Architecting Digital Signature/ PKI based Secure Web Based Systems Through 3-D Probabilistic Software Stability Model (PSSM)

Eugene Xavier. P.[†] **and Naganathan.E.R.**[††],

[†] Research Scholar, Dept of CSE, Alagappa University, Karaikudi, India – 630 003.
†† Professor and Head, Dept. of Computer Applications, Velammal Engineering College, Chennai, India – 600 066

Summary
With advancements in the design of Software Systems, it has become necessary to think in terms of providing security to Software Systems using advanced security standards and protocols. There are advanced and widely accepted techniques used in securing web based banking software systems such as Public Key Cryptosystem (PKI), digital signatures etc. While designing such high-secure banking web applications, the methods of ascertaining and ensuring stability of such systems have always been quite challenging. We have applied the concept of 3-D Probabilistic Software Stability Model (PSSM), essentially by defining the Enduring Business Themes (EBTs), Business Objects (BOs) and Industrial Objects (IOs) to analyze the stability of the PKI/ Digital Signature based Banking (web) applications. Due to the instability of Web based Systems produced over a period of time unlike other systems, it has become essential to research upon and ascertain the stability of Web based Systems. Though theoretically there is no deterioration expected for a software product, it does owing to changes in software which involves re-engineering of the changed code. The re-engineering of the software product is not essential for small changes that would have been made in the code of the software modules. We have taken into consideration the various aspects such as analysis, design, development and tried to analyse the design aspects of Secure Web Based Systems making use of the Probabilistic Software
Stability Model (PSSM). Identifying the design pattern for a domain using Probabilistic Software Stability Model (PSSM) helps one make apply the design pattern for a different application/problem in the same domain. This has been demonstrated through the design pattern arrived at for PKI/DS based E-Banking Systems (EBS). This research work essentially integrates Secure Web based systems development with Software Stability Theory that will provide lot more stabilization of the Secure Web based Systems.

Keywords:
Public Key Infrastructure (PKI), Digital Signature(DS), Access Control System (ACS), Enduring Business Theme (EBT), Business Objects, Industrial Object (IO), Authentication, Authorization, Security Control Elements (SCE), Function Points (FP).

1. Introduction

Security is a key factor in most of the systems used widely in day to day life. This includes Drink vending machines, Automated Teller Machines, Gambling machines and various other security systems. This paper discusses the applications; in particular DS/PKI based E-Banking System which deal with the problem pertaining to accessing entities, objects and resources with pre-defined access policies and procedures.

Most of the real time applications and systems are facing this problem very often, therefore we have attempted to build a general Framework for all existing and future systems in the above mentioned categories. There are two design approaches considered newly viz., (a) Modeling the E-Banking System (EBS) as a control system, so we apply physical system stability analysis (b) Designing the E-Banking System using Probabilistic Software Stability Model (PSSM) as in [5]. Approach (a) discussed in [ ] tends to make use of the concepts derived out of physical system stability concepts viz., Controllability and Observability of the system. Approach (b) makes use of the EBT/BO/IO based patterns modeled using Probabilistic methods.

Architecting the EBS involves the following steps:

A real time online E-Banking System referred to hereafter as EBS is required to inherit basic security elements viz., *Confidentiality, Integrity, Authentication, Authorization and Non-Repudiation.*

(a) The methodology used to identify the properties / security elements is obtained by constructing a DS/PKI based EBS

(b) EBTs/BOs/IOs are identified based on the Software Stability Model (SSM) as described in M.E.Fayad's work in [1,2].

(c) Design Patterns could be obtained from the EBTs'BOs/IOs identified for the DS/PKI based EBS.

(d) PSSM as defined in [5] has been utilized to architect the EBS so as to make inherit the basic security elements / properties viz., Confidentiality, Integrity, authentication, authorization and Non-repudiation.

