Universitatea Tehnică a Moldovei

SISTEM SECURIZAT DE COMUNICARE ÎN REȚELE WIRELESS

Masterand:

Călugărescu Nicolae,

Gr. CRI - 181

Conducător:

Prof.univ.,dr.hab. Guțuleac Emilian

Chișinău – 2019

ADNOTARE

La teza de master „Sistem securizat de comunicare în rețele Wireless”, elaborat de Călugărescu Nicolae, Chișinău, 2019.

Cuvinte cheie: Model OSI, rețea, pachet de date, securitate, VPN, trafic de rețea, Wireshark, algoritm de criptare, AES, Android.

Teza de master face parte din domeniul securității rețelelor de comunicații. Scopul lucrării este dezvoltarea unui sistem securizat care permite transmiterea și recepționarea corespondenței electronice cu informații sensibile printr-un mediu sigur și izolat de rețeaua globală Internet. Analizele efectuate se încadrează în politica statului Republicii Moldova care menționează importanța realizării a mai multor strategii, programe şi politici de ţară pentru dezvoltarea societăţii informaţionale la nivel naţional, deoarece creșterea numărului de utilizatori ai Internetului şi evoluţiile tehnologiilor informaţionale conexe creează provocări substanţiale în ceea ce privește starea mediului de securitate, ordinea publică şi apărarea, prevenirea criminalităţii şi aplicarea legii în direcţia protecţiei drepturilor în spaţiul informațional.

Conexiunea la Internet reprezintă o oportunitate, dar creează de cele mai multe ori probleme de securitate pentru rețelele de comunicații. Politica de securitate este cea care, pe baza analizei de securitate a unei rețele, exprimă cel mai bine principiile care stau la baza adoptării unei anumite strategii de securitate, implementată prin diverse măsuri specifice cu tehnici și protocoale adecvate.

În teza de master s-a efectuat analiza cadrului legislativ și situația la moment în acest domeniu, s-a studiat conceptul ce se referă la securitatea, integritatea, confidenţialitatea şi disponibilitatea informației. S-a studiat dinamica tehnologiei informației ce induce noi riscuri pentru care organizaţiile trebuie să implementeze noi măsuri de control din motiv că lucrul în reţea şi conectarea la Internet induc şi ele riscuri suplimentare, de acces neautorizat la date sau chiar frauda.

Teza de master include: introducere, 3 capitole de bază, concluzii generale și recomandări și lista de surse bibliografice.

Capitolul 1 al tezei de master definește politicile de securitate a rețelelor comunicaționale și generalitățile sistemului de operare Android.

Capitolul 2 prezintă tehnologiile utilizate la elaborarea sistemului. Aici s-au ales tipurile de control a accesului în sistem, metoda și algoritmul de criptare și sistemul de operare pentru dezvoltarea aplicației.

Capitolul 3 prezintă proiectarea în detaliu a sistemului securizat de comunicare.

ANNOTATIONS

On the Master thesis "Secure communication system", elaborated by Călugărescu Nicolae, Chisinau, 2019.

Keywords: OSI model, network, data packet, security, VPN, network traffic, Wireshark, encryption algorithm, AES, Android.

The master's thesis is part of the field of communications network security. The purpose of the paper is the development of a secure system that allows the transmission and reception of electronic mail with sensitive information through a secure environment and isolated from the global Internet network. The designs carried out fall within the policy of the state of the Republic of Moldova, which mentions the importance of implementing several strategies, programs and country policies for the development of the information society at national level, the public order and the defense, the prevention of crime and the application of the law in the direction of the protection of rights in the information space.

The Internet connection is an opportunity, but most of the time it creates security problems for the communications networks. Security policy is the one that, based on the security analysis of a network, best expresses the principles underlying the adoption of a certain security strategy, implemented through various specific measures with appropriate techniques and protocols.

In the master's work, the analysis of the legislative framework and the situation at the moment in this field was performed, the concept regarding the security, integrity, confidentiality and availability of information was studied. The dynamics of information technology has been studied, which induces new risks for which organizations have to implement new control measures, because the work in the network and Internet connection also lead to additional risks, unauthorized access to data or even fraud.

