MINISTERUL EDUCAȚIEI NAȚIONALE
UNIVERSITATEA PETROL-GAZE DIN PLOIEȘTI
ȘCOALA DOCTORALĂ

TEZĂ DE DOCTORAT
- REZUMAT -

CERCETĂRI PRIVIND SECURITATEA SISTEMELOR AUTOMATE

Conducător științific
Prof. univ. dr. ing. Nicolae PARASCHIV

Autor
Ing. Emil PRICOP

Ploiești
2017

Mulțumiri

Adresez cele mai sincere mulțumiri domnului Prof. Dr. Ing. Nicolae Paraschiv, coordonatorul științific al acestei teze de doctorat, pentru răbdarea și exigența cu care mi-a îndrumat pașii în lumea științei. Aduc toată aprecierea și recunoștința de care pot da dovadă domnului Profesor pentru faptul că mi-a fost mai mult decât conducător științific, fiind un adevărat mentor, contribuind la formarea mea ca profesionist și ca om, și pentru că mi-a fost întotdeauna alături, sprijinindu-mă și încurajându-mă de fiecare dată.

Cu deosebită stimă aduc mulțumirile mele domnilor profesori Radu-Emil Precup, Dan Popescu și Nicu Bizon pentru că au acceptat să analizeze această teză de doctorat și să facă parte din comisia de susținere publică a acesteia.

Mulțumesc doamnei conf. dr. ing. Sanda Mihalache pentru colaborarea fructuoasă din ultimii ani, pentru sfaturile și sugestiile pe care le-am primit pe tot parcursul cercetărilor din stagiul doctoral.

Mulțumesc pentru răbdarea de care au dat dovadă și pentru sugestiile oferite doamnei prof. dr. ing. Otilia Cangea și domnului prof. dr. ing. Gabriel Rădulescu.

Aprecierea și mulțumirile mele sunt adresate domnilor dr. ing. Octavian Ionescu și conf. dr. ing. Zoran Constantinescu pentru sfaturile și discuțiile constructive purtate de-a lungul timpului.

Sincere mulțumiri sunt adresate colegilor și prietenilor mei conf. dr. ing. Grigore Stamatescu și conf. dr. ing. Mihai Oproescu pentru toate sfaturile primite și pentru sprijinul acordat în organizarea anuală a IWSSS – International Workshop on Systems, Safety & Security.

Mulțumesc pe această cale domnului dr. ing. Jaouhar Fattahi pentru schimburile de idei și colaborarea mai mult decât benefică pe care o avem în domeniul securității sistemelor.

Sincere mulțumiri și recunoștință domnului ing. Toader Melinte, director al S.C. Seektron S.R.L., Ploiești, unul dintre mentorii mei, care a avut un rol deosebit în formarea mea ca om, inginer și cercetător și care mi-a deschis apetitul pentru domeniul securității sistemelor.

Mulțumesc pentru sprijinul moral și material oferit pe tot parcursul stagiului doctoral domnului ing. Sabin Stamatescu, director al S.C. ASTI Automation S.R.L..

Adresez mulțumiri colegului meu ing. Florin Zamfir pentru sprijinul și prietenia oferite.

Nu în ultimul rând doresc să adresez neprețuite mulțumiri și să dedic această teză de doctorat familiei care m-a susținut și m-a înconjurat cu multă răbdare și înțelegere pe parcursul întregii perioade de studii doctorale.

Cuprins

Mulțumiri 2
Cuprins 3
Introducere 5
Capitolul 1. Conceptualizarea securității sistemelor automate 7
1.1. Importanța securității sistemelor tehnice 7
1.2. Vulnerabilitățile sistemelor automate 7
1.2.1. Caracterul integrator al sistemelor automate actuale 7
1.2.2. Analiza vulnerabilităților sistemelor automatizate ierarhizate și distribuite 8
1.3. Analiza vulnerabilităților unor protocoale de rețea industriale 9
1.3.1. Analiza vulnerabilităților protocolului Modbus 9
1.3.2. Analiza vulnerabilităților protocolului DeviceNet 9
1.3.3. Analiza vulnerabilităților protocolului PROFIBUS 10
1.4. Concluzii parțiale 10
Capitolul 2. Echipamente și metode destinate asigurării securității perimetrale a echipamentelor aferente sistemelor automate 12
2.1. Securitatea perimetrală a sistemelor automate 12
2.2. Identificarea biometrică a persoanelor 12
2.2.1. Algoritmi destinați analizei amprentei digitale 14
2.2.2. Algoritmi destinați comparării șabloanelor amprentelor digitale 15
2.2.3. Tehnologii biometrice de identificare a persoanelor pe baza analizei imaginii irisului 15
2.3. Utilizarea tehnologiei RFID pentru dezvoltarea unui sistem robust de identificare a persoanelor 15
2.4. Concluzii parțiale 16
Capitolul 3. ..... Echipamente și metode destinate asigurării securității informatice a sistemelor automate 18
3.1. Securitatea informatică a sistemelor de conducere a proceselor 18
3.2. Sisteme de tip firewall 19
3.2.1. Clasificarea sistemelor firewall 19
3.2.2. Utilizarea sistemelor firewall în cadrul asigurării securității sistemelor automate 19
3.3. Sisteme de tip honeypot și honeynet 21
3.3.1. Considerații generale privind dispozitivele de tip honeypot 21
3.3.2. Clasificarea dispozitivelor de tip honeypot 21
3.4. Rezultate experimentale obținute cu ajutorul dispozitivelor honeypot 22
3.4.1. Prezentarea sistemului T-Pot 22
3.4.2. Rezultate experimentale obținute 23
3.5. Concluzii parțiale 27
Capitolul 4.Contribuții privind dezvoltarea unor metode de estimare a probabilităților de apariție și de succes ale unui atac informatic asupra unui sistem automat 28
4.1. Introducere 28
4.2. Evaluarea automată a vulnerabilităților unui sistem informatic 28
4.2.1. Baze de date care descriu posibile vulnerabilități 28

4.2.2. Identificarea automată a vulnerabilităților sistemelor informatice....29
4.3. Contribuții la determinarea profilurilor specifice ale potențialilor atacatori....30
4.3.1. Tipologii de atacatori....30
4.3.2. Definirea scorului profilului de atacator....30
4.4. Contribuții privind estimarea probabilității de apariție a unui atac informatic asupra unui sistem automat....32
4.5. Contribuții privind estimarea probabilității de reușită a unui atac informatic asupra unui sistem automat....34
4.6. Concluzii parțiale....35
Capitolul 5. Contribuții privind dezvoltarea unui mecanism pentru autentificarea senzorilor conectați prin protocolul Modbus/TCP....37
5.1. Caracterizarea protocolului de comunicație Modbus standard....37
5.1.1. Rețele industriale și conectivitate....37
5.1.2. Protocolul Modbus standard....37
5.2. Analiza protocolului Modbus/TCP....38
5.2.1. Particularitățile protocolului Modbus/TCP....38
5.2.2. Vulnerabilități de securitate ale protocoalelor Modbus și Modbus/TCP....39
5.3. Contribuții la dezvoltarea unui mecanism de autentificare pentru senzori conectați prin Modbus/TCP....39
5.3.1. Necesitatea autentificării senzorilor conectați prin Modbus/TCP....39
5.3.2. Demonstrarea posibilităților de interceptare a datelor transmise prin protocolul Modbus/TCP....40
5.3.3. Proiectarea conceptuală a metodei de autentificare propuse....41
5.3.4. Verificarea autenticității datelor recepționate....42
5.3.5. Testarea în laborator a soluției propuse pentru autentificarea senzorilor conectați prin protocolul Modbus/TCP....43
5.4. Concluzii parțiale....44
Capitolul 6.... Contribuții privind realizarea unui sistem de identificare a personalului de operare a procesului....45
6.1. Structura sistemului propus....45
6.2. Cardul RFID biometric....45
6.2.1. Cerințe și specificații impuse cardului RFID biometric....46
6.2.2. Structura propusă pentru memoria cardului RFID biometric....46
6.2.3. Procesul de emitere a cardului RFID biometric....46
6.3. Algoritmul de verificare a identității operatorilor și a nivelului de echipare al acestora....47
6.4. Concluzii parțiale....48
Capitolul 7.Concluzii generale, contribuții, diseminarea rezultatelor și posibile direcții de continuare a cercetărilor....49
7.1. Concluzii generale....49
7.2. Contribuții originale....52
7.3. Diseminarea rezultatelor cercetării....52
7.4. Posibile direcții de continuare a cercetărilor....55
Bibliografie....57
Webografie....61

Introducere

În marea lor majoritate, sistemele automate integrează în prezent echipamente cu putere de calcul din ce în ce mai crescută și cu un înalt grad de conectivitate, care le asigură multiple posibilități de comunicare în rețele locale și chiar în Internet. Dezvoltările specifice în domeniul ingineriei sistemelor automate au vizat, printre altele, creșterea performanțelor, inclusiv a fiabilității acestora și utilizarea unor algoritmi performanți de reglare. Recent cercetările și ulterior dezvoltările industriale au fost orientate și în direcția asigurării securității sistemelor automate.

Sistemele de automatizare au devenit din ce în ce mai frecvent în ultimii ani ținta unor atacuri de natură informatică, inclusiv cu viruși dezvoltați special, așa cum reiese atât din rapoartele companiilor specializate în dezvoltarea soluțiilor de securitate, cât și din cele ale organizațiilor guvernamentale. Scopul unor astfel de acțiuni este de a perturba sau întrerupe funcționarea elementelor de infrastructură, inclusiv critică, bazate în general pe diverse categorii de sisteme automate. În acest context, unele dintre aceste atacuri informatice pot fi identificate ca amenințări teroriste sau chiar elemente ale războiului electronic, cu consecințe care de multe ori pot depăși nivelul unui stat. Din aceste motive problematica creșterii securității sistemelor de automatizare este actuală și prezintă un interes deosebit atât pentru economie, pentru organizațiile din domeniul apărării, pentru cercetare, cât și pentru comunitatea academică.

Obiectivul principal al *cercetărilor din prezenta teză de doctorat* se referă în primul rând la dezvoltarea unor metode și tehnici performante pentru creșterea securității sistemelor automate, dar și la resursele acestora care să asigure protecția împotriva amenințărilor informatice.

Cercetările desfășurare de către autor au fost orientate către trei direcții principale, corespunzătoare obiectivelor specifice ale tezei de doctorat și anume:

- dezvoltarea unor metode de analiză, evaluare și estimare a stării de securitate a sistemelor;
- dezvoltarea unei metode pentru autentificarea sursei datelor vehiculate în rețele informatice de tip industrial;
- crearea unui sistem robust pentru controlul accesului la resursele fizice și logice ale sistemelor automate, în special a celor din componența infrastructurilor industriale critice.

  Cercetările din cadrul stagiului doctoral s-au realizat prin:
  - investigații bibliografice și webografice;
  - analize ale rapoartelor generate de companii de securitate sau organizații guvernamentale (în special Centrul de Excelență NATO – CCD-COE);
  - investigații experimentale pe sisteme dezvoltate în laborator (sistemul de autentificare a sursei informației);
  - investigații experimentale în condiții reale (sistemele honeypot).

Pe parcursul cercetărilor s-a constatat necesitatea unor schimburi de bune practici și de informații privind securitatea sistemelor. În acest context autorul a inițiat în anul *2013 International Workshop on Systems Safety & Security – IWSSS*, care reprezintă un forum de discuții pentru specialiștii din domeniu și care în anul 2017 își va desfășura a cincea ediție (www.iwsss.org).

Teza de doctorat este structurată în șapte capitole, al căror conținut va fi prezentat succint în continuare.

❖ Primul capitol al tezei de doctorat este dedicat prezentării principalelor vulnerabilități, a posibilelor tipuri de atacuri și a problemelor de securitate care sunt asociate sistemelor de automatizare. În cadrul acestui capitol sunt puse în evidență cele două aspecte fundamentale specifice asigurării securității sistemelor automate și anume: controlul accesului la resurse, la care

se adaugă protecția împotriva atacurilor informatice, inclusiv a mijloacelor de susținere a acestora (viruși, wormi etc.).

❖ Al doilea capitol al tezei de doctorat tratează în detaliu problematica implementării unor mecanisme robuste și performante pentru controlul accesului la resursele fizice sau logice ale sistemelor protejate. În acest scop s-au realizat un studiu bibliografic și o prezentare a principalelor caracteristici ale sistemelor de identificare biometrică a persoanelor, bazate pe analiza amprentei digitale și a caracteristicilor irisului.

❖ Cel de-al treilea capitol se concentrează pe studiul metodelor de protecție a sistemelor automate împotriva atacurilor informatice. În acest sens au fost identificate și au fost prezentate caracteristicile a două categorii de soluții și anume soluții de tip *firewall* și respectiv, soluții de tip capcană – *honeypot*. Prin utilizarea sistemelor de tip honeypot autorul tezei de doctorat demonstrează interesul crescut al atacatorilor pentru sistemele de automatizare conectate la Internet și pentru protocoalele de comunicație de tip industrial și implicit necesitatea securizării acestora.

❖ Al patrulea capitol al tezei de doctorat este dedicat prezentării a trei metode propuse de autor pentru:

- evaluarea profilului unui anumit tip de atacator;
- estimarea probabilității de apariție a unui atac informatic, lansat de către un atacator al cărui profil este cunoscut, asupra unui sistem țintă;
- estimarea probabilității de reușită a unui atac informatic, lansat de către un atacator al cărui profil este cunoscut, asupra unui sistem țintă.

În acest context sunt introduse conceptele de *scor asociat profilului unui atacator* și de *grad de interes* pe care îl prezintă un sistem pentru un tip de atacator. De asemenea este prezentată o metodă automată de identificare a vulnerabilităților unui sistem dat, prin utilizarea unui scanner de vulnerabilități.

❖ Al cincilea capitol al tezei de doctorat este consacrat soluționării unei probleme majore de securitate cu care se confruntă majoritatea protocoalelor de comunicație industriale și anume lipsa unui mecanism destinat *autentificării sursei* datelor transmise în rețea. În acest sens este propus și validat, sub forma unui demonstrator de laborator, un mecanism pentru autentificarea senzorilor conectați în rețele bazate pe protocolul Modbus/TCP.

❖ În cel de-al șaselea capitol al tezei de doctorat se prezintă la nivel conceptual, sub forma unor specificații de funcționare și a unor algoritmi, un sistem de control al accesului în zone periculoase, bazat pe identificarea biometrică a utilizatorilor. Elementul central al sistemului propus este reprezentat de cardul RFID biometric, a cărui structură specială de memorie a fost propusă de autorul tezei de doctorat.

❖ Cel de-al șaptelea capitol al tezei de doctorat este destinat în primul rând prezentării concluziilor generale și a contribuțiilor originale. În această secțiune sunt incluse publicațiile în care au fost diseminate rezultatele cercetărilor autorului. Capitolul se încheie cu evidențierea unor posibile direcții de continuare a cercetărilor în domeniul securității sistemelor automate.

❖ Teza de doctorat se încheie cu prezentarea bibliografiei (71 titluri) și webografiei (60 titluri), cu dispunerea referințelor în ordinea citării.

Capitolul 1. Conceptualizarea securității sistemelor automate

Acest prim capitol al tezei de doctorat este consacrat încadrării conceptuale a securității sistemelor tehnice în general și a sistemelor automate în special. Se argumentează că siguranța în funcționare și securitatea sistemului sunt complementare în sensul că împreună determină îndeplinirea corectă a sarcinilor prevăzute pentru un sistem automat. Sunt identificate vulnerabilități și modalități de diminuare a acestora.

1.1. Importanța securității sistemelor tehnice

Siguranța în funcționare a sistemelor industriale constituie o problemă esențială, a cărei rezolvare revine inginerilor, producătorilor de echipamente, aparate, subansamble și, nu în ultimul rând comunității academice. Principala motivație a dezvoltării cercetărilor în acest domeniu este reprezentată de creșterea accentuată a numărului de incidente și accidente industriale, din care au rezultat victime umane și pagube materiale însemnate.

Disponibilitatea unui sistem poate fi privită ca o îmbinare a două caracteristici esențiale ale acestuia: fiabilitatea și mentenabilitatea. Această caracterizare a disponibilității ține seama doar de defectele de natură fizică sau logică ce pot apărea în sistem, dar nu evidențiază în nici un fel întreruperile în funcționare ce pot fi cauzate de diverse atacuri informatice sau de operarea necorespunzătoare a sistemului.

În mod evident un sistem cu o securitate precară suferă numeroase întreruperi din cauza atacurilor informatice, a virușilor sau a operării necorespunzătoare, determinând astfel pierderi economice masive și chiar accidente ce se pot solda cu pierderi de vieți omenești. Totodată trebuie avut în vedere faptul că securitatea trebuie asigurată fără a afecta în mod negativ performanța sistemului de automatizare și abilitatea acestuia de a-și atinge obiectivele, practic trebuie identificat un echilibru între securitate și menținerea funcțiilor sistemului protejat.

În ceea ce privește sistemele automate securitatea implică diminuarea vulnerabilității la vandalism, sabotaj, viruși informatici și atacuri informatice, implementată însă fără a afecta funcțiile și obiectivele impuse sistemului [B2], [B3].

Analizând categoriile de **infrastructuri critice** (instalații petrochimice, centrale electrice, rețele de distribuție a energiei electrice, rețele de distribuție a apei potabile, sisteme pentru gestionarea situațiilor de urgență, sisteme de apărare) se poate constata cu ușurință faptul că majoritatea **își bazează funcționarea pe sisteme automate** destinate monitorizării și controlului în timp real a instalațiilor implicate, impunându-se totodată securizarea acestora.

1.2. Vulnerabilitățile sistemelor automate

1.2.1. Caracterul integrator al sistemelor automate actuale

Sistemele de automatizare au cunoscut în ultimele decenii o largă răspândire, fiind utilizate cu precădere în domenii critice cum ar fi: generarea și distribuția energiei electrice, producția și transportul hidrocarburilor, distribuția apei potabile, producția de bunuri în procese ce folosesc materiale și substanțe toxice sau periculoase. Dacă inițial aceste sisteme de control erau independente, o dată cu dezvoltarea semnificativă a tehnologiilor de comunicații (rețele de mare viteză, transmisii de date prin rețele mobile, comunicații M2M[1]) s-a ajuns la interconectarea

[1] M2M – Machine to Machine

diverselor sisteme automate, operarea acestora de la distanță și chiar comunicarea cu sistemele economice ale întreprinderii (ERP[2], CRM[3], sisteme de planificare a producției). Dezvoltarea mijloacelor de comunicație a permis transmiterea eficientă de comenzi în timp real și raportarea continuă a diverșilor parametri către nivelurile superioare, chiar și celor cu caracter economic, dar în același timp a introdus multiple vulnerabilități, constând în principal din atacuri informatice.

Avantajele interconectării și operării de la distanță sunt de necontestat, dar ținând seama de considerațiile anterioare, chiar și un nespecialist poate intui numărul mare de probleme de securitate ridicate de sistemele automate în acest moment.

Sistemele automate pot fi caracterizate ca fiind sisteme multi-nivel, ierarhizate. Este evidentă în acest caz necesitatea dezvoltării unor metode de creștere a securității rețelelor și echipamentelor de pe fiecare nivel.

1.2.2. Analiza vulnerabilităților sistemelor automatizate ierarhizate și distribuite

Marea majoritate a sistemelor de automatizare, existente în industrie și nu numai, prezintă o structură complexă în care pot fi identificate organizări ierarhizate și distribuite.

Elementele fiecărui nivel comunică, nu doar cu cele de pe nivelurile superioare sau inferioare, ci și cu cele aflate în componența nivelului respectiv. La nivelurile superioare pot fi identificate adevărate rețele de date, infrastructuri complexe de comunicație, ce își bazează funcționarea pe protocoale standard, cum este TCP/IP. Astfel este posibilă conectarea sistemelor de automatizare la Internet. La nivelurile inferioare se operează cu protocoale specifice rețelelor industriale, cum ar fi Modbus, DeviceNet, PROFIBUS, HART, dar se constată introducerea tot mai frecventă a echipamentelor cu capabilități de interconectare prin TCP/IP.

În continuare vor fi prezentate principalele tipuri de atacuri posibile, respectiv vulnerabilitățile cel mai frecvent semnalate în literatura de specialitate pentru protocoalele specifice rețelelor industriale.

1.2.2.1. Principalele tipuri de atacuri în rețele TCP/IP

Din resursele bibliografice consultate de autor a rezultat că principalele tipuri de atacuri informatice întâlnite în rețelele care funcționează pe baza protocolului TCP/IP [B16], [B17], [B18] sunt reprezentate de:

- *Sniffing,* care constă în interceptarea, decodificarea și interpretarea traficului transmis în cadrul unei rețele. Acesta este considerat un tip de atac pasiv deoarece datele nu sunt modificate, ci sunt doar citite.
- *Denial of Service (DoS)* – Atacurile DoS sunt atacuri de tip activ și produc întreruperea serviciilor de comunicație. În principiu toate atacurile de tip DoS se produc prin transmiterea unui număr foarte mare de cereri unui sistem, ceea ce produce blocarea acestuia.
- *IP Spoofing* – Acest tip de atacuri este caracterizat de faptul că atacatorul creează pachete false folosind o adresă IP validă, din interiorul rețelei. Sistemul atacat autentifică adresa validă iar atacatorul primește răspuns.
- *Hijacking* realizează deturnarea pachetelor de pe ruta dorită, atacatorul preluând astfel controlul unuia dintre nodurile de comunicație. Este unul dintre cele mai elaborate tipuri de atacuri informatice care se pot întâlni în rețelele industriale.

[2] ERP – Enterprise Resource Planner
[3] CRM – Customer Relationship Management Software

1.3. Analiza vulnerabilităților unor protocoale de rețea industriale

Actualele echipamente de automatizare sunt caracterizate de putere de calcul și conectivitate și implicit de vulnerabilități. Aceste caracteristici conduc la posibilitatea integrării acestora în rețele specializate, cunoscute ca rețele industriale [B15].

Comunicarea între echipamente presupune existența unor protocoale specializate, care pot fi sau pot deveni vulnerabile în fața atacurilor informatice. În continuare sunt evidențiate aspecte ce privesc vulnerabilitățile protocoalelor Modbus, DeviceNet și ProfiBUS.

1.3.1. Analiza vulnerabilităților protocolului Modbus

Modbus este un protocol de nivel aplicație, corespunzător nivelului 7 din modelul ISO OSI, care permite transferul mesajelor în regim client/server între echipamente conectate pe o linie de transmisie. Protocolul implementează un mecanism de tip cerere-răspuns de nivel înalt, evitând restricțiile și problemele puse de nivelurile legătură de date și fizic. Protocolul Modbus a fost definit în anul 1979 de producătorul de automate programabile Modicon

În literatura de specialitate [B4], [B12] au fost semnalate **principalele probleme de securitate** întâlnite în cazul utilizării **protocolului Modbus,** respectiv:

- lipsa unui mecanism de autentificare a sursei mesajelor transmise;
- lipsa oricărui mecanism de criptare a datelor, toate adresele și mesajele fiind transmise sub forma de text lizibil, text care poate fi interceptat și modificat foarte ușor;
- lipsa unor mecanisme de control a integrității datelor la nivel aplicație, mai ales în cazul Modbus TCP, vulnerabilitate care permite unui atacator să introducă în mediul de comunicație mesaje care să fie validate numai la nivel transport;
- imposibilitatea blocării regimului broadcast în cazul Modbus RTU, Plus și serial. Toate echipamentele conectate pe aceeași linie de comunicație vor recepționa un mesaj broadcast, ceea ce permite desfășurarea unui atac de tip DoS[4]. Un posibil scenariu este reprezentat de transmiterea în regim broadcast a unui mesaj în care adresa expeditorului este o adresă inexistentă în rețea. Toate echipamentele care recepționează mesajul încearcă să răspundă putând astfel determina întreruperea comunicației în cadrul rețelei.

O vulnerabilitate semnificativă este reprezentată de faptul că majoritatea echipamentelor cum sunt PLC-uri sau senzori inteligenți pot fi programate prin intermediul unei interfețe de tip Modbus. Așa cum s-a arătat mai sus, prin lipsa autentificării sursei și a criptării, un atacator poate reprograma sau reconfigura echipamentul, putând produce pagube semnificative.

1.3.2. Analiza vulnerabilităților protocolului DeviceNet

Protocolul de comunicație DeviceNet a fost dezvoltat inițial de compania Allen-Bradley, iar în prezent este administrat de organizația ODVA – Open DeviceNet Vendors Application [B4],[B12].

Principala **vulnerabilitate** a protocolului DeviceNet este reprezentată de faptul că **informația se transmite în regim broadcast**. Astfel un posibil atacator ar putea introduce în rețea comenzi care să fie executate de către toate dispozitivele componente ale rețelei, cauzând o întrerupere a funcționării rețelei prin atac DoS.

