The specifications of E-Commerce Secure System using Z language

Mustafa M. Noaman
Computer Sciences Department, The Faculty of Information Technology and Computer Sciences, Yarmouk University
Irbid, Jordan
mustafa.monaf@gmail.com

Izzat M. Alsmadi
Computer Information Systems Department, The Faculty of Information Technology and Computer Sciences, Yarmouk University
Irbid, Jordan
ialsmadi@yu.edu.jo

Ameera S. Jaradat
Computer Sciences Department, The Faculty of Information Technology and Computer Sciences, Yarmouk University
Irbid, Jordan
ameera@yu.edu.jo

ABSTRACT
This paper uses formal methods to improve the security of the e-commerce system specifications and reduce the number of security threats to the minimum. The result shows the effectiveness of using formal methods for empowering e-commerce security. Z specification language is used to design the e-commerce system & specify security constraints. Besides, Z/EVES formal methods tool is considered for demonstrating our work.

Categories and Subject Descriptors
K.4.4: Electronic Commerce
K.6.5: Security and Protection

General Terms
Design, Reliability, Security

Keywords
E-Commerce Security, Specification Language

1. INTRODUCTION
Recently, the number of e-commerce users has been increasing due to the rapid wide spreading of advanced technology and the ease of internet use and access; it was very attractive especially for small businesses because they don’t have to worry about the cost of physical store and advertisement (ex. eBay & Amazon websites). Because of the security threats e-commerce systems gained bad reputation, which forces the companies work on improving the security to gain users’ trust back. When the commercial system proves its immunity and the number of information theft decreases, the number of e-commerce users increases. Commercial systems depend on users & transactions' rates to determine its success, when the security system is not capable of protecting users’ information (ex. customer credit card & account numbers) it will result in the decrease in users & transactions rates. Consequently, the system will be useless to the company. Companies seek a system that is secure enough and immune to security threats, hacking attacks and information leakage which tried to mislead customers to gain their trust. For example Mondex "is a smart card electronic cash system part of the MasterCard worldwide suite of smart card products, enables cardholders to carry, store and spend cash value using a payment card". Mondex security system must be immune enough to acquire customers trust, and as a result, increase the number of customers using the system especially when dealing with worldwide electronic cash system. Formal methods can be used to improve the security by adding more reliability, providing solutions to security threats, monitoring customer’s behaviour and highlighting suspicious actions. As we mentioned earlier the security of e-commerce system is very important for the customers and companies so the development is going to be focused on the security of the system. The main goal of this paper is to develop specifications for e-commerce secure system using Z language and to open a path for other researchers toward the solution for security issues that are affecting the e-commerce system reputation. This paper aimed to develop specifications for e-commerce secure system using Z language and to open a path for other researchers toward the solution for security issues that are affecting the e-commerce system reputation. This paper aimed to develop specifications for e-commerce secure system using Z language and to open a path for other researchers toward the solution for security issues that are affecting the e-commerce system reputation.

For example: an attempt from user to buy a product with insufficient balance results in a fault that adds one point to the user’s alert points, when Alert_Points = 5 the user account will be blocked. As a result, the user will not be able to login in or do anything else in the website unless the account unblocked. The account may be unblocked by website customer care.

First, we describe the system in specification in general; then, we will apply it on a chosen e-commerce system. Security in e-commerce system is an interesting subject as a modern business is concerned with the security problems facing e-commerce systems.

2. PROBLEM STATEMENT
Commercial systems depend on users & transactions’ rates as factors for their success. The incapability of protecting users’ information (ex. customer credit card & account numbers) results in decreasing users & transactions rates, which indicates a system that is insignificant. Companies are seeking system that is invulnerable to security threats, hacking attacks and information leakage to gain customer trust. Gaining customers trust has a significant role in increasing the number of customers which in turn is a vital when dealing with worldwide electronic cash system. Formal methods are used to improve the security by adding reliability, providing solutions to security threats, monitoring customer’s behavior and highlighting suspicious
actions. Our main concern will be the security of the system as it has a huge effect on the companies and the customers. The paper main goal is to develop specifications for e-commerce secure system using Z language. Besides, it will be an opportunity to open a path for other researchers toward the solution for security issues that affecting the e-commerce system reputation. In this, we develop an e-commerce secure system using the Z language that controls the transactions. Also, it monitors and tracks suspicious activities of customers or organizations. Despite the fact that The Z language has never been used to develop e-commerce secure activities of customers or organizations. Despite the fact that The Z language has never been used to develop e-commerce secure system in general, it was used to prove Mondex security properties [5] which are the closest research to our work. For the purpose of demonstration, we use the Z/EVES tool from the Z language. The proposed system relays on usage behavior to determine suspicious activities and confines the security threats; the proposed system uses a "5 points" method. For example: when a user makes an attempt to purchase a product with insufficient money in his balance, the system adds one fault point to user's alert points, when the user's Alert_Points reaches five, the user's account will be blocked. And so, the user will be unable to login or perform any activity in the website. The user may gain access to the website after contacting the website customer care who will unblock the account after performing user verification. The "5 points" alert method is believed to be useful in limiting security threats by tracking the sequence of suspicious activities that is performed by a certain user account and consequently make an action to stop the potential threat.

3. PROBLEM SCENARIO
The scenario we will use is an e-commerce website with some potential security threats such as:

A. Attempts to make a purchase with insufficient balance, or perform a balance recharge using illegal way, or buy a product without logging in the system (money theft).
B. A hacker login user account and have the credit card number or other user information by trying different passwords to login website (eavesdropping).

The system variables are:

1. Customer: data type describes user information and contain:
   a. Username: user's login name to the website.
   b. Password: special word chosen by the user to login the website.
   c. Account: user's money (credit card number, Bank account).
   d. Status: user’s activity status (safe, suspicious, blocked).
   e. State: user’s system logging state (Online, Offline)

2. Product: data type describes product information and contain:
   b. Quantity: product quantity.

3. Security-Alert: data type contains security alerts due to user/company behaviour and it’s types:
   a. Money-Theft: user tries to manipulate payable amount.

Eavesdropping: hacker tries to steal user information (ex. bank account number, social security number, telephone, address, e-mail).

4. LITERATURE REVIEW
This section is devoted to the e-commerce security related work.
In 1999 Jeannette W. [10] shows the correlation between formal methods and security in general, and proposed a future work to improve the use of formal method in security.
In 2002 Anthony Hall [7] applied C-by-C (Correctness by Construction) methodology to develop a commercial secure system and build a secure system using unreliable or unsecure components like COTS (Commercial off-the-shelf).
In our work, we use the Z language to express ‘Formal Security Policy Model’ for the purpose of improving the security of the e-commerce system.

James and Marshall [9] insisted on using the formal methods as a part of the secure system development due to the formal methods ability of ensuring precision, consistency and assurance during the different stages of building a trusted computing system.

John and Peter [4] used VDM-SL formal method in the commercial system development. They developed a secure system with British Aerospace (Systems &Equipment) Ltd.

Bernhard and Gerd [1] shed a light on the importance of user interface and user interface environment. They used OCL (Object Constraint Language) to model the user interface security properties and control the input/output and propose algorithm to improve security of the user interface.

Anthony Hall [5] describes the process of developing Formal Security Policy Model (FSPM) using Z language, the result of the development was successful due to the number of the faults in developed system is less than other systems developed by other approaches, the result system also have more productivity & efficiency and the using of formal language didn’t add extra cost, so the using of formal language was effective and accomplish its goal. Hall [5] used Z language to enhance the Commercial Development Process and develop system that can add more reliability & productivity.

Michael B. [2] discusses the use of formal methods to measure & analyze trust, he showed the impact of using formal methods like Z notation & B method. Michael’s work [2] takes the lead of discussing the use of formal methods to improve user trust in the system and its impacts on system usage, which indicates the importance of using formal methods to improve security and trust as well.


James D [3] emphasizes the importance of formal methods and their impact on the system as they are required to improve the software system correctness and trust. Moreover, James [3] describes the C-by-C (Correctness by Construction) methodology and how to apply formal methods with it. The paper describes how to apply the formal methods with the C-by-C methodology to increase system correctness.

Anthony Hall [7] provides a description of the Z language and shows the importance of using it. In his work, Hall described new Z using styles: one that was used with CESG (Computer and...
Electronic Security Group), and the other used for the specification of modern software systems. Both styles have been used in a real commercial system by researchers and system developers to present important properties.

Constance H. and Ourla A. [8] described an approach to verify the security of software using TLS (Top-Level Specification - a formal statement of the security property) which reduces the cost of verification. The approach was meant to support ‘Common Criteria’ evaluation of the security of embedded device called ED (Embedded Device). The 5-step ‘Code Verification’ was used to decompose the system to artefacts which was later applied in details.

5. SYSTEM DESIGN

E_COMMERCE_SYSTEM schema defines inputs and outputs variables that are needed by the system to complete operations like login, buy, and recharge. Each customer has an email address, password, balance, status, state, and an Alert_Points. These parameters will be used to determine completion for behavior and actions.

We are going to describe each one of them:

- Email: User’s email used for system logging.
- Password: User’s password used for system logging.
- Balance: User’s money used to buy & recharge operations.
- Status: User’s system usability user’s status (Safe, Suspicious, Blocked)
- State: User’s system logging state (Offline, Online)
- Alert_Points: Used to determine user’s status.

Each product has a quantity and a price which are used to determine the completion of buy operation.

- Quantity: Product quantity.
- Price: Product price.

6. SYSTEM IMPLEMENTATION

We used Z/EVES tool to implement the Z language specification for e-commerce system. The string is not defined in Z/EVES. So, we simplified the system and directed rules to work well with Z/EVES. We put ready values for each variable to demonstrate system with Z/EVES tool.

We will provide sample of usernames and passwords to overcome the problem of Z/EVES tool with strings. We set values for status, balance, state & alert point for user information and quantity and price for product information.

6.1 System Implementation

The first schema is LOGIN (shown in figure 2) and it check if the username and passwords are found in system users list, if not, the user is blocked. If the above statements are valid then user state change to online which means that the user logged-in the system.

The second schema is BUY (shown in figure 3) which checks if the user has enough balance to buy the product then the product price will be deducted from user balance. if not, the user is blocked, and the product will be made available. The first schema is LOGIN (shown in figure 2) and it checks if the username and passwords are found in system users list, if not, the user is blocked. If the above statements are valid then user state change to online which means that the user logged-in the system.
The second schema is BUY (shown in figure 3) which checks if the user has enough balance to buy the product then the product price will be deducted from user balance. If not, the user is blocked, and the product will be made available.

![Figure 3. LOGIN schema](image)

The third schema is RECHARGE (shown in figure 4) and its function is to recharge user balance with the entered amount of money.

![Figure 4. BUY schema](image)

The fourth schema is ALERT (shown in figure 5) which changes user status if the user performs suspicious activities.

![Figure 5. RECHARGE schema](image)

The fifth schema is LOGOUT (shown in figure 6) and its function to log-out the user from the system.

![Figure 6. ALERT schema](image)

7. CASE STUDY

To implement our specification, we used Amazon.com as an example of showing the importance of the proposed specification to improve and add security features. The case study starts with a user who doesn't have enough credit to buy a book. After several attempts made by the user to do the purchase, there might be a chance that the system accepts the transaction. This suspicious behaviour can identify the user intention to invalidate the buying steps in Amazon.com. In our specification we gave each user zero Alert_Point in the registration to the website. Then, incrementing the user's Alert_Point indicates performing suspicious operation in the system which enforces changing the status of the user from safe to suspicious, when user reaches a certain number in his Alert_Point he will be blocked. Consequently, the user will be forbidden from using the website for a period of time. This operation specifies and records suspicious behavior of the user. It also, prohibits him from breaking the rules of buying. As a result it assures the security of the system specifications.

8. CONCLUSION

In this paper, we proposed specifications for e-commerce secure system using Z language. Using formal methods to construct specifications for a secure e-commerce system that is capable to limit security threats, the result is promising for future expansions and elaborations.

Formal methods can be used to formally specify system requirements. This facilitates later activities related to specification checking for some requirements related to reliability,
security and some other quality attributes. This is particularly useful as those properties or specification checking can be implemented to be checked automatically during the occurrence of e-commerce transactions.

9. REFERENCES