The master's thesis includes: introduction, 3 basic chapters, general conclusions and recommendations and the list of bibliographic sources.

Chapter 1 of the Master's thesis defines the security policies of the communication networks and the generalities of the Android operating system.

Chapter 2 presents the technologies used to develop the system. Here, the types of access control in the system, the encryption method and algorithm and the operating system for the application development were chosen.

Chapter 3 presents the detailed design of the secure communication system.

CUPRINS

INTRODUCERE

Rețelele de comunicații reprezintă o realitate cotidiană pentru fiecare dintre noi indiferent de vîrstă, în toate domeniile de activitate (comercial, financiar-bancar, administrativ, educational, medical, militar, etc.), dar și în mediul familial.

Fără a depinde de mediul fizic prin care se realizează (cablu metalic, fibră optică sau mediul wireless) sau de specificul rețelei de transmisie a informațiilor (de PC, de telefonie fixă sau mobilă, de televiziune prin cablu, de distribuție a energiei electrice), securitatea comunicațiilor reprezintă un aspect esențial al serviciilor oferite, fiind critică în cazul informațiilor cu caracter secret din aplicații financiar-bancare, militare, guvernamentale și nu numai aceasta [2].

Conexiunea la Internet reprezintă o oportunitate, dar creează de cele mai multe ori probleme de securitate pentru rețelele de comunicații.

Se identifică mai multe aspecte ale securității unei rețele (securizarea accesului fizic și logic, securitatea serviciilor de rețea, secretizarea informațiilor) care se exprimă prin diverși termeni de specifici: autentificare, autorizare, asociere cu un cond de utilizator, confidențialitate, robustețe [2].

Politica de securitate este cea care, pe baza analizei de securitate a unei rețele, exprimă cel mai bine principiile care stau la baza adoptării unei anumite strategii de securitate, implementată prin diverse măsuri specifice cu tehnici și protocoale adecvate.

Securitatea informaţiei este un concept mai larg care se referă la asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei. Dinamica tehnologiei informaţiei induce noi riscuri pentru care organizaţiile trebuie să implementeze noi măsuri de control. De exemplu, popularizarea unităţilor de inscripţionat CD-uri sau a memoriilor portabile de capacitate mare, induce riscuri de copiere neautorizată sau furt de date.

Lucrul în reţea şi conectarea la Internet induc şi ele riscuri suplimentare, de acces neautorizat la date sau chiar frauda.

Dezvoltarea tehnologică a fost acompaniată şi de soluţii de securitate, producătorii de echipamente şi aplicaţii incluzând metode tehnice de protecţie din ce în ce mai performante. Totuşi, în timp ce în domeniul tehnologiilor informaţionale schimbarea este exponenţială, componenta umană rămâne neschimbată. Asigurarea securităţii informaţiilor nu se poate realiza exclusiv prin măsuri tehnice, fiind în principal o problemă umană.

Majoritatea incidentelor de securitate sunt generate de o gestiune şi organizare necorespunzătoare, şi mai puţin din cauza unei deficienţe a mecanismelor de securitate.

Este important ca organizaţiile să conştientizeze riscurile asociate cu utilizarea tehnologiei şi gestionarea informaţiilor şi să abordeze pozitiv acest subiect printr-o conştientizare în rândul angajaţilor a importanţei securităţii informaţiilor, înţelegerea tipologiei ameninţărilor, riscurilor şi vulnerabilităţilor specifice mediilor informatizate şi aplicarea practicilor de control [2, 4].

Tehnologiile informaționale, resursele de informare şi sistemele de comunicare electronică au devenit parte indispensabilă a tuturor domeniilor de activitate ale persoanei, societății și statului. Prin dezvoltarea lor accelerată, tehnologiile informaţionale contribuie la transformări sociale de esenţă, fiind un generator pentru apariţia şi consolidarea societăţii informaţionale de nivel naţional, regional şi internaţional, depăşind cadrul juridic al frontierelor de stat sau al comunităţilor de state.

