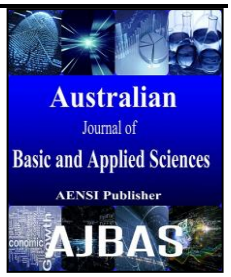
Australian Journal of Basic and Applied Sciences, 9(11) May 2015, Pages: 731-735

ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com



An Information Security Model For Air Passenger Guidance System with Byod Analysing System

[1]Vinod Duraivelu and [2]Chandrasekaran Subramaniam

[1]*Research Scholar Sathyabama, University Computer Science Engineering Chennai, India.*
[2]*Professor CSE Rangaragan Engineering College Coimbatore, India.*

ARTICLE INFO

Article history:
Received 12 March 2015
Accepted 28 April 2015
Available online 1 June 2015

Keywords:
Trust value; suspicion stack; context aware;
standard deontic logic; reputation

ABSTRACT

The objective of the research work is to propose a Predictable Context Aware Trust (PCAT) model for achieving organization security in the presence of suspicious entities and authorities. The properties of the PCAT model are including the suspicion stack pertaining to the members in various contexts. The reputation rewarded based on the contexts in which the exchange is done. The proposed trust model encompasses the trust level of the members, degree of suspicion in the information, the levels of privacy and reputation values of the trustees and their trust relationships to predict organization security. A conceptual and hierarchical trust pyramid is considered at different context levels and the formal implications are derived using context sensitive standard deontic logic. The formal specifications of a passport checking sub system are given in Temporal Logic of Actions (TLA) from which the certificate authorities and trustees are evaluated in an airway passenger guidance system. According to the BYOD concept logics has been established with air passenger system.

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: Vinod Duraivelu and Chandrasekaran Subramaniam., An Information Security Model For Air Passenger Guidance System with Byod Analysing System. ***Aust. J. Basic & Appl. Sci.,*** *9(11): 731-735, 2015*

INTRODUCTION

In any organization that demands a highly secured information system, the members in various capacity levels as per the hierarchy within or outside the organization are allowed to interact under different contexts based on their trusted and suspicious behaviour. In one such context, namely the information exchange context, their interactions may be between the members that result in the expected outcome only when the trust values of the involved entities are well within the permissible values. This exchange requires a secure and a threat free trust model under various levels of suspicion. Trust is a particular value of subjective probability with which a member determines another member's behaviour or performance of a particular action in a particular context (Gambetta, D., 1988). A trust model is a collection of rules that helps to decide the legitimacy of trust attributes or trust certificates. Trust is not only subjective, but also context dependent because the trust of one entity on another entity varies from one context to another. For a dynamic system, trust has to be predicted and managed efficiently along with consideration for trust levels in the future. The recommendation based trust model deals with the direct trust based on reputation of the trustee which is given by a feedback. In this model, there are possibilities of deceptive recommendations which increase model's susceptibility to attacks. In the evidential trust model (Sabater, J., C. Sierra, 2001), the trust calculation provides reasoning about the future interaction, but the essential security in the presence of attacks is not considered. The earlier Context Aware Trust model which is based on interaction between entities evaluates the direct trust associated with an entity based on the outcome of the interactions (Mohammad Gias Uddin, 2008). A well defined formulae or some logic of permissible implications should be applied to determine the rights associated with each entity to move on to next higher trust level. These rules are specified using standard deontic logic (McNamara, Paul, 2009) which deals with obligation, permission and related concepts. In case of Trust Management systems the permissibility or authorization problem is expressed in terms of finding a proof of a particular formula representing successful interaction, with collection of suitable logic (Peter, C., 2008). But in some scenarios when there are no frequent interactions between the entities, the trust value of an entity may tend to remain the same. Also it does not consider the suspicion values for the entities. All the earlier trust

Corresponding Author: Vinod Duraivelu, Research Scholar Sathyabama, University Computer Science Engineering Chennai, India.

models addressed the issue of context-dependency of trust during interactions but did not incorporate the logic or mechanisms to evaluate trust by accounting the suspicion levels the trust actors might be subjected to. The context implies how and why the members trust the information that is given to them (Trbovich, P.L., A.S. Patrick, 2004). In this paper, a Predictable Context Aware Trust model called PCAT has been proposed. This trust model identifies suspicion values of the trust members in each and every context using a suspicion stack. The constraints should be considered so as to determine which entities have the right to communicate to whom and when to communicate The PCAT model is applied to an airway passenger guidance system where the specifications for the passport checking subsystem are formally specified using Temporal Logic of Actions(TLA) language.