[4] DoS – Denial of Service – atac informatic ce produce întreruperea funcționării unui dispozitiv sau imposibilitatea acestuia de a furniza un anumit serviciu clienților autorizați.

1.3.3. Analiza vulnerabilităților protocolului PROFIBUS

PROFIBUS (PROces FIeld BUS) este un standard de rețea industrială, cu o largă utilizare, în special în domeniul controlului proceselor din fabricile de mari dimensiuni. Standardul permite interconectarea de senzori, traductoare, elemente de execuție, echipamente inteligente, interfețe om-mașină și chiar subrețele.

Vulnerabilitățile protocolului PROFIBUS sunt caracterizate, în mod similar celorlalte protocoale prezentate în această teză de doctorat, de **lipsa unui mecanism de autentificare.** În acest context, un atacator poate crea un nod master fals, prin care să preia controlul asupra tuturor nodurilor slave.

În consecință, un nod compromis sau un nod master artificial creat pot introduce jetoane false care produc întreruperea serviciilor de comunicație oferite de protocolul PROFIBUS. **Rețelele PROFIBUS peste Ethernet (Profinet) prezintă toate vulnerabilitățile specifice protocolului TCP/IP standard** [B4], [B12].

1.4. Concluzii parțiale

Acest prim capitol al tezei de doctorat prezintă aspecte care privesc încadrarea securității sistemelor automate în practica dezvoltării și exploatării acestora.

După ce în prima secțiune este demonstrată importanța securității sistemelor tehnice, în a doua parte a capitolului sunt detaliate aspecte care privesc vulnerabilitățile sistemelor automate.

Pornind de la importanța protocoalelor de comunicație aferente rețelelor industriale de date în care sunt conectate echipamentele de automatizare, în ultima parte a capitolului 1 sunt caracterizate vulnerabilitățile unor protocoale larg răspândite în mediul industrial (Modbus, DeviceNET, PROFIBUS).

Securitatea sistemelor de automatizare vizează în primul rând aspectele clasice legate de autenticitatea, confidențialitatea, integritatea și non-repudierea datelor. Sunt de asemenea avute în vedere aspecte care privesc protecția împotriva virușilor, worm-ilor, accesului neautorizat și a oricărui tip de atac împotriva unor astfel de sisteme. O importanță aparte prezintă și controlul accesului fizic la sistemele de automatizare.

În acest capitol au fost prezentate principalele vulnerabilități ale sistemelor de automatizare, precum și recomandări pentru limitarea sau eliminarea riscurilor de securitate. Sistemele de automatizare actuale sunt din punct de vedere topologic sisteme deschise, interconectate. Ele integrează multiple rețele de echipamente (senzori, traductoare, elemente de execuție, controllere, HMI-uri, etc.), de cele mai multe ori utilizând protocoale de comunicație diferite, cum sunt PROFIBUS, DeviceNet, Modbus, HART și din ce în ce mai des chiar TCP/IP.

Analizând rapoartele de securitate puse la dispoziție de companii din domeniu sau de organizații guvernamentale, se poate constata cu ușurință faptul că principala problemă în securizarea sistemelor automate este reprezentată în acest moment de *lipsa autentificării emițătorului,* la care se adaugă și *imposibilitatea implementării unor mecanisme adecvate de criptare*, din cauza limitării resurselor de calcul și memorare a echipamentelor. În acest sens una dintre direcțiile viitoare de cercetare poate fi legată de implementarea unor mecanisme de criptare și autentificare a sursei și receptorului datelor folosind resurse reduse, cum ar fi microcontrollere, procesoare de semnal, etc. și integrarea acestora în sistemele de automatizare existente.

Pentru monitorizarea atacurilor asupra sistemelor de automatizare se impune utilizarea de soluții de tip firewall, IPS sau IDS. Acestea există pe piață și sunt destinate rețelelor bazate pe protocolul TCP/IP. Din acest motiv o direcție de cercetare identificată constă în crearea unor infrastructuri hardware și software destinate protecției rețelelor ce utilizează protocoale de tipul

Modbus, PROFIBUS sau DeviceNet. Astfel de dispozitive și infrastructuri sunt prezentate în capitolul 2 al tezei de doctorat.

Cercetările în domeniul securității trebuie să se orienteze și către combaterea virușilor ce pot afecta sistemele de automatizare, cum este cazul cunoscutului worm Stuxnet apărut în anul 2011. Analizele efectuate de companiile de securitate renumite, cum sunt Symantec, McAffee sau Kaspersky au evidențiat faptul că producătorii și integratorii de sisteme de automatizare nu sunt pregătiți să facă față unor astfel de riscuri.

O activitate de importanță deosebită constă în estimarea probabilității de apariție a atacurilor informatice asupra sistemelor automate, în special asupra celor din componența infrastructurilor critice. În capitolul 4 al acestei teze de doctorat sunt propuse două metode de analiză a atacurilor, estimarea a impactului și a riscului de apariție, prin utilizarea unor grafuri de atac – attack graphs, respectiv a unui mecanism de inferență fuzzy. Rezultatele obținute în cadrul acestei analize permit definirea nivelului de securitate ce se impune unui anumit sistem.

Investigațiile realizate au condus la ideea că una dintre cele mai importante direcții de cercetare este reprezentată de dezvoltarea unor metode și tehnici de autentificare a sursei care generează date în cadrul rețelelor industriale. În capitolul 5 al tezei se prezintă o metodă dezvoltată de autor, destinată autentificării dispozitivelor conectate într-o rețea industrială bazată pe protocolul Modbus/TCP.

Capitolul 2. Echipamente și metode destinate asigurării securității perimetrale a echipamentelor aferente sistemelor automate

Asigurarea securității sistemelor automate este abordată în teza de doctorat din perspectiva a două aspecte importante, și anume:

- implementarea unor mecanisme pentru controlul accesului la resursele fizice sau logice puse la dispoziție, tratate în capitolul 2;
- dezvoltarea și implementarea unor măsuri de asigurare a disponibilității, autenticității, integrității și confidențialității datelor transmise în rețea sau stocate pe sistemele protejate, tratate în capitolul 3.

Acest capitol al tezei de doctorat tratează în detaliu problematica implementării unor mecanisme robuste și performante pentru controlul accesului la resursele fizice sau logice ale sistemelor protejate. În acest scop s-au realizat un studiu bibliografic și o prezentare a principalelor caracteristici ale sistemelor de identificare biometrică a persoanelor, bazate pe analiza amprentei digitale și a caracteristicilor irisului. În acest context vor fi prezentate etapele unui algoritm general, bazat pe analiza amprentei digitale pentru identificarea persoanelor.

Particularitățile soluțiilor moderne destinate asigurării securității informatice, de exemplu firewall-uri și sisteme moderne destinate detecției intruziunilor sau atacurilor – honeypot, sunt prezentate în cel de-al treilea capitol al tezei de doctorat.

2.1. Securitatea perimetrală a sistemelor automate

Controlul accesului reprezintă totalitatea mecanismelor, mijloacelor și tehnicilor prin care unui utilizator i se permite sau i se revocă dreptul de a executa o operație asupra unei resurse aparținând unui sistem [W11]. Această definiție a conceptului de *control al accesului* a fost elaborată de compania Hitachi și are un grad ridicat de generalitate. În ceea ce privește sistemele de automatizare din instalațiile industriale controlul accesului vizează două aspecte și anume:

- accesul la resursele fizice ale sistemului automat, într-un anumit perimetru bine delimitat, cum ar fi de exemplu o cameră de comandă;
- accesul la resursele informatice (logice) ale sistemului, cum ar fi de exemplu o interfață om-mașină (HMI) sau o consolă de comandă.

2.2. Identificarea biometrică a persoanelor

Cercetările autorului în domeniul biometriei au început în anul 2007, în cadrul laboratoarelor Catedrei Automatică și Calculatoare din Universitatea Petrol-Gaze din Ploiești și ale companiei S.C. SEEKTRON S.R.L, Ploiești. Aceste cercetări s-au desfășurat cu predilecție în proiecte de cercetare finanțate în cadrul competițiilor naționale CEEX[5] și PN-2[6]. O parte din rezultatele prezentate mai jos fac parte din cercetările desfășurate de autor pentru realizarea proiectului de diplomă pentru specializarea Automatică și Informatică Aplicată, cu titlul "Proiectarea și realizarea unui sistem de pontaj automat bazat pe analiza amprentei digitale", conducător științific prof. dr. ing. Nicolae Paraschiv, lucrare ce a fost susținută public în sesiunea iulie 2009, în cadrul Universității Petrol-Gaze din Ploiești.

[5] CEEX – Programul național "CErcetare de EXcelență"
[6] PN-2 – Planul Național de Cercetare, Dezvoltare și Inovare II, 2007-2013

Pentru **identificarea persoanelor** s-au utilizat de-a lungul timpului mai multe metode, modelându-se, de cele mai multe ori scheme **structurate multinivel în funcție de cerințele de securitate specifice.** Elementul cheie al primului nivel este un obiect pe care utilizatorul îl posedă, cum ar fi: un act de identitate, o legitimație, o cartelă cu bandă magnetică sau cod de bare. Al doilea nivel se bazează pe informațiile deținute și memorate de persoana respectivă, cum ar fi, de exemplu, o parolă sau un număr de identificare. La cel mai înalt nivel, nivelul al treilea, identificarea utilizatorului se realizează prin ceea ce caracterizează în mod unic o persoană, adică pe caracteristici anatomice, fiziologice sau comportamentale considerate a fi unice. Între aceste caracteristici relevante sunt *amprenta digitală, imaginea facială, semnătura olografă, timbrul vocal sau dinamica utilizării unei tastaturi.* Fiecare dintre aceste metode de identificare poate fi compromisă, prin mijloace tehnice mai mult sau mai puțin complexe sau prin utilizarea unor tehnici încadrate în domeniul ingineriei sociale [B20]. O combinare de metode de pe fiecare nivel este de preferat utilizării unei singure categorii de metode, deoarece în acest mod crește securitatea sistemului. Se poate utiliza de exemplu o metodă de identificare biometrică în corespondență cu o parolă alfanumerică și cu datele de pe un card RFID [B21], [B22], B[23].

În cele ce uremază se prezintă o sinteză realizată de autor referitoare la metodele biometrice. Acestea sunt considerate cele mai eficiente mijloace de identificare a persoanelor, fiind folosite încă din cele mai vechi timpuri. ***Biometria***, termen de origine greacă (bios însemnând viață, iar metrikos măsură), desemnează totalitatea metodelor de recunoaștere a persoanelor pe baza caracteristicilor biologice ale acestora.

Conceptual în orice sistem biometric se desfășoară trei procese distincte și anume:

- înregistrarea identității într-o bază de date;
- recunoașterea caracteristicilor biometrice ale persoane în baza de date (identificarea persoanei);
- verificarea identității (autentificarea).

Pentru funcționarea unui sistem biometric este necesară înregistrarea datelor în cadrul acestuia și implementarea unor mecanisme de regăsire a informației. Din punct de vedere logic, un sistem biometric poate fi divizat în două module și anume:

- un modul de înregistrare a datelor[7];
- un modul de identificare.

Dezvoltarea fără precedent a tehnologiilor noi în electronică, a senzorilor de tip MEMS[8], a circuitelor cu grad foarte înalt de integrare, au permis apariția și utilizarea pe scară largă a unor echipamente biometrice cu performanțe din ce în ce mai mari. Dintre caracteristicile utilizate în mod frecvent pentru identificarea biometrică a persoanelor pot fi menționate:

- forma și trăsăturile feței;
- amprenta digitală;
- geometria palmei și șabloanele vasculare din aceasta;
- caracteristicile rețelei venoase a retinei;
- forma și caracteristicile irisului;
- acidul dezoxiribonucleic (ADN);
- semnătura olografă;
- dinamica tastării;
- timbrul vocal.

[7] Cunoscut în literatură sub numele de modul de *enrollment.*

[8] MEMS – Micro Electro-Mechanical Systems – Sisteme micro-electro-mecanice

Din punct de vedere al certitudinii privind identitatea unei persoane, testarea ADN este cea mai sigură metodă de identificare, însă aplicabilitatea acestuia este limitată de procesul de colectare (probe de păr, piele, sânge sau țesut uman), ușurința cu care probele pot fi contaminate și de costul mare al resurselor tehnologice implicate

Cele mai răspândite metode, algoritmi, programe și echipamente de analiză a datelor biometrice utilizate în prezent în vederea identificării și autentificării persoanelor sunt cele bazate pe scanarea irisului, analiza caracteristicilor feței sau identificarea amprentelor digitale.

În cele ce urmează vor fi prezentate la nivel conceptual etapele unui algoritm destinat analizei amprentei digitale.

2.2.1. Algoritmi destinați analizei amprentei digitale

Investigațiile autorului tezei de doctorat au condus la ideea că orice algoritm de analiză a amprentei digitale include principial următoarele etape, ilustrate în figura 2.1:

- achiziția imaginii amprentei folosind un senzor dedicat;
- procesarea imaginii obținute prin binarizare[9] și filtrare, pentru eliminarea zgomotelor și a elementelor ce afectează calitatea acesteia;
- extragerea punctelor caracteristice din imaginea amprentei;
- generarea și memorarea fișierului șablon, aferent amprentei procesate.

Fig. 2.1 - Etapele unui algoritm generic pentru analiza amprentei digitale [B22]

Senzorii biometrici furnizează sistemului de identificare a persoanelor imaginea amprentei. Dat fiind numărul mare de factori care influențează calitatea imaginilor, cum ar fi apariția de zgomot, poziționare incorectă pe senzor, claritatea slabă sau lumină slabă se impune procesarea acestora.

În urma operațiilor de procesare trebuie să rezulte o imagine clară, de calitate pentru recunoașterea elementelor caracteristice ale amprentei. În acest sens se efectuează operații de egalizare a histogramei, binarizare a imaginii, îngroșarea a unor muchii și aplicarea diverselor filtre dedicate, așa cum este arătat în referințele [B20], [B30].

În literatura de specialitate [B20], [B24], [B30] sunt evidențiate două familii de algoritmi destinați recunoașterii amprentelor și anume:

- algoritmi bazați pe *suprapunerea punctelor caracteristice*, rezultate prin compararea detaliilor specifice striațiilor;

[9] Binarizarea reprezintă operația prin care se obține o imagine cu adâncimea de culoare de 1 bit (alb/negru).

- algoritmi bazați pe *suprapunerea unor tipare*, care vizează compararea unor trăsături de ansamblu ale amprentei (lățimea striațiilor, curbura, densitatea, etc.).

Caracteristicile acestor algoritmi sunt prezentate detaliat în cadrul celui de-al doilea capitol al tezei de doctorat.

2.2.2. Algoritmi destinați comparării șabloanelor amprentelor digitale

Algoritmii de comparare au rolul de a stabili gradul de similitudine între două șabloane (template-uri) corespunzătoare la două amprente. De cele mai multe ori, în sistemele de control al accesului bazate pe analiza caracteristicilor biometrice, datele de intrare ale algoritmului sunt reprezentate de un șablon generat în timp real, pe baza amprentei scanate de senzorul biometric, împreună cu un șablon obținut prin interogarea bazei de date. Pentru a permite accesul se stabilește o valoare de prag. Dacă în urma comparației se depășește această, cele două șabloane corespund, iar utilizatorului i se permite accesul. Dacă scorul comparației este situat sub valoarea de prag, utilizatorul nu este recunoscut, deci nu îi este permis accesul.

2.2.3. Tehnologii biometrice de identificare a persoanelor pe baza analizei imaginii irisului

Ideea de a folosi analiza irisului pentru securizarea anumitor obiective de interes major a căpătat contur în ultima perioadă de timp, respectiv după anul 2011. Individualitatea irisului a fost dovedită prin metode riguroase matematice și prin numeroase calcule statistice. La preluarea a numai 75% din detaliile irisului, probabilitatea repetabilității a fost estimată a fiind $1/10^{78}$. Chiar și cei doi ochi ai unei persoane au modele diferite și complet independente ale irisului [B36]. Principalele avantaje se referă la rate de reușită mari, scanare rapidă, securitate sporită, datorită faptului că irisul nu își modifică structura pe parcursul vieții, iar existența a două persoane cu o structură identică a irisului este imposibilă. Pe lângă aceste avantaje certe, utilizarea tehnicilor biometrice bazate pe analiza irisului prezintă și un dezavantaj major care constă în dificultatea capturii imaginilor de calitate ale acestuia, din cauza dimensiunilor mici și a posibilelor obturări cauzate de gene și pleoape.

Metodele de analiză a irisului sunt foarte complexe deoarece trebuie să fie capabile să extragă și să codifice aspectul texturii acestuia, textură cu grad mare de variație. În literatura de specialitate aceste metode au fost clasificate în două categorii și anume:

- **Metode bazate pe aspect,** care folosesc abordări statistice clasice, cum sunt Principal Component Analysis – PCA sau Independent Component Analysis – ICA, pentru reprezentarea imaginii irisului [B37]
- **Metodele bazate pe textură**, care folosesc filtre pentru procesarea imaginii, extrăgând apoi unele caracteristici ale imaginii filtrate pentru a le cuantifica în imaginea irisului, descrise în referințele [B36] și [B38].

2.3. Utilizarea tehnologiei RFID pentru dezvoltarea unui sistem robust de identificare a persoanelor

Alături de metodele biometrice de identificare a persoanelor, considerate metode avansate, se pot utiliza și așa numitele metode convenționale, cum ar fi smartcard-urile sau cardurile RFID. O combinare a celor două metode, o caracteristică biometrică, aparținând în mod irevocabil utilizatorului și un card, pe care individul îl posedă, reprezintă un sistem robust, multi-nivel de identificare și autentificare a persoanelor.

IDentificarea prin **R**adio **F**recvență **– RFID (Radio Frequency Identification)** se constituie într-o tehnologie modernă destinată colectării automate a datelor, fiind încadrată, de către literatura

de specialitate [B39], în categoria tehnologiilor AIDC (*Automatic Identification and Data Collection*). Practic RFID este un sistem de identificare automată a obiectelor asemănător tehnologiei cu cod de bare, dar care acționează fără contact direct, permițând detecția și identificarea elementelor din proximitatea unui cititor.

Sistemele RFID sunt alcătuite, în general, din trei componente după cum urmează:

- *cititor – RFID reader*, care integrează un bloc emițător-receptor radio pe o frecvență dedicată (de obicei 13,56 MHz, 125 kHz sau 900 MHz), un microcontroller și circuite de memorie RAM și ROM, pentru prelucrarea și stocarea datelor. Pentru a putea funcționa cititorul este conectat la o antenă, care poate fi integrată pe circuitul imprimat (PCB) sau externă;
- *transponder de radiofrecvență* – denumit prescurtat tag sau etichetă RFID;
- *sistem de procesare a datelor,* denumit și *middleware,* ce poate fi reprezentat de un PC, de microcontrollere sau de alte echipamente electronice capabile să prelucreze datele obținute prin citirea tag-urilor.

Cantitatea de memorie disponibilă variază în funcție de tipul de tag de la câțiva octeți până la dimensiuni de ordinul kilo-octeților.

Tag-urile RFID pot fi utilizate pentru identificarea persoanelor care accesează zone controlate din infrastructurile critice, de exemplu camere de comandă. Totodată un cititor de carduri RFID ar putea fi integrat cu diversele console de operare pentru a autentifica operatorii în mod automat. Totuși sistemul RFID prezintă riscuri majore de securitate, pierderea cardurilor fiind foarte frecventă, iar copierea informațiilor de pe acestea și crearea unei clone fiind operații nu foarte complexe.

În cadrul brevetului de invenție Nr. RO 123364 B1, cu titlul *„Card RFID biometric și metodă de stocare a informațiilor pe cardul RFID biometric*", autori ing. Melinte Toader, ing. Pricop Emil, ing. Lorentz Adrian și dr. ing. Andron Liviu, este prezentată o metodă de identificare a persoanelor ce realizează tranzacții bancare folosind un card RFID MIFARE cu memoria de 1 KB, având o structură specială.

În brevetul [B23] este definit conceptul de card RFID biometric și structura memoriei acestuia, fiind pus în evidență faptul că acel card poate stoca șabloanele a până la trei amprente digitale ale aceluiași utilizator, creând astfel o legătură biunivocă, verificabilă în mod automat între identitatea utilizatorului, șablonul amprentei digitale și cardul folosit ca element suplimentar de identificare într-un sistem biometric.

Elementul de noutate adus de acest tip de sistem constă în faptul că datele necesare identificării utilizatorului nu sunt stocate în memoria unui dispozitiv sau într-o bază de date aflată pe un server, ci pe un card aflat la utilizator, card ce poate fi citit fără contact direct. Astfel se pot construi echipamente performante destinate controlului accesului pentru un număr virtual nelimitat de utilizatori. Totodată sunt eliminate și problemele de securitate ridicate de transferul datelor biometrice prin rețea în cazul stocării acestora într-o bază de date aflată pe un server într-un datacenter.

2.4. Concluzii parțiale

În cadrul prezentului capitol al tezei de doctorat au fost analizate aspectele fundamentale referitoare la mecanismele destinate controlului accesului la resursele sistemului protejat.

Așa cum este arătat în prima secțiune a capitolului pentru a implementa un mecanism robust de control al accesului la resursele fizice sau logice ale unui sistem este necesară identificarea utilizatorului și autentificarea acestuia. Procesul de autentificare a unei persoane este un proces

complex, care poate fi realizat prin intermediul mai multor metode, cea mai utilizată fiind folosirea unei parole. O altă metodă de autentificare se bazează pe datele stocate de un obiect fizic (card / memorie USB) pe care utilizatorul îl deține. Atât parolele cât și obiectele fizice sunt ușor de compromis, existând posibilitatea ca utilizatorul să le uite sau să îi fie furate. Cele mai robuste metode de autentificare, menționate în lucrările de specialitate, sunt metodele biometrice, bazate pe o caracteristică fizică sau comportamentală a persoanei.

În următoarea secțiune a capitolului 2 a fost realizat un studiu bibliografic și o prezentare a principalelor caracteristici ale sistemelor de identificare biometrice a persoanelor, bazate pe analiza amprentei digitale. Deoarece fiecare producător de senzori sau echipamente biometrice folosește algoritmi proprietari, care nu sunt disponibili publicului, în parte au fost detaliați pașii unui algoritm general pentru analiza amprentei digitale și anume: achiziția imaginii, prelucrările primare ale acesteia, marcarea punctelor caracteristice și generarea șablonului biometric.

Tehnologia bazată pe analiza amprentei digitale a ajuns la maturitate, motiv pentru care aceasta poate fi utilizată cu succes pentru implementarea unor sisteme de autentificare a persoanelor care accesează elemente de comandă sau zone protejate care fac parte din sistemele automate, componente ale infrastructurilor critice.

O altă tehnologie biometrică destinată identificării precise a persoanelor este cea bazată pe analiza imaginii irisului. Performanțele acestei metode sunt foarte mari, dar costurile echipamentelor, necesitatea unei anumite poziții pentru citirea (scanarea) imaginii, acceptarea mai redusă de către utilizatori, nu recomandă utilizarea acestei tehnologii în sisteme care nu necesită cel mai înalt grad de securitate.

În ultima secțiune a acestui capitol al tezei de doctorat este introdus un concept brevetat de echipa de cercetători din care autorul tezei face parte, și anume *cardul RFID biometric.* Acest tip de card, destinat identificării utilizatorului prin radiofrecvență, stochează în memoria proprie șabloanele amprentei digitale a utilizatorului, permițând crearea unui sistem de autentificare/identificare cu două niveluri – card și amprentă digitală, fără a fi necesară stocarea amprentei digitale a utilizatorului într-o bază de date centralizată sau transmiterea acesteia prin Internet. Brevetul dezvoltat se referă la structura memoriei cardului RFID biometric și la utilizarea acestuia pentru creșterea securității tranzacțiilor bancare.

Rezultatele investigațiilor din prezentul capitol au permis autorului să propună, în cel de-al șaselea capitol al tezei, dezvoltarea unui sistem complex destinat identificării persoanelor care accesează zone periculoase din instalațiile industriale, bazat pe identificarea biometrică a acestora și pe utilizarea unui card RIFD a cărui structură de memorie reprezintă o extindere a conceptului introdus în brevetul de invenție menționat.

Capitolul 3. Echipamente și metode destinate asigurării securității informatice a sistemelor automate

Spre deosebire de sistemele din domeniul tehnologiei informației în cazul cărora securitatea informatică se concentrează pe confidențialitate și limitarea accesului neautorizat la date, în cazul sistemelor tehnice securitatea echivalează cu menținerea disponibilității datelor și a stării de funcționare a sistemului. Din acest motiv nu se pot folosi întotdeauna soluțiile de securitate clasice pentru asigurarea protecției infrastructurii sistemelor tehnice.

