ROMÂNIA

(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

(11) **RO 137572 A0**

(51) Int.Cl.
G06F 21/50 (2013.01),
G06F 21/55 (2013.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2023 00107**

(22) Data de depozit: **07/03/2023**

(41) Data publicării cererii:
28/07/2023 BOPI nr. **7/2023**

(71) Solicitant:
• **SAFETECH INNOVATIONS S.A.**,
STR.FRUNZEI, NR.12-14, ET.1 ŞI 2, SECTOR 2, BUCUREŞTI, B, RO

(72) Inventatori:
• **MIRIŢESCU SORIN**,
STR. ELENA CARAGIANI, NR.28, BL.8C, SC.2, ET.2, AP.25, SECTOR 1, BUCUREŞTI, B, RO;
• **PARVU MARIUS- EMIL**, *STR.CERNĂUŢI, NR.5, BL.28, SC.2, ET.6, AP.93, SECTOR 2, BUCUREŞTI, RO*

(74) Mandatar:
CABINET N.D. GAVRIL S.R.L.,
STR.ŞTEFAN NEGULESCU NR.6A, SECTOR 1, BUCUREŞTI

(54) # SIMULATOR ŞI ANALIZĂ ATACURI CIBERNETICE ÎN INFRASTRUCTURI INDUSTRIALE

(57) **Rezumat:**

Invenţia se referă la un simulator şi la o metodă de analiză a atacurilor cibernetice în infrastructuri industriale. Simulatorul conform invenţiei este format dintr-o singură platformă unitară care cuprinde o incintă pentru simularea unui proces industrial incluzând o serie de echipamente industriale similare cu cele dintr-o infrastructură de producţie şi o incintă cu senzori ce monitorizează valori precum temperatura şi umiditatea, dar şi actuatori de tipul închis/deschis, de ex. Pentru un încălzitor, ventilator, umidificator, care vor fi comandaţi atunci când se ating anumite valori de prag, sau poate fi integrată într-o reţea de echipamente industriale existente într-o companie, şi dintr-o aplicaţie software prin intermediul căreia se pot simula şi gestiona diferite atacuri cibernetice împotriva infrastructurii industriale care generează diferite atacuri cibernetice, monitorizează şi raportează progresul acestora, selectează componentele specifice ale infrastructurii împotriva cărora sunt lansate atacurile cibernetice şi care încarcă şi stochează fişiere de captură a traficului de tip PCAP şi oferă date de intrare unui analizor de evenimente de securitate cibernetică ce detectează şi alertează utilizatorii cu privire la activitatea suspectă din infrastructura de reţea şi analizează traficul Modbus şi Profinet utilizând senzori de reţea configuraţi pentru a monitoriza traficul din reţea, având incluse sisteme de detectare a intruziunilor cu reguli special concepute pentru a detecta traficul acestora.

Revendicări: 4
Figuri: 3

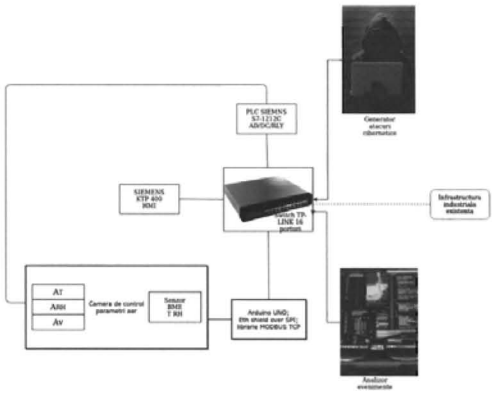

Fig. 1

RO 137572 A0

OFICIUL DE STAT PENTRU INVENŢII ŞI MĂRCI
Cerere de brevet de invenţie
Nr. a 2023 00107
Data depozit 07 -03- 2023

45

Simulator şi analiză atacuri cibernetice în infrastructuri industriale

Invenţia este aplicabilă în domeniul securităţii informaţiilor şi poate fi utilizată în companiile publice şi private care activează în domeniul industrial - companiile de energie electrică, transporturi, distribuţie apă/gaz, reţele de comunicaţii, Internet of Things (IoT), nelimitativ.