Suspicion Stack:

The four different stacks based on the contexts are as follows: (i) Entity Information Suspicion (EIS) stack (ii) Task Suspicion (TS) stack (iii) Process Suspicion (PS) stack (iv) Attack Suspicion (AS) stack. Based on the various contexts explained above, the corresponding suspicion level in the respective suspicion stack is checked and then trust value is predicted. If the suspicion value in the stack changes from high to low, then the trust value increases else if it changes from low to high, then the trust value decreases. In this manner, trust value can be predicted for any member. An instance of the suspicion stack in four contexts is illustrated in figure 1.

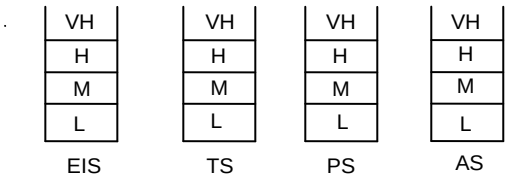


Fig. 1: Various Context Suspicion Stacks.

In the proposed model when an External Attack Context is considered, unreliable entities or tasks or processes can be eliminated. Also reputation has been given a significant role because the previous suspicion values for any context can be determined or made available using the suspicion stacks. In the lowest level of the trust model, the incoming items may be considered as the symbols in the tape of a turing machine. As the details are passed through the input tape, the corresponding context suspicion stack is checked. Only if the top value of the stack is an acceptable value; trust is assigned to that member.

Similarly consider the trust level for a member to be T_{ij} where i= {0, 1, 2} at a given context C_j and let the j^{th} context's stack top value to be ST.

Let the only acceptable suspicion value on the top of the stack be L upon which the trust value can be assigned to an item and then allowed to move to the next trust level(T_{j+1}).

This implication can be represented as

$(T_{ij}, C_j, ST) \rightarrow T_{(i+1)j}$, where j={e, t, p, a}; i={0,1,2}

Consider an input entity from an entity set {E} at the trust level T_{1e} with the suspicion value at top of stack as VH (Very High), then its transition(δ), can be represented as

$\delta (T_{1j}, \{E\}, VH) \rightarrow (T_{0j,} \varepsilon)$ where j={e, t, p, a}

When the Top value of the stack is VH, the stack top value is removed. This removing of the stack value is represented as ε. The trust level of an entity decreases to T_{0j} since it has a suspicion value of VH. For an entity {E} with the stack top appears to be at H(High),its transition can be represented as

$\delta (T_{1j}, \{E\}, H) \rightarrow (T_{0j,} \varepsilon)$

Similarly, for the entity from entity set {E} with the stack top value as M (Medium), the transition can be represented as

$\delta (T_{1j}, \{E\}, M) \rightarrow (T_{0j,} \varepsilon)$

When the entity enters, the suspicion stack is checked and if the stack top value is L (Low) which is the permissible value for a member, the entity is allowed to move to the next trust level. This transition can be represented as

$\delta (T_{1j}, \{E\}, L) \rightarrow (T_{2j,} L)$

The evaluation of trustworthiness is based on two relationships between recommendations and context. In the first case it is a reputation based on the initial trust value and the second one is context dependent [9]. For example, if a passenger who has no previous relationship with any of the entities like authority, the ITV for the context free trust or the general trust (50%) and based upon the context with which the journey is undertaken, will be fixed. In the case of a normal situation, the context aware trust varies according to the degree of importance. For a normal situation the degree of importance is 25 %, for a conference it is 50%, in case of international trading and affairs it is 75 % and for epidemics or any national alerts the ITV will be taken to be 100%. The degree of importance in assigning ITV is reflected in the weightage factor mentioned in the model.