În continuare vor fi prezentate câteva considerații generale privind asigurarea securității informatice a sistemelor tehnice. Principalele mijloace de asigurare a securității, dispozitivele de tip firewall, sunt prezentate în secțiunea 3.2. a acestui capitol. În cea de-a treia parte a capitolului sunt descrise sisteme de tip honeypot, iar în ultima parte sunt prezentate rezultate experimentale obținute prin instalarea și utilizarea unor honeypot-uri specifice pentru aplicațiile de tip industrial.

3.1. Securitatea informatică a sistemelor de conducere a proceselor

În opinia autorului tezei siguranța în funcționare a sistemului automat poate fi afectată de incidente informatice, inclusiv atacuri sau viruși. Problematica asigurării securității sistemelor automate vizează în acest context atât siguranța procesului cât și securitatea infrastructurii de automatizare existente, care poate prezenta anumite vulnerabilități.

După cum s-a arătat, în prezent infrastructurile de automatizare sunt constituite în exclusivitate din echipamente digitale, cu putere de calcul și disponibilități crescute pentru conectarea în rețele specifice. Pornind de la premisa că funcționalitatea acestor sisteme este condiționată de „veridicitatea" datelor transferate se impun măsuri de securitate în legătură cu datele, și în același timp legate de personalul implicat în operarea acestor sisteme.

În ultimii ani sistemele automate sunt vizate din ce în ce mai frecvent de atacuri informatice care urmăresc întreruperea funcționării sau funcționarea defectuoasă a acestora. În rapoartele companiilor de securitate [B40], [B41], [B42] sunt semnalate numeroase atacuri de tip DoS[10] și DDoS[11] care au ca ținte sisteme de automatizare, inclusiv sisteme SCADA, cu precădere din infrastructurile critice (centrale electrice, rafinării, infrastructuri petrochimice, sisteme de transport etc.).

Ținând seama de considerațiile anterioare, se poate afirma că asigurarea securității sistemelor tehnice are ca scop maximizarea disponibilității acestora în contextul apariției unor atacuri informatice sau a infectării cu viruși și/sau viermi (worm) informatici.

Disponibilitatea sistemelor automate poate fi afectată de următorii factori ce vizează securitatea informatică a acestora:

- obținerea accesului (logic) neautorizat la sistem și oprirea acestuia;
- injectarea de date false în rețea și producerea blocării sistemului prin imposibilitatea prelucrării acestor date;
- atacuri informatice de tip DoS și/sau DDoS.

[10] DoS – Denial of Service – Tip de atac ce urmărește indisponibilizarea unei resurse prin suprasolicitarea acesteia.

[11] DDoS – Distributed DoS – Tip de atac ce utilizează mai multe calculatoare, de obicei infectate cu un virus sau worm informatic, pentru a suprasolicita o resursă țintă, producând indisponibilizarea acesteia.

Toate tipurile de atacuri menționate anterior se pot realiza fără a avea acces fizic la sistemul țintă, prin conectarea la rețeaua protejată și desfășurarea unor acțiuni de natură subversivă.

În rapoartele unor companii de securitate [B42], dar și în ghidurile de bune practici elaborate de centre de cercetare în domeniu [B41], [W2] printre metodele de eliminare sau limitare a atacurilor de tip DDoS sunt menționate următoarele:

- instalarea unor versiuni stabile de software/firmware și actualizarea permanentă a acestora pentru eliminarea în timp util a tuturor problemelor de securitate cunoscute;
- instalarea unor sisteme firewall care să limiteze numărul de conexiuni simultane din partea unui singur client sau a unei clase de clienți;
- asigurarea redundanței hardware și software și a alocării dinamice a resurselor pentru sistemele critice, astfel încât atunci când un sistem este atacat, sistemele de rezervă să intre în acțiune;
- izolarea sistemelor a căror întrerupere în funcționare poate avea impact major asupra vieții oamenilor, mediului și infrastructurii.

Analizând metodele menționate anterior se poate observa că un rol foarte important în protecția sistemelor industriale îl pot avea dispozitivele de tip firewall, care sunt prezentate pe larg în subcapitolul 3.2.

3.2. Sisteme de tip firewall

Firewall-ul este o resursă hardware sau software, care implementează un mecanism de control al accesului la resursele unui sistem de calcul sau ale unei întregi rețele de calculatoare [B43]. Într-o abordare simplificată se poate considera că un firewall au rolul de a realiza în mod automat filtrarea traficului de rețea pe baza unor reguli bine definite, pentru a împiedica accesul neautorizat la anumite resurse sau pentru a bloca utilizarea unor aplicații potențial periculoase.

3.2.1. Clasificarea sistemelor firewall

În referința [B44] firewall-urile sunt fost clasificate în patru categorii, succint descrise în continuare.

- *Firewall-uri dedicate*;
- *Firewall-urile integrate în routere;*
- *Firewall-uri integrate în servere*;
- *Firewall-uri personale.*

După modul de definire al regulilor pe baza cărora funcționează firewall-urile pot fi clasificate în următoarele două categorii:

- *Firewall-uri permisive*, în cadrul cărora se definesc explicit reguli de blocare a traficului de rețea.
- *Firewall-uri restrictive,* în cazul cărora se definesc explicit reguli pentru caracterizarea traficului de rețea permis, iar toate pachetele de date care nu se înscriu în regulile definite sunt blocate de către sistemul firewall.

3.2.2. Utilizarea sistemelor firewall în cadrul asigurării securității sistemelor automate

Rețeaua de tip corporație (denumită și *Enterprise Network*) concentrează cu precădere traficul de date economice, care se transferă între diverse compartimente (servicii funcționale), cum ar fi contabilitate, financiar, marketing, resurse umane. Pe lângă acestea mai există și un trafic așa zis „clasic” care include serviciul de e-mail, navigare pe Internet, mesagerie instantanee etc. În această rețea calculatoarele sunt mai vulnerabile în fața atacurilor informatice, utilizatorii fiind de

cele mai multe ori mai neglijenți în ceea ce privește respectarea unei politici de securitate [W18]. În cadrul rețelei aferente sistemului informatic economic, politicile de control al accesului nu sunt foarte dure, iar utilizatorii pot accesa pagini Web și pot instala diverse programe, existând astfel pericolul infectării cu viruși sau viermi (worms) informatici.

O rețea de tip industrial (denumită și *Control Network*) concentrează toate echipamentele care comunică prin intermediul unor protocoale industriale, cum este cazul echipamentelor de automatizare (inclusiv sistemele SCADA), servere de jurnalizare, stații de inginerie sau stații pentru interfețe om-mașină. În cadrul acestei rețele politicile de control al accesului trebuie să fie foarte dure, astfel încât probabilitatea instalării și rulării unor programe neautorizate să fie extrem de mică.

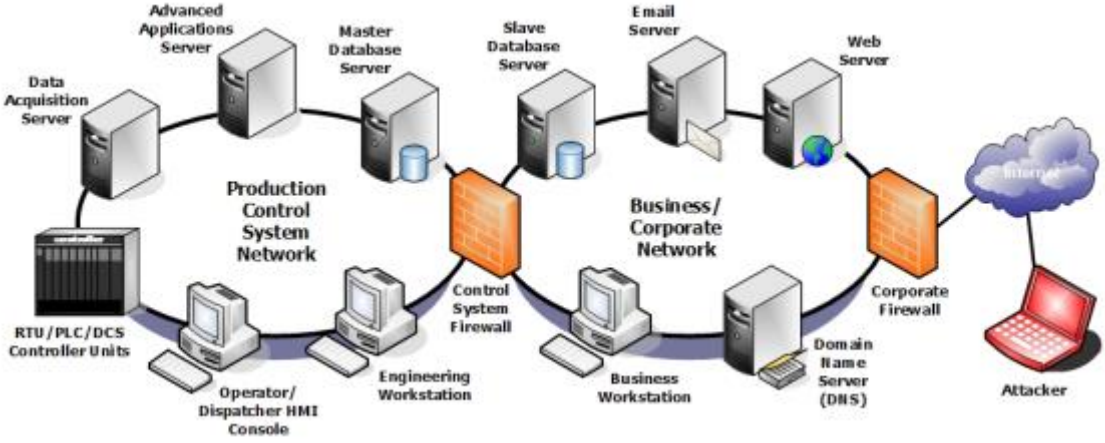

Fig. 3.1 Diagrama de rețea a unei corporații care integrează o rețea de tip corporate și o rețea industrială, conform recomandărilor ICS-CERT [W18]

Ținând seama de considerentele de mai sus, este evidentă necesitatea separării logice a celor două rețele, respectiv rețea aferentă *sistemului informatic economic* și cea specifică *sistemului informatic tehnic*. Această separare nu se poate realiza prin simpla lor deconectare, fiind necesară existența unui mecanism foarte puternic de control al traficului dintre cele două rețele. Așa cum este specificat și în recomandările ICS-CERT[12] [W18] pentru securitatea infrastructurilor industriale, acest mecanism de control al traficului include un firewall hardware, bazat pe un set de reguli identic cu cel descris pentru *Iptables* în capitolul 3 al tezei de doctorat.

În figura 3.1 sunt evidențiate cele două tipuri de rețele împreună cu cele două dispozitive firewall, dintre care unul este destinat separării între rețeaua industrială și rețeaua clasică a corporației *(Control System Firewall)* și unul care are rolul de a proteja rețeaua clasică *(Corporate Firewall)*, direct conectată la Internet de atacurile provenind din acest mediu relativ nesigur. Practic un atacator care are ca țintă o componentă a sistemului industrial ar trebui să penetreze două sisteme firewall.

Conceptul de DMZ (Zonă DeMilitarizată) a fost introdus în domeniul rețelelor de calculatoare pentru a desemna o subdiviziune logică sau fizică a rețelei care separă rețeaua internă, protejată, de accesul neautorizat din alte rețele nesigure sau din Internet. În zona DMZ sunt plasate de obicei serverele care trebuie să permită acces public, de exemplu serverele Web sau serverele de e-mail. Folosind o astfel de zonă demilitarizată rețeaua locală este izolată practic de serverele cu acces public, fiind astfel inaccesibilă atacatorilor și conducând la creșterea securității tuturor echipamentelor situate în spatele firewall-urilor.

[12] ICS-CERT - Industrial Control Systems - Cyber Emergency Response Team, organizație guvernamentală din SUA cu preocupări și responsabilități în domeniul prevenirii și limitării incidentelor informatice din infrastructurile industriale

3.3. Sisteme de tip honeypot și honeynet

Dezvoltarea recentă a tehnicilor de virtualizare și creșterea puterii de calcul a sistemelor embedded a permis introducerea unui concept asemănător armatei de teracotă din China antică, și anume *„ceața informatică”*.

Conceptul de *ceață informatică* sau *cyberfog* implică existența unor ținte „false”, care să inducă atacatorul în eroare. Prin crearea unui număr suficient de mare de astfel de ținte probabilitatea ca un atacator să reușească să inițieze un atac asupra unui obiectiv protejat poate fi semnificativ redusă. Pentru crearea unui astfel de nor de ceață informatică se pot folosi honeypot[13]-uri sau honeynet-uri (rețele de honey-poturi).

3.3.1. Considerații generale privind dispozitivele de tip honeypot

Conform referințelor [B47], [B48] și [B49] un *honeypot* reprezintă o resursă informatică, utilizată pentru evaluarea securității, putând fi testată, atacată sau compromisă, fără a produce pagube. Practic un honeypot este un mecanism de tip capcană, ce poate fi utilizat în scopuri de cercetare, pentru testarea protocoalelor de comunicație care sunt în mod frecvent ținte ale atacurilor informatice și pentru evaluarea modului de inițiere și desfășurare a unui atac, sau pot reprezenta ținte false pentru un atacator.

Conform referinței [B50] un honeypot reprezintă un sistem configurat să fie expus în Internet pentru potențialii atacatori, să-i atragă prin distribuția de informații pretins valoroase, secrete, și să fie dificil de accesat, dar nu imposibil. În momentul accesării sistemului acesta trebuie să monitorizeze și să înregistreze fiecare acțiune a atacatorului în cadrul unor fișiere jurnal (log) protejate. Compromiterea sistemului nu trebuie să producă nici un fel de pagube.

O altă funcție a dispozitivelor honeypot constă în posibilitatea de a obține informații privind noi vulnerabilități sau noi modalități de exploatare a vulnerabilităților existente.

Din punct de vedere fizic, un honeypot poate fi implementat pe un server fizic sau folosind una sau mai multe mașini virtuale.

3.3.2. Clasificarea dispozitivelor de tip honeypot

Cea mai utilizată clasificare a dispozitivelor de tip honeypot semnalată în literatura de specialitate [B47], [B48], [B50] este cea bazată pe conceptul de nivel de interacțiune, care poate fi definit ca fiind gradul de interactivitate al sistemului cu utilizatorul, respectiv măsura în care un atacator poate rula comenzi pe sistem și primi o reacție (feedback) de la acesta [B47].

Din punct de vedere al nivelului de interacțiune honeypot-urile pot fi clasificate în două categorii și anume:

Honeypot-urile cu grad redus de interacțiune (Low Interaction Honeypots – LIH) sunt în momentul de față cele mai răspândite, datorită complexității lor mai reduse și necesarului mai mic de resurse. Astfel de sisteme emulează anumite servicii care sunt tentante pentru atacatori. Activitățile care pot fi desfășurate de atacator sunt limitate, de cele mai multe ori LIH fiind configurate astfel încât după tentativa de conectare a atacatorului să îi blocheze acestuia conexiunea, eliminând astfel riscul penetrării sistemului și utilizării acestuia de către atacator pentru a lansa alte atacuri.

Honeypot-urile cu grad înalt de interacțiune (High Interaction Honeypots – HIH) sunt foarte complexe. Astfel de sisteme nu simulează doar existența unui anumit serviciu de rețea, ci replică întreaga funcționare a acestui serviciu. Practic atunci când un atacator accesează un HIH, el

[13] Denumirea honeypot se poate traduce pe baza etimologiei din limba engleză – honey = miere, iar pot = borcan, recipient, sugerând un dispozitiv capcană.

poate utiliza serviciile simulate și poate lansa comenzi, fără să realizeze că utilizează de fapt un sistem capcană.

3.4. Rezultate experimentale obținute cu ajutorul dispozitivelor honeypot

În cadrul prezentei teze de doctorat se urmărește problematica securității sistemelor automate din infrastructurile industriale. În acest context o direcție a cercetărilor întreprinse de autor în prezenta teză de doctorat a fost reprezentată de investigațiile privind cantitatea și calitatea informațiilor despre atacuri obținute cu ajutorul dispozitivelor de tip honeypot. În acest scop a fost instalat și testat sistemul complex T-Pot.

3.4.1. Prezentarea sistemului T-Pot

T-Pot este un sistem complex, open-source, dezvoltat de către echipa Deutsche Telekom AG (DTAG) Honeypot Project și pus la dispoziția utilizatorilor în mod gratuit, fără suport tehnic.

În cazul sistemului T-Pot, tehnologia Docker permite rularea simultană a mai multor honeypot-uri, independent unul de celălalt, dar partajând resursele unei singure mașini fizice: procesor, memorie RAM și o singură interfață de rețea [W19].

În cadrul containerelor Docker sunt rulate mai multe categorii de aplicații și anume:

- honeypot-uri: *ConPot, Dionaea, Cowrie, Glastopf* și *ElasticPot;*
- aplicația *Suricata,* un monitor în timp real al activității de rețea;
- tripletul *ELK (ElasticSearch – Logstash – Kibana),* destinat prelucrării și indexării datelor obținute de honeypot-uri și generării de rapoarte sub formă grafică sau text.

Dintre multitudinea de honeypot-uri disponibile în cadrul sistemului T-Pot, pentru cercetările din această teză de doctorat prezintă interes, cele orientate către servicii de rețea specifice sistemelor industriale, așa cum este cazul *ConPot, Dionaea* și *Cowrie,* care vor fi descrise pe scurt în continuare.

ConPot [W25] este un honeypot open-source, dezvoltat de grupul Honeynet Project [W26], destinat emulării serviciilor specifice sistemelor industriale de automatizare. Este un honeypot cu grad redus de interacțiune (LIH), care oferă posibilitatea de a emula diverse protocoale industriale printre care Modbus/TCP, destinat comunicației între aparatura de câmp și PLC-uri și S7Comm, protocol dezvoltat de compania Siemens pentru comunicația între PLC-uri din familia Siemens Step7. *ConPot* poate crea și o interfață om-mașină simplă ce poate fi livrată sub forma unei pagini Web prin protocolul HTTP, pe portul 80 TCP.

Dionaea [W27] este unul dintre cele mai utilizate sisteme de tip honeypot în momentul efectuării cercetărilor aferente prezentei teze de doctorat. A fost dezvoltat pe baza proiectului *Nepenthes* în cadrul proiectului Honeynet Project din ediția 2009 a Google Summer of Code. *Dionaea* urmărește nu doar crearea unei capcane simple pentru atacatori, ci și dezvoltarea unui mecanism de captură (înregistrare) a aplicațiilor malițioase (malware) folosite pentru exploatarea vulnerabilităților simulate, putând simula un număr mare de protocoale de comunicație dintre care se pot menționa HTTP, HTTPS, FTP, TFTP, SMB și MSSQL.

Cowrie [W28] este un honeypot cu grad înalt de interacțiune (HIH) dezvoltat de către Michel Oosterhof. Scopul honeypot-ului este de a simula un server SSH[14], de a jurnaliza încercările de conectare și ghicire a parolei, iar pentru încercările de conectare reușite de a înregistra toate acțiunile

[14] SSH – Secure SHell – protocol de comunicație de nivel aplicație destinat operării de la distanță a unui calculator care rulează sisteme de operare din familiile UNIX sau Linux. Protocol permite transmiterea de comenzi text și vizualizarea răspunsurilor la acestea, practic oferind acces de la distanță la consola (shell-ul) sistemului de operare.

atacatorului pe server. Protocolul SSH, chiar dacă nu este un protocol specific mediului industrial, este folosit în mod frecvent în cadrul sistemelor embedded (senzori wireless, concentratoare de date), care rulează un kernel Linux și pot fi configurate de la distanță. Din acest motiv datele furnizate de honeypot-ul Cowrie sunt valoroase pentru analiza atacurilor în mediul industrial.

3.4.2. Rezultate experimentale obținute

Sistemul T-Pot a fost utilizat în cadrul mai multor sesiuni de lucru pentru a colecta date referitoare la tentativele de conectare și de atacuri informatice ce aveau ca țintă honeypot-uri rulate de acesta.

3.4.2.1. Date colectate folosind honeypot-ul ConPot

În perioada 03.06.2016 - 06.06.2016 sistemul T-Pot a fost configurat să ruleze doar containerul care conține honeypot-ul *ConPot,* specific pentru emularea sistemelor industriale. Pentru realizarea experimentului s-a utilizat configurația implicită a *ConPot*, emulând în special servicii specifice sistemelor industriale, cum sunt comunicația prin protocoalele Modbus TCP, S7Comm (specific PLC-urilor produse de compania Siemens) și HTTP.

Întrucât *ConPot* este un honeypot cu grad redus de interacțiune, informațiile utile obținute sunt protocolul pe care s-a încercat conectarea de către atacator și adresa IP folosită de acesta. Folosind adresa IP și baza de date publică GeoIP [W30], care permite asocierea geografică între adresa IP și orașul sau țara în care a fost alocată, s-a putut localiza cu precizie țara din care provine adresa IP folosită pentru conectare.

3.4.2.2. Interpretarea rezultatelor obținute folosind honeypot-ul ConPot

Rezultatele sintetice ale experimentului realizat sunt prezentate în tabelul 3.1.

Tabel 3.1 - Rezultatele sintetice obținute cu honeypot-ul ConPot în perioada 03 -06.06.2016

Protocol / Țară	BG	CA	FR	IN	JP	PL	RU	ES	US	CN	TR	NL	Total / prot.
http	1	2	2	1	1	2	2	1	4	1	1	1	19
ipmi	0	0	0	0	0	0	0	0	3	0	0	0	3
modbus	0	1	0	0	0	2	0	0	2	1	0	0	6
snmp	0	0	1	0	0	0	0	0	7	0	0	0	8
S7Comm	0	0	0	0	0	0	0	0	1	1	0	0	2
Total / țară	1	3	3	1	1	4	2	1	17	3	1	1	38

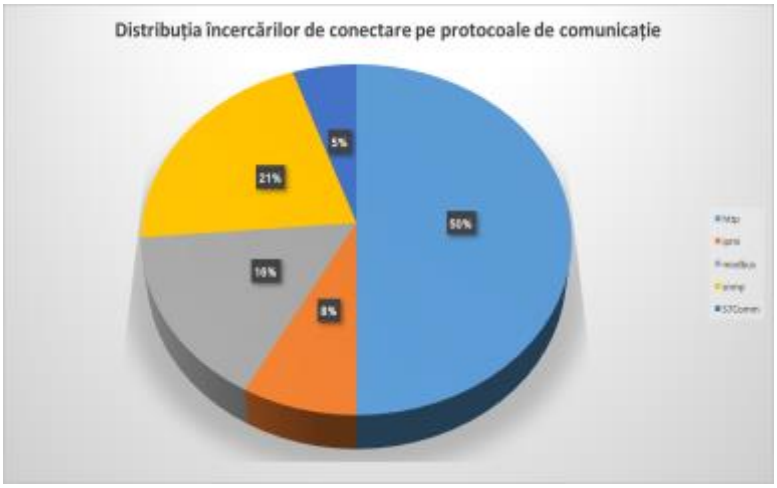

Fig. 3.2 - Distribuția încercărilor de conectare pe protocoale de comunicație în cazul experimentului realizat folosind honeypot-ul ConPot.

Analizând datele din tabelul 3.1 și graficul din figura 3.2 se poate observa că protocolul Modbus a fost ținta a 16% din încercările de conectare, ilustrând un interes crescut pentru infrastructurile industriale. Protocolul specific pentru comunicația între PLC-urile produse de compania Siemens totalizează 5% din numărul total de evenimente. Se poate constată că 21% din încercările de conectare sunt direcționate către protocoale industriale. Practic 1 din 5 atacuri a vizat o infrastructură industrială, ceea ce reprezintă o cifră îngrijorătoare, întrucât protocoale vizate, Modbus și S7Comm, au un grad ridicat de specificitate, iar încercările de conectare sunt în mod evident deliberate.

Distribuția încercărilor de conectare pe țări în care a fost alocată adresa IP sursă este prezentată în figura 3.3.

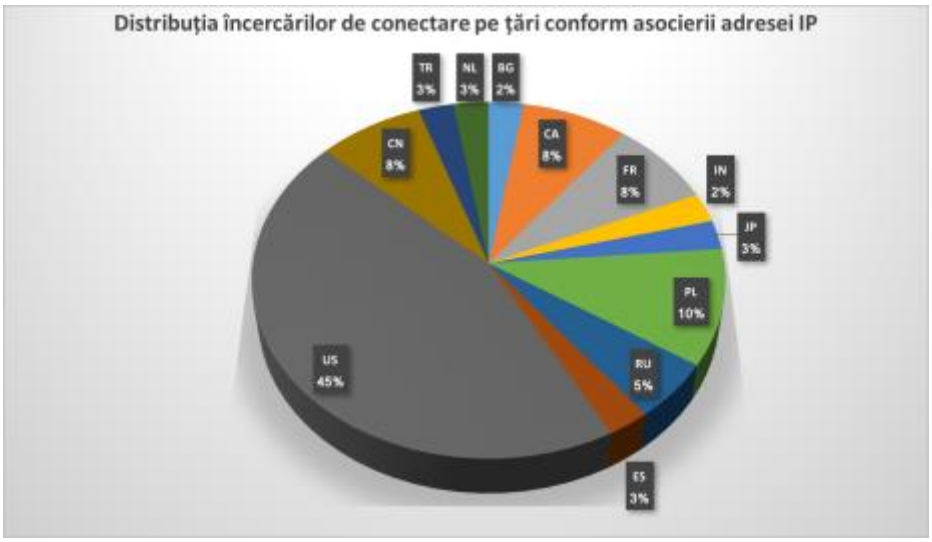

Fig. 3.3-Distribuția încercărilor de conectare pe țări conform asocierii adresei IP sursă în baza de date publică GeoIP. Codurile țărilor sunt cele menționate în tabelul 3.1

3.4.2.3. Date colectate folosind ansamblul de honeypot-uri disponibile în cadrul sistemului T-Pot

În decursul lunilor octombrie-noiembrie 2016 sistemul T-Pot a fost instalat și a rulat pe un server virtual privat (VPS) închiriat de la compania VULTR [W31]. Sistemul a fost configurat astfel încât să ruleze toate honeypot-urile disponibile, dar și panoul de administrare. Datorită faptului că T-Pot integrează tripletul ELK, care permite analiza automată a log-urilor, vor fi prezentate în continuare prin capturi de ecran rezultate reprezentative ale rulării acestui sistem.