Tehnologiile informaţionale generează modificări ale dimensiunii de informare şi comunicare, care se transformă în ritm accelerat într-o platformă multimedia, fiind dezvoltate noi componente şi mijloace de comunicare on-line şi off-line, iar libera circulaţie a informaţiilor şi ideilor la nivel local, regional şi global devin un imperativ pentru crearea şi promovarea unei societăţi informate într-un stat democratic şi de drept.

Pe lîngă beneficiile incontestabile ale tehnologiei moderne, spaţiul informaţional este supus unui șir de vulnerabilități, riscuri şi ameninţări de securitate, facilitînd competiţia injustă, confruntarea şi spionajul, dezinformarea şi propaganda, terorismul şi criminalitatea, iar încălcările de confidenţialitate determină răspîndirea de noi forme de ură şi incitare la violenţă, în special pe criterii de gen, rasă, naţionalitate, origine etnică, limbă, religie, apartenenţă politică sau pe orice alte criterii, care rămîn subestimate şi rareori remediate sau contracarate.

Crimele cibernetice, spionajul, propaganda, diversiunea şi exploatarea excesivă a datelor cu caracter personal prin reţelele de comunicaţii electronice sunt utilizate ca instrumente de bază la toate etapele de concepere a unei ameninţări hibride de securitate şi cheamă la un răspuns colectiv şi reglementat, bazat pe mecanisme şi acţiuni coordonate, de implementare a politicilor din domeniu, asistenţă tehnică şi legală din perspectiva imperativelor de securitate, orientat spre crearea unui mediu informaţional favorabil şi sigur pentru cetăţean, pentru mediul de afaceri de orice nivel şi pentru stat.

Creşterea numărului de utilizatori ai Internetului şi evoluţiile tehnologiilor informaţionale conexe creează provocări substanţiale în ceea ce privește starea mediului de securitate, ordinea publică şi apărarea, prevenirea criminalităţii şi aplicarea legii în direcţia protecţiei drepturilor în spaţiul informațional.

Pe parcursul ultimului deceniu, Republica Moldova a realizat mai multe strategii, programe şi politici de ţară pentru dezvoltarea societăţii informaţionale la nivel naţional, în conformitate cu recomandările forurilor europene şi internaţionale din domeniul tehnologiilor informaționale și comunicaţiilor electronice, al drepturilor şi libertăţilor fundamentale ale omului în mediile on-line şi off-line.

Potrivit raportului anual cu privire la monitorizarea evoluției societății informaționale la nivel mondial „Measuring the Information Society 2017”, lansat de către Uniunea Internațională a Telecomunicațiilor, Republica Moldova este plasată pe locul al 59-lea din cele 176 de state incluse în clasament. La nivel european, Republica Moldova a avansat față de media globală și din regiune, fiind printre primele 10 state cu cele mai dinamice evoluții la nivel mondial1 . Sunt implementate ori sunt în proces continuu de dezvoltare peste 21 de programe2 şi proiecte on-line de infrastructură şi servicii publice digitale, sunt lansate strategii sectoriale în domeniul tehnologiei informației şi politici de modernizare tehnologică a guvernării [1, 3, 4, 7].

Indiferent de forma pe care o îmbracă, mijloacele prin care este memorată, transmisă sau distribuită, informaţia trebuie protejată. ISO/IEC 17799 (Cod de bună practică pentru managementul securităţii informaţiei) tratează securitatea informaţiilor prin prisma a trei elemente principale:

- Confidenţialitatea – informaţiile sunt accesibile doar persoanelor autorizate;
- Integritatea – asigurarea acurateţei şi completitudinii metodelor prin care se realizează prelucrarea informaţiilor;
- Disponibilitatea – utilizatorii autorizaţi au acces la informaţii şi la activele asociate în momente oportune.

Pentru a putea realiza un program de securitate eficient este nevoie de politici, proceduri, practici, standarde, descrieri ale sarcinilor şi responsabilităţilor de serviciu, precum şi de o arhitectură generală a securităţii.

Aceste controale trebuie implementate pentru a se atinge obiectivele specifice ale securităţii şi pe cele generale ale organizaţiei.

