Logics and Illogic's in Information Security Flow on Process Development Environment

Sivanesh kumar. A, Vinod. D, Velu. C.M, Rajesh. M

Abstract: The objective of the work is to propose a formal technique encompassing the logic and the illogic involved in the security of information science. The received or collected information about the existing or past security incidents in business processes is to be identified for their correctness and preciseness. The emphasis on various segments of the information is analyzed as per the intention of the informer and the involvement of the recipient. The expectation and the acceptance of business information is quantitatively modeled so as to take a correct decision with the proposed logics when multiple business processes handling variety of information with different truth factors are collaborated. The logical deduction, abduction and induction techniques are applied to minimize the vagueness and ambiguity factors. The preciseness of the present information and the emphasis of the past information related to security are formally used to predict the reality of future information security incidents in a business scenario.

Keywords: business process, logics, truth factor, collaboration, information security, vagueness, reality

I. INTRODUCTION

Logic consists of a formal or informal approach, a deductive apparatus and a model-theoretic semantics. The deductive apparatus or inference rules provide formal mechanisms for making valid inferences, and the semantics to codify the security flaw [1]. Inference rules determine how conclusions are drawn from security incidents. It is generally agreed that there are three different inference types: deduction, induction and abduction or hypothesis. Logic allows to make [2] information access to computational systems like (semi-) automated theorem proves, model checkers, computer algebra systems, constraint solvers, or concept classifiers. Unfortunately, these systems have differing foundational assumptions and input languages, [3] which make them non-interoperable and difficult to compare and evaluate in practice. To remedy this situation, we need a foundationally unconstrained framework for knowledge representation that allows representing the meta-theoretic foundations of the mathematical knowledge in the same format and to interlink the foundations at the meta-logical level [4]. Logics allow making mathematical knowledge accessible to computational systems like (semi-) automated theorem proves, model checkers, computer algebra systems, constraint solvers, or concept classifiers. Unfortunately, these systems have differing foundational assumptions and input languages, which make them non-interoperable and difficult to compare and evaluate in practice [5]. To remedy this situation, we need a foundationally unconstrained framework for knowledge representation that allows to represent the meta-theoretic foundations of the mathematical knowledge in the same format and to interlink the foundations at the meta-logical level. Description Logics area of research that study a particular decidable fragment order Logic [6]. The expressiveness makes them a good candidate to describe onto logics every term in the ontology is in terms of necessary (or concept sub assumption), or necessary and (or concept equivalence) conditions.

Logic and Illogic in Information Security

The abduction logic is a method of reasoning in logic and is used to mean just the generation of hypotheses to explain observations or conclusions in computing. For example, if a phishing event has occurred, then an interruption to the business services will occur, thereby leading to a loss in the business. Similarly if a denial of service is occurred, then congestion will take place leading to loss of integrity of information received and in the third case, if spoofing has taken place, then the authenticated address of the sender is lost indicating a threat to the business processes. This abduction logic follows the case if the condition is satisfied and then again it follows the next conditional check for the action to be taken and trusted nodes are established as shown in Figure 1. The deductive reasoning works to narrow down into more specific and ultimately leads to be able to test the hypotheses with specific data a confirmation(or not) of original theories-a top down approach. For example, if all type of attacks happen in a wireless network of the hospital and every medical device are connected in the hospital network and so medical device in the hospital is attacked.

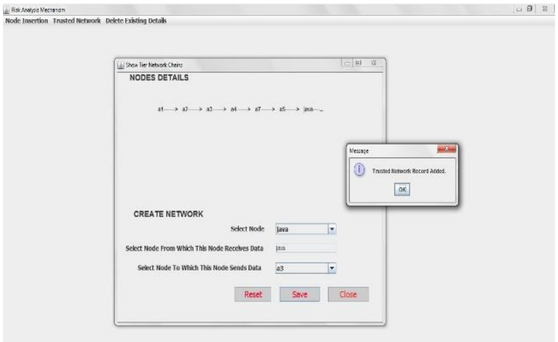
Revised Manuscript Received on September 22, 2019.

Sivanesh kumar. A, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai

Vinod. D, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai

Velu. C.M, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai

Rajesh. M, KRS College of Engineering, Vandavasi, India, Raga Academic Solutions, India



Trusted Network Record Added.

Select Node: java

Select Node From Which This Node Receives Data: java

Select Node To Which This Node Sends Data: a3

Figure 1 Logical Trusted Network Windows

The logical trusted network has been created for various internal security purposes particularly for doctors. Inductive reasoning works the other way, moving from specific observations to broader generalizations and theories and one informally calls this a "bottom up" approach in inductive reasoning, begins with specific observations and measures, begin to detect patterns and regularities, formulate some tentative hypotheses and finally ends up developing some general conclusions or theories. In a case like, a doctor or a nurse or even a lab assistant as an insider leaking or more appropriately selling the private health information of patients in a hospital to an outsider.

