Universitatea Babeş Bolyai Cluj Napoca

Facultatea de Matematică şi Informatică

http://www.ubbcluj.ro

Probleme de securitate în sisteme distribuite

- REZUMAT -

Doctorand : Incze Árpád

Conducător ştiinţific : Prof. univ. dr. Grigor Moldovan

2015

Comisia de doctorat

Preşedinte

Prof. univ. dr. Bazil PÂRV

Universitatea Babeş Bolyai Cluj Napoca

Referenți:

Prof. univ. dr. Adrian ATANASIU

Universitatea din Bucureşti

Prof. univ. dr. ing. Mihail ABRUDEAN

Universitatea tehnică Cluj Napoca

Prof. univ. dr. Florin BOIAN

Universitatea Babeş Bolyai Cluj Napoca

Mulțumiri

Adresez respectuoase mulțumiri domnului Prof. Dr. Grigor Moldovan, conducătorul ştiințific al lucrării, pentru profesionalismul cu care m-a ghidat pe drumul către obținerea titlului de doctor, pentru competența şi permanenta îndrumare ştiințifică, pentru sprijinul real acordat pe întreaga perioadă de desfăşurare a doctoratului şi a elaborări tezei de doctorat.

De asemenea, le mulțumesc domnului Prof. Dr. Adrian Atanasiu, domnului Prof. Dr. Mihail Abrudean, domnului Prof. Dr. Florin Boian, referenți care pe ultima sută de metri au contribuit la îmbunătățirea conținutului tezei prin observațiile şi sugestiile domniilor lor.

Mulțumesc domnului Prof. Dr. Ioan Ileană şi domnului Prof. Dr. Ioan Achim Moise pentru sprijinul acordat în realizarea auditului de securitate prezentat în capitolul 4. Mulțumesc tuturor colegilor din cadrul Universității 1 Decembrie 1918 Alba Iulia, pentru sprijinul moral acordat.

Mulțumesc familiei care m-a sprijinit pe toată perioada derulării stagiului de doctorat. Mulțumesc în special soției mele care a avut încredere în mine şi mi-a fost alături, dar mai ales pentru că a avut multă, foarte multă răbdare.

Mulțumesc profesoarei mele de fizică din liceu, doamna Magdalena Nicolcescu a cărei influență a lăsat o amprentă adâncă şi benefică asupra evoluției mele academice.

Mulțumesc domnului Prof. Dr. Liviu Miclea care m-a motivat să îmbrățişez cariera de informatician aruncându-mă în gura leului, cum s-ar zice, oferindu-mi şansa de a preda informatica încă din timpul studenției la şcoala postuniversitară.

Cu deosebită considerație, Incze Árpád

Cuprins rezumat

Cuvinte cheie: securitate în rețele de calculatoare şi sisteme distribuite, inginerie socială, criptografie vizuală şi partajarea secretului.

CUPRINS TEZĂ

LISTA PUBLICAȚII

Lucrările autorului:

[Incze04] dep. Informatică, contributor **Incze Arpad**, *Document intern: Raport de audit de securitate 2004*

[Incze05] **Incze Arpad**, Ioan Ileană, Manuela Kadar, *Increasing the security of an ACCESS database,* proceedings of „Several aspects on biology, chemistry, computer science, mathematics and physics", Oradea 2005 ISBN 973-759-142-9

[Incze10a] **Incze Arpad**, *Secret sharing & visual cryptography through bit sieve for fast image encryption,* proceedings AQTR 2010 THETA 17th International IEEE confernce on Automation,Quality and Testing, Robotics, ISSN 978-973-662-562-6

[Incze10b] **Incze Arpad**, *Pixel Sieve method for secret sharing & visual cryptography,* Proceedings of the 9th RoEduNet IEEE International conference, Sibiu, 24-25 june, 2010 in ***ISI Conference Proceedings Citation Index***

[Incze10c] **Incze Arpad**, Moldovan Grigor, Maria Muntean, *From pixel sieve to bit sieve. Bit level based secret sharing cryptographic method,* in proceedings 11th International symposium CINTI, Budapest 18-20 nov. 2010 978-1-4244-9278-7 indexat **IEEE**

[Incze11] **Incze Arpad**, *Social Enineering and education in fight against cybercrime*, Acta Universitas Apulensis- Special Issue, Proceeding of ICTAMI 2011, ISSN 1582-5329 p541-553 **B+ CNCSIS**

[Incze12] **Incze Arpad,** *A greater involvement of education in fight against cybercrime* 2nd WORLD CONFERENCE ON EDUCATIONAL TECHNOLOGY RESEARCHES NEAR EAST UNIVERSITY 27-30 June 2012 NICOSIA – NORTH CYPRUS Procedia-Social and Behavioral vol 83 Journal ISSN: 1877-0428 by ELSEVIER ***ISI Conference Proceedings Citation Index***

[Incze14a] **Incze Arpad**, "*Cryptographic key issues and solutions for the bit sieve/pixel-sieve method*", *AQTR*, 2014, 2014 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR) 2014, pp. 1-5, doi:10.1109/AQTR.2014.6857853 ***ISI Web of Science***

[Incze14b] **Incze Arpad**, *Solutions regarding some cryptographic key issues for the pixel-sieve cryptographic method* , 4th WORLD CONFERENCE on INNOVATION and COMPUTER SCIENCES (INSODE-2014) Sapienza University, Faculty of Economics April 11-13, 2014 Rome, Italy www.insode.org in AWERProcedia Information Technology and Computer Science // Global Journal on Technology ISSN: 2147-5369 **indexat AWER Index şi trimis spre indexare ISI**

[MunInc10] Maria Muntean, Honoriu Valean, Liviu Miclea, **Incze Arpad** *A novel intrusion detection method based on support vector machines*, proceedings of 11th International symposium CINTI, Budapest 18-20 nov, 2010. 978-1-4244-9278-7 indexat **SCOPUS**

Lucrările în care autorul este citat:

- Feldiansyah Bin Bakri Nasution, Dr. Nor Erne Nazira Bazin , Johor Bahru, Malaysia

Adjusting ICT Capacity Planning by Minimizing Cyber Crime Effects in Urban Area: A System Dynamics Approach, Proceeding of International Conference on Electrical Engineering,

Computer Science and Informatics (EECSI 2014), Yogyakarta, Indonesia, 20-21 August 2014

- Vaibhav Choudhary, Pravin Kumar, Kishore Kumar, D.S. Singh *An improved Pixel Sieve method for Visual Cryptography* , International Journal of Computer Applications, Volume 12 No. 9 January 2011 ISSN 0975-8887

- Vaibhav Choudhary, Pravin Kumar, Kishore Kumar, D.S. Singh *Modified Pixel Sieve Method for Visual Cryptography* Vaibhav Choudhary et. al. / Indian Journal of Computer Science and Engineering Vol. 1 No. 4 321-326

- Venkatesh M.R. , Roopanjali. Daddi, *SDS Technique For Secret Image Encryption,* International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 4, April – 2013 ISSN: 2278-0181

- Siddharth Malik, Anjali Sardana *A Keyless Approach to Image Encryption,* 2012 International Conference on Communication Systems and Network Technologies 978-0-7695-4692-6/12 $26.00 © 2012 IEEE DOI 10.1109/CSNT.2012.189

- Koteswari, S.; Paul, P. John; Indrani, S., *VC of IRIS Images for ATM Banking,* International Journal of Computer Applications, Volume 48 No. 18 June 2012 ISSN 0975-8887

- Deepak Aeloor,Amrita A. Manjrekar *Securing Biometric Data with Visual Cryptography and Steganography,* Security in Computing and Communications, Communications in Computer and Information Science Volume 377, 2013, pp 330-340 SprimgerLink ISBN 978-3-642-40575-4

- Anisha K Jose, Panchami V, *AN EFICIENT APPROACH FOR SECRECY BY SDS ALGORITHM* International Journal of Emerging Trends in Engineering and Development Issue 4, Vol.2 (March 2014) ISSN 2249 – 6149

- Kandar, S.; Dhara, B.C., "*Random sequence based secret sharing of an encrypted color image*," Recent Advances in Information Technology (RAIT), 2012 1st International Conference on , vol., no., pp.33,37, 15-17 March 2012 doi: 10.1109/RAIT.2012.6194475 IEEE

De asemenea autorul a fost invitat la conferința CINTI[1] 2010 pentru a prezenta şi a dezbate, în cadrul unui workshop, concluziile legate de subiectul ingineriei sociale şi a criminalității informatice.

[1] 11th IEEE International Symposium on Computational Intelligence and Informatics, November 18-20, 2010 Budapest, Hungary.

REZUMATUL TEZEI

Introducere

Comunicația reprezintă una din cele mai importante necesități ale societății moderne. Comunitățile sunt animate de această forță care stă la baza progresului actual al societății. Felul în care omul a comunicat de-a lungul timpului a evoluat odată cu evoluția societății. Progresul societății în domeniul comunicațiilor ne-a permis să trecem de la forme de comunicare lente şi cu latență mare, nesigure, ineficiente şi cu limitări de distanță serioase, la forme de comunicații cvasi-instantanee, globale şi cu un grad ridicat de securitate. Practic nu există ramură a economiei care să nu depindă de comunicații, la fel cum alte componente ale societății sunt în mare măsură dependente de comunicații: guvernare, educație, sănătate, justiție, ș.a.m.d.. Lipsa de coordonare pe un şantier, sincope în alimentarea cu subansambluri a unei linii de producție, imposibilitatea alertării asupra unui eveniment produs sau iminent care pune vieți în pericol, reprezintă tot atâtea situații în care lipsa de comunicare duce la perturbarea ordinii fireşti sau mai rău, duce la pagube ce altfel ar putea fi prevenite şi evitate.

Sistemul de comunicații trebuie să fie de încredere atât din punct de vedere al confidențialității cât mai ales din punct de vedere al disponibilității şi stabilității. Un sistem de comunicații care prezintă dese întreruperi în funcționare, fluctuații în calitatea serviciului sau prezintă neajunsuri în ceea ce priveşte integritatea şi confidențialitatea datelor va duce în cele din urmă la abandonarea lui în detrimentul utilității sau confortului social.

Dacă progresul tehnologic în domeniul comunicațiilor a rezolvat şi continuă să rezolve majoritatea problemelor legate de viteza şi siguranța cu care informația este transmisă, acelaşi progres tehnologic permite unei clase aparte a societății în care trăim, să exploateze în folos propriu şi în detrimentul societății instrumentele şi metodele de comunicații. Larga răspândire a rețelelor de calculatoare, rețeaua globală de calculatoare, infrastructura care stă la baza sistemelor distribuite, este exploatată de aceste persoane în scopuri mai puțin utile societății şi de cele mai multe ori ilegale.

Transmiterea informațiilor şi problemele de securitate din domeniul transmiterii de informații au apărut cam în acelaşi moment. Informațiile transmise sau stocate pot avea o anumită importanță deci o anumită valoare. Cel ce deține informația dispune de ceva valoros. Prin urmare informația a devenit o țintă iar arta de a intercepta şi a desluşi informația o „meserie”.

Scopul tezei

Teza de față urmăreşte două scopuri. Pe de o parte prezintă o sinteză a vulnerabilităților sistemelor distribuite pe de altă parte propune soluții pentru ameliorarea securității acestor sisteme. Aceste soluții sunt din domeniul criptografiei vizuale.

Problemele de securitate care urmează să fie discutate răspund la întrebările „Ce se întâmplă dacă mecanismele şi serviciile de securitate sunt ocolite? Cum se pot ocoli aceste servicii? Ce se poate face pentru a preveni aceste situații?"

În lucrare sunt prezentate sintetic tehnicile utilizate de hackeri pentru a pătrunde în sistemele vizate. La întocmirea acestei părți s-au avut în vedere rapoartele anuale şi multianuale ale unor firme specializate din domeniul securității, punându-se accent pe cele mai frecvente metode de atac. În paralel cu prezentarea succintă a acestor tehnici sunt descrise şi soluțiile existente pentru minimizarea vulnerabilităților.

Ca şi proiect de cercetare autorul a realizat auditul de securitate al unei instituții. Acest audit avea ca scop determinarea vulnerabilităților sistemului informatic al instituției. În acest sens rețeaua de calculatoare a instituției a fost supusă unui set de atacuri informatice pentru a detecta vulnerabilitățile existente. Concluziile auditului au fost folosite pentru îmbunătățirea politicii de securitate a instituției şi o reorganizare a sistemului informatic.

Din analiza datelor privind metodele de pătrundere ilegală în sistemele informatice rezultă clar că cea mai slabă verigă este utilizatorul uman. Se impune deci şi un studiu asupra factorilor care fac din om ținta atacurilor. Astfel autorul realizează un scurt studiu privind aspectele sociale ale criminalității informatice. Sunt puse în evidență lacunele de care fac dovadă membrii societății şi sunt propuse soluții pentru ameliorarea situației. O soluție propusă vizează educarea obligatorie a utilizatorilor în domeniul securității IT.

Pe lângă partea de sinteză, teoretică ce priveşte aspectele de securitate a sistemelor distribuite, tot ca şi contribuție proprie, autorul propune o nouă metodă criptografică. Această metodă are rădăcini în domeniul criptografiei vizuale. Ca de multe ori în criptografie şi această metodă criptografică vizuală serveşte ca o primitivă pentru metode complexe. Deşi în lucrare accentul se pune pe metoda vizuală autorul propune şi o metodă de criptare pentru informația binară bazată pe acelaşi principiu ca şi metoda vizuală. În lucrare sunt descrişi paşii dezvoltării metodei de la ideea de bază şi până la o variantă acceptabilă din punct de vedere a siguranței utilizării. Metoda propusă poate fi folosită deci pentru criptarea imaginilor dar şi a fişierelor, a informațiilor transmise prin rețea.

După testarea şi îmbunătățirea metodei autorul propune, pe lângă utilizarea evidentă, de criptare a informațiilor şi câteva aplicații posibile din domeniul anumitor mecanisme de

securitate cum ar fi autentificarea sau semnătura digitală. Metoda de autentificare propusă întăreşte autentificarea clasică bazată pe perechea *nume – parolă* cu o imagine gen CAPTCHA criptată. Pentru a putea răspunde la provocarea CAPTCHA utilizatorul trebuie să poată decripta şi interpreta imaginea. Metoda de semnătură digitală a imaginii se bazează pe o particularitate a metodei criptografice descrise, prin care putem obţine o partiţie de o dimensiune dorită a informaţiei criptate. Semnătura digitală asigură originalitatea informaţiilor şi autenticitatea expeditorului. Aceste aplicaţii prezintă subiectul unor cercetări şi dezvoltări ulterioare a metodei propuse.