Invenţia propune un mediu de laborator în care pot fi simulate diferite tipuri de atacuri cibernetice specifice mediului industrial; astfel vine în sprijinul companiilor ce deţin infrastructuri industriale.

Companiile au nevoie de măsuri solide de securitate cibernetică pentru a se proteja împotriva unor potenţiale atacuri cibernetice care ar putea avea consecinţe devastatoare. Prin simularea atacurilor cibernetice şi evaluarea eficacităţii sistemelor lor de apărare într-un mediu controlat, acestea pot înţelege şi identifica mai bine vectorii potenţiali de atac şi pot dezvolta contramăsuri şi strategii mai eficiente de apărare.

Utilizarea invenţiei poate fi extinsă şi în instituţiile de învăţământ. Studenţii şi cercetătorii din domeniul informaticii şi securităţii cibernetice pot acumula o experienţă practică prin simularea atacurilor cibernetice în medii industriale de laborator. Acest lucru le poate oferi o înţelegere mai profundă a modului în care funcţionează aceste atacuri şi cum poate o organizaţie să se apere împotriva lor. Platforma propusă poate servi drept un instrument deosebit de valoros pentru educatori pentru a demonstra scenarii posibile de atac inspirate din lumea reală şi importanţa securităţii informaţiilor. Nenumărate atacuri cibernetice au loc asupra infrastructurilor industriale, cu impact asupra proceselor automatizate (linii de fabricaţie, furnizarea de utilităţi către populaţie etc.).

Multe companii nu au vizibilitate asupra atacurilor din reţelele industriale, fie pentru că nu au instrumente eficiente de monitorizare, detecţie şi analiză, fie pentru că nu au personal pregătit pentru astfel de activităţi.

Experţii în automatizare pot administra echipamentele industriale, dar nu au cunoştinţele necesare de securitate cibernetică, pentru a înţelege şi detecta riscurile de securitate existente. Sau există experţi în securitate cibernetică care însă nu au şi

competenţe pe partea de automatizare. În general nu există veriga care să lege inginerii automatişti de cei specializaţi în securitate cibernetică.

Sunt situaţii în care o companie ce deţine infrastructuri industriale apelează la serviciile de securitate cibernetică ale unei alte companii pentru testarea infrastructurii.

Testele de securitate pentru testarea infrastructurii industriale nu se pot face în mediul de producţie, pentru că au un impact negativ major asupra procesului industrial, sau a livrării de utilităţi, după caz. În acest sens, se impune simularea într-un mediu de laborator a unei infrastructuri industriale, în cadrul căruia pot fi testate diferite scenarii de atac şi se poate verifica dacă atacurile sunt detectate de sistemele de monitorizare (dacă acestea există), sau se identifică necesitatea implementării unui sistem de monitorizare şi analiză a atacurilor cibernetice în protejarea infrastructurilor industriale.

Invenţia contribuie la reducerea decalajelor dintre diferitele medii şi expertize, ale inginerilor de securitate cibernetică şi ale inginerilor automatişti din domeniul industrial, permiţându-le să colaboreze mai eficient pentru a proteja infrastructura critică împotriva ameninţărilor cibernetice.

Pentru inginerii de securitate cibernetică, soluţia tehnică oferă oportunitatea de a-şi aplica cunoştinţele despre principiile şi tehnicile de securitate cibernetică la provocările şi ameninţările specifice cu care se confruntă sistemele de control industrial. Aceştia obţin o înţelegere mai profundă a modului în care funcţionează aceste sisteme şi a impactului potenţial al unui atac cibernetic de succes.