(e) The correlation which exists between EBTs/BOs/IOs in Design Domain to Function Points (FPs) in Development Domain of EBS is identified through

Manuscript received September 5, 2010
Manuscript revised September 20, 2010

PSSM in order to make the five basic security elements to be inherited by EBS.

(f) Stochastic / Random Process (RP) based is used to make the DS/PKI based EBS to acquire the five basic security elements.

(g) The EBS architecture developed by applying PSSM approach has been explained in the paper. This is the contribution of authors to literature.

(h) There are a few basic questions addressed in this paper viz.,

a) Does the security control system of EBS which is assumed to be Open Loop stable render the Closed Loop System with DS/PKI elements also stable?
b) Has the Software developed using PSSM approach fulfill the given specifications to be met by a generic Access Control System (ACS) / E-Banking System (EBS).

1.1 Private/Public Key Cryptosystems

1.1.1 Private Key Cryptography

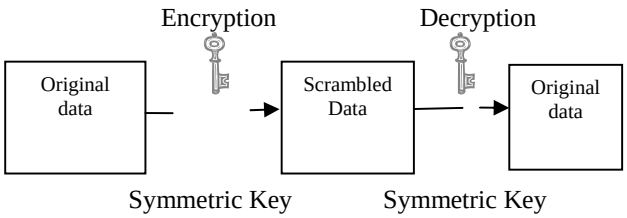


Fig 1. Private Key Cryptosystem

The heart of the EBS is securing the online transactions. Cryptography becomes inevitable when it comes to providing security to the EBS. In private key (secret key) cryptography, a single key is shared by the users involved in the Transaction. The risk involved in Private Key Cryptosystem is high compared to that of others since once the secret key is compromised, the secret information becomes public. In order to do away with this problem, Public Key Cryptosystem has come into play.

1.1.2 Public Key Cryptography

Encryption and DecrypPublic key cryptosystems makes use two kinds of keys viz., public key and private key. The public key is shared with everyone, while the private key is maintained by the owner only. Encryption of message text is first done by the public key. Decryption of the cipher text is done by the private key. This gains the original data

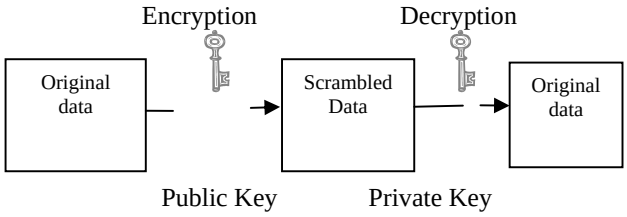


Fig 2. Public Key Cryptosystem

(message text) whereby allowing only the actual owner to recover the data which ensures confidentiality of the data which is shown as below. Data is represented by XYZ.

$$XYZ = \text{Decrypt}_{\text{PrivateKey}}(\text{Encrypt}_{\text{PublicKey}}(XYZ))$$

Performing encryption using the private key followed by decryption by using public key allows us to retrieve the data XYZ, which is widely used concept in Message Digest / Digital Signature.

$$XYZ = \text{Decrypt}_{\text{PublicKey}}(\text{Encrypt}_{\text{PrivateKey}}(XYZ))$$

1.2 Public Key Infrastructure (PKI) Components

PKI primarily consists of a Directory Server, Certificate Server and Key Recovery Server. The Directory Server is used to maintain user specific information. The primary role of the Certificate server is to issue, manage, and revoke certificates. The Key Recovery Server provides support to backup and recover the keys used for encryption/decryption. The PKI clients have a web server, browser, email and file type applications.

