International Journal of
Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2019.33501

Volume 5, Issue 9
September - 2019

Designing A New Framework for Securing Electronic Commerce Systems at Design Phase: With A Special Reference to an Emerging Economy

Andeh, Chioma P R.[1], Amujo Oluyemi E.[2], Aliyu Omeiza[3] and M.B. Hammawa[4]

Research Scholar[1-3] and Professor[4]

Department of Computer Science,

University of Abuja

Nigeria

ABSTRACT

In an emerging economy like Nigeria, internet-based businesses are growing at an exponential rate but this growth is highly threatened by many instances of fraud and e-systems' compromise. While a lot of research work has been done on how to secure e-commerce transaction protocols, improve cryptographic schemes and amend the technical and business issues in e-commerce, the area of mitigating security challenges by incorporating security modules at design time has not been thoroughly explored. Hence, in this paper we present a framework for e-commerce security with a focus on four security design countermeasures models; Authentication, Authorization, enforcement of Access Control and Protection of Transaction privacy. The proposed framework which enhances National Institutes for Standards and Technology (NIST) security model, ensures that adequate security measures are incorporated in an e-commerce system at design time. The framework also ensures designing of secured e-commerce systems which are devoid of the expensive cost implication of system development life cycle incurred by security defects in the system testing phase which traces back to design shortfalls. For the purpose of this research work, we evaluate features called Malicious Attack Enablers (MAE) which aid malicious attack to thrive. The proposed framework will, therefore, aim at securing e-systems against these MAEs while satisfying legitimate user requirements. We assert the competence of our proposed framework by incorporating our security models into a SET enabled existing e-commerce system design, which will illustrate the effectiveness of our framework at the design phase as opposed to waiting till the testing phase. So we show that our new framework will unscramble the design of cost-effective e-commerce systems with curbed security vulnerabilities while contributing to the improvement of e-commerce security standards.

Key Words: *Authorization, Authentication, Attacks, E-Commerce. Security.*

1.0 INTRODUCTION

The value of e-transactions in Nigeria as of December 2015 rose to N48.93 trillion from N43.85 trillion in 2014, indicating an increase of 11.6 per cent. This steady growth rate can somewhat be attributed to an approximate sum of 300,000 online orders made every 24 hours in the country as reported by Africa Practice [1]. As more users are embracing the convenience of online transactions, they are also becoming more aware of the security threats to themselves and their personal information such as the credit card details they leave with merchant sites. The merchant sites in return are susceptible to security oriented attacks like Denial of Service Attacks and Component Failure Attacks.

Cyber security breaches are constantly on the rise with huge uncertainty and risks. The trend is causing rife globally because of its consequences to national security and economy [2]. Report by [3] shows that about 7.1 million identity exposure in data breaches in the last 8years, 76% of e- commerce systems were found to possess vulnerabilities to cyber-attacks. Until recently, best practices for e-commerce security development were based solely on the expertise of individual system designers [4] there was no published security design standard by IT standards bodies such as ISO's Standing Committee 27 (SC 27) (ISOSC 27) for

1C. Author: andehcpr@gmail.com

incorporating countermeasures at design time. Best practices for e-commerce security were developed in an ad hoc manner as new security issues were encountered and overcome, and were not applied uniformly across even an organization, let alone the industry.

Attempts by some standardization bodies in ICT have developed documents which aim to address security design standards but there is no one size fit all security countermeasure model that will serve to counter all the likely cyber security attacks. The first of such document was the Common Criteria (CC) [5] which was steered at the standardization of security assessment/evaluation requirements for Information Technology (IT) systems. While it is possible to use CC and its recent updates as a reference for designing security in E- Commerce systems, the corresponding design process is not a systematic one and relies completely on the individual security designer expertise. A possible risk is not introducing the proper security countermeasures during the design phase. In this case, defects will either be discovered during the system testing phase, requiring an expensive fix, or not discovered at all.

The National Institute for Standards and Technology (NIST) followed suit with a document [6] [7] which describes models and recommendations for designing security in IT systems based on the CC Redbook. Still, using the NIST security services model and their various later releases alone does not guarantee the security of an E-Commerce system. This is because, while these models are intended as a general model for IT systems, extending them for EC systems is similar to using CC to guide design since the process is not systematic and relies completely on the security designer's expertise.

In line with setting security testing standard, The Open Source Security Testing Methodology Manual (OSSTMM) [8] attempted to set a standard for security testing on a running Internet system. OSSTMM can be used to test the Internet part of a running EC system. Yet, it cannot be used directly during the system design phase.

Other current industrial practices have elucidated security countermeasures for discovering defects during the system-testing phase. Any defect discovered during this phase can be traced back to an implementation error or a system design error. Design errors are much more expensive to fix during this phase than if they were discovered during the design phase which has proven to be common place in industry.

Considering Nigeria, the growth rate of e-commerce is highly threatened by the increasing instances of security attacks and the challenge of meeting the security stipulations of an e-commerce system. Security requirements can be divided into two categories: legitimate user requirements that allow legitimate users to use the system in a safe manner, even though there is never any notion of being 100% safe and malicious user requirements that allow malicious users to succeed in breaking system security, i.e. if security satisfying legitimate user requirements. Thus, a system can be considered secure if it provides enough security measures to satisfy legitimate user requirements and is devoid of malicious user requirements that may lead to successful security attacks against the implemented system security.

In present times, the process of introducing countermeasures against known security attacks during an e-commerce system design phase relies completely on the security designer's expertise. Moreover, the countermeasure selection process is ad hoc and, thus, a prescribed countermeasure at system design time might prove inadequate during the system-testing or post-release service phases. This might result in an expensive life cycle for fixing defects related to the e-commerce system design model.

Specifically, in this paper, we seek to implement a new framework for introducing security countermeasures in E-Commerce systems at design time. Our framework is based on the NIST security services model for IT systems. OSSTMM, as well as other resources, are used as points of reference for classifying the different types of security attacks that can be executed on the security features – a feature being a property or service - in the NIST security services model. The result of applying these attacks through our framework to the security features in the NIST security services model is a specialized set of security countermeasures design models that are directly useful for designing secure EC systems. In the second phase of our framework, we show how to apply and integrate these models into an existing (SET-integrated) e-commerce system design.

2.0 LITERATURE REVIEW

2.1 E-Commerce and Its Growth in Nigeria

Electronic commerce is a new way of interacting, bartering and transacting with people and businesses [9]. It is a strategic imperative for most competitive organisations today as it is a key to finding new sources of revenue, expanding into new markets, reducing costs, and creating breakaway business strategies [10]. E-Commerce focuses on the electronic exchange of information using Information and Telecommunications infrastructures to perform a wide range of commercial activities that can be divided into business-to-consumer and business-to-business sectors. Some of these commercial activities include online auctions and internet banking [11]. E-Commerce can therefore be seen as a new way of trading of goods and services over an electronic infrastructure such as the internet [12].