Pentru inginerii din domeniul industrial, platforma oferă o modalitate de a se familiariza cu problemele de securitate cibernetică şi cu importanţa protejării infrastructurii industriale. Aceştia pot învăţa despre tipurile de atacuri care pot viza sistemele industriale, cum să identifice şi să răspundă la ameninţările cibernetice şi cum să colaboreze cu specialiştii de securitate pentru a îmbunătăţi securitatea generală a sistemelor de control industrial.

Stadiul tehnicii

Brevetul EP3786827 – Simulator pentru atac cibernetic, prezintă un simulator de agresor inteligent care poate construi un grafic al unei situaţii virtualizate a unei reţele, inclusiv dispozitive care se conectează la situaţia virtualizată a reţelei, precum şi conexiuni şi căi prin situaţia virtualizată a reţelei. Rularea unui scenariu de atac cibernetic

simulat pe situaţia virtualizată a reţelei pentru a identifica unul sau mai multe dispozitive critice care se conectează la situaţia virtualizată a reţelei din punct de vedere al securităţii şi apoi aceste informaţii sunt introduse într-un raport generat pentru a ajuta la prioritizarea dispozitivelor ce ar trebui să aibă o prioritate în alocarea de resurse corespunzătoare de protecţie cibernetică. În timpul unei simulări, simulatorul de agresor inteligent calculează căile cu cea mai mică rezistenţă pentru o ameninţare cibernetică în scenariul de atac cibernetic pentru a compromite un dispozitiv sursă prin intermediul altor componente până la atingerea obiectivului final al scenariului de atac cibernetic în reţeaua virtualizată, toate bazate pe cunoştinţele istorice despre conectivitate şi modele de comportament ale utilizatorilor şi dispozitivelor din reţeaua actuală analizată.

Brevetul US20160285907 – prezintă un sistem şi o metodă de simulare a scenariului de atac cibernetic care include un simulator de aeronavă operabil pentru a genera o simulare de aeronave, un generator de atac cibernetic operabil pentru a genera o simulare de atac cibernetic, un generator de apărare cibernetică operabil pentru a genera o simulare de apărare cibernetică, un generator de scenarii operabil pentru a genera un scenariu de atac cibernetic, inclusiv simularea de atac cibernetic şi simularea de apărare cibernetică şi pentru a lansa scenariul de atac cibernetic împotriva simularii aeronavei şi un instrument de analiză a scenariului de atac cibernetic operabil pentru a evalua impactul scenariului de atac cibernetic asupra simularea aeronavei.

Brevetul RO130798 (A0) - Platformă hardware şi software pentru prevenţia şi detecţia atacurilor cibernetice, se referă la o platformă hardware şi software pentru prevenirea şi detectarea atacurilor cibernetice asupra reţelelor de calculatoare. Platforma cuprinde: un sistem (1) de detectare a intruziunilor, alcătuit dintr-un modul (1a) de decodare a pachetelor, responsabil cu decodarea diferitelor formate de pachete preluate din reţea, dintr-un modul (1b) de preprocesare, responsabil cu reconstrucţia unui flux de comunicaţie în baza pachetelor primite, şi dintr-un modul (1c) responsabil cu executarea regulilor de identificare a atacurilor asupra pachetelor de date primite din reţea, un sistem (2) de agregare a informaţiilor, alcătuit dintr-un modul (2b) care distribuie informaţiile extrase în urma prelucrării regulilor, către diferite sisteme interne sau externe, dintr-un modul (2a) care transmite alerte şi notificări către terţe sisteme, şi dintr-un modul (2c) de stocare a informaţiilor despre fluxurile din reţea, şi a informaţiilor parţiale sau totale obţinute în urma aplicării regulilor, şi un sistem (3) expert de management al reţelei, alcătuit dintr-un modul (3b) responsabil cu agregarea diferitelor informaţii din modul

(2c), şi trecerea lor printr-o serie de transformări şi corelări; rezultatele obţinute sunt adăugate la o bază de cunoştinţe (3c), fie prin adăugare, fie prin corectarea unor informaţii deja existente, cu privire la tendinţe şi activităţi înregistrate şi învăţate de către sistem, dintr-un sistem (3a) expert care poate fi declanşat de informaţii primite de la un modul (2b) şi care, folosind informaţii din baza de cunoştinţe (3c), poate declanşa una sau mai multe acţiuni corective, în reţea, pentru a stopa sau limita un atac cibernetic, şi dintr-un modul (3d) care primeşte comenzi de la sistemul (3) expert şi poate reconfigura echipamentele de reţea pentru stoparea şi/sau limitarea atacurilor cibernetice.