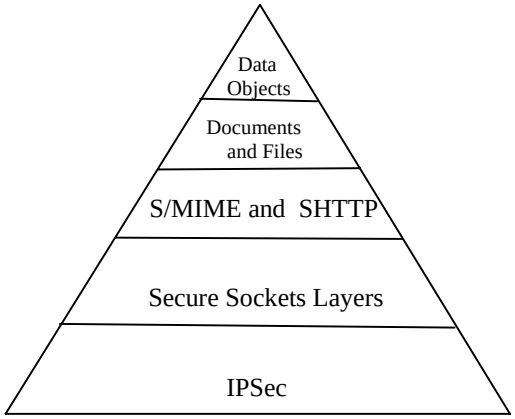


Fig 3. PKI Architectural Model

The major building blocks of PKI are – Encryption Algorithms, Private and Public Key Pairs, Digital Signatures, Digital Certificates and Certificate Authorities. A Digital Signature is a unique electronic signature which cannot be denied / refuted and which is not possible to

copy and transfer from one location to the other. Digital Certificate comprises of Public key, digital signature, identity of the owner, identification number, issuer of the certificate and period of validity. Certificate Authorities (CAs) issue the digital certificates who are considered to be trusted third party in E-banking Online Transactions.
Fig 3 shows the various security layers which are being made use of in issuing and managing Certificates in the PKI Architecture. There are various applications of PKI viz., Virtual Private Networks (VPN), E-mail, Smart Cards, Internet Telephony, Home Banking and Insurance.

1.3 Digital Signature in E-banking

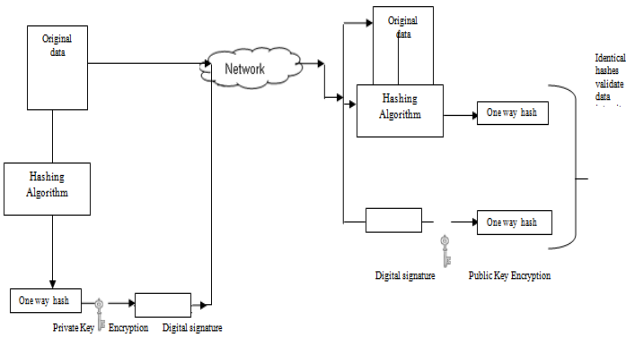


Fig 4. Digital Signature Scheme

In generic E-Commerce applications and web transactions, Digital Signatures play a vital role. Tampering and Impersonation are the two problems being addressed by Digital Signatures. A one-way hash function is used in obtaining digital signatures. The value obtained for the hash is unique for the hashed data. A different value results if there is any tampering of data done. Fig 4 explains clearly the Digital Signature scheme which is self-explanatory.

1.4 DS/PKI based secure online E-Banking System (EBS)

The E-Banking System (EBS) is modeled as a Control system as shown in Fig 5. The main aim of the model is to provide security to the E-Banking System. Access Control System (ACS) provides the fundamental level of security required for EBS. Digital Signature based PKI system provides the additional level of security. Owing to this reason, the ACS and DS/PKI elements are shown as control elements in the proposed E-Banking Control Model (EBCM)., which is also referred to as the canonical form of E-Banking Control system. The EBS shown in fig 5 is a closed loop control model. There are various control parameters identified in the prosposed model. The *optimal control* of the parameters used in the *E-Banking Control Model* utilizing the already established PSSM forms the subject matter of this research paper.

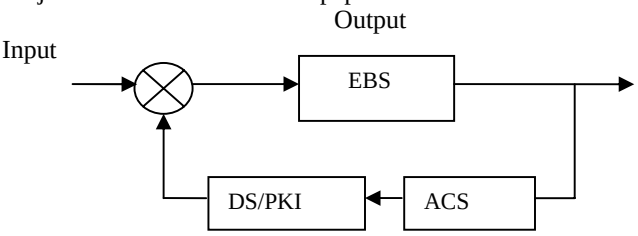


Fig 5. E-Banking Control System Model

2. Stability Models for Software

2.1 Software Stability Model (SSM)

Prof M.E. Fayad has defined EBTs/ BOs/ IOs in the SSM: The EBTs are derived by determining: “What is this system for?”, the BOs are derived by determining: “How do the intangible conceptual themes map into more concrete objects?” The IOs are derived by determining: “What is the physical representation of the BOs?” [4].