DOI: 10.31695/IJASRE.2019.33501

Initially, it was termed Electronic Data Interchange (EDI) and Electronic Funds Transfer (EFT) until 2000 when the named was changed to Electronic Commerce (E-Commerce) and at this time a great number of business companies in the United States and Western Europe represented their services in the World Wide Web [13].

In Nigeria, E-Commerce came up in 2004 when the Federal Government initiated a joint initiative between private-sector operators, which operate under National e-Government Strategies (NeGEST) and the National Information Technology Development Agency (NITDA), the project aims to improve organizational performance, service delivery and the participation of ordinary citizens in the day-to-day activities of government with information and communication technologies [14]. E-Commerce growth in Nigeria is slow but steady. Electronic banking is one area of E-Commerce that has proven successful in Nigeria. Virtually all banks in Nigeria offer online, real-time banking services. Moreover, banks that cannot offer these services are increasingly losing their customers. The online banking service lets customers conduct a variety of banking activities in any location of a particular bank. These services include among other things, deposits, withdrawals and the issuing of drafts. Banks are also increasingly looking to card-based payment solutions beyond the widely accepted electronic purse, including debit and credit cards, but these are slow to take off [14].

2.2 Security in E-Commerce

Security is a very important part of doing business via the internet since communication can be easily intercepted, messages can be inserted, and the absolute identity of involved parties may be uncertain. It is important therefore to have a dynamic, consistent and coherent set of security measures in place to cover the needs of merchants and consumers [15].

Until recently, there was no published security design standard encompassing all security features. Best practices developed as new security issues were encountered and overcome. However, improvements to security design strategies did not come from a centralized source such as the NIST security design standard. Consequently, research on how to mitigate/curb security failures in cyberspace for more reliable electronic commerce systems and internet based businesses is continuous.

Broadly, security tries to accomplish the following tasks:

- **Authentication** which identifies buyer and also makes sure that person is who he/she claims to be. Used methods are i.e. digital signature, finger prints, password or smartcards etc.

- **Data integrity** which means, that there must be a way to verify that data is not changed during the transactions.

- **Confidentially** must be preserved, so information concerning the tarns action are need to know basis.

- **Non repudiation**, which means that person who did the payments is not able afterwards deny doing so.

Furthermore, among other considerations, it needs to consider the following important issues such as level of security, client authentication, confidentiality requirements and end-user implementation requirements

2.3 Current Security Standards

This section gives an overview of current security standards.

2.3.1 Common Criteria Redbook

The Common Criteria (CC) Redbook [5] was one of the first attempts to standardize security assessment / evaluation requirements for Information Technology (IT) systems. It can be used to select the appropriate IT security measures and contains criteria for evaluation of security requirements.

However, in the domain of e-commerce systems, the Common Criteria Redbook (CC) [5] is intended to be used to evaluate system security only after the system is implemented. It cannot be used directly during the system design phase. This means that CC does not address the core problem which this paper hopes to solve, namely the lack of a security design-time standard for e-commerce systems.

2.3.2 NIST Security Services Model

The NIST security services model is depicted in Figure 2.2 and shows the primary services and supporting elements used in implementing an information technology security capability, along with their primary relationships. The model also classifies the services according to their primary purpose as follows:

- **Prevent:** These services focus on preventing a security breach from occurring
- **Recover:** The services in this category focus on the detection and recovery from a security breach.
- **Support:** These services are generic and underlie most information technology security capabilities.

DOI: 10.31695/IJASRE.2019.33501

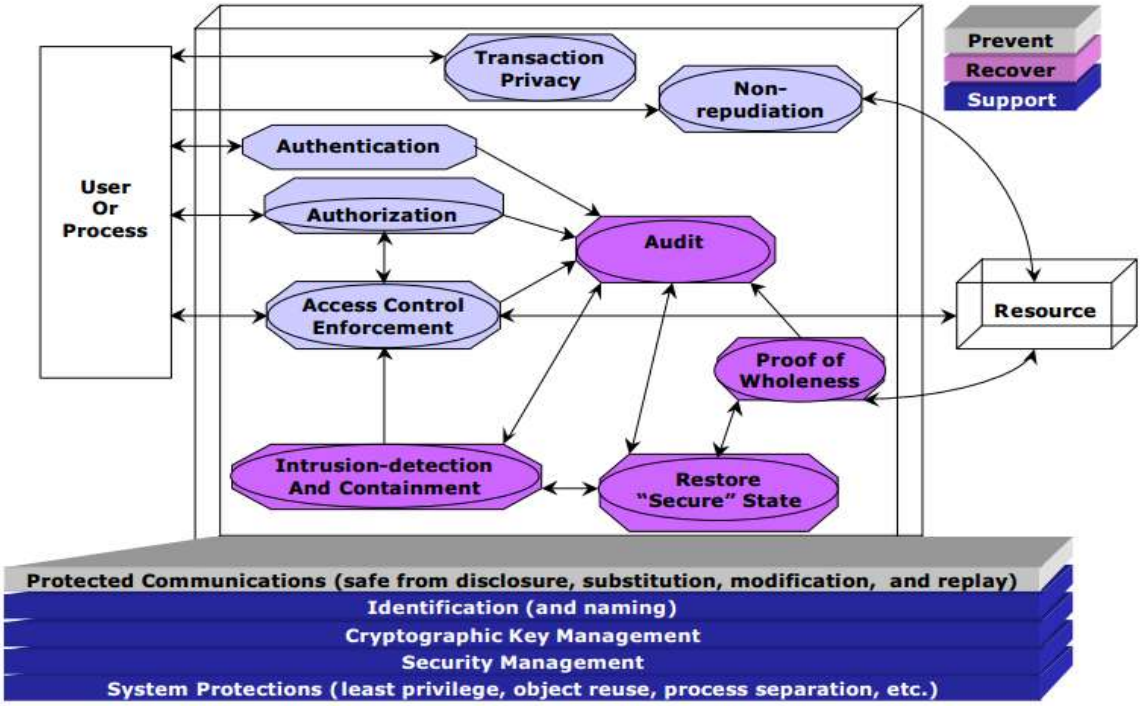

Figure 1: NIST Underlying Technical Security Services Model for IT Systems.
Source: [6], [7]

2.4 Open Source Security Testing Methodology Manual

The Open Source Security Testing Methodology Manual (OSSTMM 3) document provides specific descriptions for operational security tests over all operational channels, which include Human, Physical, Wireless, Telecommunications, and Data Networks, over any vector, and the description of derived metrics. Therefore, the manual only focuses on OpSec (operational security), it attempts to set a standard for Internet security testing on a running system. Although this type of testing cannot be done during the system design phase, the OSSTMM itself will be used throughout this paper as a reference for security attacks. An important aspect of the methodology is the way interdependencies are mapped and related to each other. We use this mapping information to "design in" security safeguards in our approach.

A security test is performed with two types of attacks according to OSSTMM3. A *passive attack* is often a form of data collection that does not directly influence the target. *An intrusive attack* however trespasses upon the target and can be monitored, logged, and used to alarm the target [16]. The process (or methodology) of a security test concentrates on evaluating areas that directly affect security presence. These areas are the following:

- *Visibility:* Visibility encompasses what can be seen, logged, or monitored in the security presence both with and without the aid of electronic devices.