Dependenţa din ce în ce mai mare de sistemele informaţionale conduce la creşterea tipologiei vulnerabilităţilor cărora organizaţiile trebuie să le facă faţă. Mai mult, problema protecţie trebuie să aibă în vedere de multe ori interconectarea reţelelor private cu serviciile publice. Dacă la acest aspect mai adăugam şi problema partajării informaţiilor se conturează un tablou destul de complicat în care implementarea unor controale eficiente devine o sarcină dificilă pentru specialistul IT&C.

Multe din sistemele existente pe piaţă au fost proiectate după metodologia structurată dar nu au avut ca principal obiectiv şi asigurarea unui anumit grad de securitate pentru că la momentul respectiv tehnologia nu era atât de dezvoltată şi nici atât de accesibilă neiniţiaţilor. Odată însă cu proliferarea Internetului ca şi mijloc important al comunicării moderne nevoia unor mecanisme de securitate proactivă a devenit o certitudine. În practică remarcăm că multe instituţii apelează la soluţii tehnice externe care să le rezolve problemele de securitate fără a căuta să-şi identifice nevoile şi cerinţele specifice.

Identificarea controalelor interne care să asigure un grad corespunzător de securitate activelor informaţionale ale unei instituţii presupune o planificare riguroasă şi identificarea exactă a obiectivelor respectivei instituţii. Pentru a fi însă eficiente aceste controale trebuie să aibă în vedere pe toţi angajaţii şi nu doar pe cei din compartimentul IT sau care au legătură directă cu acest domeniu.

Securitatea informaţiilor nu este doar o problemă tehnică. Ea este în primul rând o problemă managerială.

Standardul de securitate ISO/IEC 17799 răspunde nevoilor organizaţiilor de orice tip, publice sau private, printr-o serie de practici de gestiune a securităţii informaţiilor.

Standardul poate fi folosit în funcţie de gradul de expunere a fiecărei organizaţii în parte, pentru a conştientiza la nivelul conducerii aspectele legate de securitatea informaţiei, sau pentru a crea o cultură organizaţională în ceea ce priveşte securitatea informaţiilor, sau pentru a obţine certificarea sistemului de securitate.

Gradul de expunere a sistemelor informaţionale variază cu industria în care activează fiecare organizaţie. Cu cât acest risc este mai mare, atenţia care trebuie acordată securităţii datelor ar trebui să fie mai mare.

Instituţiile financiare, industria apărării, aerospaţială, industria tehnologiei informaţiei, industria electronică sunt sectoarele cu cel mai mare grad de risc în ceea ce priveşte securitatea informaţiilor. Tot în această categorie de risc ridicat intră şi instituţiile guvernamentale, motiv pentru care adoptarea unei culturi organizaţionale pe baza standardului ISO/IEC 17799 are un rol fundamental [2, 3, 4].

Problemele actuale în securitatea reţelelor şi sistemelor de comunicaţii rezultă din:

- necesitatea adaptării complexităţii funcţiilor de securitate la cerinţele de costuri şi de performanţă ale aplicaţiilor utilizatorilor. Aceasta are în vedere şi limitările de performanţă generate de implementarea unor funcţii de securitate complexe, cu impact asupra calităţii serviciilor de comunicaţii;
- diversificarea spectrului ameninţărilor la adresa resurselor reţelelor şi sistemelor de comunicaţii, în condiţiile extinderii reţelelor de acces de bandă largă bazate pe diferite tehnologii, cu vulnerabilităţi specifice. În plus, interconectarea reţelelor favorizează propagarea consecinţelor unor incidente locale de securitate la nivelul mai multor reţele, provocând daune unui număr mare de utilizatori rezidenţiali, dar şi operatorilor de reţea, furnizorilor de serivicii de comunicaţii şi aplicaţii, precum şi altor entităţi care deţin, administrează şi utilizează infrastructuri de comunicaţii;
- extinderea infrastructurilor de comunicaţii în zone vulnerabile la diferiţi factori de hazard natural şi artificial, insuficient documentaţi şi evaluaţi, a căror manifestare afectează funcţiile reţelelor şi sistemelor

de comunicaţii, în principal la nivel fizic, dar cu consecinţe asupra disponibilităţii şi calităţii serviciilor de comunicaţii furnizate utilizatorilor, precum şi asupra securităţii datelor transmise şi stocate.