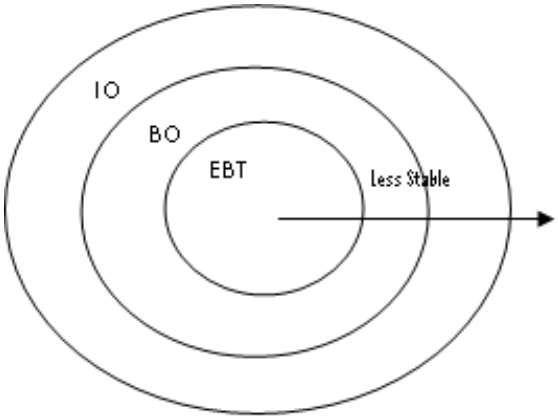


Fig 6. Software Stability Model

Enduring Business Themes (EBTs) tend to be fixed for a given system. EBTs of a system under consideration are so derived that the objects will remain stable in order to obtain a stable software system ultimately. Business Objects (BOs) also remain stable, but the internal processes might sometimes change based on the need to do so. Externally BOs will be as stable as EBTs. Industrial Objects (IOs) are the objects which are physical as in a classical object model. Stability over time, Adaptability, Essentiality, Intuition, Explicitness, Commonality to the domain, Tangibility etc are the identification criteria M.E. Fayad has suggested to identify the EBT/BO/IO [6,7].

2.2 2-D Probabilistic Software Stability Model (PSSM) [5]

PSSM has been discussed in literature [5]. Given a SDLC Process X(t,s), the probability of a system remaining stable is given by the Poisson process

$$P(X = x) = \frac{(e^{-}\lambda)(\lambda^{x})}{x!}$$

We have a fundamental fact: "higher the complexity of Software, lower is its stability".

$$Complexity of Software(C) \alpha \frac{1}{Stability of Software(S)}$$

The Software Code / Design depend on the methodology followed to select appropriate EBTs/BOs/IOs. The Data Model obtained during the Design Phase depends on the EBTs/BOs /IOs. Design is controlled by the Function Points. The method followed in distribution of the function points across the EBT/BO/IO domain, determines the stability [5].

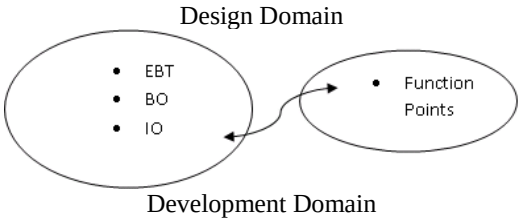


Fig 7. Domain Mapping (2-D)

By defining the probabilities of FPs producing EBT/BO/IO based on the association of the "Design Domain" to the "Development Domain", the "Inverse Square Law of Stability of Software systems" which is otherwise called the "Asymptotic Software Stability Criterion" for Software Systems (proof omitted here) is given below:

$$k^2 = (1/T)$$

where T represents the period of productivity of the software and k represents the Gain factor of the software control system. This has been derived in [5].

3. PSSM for DS/PKI based EBS

3.1 3-D PSSM for real-time E-Banking System (EBS)

2-D PSSM comprising of design domain and development domain are extended to security control domain giving a 3-D PSSM.

The probability values defined by p_{ebt} , p_{bo} *and* p_{io} for the mapping of Security Control Elements (SCEs) in *Security Control Domain* to the EBTs/BOs/IOs in the *design domain* determine the stability of EBS referring to Fig 8. The probability approach used here has enabled designers to get the needed level of stability since EBTs/BOs/IOs decide the *Stability factor* of the software system designed for EBS. The probability values p_{fp} which define the mapping of EBTs/BOs/IOs in *design domain* to their respective FPs in *development domain* determines the *ease of use* of the software system.