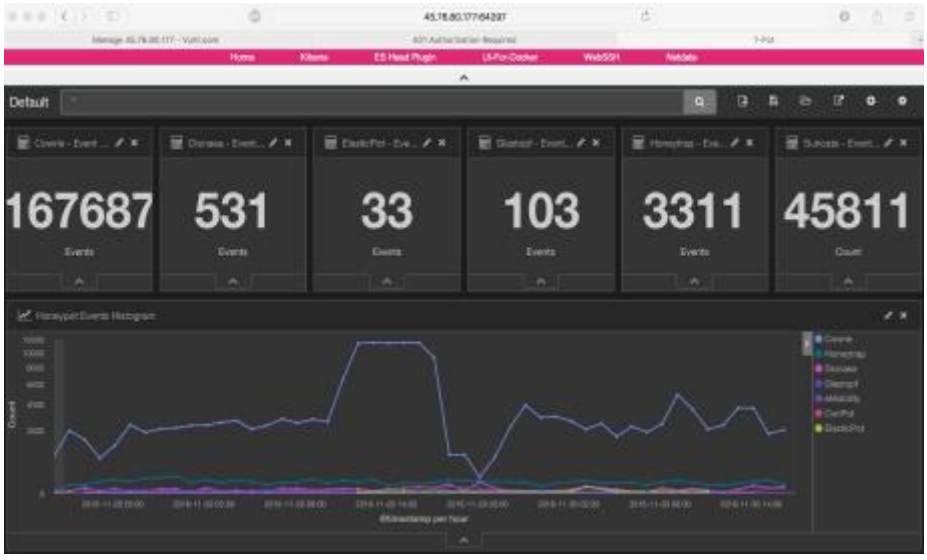

Fig. 3.4 -Ecranul principal al panoului de control pentru raportare Kibana, integrat în sistemul T-Pot

În cadrul paginii principale a panoului de raportare Kibana este listat numărul de evenimente pentru fiecare honeypot în parte. Informația este prezentată atât sub formă de text cât și sub forma unei histograme, așa cum este ilustrat în figura 3.4.

Fig. 3.5 -Informații detaliate privind evenimentele înregistrate în sistemul T-Pot

Informațiile detaliate referitoare la atacurile înregistrate sunt prezentate cu predilecție sub formă grafică, așa cum este ilustrat în figura 3.5. În graficul din partea superioară a figurii este realizată o histogramă a porturilor TCP și respectiv UDP vizate de atacatori.

3.4.2.4. Analiza rezultatelor obținute folosind sistemul T-Pot

Analizând histograma din figura 3.5 se poate constata faptul că domină încercările de conectare pe portul 80, specific protocolului HTTP, urmate de cele pe portul 443, specific pentru protocolul HTTPS. Situația este similară celei prezentate în secțiunea anterioară a acestui capitol, în cazul honeypot-ului ConPot.

În diagrama circulară din partea stângă sunt listate cele mai utilizate 10 sisteme de operare utilizate de computerele sursă ale evenimentelor. Se observă cu ușurință faptul că primele 5 poziții din clasament sunt ocupate de distribuții de Linux, cu diferite variante de kernel. Pozițiile 8 și 9 sunt ocupate de calculatoare care rulează sistemul de operare Microsoft Windows.

În diagrama din partea dreaptă a figurii 3.5 este prezentat un clasament al primelor 10 țări din care provin adresele IP care au produs evenimente în cadrul sistemului T-Pot.

Fig. 3.6 Harta (HeatMap) sursei evenimentelor înregistrate în cadrul sistemului T-Pot

Informațiile privind sursele atacurilor sunt reprezentate în cadrul panoului Kibana sub forma unei hărți denumite *HeatMap*, prezentată în figura 3.6. Harta este actualizată în timp real sau în funcție de filtrele aplicate pentru a ilustra tendințele de inițiere a atacurilor.

Fig. 3.7 - Rezultate obținute în urma aplicării unui filtru pentru evenimentele detectate de Dionaea

În figura 3.7 sunt prezentate datele rezultate în urma filtrării pentru evenimentele detectate cu ajutorul honeypot-ului Dionaea.

Alături de informațiile numerice, de natură statistică, oferite de tripletul ELK în panoul Kibana, sunt prezentate și alte informații foarte utile pentru administratorii de rețele sau sisteme informatice. Un astfel de exemplu este reprezentat de datele de autentificare ilustrate în figura 3.8, obținute de către honeypot-ul *Cowrie*, care generează automată o pagină Web capcană care conține o zonă în care se solicită autentificarea unui utilizator.

Fig. 3.8- Datele de autentificare utilizate în cadrul paginii capcană a honeypot-ului Cowrie

În figura 3.8 sunt listate sub forma unui nor de cuvinte cele mai utilizate nume de utilizator și respectiv parole utilizate pentru încercarea de autentificare pe sistemul atacat. Dimensiunea fiecărui nume de utilizator, respectiv parolă este proporțională cu numărul de utilizări ale acestuia.

Informația prezentată în figura 3.8 este foarte utilă pentru a atenționa din nou deținătorii, administratorii și utilizatorii sistemelor informatice de orice tip cu privire la riscurile asociate utilizării unor parole comune, cum ar fi „root”, „password”, „123456” și a unor nume de utilizator implicite, de exemplu „root” sau „admin”

3.5. Concluzii parțiale

Securitatea sistemelor de automatizare vizează, așa cum a fost prezentat în capitolele 2 și 3, atât asigurarea controlului accesului la resursele sistemului, prin identificare precisă a utilizatorilor, cât și protecția împotriva atacurilor informatice, fără a neglija însă instrumentele (programele) destinate infectării sau chiar distrugerii datelor și a resurselor disponibile (viruși, viermi, troieni etc.).

Principala preocupare legată de securitatea sistemelor de automatizare, mai ales în cazul celor care sunt elemente componente ale infrastructurilor critice, constă în maximizarea disponibilității acestora, prin limitarea efectelor atacurilor informatice de tip DoS (Denial of Service), DDoS (Distributed Denial of Service) și ale virușilor sau viermilor informatici. Există soluții de securitate dezvoltate cu acest scop, dedicate pentru utilizarea pe calculatoarele personale. Aceste soluții nu pot fi utilizate în cadrul unor infrastructuri industriale, unde arhitectura sistemului și prioritățile proiectantului (disponibilitate față de confidențialitate) sunt diferite și unde sunt impuse restricții legate de performanțe, consum de energie sau putere de calcul.

În prima parte a prezentului capitol au fost prezentate concepte de bază și recomandări ale marilor companii de securitate sau centre de cercetare în domeniu, aplicabile la asigurarea securității sistemelor automate. Din analiza acestor recomandări autorul a identificat două tipuri principale de soluții de securitate robuste, și anume: soluții de tip *firewall* și soluții de tip *capcană – honeypot*.

Soluțiile de tip firewall reprezintă dispozitive de tip hardware sau software care pot fi utilizate pentru a bloca anumite conexiuni de rețea, utilizând reguli predefinite care țin seama de sursa și tipul datelor, numărul de conexiuni existente etc. În cazul implementărilor industriale, resursele de tip firewall sunt utilizate pentru a delimita rețeaua industrială de rețeaua de calculatoare convențională a companiei. Așa cum a fost prezentat în acest capitol firewall-urile sunt folosite în mod curent pentru a crea DMZ-uri, *(zone demilitarizate)* în care sunt concentrate serverele care oferă servicii publice, acestea fiind izolate de restul rețelei protejate.

Sistemele de tip honeypot, prezentate în detaliu în cadrul acestui capitol, au fost dezvoltate cu scopul obținerii de date referitoare la sursele și mecanismele de desfășurare ale atacurilor informatice. Honeypot-urile pot fi privite ca sisteme capcană, care imită funcționarea unui sistem real, de interes pentru atacatori.

În acest capitol tezei de doctorat sunt prezentate honeypotul ConPot, disponibil sub formă de software open-source, și sistemul de honeypot-uri T-Pot, dezvoltat în cadrul Deutsche Telekom AG (DTAG) Honeypot Project. Rezultatele testelor efectuate de autor, evidențiate în ultima parte a capitolului, **confirmă interesul crescut al atacatorilor pentru sistemele de automatizare conectate la Internet** și pentru protocoalele de comunicație de tip industrial.

O concluzie desprinsă de autor ca urmare a efectuării acestor teste este aceea că sistemele honeypot pot fi utilizate alături de firewall-uri pentru a masca sisteme sau servicii protejate și pentru a direcționa atacatorul către o „țintă falsă". Crearea unui număr mare de honeypot-uri (ținte false), menite să creeze confuzie atacatorului, reprezintă o metodă performantă și ieftină pentru creșterea securității. Un astfel de cyber-fog, respectiv un nor de „ceață informatică" în jurul sistemului protejat, reduce probabilitatea ca atacatorul să poată identifica sistemul real, crescând timpul și efortul necesar desfășurării atacului. De asemenea, această metodă de protecție este independentă de modul de desfășurare a unui potențial atac, fiind eficientă și împotriva unor tehnici nedocumentate, spre deosebire de sistemele clasice bazate pe reguli ce caracterizează doar un anumit tip de atac studiat.

Capitolul 4. Contribuții privind dezvoltarea unor metode de estimare a probabilităților de apariție și de succes ale unui atac informatic asupra unui sistem automat

4.1. Introducere

Măsurile selectate pentru asigurarea securității informatice a sistemelor automate depind de diverși factori cum ar fi*: tipurile de atacatori, tipurile de resurse protejate, importanța sistemului automat* protejat și *raportul dintre costul asociat măsurilor de securitate și costul generat de posibilul succes al unui anumit tip de incident* informatic. Pentru a putea stabili tipul de măsuri și gradul de protecție necesar pentru un anumit sistem automat se impune identificarea vulnerabilităților și amenințărilor asupra acestuia, precum și a probabilităților de apariție și succes ale unui atac informatic.

În acest capitol al tezei de doctorat se prezintă conceptele fundamentale referitoare la evaluarea automată a stării de securitate a unui sistem conectat la rețea, precum și modul de estimare a probabilităților de apariție și de succes ale unui posibil atac.

Dezvoltările din acest capitol al tezei sintetizează contribuțiile autorului prezentate în cadrul edițiilor 2014, 2015 și 2016 ale International Workshop on Systems Safety and Security - IWSSS, prin referințele bibliografice [B8], [B9] și [B51] și în capitolul [B7] publicat de editura Springer.

4.2. Evaluarea automată a vulnerabilităților unui sistem informatic

Din perspectiva prelucrării informației un sistem automat poate fi încadrat în categoria sistemelor informatice.

Evaluarea vulnerabilităților unui sistem poate fi realizată prin două metode și anume:

- testarea manuală a nivelului de securitate a sistemului, prin procedeul cunoscut sub denumirea de „*pentesting" – penetration testing.*
- evaluarea automată a vulnerabilităților, utilizând programe sau suite de programe specializate.

4.2.1. Baze de date care descriu posibile vulnerabilități

Mari companii de securitate și instituții guvernamentale, cum este cazul Departamentului de Apărare al Statelor Unite ale Americii – US Department of Homeland Security [W35], au preocupări evidente orientate către detecția, caracterizarea și eliminarea vulnerabilităților de securitate ale sistemelor informatice. În România, Centrul Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO [W36] este organizația guvernamentală cu preocupări și responsabilități în prevenirea, analiza și reacția la incidente de securitate informatică din domeniul infrastructurilor naționale (critice).

Fiecare organizație menționată testează atât componente hardware, cât și software (sisteme de operare, aplicații, protocoale de comunicații) pentru identificarea eventualelor vulnerabilități sau probleme de securitate. Fiecare vulnerabilitate identificată este introdusă într-o bază de date publică denumită *CVE – Common Vulnerabilites and Exposures*, disponibilă gratuit on-line la adresa http://cve.mitre.org. Conform înregistrărilor din referința [W37] baza de date este gestionată de către

compania *MITRE Corporation, beneficiind de finanțare din partea National Cyber Security Division a US Department of Homeland Security* [W38].

Lista *CVE* este folosită ca un *limbaj unic* de identificare și codificare a vulnerabilităților descoperite. Marea majoritate a soluțiilor de securitate dezvoltate până în prezent descriu vulnerabilitățile existente și modul de exploatare al acestora folosind *CVE*, ceea ce confirmă rolul esențial al acestei resurse.

4.2.2. Identificarea automată a vulnerabilităților sistemelor informatice

Testarea securității unui sistem se poate realiza automat folosind pachete software special create, cunoscute sub denumirea de *vulnerability scanners*. Trebuie menționat faptul că prin intermediul scannerelor de vulnerabilități se realizează doar colectarea informațiilor legate de punctele slabe ale obiectivului protejat fără a se implementa vreo măsură de securitate. Pe baza informațiilor obținute de la scanner, administratorul obiectivului (de exemplu administratorul rețelei, dezvoltatorul unui sistem de operare, etc.) poate adopta măsuri pentru îndepărtarea riscului identificat.

Structura generală a unui scanner de vulnerabilități, acesta include patru module și anume [B52]:

- motorul de scanare;
- baza de date internă;
- motorul de raportare;
- interfața cu utilizatorul.

Motorul de scanare reprezintă nucleul unui scanner de vulnerabilități, acesta realizând procesul de verificare al fiecărui obiectiv protejat prin utilizarea unor algoritmi, care impun parcurgerea pașilor prezentați în figura 4.1.

Fig. 4.1 - Pașii aferenți unui algoritm de identificare automată a vulnerabilităților unui sistem informatic

Astfel de programe au fost realizate atât de grupuri independente de dezvoltatori, în sistem open-source, cum ar fi de exemplu OpenVAS [W40], cât și de mari companii de securitate, cum este cazul Rapid7 care comercializează pachetul Nexpose [W39].

Autorul a pus în funcțiune în anul 2016, pachetul Nexpose, cu care a testat vulnerabilitățile consolei de operare a sistemului distribuit DeltaV, produs de compania Emerson[W43], din

laboratorul Automatizarea proceselor, din Departamentul Automatică, Calculatoare și Electronică din Universitatea Petrol-Gaze din Ploiești.

4.3. Contribuții la determinarea profilurilor specifice ale potențialilor atacatori

În secțiunile următoare ale acestui capitol vor fi prezentate modul de dezvoltare și rezultatele obținute prin utilizarea a trei sisteme de inferență fuzzy pentru *evaluarea automată a scorului asociat unui profil de atacator* și pentru *estimarea probabilităților de apariție* și, respectiv, *de succes ale unui atac informatic* asupra unui sistem.

4.3.1. Tipologii de atacatori

În cadrul rapoartelor elaborate de către centre specializate în studiul atacurilor și securității sistemelor informatice, prezentate în referințele [W32], [W34], [B5], [B6], [B53], au fost identificate și clasificate mai multe categorii de atacatori, fiecare categorie fiind caracterizată printre altele de un anumit nivel de cunoștințe, de resursele tehnice disponibile și de un grad de motivație pentru a duce la bun sfârșit atacul.

Principalele tipologii de atacatori sunt menționate în publicația NIST 800-82 [B54]. În teza de doctorat s-a realizat o caracterizare a următoarelor tipologii de atacatori, pe baza studiului literaturii de specialitate: hackeri, grupări criminale, servicii de informații, angajați nemulțumiți, teroriști informatici, spioni industriali.

4.3.2. Definirea scorului profilului de atacator

După cum s-a arătat în lucrările este [B7] și [B8] fiecare dintre profilurile prezentate anterior pot fi caracterizate prin trei parametri și anume: *cunoștințele atacatorului, resursele tehnice disponibile și motivația acestuia*.

- **Cunoștințele atacatorului** reprezintă cunoștințele și implicit competențele individuale sau de grup dobândite, care pot fi utilizate pentru a iniția și desfășura un anumit tip de atac informatic. Aceste competențe variază de la un nivel foarte scăzut, de exemplu utilizarea unui instrument predefinit pentru a efectua un atac, până la un nivel foarte avansat, corespunzător cunoașterii în detaliu a arhitecturii calculatoarelor, a particularităților sistemelor de operare și a mediilor de programare avansată. Abilitățile atacatorului sunt determinate de nivelul său de cunoștințe în domenii variate cum ar fi: *protocoale de comunicații, rețele de calculatoare, programare în diverse limbaje avansate și chiar în limbaj de asamblare, dar și de experiența acestuia.*

- **Nivelul resurselor tehnice** disponibile reprezintă un parametru cheie pentru caracterizarea profilului unui atacator. Acest parametru arată nivelul de resurse hardware și software pe care un atacator le poate accesa și utiliza, în scopul de a iniția și desfășura un anumit tip de atac.

- **Motivația atacatorului**, este un parametru care, datorită complexității sale, este cel mai dificil de cuantificat. Această caracteristică arată cât de determinată este o anumită entitate (persoană sau organizație) să lanseze și să desfășoare un atac informatic. Motivația are o dinamică foarte rapidă și dependentă de context. Câștigurile financiare, dobândirea unei anumite reputații, dorința de răzbunare sau convingerile religioase pot fi surse de motivație. Este evident faptul că atacul este mai complex și are o probabilitate mai mare de reușită în cazul în care motivația este consistentă.

Cercetările autorului, prezentate în lucrările [B7] și [B8], arată că toate cele trei caracteristici prezentate anterior pot fi utilizate ca intrări pentru un sistem de inferență bazat pe logica fuzzy. După cum rezultă din figura 4.2, în care este ilustrat în abordare informațională motorul de inferență,

ieșirea acestuia este reprezentată de scorul pentru profilul unui atacator, care are rolul de a indica toate abilitățile atacatorului pentru desfășurarea atacurilor informatice.

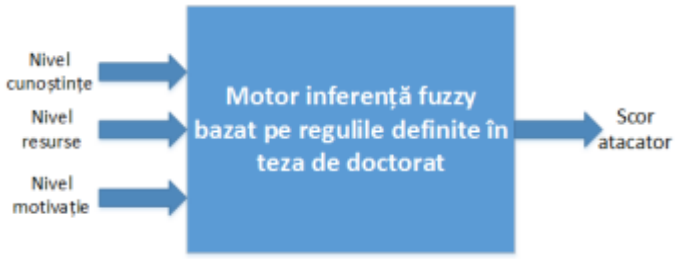

Fig. 4.2 - Schema bloc a sistemului de inferență fuzzy propus pentru stabilirea scorului de atacator

Pe baza investigațiilor autorului tezei de doctorat, a fost propus un set de reguli, prezentat în tabelul 4.1, care va fi utilizat de către motorul de inferență fuzzy.

Tabel 4.1– Regulile pe baza căruia funcționează sistemul de inferență fuzzy dezvoltat

Nr. crt.	Cunoștințe	Resurse tehnice	Motivație	Scor atacator
1	Mic	Mic	Mic	Foarte Mic
2	Mic	Mic	Mediu	Foarte Mic
3	Mic	Mic	Mare	Mic
4	Mic	Mediu	Mic	Foarte Mic
5	Mic	Mediu	Mediu	Foarte Mic
6	Mic	Mediu	Mare	Mic
7	Mic	Mare	Mic	Mic
8	Mic	Mare	Mediu	Mediu
9	Mic	Mare	Mare	Mediu
10	Mediu	Mic	Mic	Mic
11	Mediu	Mic	Mediu	Mic
12	Mediu	Mic	Mare	Mediu
13	Mediu	Mediu	Mic	Mic
14	Mediu	Mediu	Mediu	Mediu
15	Mediu	Mediu	Mare	Mediu
16	Mediu	Mare	Mic	Mic
17	Mediu	Mare	Mediu	Mediu
18	Mediu	Mare	Mare	Mare
19	Mare	Mic	Mic	Mediu
20	Mare	Mic	Mediu	Mediu
21	Mare	Mic	Mare	Mediu
22	Mare	Mediu	Mic	Mediu
23	Mare	Mediu	Mediu	Mediu
24	Mare	Mediu	Mare	Mare
25	Mare	Mare	Mic	Mare
26	Mare	Mare	Mediu	Foarte Mare
27	Mare	Mare	Mare	Foarte Mare

Fiecare dintre cele trei variabile de intrare este caracterizată de trei funcții de apartenență, corespunzătoare nivelurilor *mic*, *mediu* și, respectiv *mare*, rezultând astfel un set de 27 de reguli unice. Ieșirea asociată scorului profilului analizat, denumită *Nivel scor atacator*, este reprezentată

de cinci posibile funcții de apartenență corespunzătoare următoarelor valori: *foarte mic, mic, mediu, mare* și *foarte mare.*

Pe baza experienței autorului tezei și a interpretării rezultatelor prezentate în cadrul lucrărilor [B7], [B8], [B9], [B51] s-a realizat un sistem de inferență fuzzy în mediul MATLAB, a cărui schemă bloc este ilustrată în figura 4.3. Acest sistem are ca scop determinare automată, cu un efort redus din partea utilizatorului, a scorului profilului de atacator pe baza setului de reguli din tabelul 4.1 și a parametrilor menționați anterior.

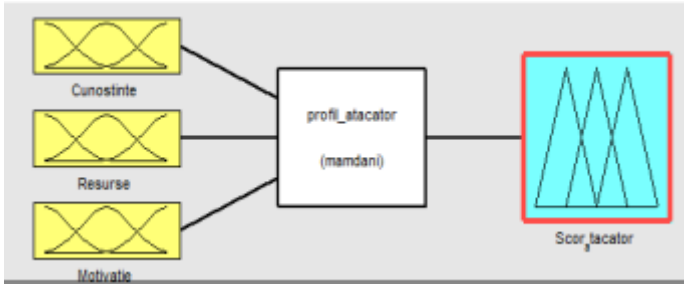

Fig. 4.3 - Schema bloc a sistemului de inferență fuzzy dezvoltat pentru determinarea scorului profilului de atacator

Utilizând sistemul dezvoltat de autor se poate evalua scorul unui potențial atacator pentru orice valori ale parametrilor pe baza căruia este definit (*cunoștințe, resurse și motivație*), introdus de către utilizator sub forma unui vector cu trei valori numerice din intervalul (*0, 1*).

Din totalul de 27 de reguli și posibile profiluri predefinite de atacator au fost selectate 4 profiluri susceptibile de a inița un număr substanțial de atacuri. În tabelul 4.2 este prezentată corespondența între profilurile de atacator semnificative, regulile, variabilele de intrare și de ieșire ale sistemului de inferență fuzzy.

Tabel 4.2 Corespondența între profilurile de atacator semnificative, regulile, variabilele de intrare și de ieșire ale sistemului de inferență fuzzy [B7]

Nr. crt.	Denumire profil atacator	Corespondență reguli – variabile intrare – variabilă ieșire				
		Nr. regulă	Resurse	Cunoștințe	Motivație	Scor profil
1	Script kiddie	1	Mic	Mic	Mic	Foarte mic
2	Angajat nemulțumit	8	Mic	Mare	Mediu	Mediu
3	Terorist informatic	14	Mediu	Mediu	Mediu	Mediu
4	Armată informatică (cyberarmy)	27	Mare	Mare	Mare	Foarte mare

În cadrul tezei de doctorat au fost analizate în detaliu cele patru profiluri prezentate în tabelul 4.2. Rezultatele obținute reliefează importanța nivelului de cunoștințe al atacatorului în domeniul tehnologiei informației, a securității informatice și a arhitecturii sistemului în determinarea scorului profilului de atacator.

4.4. Contribuții privind estimarea probabilității de apariție a unui atac informatic asupra unui sistem automat

În capitolul 3 al tezei de doctorat s-au prezentat pe larg caracteristicile sistemelor de tip honeypot. Analizând datele care provin de la acestea se pot identifica protocoalele, sistemele, localizările geografice, sistemele de operare etc. care sunt cel mai frecvent ținta unor tentative de atac informatic. Pe baza acestor date se poate introduce conceptul de *grad de interes* pe care îl prezintă un anumit sistem țintă pentru un atacator.

Gradul de interes poate fi estimat utilizând un honeypot cu proprietăți similare celor aferente sistemului protejat. De exemplu în cazul unui sistem SCADA se pot obține date referitoare la potențialele atacuri informatice folosind honeypot-ul ConPot prezentat în capitolul 3 al acestei teze.

Pe baza numărului de tentative de conectare se poate stabili dacă sistemul este „tentant” pentru atacatori sau este un sistem neglijat de aceştia. Dacă numărul de încercări de conectare pe honeypot este mare, este evident faptul că *gradul de interes* este mare şi că sistemul real trebuie să beneficieze de un număr crescut de măsuri de securitate. În schimb, dacă honeypot-ul nu este atacat pentru un interval de timp de ordinul zilelor se poate concluziona că sistemul nu prezintă interes pentru atacatori şi atunci nu se impun decât măsuri clasice de securitate de tip firewall şi antivirus.

În secţiunea 4.2. a acestui capitol al tezei de doctorat a fost prezentată o metodă de evaluare automată a vulnerabilităţilor unui sistem. *Scannerele de vulnerabilităţi* pot furniza, alături de descrierea detaliată a fiecărei vulnerabilităţi detectate, şi un indicator global (numeric sau lexical) al nivelului şi severităţii vulnerabilităţilor detectate.

Sistemul fuzzy dezvoltat în mediul MATLAB pentru estimarea probabilităţii de apariţie a unui atac informatic are ca variabile de intrare *gradul de interes prezentat de sistemul analizat* şi *nivelul de vulnerabilităţi* al acestuia. Aşa cum este prezentat în figura 4.4 se obţine o singură ieşire reprezentând *probabilitatea de apariţie a unui atac informatic asupra sistemului.*

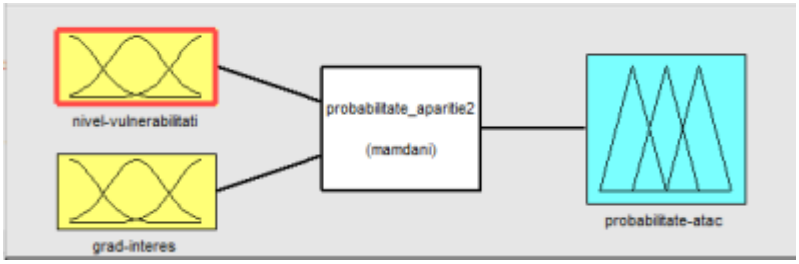

Fig. 4.4 - Schema bloc a sistemului fuzzy pentru determinarea probabilităţii de apariţie a unui atac informatic

Fiecare dintre cele două intrări este definită lexical prin trei valori: *mic, mediu şi mare.* Ieşirea este de descrisă de cinci valori lexicale: *foarte mică, mică, medie, mare, foarte mare.* Setul de reguli pe baza căruia a fost construit sistemul fuzzy este prezentat în tabelul 4.3.

Tabel 4.3 - Regulile de funcţionare ale sistemului fuzzy pentru estimarea probabilităţii apariţiei unui atac informatic

Nr. crt.	Nivel vulnerabilităţi	Grad Interes	Probabilitate atac
1	Mic	Mic	Foarte mică
2	Mic	Mediu	Foarte mică
3	Mic	Mare	Mică
4	Mediu	Mic	Mică
5	Mediu	Mediu	Medie
6	Mediu	Mare	Mare
7	Mare	Mic	Mare
8	Mare	Mediu	Mare
9	Mare	Mare	Foarte mare

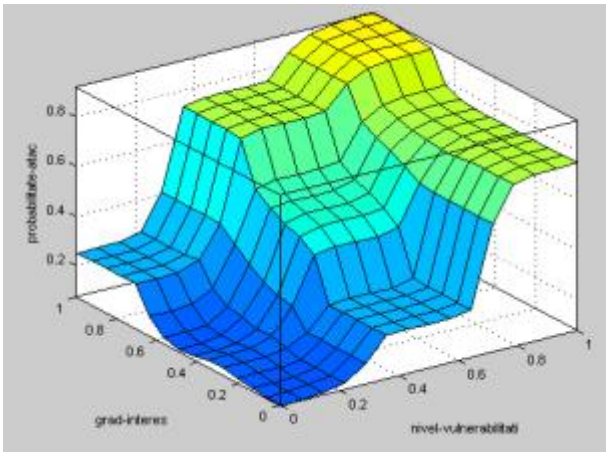

Fig. 4.5 - Variația probabilității de apariție a unui atac informatic asupra unui sistem în funcție de gradul de interes al atacatorilor și de nivelul de vulnerabilități ale sistemului

4.5. Contribuții privind estimarea probabilității de reușită a unui atac informatic asupra unui sistem automat

Scorul profilului de atacator poate fi utilizat pentru a introduce un nou concept și anume *estimarea ratei de reușită (succes) a unui anumit tip de atac*.

În opinia autorului tezei, **rata de succes a unui atac este influențată de** trei parametri și anume:

- **tipul atacatorului (mai exact scorul profilului său);**
- **vulnerabilitățile sistemului țintă;**
- **contramăsurile implementate pentru protejarea sistemului**.

Pentru evaluarea ratei de succes a unui atac a fost dezvoltat un sistem de inferență fuzzy, a cărei structură intrare-ieșire este ilustrată în figura 4.6. Sistemul dezvoltat este prezentat în detaliu în referința [B8].

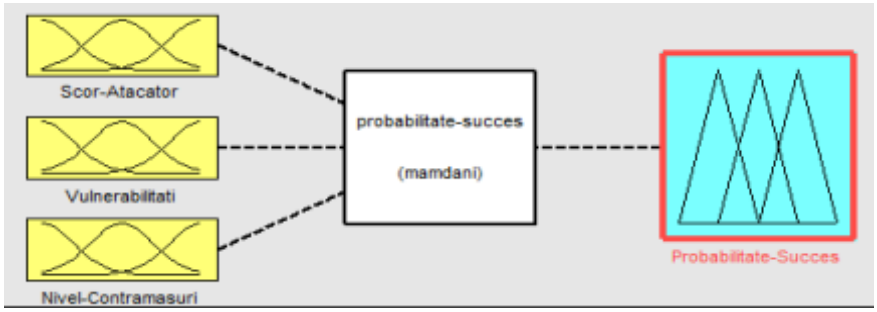

Fig. 4.6 - Reprezentarea intrare-ieșire a modelului fuzzy dezvoltat

Nivelul de vulnerabilitate al sistemului este cuantificat folosind un scanner de vulnerabilități după cum s-a prezentat în secțiunea 4.2 a acestui capitol. Nivelul determinat de scannerul de vulnerabilități poate fi ajustat ținând seama de faptul că pot exista unele breșe de securitate nedetectate sau neincluse încă în baza de date CVE. Se poate realiza astfel o ponderare a acestui nivel de vulnerabilități și în funcție de valoarea parametrului *grad de interes* definit în secțiunea anterioară a capitolului.

Nivelul de protecție a sistemului cuantifică din punct de vedere calitativ măsurile de securitate luate pentru a proteja sistemul țintă. Valoarea acestui parametru *„mic”, „mediu” sau „mare”* este apreciată de către administratorul sistemului respectiv, care cunoaște aceste măsuri.

Tabel 4.4- Selecție a regulilor sistemului de inferență fuzzy) [B7]

Nr. regulă				
	Scor profil atacator	***Nivel vulnerabilități***	***Nivel contramăsuri***	***Probabilitate de succes a atacului***
1	Foarte mic	Mic	Mic	Foarte scăzută
2	Mic	Mic	Mic	Scăzută
6	**Foarte mic**	**Mediu**	**Mediu**	**Scăzută**
10	Foarte mare	Mediu	Mic	Medie
15	**Foarte mare**	**Mare**	**Mic**	**Foarte înaltă**
20	Foarte mare	Mic	Mediu	Înaltă
27	Mic	Mare	Mediu	Medie
35	**Foarte mare**	**Mic**	**Mare**	**Medie**
40	Foarte mare	Mediu	Mare	Înaltă
45	Foarte mare	Mare	Mare	Foarte înaltă

Sistemul de inferență fuzzy dezvoltat funcționează pe baza unui set de 45 de reguli, prezentate pe larg în [B7]. O selecție a celor mai importante dintre acestea este listată în tabelul 4.4.

Este de menționat faptul că regulile prezentate în tabelul 4.4 sunt construite pe baza experienței autorului în domeniul securității informatice.

4.6. Concluzii parțiale

În cadrul prezentului capitol al tezei de doctorat s-au prezentat două metode destinate estimării probabilităților de apariție și respectiv de succes ale unui atac informatic asupra unui sistem.

Pentru estimarea probabilității de apariție a unui atac informatic a fost dezvoltat și implementat în MATLAB® un sistem fuzzy,bazat pe reguli, a cărui funcționare analizează două intrări și anume:

- nivelul de vulnerabilități al sistemului;
- gradul de interes pe care îl prezintă sistemul pentru atacatori.

Pentru dezvoltarea sistemului fuzzy **autorul tezei a introdus conceptul** de *grad de interes*, care cuantifică într-o variabilă lexicală (*mic, mediu, mare*) numărul de încercări de atac asupra unui honeypot care este similar sistemului protejat sau care simulează serviciile oferite de acesta.

Prin analiza datelor obținute cu ajutorul sistemului fuzzy dezvoltat se poate constata că probabilitatea de apariție a atacurilor informatice este afectată semnificativ de nivelul de vulnerabilități al sistemului și mai puțin de gradul de interes pe care îl prezintă acesta atacatorilor.

Pentru estimarea probabilității de succes a unui atac a fost implementat un sistem de inferență bazat pe logică fuzzy, care are asociate trei intrări și anume:

- scorul profilului de atacator;
- nivelul de vulnerabilități existente;
- nivelul măsurilor de protecție de care beneficiază sistemul țintă.

Scorul profilului de atacator este **un concept introdus de** autor pentru a permite cuantificarea "*abilităților*" unui atacator prin evaluarea nivelului de cunoștințe, a resurselor disponibile și a motivației acestuia. Acest scor este determinat cu ajutorul unui sistem de inferență

fuzzy implementat în mediul MATLAB®. Sistemul fuzzy dezvoltat evidențiază dependența între abilitățile atacatorului și nivelul de cunoștințe pe care acesta le posedă

Nivelul de vulnerabilități al unui sistem poate fi evaluat cu ajutorul unor aplicații specializate, denumite *scannere de vulnerabilități*, al căror mod de funcționare a fost prezentat în secțiunea 4.2 a capitolului. O direcție viitoare de cercetare este reprezentată de dezvoltarea unei metode de ajustare a nivelului de vulnerabilități, nivel rezultat prin scanare pentru a se evidenția și impactul unor breșe de securitate necunoscute scannerului sau care nu au fost introduse în bazele de date CVE.

Nivelul de protecție al unui sistem este evaluat de către administratorul sistemului, pe baza măsurilor de securitate pe care acesta le-a implementat.

Probabilitatea de reușită a unui atac este dependentă în mod evident de nivelul de vulnerabilitate al sistemului țintă și de abilitățile atacatorului. Măsurile de protecție permit scăderea acestei probabilități la un nivel acceptabil.

Metoda propusă poate fi îmbunătățită astfel încă să fie incluse mecanisme de senzitivitate la context, care să permită utilizarea sa în timp real, în funcție de apariția unor noi amenințări de securitate sau detecția unor noi vulnerabilități.

Capitolul 5. Contribuții privind dezvoltarea unui mecanism pentru autentificarea senzorilor conectați prin protocolul Modbus/TCP

Problematica creșterii securității sistemelor de automatizare este actuală și prezintă un interes deosebit pentru industrie, apărare, cercetare, dar și pentru comunitatea academică. Asigurarea unor mecanisme de control al accesului eficiente, rapide și care să nu afecteze performanțele sistemului protejat constituie o provocare lansată comunității științifice internaționale. În acest context accesul se referă preponderent la intruziuni în sistemele informatice.

Protocoalele de comunicații în mediul industrial folosite în mod curent, nu posedă mecanisme de autentificare a sursei datelor transmise. Din acest motiv desfășurarea unor atacuri de tip *man-in-the-middle* este posibilă și destul de simplu de realizat. În cadrul acestui capitol al tezei de doctorat se propune un mecanism pentru autentificarea senzorilor conectați într-o rețea bazată pe protocolul Modbus/TCP.

5.1. Caracterizarea protocolului de comunicație Modbus standard

5.1.1. Rețele industriale și conectivitate

Funcționarea oricărui sistem de automatizare are la bază prelucrarea și transferul de informație. Sistemele actuale de conducere au în componență sisteme de prelucrare a informației mai mult sau mai puțin complexe, între care regulatoare numerice, automate programabile, calculatoare de proces. Integrarea acestora între ele și cu echipamentele de câmp (traductoare, elemente de execuție) este un obiectiv dificil ce nu poate fi atins decât prin realizarea unei rețele de comunicații industriale, cu protocoale specifice și o bună ierarhizare. Problema compatibilizării acestor protocoale este deosebit de complexă și prezintă un interes deosebit pentru comunitatea academică și pentru cea industrială, în calitate de beneficiar sau producător de echipamente. În acest moment, cei mai mulți producători de echipamente utilizează protocoale proprietare, standardizate, oferind însă și posibilități de export al datelor în formate compatibile cu alte echipamente existente pe piața de profil. [B12]. Deoarece nu există un protocol universal pentru rețele industriale, descrierea funcționării acestora se poate realiza pe baza modelului de referință ISO-OSI, consacrat ca model teoretic pentru rețelele de calculatoare. Particularitățile modelului ISO-OSI și ale nivelurilor sale au fost prezentate în primul capitol al acestei teze de doctorat. În continuare se vor prezenta unele rețele și protocoale utilizate cu precădere în mediul industrial și se va face referire la nivelul corespunzător al modelului OSI pentru fiecare protocol prezentat.

5.1.2. Protocolul Modbus standard

Modbus [W8] este un protocol de nivel aplicație, corespunzător nivelului 7 din modelul ISO OSI, care permite transferul mesajelor în sistem client/server, corespunzător mecanismului producător-consumator, între echipamente conectate pe o linie de transmisie. Protocolul implementează un mecanism cerere-răspuns de nivel înalt, evitând restricțiile și problemele puse de nivelurile *legătură de date și fizic*.

Protocolul Modbus are două variante de implementare și anume **Modbus ASCII** și **Modbus RTU**. În versiunea ASCII toate caracterele unui pachet sunt codificate ASCII spre deosebire de RTU în care datele se codifică binar [B12].

În evoluția protocolului Modbus pot fi identificate două direcții, și anume Modbus TCP și Modbus Plus. Implementarea **Modbus/TCP** este similara cu **Modbus RTU**, deosebirea constând în

faptul că datele sunt transmise sub forma pachetelor TCP/IP. În ceea ce privește varianta **Modbus Plus** este specifică echipamentelor produse de compania Modicon și necesita un coprocesor dedicat, folosind ca mediu fizic pentru comunicație cablu torsadat, care permite o viteză de transfer a datelor de aproximativ 1 Mbps [B12].

La nivel fizic, protocolul Modbus standard se bazează pe o rețea RS-485 tipică.

La nivelul legăturii de date se stabilește structura de date a pachetului transmis în rețea, structură evidențiată în figura 5.1 și ale cărei specificații sunt prezentate în continuare.

Adresa slave (1 byte)	Cod funcție (1 byte)	Date (variabil)	CRC (2 bytes)

Fig. 5.1 - Structura unui pachet conform protocolului Modbus [B12]

- Câmpul *Adresa slave* are dimensiunea de un octet și reprezintă identificatorul unic al dispozitivului slave căruia îi este adresat pachetul.
- Câmpul *Cod funcție* are lungimea de un octet și desemnează operația ce trebuie executată de unitatea slave destinatară.
- Câmpul *Date* este de lungime variabilă, având maxim 251 de octeți. Semnificația sa este impusă de valoarea câmpului *Cod funcție.*
- Câmpul *CRC* reprezintă suma de control calculată la nivelul întregului pachet de date. Dispozitivul care emite pachetul calculează și înscrie suma CRC înainte de emisie. La recepție se calculează suma CRC și se compară cu valoarea recepționată, pachetele cu CRC eronat fiind ignorate.

5.2. Analiza protocolului Modbus/TCP

5.2.1. Particularitățile protocolului Modbus/TCP

Protocolul Modbus/TCP [B65] este un protocol modern pentru comunicații industriale, în cazul căruia cadrul de date Modbus standard este împachetat (încapsulat) într-un cadru Ethernet și transmis în rețea.

Încapsularea datelor se realizează prin includerea unui pachet de tip MBAP – Modbus Application Protocol în zona de date a pachetului TCP/IP. Modul de construire al pachetului MBAP pe baza unui cadru de date Modbus standard este ilustrat în figura 5.2.

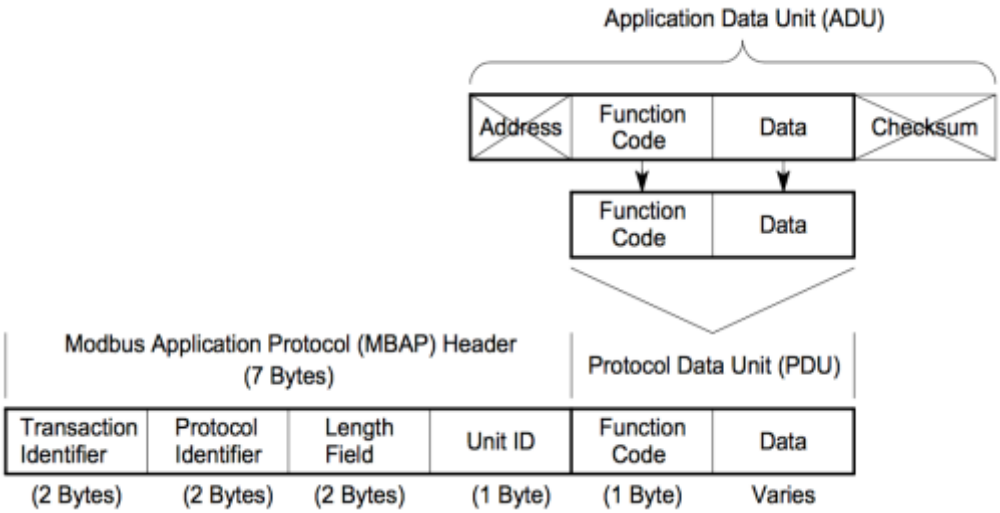

Fig. 5.2 - Modul de construire al unui pachet de tip MBAP [B65]

Datele în format MBAP sunt încapsulate într-un cadru Ethernet conform standardului TCP/IP, așa cum este ilustrat în figura 5.3.

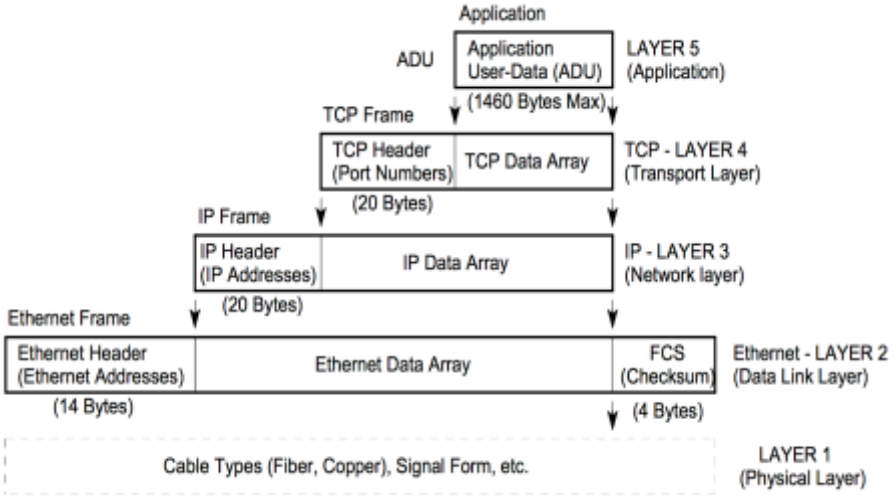

Fig. 5.3 - Formarea cadrului TCP/IP care include pachetul MBAP [B65]

5.2.2. Vulnerabilități de securitate ale protocoalelor Modbus și Modbus/TCP

În literatura de specialitate, conform referințelor [B4], [B12] și [W50] au fost semnalate **principalele probleme de securitate** întâlnite în cazul utilizării **protocolului Modbus,** între care semnificative sunt:

- lipsa unui mecanism de autentificare a sursei mesajelor transmise;
- lipsa oricărui mecanism de criptare a datelor, toate adresele și mesajele fiind transmise sub forma de text lizibil, care poate fi interceptat și modificat relativ ușor;
- lipsa unor mecanisme de control a integrității datelor la nivel aplicație, mai ales în cazul Modbus/TCP), vulnerabilitate care permite unui atacator să introducă în mediul de comunicație mesaje validate numai la nivel transport;
- imposibilitatea blocării regimului broadcast în cazul variantelor Modbus RTU, Plus și serial.

5.3. Contribuții la dezvoltarea unui mecanism de autentificare pentru senzori conectați prin Modbus/TCP

5.3.1. Necesitatea autentificării senzorilor conectați prin Modbus/TCP

Dacă în cadrul rețelelor de calculatoare este foarte importantă asigurarea confidențialității datelor transmise, în rețelele industriale este critică asigurarea *integrității și autenticității* datelor.

Majoritatea protocoalelor industriale utilizate în momentul de față nu asigură un mecanism de *autentificare* a sursei informației transmise în rețea, respectiv a emițătorului, din acest motiv fiind vulnerabile în fața unor atacuri de tip *IP-spoofing / hi-jacking/ man-in-the-middle*. Mecanismele de producere ale atacurilor din aceste categorii au fost prezentate în primul capitol al tezei de doctorat.

Un caz particular de atac, care constă în interceptarea și deturnarea datelor provenind de la un senzor sau transmiterea de informații false în rețea, presupune parcurgerea următoarelor etape:

1. **Interceptarea canalului de comunicație**
2. **Falsificarea adresei IP a senzorului**
3. **Transmiterea de informații false către celelalte echipamente din rețea**

Un alt tip de atac poate fi reprezentat de în înlocuirea fizică a unui senzor cu un echipament care transmite date false în rețea, producând aceleași efecte cu atacul de tip IP-spoofing / hi-jacking prezentat anterior.

5.3.2. Demonstrarea posibilităților de interceptare a datelor transmise prin protocolul Modbus/TCP

Pentru a reduce probabilitatea de reușită a unor astfel de atacuri este necesară introducerea unui mecanism de autentificare a senzorilor care transmit date folosind protocoale de comunicație industrială

Pentru a demonstra posibilitatea de a intercepta cu ușurință traficul de date transmis într-o rețea folosind protocolul Modbus/TCP s-a realizat, în laborator, un stand experimental, a cărui structură este prezentată în figura 5.4.

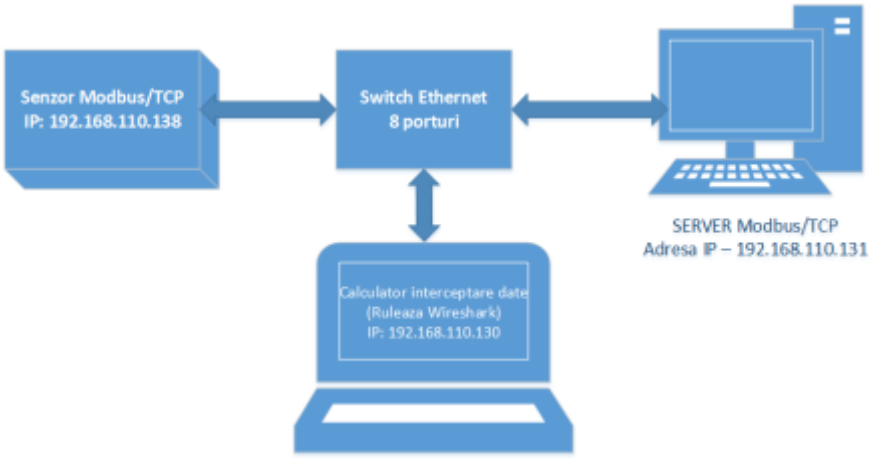

Fig. 5.4 - Structura standului pentru interceptarea datelor transmise între un senzor și un server Modbus/TCP

Scenariul de test care a fost implementat de către autor în laborator, într-o rețea izolată, constă în conectarea unui senzor Modbus/TCP și a unui server corespunzător, interceptarea și afișarea comenzilor transmise de server și a răspunsurilor emise de senzor de către un calculator mobil, conectat la aceeași rețea.

Elementele utilizate pentru realizarea standului experimental sunt descrise în cele ce urmează:

- **Senzor conectat prin protocolul Modbus/TCP** – este un senzor de temperatură standard, care transmite date prin intermediul protocolului investigat.
- **Server Modbus/TCP** – este un calculator pe care rulează sistemul de operare Windows și pe care a fost instalată aplicația QModMaster [W51]. Acest program open-source permite simularea unui echipament Modbus/TCP de tip master (server) capabil să interogheze și să transmită comenzi către dispozitive (senzori) conectați ca module slave în rețea.
- **Calculator interceptare date** – este un notebook pe care rulează sistemul de operare MacOS X, sistem proprietar al companiei Apple și are instalat programul Wireshark destinat înregistrării pachetelor TCP/IP.

În cadrul Wireshark se pot configura filtre, folosind funcțiile de analiză automată a pachetelor recepționate. Astfel pot fi evidențiate doar pachetele transmise prin Modbus/TCP, așa cum este ilustrat în figura 5.5. Analizând această figură se poate observa faptul că este înregistrată toată comunicația între server (adresa IP 192.168.110.131) și senzor (adresa IP 192.168.110.138).