Let the initial trust value (ITV) for various contexts are represented as T_{0e}, T_{0t}, T_{0p},T_{0a}. The trust of an entity with its initial trust valueT_{0e} at Information Exchange Context (IEC) can be predicted as in (1).

$\text{Trust@ IEC} = [T_{0e} + 1 - p(s)]$ (1)

Similarly equations (2), (3), (4) predict the trust values at the Internal Task Context, Internal Process Context, External Attack Context with initial trust values T_{0t}, T_{0a}, T_{0p} respectively.

$\text{Trust@ ITC} = [T_{0t} + 1 - p(s)]$ (2)

$\text{Trust@ IPC} = [T_{0p} + 1 - p(s)]$ (3)

$\text{Trust@ EAC} = [T_{0a} + 1 - p(s)]$ (4)

Information security model for BYOD:

Security manager is responsible for developing, maintaining, monitoring, compliance of all information security policy and procedures. Performs security tests and Manages internal audits on information security process controls. It compares the IP address and return address of the requesting domain. If it matches, then they are allowed to enter into the organization or else they are blocked at the initial stage itself. It raises awareness about the information security issues, promotes safe computing and manages disaster recovery and business continuity activities. It provides coordination in the development of policies standards and access control for the safeguards of the organization information assets.

It ensures confidentiality, integrity and availability. It also leads the information security, incident response (IRT), conducts security awareness session for department of organization. The business loss and the reputation damage are very high in the case of illegal document release and untimed release of legal evidences through networking. In all these scenarios, the computational structure of the information is the most important criteria in managing the security activities. Hence the structure of information can be represented as a tuple of <*Identity of Info, Uniqueness, Location, Size* > where the identity is a kind of token or a valid keyword pertaining to the business. For illustration, the identity can be expressed as a name or a type or an instance and as a parameter that is hidden or explicit. The uniqueness of the structure can be expressed as a member in the set of {*Context, Content, Pixel, and Mixed*}.Similarly the location feature of the information asset or its cyber markup can be expressed as a member in the set of {*User Defined, Static, Dynamic, and Random*}. The information size which plays a vital role in the end user transaction as the raw information which may be of types belonging to a set of elements like {*Computational, Application, Duration, Resolution*}, For example, the structuredness of a design data from a product center is very well represented by its identity name or number and its data type with all its related names or fields mentioned explicitly or implicit in the information exchange. Risk identifier classifies the different levels of risk. It estimates the loss, when the asset gets attacked. The below flowchart guides the process of deciding how to proceed after the information is designed. Check whether the protected system has vulnerabilities that can be exploited.

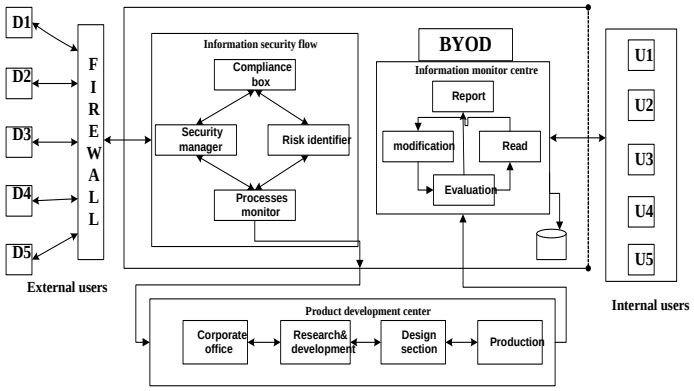


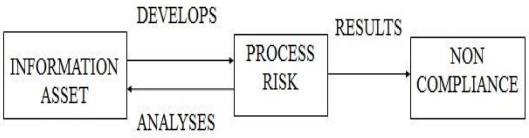
Fig. 2: Information security flow management for product development center.