- *Access:* Access is an entry point into the security presence. Since security is the separation of a threat and an asset then the ability to interact with the asset directly is to access it.

- *Trust:* Trust includes the kind and amount of authentication, non-repudiation, access control, accountability, confidentiality, and integrity between two or more features within the security presence.

2.5 Secure Electronic Transactions (SET)

Secure Electronic Transactions (SET) is a standardized industry wide protocol specification designated to secure payment transactions and authenticate the parties involved in the transaction in any type of networks including Internet. VISA and MasterCard developed the SET standard with collaboration from leading software companies such as Microsoft, Netscape, RSA, VeriSign, and other. SET was created to provide the trust needed for consumers [17].

2.5.1 SET Specifications

• SET uses RSA Data security public key cryptography in order to encrypt and decrypt transaction packets along with the use of digital certificates and digital signature for authentication of all parties to the transaction and validation that information has not been tampered with.

DOI: 10.31695/IJASRE.2019.33501

- SET makes online transactions even safer by using digital certificates to verify that consumers and merchants are both authorized to use and accept Visa cards. It's the electronic equivalent of a consumer looking for a Visa decal in a merchant's store window, and a merchant checking the consumer's signature on the back of a Visa card. Merchants worldwide are currently adopting SET.
- SET incorporates the use of public key cryptography to protect the privacy of personal and financial information. As a result, with SET, consumers' payment card information is protected all the way to the financial institution. The merchant cannot read this information in the payment transaction.
- With SET, cardholders can validate that the Internet merchant is legitimate through the merchant's digital certificate. SET software automatically checks that merchant has a valid certificate representing their relationship with their financial institution.

3.0 RESEARCH METHODOLOGY

In order to satisfy the objectives of the research work, a qualitative research will be held. Since the basis of this paper is a qualitative research methodology, surveys are based on study documents, published works and other pertinent works that are relevant to solving the research problem.

3.1 Our Framework for Deriving and Integrating Countermeasures Design Models for Electronic Commerce Systems

3.2 Framework Overview

In this section, we provide a detailed description of our proposed framework for deriving and applying EC security countermeasures design models from the existing IT standards. As mentioned earlier, the NIST security services model is at the basis of our model. Our goal is to describe a model-based approach of how to extend such a model or “specialize” it in order to apply it to e-commerce systems.

3.3 Our Solution Requirements and Rationale

Our discussion of the current state of e-commerce security formulates a problem whose solution requires a framework or approach that satisfies the following four requirements.

1. The solution has to be systematic in nature. This is required to avoid relying on the expertise of security designers.

2. The framework or approach must introduce security countermeasures during an E- Commerce system design phase. This is required to avoid expensive system development life cycles by minimizing the probability of having defects related to the e-commerce system design model discovered in the system-testing phase.

3. The solution must extend / specialize security features, as described in referenced literature standards [5] and [6], and must not break interdependent relationships among the security features. This requirement is important to preserve the validity of the overall e-commerce security design model.

4. The solution must be *extensible*. This is a requirement for the ability to support countermeasures against possible unknown security attacks discovered in the future.

3.4 Phases of the Framework

Our framework, depicted in Figure 3.1, can be divided into two functional phases. In Phase 1, security features are selected and security-oriented design models are derived and verified. In Phase 2, the derived security-oriented design models from Phase 1 are instantiated and integrated into an existing e-commerce system design.

DOI: 10.31695/IJASRE.2019.33501

Figure 2: Our Framework to derive specialised EC Security Countermeasures Design Models.

4.0 IMPLEMENTATION AND APPLICATION OF OUR NEW FRAMEWORK TO THE NIST SECURITY SERVICES MODEL AND TO A SET- INTEGRATED E- COMMERCE SYSTEM

4.1 Part A: Case Study Phase 1

4.1.1 Applying the Design for Security Framework to the NIST Security Services Model

Our objective in this chapter is to employ a case study of four features in order to demonstrate that our design-for-security models:

- Meet or exceed security requirements provided in current security standards at system design time for these four features.
- Are able to disable malicious user requirements at system design time for these four features.
- Provide effective security against all known security attacks related to the e- commerce domain with respect to these four features.
- Can be readily integrated into high-level design documents of e-commerce systems.

4.1.2 Security-Oriented Authentication Design Model

The first is to select a NIST model security feature. Here we select authentication**.** Figure 4.2 shows all security attacks related to authentication in e-commerce systems along with the attack enablers and prescribed countermeasures. Such attacks are Sniffing Attacks, ID Spoofing Attacks, Brute-Force Attacks, Dictionary Attacks, Replay Attacks, Credential Decryption Attacks and Side-Channel Attacks

DOI: 10.31695/IJASRE.2019.33501

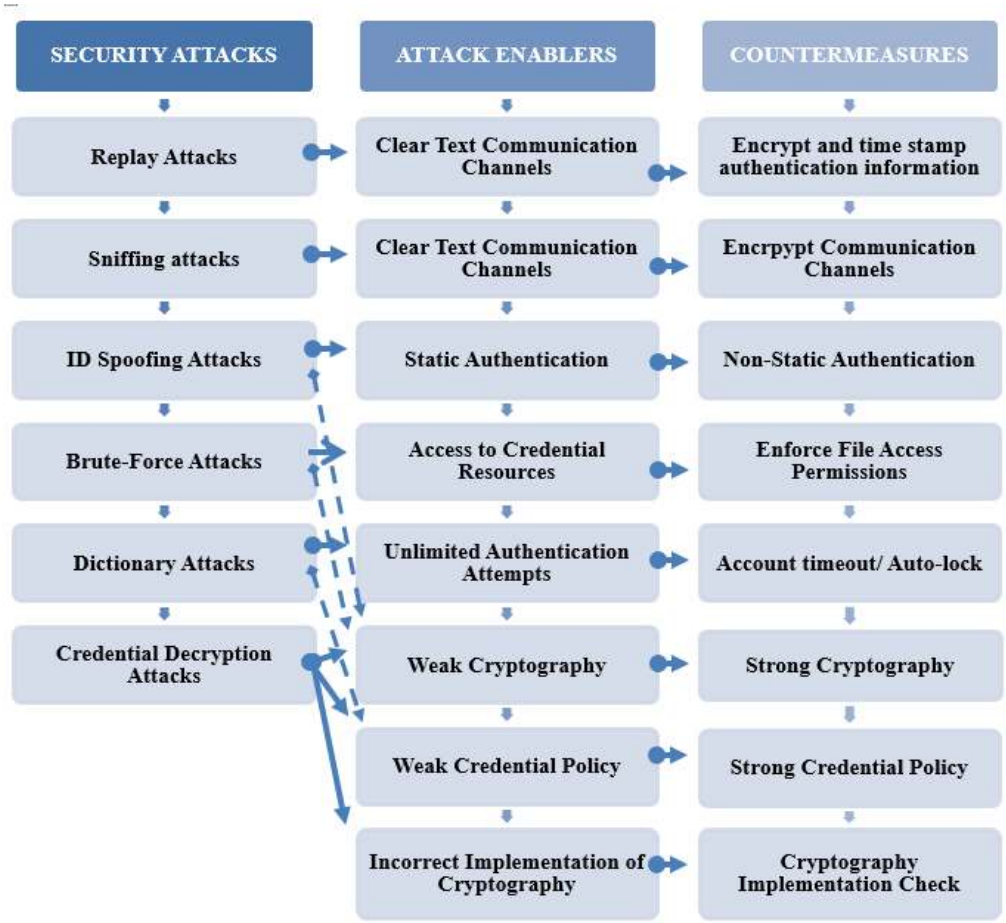

Figure 3: Representation of Authentication Security Attacks, Attack Enablers and Countermeasures