Istoria a arătat că oricât de sigură ar fi o metodă criptografică la un moment dat, după un timp se va găsi o slăbiciune a metodei care va fi exploatată. Prin urmare autorul îşi propune pentru viitor să îmbunătăţească mai departe metoda şi să-i găsească noi utilizări.

Formularea problemei

„Unde-s mulţi puterea creşte!" este şi principiul care stă la baza dezvoltării sistemelor distribuite. Acceptăm ca definiţie larg răspândită pentru sisteme distribuite afirmaţia că un **sistem distribuit de calcul** sau **sistem informatic distribuit** este mulţimea programelor dintr-o reţea de calculatoare având ca scop partajarea resurselor pentru rezolvarea unor probleme paralelizabile[2]. Această abordare are ca şi rezultat rezolvarea mai rapidă a problemelor prin distribuirea sarcinilor pe nodurile sistemului.

Când vine vorba de această distribuire a sarcinilor, sistemele distribuite se bazează în întregime pe sistemele de comunicaţii. Problemele de securitate ale sistemelor de comunicaţii reprezintă deci, în cea mai mare măsură, şi probleme de securitate ale sistemelor distribuite.

Să luăm o formă de comunicare între indivizi, spre exemplu simplul act al vorbirii. Situaţiile în care vorbirea este împiedicată de o cauză oarecare sau perturbată din cauza multitudinii de voci din apropiere sunt situaţii excepţionale cărora indivizii societăţii le găsesc mijloacele necesare pentru evitare sau corectare. În situaţiile în care comunicarea este afectată, individul identifică cauzele şi ia măsurile de corecţie necesare, spre exemplu se deplasează într-o direcţie care să-i permită o comunicare bună cu interlocutorul. Se observă că părţile implicate în comunicaţie participă activ la îmbunătăţirea comunicaţiei prin acţiunile pe care le întreprind.

[2] Ioan Dziţac, Gligor Moldovan, *Sisteme distribuite. Modele informatice,* Editura Universităţii Agora, 2006 isbn 10 973-87960-9-1

Cum *societatea virtuală este o oglindire cvasi-fidelă a societății reale*[3], situația este similară în cazul comunicației electronice: imposibilitatea comunicării a două entități poate fi provocată de un atac de interzicere a accesului (Denial of Service – DoS), iar comunicarea cu o rată redusă poate fi dată de lipsa scalabilității sistemului de comunicație. Pentru ameliorarea acestor stări de fapt, sistemele implicate în comunicație trebuie să dispună de metode şi protocoale de acțiune pentru detectarea, eliminarea şi evitarea cauzelor care perturbă comunicația. Putem distinge trei parametri ai sistemelor de comunicație care definesc şi dau o măsură calității comunicației:

Disponibilitatea *unui sistem de comunicație reprezintă capacitatea acestuia de a fi gata a efectua o transmisie într-un timp rezonabil. Lipsa disponibilității se poate datora fie întreruperii fizice a căii de comunicație (fire telefonice, cablu de rețea, emițător radio) sau se poate datora unui atac de tip DoS care împiedică transferul de date pe toată perioada sa. În prezent, rezistența la astfel de atacuri nu este un obiectiv de proiectare pentru majoritatea sistemelor de comunicație.*

Scalabilitatea *unui sistem de comunicații este capacitatea acestuia de a se adapta la diverse scenarii de încărcare. În cazul creşterii valorilor traficului, degradarea calității serviciului trebuie să se facă gradual şi proporțional, evitându-se astfel căderi rapide ale serviciului care ar putea fi exploatate ulterior de un atacator. În general protocoalele de distribuție a conținutului deservesc clienții unul câte unul, lucru ce reprezintă o gâtuire a performanței care s-ar putea obține prin abordarea paralelă a distribuției.*

Securitatea *sistemului de comunicații reprezintă capacitatea sistemului de a funcționa în condiții normale sau apropiate de normal sub acțiunea unor factori externi perturbatori. În mod tradițional când vorbim de securitate ne gândim la protecția şi confidențialitatea datelor transmise de sistem, iar literatura de specialitate abundă de protocoale şi procedee de securizare a informațiilor aflate în tranzit prin diverse medii. Disponibilitatea şi scalabilitatea sunt factori care afectează în mod direct nivelul de securitate al unui sistem de comunicații, de aceea considerăm că o abordare corectă a îmbunătățirii securității presupune şi o creştere a celor doi factori.*

[3] ing. Valer Bocan, *CONTRIBUȚII LA CREŞTEREA DISPONIBILITĂȚII, SCALABILITĂȚII SI SECURITĂȚII SISTEMELOR DE COMUNICAȚIE*, Teza de doctorat, Universitatea "Politehnica" din Timişoara 2006

Securitatea informațiilor

Noțiunile de bază vehiculate laolaltă cu termenul securitate sunt următoarele: atac, compromitere, intruziune, apărare, detectare, mecanism de securitate. Toate aceste aspecte sunt tratate în amănunt în literatura de specialitate.[4]

Prin atac se înțelege orice acțiune voluntară prin care se intervine în comunicația de informații, cu scopul de a **întrerupe**, **intercepta**, **modifica**, **falsifica** informația.

Clasificând tipurile de atacuri putem vorbi despre **atacuri pasive** (interceptarea mesajelor, analiza traficului) sau **atacuri active** (retransmiterea unor mesaje modificate, transmiterea unor mesaje false, blocarea unor servicii prin atacuri de tip DoS, ...)

Mecanismele de securitate au menirea de a detecta eventualele atacuri şi împreună cu serviciile de securitate trebuie să prevină sau să înlăture aceste atacuri. Serviciile de securitate pun la dispoziția utilizatorului sau a sistemului o serie de instrumente prin care sunt asigurate următoarele:

- **Controlul accesului** garantează că doar persoanele vizate, cu anumite privilegii, au acces la resurse. Acest lucru se realizează de cele mai multe ori prin utilizarea aşa numitelor conturi de utilizator (login credentials) adică o combinație de nume – parolă ce trebuie introdusă pentru a avea acces la sistem sau la o resursă din sistem. Dacă numele utilizatorului poate fi vizibil şi altor indivizi, parola asociată trebuie să fie secretă şi cunoscută doar de persoana/persoanele autorizate.
- **Confidențialitatea şi integritatea datelor**. Datele pot fi accesate/consultate/manipulate numai de utilizatorii legitimi şi nu pot fi alterate de persoane neautorizate.
- **Disponibilitatea resurselor** garantează că în orice moment un utilizator veridic va avea acces la resursele sistemului. La acest capitol excelează de fapt sistemele distribuite care

[4] Schneier, Bruce - *Secrets & Lies*, Wiley Publishing, Inc., 2004

D. E. Comer. *Internetworking with TCP/IP: Principles,Protocols, and Architecture,* volume I. Prentice-Hall, Englewood Cliffs, NJ, second edition, 199

Steve Bellovin, *Security Problems in the TCP/IP Protocol Suite*, Computer Communication Review, Vol. 19, no. 2 (April 1989) pg 32-48

Steven M. Bellovin, *A Look Back at "Security Problems in the TCP/IP Protocol Suite"* 20th Annual Computer Security Applications Conference (ACSAC), December 2004, in as part of the "classic papers" track.

L. Joncheray. *A simple active attack against TCP,* Proceedingsof the Fifth Usenix Unix Security Symposium, Salt Lake City, UT, 1995.

Burtescu Emil, *"Securitatea Datelor în Sistemele Informatice Economice*", 2004

Peter Norton , Dave Kearns, *Rețele de calculatoare,* Editura Teora, 2002

Andrew S. Tanenbaum, *Rețele de calculatoare,* Computer Press Agora 1998 (traducere)

prin definiție trebuie să asigure funcționarea, cel puțin parțială, a ansamblului chiar dacă anumite noduri din sistem sunt scoase din uz.

- **Autenticitatea şi nerepudierea** garantează pe de o parte identitatea participanților la o sesiune de comunicații pe de altă parte exclude refuzul unui utilizator de a recunoaşte accesul la un anumit serviciu sau transmiterea anumitor informații.

Vulnerabilități

Vulnerabilitățile sistemelor distribuite se împart în câteva categorii majore pe care le vom aminti aici:

1. **Vulnerabilitatea fizică a canalelor de comunicații** adică accesul fizic la infrastructura folosită pentru manipularea şi transportul informației. Datorită faptului că sistemele distribuite se bazează pe canale de comunicații publice (de exemplu rețeaua globală World Wide Web) este practic imposibilă securizarea fizică a acestuia. Dacă stațiile de lucru pot fi ținute sub cheie într-o încăpere bine păzită nu acelaşi lucru se poate spune despre căile de comunicații prin care sunt transmise informațiile mai ales dacă aceste informații depăşesc perimetrul instituției.

2. **Vulnerabilitatea fizică a terminalelor** deşi aparent nu ar trebui să prezinte o problemă, prin plasarea nodurilor sensibile în locații cu acces limitat, în realitate sunt numeroase cazurile când informațiile sunt compromise prin accesarea de la distanță a nodurilor (remote procedure).

3. **Vulnerabilități care privesc accesul la informație** respectiv la infrastructura prin care circulă informația, derivă din vulnerabilitatea fizică enunțată la punctul doi. Accesul logic se traduce prin accesul la resursele informatice (soft) după ce s-a dobândit accesul fizic la stația de lucru. Se vehiculează noțiuni de genul: autentificare, acces, semnătură digitală, nerepudiere.

4. **Vulnerabilități care privesc informația propriu zisă**. Aici putem aminti interpretabilitatea informației adică dacă informația este criptată sau nu, posibilitatea de a deturna informația, de a modifica/denatura informația sau de a bloca transferul informației.

Securizarea unui sistem informatic înseamnă abordarea fiecărui tip de vulnerabilitate mai sus amintit. Rezultă deci o structură stratificată pe nivele a măsurilor de securitate:

- la nivelul cel mai exterior, la nivelul fizic, să limiteze accesul la căile de comunicații
- dacă persoane neautorizate au totuşi acces la căile de comunicații atunci să se limiteze accesul la nodurile în care informația se poate extrage, modifica, etc.

- dacă persoane neadecvate au acces fizic la nodurile/terminalele sistemului să se limiteze pe cât posibil accesul logic la informație (autentificare, drepturi limitate, ...)
- dacă securitatea accesului la informație este compromisă şi informația este extrasă atunci măcar această informație să fie într-o formă care să nu poată fi interpretată de persoane neautorizate adică informația sensibilă să fie arhivată/criptată.

Criptografia. Criptografia vizuală

Ultima linie de apărare împotriva vulnerabilităților enumerate mai sus este ascunderea informației care tranzitează rețeaua. Pentru aceasta datele trebuie criptate. Criptografia joacă deci un rol foarte important în securitatea/securizarea comunicațiilor de date.

În securitatea sistemelor distribuite în general şi în securitatea bazelor de date în particular se urmăreşte securizarea mesajelor şi a tranzacțiilor ce se efectuează în sistem.

Criptografia este o "unealtă" folositoare în realizarea securității sistemului (nu este singura, se adoptă pachete de măsuri grupate în politici de securitate pentru a asigura securitatea sistemului). Există două tipuri de sisteme criptografice: simetrice şi asimetrice. Sistemele criptografice simetrice (cu cheie secretă) folosesc aceeaşi cheie, atât la criptarea cât şi la decriptarea mesajelor. Sistemele criptografice asimetrice (cu cheie publică) folosesc chei distincte la criptare şi decriptare (dar legate una de alta). Algoritmii criptografici (cifrurile) folosiți în sisteme criptografice simetrice se împart în cifruri flux (stream ciphers) şi cifruri bloc (block ciphers). Cifrurile flux pot cripta un singur bit de text clar la un moment dat, pe când cifrurile bloc criptează mai mulți biți (64sau 28 de biți) la un moment dat.

Criptografia vizuală este acel segment a criptografiei care are ca scop criptarea informației vizuale, a imaginilor. De multe ori se întâmplă ca informația transmisă prin rețea să fie de fapt informație vizuală. De exemplu, o bancă scanează contractele clienților şi le trimite electronic la sediul central. Aceste contracte trebuie criptate astfel încât chiar dacă datele ar fi interceptate informația să nu poată fi extrasă, interpretată.

CONȚINUTUL TEZEI

Capitolul 1. Introducerea. Răspunde la întrebarea "De ce alegerea acestei teme?" Sunt descrise pe scurt elementele constitutive ale sistemelor de calcul distribuite, problemele legate de securitatea sistemelor distribuite.

Capitolul 2, după o scurtă prezentare a noțiunilor generale vehiculate în această lucrare, se face o prezentare a jucătorilor principali în domeniu, ai celor care se ocupă cu găsirea şi exploatarea vulnerabilităților, aşa numiții hackeri.

Tot în acest capitol se face o trecere în revistă a celor mai importante metode de penetrare a securității sistemelor informatice. Pentru aceasta am folosit datele sintetizate de câteva firme specializate în securitatea IT. Cel mai de folos instrument a fost raportul anual al firmei VERIZONE[5] . Conform acestora cele mai răspândite tipuri de atac sunt:

Categorie amenințare	**Tip atac**	**% atacuri**	**% articole compromise**
Malware	Keylogger şi Spyware	19%	82%
Malware	Backdoor şi/sau RAT	18%	79%
Hacking	SQL Injection	18%	79%
Abuz	Abuz de privilegii de sistem	17%	1%
Hacking	Acces neautorizat folosind conturi de acces/setări implicite	16%	53%
Abuz de privilegii	Violarea politicilor de securitate (acces la PC, mail, internet, etc în cadrul organizației)	12%	Sub 1%
Hacking	Acces neautorizat prin puncte de acces configurate necorespunzător	10%	66%
Malware	Packet sniffer (furt de date aflate în tranzit prin rețea)	9%	89%
Hacking	Acces neautorizat folosind date de autentificare furate	8%	Sub 1%
Înşelăciune	Inginerie socială	8%	2%
Hacking	Ocolirea autentificării	6%	Sub 1%
Fizic	Furt fizic al suporturilor de date	6%	2%

[5] http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

Categorie amenințare	Tip atac	% atacuri	% articole compromise
Hacking	Brute force attack	4%	7%
Malware	RAM Scraper	4%	Sub 1%
Înşelăciune	Phishing	4%	4%

Tabel 1 Principalele tipuri de atacuri şi ponderea lor

Aceste rapoarte sunt prezentate sintetic în tabele. Din studierea rapoartelor se pot trage câteva concluzii importante.