Brevetul US8554536 B2 – Sistem de suport pentru operaţii informatice şi program informatic, se referă la crearea unui mediu de învăţare în reţea, care simulează o reţea largă şi foloseşte simularea şi tehnologii de reţele virtuale, pe lângă reţelele fizice, pentru a învăţa cum se poate exploata o reţea de calculatoare şi ce tehnici de atac ale reţelelor de calculatoare se pot folosi în exerciţii gândite pentru personalul responsabil cu protejarea reţelelor şi pentru testarea atacurilor în reţele. Acest sistem, metodă şi program informatic suportă integrarea unor calculatoare reale, pentru a oferi exerciţii mult mai realiste.

Brevetul US7921462 B2 – Identificarea şi blocarea unui atac Distributed Denial of Service (DDoS) într-o reţea, oferă metode, dispozitive şi sisteme pentru a detecta un atac de tipul Distributed Denial of Service (DDoS) în Internet, prin luarea unor mostre de pachete de trafic de reţea în unul sau mai multe puncte din conexiunile backbone din Internet, pentru a determina metrica pachetelor. Metrica pachetelor poate fi compusă din volumul pachetelor primite, fiind analizate pe anumite intervale de timp, ţinând cont de localizarea geografică de unde sunt transmise. Comportamentul detectat poate indica o distorsiune în traficul de reţea, descoperind astfel un atac DDoS. De asemenea, invenţia oferă o metodă de autentificare a pachetelor la nivelul router-erelor din reţea, pentru a creşte nivelul de calitate a serviciilor (QoS) pentru pachetele de încredere. Această metodă poate fi utilizată pentru a bloca, ori filtra pachetele şi poate fi folosită împreună cu un sistem de detecţie a unui atac DDoS, pentru a oferi protecţie în faţa acestor atacuri din internet, într-un mod distribuit.

Brevetul EP 2149087B1 - Sistem şi metodă de analiză a intrusiunii neautorizate într-un reţea de calculatoare, se referă la domeniul metodelor şi sistemelor de protecţie a reţelelor de calculatoare şi în special, dar nu în mod limitativ, la tehnologia reţelelor de

tip capcană cu generare automată de semnături pentru sistemele de detectare şi prevenire a intruziunilor.

Una sau mai multe forme de realizare ale invenţiei se referă la o metodă şi un sistem îmbunătăţit pentru protejarea reţelelor de calculatoare. Una dintre formele de realizare ilustrează activitatea atacatorului îndreptată spre reţeaua de calculatoare protejată. Ca într-un atac tipic, atacatorul scanează un port deschis pe reţeaua de calculatoare în încercarea de a realiza o conexiune şi apoi de a accesa unul sau mai multe dispozitive de reţea protejate din reţea.

În context, se discută despre vulnerabilitatea reţelelor de calculatoare la atacurile de tip "zero-day", care exploatează vulnerabilităţi de securitate necunoscute. Sistemele convenţionale de securitate a reţelelor, cum ar fi firewall-urile şi sistemele de detectare/prevenire a intruziunilor, se bazează pe semnături statice şi sunt limitate în ceea ce priveşte capacitatea lor de a opri atacurile de tip zero-day. Sistemele Honeynet, care îi prind în capcană pe atacatori prin imitarea unor ţinte valoroase, sunt pasive şi ineficiente împotriva atacatorilor sofisticaţi. Prin urmare, brevetul semnalează nevoia de metode şi sisteme care să asigure actualizări în timp real ale bibliotecii de semnături de atac a unei reţele şi să protejeze în mod adecvat reţelele împotriva atacurilor noi şi nedefinite. Este menţionată invenţia dezvăluită în US 2006/13670 A1 ce răspunde acestei necesităţi prin utilizarea unui sistem de detectare a intruziunilor pentru a detecta atacurile de reţea asupra unei maşini virtuale care rulează pe un sistem de operare al hipervizorului.