4.1.3 Deriving the Authentication Security-Oriented Design Model

After identifying the attacks, attack enablers, and countermeasures for authentication, the prescribed countermeasures are grouped and ordered into a countermeasures design model as shown in Figure 4.

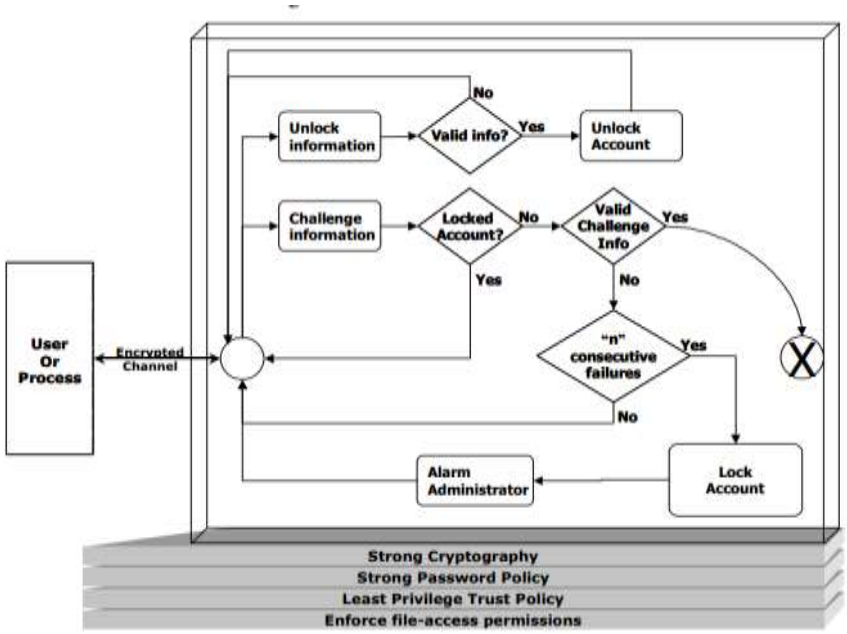

Figure 4: The Derived E-Commerce Authentication Countermeasures Design Model.

DOI: 10.31695/IJASRE.2019.33501

The process of deriving the authentication design model (shown in Figure 4) proceeds as follows:

- We start by grouping all prescribed countermeasures. The result is a set of countermeasures that must be applied to the e-commerce system for this feature.
- We separate countermeasures into action countermeasures and underlying countermeasures. An action countermeasure is an action that must be done to disable an attack (e.g. lock an account). An underlying countermeasure is a countermeasure that does not specify an action but is required to disable an attack (e.g. strong cryptography).
- Our countermeasures design model is divided into two sections: an action-flow box and a set of planes below the box containing underlying countermeasures.
- Countermeasures that represent actions are placed inside the box. Similarly, underlying countermeasures are placed in the planes below the box.
- We then advance to group action countermeasures into process flow charts. A process flowchart specifies the sequential order for applying countermeasures.

4.1.4 Security-Oriented Authorization Design Model

First, we select a NIST model security feature. Here we select authorization**.** Figure 5 shows all security attacks related to authorization in e-commerce systems, along with the attack enablers and prescribed countermeasures.

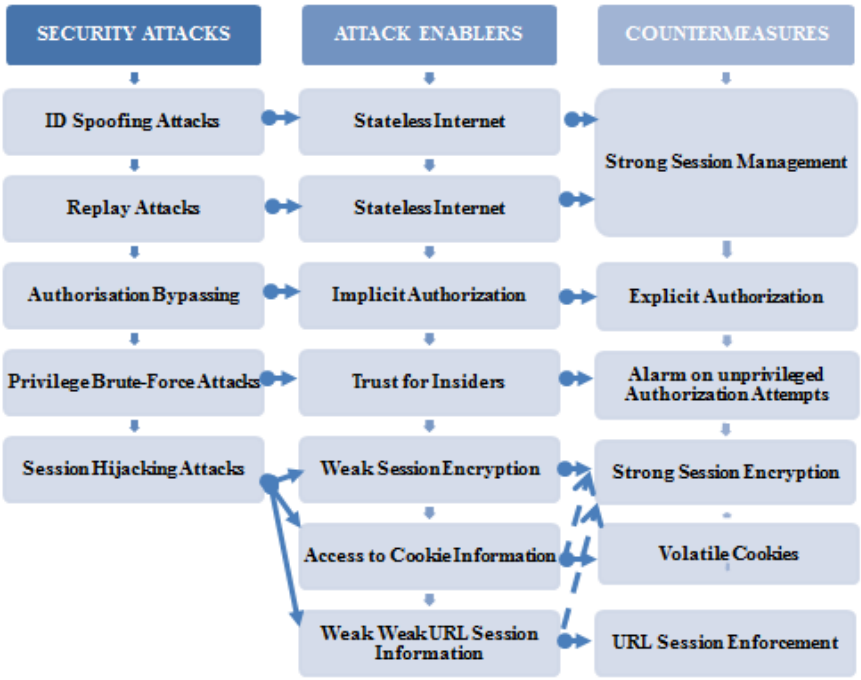

Figure 5: Representation of Authorization Security Attacks, Enablers and Countermeasures

4.1.5 Deriving the Authorization Security-Oriented Design Model

After identifying the attacks, attack enablers, and countermeasures for authorization, the prescribed countermeasures are grouped and ordered in a design model. Figure 6 shows the detailed authorization design model derived by applying our framework. As seen in the figure, the main entry point to the authorization model is explicit authorization.