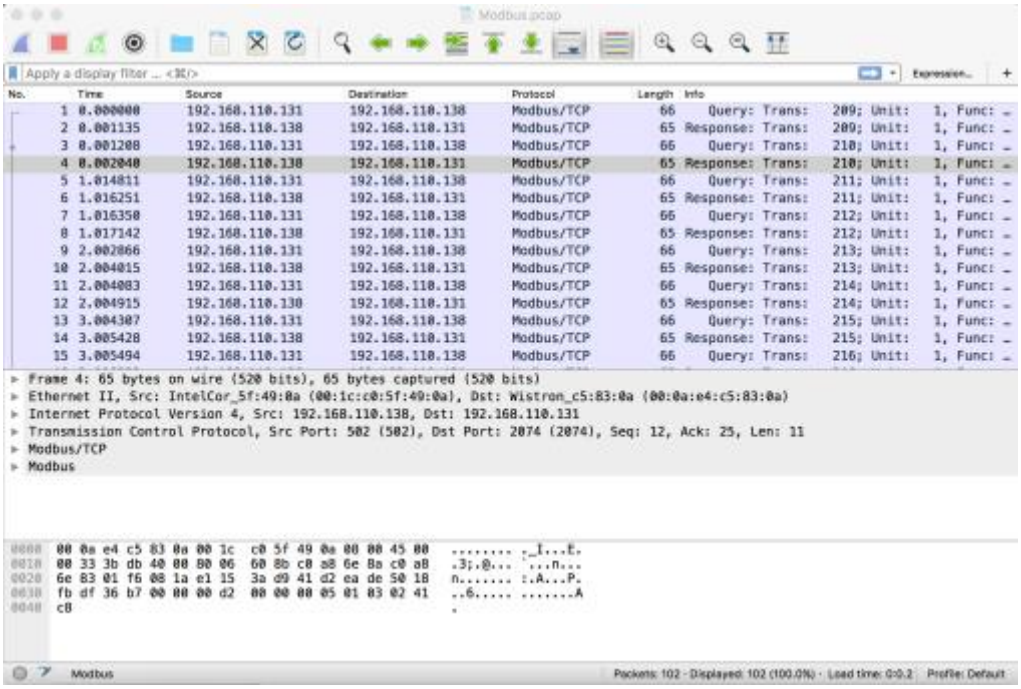

Fig. 5.5 - Captură de ecran cu pachetele Modbus/TCP recepționate de către programul Wireshark

În partea de jos a ferestrei din figura 5.5 este prezentat conținutul pachetului recepționat în format hexazecimal, poate fi evidențiată semnificația la nivel de bit a datelor din pachet. *Aceasta constatare a permis autorului tezei să concluzioneze că protocolul Modbus/TCP este vulnerabil în fața atacurilor de interceptare a datelor transmise.*

5.3.3. Proiectarea conceptuală a metodei de autentificare propuse

Autentificarea unui mesaj este procesul prin intermediul căruia destinatarul se poate asigura că mesajul provine de la un anumit expeditor și totodată că pe parcursul transmisiei mesajul nu a fost modificat. Practic prin autentificare se poate răspunde la întrebarea *„Mesajul primit este cel transmis de sursă, iar sursa este cea reală?”*.

Autentificarea unui senzor de către un server se poate realiza pe baza unor informații suplimentare transmise de acesta. Întrucât structura unui pachet Modbus/TCP este foarte bine definită, orice intervenție asupra conținutului pachetului de date ar face funcționarea rețelei imposibilă.

Datele la nivel transport sunt mai ușor de modificat de către entitățile de la nivelul aplicație al modelului ISO/OSI, din acest motiv pentru metoda de autentificare propusă vor fi folosite câmpurile opționale din antetul TCP.

Câmpul **Opțiuni** al pachetului TCP are dimensiunea de maxim 96 biți și poate fi utilizat pentru transmiterea de informații care nu au fost incluse în varianta inițială a standardului TCP. ***În această zonă poate fi introdusă informația de autentificare a senzorului, întrucât această informație nu este modificată pe parcursul transmisiei de date și poate fi citită la destinație pentru a confirma identitatea sursei [B16, B17].***

Pentru a genera semnătura senzorului trebuie să se folosească o funcție de tip *hash* (funcție de dispersie, neinversabilă), așa cum sunt MD5 sau SHA-1.

Ținând seama de considerentele prezentate anterior, algoritmul propus de autorul tezei pentru introducerea informației de autentificare într-un pachet de tip Modbus/TCP conține etapele de mai jos.

- Etapa 1 - Generarea pachetului de date MBAP standard.
- Etapa 2 – Calcul funcție *hash.*

- Etapa 3 – Adăugarea semnăturii obținute în antetul TCP al pachetului.
- Etapa 4 – Generarea pachetului TCP propriu-zis.
- Etapa 5 – Generarea pachetului IP și transmiterea acestuia în rețea.

O abordare alternativă pentru autentificarea senzorilor conectați prin Modbus/TCP constă în introducerea informației de autentificare, respectiv semnătura *hash* a senzorului, în zona de date a pachetului TCP/IP. Această soluție este echivalentă metodei propuse în cadrul acestui subcapitol, dar spre deosebire de aceasta, impune existența unui receptor compatibil, care să extragă datele de autentificare și să reconstruiască pachetul TCP/IP la recepție. Acest dezavantaj nu există în cadrul soluției bazate pe introducerea datelor de autentificare în câmpul *Options* din antetul TCP.

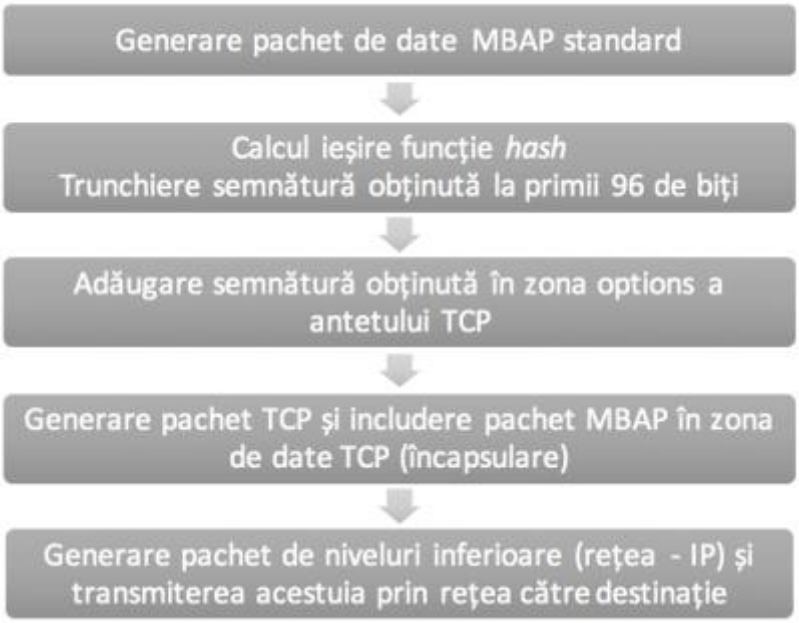

Fig. 5.6 – Secvențierea algoritmului propus pentru introducerea datelor de autentificare

5.3.4. Verificarea autenticității datelor recepționate

Pentru verificarea autenticității datelor recepționate trebuie comparat conținutul câmpurilor opționale din antetul TCP al pachetului recepționat cu hash-ul calculat de către receptor.

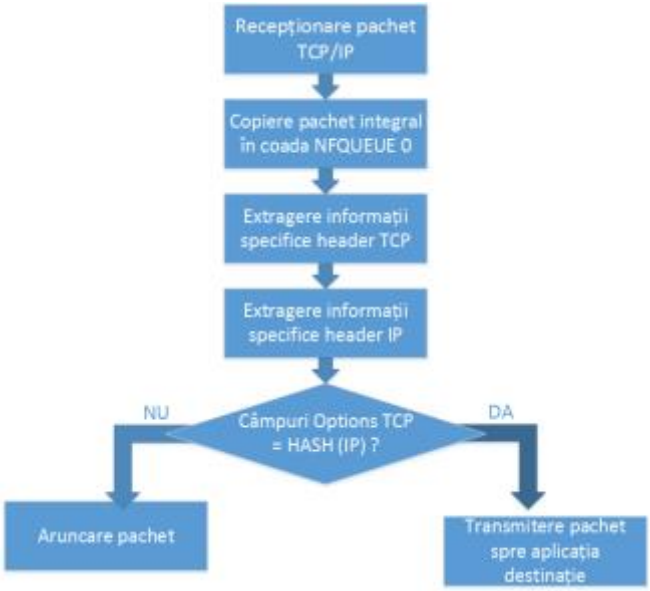

Fig. 5.7 - Schema logică a programului pentru extragerea și validarea datelor de autentificare din pachetul Modbus/TCP

În figura 5.7 este prezentată schema logică a programului dezvoltat pentru extragerea și validarea informației de autentificare din pachetul Modbus/TCP securizat.

Programul corespunzător algoritmului prezentat în figura 5.7 poate fi scris în limbajul de programare C și utilizează mecanismele specifice sistemului de operare Linux pentru a putea extrage informația de autentificare din pachete TCP/IP, mecanisme ce vor fi prezentate în următoarea secțiune a acestui capitol.

5.3.5. Testarea în laborator a soluției propuse pentru autentificarea senzorilor conectați prin protocolul Modbus/TCP

Pentru confirmarea validității metodei propuse pentru autentificarea senzorilor conectați prin Modbus/TCP într-o rețea industrială a fost realizat de către autor un demonstrator, a cărui structură este prezentată în figura 5.8.

Demonstratorul integrează un senzor de temperatură conectat la rețea prin protocolul Modbus/TCP, implementat cu ajutorul unui sistem de dezvoltare (modulul) NXP LPC1768. Ieșirea Ethernet (RJ45) a acestui sistem este conectată la una din intrările Ethernet aferente sistemului de dezvoltare ATMEL ATSAMA5D3-Xplained, sistem care are rolul de a genera și introduce datele de autentificare în pachetul TCP/IP care este transmis în rețea prin intermediul celei de-a doua interfețe Ethernet (RJ45). Sistemul de dezvoltare ATSAMA5D3 este conectat la un switch sau la un router Ethernet standard, la care este conectat și un calculator portabil care rulează sistemul de operare Linux și care are rolul de a recepționa și decodifica datele transmise de senzor. În continuare vor fi prezentate succint caracteristicile elementelor componente ale demonstratorului realizat.

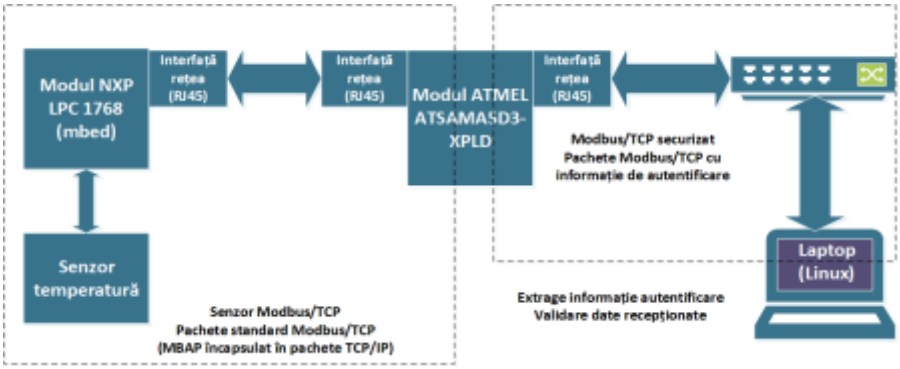

Fig. 5.8 - Structura demonstratorului pentru soluția de autentificare a senzorilor conectați prin Modbus/TCP

```
1  import os,sys,nfqueue,socket
2  from scapy.all import *
3  import os
4
5  def callback(i, payload):
6      data = payload.get_data()
7      pkt = IP(data)
8      pkt[TCP].options=[(25,"\x54\x45\x53\x54\x5f\x54\x43\x50\x5f\x4f\x50\x54\x49\
*      x4f\x4e\x53\x5f\x4d\x4f\x44\x42\x55\x53\x5f\x41\x55\x54\x45\x4e\x54\x49\x46\
*      x49\x43\x41\x54")]
9      print pkt[TCP].options
10     del pkt[TCP].chksum
11     del pkt[IP].chksum
12     payload.set_verdict_modified(nfqueue.NF_ACCEPT, str(pkt), len(pkt))
13
14 def main():
15     q = nfqueue.queue()
16     q.open()
17     q.bind(socket.AF_INET)
18     q.set_callback(callback)
19     q.create_queue(0)
20     try:
21         q.try_run() # Main loop
22     except KeyboardInterrupt:
23         q.unbind(socket.AF_INET)
24         q.close()
25 main()
```

Secvența de program, prezentată anterior, este realizată de autor în limbajul Python folosind funcțiile specifice aplicației Scapy pentru adăugarea informației de autentificare în pachetul TCP.

Pentru verificarea datelor transmise de către senzorul Modbus/TCP securizat, în speță sistemul de dezvoltare ATSAMA5D3, a fost utilizat un calculator care rulează sistemul de operare Ubuntu Linux, în cadrul căruia s-a instalat aplicația *modpoll,* disponibilă la adresa Web [W55], care are rolul de a simula un dispozitiv de tip Mobus/TCP master. Practic folosind această aplicație se pot transmite interogări către un echipament de tip slave și se pot recepționa pachetele transmise ca răspunsuri.

Pentru a vizualiza pachetele recepționate a fost utilizat programul *Wireshark,* care așa cum a fost evidențiat în capitolele anterioare ale tezei de doctorat, are abilitatea de a intercepta traficul de rețea și de a efectua anumite analize asupra pachetelor capturate.

Testarea demonstratorului s-a realizat în laborator prin conectarea senzorului Modbus/TCP la rețea și transmiterea unei comenzi de interogare de către calculatorul pe care rulează programul Wireshark, prin intermediul căruia s-a interceptat traficul din rețea. Conținutul câmpului *Options* din antetul TCP, ilustrat în figura 5.9, și anume textul „*TEST_TCP_OPTIONS_MODBUS_ AUTENTIFICAT*”, permite validarea la nivel de laborator a soluției propuse pentru autentificarea senzorilor.

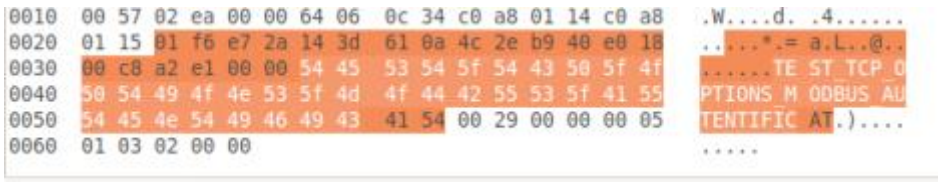

Fig. 5.9 - Conținutul pachetului Modbus/TCP recepționat

5.4. Concluzii parțiale

Autentificarea sursei datelor transferate în mediul industrial este o problemă de actualitate prin intermediul căreia se pot elimina sau reduce atacurile de tip furt de identitate/ sensor hi-jacking.

Deși autentificarea unei entități nu mai este de mult timp o problemă în rețelele de calculatoare, pentru rețelele de senzori este o temă nouă și complexă, datorită restricțiilor impuse de resursele de calcul limitate existente la nivelul senzorilor și din cauza necesității păstrării compatibilității cu toate protocoalele și echipamentele existente.

În acest capitol s-a prezentat un mecanism de autentificare al senzorilor bazat pe generarea unei „semnături” și transmiterea acesteia alături de datele propriu-zise prin rețea, în câmpul *Options* al fiecărui pachet TCP. Verificarea autenticității datelor se realizează la destinație prin analiza structurii pachetului TCP/IP recepționat. Această abordare permite compatibilitatea cu toate echipamentele de rețea existente (routere, switch-uri), nu afectează performanțele sistemului de comunicație, este eficientă și se poate implementa cu costuri relativ reduse în industrie.

Soluția propusă a fost testată în condiții de laborator, demonstrându-se astfel funcționalitatea acesteia. S-a constatat că performanțele și funcționarea rețelei nu sunt afectate de introducerea datelor de autentificare în cadrul pachetului TCP.

Pentru implementarea unei metode robuste de autentificare se impune utilizarea unui algoritm de hashing cu o distribuție mai largă a valorilor, așa cum este cazul algoritmului SHA-1. De asemenea pentru a putea valida și momentul transmiterii informației în rețea se impune folosirea unor hash-uri de tip OTP – One Time Pad / Password, cu marcare temporală.

Capitolul 6. Contribuții privind realizarea unui sistem de identificare a personalului de operare a procesului

Securitatea sistemelor automate vizează, așa cum a fost arătat în primele trei capitole ale tezei de doctorat atât asigurarea controlului accesului fizic la resursele sistemului, cât și securitatea informatică a acestuia, adică protecția la atacuri informatice, care de obicei provin din rețea.

Chiar dacă nivelul de protecție al sistemului față de atacurile provenind din rețeaua proprie sau din Internet este crescut, pot apărea probleme de securitate cauzate de utilizatori neautorizați care obțin acces fizic la resursele sistemului. Acest inconvenient poate fi eliminat prin intermediul unor mecanisme de control al accesului fizic, bazate pe analiza unor caracteristici biometrice (amprentă digitală, iris, voce) după cum a fost prezentat în capitolul 2.

Un sistem performant de identificare a persoanelor este complementar celorlalte mijloace de creștere a securității unei infrastructuri industriale, cum sunt de exemplu instalarea unor sisteme de tip firewall sau a unor mecanisme de verificare a datelor transmise.

În cadrul acestui capitol al tezei de doctorat se urmărește dezvoltarea conceptuală a unui *sistem hibrid* destinat identificării personalului care accesează zone protejate și verificării gradului de echipare al acestuia. Sistemul se bazează pe conceptul de card RFID[15] biometric, introdus de colectivul de cercetători din care autorul tezei face parte în brevetul de invenție [B23] și în lucrarea [B69]. În prima parte a capitolului este prezentată structura sistemului propus, alături de extinderea conceptului de *card RFID biometric.* În cea de-a doua parte a capitolului este descris, la nivel conceptual, modul de funcționare a sistemului propus.

6.1. Structura sistemului propus

Sistemul destinat verificării identității operatorilor și personalului care accesează zone protejate are în componență patru entități, după cum urmează:

- cardul RFID biometric;
- stații de emitere a cardurilor RFID biometrice;
- puncte de control al accesului;
- baza de date centralizată,

care sunt descrise detaliat în cadrul tezei de doctorat.

6.2. Cardul RFID biometric

Conceptul de *card RFID biometric,* care a fost introdus de către autor în brevetul de invenție [B23], a fost descris în cadrul celui de-al doilea capitol al tezei de doctorat. Cardul RFID biometric descris în referința [B23] este destinat efectuării de tranzacții bancare la bancomate (ATM-uri) care au în echipare un cititor de amprente. Șabloanele amprentelor utilizatorului sunt stocate pe card, identificarea persoanei realizându-se *local, rapid și sigur,* fără transmiterea datelor personale prin Internet. În acest subcapitol al tezei de doctorat se va prezenta o propunere de extindere a conceptului introdus în [B23] prin definirea unui **card RFID biometric destinat identificării personalului care accesează zone periculoase sau facilități de comandă ale infrastructurilor industriale.**

[15] RFID – Radio Frequency IDentification – Tehnologie destinată identificării obiectelor prin radiofrecvență

6.2.1. Cerințe și specificații impuse cardului RFID biometric

Cardul RFID biometric destinat identificării personalului care accesează zone periculoase este un tag sau o etichetă, care respectă în totalitate standardul RFID MiFare funcționând pe frecvența de 13,56 MHz și având 1 KB de memorie.

6.2.2. Structura propusă pentru memoria cardului RFID biometric

Cardul RFID biometric utilizat are memoria de 1 KB. Pentru a putea răspunde cerințelor formulate anterior, în cadrul acestui sistem sunt utilizate carduri RFID MiFare pasive, reinscriptibile. Etichetele din această categorie permit modificarea informațiilor din memorie de către un dispozitiv specializat, denumit *inscriptor de carduri*.

Structura de memorie propusă constituie o personalizare a structurii descrise în brevetele [B23] și [B70] în capitolul 2 al prezentei teze de doctorat.

În figura 6.1 este ilustrată o „hartă" a memoriei de 1 KB a cardului RFID biometric. Pentru o interpretare simplificată a structurii, fiecare byte are o adresă proprie exprimată în hexazecimal, cu valori între 0 și 3FF. În prima coloană (*Adresa Octet 0*) este specificată adresa primului octet de pe rândul respectiv.

Adresa Octet 0	Octet 0	Octet 1	Octet 2	Octet 3	Octet 4	Octet 5	Octet 6	Octet 7
0x0000	ID UTILIZATOR							
0x0008								0x000F
0x0010	SABLON AMPRENTA1							
...								
0x0108								0x010F
0x0110	SABLON AMPRENTA2							
...								
0x0208								0x020F
0x0210	SABLON AMPRENTA3							
...								
0x0308								0x030F
0x0310	DATA EXPIRARE							0x0317
0x0318	PIN							0x031F
0x0320	COD ZONA ACCES 1				COD ZONA ACCES 2			
...	COD ZONA ACCES n				COD ZONA ACCES n+1			
0x0368	COD ZONA ACCES 9				COD ZONA ACCES 10			0x36F
0x0370	COD OPERATIE PERMISA 1				COD OPERATIE PERMISA 2			
...	COD OPERATIE PERMISA n				COD OPERATIE PERMISA n+1			
0x03B8	COD OPERATIE PERMISA 9				COD OPERATIE PERMISA 10			0x3BF
0x03C0	PIN SUPERIOR							0x03C7
0X03C8	ID EMITENT CARD							
0X03D0								0X03D7
0X03D8	DATA ULTIMA MODIFICARE							0X03DF
0X03E0	ID UTILIZATOR MODIFICARE							
0X03E8								0X03EF
0x03F0				SUMA CONTROL				
0x03F8								0x03FF

Fig. 6.1 –Harta memoriei propuse pentru cardul RFID biometric

6.2.3. Procesul de emitere a cardului RFID biometric

Cardurile RFID biometrice, având structura memoriei descrisă anterior, sunt emise folosind o stație specializată care include următoarele componente:

- cititor și inscriptor RFID pe frecvența de 13,56 MHz;
- scanner pentru amprenta digitală;
- calculator pe care rulează o aplicație specializată care implementează algoritmul etapizat în figura 6.2 și care se poate conecta la baza de date a sistemului propus de control al accesului.

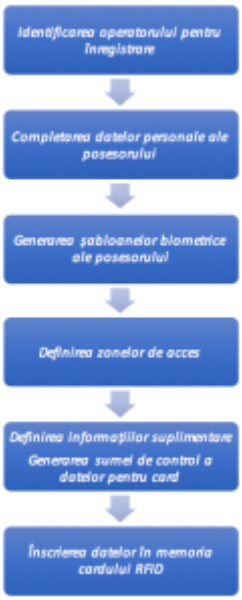

Fig. 6.2 - Etapele aferente procesului de emitere a cardului RFID biometric

6.3. Algoritmul de verificare a identității operatorilor și a nivelului de echipare al acestora

Principala funcție a sistemului propus constă în verificarea identității posesorului cardului și implementarea unui mecanism de control al accesului în zone protejate. Pentru atingerea acestui obiectiv se propune algoritmul de funcționare cu schema logică din figura 6.3.

Fig. 6.3 - Schema logică a algoritmului pentru verificare identității

Conform algoritmului descris, sistemul poate verifica identitatea utilizatorului și drepturile sale de acces. În cererea de brevet de invenție [B70], depusă de colectivul de cercetători din care autorul tezei face parte, și în articolul [B71] este prezentată o modalitate de extindere a funcționalității sistemului pentru verificarea suplimentară a nivelului de echipare.

În referința [B70] este propusă și o structură de card RFID pentru identificarea utilizatorului, dar acesta spre deosebire de propunerea din subcapitolul 6.3 nu include informațiile biometrice ale posesorului.

Sistemul propus în cadrul acestui capitol al tezei de doctorat poate fi extins cu funcționalitatea descrisă în [B70] prin adăugarea unui cititor de tip portal care operează pe frecvența de 850 MHZ și prin introducerea pe echipament a unor etichete RFID compatibile, care să conțină informații privind starea echipamentului și categoria din care face parte acesta. Un astfel de cititor ar trebui să includă și un fișier local, care să descrie piesele de echipament de protecție necesar pentru a permite accesul în zona protejată.

6.4. Concluzii parțiale

În acest capitol al tezei de doctorat a fost prezentat la nivel conceptual, sub forma unor specificații de funcționare și a unor algoritmi, un sistem de control al accesului în zone periculoase, bazat pe identificarea biometrică a utilizatorilor. Elementul de inovație adus de această propunere constă în faptul că verificarea **identității se efectuează local** pe baza comparației între o caracteristică biometrică scanată la momentul încercării de pătrundere în zona protejată și șablonul aceleiași caracteristici biometrice stocate pe un card RFID cu o structură de memorie, propusă de autorul tezei, special destinată acestui tip de sistem.