Aceste tendinţe justifică interesul pentru fundamentarea, evaluarea şi introducerea de soluţii moderne combinate pentru protecţia infrastructurilor critice de comunicaţii, în acord cu tendinţele şi preocupările la nivel european în acest domeniu [5].

În acest context s-a luat decizia de a fi cercetată elaborarea unui sistem de comunicații securizat și anume, o aplicație de tip chat pe platforma Android cu scopul principal de a securiza traficul ce va circula între dispozitivele terminale (smartphone-urile).

BIBLIOGRAFIE

1. HOTĂRÎRE Nr. 257 din 22.11.2018 privind aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019 – 2024 și a Planului de acțiuni pentru implementarea acesteia. Disponibil pe Internet: http://lex.justice.md/viewdoc.php?action=view&view=doc&id=378899&lang=1 (accesat 05.09.2019).
2. Luminița Scripcariu, Ion Bogdan etc., Securitatea rețelelor de comunicații, Casa de editură Venus, Iași, 2008. - 193 p.
3. Aurel Şerb, Constantin Baron, Narcisa Isăilă, Securitatea informatică în societatea informaţională, Bucureşti : Pro Universitaria, 2013. – 546 p.
4. Popa Sorin Eugen, Securitatea sistemelor informatice, Bacău, 2007. – 136 p.
5. Securitatea rețelelor de comunicații. Disponibil pe Internet: http://www.inscc.ro/index.php?option=com_content&view=category&layout=blog&id=102&Itemid=488&lang=ro (accesat 20.10.2019).
6. Note de curs – Rețele de calculatoare. Disponibil pe Internet: https://www.studocu.com/en/document/universitatea-alexandru-ioan-cuza/calculatoare/lecture-notes/note-de-curs-retele-de-calculaoare/2529006/view (accesat 25.10.2019).
7. Raportul mondial privind evoluția societății mondiale a Republicii Moldova. Disponibil pe Internet: http://mei.gov.md/ro/content/republica-moldova-urcat-4-pozitii-raportul-mondial-privind-evolutia-societatii (accesat 25.10.2019).
8. Rețea fără fir. Disponibil pe Internet: https://ro.wikipedia.org/wiki/Re%C8%9Bea_f%C4%83r%C4%83_fir (accesat 28.10.2019).
9. Introducere în programarea Android. Disponibil pe Internet: https://ocw.cs.pub.ro/courses/eim/laboratoare/laborator01 (accesat 28.10.2019).
10. Algoritmi simetrici de criptare. Algoritmul AES. Disponibil pe Internet: https://biblioteca.regielive.ro/laboratoare/calculatoare/algoritmi-simetrici-de-criptare-algoritmul-aes-240549.html (accesat 2.11.2019).
11. Algoritmul de criptare AES. Disponibil pe Internet: http://www.securitatea-informatiilor.ro/solutii-de-securitate-it/algoritmul-de-criptografie-aes/ (accesat 5.11.2019).
12. Capturarea și analizarea traficului de rețea. Disponibil pe Internet: http://www.tc.etc.upt.ro/teaching/arc/Lab6.pdf (accesat 17.11.2019).
13. Introduction to Wireshark. Disponibil pe Internet: https://www.geeksforgeeks.org/introduction-to-wireshark/ (accesat 23.11.2019).
14. RBM33G. Disponibil pe Internet: https://mikrotik.com/product/rbm33g (accesat 01.12.19).
15. Android Logo. Disponibil pe Internet: https://www.google.com/search?q=android&sxsrf=ACYBGNQG-PLvqNC1A6cwadgmvTnccrSBhQ:1576572215495&source=lnms&tbm=isch&sa=X&ved=2ahUKEwin7veWpbzmAhXrk4sKHaTNBsoQ_AUoAXoECBIQAw&biw=1366&bih=576#imgrc=k74b27jAC706GM: (accesat 01.12.19).