The EC authorization countermeasures design model shown in Figure 6 is detailed enough to be directly applied to the design of EC systems. This model satisfies security requirements and blocks malicious user requirements at system design time. It provides effective security against all known security attacks related to authorization in the e- commerce domain

DOI: 10.31695/IJASRE.2019.33501

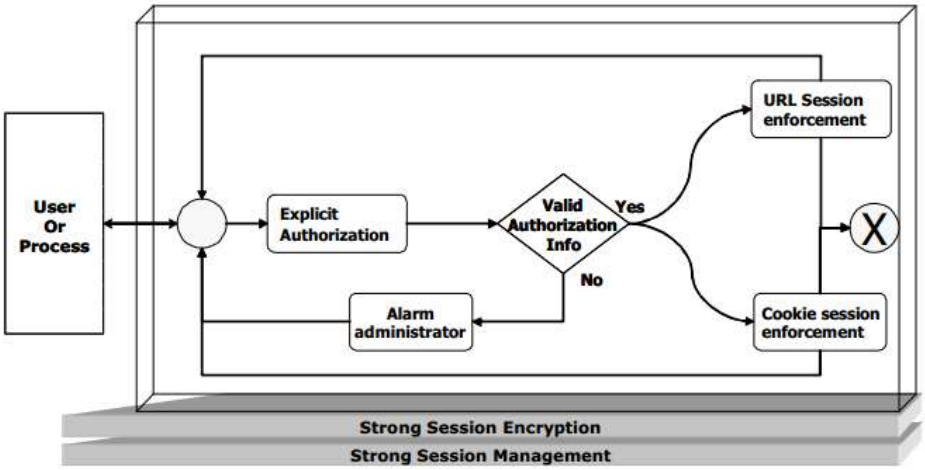

Figure 6: The Derived E-Commerce Authorization Countermeasures Design Model.

4.1.6 Security-Oriented Access Control Enforcement Design Model

The goal of this section is to have a preventive design model for access control enforcement that can be incorporated into any integrated access control enforcement model or can be implemented as a standalone access control enforcement module in e-commerce systems.

Figure 7 shows all security attacks related to access control enforcement in e-commerce systems along with the attack enablers and prescribed countermeasures.

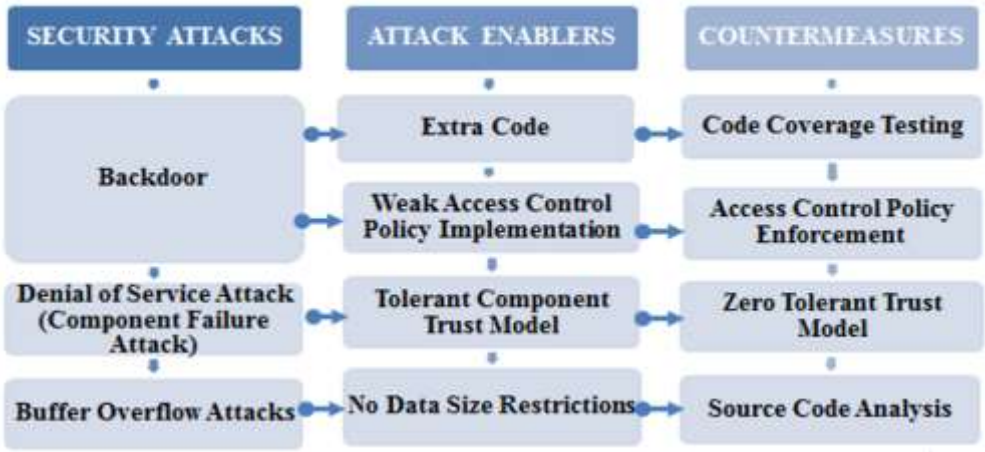

Figure 7: Representation of Access Control Enforcement Security Attacks, Attack Enablers, and Countermeasures.

4.1.7 Deriving the Access Control Enforcement Security- Oriented Design Model

After identifying the attacks, attack enablers, and countermeasures for access control enforcement, the prescribed countermeasures are grouped and ordered in a countermeasures design model. As seen in Figure 8, the main entry point to the model is zero-tolerance.

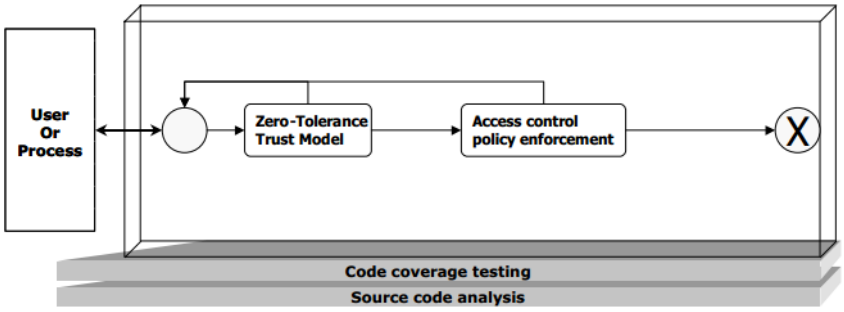

Figure 8: The Derived E-Commerce Access Control Enforcement Countermeasures Design Model.

DOI: 10.31695/IJASRE.2019.33501

The access control enforcement design model shown in the figure is detailed enough to be directly applied to the design of EC systems. This model satisfies security requirements and blocks malicious user requirements at system design time. It provides effective security against all known security attacks related to access control enforcement in the e-commerce domain.

4.1.8 Security-Oriented Transaction privacy Design Model

Figure 9 shows all security attacks related to transaction privacy in e-commerce systems along with the attack enablers and prescribed countermeasures.

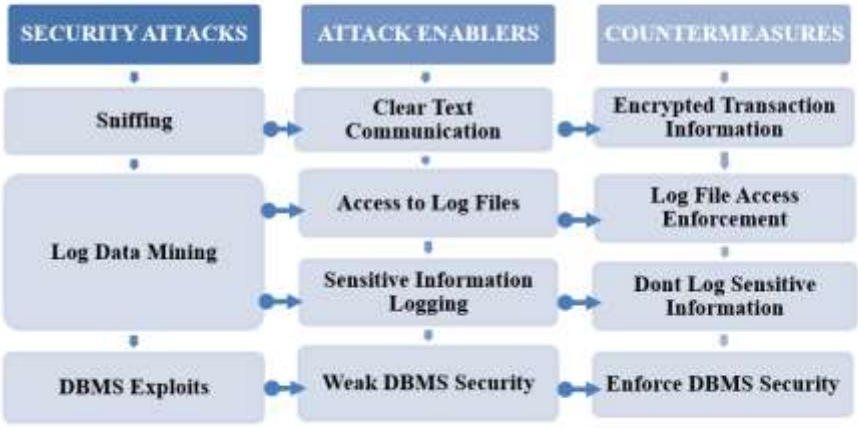

Figure 9: Representation of Transaction Privacy Security Attacks, Attack Enablers and Countermeasures.

4.1.9 Deriving the Transaction privacy Security-Oriented Design Model

The process of deriving the design model was described earlier in section 4.1.8. and Figure 10 shows the detailed transaction privacy countermeasures design model for EC systems derived by applying our framework. As seen in the figure, the communication channel between the user or process and the EC system has to be encrypted for transaction privacy purposes. If this is not the case, then at least sensitive transaction information should be encrypted.

This model satisfies security requirements and blocks malicious user requirements at system design time. It provides effective security against all known security attacks related to transaction privacy in the e-commerce domain.