Următoarele valori statistice oglindesc o stare de fapt larg răspândită printre utilizatorii sistemelor distribuite şi a rețelelor de calculatoare şi anume faptul că nu lipsa instrumentelor de securitate este cauza principală a breşelor de securitate ci lipsa cunoştințelor în domeniu şi implicit lipsa implementării acestor instrumente de securitate. Iată datele:

69% din breşe au fost descoperite de terți după ce angajații firmei au sesizat anumite nereguli şi au solicitat o expertiză

83% din atacuri erau de o dificultate redusă care nu necesitau cunoştințe laborioase din partea hackerului. Numai 17% din atacuri erau complicate.

87% din atacuri puteau fi evitate prin aplicarea unor măsuri şi instrumente de securitate **elementare!** Această ultimă cifră este subliniată şi de rezultatele experimentului condus de autor pe parcursul evaluării vulnerabilităților de securitate ale unei instituții

În continuare se face o radiografie a aspectelor sociale, a implicațiilor social-economice ale fenomenului. Sunt tratate aspecte ale criminalității informatice şi după o inspecție a modului în care se raportează societatea la acest fenomen sunt propuse anumite soluții pentru ameliorarea situației. Soluțiile implică în primul rând factorul educațional. Concluziile acestui capitol ar fi că populația nu este pregătită pentru a face față atacurilor şi această lipsă de pregătire se datorează în primul rând lipsei unor cunoştințe elementare şi de bun simț al celor care utilizează calculatorul.

Atât din concluziile prezentate în acest capitol cât şi din experiența proprie dobândită pe parcursul auditului de securitate desfăşurat la instituția vizată rezultă că cea mai slabă verigă în lista componentelor de securitate este utilizatorul uman. Metodele, instrumentele şi mijloacele de securitate există ! Aplicate corespunzător ar îngreuna considerabil munca unui hacker.

Odată cu dezvoltarea mijloacelor de protecție şi introducerea lor automată în procesul de comunicații, atacatorii nu mai încearcă să găsească breşe în aceste sisteme. Ținta lor este

utilizatorul. Acesta, din lipsă de experiență, din lipsă de educație în domeniu, sau câteodată din comoditate oferă atacatorului căile de acces la sistem.

În **capitolul 2.3.1** pentru a dovedi acest punct de vedere am conceput şi aplicat un test în care unor grupuri de studenți li s-a cerut să instaleze o aplicație oarecare. Însă pe parcursul instalării pe ecranul calculatorului apăreau avertizări care indicau faptul că aplicația este una dăunătoare.

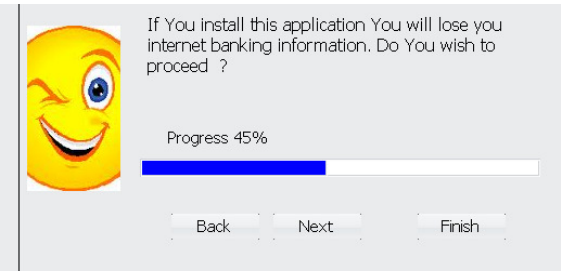


Figura 1 Interfața de instalare cu avertisment

Testul a fost derulat pe trei grupe de câte 20 de studenți de la specializări diferite. Din păcate rezultatele testului au fost surprinzătoare dar totuşi aşteptate. Tabelul următor sintetizează rezultatele testului.

Specializarea	Cunoştințe IT	„Promovat”	„Nepromovat”
Administrație publică	medii	5	15
Contabilitate informatică	medii spre bune	8	12
Informatică	avansate	2	18

Tabel 2 Rezultatele testului de vigilență

„Promovat” este pentru cei care au sesizat mesajul necorespunzător şi la un moment dat al instalării au oprit procesul.

„Nepromovat” este calificativul dat celor care au parcurs toate etapele instalării, practic au dat click pe Next şi OK fără să citească şi să interpreteze mesajele afişate.

Rezultatele vorbesc de la sine. Mai bine de 80% din subiecți au fost „de acord” să instaleze o aplicație care, culmea, îi avertiza că este o aplicație dăunătoare. Ce să mai vorbim despre alte aplicații care respectă formatul mesajelor sau care se instalează fără a ne da nici un fel de informație?!

După cum reiese şi din rezultatele testului de mai sus dar şi din testul de plasare a unui backdor descris la capitolul 2 , oamenii pot fi „convinşi” (a se înțelege păcăliți !) destul de uşor. Atât succesul tentativei de plasare a unor aplicații backdoor cât şi modul superficial de instalare a unui program oarecare subliniază necesitatea educării în masă a utilizatorilor. Această educare

trebuie să înceapă de pe băncile şcolii şi să continue chiar şi după terminarea studiilor la locul de muncă, unde sistemele de calcul sunt implicate.

Capitol 3 se doreşte a fi un capitol de sinteză în care se face o prezentare a rețelelor de calculatoare ca suport a sistemelor distribuite. Sunt prezentate vulnerabilitățile inerente ale acestora. Sunt tratate pe scurt nivele TCP/IP din prisma vulnerabilităților pe fiecare nivel. Tot aici sunt descrise şi instrumentele utilizate pentru prevenirea atacurilor. Este prezentată, în continuare, tehnologia Firewall ca o linie de apărare împotriva atacurilor. Fiind un capitol teoretic, de sinteză nu vom insista mai mult cu descrierea celor menționate în acest capitol.

Capitolul 4 conține etapele realizării auditului de securitate a unei instituții. Scopul acestui ”experiment” practic a fost determinarea vulnerabilităților sistemului informatic al instituției la momentul respectiv. Prin acest audit de securitate s-a urmărit identificarea breşelor de securitate, identificarea nivelului de acces neautorizat (până unde poate ajunge un hacker în sistem), dar şi identificarea nivelului minim de cunoştințe necesare unui hacker pentru a pătrunde în sistem. Pentru o analiză mai amplă s-a mers pe două scenarii posibile: un scenariu fiind un atac din partea unui angajat intern cu acces limitat la nodurile rețelei şi un alt scenariu care simula un atac extern.

Slăbiciunile interne ale arhitecturii IT a instituției au fost testate din următoarele puncte de vedere:

- accesul fizic la nodurile şi echipamentele de calcul ale rețelei **cap 4.2.1**
- accesul logic la informația de pe calculatoare **cap 4.2.2**
- accesul la distanță la calculatore şi resurse din rețeaua internă **cap 4.2.3**
- posibilitățile de penetrare spre exterior în vederea transmiterii de informații în afara instituției **cap 4.2.5.1**

În urma testelor am reuşit să accesăm de la un nod nesemnificativ al rețelei informații aflate pe stații din departamente cu un grad ridicat de confidențialitate. Acest lucru era posibil datorită proiectării şi configurării greşite a rețelei dar şi modului în care erau sau mai bine zis nu erau configurate stațiile de lucru. Am descoperit că oricine avea acces fizic la un calculator se putea conecta pe un alt calculator fără probleme, folosind setări implicite (conturi de administrator fără parolă, partajări administrative,…). Astfel se puteau accesa resurse care în mod normal trebuiau să fie inaccesibile.

Dacă în cazul atacului intern scopul era determinarea defectelor de configurare ale rețelei interne, în cazul atacului extern scopul a fost găsirea breşelor care permiteau accesarea din exterior a resurselor instituției.

În **capitolul 4.3** sunt descrise paşii implementării unui atac de tip inginerie socială care avea ca scop instalarea unei aplicații de tip backdoor care să permită mai apoi accesul la rețeaua internă a organizației. Concret, am conceput şi am pus în aplicare un plan prin care angajații instituției au fost induşi în eroare şi convinşi să descarce şi să instaleze un program de calculator, aparent util.

Atacul a fost orchestrat în trei paşi (**capitolul 4.3.1**)

Pasul unu: planificarea şi culegerea de informații, respectiv stabilirea grupului țintă

Pasul doi: pretextarea, găsirea unui motiv plauzibil care să fie crezut de grupul țintă

Pasul trei: atacul propriu zis

Astfel, un grup țintă de angajați au primit un email prin care li s-a cerut să instaleze un patch al aplicației de antivirus folosit de instituție. Mailul a fost astfel conceput încât să pară că acesta vine din partea departamentului de informatică al instituției. Patch-ul instalat de angajați nu era unul dăunător dar într-o situație reală putea conține troieni de tip backdoor care ar fi compromis securitatea instituției.

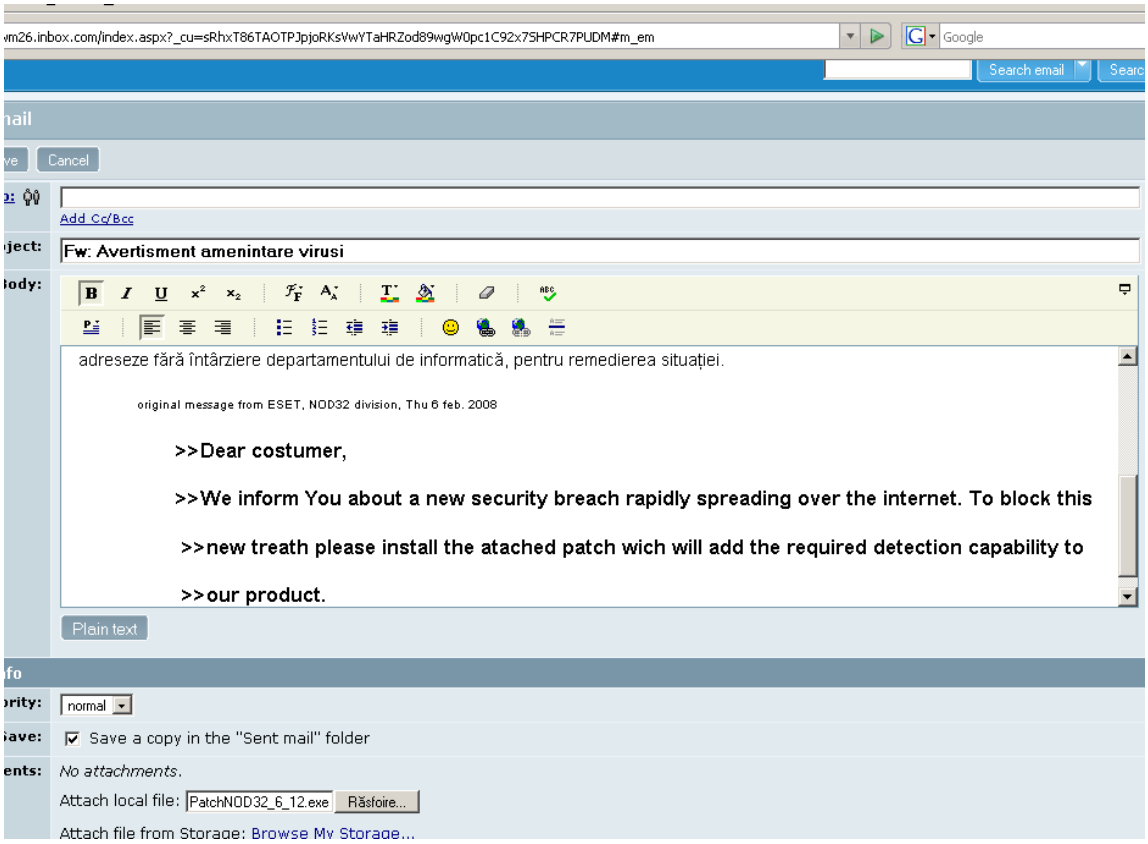


Figura 2 Mesajul fabricat tendențios

Mesajul a fost trimis unui număr de 36 de persoane. Din păcate putem spune că am avut un succes răsunător, având in vedere că până la depistarea atacului am primit mesajul de confirmare de la 51 de persoane!!! În tabelul următor se poate vedea situația confirmărilor (deci a instalărilor) aplicației „backdoor".

Ziua	0(expediere)	1	2	3	4	5(depistare)	6,7	total
Confirmări	19	12	4	5	4	3	4	51

Tabel 3 Numărul instalărilor aplicației backdoor

În **capitolul 4.4** se fac recomandări pentru îmbunătățirea securității instituției. În urma acestui audit, sistemul informatic al instituției a fost regândit şi reorganizat. De asemenea, s-a cristalizat o politică de securitate care a fost impusă angajaților instituției. [Incze04]

Capitolul 5 este dedicat criptografiei ca ultim bastion de apărare. După o scurtă introducere în criptografie, autorul descrie etapele dezvoltării propriei metode criptografice, de la ideea originală până la produsul finit. Metoda propusă are la bază elemente de criptografie vizuală şi tehnica partajării secretului.

Metoda strecurătorii de pixeli are la bază următoarele concepte:

Criptografia vizuală are ca scop ascunderea, mascarea informațiilor prezentate sub formă de imagini. Imaginea originală trebuie sa poată fi reprodusă din imaginea criptată integral. În unele cazuri putem vorbi şi de o reproducere parțială, situație în care imaginea obținută trebuie să poată fi interpretată de om. Din acest punct de vedere metoda noastră poate fi încadrată în ambele categorii. Putem avea o imagine decriptată identică cu originalul sau putem avea o imagine decriptată cu zgomot dar interpretabilă vizual.

Partajarea secretului[6],[7] este o metodă de securizare a informației prin care informația este divizată în partiții. Față de aceste partiții se impun anumite cerințe:

- o partiție nu poate furniza suficientă informație pentru a descifra tot mesajul.
- în funcție de schema de partajare pentru refacerea informației originale poate fi nevoie de toate partițiile (scheme n din n) sau un număr minim de parții (scheme k din n)
- ca şi cerințe asupra partițiilor, metoda de divizare impune şi un algoritm sau o cheie secretă. Reconstrucția informației se poată realiza doar în prezența cheii secrete.