Logics in Information Security

The Logics of information security have been established based on the policy aspects of any organization. Generally in product oriented business process the function of availability is authenticated due to lack of defending security safeguards. The logic of information security flow is described below

$$Information \rightarrow Description \rightarrow More\ or\ less\ Factorial \rightarrow Past\ or\ \Pr esen$$

It is intended to form an information security attribute in the recipient of the context, a picture or an idea of what has happened or what exists and what existed in the past information structure. The type of information has been checked in various context for formal logic intention in any form of value based on the time specific either 0 or 1 based on the logical situation as shown below.

Time 0

[Type, value, context, structure/ Information] * Intention (informers) *

Time 1 Involvement (recipient)

T 0

Expectation of information: [info] * intention (info) * inception

T 1 (recipient)

Generally, the information processing flow deals with the prevention and recovery of unstructured information from external attacks. It focuses on the information leakage of the organization which addresses the business outcome. The acceptance of information with the recipient for the change of factor with respect to assets which is needed for the business and also the recovery time for the assets after the attacks are such as to put them into use for business days. The logics of information security assurance pathway are brought out to quantitatively model and estimate the total risks covered when more number of services are interacting if the attack and asset may become non-complaint entities for internal and external users based on acceptance level as shown below.

$$Acceptance\ of\ Information \rightarrow No.\ of\ Recipient * Change\ Factor + No.\ of\ Informers * Truth\ Factor$$

Where the acceptance of information represented AOI is (Acceptance of information), Nr as number of recipients, Ni as number of informers, T.F is a truth factor as shown in Equation (4.1).

$$(AOI) = Intention\left[N_r + N_i\right]T.F$$

(1)

The acceptance of information is a logical comparative and it is not just a matter of black and white; it is up on the intention of the informers recipient by verifying the truth factor of information exchange internally and externally but allows for gradients or fuzzy to evaluate more effectively. An environment defined by a single set of security policies, including a set of people, tools, services and procedures is known as security domain. A Security Domain may consist of a single enterprise or a collection of enterprises. Integrity may vary in three different attributes vulnerability, attack and risk. The vulnerability can create a corruption in data integrity and it is increasingly lockdown when it is attacked which allows the attacker to modify the original data that leads to risk factor.

Information Risk Analysis Logic

Information assurance flow through various risk factors is evaluated and managed in each stage of the process based on risk, vulnerability and cost. It is the process of identifying vulnerabilities to defend future attack through the availability in an organization’s information system. When such vulnerability exists, then security controls are implemented to reduce the likelihood of vulnerability being exercised. When the vulnerability can be exploited, apply layered protections, architectural designs, and administrative controls to minimize the risk or prevent occurrence. When the attacker’s cost is less than his potential gain, protection is applied to increase the attacker’s cost. When the potential loss is substantial, design principles, architectural designs, and technical and non-technical protections are applied to calculate the risk of acceptance; basically risk is up on the threat and vulnerable design of any security policy in an organization to limit the extent of the attack due to the acceptance level of risk represented as follows

$$Risk \rightarrow Threat * Vu\ln erability * \mathrm{Cos}t$$

$$Threat \rightarrow Vu\ln erability * Compliance$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

$$Vu\ln erability \rightarrow Information * \mathrm{Im}\,pact$$

This expression is fundamental to information security.

$$Accep\tan ce\ of\ Information\ asset \rightarrow \text{Availability} * Change\ Factor + Compliance * Truth\ Factor$$

By taking reasonable steps, the confidentiality, integrity, and availability of all components of the organization's information system can be ensured. The information security flow with the expected asset in process p is less than the attack severity index i it is to decide how the process of security failure has occurred in unavoidable circumstances like type improper, context free, data critical and improper information. Based on the process of security failure the availability of assurance (AOA) had been adopted to protect the required level of truth factor which will give the perfect balance between the information security and availability and expectation of asset verified in the equation in (2).

$$Expectation\ of\ asset = \left(1 - p\left[attack_i\right] v\ p\left[insider\ threat\right]\right) \qquad (2)$$

An information security safeguard verifies and understands the present situation to moderate requirement based on the risk level. The process of attack from different methodology will lead to threat by taking advantage over vulnerability as shown in Equation (3)

$$Threat = P\left(attack\right) * V \qquad (3)$$

It is to identify the process of intruder internally and externally with security measures to prevent security failure based on the false entry or improper type of responds; such situation further can be prevented by establishing security policy. Information compromised in many organizations due to security failure, improper information type built poor information structure with respect to attack needs as represented below