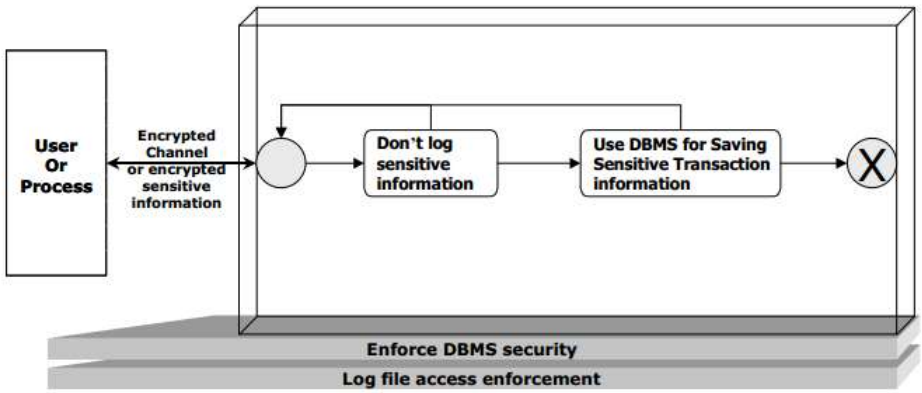

Figure 10: The Derived E Commerce Transaction Privacy Countermeasures design model.

4.2 Part B: Case Study Phase 2

4.2.1 A SET-Integrated E-Commerce System

In this section, we present our case study of designing for security a SET-integrated e- commerce system. Our case study e-commerce system, shown in Figure 11, is a virtual store system that involves four entities: a merchant EC system, a client, an EC system administrator, and a payment gateway.

In this case study, we will apply our derived countermeasures design models to the merchant entity of the e-commerce system only. Designing the security of the other entities (client and payment gateway) will not be considered as the responsibility, in this case, relies on their respective owners; i.e. the client and the payment gateway provider respectively. Other entities described in SET- namely the issuer, acquirer, brand, and certificate authority– are not directly related to our case study e-commerce system.

DOI: 10.31695/IJASRE.2019.33501

For example, a certificate authority is only required to check the validity of a certificate. This only occurs at the payment gateway side and at the client (cardholder) side.

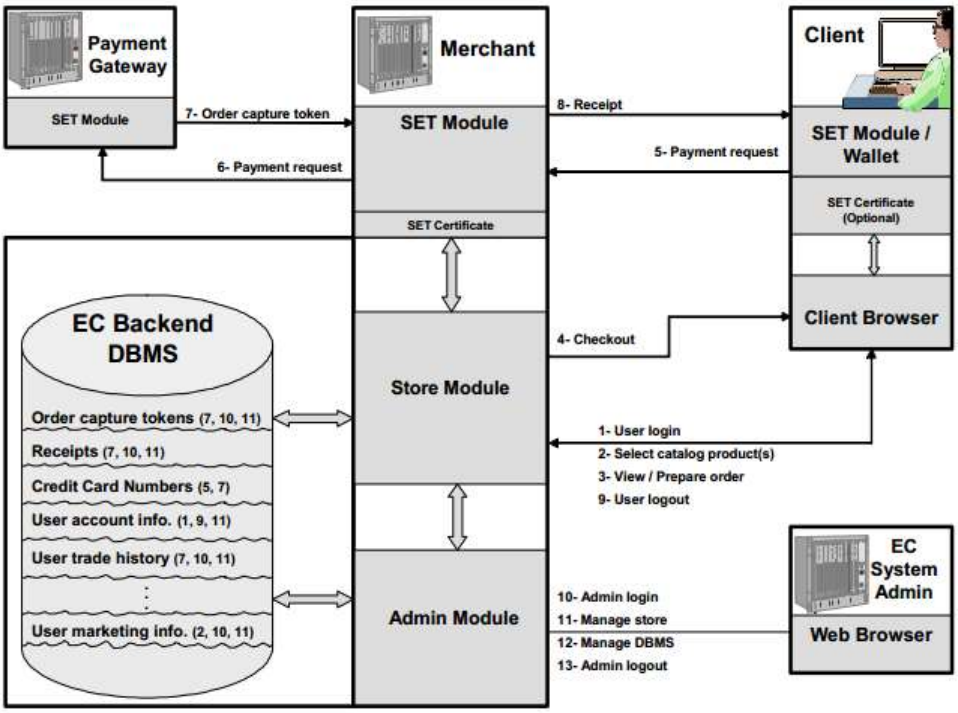

Figure 11: A SET-Integrated E-Commerce System.

Based on the instantiation illustrated in Figure 12, the derived authentication countermeasures design model is instantiated to become as shown in Figure 12 below:

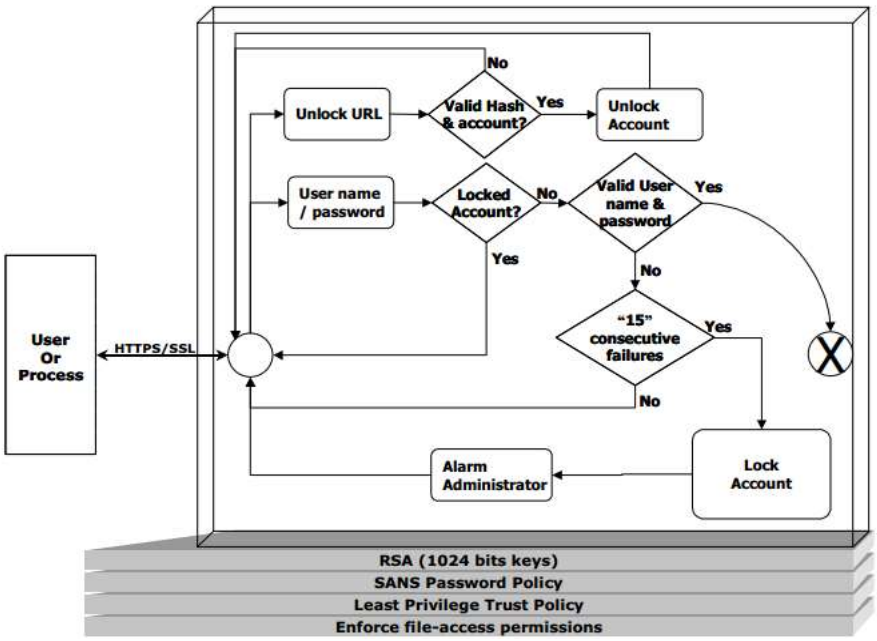

Figure 12: The SET-Integrated System Authentication Countermeasures Design Model.

4.2.2 Authorization Summary

Based on the instantiation illustrated in Figure 12 above, the derived authorization countermeasures design model is instantiated to become as shown in Figure 13.