[6] Ronald L. Rivest, Adi Shamir, Yael Tauman *How to share a secret* - Communications of the ACM , 1979

[7] Gustavus J. Simmons *How To (Really) Share A Secret* , 1998

Criptografie vizuală prin partajarea secretului obținem atunci când cele două principii enunțate anterior le aducem împreună.

Schemele de criptografie vizuală prin partajarea secretului inițial se bazau pe cifrarea apoi tipărirea partițiilor pe folii transparente[8]. Pentru a descifra imaginea era suficientă suprapunerea partițiilor. Între timp au apărut şi alte scheme care necesită o cheie de criptare/decriptare şi un algoritm implementat pe un calculator, vizualizarea informației decriptate realizându-se pe ecranul calculatorului.

În **capitolul 5.3**, pornind de la aceste considerente inițiale, am propus metoda strecurătorii de pixel. Conceptul este unul foarte simplu şi constă în generarea imaginilor care formează cele două partiții prin „strecurarea" pixelilor imaginii originale prin pixelii unei imagini cheie. Dacă ne imaginăm cheia ca o sită cu ochiuri neregulate (găurile reprezentate prin pixeli negri şi materialul sitei reprezentat prin pixeli albi), ne putem imagina cum anumiți pixeli ai imaginii originale cad prin găurile (pixelii negrii) ai sitei, iar alți pixeli ai imaginii originale situați peste pixelii albi rămân pe strecurătoare. Pixelii care trec de strecurătoare formează o partiție, pixelii care rămân pe strecurătoare formează cealaltă partiție.

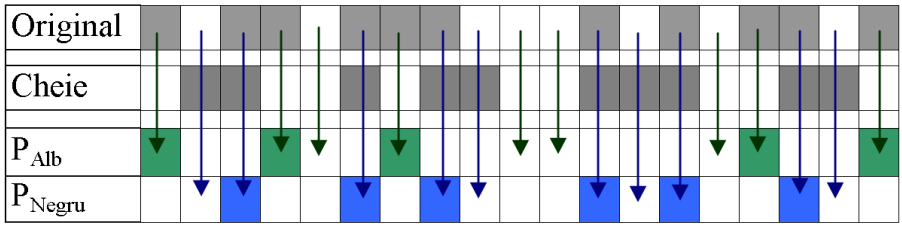


Figura 3 Principiul de funcționare al strecurătorii de pixeli

Ca şi în cazul criptografiei vizuale descrisă de Shamir [Sham79] avem cele trei componente:

- Cheia ținută secret, folosită la criptare
- P^{Alb} imaginea obținută prin trecerea corespunzătoare pixelilor albi ai cheii
- P^{Negru} imaginea obținută prin trecerea corespunzătoare pixelilor negri ai cheii

Înlocuind pixelii albi şi negri cu biții 0 şi 1, formal această metodă se poate scrie astfel:

$$P_{ij}^{0} = \begin{cases} O_{ij}, \text{ dacă } K_n = 0 \\ x \text{ random, dacă } K_n = 1 \end{cases}$$

$$P_{ij}^{1} = \begin{cases} O_{ij}, \text{ dacă } K_n = 1 \\ x \text{ random, dacă } K_n = 0 \end{cases}$$

$\mathbf{P_{ij}}$ este valoarea pe care o va primi pixelului din poziția curentă (i,j) în partiția 0 sau 1.

[8] Moni Naor and Adi Shamir, *Visual Cryptography,* EUROCRYPT 1994, pp1–12 [1].

$\mathbf{O_{ij}}$ este valoarea pixelului în poziția curentă (i,j) în imaginea originală

$\mathbf{K_n}$ este poziția curentă în cheie; $K_n \in \{0,1\}$

Procedeul este ilustrat schematic în figura 6.

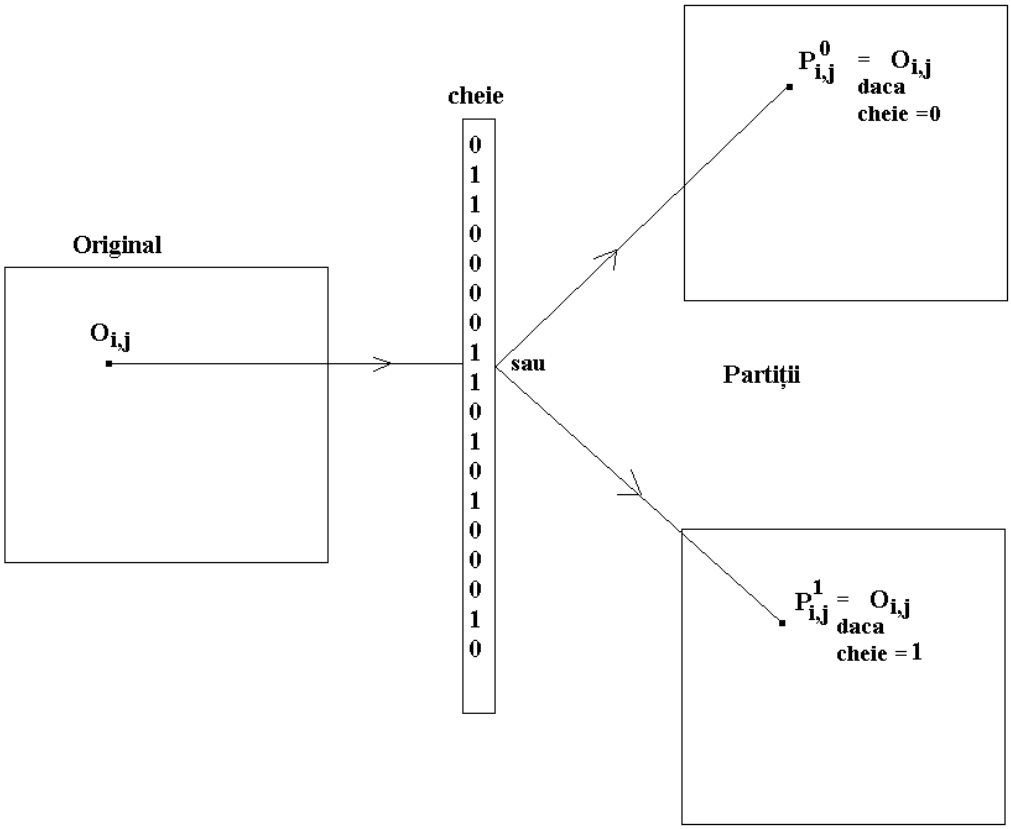


Figura 4 Generarea partițiilor dependente de valoarea cheii

Capitolul 5.4 Dacă înlocuim pixelii albi şi negri cu biți ajungem la strecurătoarea binară (bit sieve) descrisă în [Incze10c]. Dacă ***T*** text clar de lungime n, ***C*** cheia de criptare de lungime k, $\boldsymbol{P_1}$ prima partiție, $\boldsymbol{P_2}$ a doua partiție, toate fiind şiruri binare avem situațiile:

Text clar	1	0	0	1	0	1	0	1	0	1	0	0	1	1	1	1
Cheie	0	0	0	0	1	1	0	1	0	1	1	0	1	0	1	0
Partiție 1	x	x	x	x	0	1	X	1	x	1	0	X	1	x	1	x
Partiție 2	1	0	0	1	x	x	0	x	0	x	x	0	x	1	x	1

Tabel 3 Exemplificarea metodei bit sieve cu *avans total*

Text clar	1	0	0	1	0	1	0	1	0	1	0	0	1	1	1	1
Cheie	0	0	0	0	1	1	0	1	0	1	1	0	1	0	1	0
Partiția 1	0	1	1	1	0	1	1									
Partiția 0	1	0	0	1	0	0	0	1	1							

Tabel 4 Metoda bit sieve cu *avans parțial*

Pentru varianta *bit sieve* se pot scrie următoarele :

$$T = \{w = t_1 t_2 ... t_n \mid t_i \in \{0,1\},\ i = \overline{1,n}\ \}$$

$$C = \{u = c_1 c_2 ... c_k \mid c_j \in \{0,1\},\ j = \overline{1,k}\}$$

$$P_1 = \begin{Bmatrix} t_i \ \ dacă \ \ c_x = 0 \\ random \ \ dacă \ c_x = 1 \end{Bmatrix}$$

$$P_2 = \begin{Bmatrix} t_i \ \ dacă \ c_x = 1 \\ random \ \ dacă \ c_x = 0 \end{Bmatrix}$$

$$unde \ \ x = \begin{Bmatrix} i \bmod k, dacă \ i \bmod k \neq 0 \\ k, dacă \ i \bmod k = 0 \end{Bmatrix}$$

Mai multe posibilități de îmbunătățire sunt descrise în lucrare. Acestea se referă fie la îmbunătățiri care țin cont de fiziologia umană, de modul în care ochiul uman percepe imaginea, fie la îmbunătățiri aduse prin metode şi tehnici specifice criptografiei. Aceste metode sunt transpoziția (amestecarea), operații logice (XOR în cazul de față) , diferite tehnici de parcurgere, citire a informației originale, adăugarea unor chei de criptare suplimentare, introducerea unor runde pentru obținerea unei criptări mai sigure. Îmbunătățirile descrise pot fi aplicate, unele la ambele variante altele doar la una din variante adică pixel-sieve sau bit-sieve.

Capitolul 5.5 Cheia extinsă [Incze14a]

Inspirându-ne şi din tehnicile de îmbunătățire propuse de alți cercetători [Jiun99, Chou10] am adus câteva modificări metodei. Aceste noi îmbunătățiri se referă în primul rând la cheia de criptare dar şi la noi abordări privind construcția informației criptate.

În ceea ce priveşte cheia de criptare propunem o metodă prin care se obține o cheie de dimensiuni mai mari din cheia originală. Vorbim de o expandare a cheii. Metoda propusă are la bază un procedeu larg răspândit în criptografie dar mai ales în domeniul generatoarelor de numere aleatoare. Este vorba de ***Linear Feedback Shift Register*** sau prescurtat ***LFSR***

Capitolul 5.5.2. Key Shifting şi XOR pentru extinderea cheii [Incze14b]

În cele ce urmează propunem o metodă asemănătoare cu LFSR pentru a genera o cheie de criptare mai lungă dintr-o parolă relativ scurtă introdusă de utilizator.

Această metodă constă în generarea unei chei a cărei elemente sunt obținute printr-o operație de XOR după cum urmează:

Fie $\mathbf{a_i}$ elementele cheii originale şi $\mathbf{b_j}$ elementele cheii expandate. Primul element al cheii expandate se obține printr-o operație de XOR între primele două elemente ale cheii originale.

$$b_1 = a_1 \ XOR \ a_2$$

În continuare se parcurge cheia originală. Următoarele elemente ale cheii expandate sunt

obținute ca rezultat al operației de XOR între elementul curent din cheia originală şi ultimul element al cheii expandate:

$b_i=b_{i-1}\ XOR\ a_i$ unde i =(2… n) cu n lungimea şirului

De exemplu, pentru caracterul „*a*" cu codul ASCII = 97 = 1100001, aplicând metoda descrisă mai sus obținem:

a_i	1	1	0	0	0	0	1
b_i	0	1	1	1	1	1	0

Am observat că putem să continuăm procesul de generare a noii chei folosind pentru următorul element *n+1* al cheii extinse, rezultatul operației de XOR între primul element al cheii inițiale şi ultimul element al cheii extinse.

$$b_{n+1}=b_n\ XOR\ a_1$$

Practic, reluăm elementele cheii inițiale şi continuăm astfel generarea cheii extinse.

În general, formula de calcul poate fi scrisă astfel:

$$b_{n+i}=a_i\ XOR\ b_{n+i-1}$$

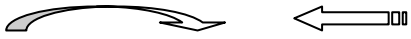
sau folosind funcția modulo pentru calculul poziției în cheia inițială:

$$b_k=a_{k\ mod\ n}\ XOR\ b_{k-1}$$

unde **n** este lungimea cheii inițiale iar **k**=(1..n)

Însă acest lucru este adevărat numai dacă $\boldsymbol{b_1 \neq b_{n+1}}$ deci trebuie ținut cont de acest lucru

Pentru că dorim să extindem cheia şi mai mult vom folosi o tehnică de key-shifting. Key-shifting este procedeul în care elementele cheii sunt rotite, deplasate circular. Putem vorbi de deplasare la stânga a şirului care formează cheia. În acest caz, primul element devine ultimul, iar restul elementelor se mută câte o poziție spre stânga.



$(a_1, a_2,\ldots a_{n-1}, a_n) \rightarrow (a_2, a_3, \ldots, a_n, a_1)$ $\quad a_n=a_1\ iar\ a_i=a_{i+1}$, i=(2..n-1)

O deplasare spre dreapta înseamnă evident mutarea spre dreapta a elementelor şirului iar ultimul element devine primul.

$(a_1, a_2,\ldots a_{n-1}, a_n) \rightarrow (a_n, a_1, a_2, a_3, \ldots, a_{n-1})$ $\quad a_1=a_n\ \ iar\ \ a_i=a_{i-1}$, i=(2..n)

Pentru a ilustra metoda să considerăm un cuvânt "CHEIE". Prin rotirea elementelor (literelor) cuvântului se obțin următoarele şiruri:

HEIEC, EIECH, IECHE, ECHEI apoi se revine la CHEIE.

Teoretic prin această metodă dintr-o cheie de lungime $\boldsymbol{n}$ se poate genera o cheie extinsă de lungime $\boldsymbol{2n^2}$. În practică însă se obțin blocuri repetitive. Astfel introducem o cheie numerică,

ca şi parte a secretului. Cifrele acestei chei vor da paşii cu care este deplasată cheia originală la fiecare ciclu, respectiv numărul elementelor cheii numerice va determina numărul de ciclări. Pentru o cheie numerică de lungime ***k (k<n)*** vom putea genera o cheie extinsă de lungime $2k^2$

Capitolul 5.6 Problema ratei de transfer a informației în partiții

Din modul în care informația este împărțită în cele două partiții rezultă că numărul de biți preluați într-o partiție este direct proporțional cu numărul de biți ai cheii care corespund partiției respective.

Astfel una din partiții va putea conține o cantitate considerabilă de informație utilă, poate chiar informație nealterată, care în cazul metodei vizuale poate duce la interpretarea mesajului din partițiile criptate, după cum se poate vedea în fig. 5.