If the answer is yes, and a viable threat exists, begin to examine what the attacker would gain from a successful attack. To determine if the risk is acceptable or not, estimate the expected loss the organization will incur if the risk is exploited. Process monitor is used for monitoring the overall process of the organization. It monitors and reports if any abnormal behavior occurs. It makes decision (i.e.) mitigating risk in a processes flow for every access from an external user. The accesses by the internal users are monitored continuously. In case of any modification, they are evaluated and reported to the concerned authorities. Modified users will be trigged based on the system log maintained through the monitor centre. It is a method that helps in preventing the original document of the organization form the attack. In case of any change or modification, only the duplicate copy of the document is created and modification is done. It contains details of the person who performs modification like IP address, time, date, etc. The organization allows appending the data, only if it is valid.

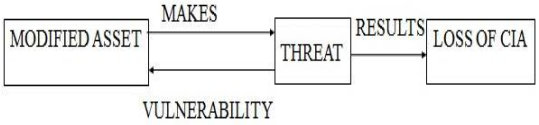
Information risk analysis module:

The information security governance module (ISG) indicates the objectives and operations about the security incidents that had happened or may happen inside or outside the organization. The focus of governance is to identify the various risk and security compliance (ISC) in different directions and dimensions so as to take decisions that defines the expectations to grant the regulation processes. The information security risk (ISR) analysis based on the business processes is configured not only to regulate the processes but also report the necessary updates.

Interface 1: Interface (process risk & noncompliance):



Interface 2: Interface (threat & CIA):



Interface 3: Interface (process risk):

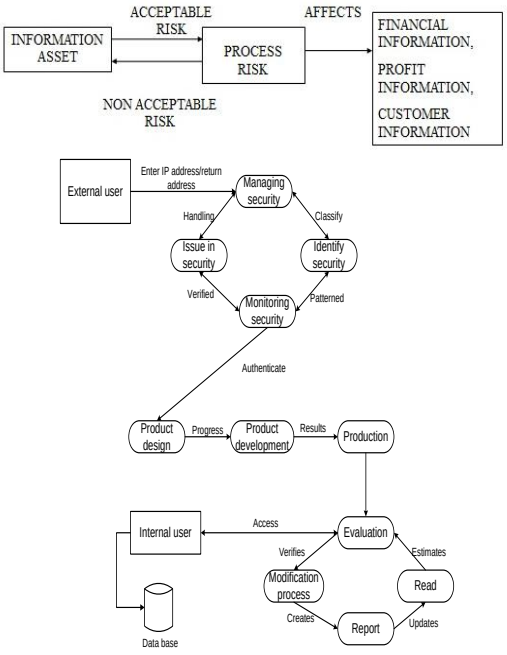


Fig. 3: Information security process flow model.

The above interfaces process through an information security assets which develops process risk that results in non compliance in interface 1,while the other interface process through modified asset which results threat and leads in confidentiality , integrity and authorization in interface2.The interface makes a sensible information assets in interface 3 which brings non acceptable risk that leads in organisations information failure. In order to archive certain information assurance the information flow process has been adopted with external and internal process with monitoring product design in fig 3.

Case Study: An Airway Passenger Guidance System:

The proposed Predictable Context Aware Trust (PCAT) Model has been applied to Airway Passenger Guidance System where interactions are allowed between the passenger and the various authorities based on the trust certificates and the suspicion levels at each context. The various authorities include Passport check Authority, (PCC) Passport Issue Authority (PIA), Ticket Check Authority (TCA), Ticket Issue Authority (TIA), Custom Check Authority (CCA), Immigration Authority (IMA) and the Chief Airport Authority (CAA). The various trust certificates include the Passport Checked Certificate (PCC), Ticket Checked Certificate (TCC) and Immigration Checked Certificate (ICC). At each context, the various trust certificates are checked and only if there is no suspicion (i.e.) if the certificate is valid, the passenger can move to the next level in the system. Standard deontic logic is used to specify the appropriate conditions for trust to be assigned to a passenger to move on to next level in the system. This is given using a trust pyramid which specifies the various trust levels and certificates.