DOI: 10.31695/IJASRE.2019.33501

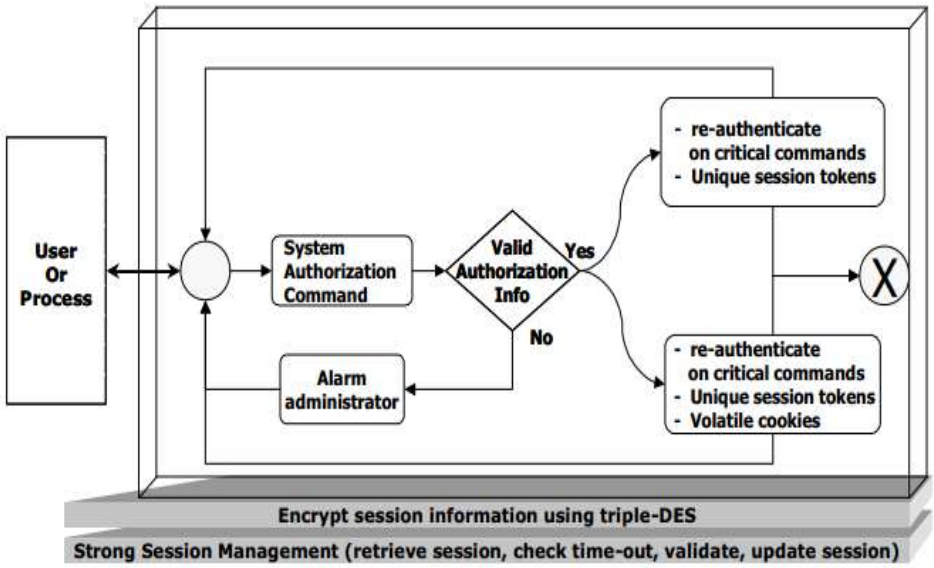

Figure 13: The SET-Integrated System Authorization Countermeasures Design Model.

4.2.3 Access Control Enforcement Summary

Based on the instantiation illustrated in Figure 13, the derived access control enforcement countermeasures design model is instantiated to become as shown in Figure 14.

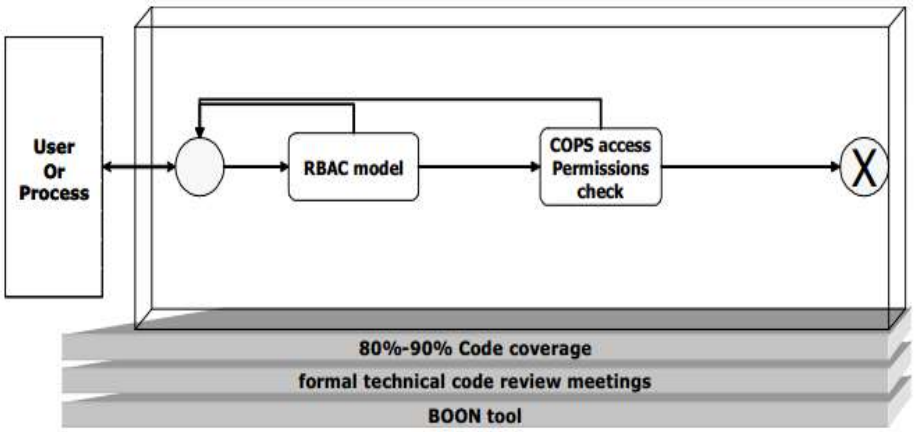

Figure 14: The SET-Integrated System Access Control Enforcement Countermeasures Design Model.

4.2.4 Applying and Integrating Transaction Privacy Design Model

In this section, we will apply the derived transaction privacy countermeasures design model to the e-commerce system. This application is intended to prove the applicability of the derived transaction privacy countermeasures design model. The first step in applying the derived countermeasures design model is to instantiate its features. This is a straightforward process that takes every feature of the model and converts it into an implementable feature. A description of how the transaction privacy model features, described in section 4.5, are instantiated is provided below.

Encrypted Channel / Transaction Information, Saving Sensitive Data in DBMS, Not Logging Sensitive Information, Enforce DBMS Security, Log File Access Enforcement and Transaction Privacy Summary.

Based on these instantiations, the derived transaction privacy countermeasures design models are instantiated to become as shown in Figure 15.

DOI: 10.31695/IJASRE.2019.33501

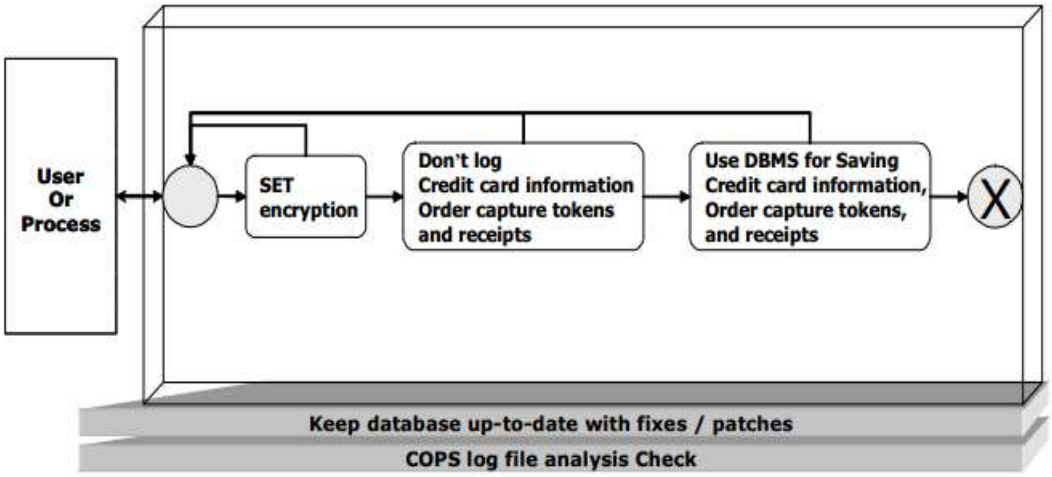

Figure 15: The SET-Integrated System Transaction Privacy Countermeasures Design Model.

4.3 Case Study System Security Comparison

In this section, we compare in Figure 16 the state of security in our SET-integrated e-commerce system before applying our countermeasures design models, i.e. while relying on SET security alone, and after applying the models.

Security feature	Security attack	Before	After
Authentication	Sniffing attacks	Partial	Complete
	ID spoofing attacks	Partial	Complete
	Brute-force attacks	No	Complete
	Dictionary attacks	No	Complete
	Replay attacks	Partial	Complete
	Credential decryption attacks	Partial	Complete
	Side-channel attacks	N/A	N/A
Authorization	ID spoofing attacks	Partial	Complete
	Authorization bypassing attacks	No	Complete
	Privilege brute-force attacks	Partial	Complete
	Replay attacks	Partial	Complete
	Session hijacking attacks	Partial	Complete
Access control enforcement	Backdoors	No	Complete
	Denial of service attacks	N/A	N/A
	Component failure attacks	No	Complete
	Buffer overflow attacks	No	Complete
Transaction privacy	Sniffing attacks	Partial	Complete
	Log data mining attacks	No	Complete
	DBMS exploits	No	Complete

Figure 16: A Comparison of Our SET-Integrated E-Commerce System Security before and after Applying the Countermeasures Design Models.