Figura 5 Mesaj vizibil pe una din partiții

Notăm cu R_K raportul dintre pixelii albi şi negri ai cheii.

$$R_k = \frac{m}{n} = \frac{L-n}{n} = \frac{L}{n} - 1$$

Unde m şi n reprezintă numărul de pixeli albi respectiv negri ai cheii (sau biții 0 şi 1).

Pentru un număr dat n (sau m) spațiul cheilor conține C_L^n chei posibile. Ținând cont însă de fenomenul descris mai sus doar acele chei vor fi sigure pentru care diferența dintre pixelii albi şi negri nu depăşeşte o anumită valoare.

Evident un raport ideal ar fi $R_k=1$ însemnând că numărul de pixeli albi şi negri ai cheii sunt egali.

$$R_k \cong 1 \quad \Leftrightarrow \quad \frac{L}{m} \cong 2 \quad \Rightarrow \quad \frac{m+n}{m} \cong 2 \quad \cdots \quad m \cong n$$

În urma unor determinări empirice am ajuns la concluzia că este nevoie de un raport de cel mult 1 la 3 adică:

$$\frac{1}{3} < R_k < 3$$

Datorită acestui raport am denumit această problemă, problema L3.

Tot legat de elementele cheii se pune problema entropiei, adică dispersiei valorilor de 0 şi 1 pentru o cheie dată. Fie două chei, ambele de lungime L şi R_k =1

C_1=0000001001111111 C_2=1100101110010010

Datorită aglomerării de 0 (1) în cheia C_1 într-o zonă a cheii, deşi R_k=1 (ideal) informația

va fi trimisă către partiții în blocuri.

Capitolul 5.6.1 Rezolvarea problemei *L3. Metoda threshold-swap*

Am folosit două variabile contor în care se ține evidența biților transferați până la un moment dat în partiții. La fiecare transfer de informație într-una din partiții vom incrementa contorul partiției respective. După fiecare incrementare se compară cele două contoare şi dacă diferența lor depăşeşte o anumită valoare *prag* vom schimba rolul partițiilor.

n_0 - numărul de biți recepționați de partiția A

n_1 - numărul de biți recepționați de partiția B

$\delta = | n_0 - n_1 |$ - diferența dintre numărul de valori primite de cele două partiții

t_i - elementul curent ***i*** din şirul original

c_x - elementul curent al cheii

prag este limita maximă admisă pentru diferență în favoarea unuia dintre biți

$$t_i \rightarrow \begin{cases} A, \ dacă\ c_{i \bmod k} = 0 \ \text{şi}\ \delta \le \text{prag} \\ B, \ dacă\ c_{i \bmod k} = 1 \ \text{şi}\ \delta \le \text{prag} \end{cases} \qquad t_i \in \{0,1\},\ i = \overline{i,n}$$

- am marcat cu „ → „ operația de transfer a bitului curent t_i

Această limită este stabilită de utilizator şi poate fi o componentă a secretului necesar decriptării mesajului.

Prin implementarea metodei *threshold-swap* cheia extinsă este practic înlocuită cu cheia echivalentă, **capitolul 5.6.2.** În urma inversării biților cheii extinse, astfel încât pragul să nu fie depăşit, se obține cheie echivalentă.

$$C_e = Cif_{(prag)}$$

Redăm această situație în tabelul 5.10 în care am notat cu *Ci* cheia inițială şi cu *Ce* cheia echivalentă. Am colorat cu roz porțiunea în care biții cheii echivalente sunt inversați

poziția	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
C_i	1	0	1	0	0	1	0	0	0	1	0	0	1	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	1	0	0	1	0
C_e	1	0	1	0	0	1	0	0	0	1	0	1	0	1	0	1	1	1	1	1	1	0	1	0	1	0	0	0	1	0	0	1	0
n_0		1		2	3		4	5	6		7		8		9							10		11		12	13	14		15	16		17
n_1	1		2			3				4		5		6		7	8	9	10	11	12		13		14				15			16	
δ		0	1	0		0	1			2	3	2	3	2	3	2	1	0	1	2	3	2	3	2	3	2	1	0	1	0	1	0	1

Tabel 5 Cheia echivalentă ținând cont de prag

Am introdus o nouă măsură de întărire a metodei prin folosirea ambelor chei, atât cheia extinsă cât şi cea echivalentă:

- din cheia extinsă nemodificată, folosind metoda *prag-swap* vom genera **cheia echivalentă C_{eq}**

- folosim C_{eq} doar pentru a determina partiția în care bitul/pixelul curent va fi repartizat. Astfel ne asigurăm că cele două partiții au primit o cantitate de informație aproximativ egală
- folosim **cheia extinsă nemodificată** pentru a altera reversibil informația transmisă în partiții. Pentru aceasta vom folosi criptografia XOR descrisă în continuare.

Capitolul 5.7 Disimularea informației utile prin criptografie XOR

Pentru varianta pixel-sieve simpla plasare a unui pixel într-o partiție sau alta nu este de mare folos. Aproximativ jumătate din imagine va conține informație utilă, imaginea fiind interpretabilă.

Figura 6 O partiție cu pixeli nemodificați

Ascundem informația utilă prin criptografie XOR aplicată componentelor de culoare a fiecărui pixel în felul următor:

- se citeşte pixelul curent
- se descompune pixelul citit pe componentele de culoare pixel(x,y) = {R(x,y) ; G(x,y) ; B(x,y)} unde R-Red (roşu), G-Green (verde), B-Blue (albastru) fiecare putând lua o valoare între 0 şi 255 (pentru o imagine pe 24 biți adică 3x8 biți pentru fiecare culoare).
- blocul de 8 biți al fiecărei componente de culoare este supus unei operații XOR cu blocul curent de biți din cheie
- în urma operației de XOR se schimbă valoarea fiecărei componente de culoare, implicit şi culoarea finală a pixelului curent. Acest pixel alterat va fi de fapt transmis în partiția corespunzătoare.

În tabelul 4 redăm o asemenea situație în care din culoarea verzuie, în urma operației de

XOR, am obținut o culoare portocalie.

Culoarea inițială	Cod culoare	Cheie	Rezultat XOR	Culoarea finală
R	128=10000000	01101000	11101000=232	R
G	159=10011111	00011100	10000011=131	G
B	87=01010111	01110100	00100011=35	B

Tabel 6 Modificarea culorii unui pixel prin XOR pe componentele RGB

5.8 Criptarea şi decriptarea prin „strecurare”

Rezumând cele descrise până aici, un sistem care va utiliza metoda *strecurării* va avea următoarele componente:

Mc - mesajul/şirul clar transformat în şir binar **BMc**

Ci - cheia inițială transformată în cheia inițială binară **CiB**

R_k - cheia numerică - indică paşii cu care se face deplasarea pentru generarea cheii extinse

T - prag (*threshold*)

C_{ex} - cheia extinsă în binar

C_{eq} - cheia echivalentă în binar CEB=f(CB,prag)

P - partiția corespunzătoare elementelor **BMc** $\oplus$ **CiB** care corespund unei valori de 0 a cheii echivalente

Q - partiția corespunzătoare elementelor **BMc** $\oplus$ **CiB** care corespund unei valori de 1 a cheii echivalente

$$M = \{w = m_1 m_2 ... \mathrm{m_n} \mid \mathrm{m_i} \in \{0,1\},\ \mathrm{i} = \overline{1,n}\ \}$$

$$\mathrm{C_i} = \{a = a_1 a_2 ..... a_k \mid a_j \in \{0,1\},\ \mathrm{j} = \overline{1,k}\ \}$$

$$C_{ex} = \{u = c_1 c_2 ... c_k \mid \mathrm{c_j} \in \{0,1\},\ \mathrm{j} = \overline{1,k}\ \} \quad şi \quad C_{ex} = f_{Rk}(C_i)$$

$$C_{eq} = \{v = d_1 d_2 ... d_k \mid \mathrm{d_j} \in \{0,1\},\ \mathrm{j} = \overline{1,k}\ \} \quad şi \quad C_{eq} = f_T(C_{ex})$$

$$P = \left\{p = p_1 p_2 .... p_n \mid \mathrm{p_i} \in \{0,1\},\ \mathrm{i} = \overline{1,n}\ \right\} \quad (avans\ \ total)$$

$$sau\ P = \left\{p = p_1 p_2 .... p_l \mid \mathrm{p_i} \in \{0,1\},\ \mathrm{i} = \overline{1,l}\ \right\} \quad (avans\ partial)$$

$$Q = \left\{q = q_1 q_2 .... q_n \mid \mathrm{q_i} \in \{0,1\},\ \mathrm{i} = \overline{1,n}\ \right\} \quad (avans\ total)$$

$$sau\ Q = \left\{q = q_1 q_2 .... q_m \mid \mathrm{q_i} \in \{0,1\},\ \mathrm{i} = \overline{1,m}\ \right\} \quad (avans\ partial)$$

Unde am notat :

- ***M*** - mesajul clar binar
- ***C_i*** **–** cheia inițială (text ASCII)
- ***C_{ex}*** **-** cheia extinsă folosită la operația XOR
- ***C_{eq}*** - cheia echivalentă pentru a determina partiția în care se va scrie bitul
- ***P, Q*** - cele două partiții care conțin mesajul criptat

În cazul avansului total cele două partiții au dimensiunea egală cu cea a mesajului original ***n***. În cazul în care avem avans parțial, suma dimensiunilor partițiilor va fi egală cu dimensiunea originalului ***n=l+m.***

5.8.1 Criptarea

Folosind notațiile anterioare, pentru criptarea prin metoda strecurării cu *avans total* se poate scrie:

$$P = \begin{Bmatrix} p_i = m_i \otimes c_x & dacă & d_x = 0 \\ p_i = random & dacă & d_x = 1 \end{Bmatrix}$$

$$Q = \begin{Bmatrix} q_i = m_i \otimes c_x & dacă & d_x = 1 \\ q_i = random & dacă & d_x = 0 \end{Bmatrix}$$

$$unde \;\; x = \begin{Bmatrix} i \bmod k, dacă\; i \bmod k \neq 0 \\ k, dacă\; i \bmod k = 0 \end{Bmatrix}$$

$$d_x \in \{0,1\},\; \mathrm{i} = \overline{1,k}$$

Iar pentru varianta cu avans parțial putem scrie :

$$P = \{ p_i = m_i \otimes c_x \quad dacă \quad d_x = 0 \} \qquad \mathrm{p_i} \in \{0,1\},\; \mathrm{i} = \overline{1,l}$$

$$Q = \{ q_i = m_i \otimes c_x \quad dacă \quad d_x = 1 \} \qquad q_\mathrm{i} \in \{0,1\},\; \mathrm{i} = \overline{1,m}$$

Etapele criptării sunt următoarele:

1 Se citesc mesajul clar **M**, cheia inițială C_i şi cheia numerică R_k

2 Mesajul clar şi cheia inițială sunt binarizate.

3 Se generează cheia extinsă C_{ex} şi cheia echivalentă C_{eq} ținând cont de *prag* ***T*** şi de cheia numerică R_k conform procedeului descris în capitolul 5.5.4.

4 Se construiesc cele două partiții. Partițiile primesc biți în funcție de cheia extinsă şi cheia echivalentă.

Cele două partiții pot fi obținute fie prin metoda *avansului total,* fie prin metoda *avansului parțial*. În cazul avansului total se adaugă zgomot aleatoriu în partiții.

Schema bloc a sistemului de criptare este reprezentată în figura 7.

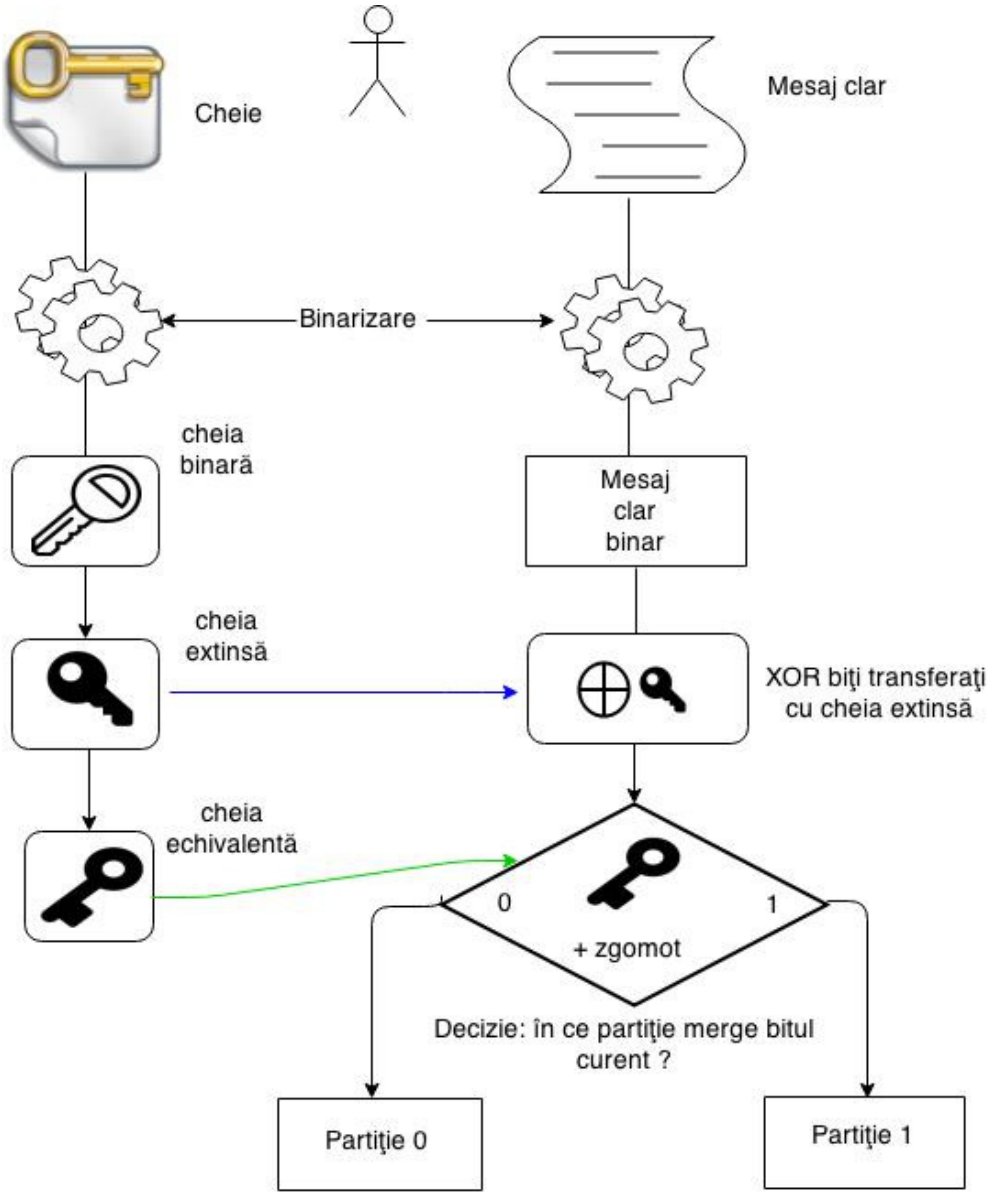


Figura 7 Schema bloc a operației de criptare

5.8.2 Decriptarea

În varianta cu ***avans total***, pentru decriptare putem scrie următoarele:

$$M = \begin{Bmatrix} m_i = p_i \otimes c_x & dacă & d_x = 0 \\ m_i = q_i \otimes c_x & dacă & d_x = 1 \end{Bmatrix} \qquad unde \;\; x = \begin{Bmatrix} i \bmod k, dacă\; i \bmod k \neq 0 \\ k, dacă\; i \bmod k = 0 \end{Bmatrix}$$

Practic reconstruim mesajul clar, bit cu bit, citind câte un bit dintr-una din partiții în funcție de bitul curent al cheii echivalente. Acest bit este apoi făcut XOR cu bitul curent al cheii extinse pentru a afla bitul original.