Prin verificarea la nivel local a identității utilizatorului se evită transferul prin rețea sau prin Internet a datelor biometrice ale acestuia, date deosebit de sensibile din punct de vedere al securității și protecției intimității utilizatorilor.

Elementul principal al sistemului propus este cardul RFID biometric, concept introdus de colectivul de cercetători din care autorul tezei face parte în brevetul de invenție [B23], RO 123364 B1 - "Card RFID biometric și metodă de stocare a informațiilor pe cardul RFID biometric". Conceptul descris în brevetul de invenție se referă la un card care poate fi utilizat pentru efectuarea de tranzacții bancare la bancomate. În cadrul acestui capitol al tezei de doctorat conceptul introdus în [B23] este extins pentru a putea fi utilizat în cadrul sistemelor de control al accesului în zonele protejate ale infrastructurilor industriale și ale infrastructurilor critice.

Se impune continuarea cercetărilor în domeniu pentru implementarea soluției propuse în cadrul acestui capitol al tezei de doctorat. Echipamentele necesare sunt disponibile pe piață, fiind dezvoltate la scară largă de marii producători, cu excepția cardului biometric, care este un element proprietar. Prin integrarea soluției și dezvoltarea componentelor software descrise în acest capitol se poate realiza un sistem robust și foarte sigur pentru controlul accesului în zone protejate.

Capitolul 7. Concluzii generale, contribuții, diseminarea rezultatelor și posibile direcții de continuare a cercetărilor

În prima parte a acestui ultim capitol al tezei de doctorat va fi realizată o sinteză a concluziilor parțiale prezentate la finalul fiecăruia dintre capitole.

A doua secțiune a capitolului este consacrată prezentării unei sinteze a contribuțiilor aduse în prezenta teză de doctorat.

O preocupare constantă a autorului pe parcursul studiilor doctorale a fost reprezentată de diseminarea rezultatelor cercetărilor. A treia parte a capitolului este consacrată evidențierii publicațiilor și brevetelor autorului.

În ultima parte a capitolului 7 sunt indicate câteva posibile direcții, pe care autorul le consideră relevante, de continuare a cercetărilor inițiate în prezenta teză de doctorat.

7.1. Concluzii generale

Asigurarea securității sistemelor de automatizare a devenit o prioritate în contextul în care toate echipamentele aferente acestor sisteme sunt conectate în rețele și pot constitui ținte ale unor atacuri care țin de terorismul informatic sau chiar de războiul electronic. Prin exploatarea unor vulnerabilități ale sistemelor de automatizare aflate în componența unor infrastructuri critice, un atacator (fie el terorist sau un stat inamic) poate produce pagube impresionante fără a-și mobiliza forțele armate. De exemplu, un sistem de automatizare compromis, aflat în componența sistemului de producere și/sau distribuție a energiei electrice poate paraliza întreaga economie a unei țări.

Securitatea sistemelor de automatizare vizează în primul rând aspectele clasice legate de autenticitatea, confidențialitatea, integritatea și nerepudierea datelor. Sunt de asemenea avute în vedere aspecte care privesc protecția împotriva virușilor, a wormilor, a accesului neautorizat și a oricărui alt tip de atac împotriva unor astfel de sisteme. O importanță aparte prezintă și controlul accesului fizic la sistemele de automatizare.

În cadrul primul capitol al tezei de doctorat au fost prezentate principalele vulnerabilități, posibile atacuri la care se adaugă și probleme de securitate care sunt asociate sistemelor de automatizare. Prin analiza rapoartelor de securitate puse la dispoziție de către companii din domeniu sau de către organizații guvernamentale și prin realizarea unor studii bibliografice s-a putut constata că principala problemă în securizarea sistemelor automate este reprezentată în acest moment de *lipsa autentificării sursei datelor transmise în cadrul rețelelor industriale*, în special a celor care provin de la senzori sau elemente de comandă (regulatoare, calculatoare etc.). De asemenea, a fost evidențiată existența unor amenințări care existau în domeniul calculatoarelor personale, dar care și-au schimbat țintele, așa cum este cazul virușilor informatici care vizează echipamente de automatizare, care sunt din ce în ce mai frecvent conectate în rețele locale sau la Internet.

Vulnerabilitățile identificate de către autorul tezei de doctorat și prezentate în primul capitol al acesteia, pot fi exploatate de la distanță, prin rețea, prin Internet, sau local, având acces fizic la resursele sistemului țintă. Cercetările prezentate în următoarele două capitole ale tezei s-au concentrat pe controlul accesului fizic la resursele sistemelor, pe securizarea transferurilor de date și pe protecția împotriva atacurilor informatice.

În scopul dezvoltării unor metode inovative, robuste și performante pentru controlul accesului s-a realizat un studiu bibliografic și o prezentare a principalelor caracteristici ale sistemelor de identificare biometrice a persoanelor, bazate pe analiza amprentei digitale. Unicitatea, gradul

mai redus de complexitate a senzorilor utilizați, performanțele algoritmilor existenți, costul redus al echipamentelor necesare și gradul mai mare de acceptare de către utilizatori au permis dezvoltarea unui număr mare de aplicații și utilizarea identificării și autentificării persoanelor pe baza analizei amprentei digitale pe scară largă. Tehnologia a ajuns la maturitate, și în consecință autorul consideră că aceasta poate fi utilizată cu succes pentru implementarea unor sisteme de autentificare a persoanelor care accesează elemente de comandă sau zone protejate aferente sistemelor automate, componente ale infrastructurilor critice. O altă tehnologie biometrică studiată, a fost cea bazată pe analiza imaginii irisului. Performanțele acestei metode sunt foarte mari, dar costurile echipamentelor, necesitatea unei anumite poziții pentru citirea (scanarea) imaginii și acceptarea mai redusă de către utilizatori nu recomandă utilizarea acestei tehnologii în sisteme care nu necesită cel mai înalt grad de securitate.

În ceea ce privește protecția împotriva atacurilor informatice, subiect tratat în detaliu în cel de-al treilea capitol al tezei de doctorat, cercetările s-au concentrat asupra maximizării disponibilității sistemelor, în special a celor care se află în componența infrastructurilor critice, prin limitarea atacurilor informatice de tip Denial of Service (DoS și DDoS). Autorul tezei a identificat două tipuri principale de soluții de securitate robuste, și anume: *soluții de tip firewall și, respectiv, soluții de tip capcană – honeypot*.

Dispozitivele de tip firewall sunt recomandate pentru a delimita rețeaua industrială de rețeaua de calculatoare a companiei și pentru a crea DMZ-uri (zone demilitarizate), în care sunt plasate serverele care oferă servicii publice. În acest mod, chiar și în cazul compromiterii unuia dintre serverele expuse, este imposibilă accesarea entităților din rețeaua locală.

Sistemele de tip honeypot au o dublă utilizare pentru protecția sistemelor de automatizare, putând fi privite atât ca mijloace de culegere a informațiilor referitoare la sursele și mecanismele de desfășurare a atacurilor informatice, cât și ca dispozitive de tip capcană, care imită funcționarea unui sistem real, de interes pentru atacatori.

În cadrul cercetărilor desfășurate au fost utilizate sisteme de tip honeypot pentru a colecta date, care au certificat interesul crescut al atacatorilor pentru sistemele de automatizare conectate la Internet și pentru protocoalele de comunicație de tip industrial. Acest interes crescut, justifică necesitatea securizării acestor sisteme.

Analizând funcționarea sistemelor de tip honeypot autorul tezei consideră că acestea pot reprezenta nu doar un simplu mijloc de culegere a informațiilor, ci și o metodă foarte eficientă de protecție împotriva atacurilor. Prin crearea unui nor de „*ceață informatică*”, adică prin crearea unui număr suficient de mare de honeypoturi în jurul sistemului protejat, se poate reduce semnificativ probabilitatea ca atacatorul să poată identifica sistemul real, crescând timpul și efortul necesar desfășurării atacului.

În cel de-al patrulea capitol au fost propuse trei metode destinate după cum urmează: *evaluării profilului unui anume tip de atacator, estimării probabilității de apariție și respectiv de reușită a unui atac informatic*, lansat de către un atacator al cărui profil este cunoscut, asupra unui sistem țintă. Metodele propuse utilizează mecanismele logicii fuzzy și seturi de reguli elaborate de către autorul tezei pe baza experienței dobândite în decursul stagiului de cercetare și a colaborării cu companii din domeniul securității informatice.

Pentru estimarea probabilității de apariție a unui atac informatic a fost dezvoltat și implementat în mediul MATLAB un sistem fuzzy bazat pe reguli, a cărui funcționare analizează două intrări și anume: nivelul de vulnerabilități și gradul de interes pe care îl prezintă sistemul pentru atacatori.

Gradul de interes este un concept introdus de autorul tezei, prin care se cuantifică într-o variabilă lexicală (cu valorile *mic, mediu, mare*) numărul de încercări de atac asupra unui honeypot care este similar sistemului protejat sau care simulează serviciile oferite de acesta.

Pentru estimarea probabilității de succes a unui atac a fost implementat un sistem de inferență bazat pe logică fuzzy, axat pe utilizarea a trei intrări și anume: *scorul profilului de atacator, nivelul de vulnerabilități existente și nivelul măsurilor de protecție de care beneficiază sistemul țintă*. Scorul profilului de atacator este de asemenea un concept introdus de autor pentru a permite cuantificarea "abilităților" unui atacator prin evaluarea nivelului de cunoștințe, a resurselor disponibile și a motivației acestuia. Nivelul de vulnerabilități al unui sistem poate fi evaluat cu ajutorul unor aplicații specializate, denumite scannere de vulnerabilități, al căror mod de funcționare a fost prezentat în capitolul 4 al tezei de doctorat.

Din analiza rezultatelor obținute utilizând sistemele descrise anterior s-a putut constata că probabilitatea de apariție a atacurilor informatice este afectată semnificativ de nivelul de vulnerabilități al sistemului și mai puțin de gradul de interes pe care acesta îl reprezintă pentru atacatori. În ceea ce privește rata de reușită a unui atac, aceasta este dependentă în mod evident de nivelul de vulnerabilitate al sistemului țintă și de abilitățile atacatorului. Autorul tezei consideră că implementarea unor măsuri de protecție adecvate determină scăderea probabilității de reușită a unui atac la un nivel acceptabil.

În cel de-al cincilea capitol al tezei de doctorat este propusă o metodă robustă pentru autentificarea senzorilor conectați prin protocolul Modbus/TCP. Autorul tezei de doctorat a realizat un studiu bibliografic privind specificațiile și modul de funcționare ale protocolului Modbus în general și ale protocolului Modbus/TCP în special. Pe baza acestui studiu s-au putut evidenția la nivel de laborator, vulnerabilitățile protocolului menționat acesta fiind susceptibil la atacuri de tip Man-in-the-middle (MITM).

Autorul tezei a propus un mecanism de autentificare a senzorilor conectați prin protocolul Modbus/TCP, mecanism care constă în adăugarea unei semnături (de tip *hash)* a senzorului în cadrul câmpului Options din pachetele TCP/IP care sunt transferate în rețea. Metoda propusă a fost implementată și validată sub forma unui demonstrator de laborator. Demonstratorul a confirmat premisele corecte ale metodei și faptul că utilizarea acesteia nu afectează performanțele rețelei, putând funcționa cu toate echipamentele deja conectate în rețea.

În cel de-al șaselea capitol al tezei de doctorat a fost prezentat la nivel conceptual, sub forma unor specificații de funcționare și a unor algoritmi, un sistem de control al accesului în zone periculoase, bazat pe identificarea biometrică a utilizatorilor. Elementul de inovație adus de această propunere constă în faptul că verificarea identității se efectuează local pe baza comparației între o caracteristică biometrică scanată la momentul încercării de pătrundere în zona protejată și șablonul aceleiași caracteristici biometrice stocate pe un card RFID cu o structură de memorie, propusă de autorul tezei, special destinată acestui tip de sistem. Conceptul de card RFID biometric descris în teza de doctorat reprezintă extinderea structurii propuse de colectivul de cercetători din care autorul tezei face parte în brevetul de invenție cu titlul „*Card RFID biometric și metodă de stocare a informațiilor pe cardul RFID biometric*". Brevetul de invenție se referă la securizarea tranzacțiilor bancare la ATM-uri care integrează cititoare de amprente și a fost extins în cadrul prezentei teze pentru a putea fi utilizat în cadrul sistemelor de control al accesului în zonele protejate ale infrastructurilor industriale și ale infrastructurilor critice.

7.2. Contribuții originale

În teza de doctorat, cu precădere în ultimele trei capitole ale acesteia au fost detaliate contribuțiile autorului în ceea ce privește problematica abordată. În cele ce urmează este prezentată o sinteză a contribuțiilor, insistând asupra celor cu o semnificație aparte.

1. A fost realizat un studiu bibliografic de o complexitate ridicată, care a permis autorului conturarea unei imagini referitoare la stadiul cercetărilor și al realizărilor din domeniul securității sistemelor automate.
2. Au fost instalate, configurate și utilizate dispozitive de tip honeypot (ConPot și T-Pot) pentru confirmarea interesului atacatorilor față de sistemele industriale conectate la Internet și colectarea de date privind dinamica tentativelor de acces neautorizat sau atac informatic.
3. Din perspectiva procesării informației, sistemele automate au fost tratate ca sisteme informatice.
4. Au fost introduse conceptele: *profil de atacator* și *scor asociat profilului de atacator*, acesta din urmă permițând cuantificarea abilităților unui atacator prin evaluarea nivelului de cunoștințe, a nivelului de resurse disponibile și a motivației acestuia.
5. A fost propus un set de reguli pentru definirea scorului asociat profilului de atacator.
6. A fost introdus conceptul *grad de interes*, care cuantifică printr-o variabilă de tip lexical, numărul de încercări de acces neautorizat (conectare sau atac) asupra unui honeypot similar sistemului protejat.
7. Au fost identificate și formulate riscurile aferente activităților de testare a securității unui sistem prin activități de pen-testing.
8. A fost dezvoltat și testat un sistem bazat pe logică fuzzy pentru evaluarea scorului asociat profilului de atacator pe baza atributelor atacatorului: *cunoștințe, resurse tehnice disponibile și motivație.*
9. A fost dezvoltat și testat un sistem bazat pe logică fuzzy destinat estimării probabilității de apariție a unui atac informatic asupra unui sistem automat, în funcție de gradul de interes pe care îl prezintă sistemul pentru potențialii atacatori și de nivelul de vulnerabilități.
10. A fost dezvoltat și testat un sistem bazat pe logică fuzzy pentru estimarea probabilității de reușită a unui atac informatic asupra unui sistem automat, în funcție de scorul profilului de atacator, de nivelul de vulnerabilități și de nivelul contramăsurilor existente.
11. A fost demonstrată în laborator posibilitatea de interceptare a datelor transmise prin protocolul Modbus/TCP, în vederea derulării unui atac de tip Man-In-The-Middle sau spoffing.
12. A fost dezvoltat și testat un mecanism destinat autentificării senzorilor conectați în rețele Modbus/TCP.
13. A fost propus la nivel conceptual un sistem de control al accesului în zone periculoase din instalațiile industriale sau la consolele de operare bazat pe analiza amprentei digitale a persoanei și comparația acesteia cu șablonul stocat pe un card RFID.
14. A fost propusă o structură specială de memorie pentru cardul RFID care să stocheze trei șabloane ale amprentelor digitale ale utilizatorului alături de informații privind drepturile sale de acces.

7.3. Diseminarea rezultatelor cercetării

Rezultatele obținute în cursul cercetărilor desfășurate de către autor s-au concretizat în publicații științifice recunoscute după cum urmează: o carte la editura Springer Verlag în calitate de

editor, coautor la trei capitole incluse în această carte, 16 articole dintre care 8 articole indexate Thomson-Reuters Web of Science (ISI) , 6 articole publicate în baza de date IEEE Xplore și 2 articole în baza de date internațională ProQuest Central, 2 brevete de invenție acordate și 2 cereri de brevet de invenție în evaluare la Oficiul de Stat pentru Invenții și Mărci. În continuare este prezentată o listă completă a acestor publicații, în ordine cronologică, organizată pe categorii.

A. Cărți și capitole de cărți publicate în edituri internaționale de prestigiu

1. **Pricop E.**, Stamatescu G. (editori), *Recent Advances in Systems Safety and Security*, Springer International Publishing AG, Cham, Switzerland, 2016, ISBN: 978-3-319-32523-1;
2. Fattahi, J., Mejri M., **Pricop E.**, - *The Theory of Witness-Functions*, capitol publicat în Recent Advances in Systems Safety and Security, Springer International Publishing AG, Cham, Switzerland, 2016, ISBN: 978-3-319-32523-1, pag. 1-19;
3. Rădulescu G., **Pricop E.**, Nicolae M., Roșca C. – *Using Modelling and Dynamic Simulation Techniques for Systems' Safety and Security*, capitol publicat în Recent Advances in Systems Safety and Security, Springer International Publishing AG, Cham, Switzerland, 2016, ISBN: 978-3-319-32523-1, pag. 57-77;
4. **Pricop E.**, Mihalache S.F., Fattahi J. – *Innovative Fuzzy Approach on Analyzing Industrial Control Systems Security*, capitol publicat în Recent Advances in Systems Safety and Security, Springer International Publishing AG, Cham, Switzerland, 2016, ISBN: 978-3-319-32523-1, pag. 223-239;

B. Articole indexate Thomson-Reuters - Web of Science (ISI Papers & ISI Proceedings)

1. Paraschiv N., **Pricop E.** – *Adequacy testing of some algorithms for feedforward control of a propane propylene distillation process*, Revista de Chimie, vol. 67, nr. 7, iulie 2016, pag. 1363-1369, ISSN: 0034-7752 (**Articol ISI, IF: 0,973**);
2. Fattahi J., Mejri M., **Pricop E.**– *Tracking Security Flaws in Cryptographic Protocols using Witness-Functions*, IEEE International Conference on Systems, Man & Cybernetics (SMC) 2015 Proceedings, pp. 1189-1196, doi: 10.1109/SMC.2015.213 (**ISI Proceeding**), Hong Kong, 2015;
3. **Pricop E.**, Zamfir F., Paraschiv N. – *Feedback control system based on a remote operated PID controller implemented using mbed NXP LPC1768 development board*, Journal of Physics: Conference Series, Vol. 659, Article number: 012028, doi: 10.1088/1742-6596/659/1/012028, IOP Publishing, 2015 (**ISI Proceeding**);
4. **Pricop E.**, Mihalache S.F. – *Fuzzy approach on modelling cyber attacks patterns on data transfer in industrial control systems*, 3rd International Workshop on Systems Safety & Security – IWSSS 2015 - Proceedings of the 7th International Conference on Electronics, Computers & Artificial Intelligence – ECAI 2015, vol. 7, SSS-23 - SSS-28, nr. 2/2015 – ISSN: 1843-2115; ISBN: 978-1-4673-6646-5 (**ISI Proceeding**)
5. **Pricop E.**, Mihalache S.F. – *Assessing the security risks of a wireless sensor network from a gas compressor station*, 2nd International Workshop on Systems Safety & Security – IWSSS 2014, , București, România - Proceedings of the 6th International Conference on Electronics, Computers & Artificial Intelligence – ECAI 2014, vol. 5, pag.45-50, ISBN: 978-1-4799-5478-0 (**ISI Proceeding**)

6. Ionescu O., **Pricop E.** – *On the design of a system for airport protection against terrorist attacks using MANPADS*, International Conference on Systems, Man and Cybernetics - SMC 2013 Proceedings, , pag. 4778-4782, ISBN 978-0-7695-5154-8, Manchester, UK, 2013 (**ISI Proceeding**)
7. **Pricop E.** – *On the design of an innovative solution for increasing hazardous materials transportation safety*, International Workshop on Systems Safety & Security for Automotive, Passengers & Goods Protection – IWSSS 2013 - Proceedings of the 17th International Conference System Theory, Control and Computing (ICSTCC 2013), 2013, Sinaia, Romania, pag. 624-629, ISBN: 978-1-4799-2228-4 (**ISI Proceeding**)
8. Ionescu O., **Pricop E.**, Paraschiv N. – *The management of health & safety issues related to the wearing of protective clothing by using RFID technology* The 2nd International Conference on Economic, Education and Management – ICEEM 2012 Proceedings, Shanghai, China, Volume 1, pag. 495, ISBN 978-988-19750-3-4 (**ISI Proceeding**)

C. Articole publicate în IEEE Xplore

1. **Pricop E.**, Fattahi J., Paraschiv N., Zamfir F., Ghayoula E. - *Method for authentication of sensors connected on Modbus TCP*, Proceedings of the 2017 4th International on Control, Decision and Information Technologies (CoDIT'17), Barcelona, Spania, 2017 (Acceptat pentru publicare pe **IEEE Xplore)**
2. Zamfir F., Paraschiv N., **Pricop E.** - *Performance analysis in WiMAX networks using Random Linear Network Coding*, Proceedings of the 2017 4th International on Control, Decision and Information Technologies (CoDIT'17), Barcelona, Spania, 2017 (Acceptat pentru publicare pe **IEEE Xplore)**
3. **Pricop E.**, Mihalache S.F., Paraschiv N., Fattahi J., Zamfir F. – *Considerations regarding security issues impact on systems availability*, 4th International Workshop on Systems Safety & Security - Proceedings of the 7th International Conference on Electronics, Computers & Artificial Intelligence – ECAI 2016, Vol. 8, No. 4/2016, ISSN: 1843-2115, doi: 10.1109/ECAI.2016.7861110, 2016, Ploiești, România (**IEEE Xplore, Scopus**)
4. Fattahi J., Mejri M., **Pricop E.** - *Authentication by Witness Functions* 2016 IEEE Trustcom/BigDataSE/ISPA Conference Proceedings, pp. 1990-1997, doi: 10.1109/ TrustCom.2016.0304, Tianjin, China, 2016 (**IEEE Xplore, Scopus**)
5. Fattahi J., Mejri M., Ghayoula R., **Pricop E.** - *Formal reasoning on authentication in security protocols*, IEEE International Conference on Systems, Man, and Cybernetics (SMC) 2016 Proceedings, pp. 282-289, doi: 10.1109/SMC.2016.7844255, Budapesta, Ungaria, 2016 (**IEEE Xplore**)
6. Ghayoula E., Fattahi J., Ghayoula R., **Pricop E.**, Stamatescu G., Chouinard J.-Y., Bouallegue A. – *Sidelobe Level Reduction in Linear Array Pattern Synthesis Using Taylor-MUSIC Algorithm for Reliable IEEE 802.11 MIMO Applications*, IEEE International Conference on Systems, Man, and Cybernetics (SMC) 2016 Proceedings, pp. 4700-4705, doi: 10.1109/SMC.2016.7844973, Budapesta, Ungaria, 2016 (**IEEE Xplore**)

D. Articole indexate în baze de date internaționale

1. **Pricop E.** – *On the design of a monitoring and alarming system for hazardous goods transportation by ships***,** Scientific Bulletin "Mircea Cel Bătrân" Naval Academy, vol. 18, nr. 1, pag. 235-239, Constanța, România 2015 (**ProQuest Central**);

2. **Pricop E.** – *Security of industrial control systems – an emerging issue in Romania national defense*, Scientific Bulletin "Mircea Cel Bătrân" Naval Academy, vol. 18, nr. 2, pag. 142-147, Constanța, România 2015 (**ProQuest Central**);

E. Brevete de invenție acordate și cereri de brevet de invenție

1. *Card RFID biometric și metodă de stocare a informațiilor pe cardul RFID biometric,*
   Brevet de invenție RO 123364 B1 din 28.10.2011 - acordat de Oficiul de Stat pentru Invenții și Mărci – OSIM, România.
   Inventatori: Melinte Toader, **Pricop Emil**, Lorentz Adrian, Andron Liviu
2. *Sistem de securitate a aeroporturilor civile împotriva atacurilor teroriste cu rachete portabile sol-aer*
   Brevet de invenție RO 129740 B1 din 30.06.2016 acordat de Oficiul de Stat pentru Invenții și Mărci – OSIM, România.
   Inventatori: Ionescu Octavian Narcis, **Pricop Emil**, Ionescu Gabriela Cristina
3. *Sistem automat de monitorizare a portului echipamentului de protecție obligatoriu în zonele cu potențial ridicat de pericol* – în procedură de evaluare
   Cerere de brevet de invenție nr. 129906 A0, publicată în Buletinul Oficial de Proprietate Intelectuală (BOPI) al Oficiului de Stat pentru Invenții și Mărci (OSIM), nr. 11/2014
   Inventatori: Ionescu Octavian Narcis, Crăciun Daniel, **Pricop Emil**
4. *Sistem bazat pe senzori conectați wireless pentru monitorizarea tentativelor de distrugere a infrastructurii strategice de transport a energiei electrice* – în procedură de evaluare
   Cerere de brevet de invenție nr. 129850 A0, publicată în Buletinul Oficial de Proprietate Intelectuală (BOPI) al Oficiului de Stat pentru Invenții și Mărci (OSIM), nr. 10/2014.
   Inventatori: Ionescu Octavian Narcis, Ionescu Gabriela Cristina, **Pricop Emil**

Pe parcursul derulării cercetărilor desfășurate în cadrul stagiului doctoral s-a impus necesitatea unui schimb de informații între specialiștii ale căror preocupări sunt orientate în direcția securității sistemelor tehnice, inclusiv a celor automate.