P (Security Failure)→ P (Improper Type) + P (Poor structure) +

P (Context Free) + P (Data criticality) +

P (Improper information)

Before validating the information flow to find the threat, the availability of assurance (AOA) has to be given for all potential user to find the change factor (CF) and truth factor (TF) based on the accessibility given as shown in Equation (4)

$$AOA = \left[N_r * CF\right] + \left[N_I * TF\right] \qquad (4)$$

Generally it is to verify that the inside potential user has been given more privilege than the external user in any business process to take advantage on this change factor (CF) and truth factor(TF) of present information and it may cause huge loss that leads to insider threat which is represented as

$$CF\,\alpha\,Attack * Insider\ Threat$$

$$TF\ \alpha\ Confidentiality * Authentication$$

Meantime Presence Edgy Logic (MPEL)

In the semantics of classical logic, the dynamic nature of the security incident and activity cannot be fully explored so as to reason the future security strategies. According to Arthur Prior, a time-dependent notion of the truth values has to be applied not only to the past but also to the latest incidents. The temporal logic representing any particular interval of time or at any exact point of time is to be specified so as to manipulate the tenses in a formal way. The Linear Temporal Logic and Computation Tree Logic are used to capture the different aspects of computation. The semantics of LTL can be defined using the flow of time with a path quantifier and without introducing a transition whereas the CTL operator is defined with respect to transition systems.

The paper addresses the important qualitative relations not only based on the time intervals but also their proximity with respect to each other. The work proposes Interval Proximity Tense Logic (IPTL) in which the operators like before, after, during, since and until are in the interval category and operators like just now, just before and just after are in the proximity category and now or present, past, future are in the tense category. Bi= before an incident, Ai = after an incident, Di = during a period, Si = since a time mark Ui = until a time mark JNi= Just Now an incident, JBi = Just before an incident, JAi = Just after an incident N = now an incident, P= was an incident, F= will be an incident Xi = never an incident, Yi = always an incident, Zi = sometimes an incident as given in Table 1.

Table 1 Meantime Presence Edgy Logic Operators

Meantime Logic		Presence Logic		Edgy Logic	
Emblem	Temp. Logic	Emblem	Temp. Logic	Emblem	Temp. Logic
Bi	Before an incident	JNi	Just Now an incident	Ni	Now an incident
Ai	After an incident	JBi	Just before an incident	Pi	Was an incident
Di	During a period	JAi	Just after an incident	Fi	Will be an incident
Si	since a time mark	Xi	never an incident	Zi	Some time an incident
Ui	until a time mark	Yi	always an incident	Oi	Often an incident

Logical attack detection in information security

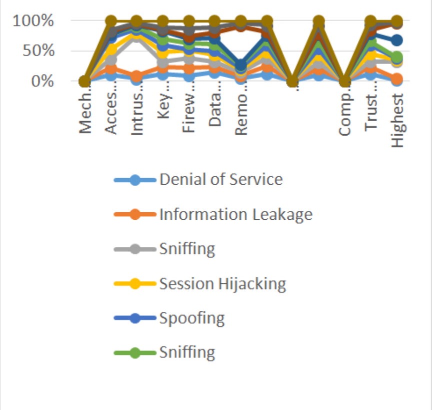
The three dimensional approach in Reality, Perfection and Emphasis in Information Theory is a basic aspect of information flow in a security emphasized organization, during a decay information flow in an organization is an abundant, so most of the assets cannot be protected from compliances. Now the Illogic in Information Security can be constructed using the reality, emphasis and the perfection or preciseness of the information related to security. The security compliances and regulations are to emphasized and governed so as to reduce the risk and compliances in an organization to module the security.

In most of the software enlargement environment in any organization a minor coding inaccuracy can consequence in a serious vulnerability that tops up conceding the security of a complete classification or network. In most of the intervals, a security weakness is not instigated by minor error, still, by a categorization of mistakes that occur throughout the course of the information progress cycle. A coding error is familiarized, it drives unnoticed for the duration of the testing segments, and accessible protection devices that do not halt a positive attack in logical business environment as shown in table 2 and illustrated in figure 2.