Se poate observa că la decriptare ținem cont numai de acei biți din partiții care conțin informația utilă. Biții care au fost introduşi ca şi *zgomot* în partiții sunt pur şi simplu ignorați. Acest lucru este posibil datorită mecanismului prin care un bit este citit din partiția indicată de

valoarea cheii echivalente.

Etapele principale de decriptare :

1. Se introduc cheile de decriptare şi cheia numerică
2. Cheia de decriptare este convertită în şir binar
3. Se generează cheia extinsă binară şi cheia echivalentă binară
4. Din partiția indicată de valoarea *cheii echivalente* se extrage bitul util
5. Se decriptează bitul extras prin XOR cu bitul curent din *cheia extinsă* şi se adaugă şirului deja decriptat (în continuare, mesajul clar binar obținut se poate converti în şir ASCII)
6. Avansăm la următoarea valoare în chei, respectiv, indiferent din ce partiție s-a citit bitul util, vom avea avans în ambele partiții.

Pentru a doua variantă, cea cu ***avans parțial,*** decriptarea presupune aproximativ acelaşi lucru cu diferența că nu mai există biți *zgomot* care ar trebui ignorați. Cele două partiții care conțin mesajul criptat au lungimi proporționale cu numărul elementelor de 0 şi 1 ale cheii extinse.

Vom avea patru variabile contor:

- un i pentru poziția curentă în mesajul decriptat
- un j^0 pentru poziția curentă în partiția 0
- un j^1 pentru poziția curentă în partiția 1
- un x pentru poziția curentă în chei

Cu aceste notații putem scrie:

$$M = \begin{Bmatrix} m_i = p_{j0} \otimes c_x & dacă & d_x = 0 \\ m_i = q_{j^1} \otimes c_x & dacă & d_x = 1 \end{Bmatrix}$$

Etapele de decriptare sunt identice până la punctul 5. La punctul 6 avem avans numai în acea partiție din care s-a citi bitul curent. Nu se mai pune problema saltului peste un bit *zgomot.*

Schema bloc pentru decriptare în cazul strecurătorii de biți este redată în figura 8.

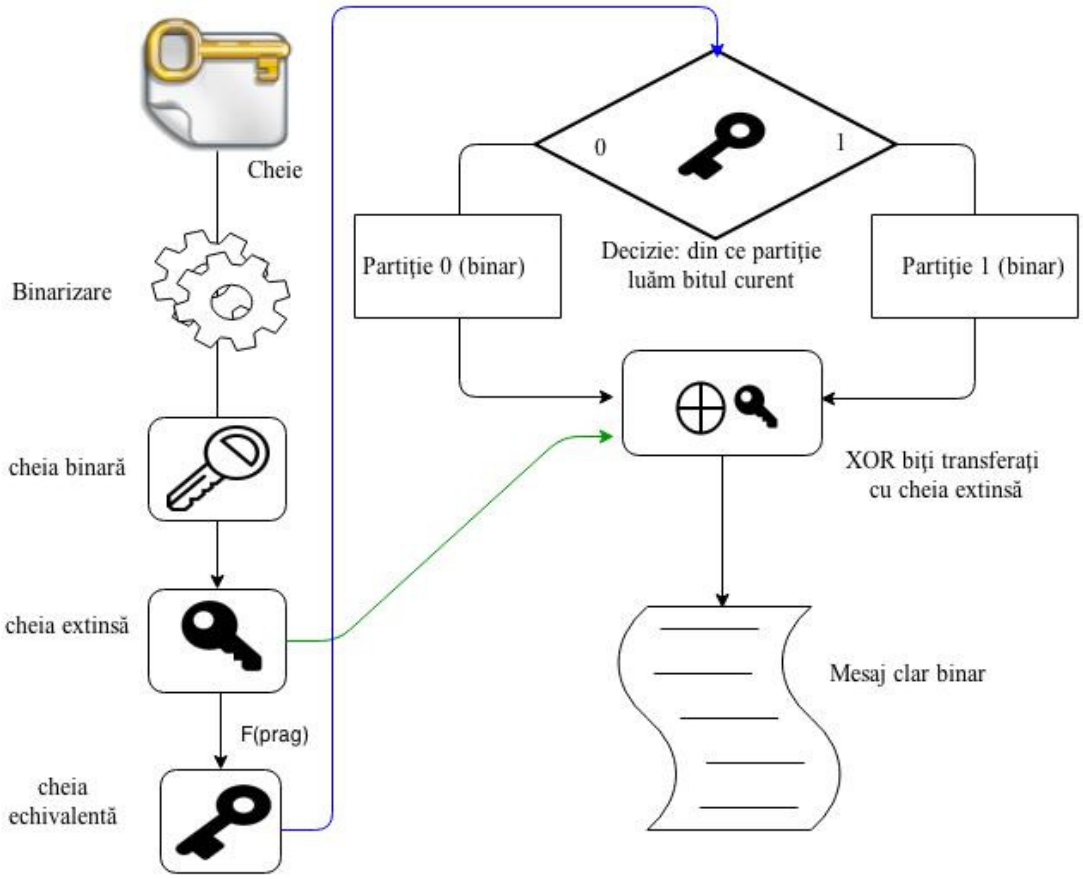


Figura 8 Schema bloc a operației de decriptare

Capitolul 9 Cu aceste considerații am realizat o aplicație pentru criptarea imaginilor .

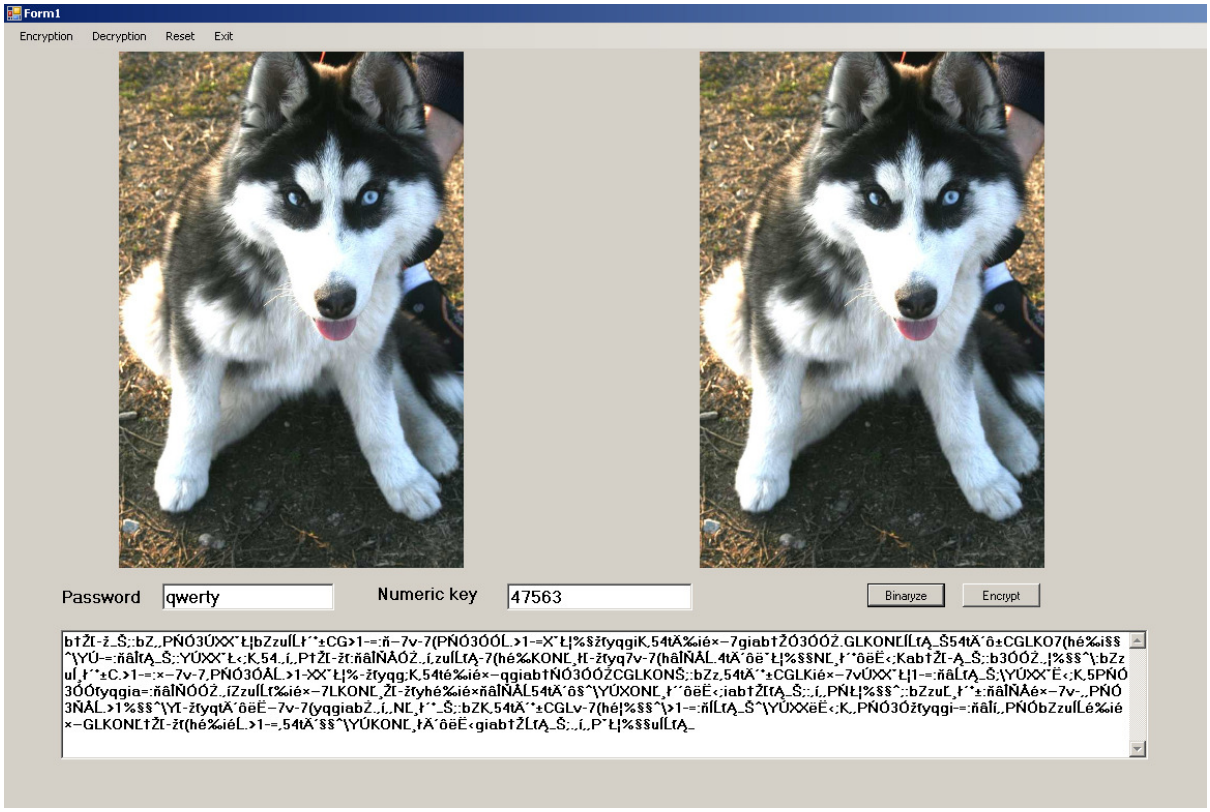


Figura 9 Interfața aplicației pixel-sieve

După introducerea parolei şi a cheii de criptare aplicația generează cheia extinsă, cheia echivalentă şi criptează informația. Rezultatul criptării este redat in figura următoare:

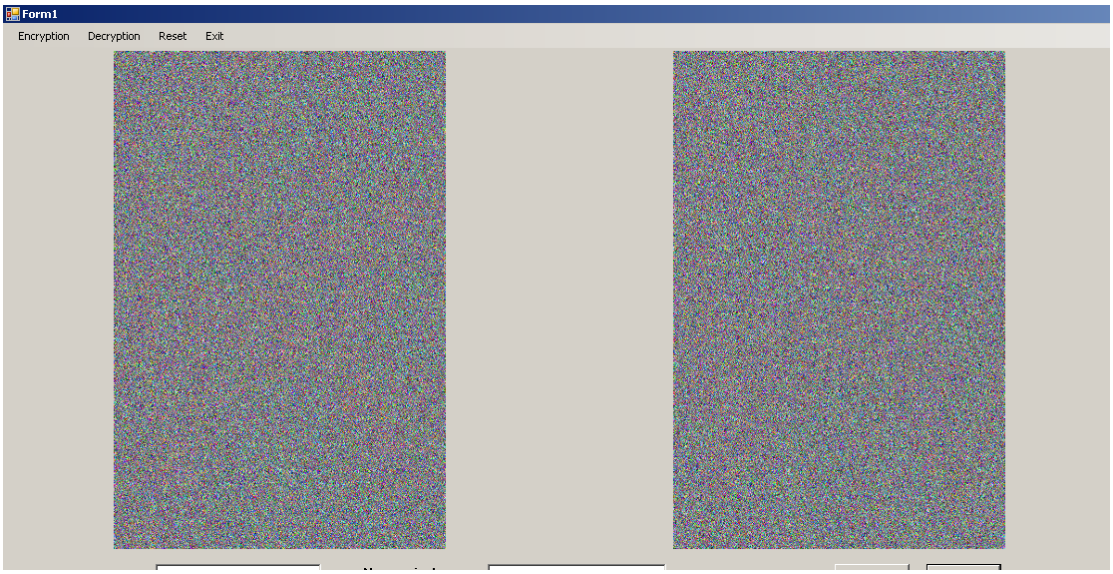


Figura 10 Rezultatul criptării

Testarea robusteții metodei criptografice este descrisă în **Capitolul 5.10.**

Pentru început au fost comparate originalul cu una din partiții:

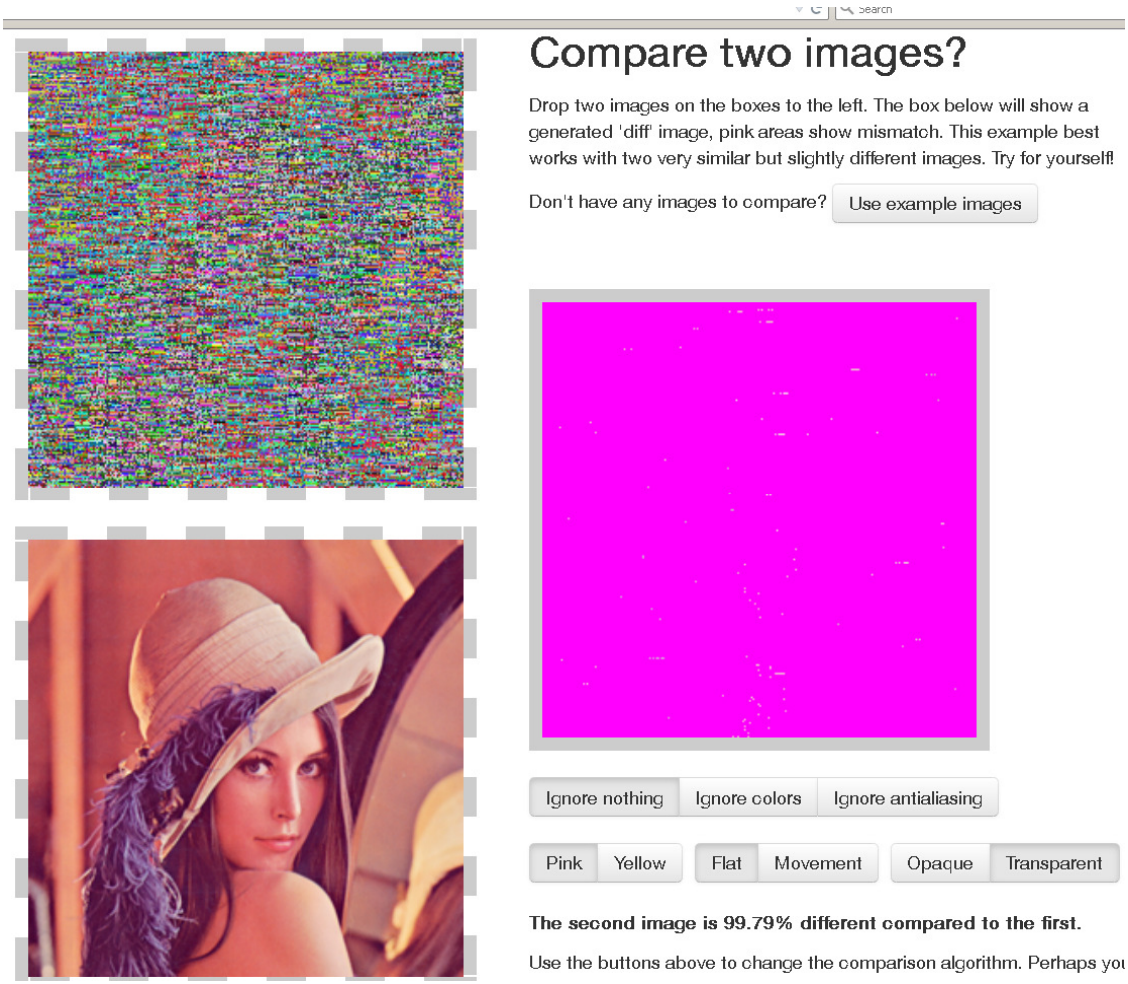


Figura 11 Rezultatul comparației unei partiții criptate cu originalul

Respectiv partițiile între ele

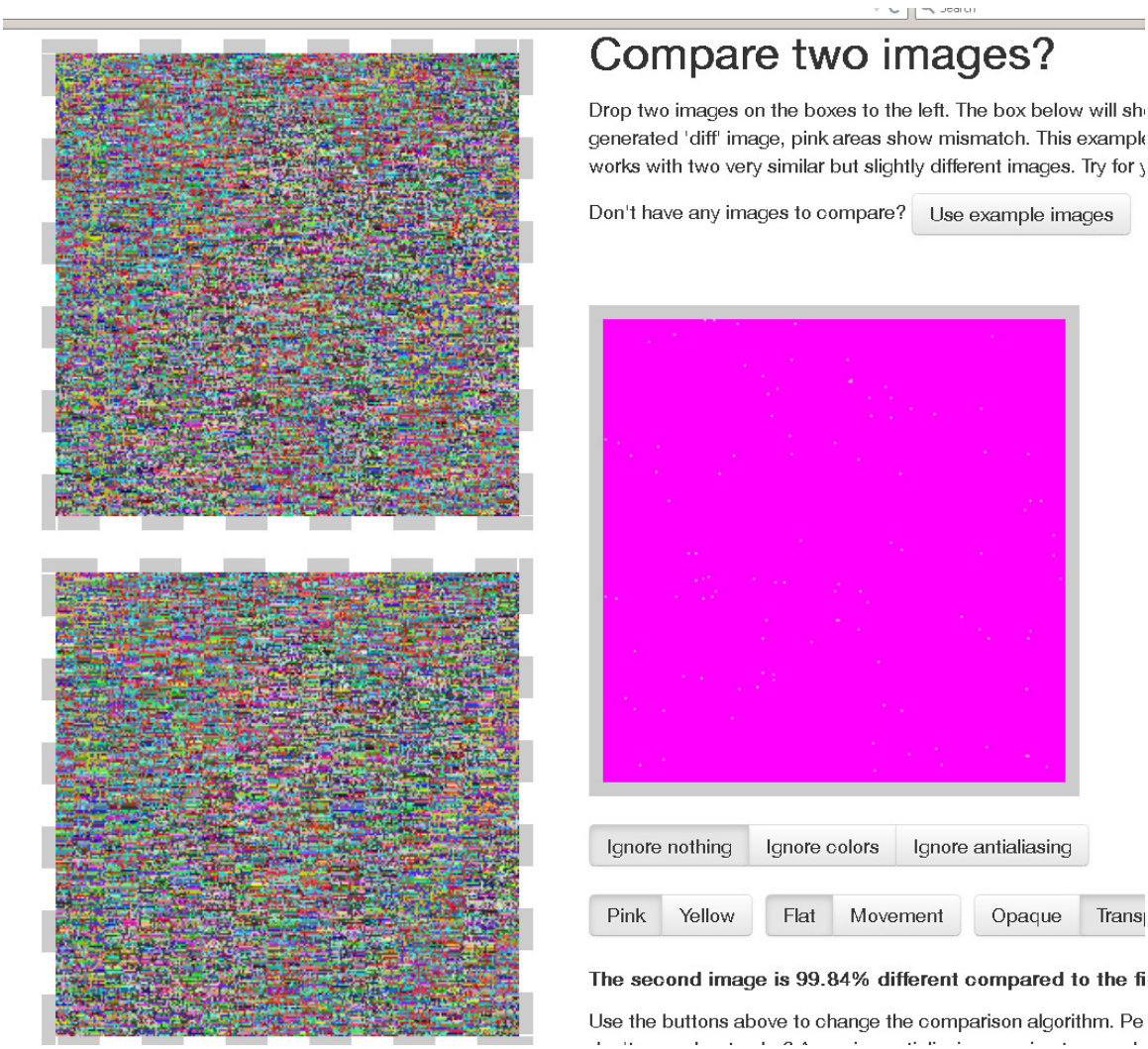


Figura 12 Comparația partițiilor

Au fost aplicate metode specifice de prelucrare/filtrare de imagine pentru a vedea dacă din partiții se poate extrage informație utilă:

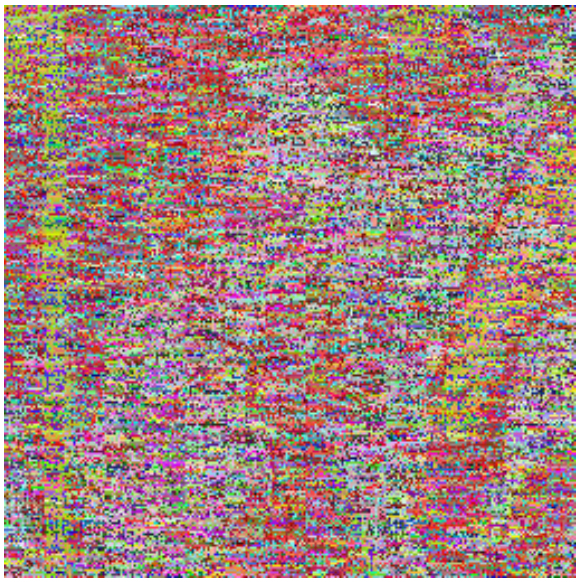


Figura 13 Rezultatul filtrării partițiilor suprapuse în Photoshop

Şi în final am făcut măsurători statistice pentru a vedea gradul de mascare a informației.

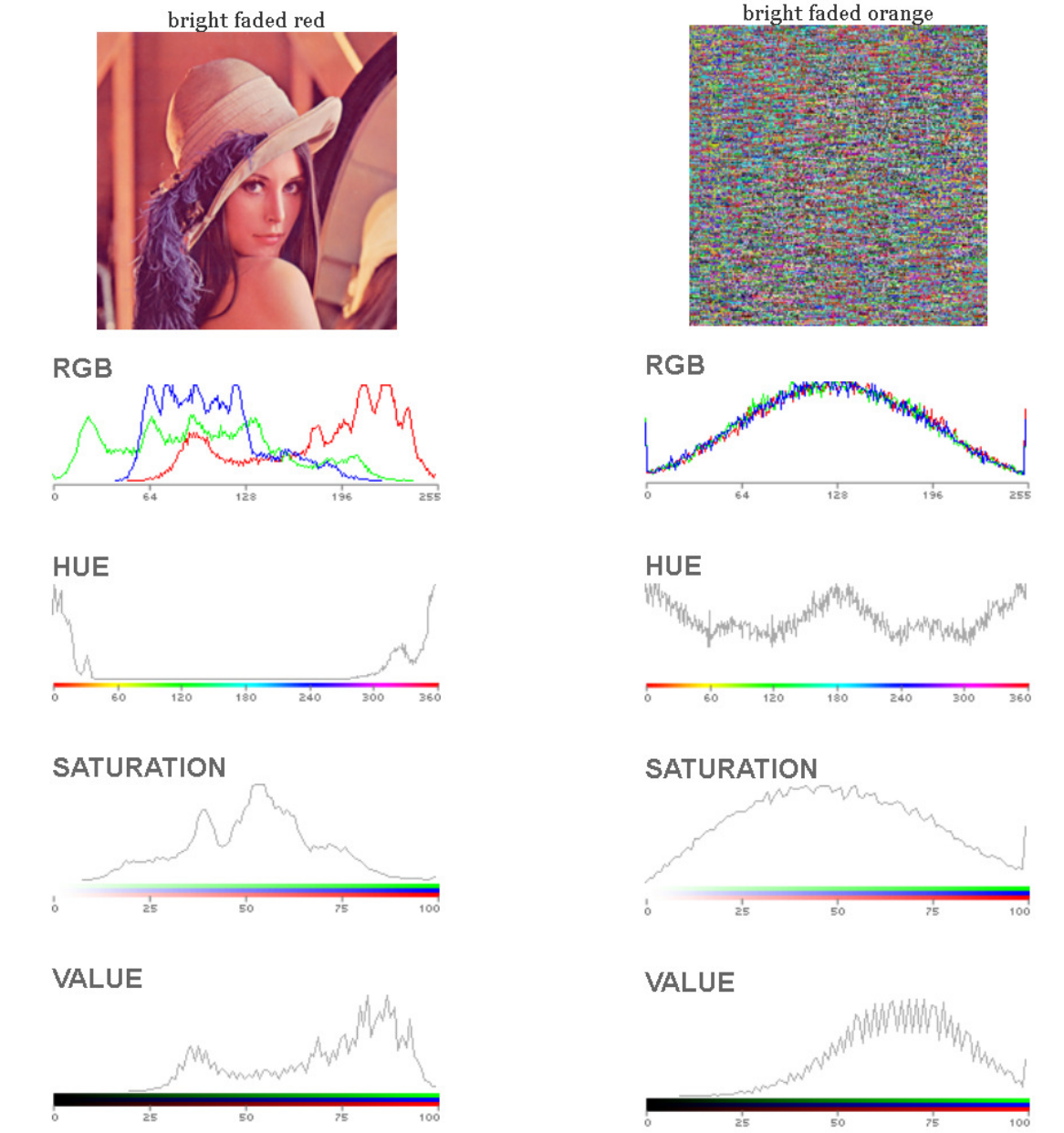


Figura 14 Histogramele imaginii originale şi a imaginii criptate

După analiza rezultatelor obținute cu aceste metode putem spune că metoda pixel sieve este sigură şi produce imagini criptate cu o bună disimulare a informației.

În **capitolul 5.10.2** am testat **performanțele computaționale** ale metodei. Din testele efectuate rezultă că timpul de criptare depinde, după cum era de aşteptat, de rezoluția imaginii (dimensiunea în pixeli X•Y) fără însă a depinde de dimensiunea fişierului.

În ceea ce priveşte timpul de generare a cheilor extinse şi echivalente, timpul de generare a cheii depinde de:

- lungimea cheii inițiale,

- lungimea cheii numerice,
- numărul de iteraţii datorate deplasării biţilor cheii.

În final, în **capitolul 5.11** sunt propuse câteva **utilizări ale metodei** criptografice:

- Autentificarea sistemelor şi a utilizatorilor

- Autentificarea unui document

CONCLUZII. DIRECŢII DE CERCETARE VIITOARE

Ca şi direcţii viitoare de cercetare dorim să testăm şi să îmbunătăţim metodele pixel-sieve şi bit-sieve. Intenţionăm să creem o aplicaţie care să permită autentificarea suplimentară prin metoda CAPTCHA descrisă în **capitolul 5.11.2**. Metoda generării de chei extinse prin XOR şi key-shifting merită de asemenea studiată mai în detaliu. O altă idee pentru cercetări viitoare se referă la îmbinarea metodei strecurării cu steganografia. Cum ar fi de exemplu dacă informaţia pe care dorim să o ascundem ar fi de fapt împărţită pe două sau mai multe imagini purtătoare. Şi cu studiul şi dezvoltarea acestui aspect îşi propune autorul continuarea cercetărilor în domeniu.

