Andrii Vynokurov
Master Student,
Economic Cybernetics Department,
Taras Shevchenko National University,
Kyiv, Ukraine
prostofrukta@gmail.com

MANAGING CYBERSECURITY IN E-COMMERCE USING STRIDE, DOMAIN AND ISSRM MODELS

Introduction

The ease that an e-commerce system provides ensures that a large volume of customers will continue to use these systems with growing orders made electronically and delivery carried out with no geographical limitations. These systems enhance normal business flows as now, e-commerce transactions occur between businesses, customers, businesses and customers, and so on. A survey of customer's online shopping habits reveals that more than 5,000 customers will make at least two online purchases within a three-month period [1]. According to this survey, compared with a 47% purchases in 2014 and 48% in 2015, customers now carry out 51% of their purchases online [1]. With the advantage of the possibilities of online purchases, businesses which decide to choose the e-commerce option typically show a rise in sales [1]. However, the ease introduced by e-commerce solutions has also been accompanied by severe cyber threats to the system. Sensitive information is now being generated, collected, stored, transmitted, and manipulated on technologies and through processes that may not have adequate security capabilities. Customers now fear the loss of financial data and e-commerce systems fear the financial losses as well as other losses associated with security risks. With these security concerns, a consistent analysis of threats that pose security risks, as well as a continuous process into the treatment of these risks. This paper seeks to provide a structured and logically illustrated approach to continuous threat analysis and security risk management specific to the e-commerce domain. This approach will also facilitate participation between business professionals (who want to participate in a more effective way in building, using and managing e-commerce systems), and the IT professionals (who seek to work more effectively with the business professionals when building and maintaining their e-commerce systems).

The benefits of e-commerce encourage businesses to seek an e-commerce solution for transactions. Thus, e-commerce systems are increasingly being built and business sensitive assets are now used on technologies and processes that may not be secure. These technologies and processes pose threats, evolving over time, to the e-commerce system. As such, an enhancement to the procedure of following risk management is needed. This should allow for continuous threat analysis and management of the resulting risk, applicable for the phases of an e-commerce system development.

The purpose of this work is to verify models STRIDE, ISSRM and Domain models for their possibility to be used to carry out risk management in e-commerce systems.

Literature overview

This work is based on three main models, namely STRIDE, ISSRM and Domain models.

STRIDE is a model which was developed by Prarit Garg and Loren Kohnfelder at Microsoft in April of 1999 in a paper titled “The Threats to our Products”. Also we must emphasize that STRIDE is a mnemonic for the different types of vulnerabilities to a system under review: Spoofing, Tampering, Repudiability, Information Disclosure, Denial of Service, and Elevation of Privilege.

The STRIDE threat modeling, introduced by [3] which helps to find, recognize and model these threats on a system has been known to be easy to use, produce a significant number of threats for analysis and result in the relatively high number of the correctly determined security threats [2] and will be applied in this research to derive security threats in e-commerce systems. It is the responsibility of those performing threat modeling and analysis to discover and describe the threats and attack vectors, within the unique context of a system under analysis.

The use of the ISSRM methodology and its Domain Model for risk management and as a reference to the enhancement of risk management procedures is not a new topic, as there has been previous research works done on this. This work is based on the notion that ISSRM and its Domain Model is a reliable methodology that can be used in

a security risk management process and as a guiding reference when developing concepts that enhance the security risk management process.

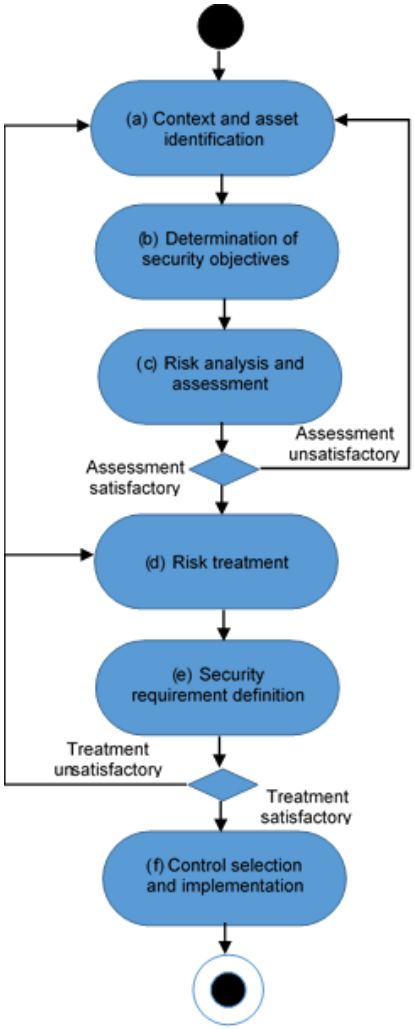

Figure 1: ISSRM Process [2]

Risks scenarios are developed from the existence of threat events having an impact on the concerned system. According to [4], in order to discuss threats in e-commerce, provided a model to analyze threat classification. Here threats were classified from two points of view: threat agents and threat techniques. In [2], a security threat is an event that is initiated by a threat agent using an attack method against one or more system assets by exploiting their vulnerabilities. Current attacks on e-commerce systems such as Webshops are similar to typical web applications. By exploring the attacker's perspective, the nature and existence of risks in the system can be analyzed. Also, proper defenses can only be established if the attack pattern or method can be predicted. The CAPEC's list of attack patterns [5] is a useful collection of specific attack patterns that result in threats relevant to the Webshop example and also to e-commerce systems. Out of the total attack patterns listed, nine relevant to e-commerce

systems were collated and categorized. These attack patterns also contain estimations on attack severity, the likelihood of exploitation, technical impact as a result of attack motivation-consequences and mitigation, helpful when carrying out risk measurement activities.

Results

This research work concentrated on only one type of e-commerce system which is the business-to-customer e-commerce system. As explained in the scope, there are other types of e-commerce systems not considered in this research work. We also concentrate on the order fulfilment process of a B2C e-commerce system which limits the business view of the applicability of the approach. The case-study used for this security risk management process was from a generalisation of the concepts of a standard e-commerce system following re-search on a of popularly used e-commerce systems.

Also, with the illustration of security metrics for risk treatment, it is acknowledged that such metrics are subjective and are highly business specific. The research work only provides a general estimation for risk metric values for its calculations.

The idea for this research work was guided by a main research question, “What procedure can be used to carry out risk management with a focus on evolving threats to e-commerce systems?” Thus, this research work used the ISSRM method and STRIDE approach in the identification of business context and assets for an e-commerce system, threat modelling, and risk analysis as well as the application of risk treatment procedures.

In carrying out security risk management, it can be seen that a meaningful continuous security risk assessments and treatment decisions in e-commerce systems be carried out in an unambiguous and clear manner using business-relevant terms and proffering mutual under-standing between IT and business stakeholders. This has been illustrated throughout this research work with the example of an order fulfilment management process for a Webshop case-study.

Conclusions

It was noticed that this approach is useful for the stages of the e-commerce system development cycle and following this approach allowed the introduction of new requirements and the improvement of old requirements to the system depending on the phase of development. With the use of risk measurement procedures, risk reduction levels can be estimated and help with risk treatment decisions provided from a trade-off analysis on the resulting risk metric estimations. It can be summarized that this approach to security risk management is a relevant approach towards a continuous security risk management cycle with emphasis on the evolving threats posed on e-commerce systems.

References

1. Fortune. Consumers Are Now Doing Most of Their Shopping Online. 2018 [An electronic resource]. – URL: http://fortune.com/2016/06/08/online-shopping-increases/
2. Matulevičius R., Fundamentals of Secure System Modelling. Cham: Springer, 2017.
3. Shostack A., Threat modeling: Designing for Security. Indianapolis: Wiley, 2014.
4. Yanyan W., “Research on e-commerce Security based on Risk Management Perspective”, International Journal of Security and Its Applications, vol.8, No.3, pp. 153-162, 2014.
5. Capec.mitre.org. "CAPEC - CAPEC List Version 2.11." 2018. 2018 [An electronic resource]. – URL: https://capec.mitre.org/data/index.html
6. Tsoumas B., Papagiannakopoulos P., Dritsas S., Gritzalis D., Security-by-ontology: A Knowledge-centric Approach. In: Boston, S. (ed.) Security and Privacy in Dynamic Environments. pp. 99–110, 2006.
7. Turban E., Volonino L., McLean E., and Wetherbe J., Information Technology for Management: Transforming Organisations in the Digital Economy, the seventh International student edition. Hoboken, NJ: Wiley, 2010
8. Iso.org. 2018 [Електронний ресурс] Режим доступу: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en:term:3.1
9. Msdn.microsoft.com, "The STRIDE Threat Model", 2018. [Електронний ресурс] Режим доступу: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx.