Universitatea Tehnică a Moldovei

Proiectarea dispozitivelor IoT cu elemente de securizare Hardware și software

Student: **Baciu Eugeniu**

Coordonator: **Sudacevschi Viorica, Conf. Univ., dr. în științe tehnice**

Chișinău, 2022

Adnotare

La teza de master cu tema "Proiectarea dispozitivelor IoT cu elemente de securizare hardware și software" **a st. gr. CRI-201M, Baciu Eugeniu**

Scopul tezii: Teza de master are drept scop cercetarea, analiza tehnologiei IoT, cu accent pe rețele și securitate, și impactul ei asupra societății. Sinteza cunoștințelor acumulate și proiectarea, realizarea unui dispozitiv IoT și mediului pentru automatizarea și eficientizarea activităților casnice pentru utilizatorii finali. Accentul este pus pe asigurarea confortului și securității la utilizarea dispozitivului și serviciilor din rețea.

Cuvintele cheie: Internet of Things, rețea locală, securitate, arhitectură, reverse proxy, smart kettle, virtulizare, criminalitate informatică, proiectare, IDS/IPS, proiectare, web server, senzor, acutator, algoritm PID

Tehnologii utilizate: La elaborarea rețelei și dispozitivului au fost utilizate tehnologiile: virtualizarea, pentru desfășurarea mai multor servicii pe un echipament; port knocking și ssh pentru asigurarea accesuli securizat la echipamente; vlan, pentru o gestionare și securizare comunicării în rețea, etc.

Memoriu explicativ: Introducere, 4 capitole, concluzii, 26 figuri, un tabel, fără anexe, 21 surse bibliografice, 51 pagini text de bază.

Capitolul I: Primul capitol este dedicat analiza domeniul propus pentru studiu. În cadrul acestui capitol au fost studiate conceptele fundamentele despre tehnologia IoT și rețele unde se aplică nemijlocit dispozitivele IoT, precum și dispozitivele deja existene. Au fost asemenea atins subiectul despre evoluția dispozitivelo IoT și impactul criminalității cibernetice, atingînd date din statistici curente.

Capitolul II: Al doilea capitol a fost destinat stabilirii cerințelor funcționale și non-funcționale și modelării, proiectării dispozitivului și rețelei unde va fi plasat dispozitivul. A fost decrisă arhitectura fizică și logică a dispozitivului, rețelei. Prin intermediul diagramelor a fost descrisă procesele și interacțiunea componentelor.

Capitolul III: În capitolul 3 au fost studiate și identificate tehnologiile, aplicațiile, componentele și echipamente care vor fi în stare să corespundă arhitecturii și cerințelor înaintate pentru rețea și dispozitiv IoT.

Capitolul IV: Modul cum a fost realizat dispozitivul IoT, rețeaua, după modele elaborate și descrise în capitolul III. A fost descris cum au fost implementate tehnologiile descrise în capitolul III.

ANNOTATION

For the master thesis "Design of IoT devices with hardware and software security features"

The purpose of the thesis: The master's thesis aims at research, analysis of IoT technology, with a focus on networking and security, and its impact on society. Synthesis of accumulated knowledge and design, realization of an IoT and environment device for automation and efficiency of household activities, for end users. Emphasis will be placed on ensuring comfort and security when using the device and network services.

Keywords: Internet of Things, local area network, security, architecture, reverse proxy, smart kettle, virtualization, cybercrime, design, IDS / IPS, design, web server, sensor, accelerator, PID algorithm

Technologies applied: The technologies were used to develop the network and the device: virtualization, for performing several services on one piece of equipment; port knocking and ssh to ensure secure access to equipment; vlan, for managing and securing network communication, etc.

Thesis structure: Introduction, 4 chapters, conclusions, 26 figures, a table, no appendices, 21 bibliographic sources, 51 pages of basic text.

Chapter I: The first chapter is dedicated to the analysis of the field proposed for the study. In this chapter, we have studied the basic concepts of IoT technology and networks where IoT devices are directly applicable, as well as existing devices. The topic of the evolution of IoT devices and the impact of cybercrime was also addressed, reaching data from current statistics.

Chapter II: Second chapter is intended to establish functional and non-functional requirements, modeling, design of the device and the network where the it will be placed. The physical, logical architecture of the device, the network, was described. The diagrams describe the processes and interaction of the components.

Chapter III: Chapter 3 examines and identifies the technologies, applications, components, and equipment that will be able to meet the advanced architecture and requirements for the IoT network and device.

Chapter IV: It was described how the technologies described in Chapter III were implemented. How the IoT device was made, the network, according to models developed and described.

CUPRINS

INTRODUCERE

Domeniul tehnologiilor informaționale(TI) se află într-o dezvoltarea intensă pe parcursul ultimelor decenii, generând un impact imens asupra componentelor societății umane. Soluțiile din acest domeniu au devenit o normă și un element de bază al societății.

Unul din motivele evoluției și aplicării tot mai active a TI în viața omului este necesitatea și dorința omului de a își ușura activitățile și de a le realiza cu o eficacitate mai mare. Actualmente, un exemplu poate servi dispozitivele internet of things IoT. Ele își aduc aportul prin automatizarea și monitorizarea diferitor procese de producere în industrii, securitate, agricultură, business procese, etc.

Odată ce aceste au cucerit toate sferele de activitate a omului ele au început să apară tot mai activ și în viața de zi cu zi a omului. Manifestându-se prin diferite obiecte inteligente: ceasuri, becuri, prize, obiecte de uz casnic inteligente, etc. Menirea lor este de a ușura activitățile obișnuite, de zi cu zi a persoanei, permițând să fie accesate chiar și la distanță.

Iar astfel de cazuri cum ar fi căderea unor servicii globale, de exemplu a rețelelor de socializare ce a avut loc recent, ce slăbește încrederea în serviciile online. Și în scurt timp mulți utilizatori pot să-și treacă serviciile local ca să fie accesate de acasă.

Cu toate acestea s-a observat că în ultimii ani, în timp ce soluțiile TI oferă beneficii esențiale, de asemenea, ele sunt și vulnerabile. Incidentele legate de crime cibernetice, intenționate sau neintenționate, sunt în creștere și afectează negativ asupra diferitor sectoare cheie a societății în special asupra domeniului economic.

Astfel pe lângă aportul său important, dispozitivele IoT au și minus pentru securitate fiind ținta suplimentară pentru infractori cibernetici. Este greu de imaginat consecințele, dacă prin intermediul unui dispozitiv IoT se poate compromite o stație de electroenergie, infrastructura de transporturi, bănci, etc. Consecințele pot fi catastrofale nu doar pentru clienți dar pentru state și întreaga lume.

Dispozitivele IoT prezintă pericol și pentru utilizare personală, în apartament, casă. Răufăcătorii având acces la camera video, un calorifer electric, etc. pot atât să jefuiască o casă, cât și să provoace un incendiu. Deja acest fapt nu este noutate, sunt suficiente exemple cu compromiterea camerelor ip sau pentru urmărirea copiilor, stațiilor radio pentru bebeluși, etc.

Ultimele evenimente care au cutreierat lumea, pandemia, a provocat trecerea angajaților la lucru de la distanță și utilizarea preponderentă a diferitor servicii online. Un scenariu clasic, poate deveni ingineria socială prin intermediul dispozitivului IoT. Atacând prin dispozitiv IoT angajatul, ce lucrează de acasă, se poate obține acces la rețeaua în care el se află și la stația de la lucru. Ca urmare poate fi compromisă și întreprinderea la care el lucrează.

BIBLIOGRAFIE

1. Gillis, Alexander (2021). "What is internet of things (IoT)?". IOT Agenda. Retrieved 17 August 2021.
2. "CORRECTING THE IOT HISTORY". CHETAN SHARMA. 14 March 2016. Retrieved 1 June 2021.
3. Stallings, William (2016). Foundations of modern networking: SDN, NFV, QoE, IoT, and Cloud. Florence Agboma, Sofiene Jelassi. Indianapolis, Indiana. ISBN 978-0-13-417547-8. OCLC 927715441.
4. „State of IoT 2021: Number of connected IoT devices growing 9% to 12.3billion globally, cellular IoT now surpassing 2 billion" [online]. [citat 30 octombrie 2021] Disponibil: https://iot-analytics.com/number-connected-iot-devices/
5. "Over $100 Billion Invested in Driverless Technology" [online]. [citat 12 noiembrie 2021] Disponibil: https://www.leasingoptions.co.uk/driverless-cars/index.html#investments
6. "NOKIA Threat Intelligence Report 2020" [online]. [citat 4 septembrie 2021] Disponibil: https://onestore.nokia.com/asset/210088
7. "2020 Unit 42 IoT Threat Report Palo alto networks unit42" [online]. [citat 8 august 2021] Disponibil: https://iotbusinessnews.com/download/white-papers/UNIT42-IoT-Threat-Report.pdf
8. "Dozens sue Amazon's Ring after camera hack leads to threats and racial slurs" [online]. [citat 19 aprilie 2021] Disponibil: https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats
9. "Bitdefender BOX" [online]. [citat 4 decembrie 2021] Disponibil: https://www.bitdefender.ro/box/
10. "Smart Kettle Module" [online]. [citat 25 iulie 2021] Disponibil: https://courses.engr.illinois.edu/ece445/getfile.asp?id=18730
11. "Smart cup/kitchen kettle IoT device" [online]. [citat 3 noiembrie 2021] Disponibil: https://www.encata.net/projects/smart-cup-kitchen-kettle-iot-device
12. "ESXi Arm Edition" [online]. [citat 22 octombrie 2021] Disponibil: https://flings.vmware.com/esxi-arm-edition
13. "Water Heating Time Calculator" [online]. [citat 19 decembrie 2021] Disponibil: https://gettopics.com/en/calc/water-heating-time?tsusid=bl1wht
14. "Introduction to the Consumer Internet of Things (CIoT)" [online]. [citat 5 mai 2021] Disponibil: https://www.i-scoop.eu/internet-of-things-iot/what-is-consumer-internet-of-things-ciot/
15. "The 5 worst examples of IoT Hacking and Vulnerabilities in Record History" [online]. [citat 14 iunie 2021] Disponibil: https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities
16. "IoT Security Breaches: 4 Real-World Examples" [online]. [citat 20 iulie 2021] Disponibil: https://www.conosco.com/blog/iot-security-breaches-4-real-world-examples/
17. "2021 Cyber Security Statistics the Ultimate List Od Stats, Data & Trends" [online]. [citat 4 decembrie 2021] Disponibil: https://purplesec.us/resources/cyber-security-statistics/
18. "THE BASIC ELEEMENTS OF IOT" [online]. [citat 18 august 2021] Disponibil: https://spgcontrols.com/zh/elements-of-iot-2/
19. "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey" [online]. [citat 28 decembrie 2021] Disponibil: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6165453/
20. "Internet of Things: Architectures, Protocols and Applications" [online]. [citat 2 septembrie 2021] Disponibil: https://www.hindawi.com/journals/jece/2017/9324035/
21. "IoT Architecture: The Pathway from Physical Signals to Business Decisions" [online]. [citat 1 decembrie 2021] Disponibil: https://www.altexsoft.com/blog/iot-architecture-layers-components/