BIBLIOGRAFIA TEZEI

[AAtan] Adrian Atanasiu, *Curs de Criptografie* http://www.galaxyng.com/adrian_atanasiu/cript.htm

[Baden915] Sir Robert Baden-Powell *My Adventures as a Spy* 1915

[Bor96] Boran Sean, IT Security Cookbook, Draft V0.84 1996

[BreNa89] David F. C. Brewer, Michael J. Nash *The Chinese wall security policye* IEEE Symposium on reasarch in security and privacy , 1-3 may 1989, OAKLAND, CALIFORNIA. (pp 206-14)

[Burt04] Emil Burtescu, *"Securitatea Datelor în Sistemele Informatice Economice"*, 2004

[CheBel94] Bill Cheswick , Steve M. Bellovin, *Firewalls and Internet Security*, Addison-Wesley, 1994

[Chen01] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, *A new encription algorithm for image cryptosystems,* The Journal of Systems and Software 58 (2001), 83-91

[Chen06] Chao-Shen Chen, Rong-Jian Chen, *Image Encryption and Decryption Using SCAN Methodology*, Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06), 2006

[Chou10] Vaibhav Choudhary, Pravin Kumar, Kishore Kumar, D.S. Singh *Modified Pixel Sieve Method for Visual Cryptography* Indian Journal of Computer Science and Engineering Vol. 1 No. 4 321-326 2010

[Chou11] Vaibhav Choudhary, Pravin Kumar, Kishore Kumar and D S Singh. *An Improved Pixel Sieve Method for Visual Cryptography*. International Journal of Computer

Applications 12(9):7–10, January 2011. ISSN 0975-888

[CHUKS] Chuck Semeria, *Internet Firewalls and Security A Technology Overview,* http://www.linuxsecurity.com/resource_files/firewalls/nsc/500619.html

[ClWil87] Clark, David D.; Wilson, David R.; *A Comparison of Commercial and Military Computer Security Policies*; in Proceedings of the 1987 IEEE Symposium on Research in Security and Privacy (SP'87), May 1987, Oakland, CA; IEEE Press, pp. 184–193

[DECo00] D. E. Comer. *Internetworking with TCP/IP: Principles,Protocols, and Architecture*, volume I. Prentice-Hall, Englewood Cliffs, NJ, fourth edition, 2000

[DzMo06] Ioan Dziţac, Grigor Moldovan, *Sisteme distribuite. Modele informatice,* Editura Universităţii Agora, 2006 isbn 10 973-87960-9-1

[FYS07] Frank Y. Shih *Digital Watermarking and Steganography: Fundamentals and Techniques* , CRC Press, 2007, ISBN: 9781420047578

[Gra72] Graham, G.S. , P. J. Denning, *Protection : Principles and Practice*, Proc. Of AFIPS Spring joint compute conference, vol. 40, 1972

[GRB79] G. R. Blakley, *Safeguarding cryptographic keys*, proceedings of the National Computer Conference, 48, pp 313–317, 1979.

[GRN] Sarah Granger, *Social Engineering Fundamentals, Part I: Hacker Tactics*, on http://www.securityfocus.com/infocus/1527/ (accesat in marte 2007)

[Guha96] Biswaroop Guha, Biswanath Mukherjee, *Network Security via Reverse Engineering of TCP Code: Vulnerability Analysis and Proposed Solutions*. Proc. of the IEEE Infocom'96 , San Francisco, CA, March 1996, pp. 603-610

[Incze04] dep. Informatică, contributor **Incze Arpad**, *Document intern: Raport de audit de securitate 2004*

[Incze05] **Incze Arpad**, Ioan Ileană, Manuela Kadar, *Increasing the security of an ACCESS database,* proceedings of „Several aspects on biology, chemistry, computer science, mathematics and physics", Oradea 2005 ISBN 973-759-142-9

[Incze10a] **Incze Arpad**, *Secret sharing & visual cryptography through bit sieve for fast image encryption,* proceedings AQTR 2010 THETA 17th International IEEE confernce on Automation,Quality and Testing, Robotics, ISSN 978-973-662-562-6

[Incze10b] **Incze Arpad**, *Pixel Sieve method for secret sharing & visual cryptography,* Proceedings of the 9th RoEduNet IEEE International conference, Sibiu, 24-25 june, 2010 in ***ISI Conference Proceedings Citation Index***

[Incze10c] **Incze Arpad**, Moldovan Grigor, Maria Muntean, *From pixel sieve to bit sieve. Bit level based secret sharing cryptographic method,* in proceedings 11th International symposium CINTI, Budapest 18-20 nov. 2010 978-1-4244-9278-7 indexat **IEEE**

[Incze11] **Incze Arpad**, *Social Enineering and education in fight against cybercrime*, Acta Universitas Apulensis- Special Issue, Proceeding of ICTAMI 2011, ISSN 1582-5329 p541-553 **B+ CNCSIS**

[Incze12] **Incze Arpad,** *A greater involvement of education in fight against cybercrime* 2nd WORLD CONFERENCE ON EDUCATIONAL TECHNOLOGY RESEARCHES NEAR EAST UNIVERSITY 27-30 June 2012 NICOSIA – NORTH CYPRUS Procedia-Social and Behavioral vol 83 Journal ISSN: 1877-0428 by ELSEVIER ***ISI Conference Proceedings Citation Index***

[Incze14a] **Incze Arpad**, "*Cryptographic key issues and solutions for the bit sieve/pixel-sieve method*", *AQTR*, 2014, 2014 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR) 2014, pp. 1-5, doi:10.1109/AQTR.2014.6857853 ***ISI Web of Science***

[Incze14b] **Incze Arpad**, *Solutions regarding some cryptographic key issues for the pixel-sieve cryptographic method* , 4th WORLD CONFERENCE on INNOVATION and COMPUTER SCIENCES (INSODE-2014) Sapienza University, Faculty of Economics April 11-13, 2014 Rome, Italy www.insode.org in curs de publicare in AWERProcedia Information Technology and Computer Science // Global Journal on Technology ISSN: 2147-5369

[IPSEC95] IPSEC Working Group, Ashar Aziz, Tom Markson, Hemma Prafullchandra *Simple Key-Management For Internet Protocols* Sun Microsystems, Inc. December 21, 1995, http://tools.ietf.org/html/draft-ietf-ipsec-skip-06

[Jiun99] Jiun-In Guo, Jui-Cheng Yen, *A new mirror-like image encryption algorithm and its VLSI architecture*, Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China 1999

[Kot12] Koteswari, S.; Paul, P. John; Indrani, S., *VC of IRIS Images for ATM Banking,* International Journal of Computer Applications, Volume 48 No. 18 June 2012 ISSN 0975-8887

[LJo95] L. Joncheray. *A simple active attack against TCP*. Proceedingsof the Fifth Usenix Unix Security Symposium, Salt Lake City, UT, 1995.

[MaBo01] S.S.Maniccam, N.G. Bourbakis, *Lossless image compression and encryption using SCAN*, Pattern Recognition 34 (2001), 1229-1245

[Men96] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone *Handbook of Applied Cryptography* CRC Press ISBN: 0-8493-8523-7 October 1996 on http://www.cacr.math.uwaterloo.ca/hac/

[Mill88] S. P. Miller , B. C. Neuman , J. I. Schiller , J. H. Saltzer, *Kerberos Authentication and Authorization System,* In Project Athena Technical Plan ,1988

[Mit02] Kevin Mitnick, William L. Simon, *The Art of Deception*, Wiley Publishing inc 2002, Hardback ISBN 0-471-23712-4

[MOL06] Grigor Moldovan, Ioan Dziţac, *Sisteme distribuite. Modele matematice,* Editura Universităţii Agora, 2006 isbn 10 973-88205-0-2

[Morr85] Robert T. Morris, *A Weakness in the 4.2BSD Unix TCP/IP Software*, Computing Science Technical Report 117, AT&T Bell Laboratories, Murray Hill, NJ, February 1985.

[MOV--] A. Menezes, P. Oorschot, S. Vanstome, *Handbook of Applied Cryptography* (https://notendur.hi.is/pgg/Handbook%20of%20Applied%20Cryptography.pdf)

[MRan04] Marcus J. Ranum , *Tales From The Early Days of the Firewall* , CyberGuard User Conference, 2004, West Palm Beach http://www.ranum.com/security/computer _security/archives/

[MunInc10] Maria Muntean, Honoriu Vălean, Liviu Miclea, **Incze Arpad** *A novel intrusion detection method based on support vector machines*, proceedings of 11th International symposium CINTI, Budapest 18-20 nov, 2010. 978-1-4244-9278-7 indexat **SCOPUS**

[NamSnet02] SamsNet*, Securitatea în internet*, Editura Teora, Bucureşti, 2002

[Naor94] Moni Naor and Adi Shamir, Visual Cryptography, EUROCRYPT 1994, pp1–12

[Nort02] Peter Norton , Dave Kearns, *Reţele de calculatoare,* Editura Teora, 2002

[Perl88] R. Perlman. *Network Layer Protocols with Byzantine Robustness*. PhD thesis, M.I.T., 1988

[PRM14] Praveen Gujjar J., Raghvendra M. Dev *Concealment of Images using S^3 approach* ISRASE First International Conference on Recent Advances in Science & Engineering 2014 (ISRA SE-2014) ISRASE eXplore digital library

[SBel04] Steven M. Bellovin, *A Look Back at "Security Problems in the TCP/IP Protocol Suite"* 20th Annual Computer Security Applications Conference (ACSAC), December 2004, in as part of the "classic papers" track.

[SBel89] Steve Bellovin, *Security Problems in the TCP/IP Protocol Suite*, Computer Communication Review, Vol. 19, no. 2 (April 1989) pg 32-48

[SBel95] Steven M. Bellovin, *Using the Domain Name System for System Break-Ins,* Proceedings of the Fifth Usenix Unix Security Symposium 1995

[SCH04] Schneier, Bruce - *Secrets & Lies,* Wiley Publishing, Inc., 2004

[Schu94] Christoph L. Schuba. and Eugene H. Spafford *Countering Abuse of Name-Based Authentication,* Computer Sciences Department Purdue University West Lafayette, IN 47907 CSD-TR-94-029 April, 1994

[Sham79] Shamir, Adi , *How to share a secret*, Communications of the *ACM* 22 1979 : 612–613

[Shob13] Shobha Patil, V.R.Udupi *A Secure Approach to Image Encryption of color image without using key* International Journal of Current Engineering and Technology ISSN 2277 – 4106 ©2013 INPRESSCO. Available at http://inpressco.com/category/ijcet

[Sidd12] Siddharth Malik, Anjali Sardana *A Keyless Approach to Image Encryption,* 2012 International Conference on Communication Systems and Network Technologies 978-0-7695-4692-6/12 $26.00 © 2012 IEEE DOI 10.1109/CSNT.2012.189

[Sin03] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, ARTICLE IN PRESS, 2003, 1-6, www.elsevier.com/locate/optcom

[Stein88] Jennifer G. Steiner , Clifford Neuman , Jeffrey I. Schiller, Kerberos: *An Authentication Service for Open Network Systems,* Usenix Conference Proceedings 1988

[Tan98] Andrew S. Tanenbaum, *Reţele de calculatoare*, Computer Press Agora 1998

[TWO01] Terry William Ogletree – FIREWALLS. Protecţia reţelelor conectate la internet, Ed TEORA 2001

[VBOC06] ing. Valer Bocan, *CONTRIBUŢII LA CREŞTEREA DISPONIBILITĂŢII, SCALABILITĂŢII SI SECURITĂŢII SISTEMELOR DE COMUNICAŢIE*, Teza de doctorat, Universitatea "Politehnica" din Timişoara 2006

[Venk13] Venkatesh M.R. , Roopanjali. Daddi, *SDS Technique For Secret Image Encryption,* International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 4, April – 2013 ISSN: 2278-0181

[VERIZONE] http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

[VVP00] Victor-Valeriu Patriciu, Neculai-Daniel Stoleru *APLICAŢII LA CRIPTOGRAFIA*

VIZUALĂ, Volumul Conferinței de Informatică Teoretică şi Tehnologii Informatice, Univ. Ovidius, Constanța, mai. 2000

[VVP95] Victor-Valeriu Patriciu – *Criptografia si securitatea rețelelor de calculatoare cu aplicîtii în C şi Pascal* Editura: Tehnica, 1996

[WhNew05] Whitaker A., Newman D, *Penetration testing and Network Defence* , Publisher: Cisco Press November 04, 2005 , ISBN: 1-58705-208-3

[YuvJn08] Yuval Ben-Itzhak, "*The Cybercrime 2.0 Evolution*", The ISSA Journal, June 2008

[YuvOc08] Yuval Ben-Itzhak, "*Organized Cybercrime*", The ISSA Journal, October 2008

Bibliografie de sinteză. Resurse online.

Jim Doherty, "*A Brief History of Data Theft*", The ISSA Journal, June 2008

Bruce Schneier, *Schneier on security,* Wiley Publishing inc., 2008, ISBN 978-0470-39535-6

Bruce Schneier, *Secrets & Lies Digital Security in a Networked World*, John Wiley & Sons, 2000 ISBN 0-471-25311-1

Schell, B.H. and Martin, C. *Contemporary World Issues Series: Cybercrime: A Reference Handbook*. Santa Barbara, CA: ABC-CLIO, 2004

T. ElGamal (1985). "*A public key cryptosystem and a signature scheme based on discrete logarithms*". IEEE Trans inf Theo 31 (4): 469–472.

Ralph Merkle and Martin Hellman, Hiding Information and Signatures in Trapdoor Knapsacks, IEEE Trans. Information Theory, 24(5), September 1978

Farmer, Dan and Venema, Wietsa *Improving the Security of your site by breaking into it* Sun Microsystems (11/29/2000) URL:http://www.geocities.com/hackernet_99/breakintoyoursite.htm

Gibbs, Mark *Any Port is a Hacker Storm* (11/29/2000) URL: http://www.antionline.com/

Fordham, Doug *Intelligence Preparation of the Battlefield* (6/19/2000)

URL: http://www.securityfocus.com/focus/ih/articles/battlefield.html (12/3/2000)

Kubin, Larry *Protect Your Business From Hacker Attack*s

Reto E. Haeni, *Firewall Penetration Testing*, , 1997 r.haeni@cpi.seas.gwu.edu

Diffie W, , Hellman M., *Multiuser criptography* , National Computer Conference, New York 1976

R. Rivest, A. Shamir, L. Adleman. "*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*". Communications of the ACM, Vol. 21 (2), pp.120–126. 1978. Previously released as an MIT "Technical Memo" in April 1977. Initial publication of the RSA scheme. (http://theory.lcs.mit.edu/~rivest/rsapaper.pdf)

URL: http://www.suite101.com/article.cfm/1345/11549 (11/29/2000)

http://www.winpcap.org/

http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.42.1117&rep=rep1&type=pdf

http://www.brainbell.com/tutorials/Networking/Proxy_Servers.html

http://hermes.etc.utt.ro/teaching/tart/FINAL.pdf

http://www.linuxsecurity.com/resource_files/firewalls/nsc/500619.html

www.buzzsurf.com/surfatwork/

http://www.webopedia.com/TERM/S/SOCKS.html

www.buzzsurf.com/surfatwork/

http://www.bitvise.com/winsshd

http://www.chiark.greenend.org.uk/~sgtatham/putty/

http://www.no-ip.com/services/managed_dns/free_dynamic_dns.html

http://www.ssh.com/.

http://www.teamviewer.com/en/index.aspx

http://sourceforge.net/projects/packetyzer/

http://www.securityfocus.com/infocus/1527

http://www.dcd.uaic.ro/default.php?t=site&pgid=82
http://www.hackerwhacker.com/

.