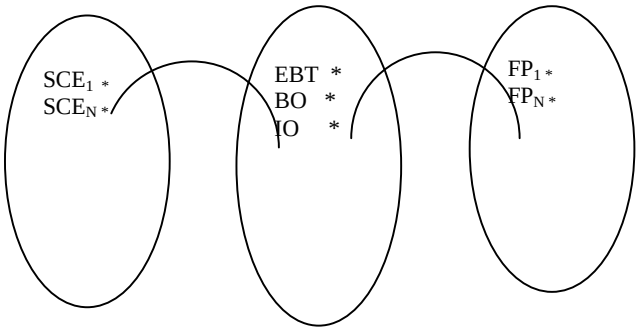


Figure 8. EBS Domain Mapping (3-D)

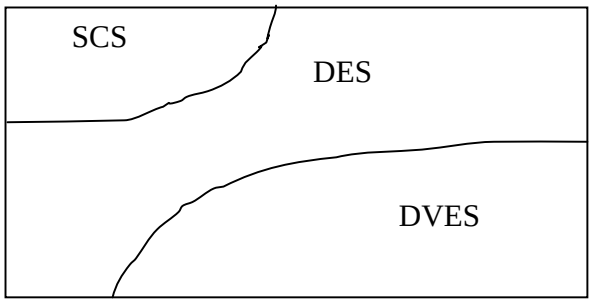


Fig 9. Security Control Element (SCE) Probability Space

The correlation of the SCEs in Security Control Space (SCS) with the EBTs/BOs/IOs in the Design Element Space (DES) is derived using Random Process approach. The cross-correlation of XSCS and YDES given by

$$Rxy(t, t+T') = E[Xscs(t)Ydes(t, t+T')]$$

since time is an essential factor in online transactions in E-banking systems (EBS).

Here E[.] represents the expected value of the product of the two Random Processes XSCS and YDES.
Hence we have

$$Rxy(t, t+T') = \sum_{t=0}^{t=N} Xscs(t)Ydes(t, t+T)$$

Assuming N number of FPs and EBTs, the cross-correlation between the EBTs/BOs/IOs in the DES domain with FPs in the DVES domain is given by

$$Ryz(t, t+T) = \sum_{t=0}^{t=N} Ydes(t)Zdves(t+T)$$

Correlation function values are calculated from observed values of XSCS, YDES and ZDVES. Deviation of Security Control (SC) parameters is indicated by Cross-correlation.

3.2 Architecting real-time EBS through 3-D PSSM

3.2.1 Identification of EBTs/BOs/IOs in EBS

The various EBTs/BOs/IOs have been obtained for EBS. The grouping of the EBTs/BOs/IOs are done based on the level of stability. Security control is provided to the E-banking systems. This is achieved by identifying different EBTs as given below:

Authentication is an Enduring Theme since it remains stable externally and internally as long as the system exists.

Authorisation is an Enduring Theme that represents the access control being provided to the E-banking system.

Confidentiality is an Enduring Theme that ensures that the information in the E-banking system is not disclosed to unauthorized users.

Integrity is another Enduring Theme which ensures that there is no modification being made to the data during transit, on the network or elsewhere.

Non-repudiation is an Enduring Theme that ensures that no one can deny their roles in a typical banking transaction.

Encryption Techniques address the problem that arises due to *eavesdropping* whereas *Digital Signature* addresses the problems of *Tampering* and *Impersonation.*

There are two Business Objects (BOs) identified viz., Access Control System (ACS) Element parameters and DS/PKI Element parameters. Every BO identified here are