Table 2. Positive attack in logical business environment

Attack / Mechanism	Denial of Service	Information Leakage	Sniffing	Session Hijacking	Spoofing	Sniffing	Elevation of rivileges	Virus and Trojans	Insider Threat	Buffer Overflow
Access control	0.5	0.6	0.7	0.8	0.9	0.3	0	0.2	0.1	0.8
Intrusion Detection	0.6	0.8	10	0.9	0.8	0.7	0.5	0.3	0.2	0.6
Key Established	0.7	0.7	0.5	0.9	0.7	0.6	0.8	0.1	0.2	0.7
Firewall Setup	0.5	0.7	0.8	0.7	0.1	0.5	0.4	0.2	0.7	0.7
Data Integrity	0.7	0.4	0.4	0.5	0.3	0.5	0.5	0.4	0.4	0.5
Remote monitoring	0.7	0.8	0.9	0.7	0.4	0.7	0.3	10	0.9	0.6
Network Monitoring	0.8	0.9	0.9	0.7	0.7	0.6	0.5	0.4	0.8	0.5
Security Compliance	0.7	0.6	0.7	0.8	0.6	0.8	0.7	0.1	0.9	0.5
Trust Setup	0.7	0.6	0.5	0.7	0.8	0.4	0.7	0.3	0.5	0.4
Highest	0.8	0.9	10	0.9	0.9	0.8	10	10	0.9	0.8

Figure 2. Logical Attack and logical sequence



The largest value is 0.65 and it is obtained for logics in information security monitoring. Hence this is taken as the best mechanism to predict the probability of attack in any logical business organization.

II. CONCLUSION

The logics and illogic’s as been identified with various methodologies in information security model and it is necessary in order to continue the business in a secure environment. The users are authenticated with their unique return address, which helps to avoid the entry of unauthorized users into the organization. The

Meantime Presence Edgy Logic (MPEL) model provided will keep the availability and security of the information in a balanced state. The correctness, precision and vagueness helps in identification of all the possible risk associated with the assets. These techniques help in maintaining the logical detection from the attackers, in case of any modification by the internal user only the duplicate document is created and reported to the higher authority. This helps in enhancing the development of product of the organization. It evaluates the total risk involved for a process and also provides the mitigation policies in order to extend and continue the business process.

REFERENCES

1. Smith, T.F., Waterman, M.S.: Identification of Common Molecular Subsequences. J. Mol. Biol. 147, 195--197 (1981).
2. May, P., Ehrlich, H.C., Steinke, T.: ZIB Structure Prediction Pipeline: Composing a Complex Biological Workflow through Web Services. In: Nagel, W.E., Walter, W.V., Lehner, W. (eds.) Euro-Par 2006. LNCS, vol. 4128, pp. 1148--1158. Springer, Heidelberg (2006).
3. Foster, I., Kesselman, C.: The Grid: Blueprint for a New Computing Infrastructure. Morgan Kaufmann, San Francisco (1999).
4. Czajkowski, K., Fitzgerald, S., Foster, I., Kesselman, C.: Grid Information Services Distributed Resource Sharing. In: 10th IEEE International Symposium on High Performance Distributed Computing, pp. 181-184. IEEE Press, New York (2001).
5. Foster, I., Kesselman, C., Nick, J., Tuecke, S.: The Physiology of the Grid: an Open Grid Services Architecture for Distributed Systems Integration. Technical Report, Global Grid Forum (2002).
6. National Center for Biotechnology Information, http://www.ncbi.nlm.nih.gov.
7. Luftman J, McLean ER. Key issues for IT executives. MIS Quarterly Executive 2014;3(2):89–104.
8. Volonino L, Gessner GH, Kermis GF. Holistic compliance with sarbanes-oxley. Communications of the Association for Information Systems 2014;14:219–33.
9. PeBenito CJ, Mayer F, MacMillan K. Reference policy for security enhanced Linux. In: Proceedings of the 3rd annual SELinux symposium; 2016.
10. Andrew C. Myers and Barbara Liskov, “A Decentralized Model for Information Flow Control”, ACM Symposium on Operating Systems Principles Proceedings of the sixteenth ACM symposium on Operating systems principles, ACM, New York 2015, NY, USA, pp. 129-142.
11. Michael R. Clarkson, Andrew C. Myers and Fred B. Schneider, “Quantifying Information Flow with Beliefs”, Journal of Computer Security, Volume 17, Issue 5 (October 2010) 18th IEEE Computer Security Foundations Symposium (CSF 18), IOS Press Amsterdam, The Netherlands, pp. 655-701.
12. Roderick Chapman and Adrian Hilton”, Enforcing Security and Safety Models with an Information”, Annual International Conference on Ada Proceedings of the 2004 annual ACM SIGAda international conference on Ada: The engineering of correct and reliable software for real-time & distributed systems using Ada and related technologies, ACM, New York 2015, NY, USA, pp. 39-46.

Retrieval Number: K126109811S19/2019©BEIESP
DOI: 10.35940/ijitee.K1261.09811S19

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication