MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică şi Microelectronică
Departamentul Ingineria Software și Automatică

Admis la susţinere
Şef departament:
FIODOROV Ion dr., conf.univ.

„___” _____2024

ANALIZA PROBLEMELOR DE SECURITATE ÎN SISTEME ELECTRONICE DE PLATĂ

Proiect de master

Student: _____ **Semeniuc Eric, SI-211M**

Coordonator: _____ **Ion Bolun, prof. univ.**

Consultant: _____ **Rodica Bulai, asist.univ.**

Chişinău, 2024

REZUMAT

la teza de master „Analiza problemelor de securitate în sisteme electronice de plată” a masterandului din grupa SI-211M, programul de studii „Securitatea informațională”,
Semeniuc Eric

Teza de cercetare de master propusă analizează problemele de securitate în sisteme electronice de plată. Lucrarea cuprinde introducerea, patru capitole, concluzii și bibliografia.

În primul capitol, de explorează evoluția sistemelor de plată de la tranzacțiile cash la cele electronice, evidențiind schimbările semnificative în comportamentul financiar al utilizatorilor. Se analizează creșterea utilizării cardurilor bancare și a plăților online, subliniind importanța facilității și rapidității în procesul de plată. De asemenea, se examinează diverse categorii de sisteme electronice de plată, precum eCash, eCheque, carduri inteligente și plăți online, oferind o perspectivă comprehensivă asupra evoluției tehnologiei de plată.

Al doilea capitol aduce în prim-plan impactul negativ al fraudelor și atacurilor asupra utilizatorilor și companiilor în contextul sistemelor electronice de plată. Se subliniază esențialul încredere a utilizatorilor și reputația instituțiilor financiare, evidențiind necesitatea unei securități solide în sistemele de plată electronice. De asemenea, sunt analizate diverse amenințări precum furtul de identitate, clonarea cardurilor și insuficienta educație a utilizatorilor. Capitolele ulterioare explorează mecanisme de autentificare și strategii de securitate în detaliu.

În al treilea capitol, se propun soluții și tehnologii avansate pentru a aborda provocările și riscurile asociate sistemelor electronice de plată. Sunt analizate metode precum SSL/TLS, hashing, criptare cu curbe eliptice, semnături digitale, firewall-uri, tehnologii biometrice și implementarea inteligenței artificiale în prevenirea fraudelor. Importanța actualizărilor continue pentru remedierea vulnerabilităților cunoscute este, de asemenea, evidențiată..

În ultimul capitol, se examinează studii de caz cu privire la atacuri notorii asupra sistemelor de plată electronice, cum ar fi atacul asupra Equifax sau atacul ransomware WannaCry. Totodată, sunt prezentate modele de succes, precum modelul de securitate cibernetică al Estoniei sau programele de recompensare ale unor companii precum Google și Microsoft, subliniind importanța investițiilor în securitatea cibernetică. Concluziile finale evidențiază importanța continuă a securității și inovării în evoluția sistemelor electronice de plată.

ABSTRACT

for the master's thesis "Analysis of Security Issues in Electronic Payment Systems" authored by Eric Semeniuc, a graduate student from the SI-211M group, enrolled in the "Information Security" study program

In the first chapter, the evolution of payment systems from cash transactions to electronic ones is explored, highlighting significant changes in user financial behavior. The increase in the use of bank cards and online payments is analyzed, emphasizing the importance of convenience and speed in the payment process. Additionally, various categories of electronic payment systems, such as eCash, eCheque, smart cards, and online payments, are examined, providing a comprehensive perspective on the evolution of payment technology.

The second chapter focuses on the negative impact of fraud and attacks on users and companies within electronic payment systems. It emphasizes the essential trust of users and the reputation of financial institutions, highlighting the need for robust security in electronic payment systems. Various threats, including identity theft, card cloning, and inadequate user education, are also analyzed. Subsequent chapters delve into authentication mechanisms and security strategies in detail.

The third chapter proposes advanced solutions and technologies to address challenges and risks associated with electronic payment systems. Methods such as SSL/TLS, hashing, elliptic curve cryptography, digital signatures, firewalls, biometric technologies, and the implementation of artificial intelligence in fraud prevention are analyzed. The importance of continuous updates to address known vulnerabilities is also emphasized.

In the final chapter, case studies of notorious attacks on electronic payment systems, such as the Equifax breach and the WannaCry ransomware attack, are examined. Successful models, such as Estonia's cybersecurity model, and reward programs from companies like Google and Microsoft, underscore the importance of investments in cybersecurity. The concluding remarks highlight the ongoing importance of security and innovation in the evolution of electronic payment systems.

CUPRINS

INTRODUCERE

În era digitală în care trăim astăzi, sistemele electronice de plată au devenit fundamentale pentru modul în care societatea gestionează tranzacțiile financiare. De la simpla utilizare a cardurilor bancare până la tehnologii avansate de criptomonede, modul în care oamenii plătesc pentru bunuri și servicii s-a schimbat radical. Odată cu această evoluție, însă, au apărut și provocări semnificative în ceea ce privește securitatea acestor sisteme. Analiza problemelor de securitate în sistemele electronice de plată devine astfel esențială pentru înțelegerea amenințărilor cu care ne confruntăm și pentru identificarea unor soluții eficiente.

Cu tot mai mulți oameni renunță la utilizarea banilor fizici în favoarea cardurilor bancare și a plăților online, comoditatea și rapiditatea devin criterii decisive în alegerea metodei de plată. Această schimbare a adus cu sine beneficii semnificative, precum eficiența sporită și accesibilitatea crescută la serviciile financiare, însă a generat și o creștere concomitentă a riscurilor asociate securității.

Importanța securității în domeniul plăților electronice devine evidentă atunci când privim consecințele negative ale fraudelor și atacurilor cibernetice asupra utilizatorilor și instituțiilor financiare. Pierderile financiare și impactul asupra încrederii consumatorilor reprezintă doar vârful aisbergului, având în vedere că există implicații mai adânci în ceea ce privește protecția datelor personale și integritatea sistemelor financiare. În acest context, securitatea devine nu doar un aspect tehnic, ci o componentă esențială a încrederii în întregul ecosistem al plăților electronice.

Tipurile diverse de sisteme electronice de plată, de la cardurile bancare și plățile online până la portofelele electronice și tehnologiile blockchain, aduc cu sine amenințări specifice. Fraudele cu carduri bancare, atacurile de tip phishing și malware, vulnerabilitățile în procesele de autentificare și autorizare, precum și riscurile asociate cu tehnologiile fără contact reprezintă doar câteva exemple ale provocărilor cu care se confruntă aceste sisteme. Este esențial de înțeles în profunzime aceste amenințări pentru a putea dezvolta și implementa măsuri de securitate eficiente.

Măsurile de securitate în sistemele electronice de plată sunt variate și complexe, de la criptarea datelor și securitatea canalelor de comunicare până la autentificarea puternică a utilizatorilor și monitorizarea tranzacțiilor suspecte. Protejarea împotriva fraudelor necesită nu doar tehnologii avansate, ci și o abordare holistică care să includă educația utilizatorilor, actualizări regulate ale software-ului și conformitatea cu standardele de securitate din industrie, cum ar fi PCI DSS.

Reglementările și standardele în domeniul securității plăților electronice au un rol crucial în asigurarea unui cadru coerent și eficient. Agențiile guvernamentale și organismele de reglementare joacă un rol important în supravegherea și implementarea acestor reguli, iar conformitatea cu standardele recunoscute devine un criteriu esențial pentru instituțiile financiare. Colaborarea între sectorul public și cel privat este, astfel, esențială pentru a asigura un mediu de plată electronic sigur și robust.

Pe parcursul acestei analize, se va explora mai detaliat amenințările specifice, măsurile de securitate, reglementările existente și tendințele viitoare în domeniul plăților electronice.

Studii de caz și exemple practice vor ilustra modul în care aceste aspecte se manifestă în practică, evidențiind atât riscurile cât și soluțiile de succes implementate de anumite organizații. În final, se va face concluzii asupra importanței continue a inovării și adaptabilității în asigurarea securității într-un mediu digital în continuă schimbare.

BIBLIOGRAFIE

1. Security Issues and Solutions in E-Payment Systems, © 2023 Disponibil: https://www.academia.edu/50958612/Security_Issues_and_Solutions_in_E_Payment_Syste
2. The History and Future of Payment Trends, © 2023.Disponibil: The History and Future of Payment Trends (icterra.com)
3. Fourcan, KM, Isear, J. și Utpal, KD (2015). Securitate în tranzacțiile de plată electronică. Jurnalul Internațional al Cercetare științifică și inginerie, 6(2), 955-960.
4. Hassan, MA, Zarina, S., Mohammad, KH și Ahmed, SA-K. (2020). O revizuire a securității plăților electronice. Disponibil: https://doi.org/10.3390/sym12081344
5. Rachna. (2013). Problema și provocările sistemelor electronice de plată.Jurnalul Internațional de Cercetare în Management și Farmacie.
6. Sana, K. și Shreya, J. (2018). Un studiu privind utilizarea plății electronice pentru creșterea durabilă a afacerilor online
7. Atacurile Cibernetice Sunt O Problemă Pentru Fiecare, © 2023.Disponibil: » Atacurile cibernetice sunt o problemă pentru fiecare (cert.md)
8. 143 milioane de clienţi ai companiei de analiză de credit Equifax, expuşi în urma unui atac cibernetic de proporţii. Disponibil: https://www.agerpres.ro/cybersecurity/2017/09/08/sua-143-milioane-de-clienti-ai-companiei-de-analiza-de-credit-equifax-expusi-in-urma-unui-atac-cibernetic-de-proportii-13-31-57
9. Sistemul SWIFT atacat de malware-ul folosit în jefuirea Băncii Centrale din Bangladesh. Disponibil: https://epochtimes-romania.com/news/sistemul-swift-atacat-de-malware-ul-folosit-in-jefuirea-bancii-centrale-din-bangladesh---246776
10. What was the WannaCry ransomware attack?. Disponibil: https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/
11. The 2011 PlayStation Network Hack – What Actually Happened?. Disponibil: https://wsswired.com/4837/entertainment-3/the-2011-playstation-network-hack-what-actually-happened/
12. E-Estonia Programme for Cyber Security. Disponibil: https://e-estonia.com/programme/cyber-security/#:~:text=Government%20Cyber%20Security%20Strategy&text=This%20cybersecurity%20strategy%20for%202019,activity%20planning%20and%20resource%20allocation.