Indian J.Sci.Res. 17(2): 629-633, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

AN EFFICIENT CONJUNCTIVE OPTIMIZATION ALGORITHM FORNETWORKSECURITY

S.ARCHANA[1], K.LAVANYA[2], R.ANUSHA[3]
[1,2] Department of Computer Science and Engineering, Aurora's Scientific Technological & Research Academy, Hyderabad, TS, India.
[3] Dept of Humanities and Sciences, Aurora's Scientific Technological & Research Academy, Hyderabad.

Abstract:Security is the most important issue in a network system. Administrators can more easily understand threats to the network by using a model. In this paper, we present an approach for modeling a network that considers the benefits of the network as well as its limitations. In our approach, we model the system as an optimization problem, which is solved using three algorithms. As the proposed approach is Probabilistic, it works very efficiently in a network environment. This paper, presents a mathematical model of the system. Model provides easy comprehend of system. Presented model is based on Conjunctive Optimization problem. One parameter in the presented model is security and another parameter is user productivity. Security is the most important issue in a network system. Administrators can more easily understand threats to the network by using a model. In this paper, we present an approach for modeling a network that considers the benefitsofthenetworkaswellasitslimitations.

Keywords : Modeling network security, Conjunctive Optimization approach, network system, optimization

Introduction

Amodelisatoolthatfacilitatescreatingarepresentation of the target object, thereby helping the users to understandthatobject.Amodel isnecessaryforunderstanding network systems, because these systems typically comprise many sub-systems and having knowledge aboutall sub-systemsispracticallyimpossible.Theimportanceofamodelofanetworksystemincreaseswhenconsidering security. Security is the most important issue in a networksystemandahigherdegreeofsecurityisconstantlybeingsought.Focusingonsecurity,wecandividenetwork systems into two main groups: open and closed systems. In the first group, network systems are free to join the network.Inother words,allmachinesinthenetwork can access their assets. Despite the open system, nomachine.Inthenetworkcanaccesstheassetsofaclosed system.In practice,becausethisdivisionisabsolute,manynetwork systemsfallbetweenopenandclosedsystemsinthereal world. The main goal of a security model is to represent the security level of a networksystem.Security is the generic term for a collection of techniques and tools designed to protect data and prevent counter attacks [7].our proposed algorithm together with our experimental results. Finally, our conclusions are presented in Section 4.

Security involves three aspects: confidentiality means hiding the contents of a file, integrity means detecting tampering, and availability means ensuring access to assets. All three security aspects can be applied using an authorization system. In this context, confidentiality means unauthorized disclosure of information, integrity means unauthorized modification, and availability means denial of unauthorized access to information. A security model clearly depicts the level of authorization for eachsub-system.

The major benefit of a network is user productivity. In other words, a network is created to facilitate access touser'sfavoritedataresources.Therefore,applicationof security should not be limited to user's access toassets.

Contrarily, certain constraints are applicable to an authorization system. The main constraint is an economic one. Given that the financial resources of an organization are normally limited, costs must be constrained. As such,therearetwoconflictinggoalsforsecurity(increasing authority as well as user productivity) and one constraint(theeconomicissue). Anynetworksecuritymodel must consider the goals and the constraint. In this paper, wepresentamodelbasedonevolutionaryConjunctive Optimization (ECO).

We use an evolutionary algorithm because it can adapt to the dynamic nature of a network, and Conjunctive Optimization because it allows us to optimizeanumberofconflictingobjectives.ECOallows ustooptimizeConfidentiality,Integrity,Availabilityand User Productivitysimultaneously.In HASBE [8], the user access rights were provided by the hierarchical access structure framed for each user ofthe system. This scheme ensures the property of scalability through the extension of ASBE (Attribute-Set Based Encryption) technique [6].

[1]Corresponding Author

It defines a hierarchical structure that delegates the operation of trusted authority and private key generation to the domain authorities of the lower level. Here the user attributes were converted into the stable structure of the recursive type that permits the users to de ne constraints dynamically by representing a different combination of attributes, which satisfies the user access policy. That ensures the property of flexibility and ne-grained access control over HASBE systems.The rest of this paper is organized as follows: In Section 2, we define a number of preliminaries that are needed for our proposed algorithm. We also present an overview ofrelatedresearch.InSection3,weintroducesecurity model is to represent the security**RelatedWorks:**

The evolution of the current industrial context and the increase of competition pressure, has led companies to adopt new concepts of management [4]. The implementation of the most important part of the plan phase, consisting of the definition of an appropriate global management plan QSE (Quality, Security and Environment) has been proposed [3].

This implementation is based on the multi- objective influence diagrams (MIDs).The proposed approach has three phases: Plan phase, Do phase and Check & Art phase. The first phase gathers all quality, security and an environmental objective issued from the requirements, and then analyzes them. In this phase we can define a global management QSE plan. The second phase has the input of the global management plan QSE and the corresponding global monitoring plan generated from the plan phase and will also implement the selected treatments. In the third phase, finalization of the process of integration occurs through measuring the effectiveness of different decisions. Neuberger et al. provide a structured and repeatable process that includes: defining evaluation criteria according to corporate requirements, strategy, assessing and/or refining the existing IT security infrastructure, identifying stakeholder preferences (risks, boundaries), determining the solution space of all efficient (Pareto optimal) safeguard portfolios, and inter- actively selecting the individually best safeguard portfolio.

This paper tries to combine different benefits and costs into one formula. This presents a problem because the authors do not present a Conjunctive Optimization problem. Kumar et al. focus on PGP (pretty good privacy) which was shown by Zimmerman in 1991 to provide security with available cryptographic algorithms. Algorithms are chosen according to the user requirements of time, cost and required security level. Kumar et al. answer the question: How do you choose appropriate algorithms, from the available pool, tosuit the user requirements of time, cost and security? They assign a security level to an algorithm according to its performance P. Authors of investigate security models, which consider risk assessment approaches to be applied for threat modeling, network hardening and risk analysis. Overall, security models can be classified based on the methodologies used to optimally invest into computer security.

We have specified thefollowing:

Risk assessmentmodels;

Cost-benefitmodels;

Gamemodels;

Conjunctive Optimization decision supportmodels.

Cost-benefit analysis looks into intangible costs/returns and addresses the perspective of time. The simplicityof the frameworks can give suitable investment solutions for low risk investments. However, these methods do not consider uncertainty and give misleading indications for long-term investments.

In the risk assessment involves a calculation of risk in relation to financial returns, rather than the defined risk of possible losses related to degradation of information security. They demonstrated a novel approach of selecting security countermeasures with respect to both investment cost and the risk of possible degradation of CIA. Their security countermeasure is rep- resented as a binary value. Also, they thought security solutions can be classified based on the function they pro- vide The main challenge Information System (IS) man- agers face is to strike an appropriate balance between risk exposure and the opportunity to mitigate risk through in- vestments in security. Thus, the authors of propose a decision analytical approach, but the paper does not present a formula for Conjunctive Optimization.

Service provisioning (SP) is defined as the set of interrelated decisions in order to select a service (by a server) to attend to a request (by a client). The results of the author case study provides evidence in support of the notion that the use of imitation (recall) in DPSP (dynamic provider of serviceprovision)cipherselectionprocessreducesitsover-heads dramatically. In paper the authors introduce a novel presentation for cyber security problems using the formalization of a Conjunctive Optimization Distributed Constraint Optimization Problem (MO-DCOP). An MO-DCOP is the extension of a mono-objective Distributed Constraint Optimization Problem (DCOP) which is a fundamental problem that can formalize various applications related to multi-agent cooperation. They develop a novel algorithm called Branch and Bound search algorithm (BnB) for solving a cyber security problem. This algorithm utilizes the well-known and widely used branch and bound technique and depth-first search strategy and finds all trade-off