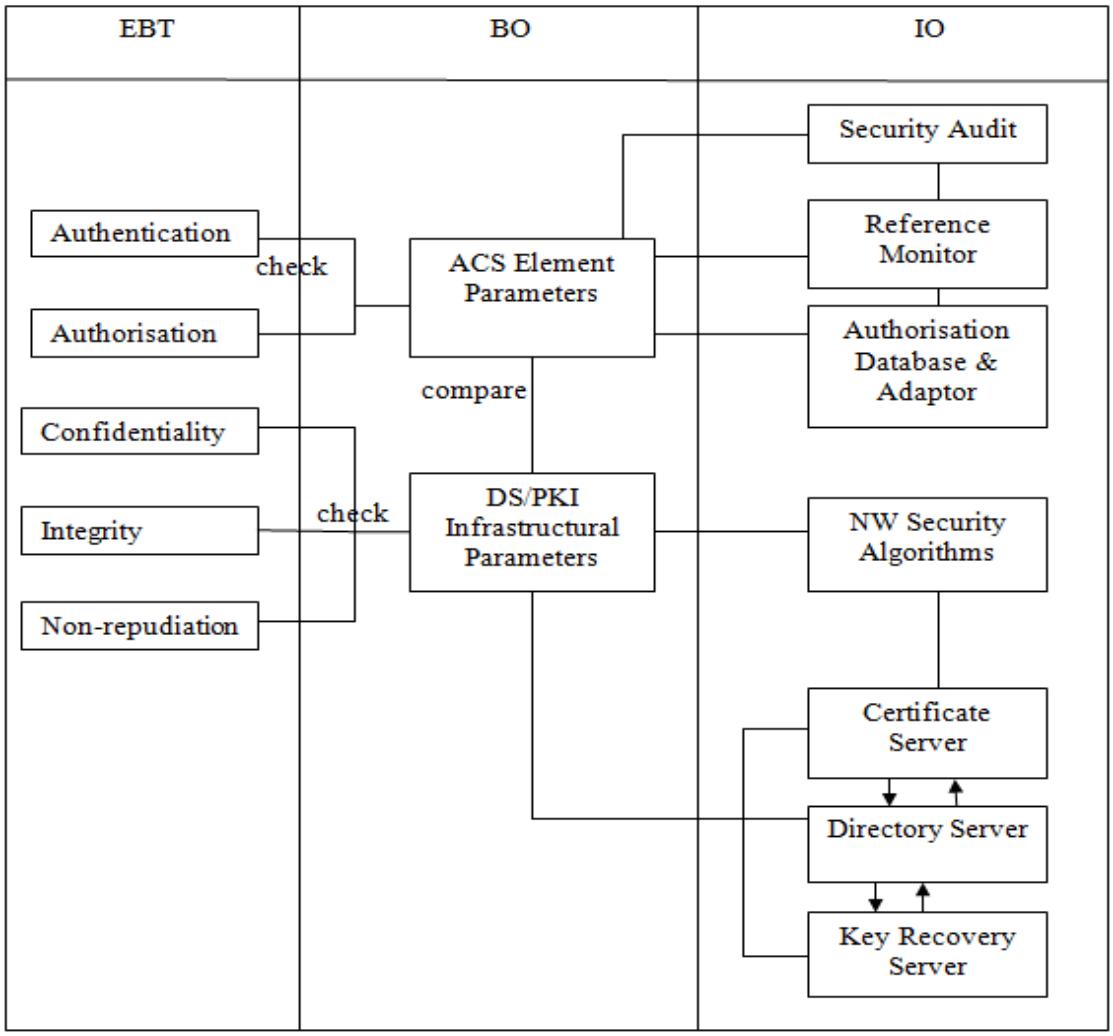
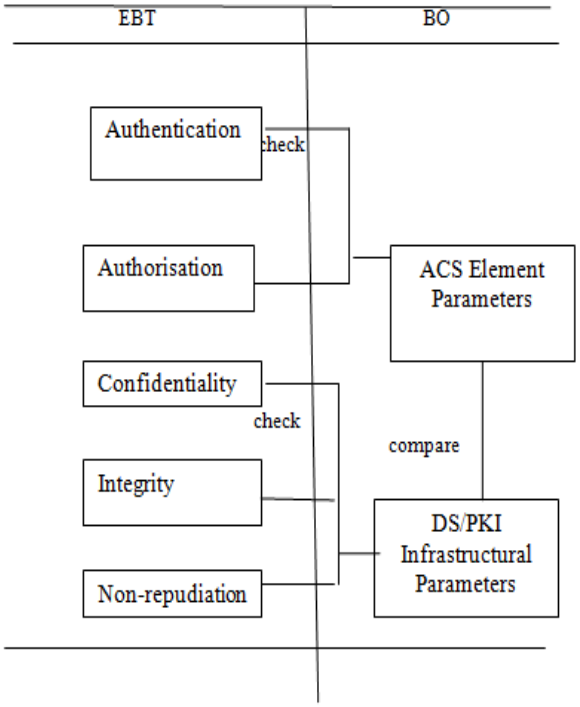


Fig 10 PSSM for EBS

externally stable and highly adaptable internally. For example, the ACS is an key element which is stable for the E-banking system yet can depend on various IOs such as Reference Monitors, Audit Elements, Authorization database, Adaptors etc.

Fig 10 shows the stable model of a DS/PKI based EBS. A domain pattern is derived for the E-banking system based on 3-D PSSM by extracting the EBTs/BOs of the stable EBS. The PSSM for any other application in the EBS will



have these objects as their EBTs and BOs.

Fig 11 EBS Design Pattern

Fig 11 shows a domain pattern for EBS. This has relationship with the FPs in the development domain.

3.3 Design Pattern Identification in EBS

The various elements of PSSM used in EBS have been discussed here.

Intent: This EBS pattern suggests the basic structure of EBS.

Context: There are many industry/domain applications that need EBS.

Problem: To obtain the stable objects which signify the basic structure of EBS.

Forces: The pattern that is obtained has to signify the basic structure of the system.

Participants:

Authentication: Represents the enduring concept of identifying and ensuring the right person of the transaction.

Authorisation: Represents the enduring concept of not allowing unauthorized users.

Confidentiality: Represents the enduring concept of not disclosing the information to unauthorized users.

Integrity: Represents the enduring concept of checking for the correctness of data.

Non-repudiation: Represents the enduring concept of defining and not allowing users to revoke their roles in a transaction.

3.4 Linkage of Controllability/Observability to EBT/BO/IO – A PSSM approach in EBS

Controllability as applied to EBS:

An E-Banking System (EBS) is said to be *"Controllable"* if it can be driven by a model in a desired direction. This is defined in the PSSM in [5].

Observability as applied to EBS:

An EBS is said to be *"Observable"* if it is possible to get correct values about the state of the system at any point of time with a closed loop EBS with ACS and DS/PKI based system as an EBS and is driven by the same model in the desired direction.

The controllability of EBS depends on the fact how far the EBS is functionally dependent on input variables. Similarly the Observability of EBS is determined by the fact how far the output variables determine the observability of EBS.

The BOs defined based on Security Control Elements (SCEs) finally determines the EBTs in the Security Control Domain which in turn controls the EBTs in the Design Domain which turn controls the FPs in the Development Domain.

4. Conclusion

The importance lies in linking the Security Aspects to Software Systems with Control Engineering concepts, which is the value addition we have brought out through this work. The software stability analysis done through PSSM provided an opportunity to identifying the Stable Design Patterns which could be reused in other similar systems like Drink vending machines, Automated Teller Machines, Gambling machines etc which also lie in the same security domain. There is a new direction set while designing EBS using Control Engineering and Software Engineering Approaches utilizing the concepts of Controllability/Observability and Design Patterns making use of the already established core PSSM through the use of Random Processes based Correlation Functions.

Acknowledgements

The authors convey their heartfelt thanks to Prof M E Fayad who is the inspiration for them to initiate the research in Software Stability and attaining a new model - PSSM. They also profusely thank all the contributors to this research project and the reviewers who provided very valuable feedback for the revision of this paper.