Textul descrie o invenţie pentru protejarea reţelelor de calculatoare împotriva atacurilor prin utilizarea unui dispozitiv de reţea capcană modular care prezintă un sistem de operare standard ca un front-end pentru a atrage atacatorii să acceseze şi să ruleze exploit-uri personalizate sau cunoscute. Un driver de kernel sentinelă monitorizează conexiunile şi activitatea sistemului de operare şi trimite datele capturate, care conţin informaţii de identificare a atacurilor, către un modul back-end de procesare separat. Modulul de procesare generează un raport al atacului, creează o semnătură de atac şi o încarcă într-un sistem de detectare/prevenire a intruziunilor pentru protecţia sistemelor de producţie. O altă formă de realizare implică permiterea accesului la sisteme de operare capcană virtualizate pe sistemul de operare al hipervizorului găzduit pe un dispozitiv de reţea capcană şi interceptarea atacurilor de reţea prin intermediul unui modul de tip rootkit. Informaţiile de identificare a atacului sunt comunicate printr-un canal de interfaţă

de reţea privată şi stocate pentru a genera o semnătură de atac pentru a preveni atacurile ulterioare.

Dezavantajul acestor invenţii este faptul ca nu oferă un mediu integrat de laborator cu elemente de infrastructură industrială miniaturizată care să urmărească controlul parametrilor aerului şi a altor categorii de resurse instrumentale şi care poate fi folosit ca suport eficient de instruire precum şi evaluare a securităţii cibernetice în domeniul industrial.

Problema tehnică pe care o rezolvă invenţia este realizarea unui mediu de laborator în care pot fi simulate diferite tipuri de atacuri cibernetice specifice mediului industrial; astfel vine în sprijinul companiilor ce deţin infrastructuri industriale.

O altă problemă pe care o rezolvă invenţia este pregătirea resursei umane în securitatea cibernetică aplicată pe infrastructuri industriale.

Invenţia este folosită ca instrument de învăţare atât pentru inginerii automatişti, cât şi pentru inginerii în securitate cibernetică.

Invenţia prezintă următoarele avantaje:

- Validarea eficienţei sistemelor de protecţie implementate într-o infrastructură industrială prin testarea într-un mediu controlat a unor atacuri cibernetice simulate, îndreptate către un sistem ce nu face parte din procesul de producţie.
- Facilităţile de detecţie şi analiză ale analizorului de evenimente de securitate, în situaţia în care nu este implementată deja o soluţie de monitorizare într-o infrastructură industrială.
- Instruirea eficientă prin practica bazată pe scenarii de atac orientate către infrastructuri industriale şi înţelegerea utilităţii instrumentelor de detecţie şi analiză a evenimentelor de securitate.
- Contribuie la crearea unei comunităţi de profesionişti în domeniul securităţii cibernetice care poate face schimb de cunoştinţe şi bune practici.

Simulator şi analiză atacuri cibernetice în infrastructuri industriale, conform invenţiei, înlătură dezavantajul menţionat prin aceea că este format dintr-o singură platformă unitară ce cuprinde o incintă pentru simularea unui proces industrial, care include o serie de echipamente industriale similare cu cele dintr-o infrastructură de