At the first level in the trust pyramid as shown in Fig. 2, the passenger submits the various passenger details to the Passport Checking Authority for verification. The PCA has to ensure that the certificate issued by the PIA is valid. The PIA is checked and PCC is issued which along with the passport details passes on to the TCA. The TCA

verifies the ticket details (TD) and then issues the TCC. Similarly the trust certificates are checked in the other higher levels based on the suspicion values and the trustworthiness of an entity is determined. In this manner the trust for the entire organization can be established and managed. Consider the interactions in the Information Exchange Context where the passport details of the passenger are checked. As each detail is verified, the top value of the context suspicion stack should be checked for a low value to ensure a trusted interaction between the members involved. In the illustrated scenario, the passenger is guided by an airway guidance system at the airport. Initially the passenger encounters the passport verification authority and has to submit the needed details to the checking authority. The passengers submit each of the passport details like the passport number, the expiry date of the passport, the code number of the passenger, the passenger's name to the checking authority. When the passenger details are checked, the contents of the suspicion stack are also checked to see if the stack top points to Low.

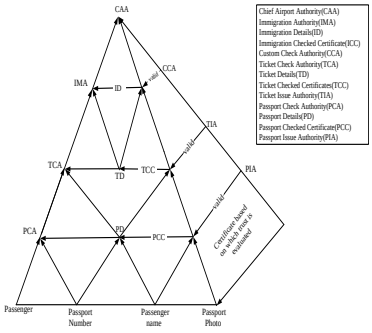


Fig. 4: Airway Passenger Trust Levels and Certificates.

Conclusions:

In the proposed model, the trust value of an organization is predicted based on the contexts in which its internal and external actors with their various capacity levels are interacting .The trust level and the trust entities in various levels are represented as a trust pyramid. The concept of a suspicion stack is introduced whose elements are the values of suspicion due to misbehavior within the organization and the trust is managed using the standard deontic logic. The context aware trust is determined by considering the previous trust value and the weightage of the capacity level of the member or entity. Through the formal specifications of an airway passenger guidance system, a scenario is considered in which a passenger is allowed to proceed to the next level of checking only after being certified by the authorities with respect to the trusted certificates.

The various levels like passport check, ticket check and immigration check in the airport organization are considered to validate the model. The logic and the reputation based trust can also be determined in the contexts of internal process and external attack using the PCAT model. The effectiveness of the model lies in the fact that the suspicion stack is trusted to predict the trust values for the members and entities in an organization .The accuracy of the prediction improves as the height of the pyramid or in other words the number of capacity levels increases. When a new member or entity is introduced in to the organization or if the organization policy is revised, the new trust logic has to be applied.

REFERENCES

Gambetta, D., 1988. Can we trust trust? in Trust: Making and Breaking Cooperative Relations, Gambetta, D. (ed.), Chapter 13. University of Oxford: 213–237.

Sabater, J., C. Sierra, 2001. REGRET: A reputation model for gregarious societies. In: Proc of the 4th workshop on deception fraud and trust in agent societies, Montreal, Canada, 61-70.

Mohammad Gias Uddin, Mohammad Zulkerninem, Sheikh Iqbal Ahamed, 2008. CAT: A Context Aware Trust Model for Open and Dynamic Systems. In: Proc of the 2008 ACM symposium on Applied computing, Fortaleza, Ceara, Brazil. ACM Press: 2024–2029.

McNamara, Paul, 2009. "Standard deontic Logic", The Stanford Encyclopedia of Philosophy (Spring Edition), Edward N. Zalta (ed.), http://plato.stanford.edu/archives/spr2009/entries/lol og-standard deontic/

Peter, C., Chapin, Christian Skalka and Sean Wang, 2008. Authorization in trust management: Features and foundations.In: ACM Computing Surveys, 40(3): Article, 9.

Trbovich, P.L., A.S. Patrick, 2004. The impact of context upon trust formation in ambient societies. Position paper presented at the CHI. Workshop on Considering Trust in Ambient Societies, 26. Vienna, Austria.

Jianqiang Shi *et al*., A Trust Model with statistical foundation.