În acest context, începând cu anul 2013 autorul tezei de doctorat a organizat „*International Workshop on Systems Safety & Security – IWSSS*", manifestare științifică anuală care a beneficiat de prezența unor cercetători de prestigiu atât din România cât și din străinătate. Lucrările prezentate la fiecare ediție din perioada 2013-2016 au fost publicate în baza de date IEEE Xplore și indexate în prestigioasa bază de date Thomson Reuters – Web of Science (ISI).

7.4. Posibile direcții de continuare a cercetărilor

Cercetările desfășurate în cadrul stagiului doctoral reprezintă începutul unei activități cu un grad crescut de complexitate, într-un domeniu de nișă – securitatea sistemelor tehnice în general și cu o concentrare specială asupra celor integrate în infrastructurile critice.

Contextul internațional actual, caracterizat prin creșterea numărului de atacuri ce vizează infrastructurile critice și sistemele tehnice, prin dezvoltarea de viruși care țintesc echipamente industriale (PLC-uri, sisteme SCADA etc.), indică faptul că securitatea sistemelor tehnice trebuie să devină o prioritate a cercetătorilor și a factorilor de decizie inclusiv a celor din domeniul apărării. Trebuie menționat faptul că acest domeniu este definit ca fiind prioritar în Statele Unite ale Americii încă din 2013, când administrația Obama a formulat reglementări în domeniul securității cibernetice a infrastructurilor critice. De asemenea Organizația Tratatului Atlanticului de Nord – NATO a înființat în Tallin un centru de cercetare de excelență – CCD COE - Cooperative Cyber Defence Centre of Excellence, cu scopul de a studia și dezvolta metode de protecție împotriva atacurilor informatice.

În continuare vor fi prezentate succint posibile direcții de cercetare și dezvoltări, care pot fi avute în vedere, pentru creșterea securității sistemelor tehnice în care sunt evident incluse și cele automate.

- Extinderea și implementarea metodei propuse pentru autentificarea senzorilor conectați în rețele Modbus/TCP. În cadrul demonstratorului prezentat în teza de doctorat pentru validarea metodei propuse s-a utilizat un text clar pentru semnătura senzorului, dar într-o implementare industrială se impune utilizarea unei semnături generate sub forma unui hash de tip TOTP – Time One Time Pad / Password, care permite pe lângă verificarea identității și validarea momentului de timp la care informația a fost generată și transmisă în rețea.
- Dezvoltarea unor alte metode și tehnici pentru autentificarea sursei care generează date în cadrul rețelelor industriale, pentru cele mai utilizate protocoale, cum ar fi Profibus, Fieldbus, Profinet etc, după modelul propus în cadrul tezei pentru protocolul Modbus/TCP.
- Dezvoltarea unor sisteme honeypot senzitive la context, cu grad înalt de interacțiune, care să utilizeze tehnici specifice inteligenței artificiale (machine learning, artificial reasoning). Astfel de honeypot-uri ar trebui să interacționeze cu atacatorul, să fie capabile să se reconfigureze în timp real, în funcție de acțiunile acestuia și să răspundă unui număr foarte mare de comenzi, pentru a reproduce cât mai fidel un sistem real, determinând imposibilitatea atacatorului să decidă dacă atacă un sistem real sau a fost prins într-o capcană.
- Implementarea la nivel demonstrator și apoi la nivel industrial a unui sistem de control al accesului bazat pe conceptul introdus în capitolul 6 al tezei de doctorat. Concret direcția presupune dezvoltarea unui sistem multi-factor de verificare a identității persoanelor utilizând analiza amprentei digitale și compararea șablonului obținut cu cel stocat pe cardul RFID biometric.
- Perfecționarea metodelor automate (respectiv a scannerelor de vulnerabilități) prin dezvoltarea de facilități care să permită estimarea impactului unor vulnerabilități care nu sunt incluse în bazele de date existente.
- Dezvoltarea unor metode pentru evaluarea impactului securității (a vulnerabilităților existente și posibilelor atacuri) asupra disponibilității sistemului analizat.
- Propunerea unei noi metode de calcul (ajustare) a coeficientului de disponibilitate K_D al unui sistem tehnic, care pe lângă fiabilitate și mentenabilitate (așa cum este în prezent) să țină cont și de nivelul de securitate al sistemului.
- Extinderea metodelor propuse în cadrul tezei de doctorat pentru estimarea probabilității de apariție și de reușită a unui atac informatic asupra unui sistem dat, astfel încât acestea să fie senzitive la context și să detecteze în timp real schimbările apărute la nivelul rețelelor supervizate.

Bibliografie

B1. Paraschiv, N. *Achiziția și prelucrarea datelor*, Editura Universității Petrol-Gaze din Ploiești, Ploiești, 2013

B2. Hessami, A.G., *A Systems Framework for Safety & Security, The Holistic Paradigm, Systems Engineering* - The Journal of the International Council on Systems Engineering, Volume 7 Number 2, pp 99-112, 2004

B3. Hessami, A.G., *Cybernetic safety & security, a new paradigm*, 2008. CIS 2008 - 7th IEEE International Conference on Cybernetic Intelligent Systems, pp.1,10, 9-10 Sept. 2008

B4. Knapp, E. *Industrial network security: securing critical infrastructure networks for Smart Grid, SCADA, and other industrial control systems*, Syngress, USA, 2011

B5. ***, *Cyber Security Status Watch - 2013 Q2*, NATO CCDCOE, Tallinn, Estonia, 2013

B6. ***, *Cyber Security Status Watch - 2012* , NATO CCDCOE, Tallinn, Estonia, 2013

B7. Pricop, E., Mihalache, S.F., Fattahi, J., *Innovative Fuzzy Approach on Analyzing Industrial Control Systems Security*, capitol publicat în Recent Advances in Systems Safety and Security, Springer International Publishing AG, Cham, Switzerland, 2016, ISBN: 978-3-319-32523-1;

B8. Pricop E., Mihalache S.F., *Fuzzy approach on modelling cyber attacks patterns on data transfer in industrial control systems*, 3rd International Workshop on Systems Safety & Security – IWSSS 2015 - Proceedings of the 7th International Conference on Electronics, Computers & Artificial Intelligence – ECAI 2015, vol. 7, SSS-23 - SSS-28, nr. 2/2015 – ISSN: 1843-2115; ISBN: 978-1-4673-6646-5

B9. Pricop E. , Mihalache S.F., *Assessing the security risks of a wireless sensor network from a gas compressor station*, 2nd International Workshop on Systems Safety & Security – IWSSS 2014, București, România - Proceedings of the 6th International Conference on Electronics, Computers & Artificial Intelligence, ECAI 2014, vol. 5, pag.45-50, ISBN:978-1-47995478-0

B10. Pricop E., *Security of industrial control systems – an emerging issue in Romania national defense*, Scientific Bulletin "Mircea Cel Bătrân" Naval Academy, vol. 18, nr. 2, pag. 142-147, Constanța, România 2015

B11. Alexandrescu, G., Văduva, Gh. – *Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție*, Editura Universității Naționale de Apărare „Carol I", București, 2006

B12. Mackay, S., Wrigth, E., Reynders, D., Park J. - *Practical Industrial Data Networks - Design, Installation and Troubleshooting*, Ed. Newnes, USA, 2004

B13. Kaminsky M.A., *Manufacturing Automation Protocol (MAP).* in: Thoma M., Schmidt G. (eds) Fortschritte in der Meß- und Automatisierungstechnik durch Informationstechnik. Fachberichte Messen · Steuern · Regeln, vol 14. Springer, Berlin, Heidelberg, 1986

B14. Guran, M., Filip, F.G., *Sisteme ierarhizate în timp real, cu prelucrarea distribuită a datelor*, București, Editura Tehnica, 1986

B15. Paraschiv, N., Popescu, M., *Sisteme distribuite de supervizare și control*, Editura Universității Petrol-Gaze din Ploiești, 2014, ISBN: 978-973-719-557-9

B16. Tanenbaum, A., *Reţele de calculatoare*, Editia a 4-a, Ed. Byblos, Bucureşti, 2007

B17. Parker, T., Sportack, M., *TCP/IP*, Ed. Teora, București, 2002

B18. Zouheir, T., Kadhim, H., et. al., *Network attacks and defenses : a hands-on approach*, CRC Press, USA, 2013

B19. Electronic Industries Association, *Electrical Characteristics of Generators and Receivers for Use in Balanced Multipoint Systems. EIA Standard RS-485,* 1983

B20. Maltoni, D., Maio, D., Jain, A., Prabhakar, S. - *Handbook of Fingerprint Recognition*, Springer-Verlag London, ISBN: 978-1-84882-253-5, 2009
B21. Pricop, E., *Biometric identification of persons – A solution for time & attendance problems*, Sesiunea de comunicări ştiinţifice IMT 2008, Universitatea din Oradea, Băile Felix, mai 2008
B22. Pricop, E., *Consideraţii privind utilizarea cardurilor RFID MIFARE pentru stocarea amprentelor digitale*, Sesiunea de comunicări științifice Zilele Tehnice Studențești – Volum de lucrări, pag. 185, ISSN 1843-1917, Timişoara, 2008
B23. Melinte T., Pricop E., Lorentz A., Andron L., *Brevet de invenție Nr. RO 123364 B1 / 28.10.2011 - Card RFID biometric și metodă de stocare a informațiilor pe cardul RFID biometric*, 2011
B24. Andron, L., Melinte, T., Pricop, E., *Prezentarea unui algoritm de recunoaştere automată a amprentei digitale în sistemele de identificare şi autentificare a persoanelor pentru autorizarea accesului în reţele informatice şi obiective de importanţă majoră*, Sesiunea de comunicări Ştiinţifice CERC 2007, Academia Tehnică Militară, Bucureşti, mai 2007
B25. Andron, L., Lorentz, A., Pricop, E., *Evaluarea performanţelor algoritmilor de recunoaştere a amprentei digitale în sistemele de identificare şi autentificare a persoanelor pentru autorizarea accesului în reţele informatice şi obiectivele de importanţă majoră*, Sesiunea de comunicări ştiinţifice CERC 2007, Academia Tehnică Militară, mai 2007
B26. Mansfield, A. J., Wayman, J.L., *Best practices in testing and reporting performance of biometric device*, Report for Biometric Working Group, August 2002
B27. ***, Contact de cercetare - *Echipamente si sisteme biometrice de identificare si autentificare a persoanelor pentru autorizarea accesului in retelele informatice si obiectivele de importanta majora*, Contract nr. 13/2006 Acronim: AMPRENTA, http://www.mta.ro/celem/p2006_01a.php
B28. Paul de Hert, *Biometrics: Legal issues and implications. Background paper for the Institute of Prospective Technological Studies*, Sevilla, European Commission, 2005
B29. Reid, P., *Biometrics for Network Security*, Prentice Hall PTR, USA, 2003
B30. Maltoni D., *A Tutorial on Fingerprint Recognition in Advanced Studies in Biometrics*, Summer School on Biometrics, Alghero, Italy, June 2-6, 2003. Revised Selected Lectures and Papers, Springer-Verlag Berlin Heidelberg, ISBN: 978-3-540-26204-6, 2005
B31. Vertan C., *Prelucrarea și analiza imaginilor*, Editura Printech Bucuresti, ISBN 973-9475-71-X, 1999
B32. Galton F.**,** *Finger prints*, London, Ed. McMillan, 1892
B33. Jain, L.C., Halici, U., Hayashi, I., Lee, S.B., Tsutsui, S., *Intelligent biometric techniques in fingerprint and face recognition*, CRC Press, USA, 1999
B34. Garaiman D.D., *Content based search system in a multimedia database with medical images II. The methods of establishing image similitudes*. Craiova Medicala, Vol. 10, Nr. 4, 2008
B35. Wildes R., *Iris recognition: An emerging Biometric Technology*, Proceedings of the IEEE, vol. 9, nr. 85, p. 1348 – 1363, September 1997
B36. Daugman, J., *How iris recognition works*, Proceedings of 2002 International Conference on Image Processing, Vol.1, 2002
B37. Noh, S. et al., A *New Iris Recognition Method Using Independent Component Analysis*. IEICE - Transactions on Information and Systems, vol. E88-D, vol. 11, ISSN 2573-2581, 2005
B38. Li, M., Tieniu, T., Yunhong, W., Dexin Z., *Efficient iris recognition by characterizing key local variations*, IEEE Transactions on Image Processing, vol. 13, no. 6, pp. 739-750, 2004

B39. Finkenzeller K., *RFID Handbook – Fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*, 3rd ed. John Wiley & Sons, Ltd., United Kingdon, ISBN 978-0-470-69506-7, 2010

B40. *** US Department of Homeland Security - *Industrial Control Systems Cyber Emergency Response Team*, NCCIC/ICS-CERT Year in Review Report – FY 2015

B41. *** US Department of Homeland Security- *Industrial Control Systems Cyber Emergency Response Team*, ICS-CERT Year in Review – 2016

B42. Andreeva, O., Gordeychik S., et. al. – *Industrial Control Systems Vulnerabilities Statistics*, Kaspersky Ltd., 2016

B43. Vacca J., Ellis S., *Firewalls: Jumpstart for Network and Systems Administrators*, Elsevier Digital Press, ISBN: 978-1-55558-297-5, 2005

B44. Rughiniş, R., Deaconescu, R., Ciorba, A., Doinea, B., *Reţele locale*, Bucureşti, Editura Printech, 2009

B45. Rughiniş, R., Carabas, M., Deaconescu, R., Costea. S., *Configurarea și administrarea rețelelor locale*, Printech, București, 2013

B46. Paraschiv N., Pricop E., *Industrial process control network security*, Petroleum-Gas University of Ploiesti Scientific Bulletin – Technical Series, Volume LX, No. 3B/2008, ISSN 1224-8495

B47. Sokol, P., Host J., *Evolution of Legal of Honeynets*, capitol publicat în Recent Advances in Systems Safety and Security, Springer International Publishing AG, Cham, Switzerland, 2016, ISBN: 978-3-319-32523-1,

B48. Pouget, F., Dacier, M., Debar, H., *White paper: honeypot, honeynet, honeytoken: terminological issues.* Rapp. Tech. EURECOM, p.1–26, 2003

B49. Joshi, R.C., Sardana, A., *Honeypots: A New Paradigm to Information Security*, Science Publishers, USA, 2011

B50. Lopez, M.H., Resendez Lerma, C.F., *Honeypots: Basic Concepts, Classification and Educational Use as Resources in Information Security Education and Courses*, Proceedings of the Informing Science & IT Education Conference InSITE, 2008

B51. Pricop E., Mihalache S.F., Paraschiv N., Fattahi J., Zamfir F., *Considerations regarding security issues impact on systems availability*, 4th International Workshop on Systems Safety & Security - Proceedings of the 7th International Conference on Electronics, Computers & Artificial Intelligence – ECAI 2016, Vol. 8, No. 4/2016, ISSN: 1843-2115, 2016, Ploiești, România

B52. ***, The Government of the Hong Kong SAR, *An overview of vulnerability scanners*, Februarie 2008

B53. ***, US Department of Homeland Security – *ICS-CERT Monitor Reports* – September 2014 – February 2015

B54. Stouffer, K., Pillitteri, V., et. al., *NIST Special Publication 800-82 Rev.2 – Guide to Industrial Control Systems (ICS) Security*, Mai 2015

B55. Shostack, A., *Threat Modeling. Designing for Security*, John Wiley & Sons, Inc., Indiana, ISBN: 978-1-118-80999-0, 2014

B56. Preitl, St., Precup, R.-E., *Introducere in conducerea fuzzy a proceselor*, Editura Tehnica, București, 1997

B57. Precup, R.-E., Preitl, St., *Fuzzy Controllers (in English)*, Editura Orizonturi Universitare Publishers, Timișoara, 1999.

B58. Jager, R., *Fuzzy Logic in Control - Ph.D. thesis* Delft University of Technology, Department of Electrical Engineering, Control Laboratory, Delft, The Netherlands, ISBN 90-9008318-9, 1995
B59. Mamdani, E.H., Assilian S., *An experiment in linguistic synthesis with a fuzzy logic controller*, International Journal of Man-Machine Studies, Vol. 7, No. 1, pp. 1-13, 1975.
B60. Sugeno, M., *Industrial applications of fuzzy control*, Elsevier Science Pub. Co., 1985
B61. Sivanandam, S.N., Sumathi, S., Deepa, S.N- *Introduction to Fuzzy Logic using MATLAB*, Springer-Verlag Berlin Heidlberg, ISBN 978-3-540-35780-3, 2007
B62. ***, Standardul TIA/EIA-232E.
B63. ***, Standardul TIA/EIA-422-B
B64. ***, Modicon Inc., Modbus Application Protocol Specification
B65. ***, Acromag, Inc. - *Technical Reference – Introduction to Modbus TCP/IP*, Documentatie disponibila on-line la adresa: http://www.prosoft-technology.com/kb/assets/intro_modbustcp.pdf.
B66. ***, RFC1321 – The MD5 Message-Digest Algorithm
B67. ***, RFC4226 – HOTP: An HMAC-Based One-Time Password Algorithm
B68. ***, RFC6238 – TOTP: Time-Based One-Time Password Algorithm
B69. Melinte, T., Pricop E. – *Biometric RFID Card – A solution for securing industrial control systems*, Petroleum-Gas University of Ploiesti Scientific Bulletin – Technical Series, Volume LX, No. 3B/2008, ISSN 1224-8495
B70. Ionescu, O., Crăciun, D., Pricop, E., *Cerere de brevet de invenție nr. 129906 A0, Sistem automat de monitorizare a portului echipamentului de protecție obligatoriu în zonele cu potențial ridicat de pericol,* publicată în Buletinul Oficial de Proprietate Intelectuală (BOPI) al Oficiului de Stat pentru Invenții și Mărci (OSIM), nr. 11/2014
B71. Ionescu, O., Pricop, E., Paraschiv, N., *The management of health & safety issues related to the wearing of protective clothing by using RFID technology*, The 2nd International Conference on Economic, Education and Management – ICEEM 2012 Proceedings, Shanghai, China, Volume 1, pag. 495, ISBN 978-988-19750-3-4

Webografie

W1. Pagina web a Federal Bureau of Investigation, www.fbi.gov

W2. Pagina web a NATO CCDCOE – Cooperative Cyber Defence Centre of Excellence Tallin, Estonia http://ccdcoe.org

W3. U.S. Department of Homeland Security, Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection, https://www.dhs.gov/homeland-security-presidential-directive-7

W4. European Commision – Site-ul web specific pentru Infrastructurile Critice - https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

W5. ISO – International Standard Organization – www.iso.org

W6. ITU-T – International Telecommunications Union- www.itu.int

W7. Site-ul web și documentația programului Wireshark - https://www.wireshark.org

W8. Modbus Specification, Modbus Inc. http://www.modbus.org/

W9. Profibus Specifications, Profibus & Profinet International, www.profibus.com

W10. Falliere, N, Murchu L, Chien E. – W32.Stuxnet Dossier, 2011,Symantec Security Report – disponibil on-line https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/security-response-w32-stuxnet-dossier-11-en.pdf

W11. ***, http://hitachi-id.com/concepts/access_control.html , Hitachi ID Systems, Inc.

W12. Jeremy Kirk, „Heathrow to Install Facial Recognition Scanners", PCWorld on-line, 22 iulie 2011, http://www.pcworld.com/article/236328/article.html

W13. Documentație utilizare MATLAB - https://www.mathworks.com/help/matlab/

W14. ***,** *Precise Biometrics Technical Solutions*, Precise Biometrics, https://precisebiometrics.com/fingerprint-technology/

W15. Introduction to Iris Recognition, Cambridge University, https://www.cl.cam.ac.uk/~jgd1000/iris_recognition.html

W16. Directiva 95/46/CE a Parlamentului European și a Consiliului din 23 octombrie 1995, on-line: http://www.dataprotection.ro/servlet/ViewDocument?id=44

W17. Documentația *iptables* - https://www.netfilter.org/projects/iptables/index.html

W18. U.S. Department of Homeland Security – Site-ul web al ICS-CERT - https://ics-cert.us-cert.gov

W19. Site-ul și documentația sistemului complex de honeypot-uri T-POT http://dtag-dev-sec.github.io/mediator/feature/2016/10/31/t-pot-16.10.html

W20. Site-ul și documentația aplicației Docker - http://docker.com

W21. Neagu, C. – Îndrumar Docker, publicat 21.08.2014 - http://clneagu.ro/docker/

W22. Site-ul și documentația aplicației ElasticSearch - https://www.elastic.co

W23. Site-ul si documentația aplicației Logstash - https://www.elastic.co/products/logstash

W24. Site-ul si documentația aplicației Kibana - https://www.elastic.co/products/kibana

W25. Site-ul honeypot-ului Conpot – http://conpot.org

W26. Site-ul Honeynet Project - https://www.honeynet.org

W27. Site-ul Dionaea – https://www.edgis-security.org/honeypot/dionaea/

W28. Site-ul Cowrie – http://www.micheloosterhof.com/cowrie/

W29. Site-ul companiei de hosting DigitalOcean – https://www.digitalocean.com

W30. Baza de date de geolocalizare GeoIP – GeoLite - http://dev.maxmind.com/geoip/legacy/geolite/

W31. Site-ul companiei de hosting VULTR - https://www.vultr.com
W32. Site-ul companiei Symantec, USA - https://www.symantec.com
W33. Site-ul companiei FireEye, Inc. - https://www.fireeye.com
W34. Site-ul companiei Kaspersky Lab - https://www.kaspersky.com/about
W35. Site-ul Department of Homeland Security - https://www.dhs.gov
W36. Site-ul Centrului National de Raspuns la Incidente de Securitate Cibernetica – CERT-RO – www.cert.ro
W37. Site-ul companiei MITRE și baza de date CVE- http://cve.mitre.org
W38. Site-ul Cyber Security Division – US Department of Homeland Security - https://www.dhs.gov/science-and-technology/cyber-security-division
W39. Site-ul aplicatiei *Nexpose (Rapid 7),* https://www.rapid7.com/products/nexpose/
W40. Site-ul aplicatiei *OpenVAS, http://www.openvas.org*
W41. Site-ul aplicatiei *nmap, https://nmap.org*
W42. Site-ul aplicatiei *nessus, https://www.tenable.com/products/nessus-vulnerability-scanner vu*
W43. Site-ul companiei Emerson, http://www.emerson.com/en-us/automation/deltav
W44. Documentația Fuzzy Logic Toolbox – Matlab - https://www.mathworks.com/help/fuzzy/
W45. http://www.bel.utcluj.ro/rom/dce/goltean/tice/lab/2%20SimulareaSLF_Matlab.pdf
W46. Ivanovici, M - Procesarea imaginilor folosind logica fuzzy, 2007, http://miv.ro/ro/documentatie/pi/PIlab12.pdf
W47. http://ac.upg-ploiesti.ro/cursuri/tra/curs_tra.pdf
W48. Site-ul ICS-CET Insider Threat Center - https://www.cert.org/insider-threat/
W49. Texas Instruments, The RS-485 Design Guide, http://www.ti.com/lit/an/slla272b/slla272b.pdf
W50. Cisco Inc., Modbus/TCP Protocol Multiple Protocol Implementation Vulnerabilities - https://tools.cisco.com/security/center/viewAlert.x?alertId=23280
W51. Site-ul aplicației QModMaster - https://sourceforge.net/projects/qmodmaster/
W52. Documentația sistemului de dezvoltare ATMEL ATSAMA5D-Xplained - http://www.atmel.com/tools/ATSAMA5D3-XPLD.aspx
W53. Documentația sistemului de dezvoltare NXP LPC1768 - https://developer.mbed.org/platforms/mbed-LPC1768/
W54. Documentația pentru interfațarea senzorului de temperatură cu modulul MBed https://developer.mbed.org/cookbook/Grove-temperature--humidity-sensors
W55. Site-ul aplicației *modpoll - http://www.modbusdriver.com/modpoll.html*
W56. Linux On ARM, http://eewiki.net/display/linuxonarm/ ATSAMA5D3+Xplained
W57. Element14 Tutorial instalare Debian pe AT SAMA5D3-Xplained www.element14.com/community/community/designcenter/sama5d3xplained/blog/2014/04/25/debian-on-the-sama5d3-xplained
W58. Documentația limbajului Python - https://www.python.org
W59. Site-ul și documentația programului Scapy - http://www.secdev.org/projects/scapy/
W60. Site-ul standardului RFID Mifare - https://www.mifare.net/en/