availability requires the availability of database backup. Availability database backup requires the confidentiality of the application obtained from confidentiality of internal data C.

Based on the model requirements, the case presented in the form of the initial graph G1 (Figure 2). G1 shows the connection between:

1. Availability of data center (DC.A)
2. Availability of routers (R.A)
3. Availability of server (S.A)
4. Availability of database (DB.A)
5. Availability of internal data A (ID.A)
6. Availability of transaction data A (TD.A)
7. Availability of database backup (BD.A)
8. Confidentiality of application (A.C), and
9. Confidentiality of data internal (ID.C)
Based on first step, the proposed method identified and extracted cyclic sub graphs from G1. For the sake of simplicity, in this case there was only one cyclic graph: DB.A → BD.A → A.C → ID.C → DB.A, with DB.A as entry point. Result of this step is the extraction of sub graph cyclic G2 (Figure 3).

**Figure 3. G2 Sub Graph Cyclic**

In the second step, the proposed method is reconstructing G1 into a compound node (CN.DB.A). In G2, there are 2 incoming edges: ID.A → DB.A, and TD.A → DB.A, both of which then became the incoming edge for CN.DB.A. G2 has one outgoing edge DB.A → S.A, similar to the incoming edge; this also became the outgoing edge of CN.DB.A. G3 stored the results of this reconstruction (Figure 4). The initial form of G1, which originally had a cyclic structure, was fully acyclic in its new form.

**Figure 4. G3 Graph acyclic**

Final step is to reconstruct it into the acyclic form because G2 is still cyclic. This stage is different from the G3 reconstruction process, simplifying DB.A as an entry point through one execution with placement as the initial node. The graph became acyclic by removing the edge ID.C → DB.A, then extracted into G4 (see Figure 5).

**Figure 5. G4 Sub graph acyclic**

The use of compound nodes simplifies the attack graphics. The complexity that initially tends to be complicated can be modulated quantitatively. We can see the separate discussion of the composite nodes in acyclic structure.

4. Discussion
Several studies [5]–[15] have offered asset dependency solutions in information security risk taking into account a small number of important assets. In practice, the actual amount of assets in an organization is very large, although the proposed solution might be to model the system in general; the complexity
The biggest challenge in analysing information security risks analysis is to involve asset dependencies. It is always difficult to find achievements that can serve as an organizational basis for identifying risks. The popularity of qualitative solutions will depend largely on the availability of experts for the organization, which will generally have increased costs and subjectivity. Developing a quantitative model that can be cost-benefit oriented and easily understood by managers will be a major step towards meeting these needs.

The attack graph as a form of probability is very promising in the analysis of information security risks because of its flexibility and the support of the dependency cycle. It is just that the complexity of...
some previous studies is difficult to be implemented in the real world. The proposed method makes it possible to analyze the complexity of the risk analysis.

Future work will focus on an evaluation of the proposed method, which may not be presented due to incomplete data. This study will compare several risk analysis models to compare process speed and readability (if possible).