References

[1] Ahmed Mahdy and Mohamed E.Fayad. "A Software Stability Model Pattern", found online at http:// www.hillside.net/plop/plop2002/final/StabilityPatternPLoP02Correct.pdf

[2] Mohamed Fayad, "Accomplishing Software Stability" (Thinking Objectively) found online at http://www.engr.sjsu.edu/fayad/workshops/iri03/col2-fayad.pdf

[3] Naganathan.E.R, Eugene X.P,"Software Stability Model (SSM) for Building Reliable Real Time Computing Systems", Third IEEE Conference - SSIRI,8-10 July 2009, Shanghai

[4] Ahmed M Mahdy, Haitham S Hamza, M E Fayad, Marshall Cline,"Identifying Domain Patterns using Software Stability", IEEE Digital Library, Downloaded on 31 Dec, 2008 found online at http://ieeexplore.ieee.org/iel5/9790/30875/01431430.pdf

[5] Naganathan.E.R, Eugene X.P,"Productivity Improvement in Software Projects using 2-Dimensional Probabilistic Software Stability Model (PSSM)", ACM SIGSOFT, Software Engineering Notes, Sep 2009.

[6] Yan Liu et al., "Adaptive Control Software: Can we Guarantee Safety?", Proceedings of the 28th International Computer Software and Applications Conference (COMPSAC '04) DOI: http://ieeexplore.ieee.org/iel5/9304/29573/01342686.pdf?arnumber=1342686

[7] Ahmed M Mahdy, Haitham S Hamza, M E Fayad, Marshall Cline, "Identifying Domain Patterns using Software Stability", , IEEE Digital Library, Downloaded on 31 Dec, 2008 DOI: http://ieeexplore.ieee.org/iel5/9790/30875/01431430.pdf

[8] Naganathan.E.R, Eugene X.P, "Designing Adaptive Reconfigurable Control (ARC)Based Real-Time transaction Processing Systems (RTTPS) Through Software Stability Model (SSM)", Advances in Computational Sciences and Technology ISSN 0973-6107 Volume 2 Number 2 (2009) pp. 101–116,© Research India Publications, http://www.ripublication.com/acst.htm

[9] Sven Hammar: PKI enables digital signatures http://www.nwfusion.com/news/tech/2000/1030tech.html, Network World Fusion.

[10] Records Management Guidance for PKI-Unique Administrative Records, NARA, March 2003, http://www.archives.gov/records_management/pdf/final_pki_guidance.pdf.

[11] PKI Basics – A Technical Perspective, PKI Forum, November 2000 http://www.pkiforum.org/pdfs/PKI_Basics-A_technical_perspective.pdf.

Eugene Xavier P, is a part-time Research Scholar in the Department Computer Science and Engineering, Alagappa University, Karaikudi, India. He received his B.E and M.E degrees from University of Madras and Anna University respectively in 1989 and 1992. After working as a teaching faculty in Engineering Schools (from 1989) in Electrical, Electronics, Communication and Instrumentation Engineering for around 7 years, he worked for Infosys Technologies Limited as a member of the Education and Research Department from 1997 - 2006. Since 2006 he is working for Hexaware Technologies Limited and currently he is an Assistant Vice President, heading the Technical Competency Development Team. His research interest includes Web Technologies, Software Engineering and Control Systems. He is a member of ACM (USA) and an elected Fellow of Institution of Engineers (FIE), India.

Dr. E.R.Naganathan, is a Professor and Head, Department of Computer Applications, Velammal Engineering College, Chennai India. He has completed his Masters in Applied Mathematics from Thiagarajar College of Engineering, Madurai, India in the year 1985. He has received his Ph.D in Computer Applications from Alagappa University, Karaikudi, Tamil Nadu, India in the year 2000. He has 24 years of teaching and Research experience in the field of Computer Science at different Institution in India. Also he has visited Jordon as Assistant Professor for two years in the Department of Computer Science, Jerash University. He has published 36 research papers in National and International Journals/Conferences. His area of interest is Optimization Algorithms, Data Mining and Information Security.