5.0 SUMMARY

5.1 Benefits of the new model

In this section, we discuss four benefits of applying our security-oriented design models. The benefits are:

- Our security-oriented models can be directly instantiated and applied for e-commerce systems. This was shown throughout this case study as a straightforward process of instantiating each model feature into an existing technology.
- Our models are helpful for providing implementation guidelines and planning security testing. An example of providing implementation guidelines is instantiating the strong password policy countermeasure to the SANS standard for strong

DOI: 10.31695/IJASRE.2019.33501

passwords. This provided guidelines for implementing strong passwords into the e- commerce system by specifying how to identify a strong password.

- Our security-oriented models minimize relying on the expertise of security architects for designing secure e-commerce systems. This benefit is inherited from our systematic framework and is also achieved in this case study. The process of instantiating our security-oriented model only require research for existing technologies and does not require strong security expertise.
- Our models provide complete protection against all known security attacks in the e-commerce domain. This benefit is also inherited from our systematic framework and applies in this case study as well. Section 5.7 provided a comparison between the state of security in our SET-integrated e-commerce system before and applying our design models for authentication, authorization, access control enforcement, and transaction privacy.

5.2 Limitations of the new model

As we have clearly illustrated, the security range of our design models is limited to the e- commerce system itself. Third party components (such as network components, operating system platforms, etc.) are not taken into consideration. In practice, of course, these components must be taken into consideration.

In this paper, this limitation was introduced because, in most cases, EC system designers limit their security range to that of the e-commerce system that they provide. This is logical because the security of any component relies on the security of its designer. Furthermore, it is almost impossible to guarantee security of third-party components that are used in the e-commerce system since these components provide the required functionality in a "black-box" manner.

6.0 CONCLUSION

This paper described a new framework for deriving countermeasures design models for e-commerce systems. The framework is based on the NIST security services model. Our approach focuses on satisfying legitimate user requirements while blocking malicious user requirements at system design time. We assessed and showed that our framework is systematic through a case study that derived four countermeasures design models for authentication, authorization, access control enforcement, and transaction privacy.

The derived countermeasures design models were assessed through a realistic case study on a SET-integrated in e-commerce systems. These models were also proven to be effective against all security attacks related to the e-commerce domain.

We see the primary benefits of our research as follows:

- ✓ A comprehensive matrix listing and mapping all rampant security attacks to four security features in e-commerce systems; namely authentication, authorization, access control enforcement, and transaction privacy.
- ✓ Four new security models that extend the NIST security services model for e- commerce systems. These models are proven to be effective against all known security attacks related to e-commerce systems.
- ✓ A faithful implementation of a countermeasures design model was proven to be guaranteed to block all known security attacks related to that feature.
- ✓ Security architects can avoid expensive system development life cycles fixes. This is achieved by having an effective countermeasures design model that is directly applicable to EC systems and that specifies detailed requirements for the security feature.
- ✓ A cost-effective, systematic framework for deriving countermeasures design models for the other security features of e-commerce systems.
- ✓ An overview of all known security attacks related to the four security features discussed in this paper; namely authentication, authorization, access control enforcement, and transaction privacy.

7.0 FURTHER WORKS

Further research is needed to optimize our framework and countermeasures design models. In particular, further studies should:

- ➢ Apply our framework and approach to the remaining features of the NIST security services model.
- ➢ Further enhance the framework to map other security-related features, such as impact on performance, into the design process.
- ➢ Formally describe the framework and provide automation.
- ➢ Apply the framework to other standard security models once available.
- ➢ Update the derived countermeasures design models with new security attacks once available.

DOI: 10.31695/IJASRE.2019.33501

REFERENCES

[1] T. Newbold, "*Africa Practice: Africa on the Verge (AoV) Convergence Series," 2016,* AOV Convergence Series White Paper 2016)

[2] U. Emmanuel Chinanu and Oluyemi Amujo, "Comparative Survey of Cyber-Threat and Attack Trends and Prediction of Future Cyber-Attack Patterns," International Journal of Innovative Research in Computer and Communication Engineering, vol. 6, Issue 4, April 2018

[3] The Symantec Cooperation 2017 Internet Security Threat report, vol. 22, 2017, Online: https://digitalhubshare.symantec.com/content/dan/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-APR24.pdf?aid=elq_12438

[4] D. Brinkley, and R. Schell, "Concepts and Terminology for Computer Security, Information Security: An Integrated Collection of Essays," *IEEE Computer Society Press*, pp. 40-97, 1995.

[5] Common Criteria (CC), "Common Criteria for Information Technology Security Evaluation," Feb 1999, Online: http://www.commoncriteria.org/

[6] National Institute of Standards and Technology (NIST), "Underlying Technical Models for Information Technology Security," NIST Special Publication 800-33, 2001.

[7] National Institute of Standards and Technology (NIST), "Role Based Access Control", NIST Special Publication 350-29, August 2002.

[8] P. Herzog, "The Open Source Security Testing Methodology Manual", version1.5, 2001, Online: http://ideahamster.org/

[9] A. Ghosh, "E-Commerce Security: Weak links, Best Defences," Wiley Computer Publishing, Canada. pp. 222-232, 1998

[10] Verisign, "Building the Infrastructure for secure Electronic Commerce," 2004, Online: http://www.verisign.com.au/whitepapers/enterprise/ecommerce/infra5.shtml

[11] D. Hutchinson & M. Warren, "Security for internet banking: A framework in Logistics Information Management," pp. 59-78, 2003

[12] Z. Jiemiao, "Information Management, Innovation Management and Industrial Engineering," Research on E-Payment Protocol (ICIII), 121 – 123, 2011

[13] M. Foluke, "History of E- commerce," Aug 2015, Online: https://www.zutasia.com/blog/history-of-e-commerce-2/

[14] O. M. Obafemi, "The Challenges of Globalization on e-commerce in Nigeria," 2012, Online: http://kubani.abu.edu.ng:8080/jspui/handle/123456789/1706

[15] E. I. Houssam, H. Hanane, & M. Hicham, "A Secure Electronic Transaction Payment Protocol Design and Implementation," *International Journal of Advanced Computer Science and Applications,(IJACSA),5*(5), pp. 172-180, 2014.

[16] P. Herzog, "The Open Source Security Testing Methodology Manual," version 3.02, June 2010, Online: http://trustanalyst.org/

[17] M. S. Merkow. J. Breithaupt and K.L. Wheeler, "Building SET Applications for Secure Transactions," John Wiley and Sons, New York. 1st Edition, 13, 315-402, 1998.

[18] Secure Electronic Transaction Specification, "Business Description, Book 1", SET, Programmer's Guide, Version 1.0., 1997

[19] Secure Electronic Transaction Specification, "Business Description, Book 2", SET, Programmer's Guide, Version 2.0., 1997

[20] Secure Electronic Transaction Specification, "Business Description, Book 3", SET, Formal Protocol Definition, Version 1.0., 1997.

DOI: 10.31695/IJASRE.2019.33501