References
[1] Peltier T R 2010 Information Security Risk Analysis (Florida: Auerbach publications)
[2] Shameli-Sendi A, Aghababaei-Barzegar R and Cheriet M 2016 Taxonomy of information security risk assessment (ISRA) Computers & security 57 pp 14–30
[3] Landoll D J and Landoll D 2005 The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments (Florida: CRC Press)
[4] Haines Y Y 2018 Risk modeling of interdependent complex systems of systems theory and practice Risk Analysis 38(1) pp 84–98
[5] Alpcan T and Bambos N 2009 Modeling dependencies in security risk management 2009 Fourth Int. Conf. on Risks and Security of Internet and Systems (CRiSIS 2009) pp 113–6
[6] Suh B and Han I 2003 The IS risk analysis based on a business model Information & Management 41(2) pp 149–58
[7] Rahmad B, Supangkat S H, Sembiring J and Surendro K 2010 Threat scenario dependency-based model of information security risk analysis IJCSNS 10(8) pp 93–102
[8] Rahmad B, Supangkat S H, Sembiring J and Surendro K 2012 Modeling asset dependency for security risk analysis using threat-scenario dependency Int. J. of Computer Science and Information Security 10(4) pp 103–11
[9] Rahmad B 2010 Analisa Risiko Keamanan Informasi dengan Mempertimbangkan Dependensi Skenario Threat dan Kontrol sebagai Pereduksi Likelihood dan Impact Dissertation (Bandung: Institut Teknologi Bandung)
[10] Tatar U and Karabacak B 2012 An hierarchical asset valuation method for information security risk analysis Int. Conf. on Information Society (i-Society 2012) pp 286–91
[11] Breier J 2014 Asset valuation method for dependent entities J. of Internet Services and Information Security 4(3) pp 72–81
[12] Breier J and Schindler F 2014 Assets dependencies model in information security risk management Information and Communication Technol. (Heidelberg: Springer) pp 405–12
[13] Khanmohammadi K and Houmb S H 2010 Business process-based information security risk assessment 2010 Fourth Int. Conf. on Network and System Security pp 199–206
[14] Schmidt S and Albayrak S 2010 A quantitative framework for dependency-aware organizational IT Risk Management 2010 10th Int. Conf. on Intelligent Systems Design and Applications pp 1207–12
[15] Loloei I, Shahriari H R and Sadeghi A 2012 A model for asset valuation in security risk analysis regarding assets dependencies 20th Iranian Conf. on Electrical Eng. (ICEEE2012) pp 763–8
[16] Li K, Ren Y, Fan D, Liu L, Wang Z and Ma Z 2018 Enhance GO methodology for reliability analysis of the closed-loop system using Cyclic Bayesian Networks Mechanical Systems and Signal Processing 113 pp 237–52
[17] Muller S, Harpes C, Le Traon Y, Gombault S and Bonnin J M 2017 Efficiently computing the likelihoods of cyclically interdependent risk scenarios Computers & Security 64 pp 59–68
[18] Muller S, Harpes C, Le Traon Y, Gombault S, Bonnin J M and Hoffmann P 2016 Dynamic risk analyses and dependency-aware root cause model for critical infrastructures Int. Conf. on Critical Information Infrastructures Security pp 163–75
[19] Muller S 2018 Risk Monitoring and Intrusion Detection for Industrial Control Systems PhD Thesis (Luxembourg: University of Luxembourg)
[20] Badurdeen F et al 2014 Quantitative modeling and analysis of supply chain risks using Bayesian theory J. of Manufacturing Technol. Management 25(5) pp 631–54
[21] Eusgeld I, Nan C and Dietz S 2011 System-of-systems: approach for interdependent critical infrastructures Reliability Eng. & System Safety 96(6) pp 679–86
[22] Ouyang M 2014 Review on modeling and simulation of interdependent critical infrastructure systems Reliability engineering & System safety 121 pp 43–60
[23] Omer A M and Schill A 2011 Automatic management of cyclic dependency among web services 2011 14th IEEE Int. Conf. on Computational Sci. and Eng. pp 44–51
[24] Rinaldi S M, Peerenboom J P and Kelly T K 2001 Identifying, understanding, and analyzing critical infrastructure interdependencies IEEE Control Systems Magazine 21(6) pp 11–25
[25] Rinaldi S M 2004 Modeling and simulating critical infrastructures and their interdependencies 37th Annual Hawaii Int. Conf. on System Sciences pp 1–8
[26] Ionita D 2013 Current Established Risk Assessment Methodologies and Tools Master’s Thesis (Enschede: University of Twente)
[27] Khakzad N, Khan F and Amyotte P 2013 Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network Process Safety and Environmental Protection 91(1–2) pp 46–53
[28] Tarjan R 1973 Enumeration of the elementary circuits of a directed graph SIAM J. on Computing 2(3) pp 211–6
[29] Wang L, Islam T, Long T, Singhal A and Jajodia S 2008 An attack graph-based probabilistic security metric IFIP Annual Conf. on Data and Applications Security and Privacy pp 283–96