producţie, ce include o incintă cu senzori care monitorizează valori precum temperatură şi umiditate, dar şi actuatori de tipul on/off (încălzitor, ventilator, umidificator), care vor fi comandaţi atunci când se ating anumite valori prag ale valorilor, sau poate fi integrată în reţeaua echipamentelor industriale existente într-o companie, o aplicaţie software prin intermediul căreia se pot simula şi gestiona diferite atacuri cibernetice împotriva infrastructurii industriale care generează diferite atacuri cibernetice împotriva infrastructurii industriale, monitorizează şi raportează progresul atacurilor cibernetice, selectează componentele specifice ale sistemului infrastructură critică împotriva cărora sunt atacurile cibernetice, totodată poate încărca şi stoca fişiere de captură trafic de tip PCAP şi, oferă datele de intrare pentru un analizor de evenimente de securitate cibernetică ce detectează şi alertează utilizatorii cu privire la activitatea suspectă din infrastructura de reţea, analizează traficul Modbus şi Profinet utilizând senzori de reţea configuraţi pentru a monitoriza şi captura traficul din reţea unde sunt incluse sistemele de detectare a intruziunilor cu reguli special concepute pentru a detecta traficul acestora.

Se dă în continuare un exemplu de realizare a invenţiei, nelimitativ, în legătură şi cu fig. 1-3, care reprezintă :

Fig. 1 – componentele platformei pentru simularea şi analizarea unui atac cibernetic

Fig. 2 – incinta echipamentelor de comandă a parametrilor aerului

Fig. 3 – incinta camerei de control a parametrilor aerului

Invenţia constă în realizarea unui mediu de laborator prin integrarea într-o singură platformă unitară A a unei incinte pentru simularea unui proces industrial A_1, a unei aplicaţii software A_2 prin intermediul căreia se pot genera diferite atacuri cibernetice împotriva infrastructurii industriale, şi a unui software de analiză evenimente de securitate A_3.

Incinta pentru simularea unui proces industrial A_1 include o serie de echipamente industriale similare cu cele dintr-o infrastructură de producţie.

Aplicaţia software A_2 prin intermediul căreia se pot genera diferite atacuri cibernetice împotriva infrastructurii industriale, şi analizorul de evenimente de securitate cibernetică A_3

Incinta ce simulează procesul industrial A_1 poate fi integrată în reţeaua echipamentelor industriale existente într-o companie, la fel şi aplicaţia software A_2 care generează atacurile cibernetice.

În situaţia în care o companie are deja implementată o soluţie de monitorizare şi analiză a atacurilor cibernetice, se va putea testa eficacitatea soluţiei respective în urma simulării atacurilor asupra incintei ce simulează procesul industrial. În cazul în care compania nu are o soluţie de analiză, se poate folosi analizorul de evenimente de securitate cibernetică A_3 ce face parte din soluţia propusă.

Invenţia este construită astfel încât să fie uşor de instalat şi operat şi oferă posibilitatea integrării într-o infrastructură industrială existentă, pentru a putea simula atacuri cibernetice, care să nu impacteze mediul de producţie, dar care să poată testa detecţia automată a atacurilor prin soluţia existentă în infrastructură, sau, în lipsa acesteia, să poată suplini detecţia şi analiza atacurilor prin analizorul de evenimente integrat.

Invenţia prezintă o interfaţă grafică utilizator (UI) ce permite utilizatorilor să interacţioneze cu procesul de simulare şi control a atacurilor cibernetice. Sunt incluse capabilităţi funcţionale precum selectarea scenariilor de atac care urmează să fie rulate, modificarea parametrilor pentru un anumit atac şi vizualizarea rezultatelor simulării. Interfaţa grafică utilizator (UI) este intuitivă, uşor de utilizat şi atractivă din punct de vedere vizual.

Prin utilizarea interfeţei grafice accesibile prin intermediul unui browser web se pot simula următoarele tipuri de atacuri cibernetice:

- Atacuri de tip "Recomaissance" (de recunoaştere) prin scanare adrese şi porturi în vederea descoperirii porturilor vulnerabile
- Atacuri de tip "Command injection" (injectarea de comenzi) ce presupun trimiterea de comenzi şi /sau parametri rău intenţionaţi către procesele industriale şi infrastructurile critice ce pot conduce la pierderea controlului proceselor industriale în sistemele critice industriale, întreruperea canalelor de comunicare ale controlerelor SCADA din sistemele critice industriale, modificarea neautorizată a parametrilor de configurare şi a controlerelor SCADA (PLC), a interfeţelor om-maşină (HMI) şi a punctelor de configurare a proceselor aferente acestora
- Atacuri de tip "Denial of Service" (blocarea serviciilor) care încearcă să epuizeze resursele de comunicare şi aplicaţii ale sistemului, făcând imposibilă

comunicarea între echipamentele industriale şi implicit funcţionarea unui proces industrial.

Fiecare tip de atac menţionat mai sus poate fi personalizat cu diferiţi parametri, cum ar fi frecvenţa şi durata atacului. Aplicaţia software A_2 oferă posibilitatea de a selecta componentele specifice ale sistemului infrastructură industrială din laborator împotriva cărora dorim să îndreptăm atacurile cibernetice. Utilizatorii pot astfel selecta configuraţii specifice şi ajusta parametrii de atac pentru a se potrivi obiectivelor lor de instruire sau validare a securităţii componentelor infrastructurii testate.

Aplicaţia software A_2 monitorizează şi raportează progresul atacurilor simulate. Acest lucru îi va ajuta pe utilizatori să înţeleagă mai bine impactul fiecărui atac şi să identifice domeniile în care ar putea fi necesară o pregătire suplimentară.

Prin intermediul aplicaţiei software A_2 se mai pot încărca şi stoca fişiere de captură trafic de tip PCAP. Se poate astfel reproduce un anumit trafic de reţea prin transmiterea automată a acestuia la interfaţa de reţea, simulând în esenţă acelaşi trafic ca şi cum ar fi generat de dispozitive reale.

Aplicaţia software A_2 permite de asemenea utilizatorilor să colaboreze cu alte persoane şi să partajeze scenariile de simulare şi rezultatele acestora precum şi sugestiile de îmbunătăţire a securităţii componentei atacate.

Aplicaţia software A_2 oferă datele de intrare pentru componenta analizor de evenimente de securitate cibernetică A_3 ce detectează şi alertează utilizatorii cu privire la activitatea suspectă din infrastructura de reţea a laboratorului.

Analizorul de evenimente de securitate cibernetică A_3 e capabil să analizeze traficul Modbus şi Profinet. Atât Modbus, cât şi Profinet sunt protocoale ce sunt utilizate în mod obişnuit în sistemele de control industrial. Pentru a analiza traficul Modbus şi Profinet, utilizăm senzori de reţea care sunt configuraţi pentru a monitoriza şi captura traficul din reţea. Sunt incluse sistemele de detectare a intruziunilor ca Snort şi Suricata, cu reguli special concepute pentru a detecta traficul Modbus şi Profinet.

Incinta de simulare a unui proces industrial A_1, reprezentată schematic în figura 1, include o incintă cu senzori, în sine cunoscuţi, care monitorizează valori precum temperatură şi umiditate, dar şi actuatori de tipul on/off (încălzitor, ventilator, umidificator), care vor fi comandaţi atunci când se ating anumite valori prag ale valorilor transmise de senzori. Scopul incintei A_1 ce simulează un proces industrial este să păstreze parametrii aerului (temperatură şi umiditate) în anumite limite, stabilite anterior, dar care pot fi ajustate.

In continuare sunt prezentate componentele simulatorului şi actorii care interacţionează cu sistemul:

Un hacker etic 1 (atacator) simulează diferite atacuri, pornind de la tipurile de atac amintite mai sus. Se foloseşte un scenariu în care are acces la echipamentul de tip Switch de reţea. Pentru a putea rula atacurile, procedează astfel:

- se conectează la switch-ul de reţea
- interceptează traficul
- descoperă subnetul de reţea utilizat de echipamente (dacă nu ştie deja acest lucru)
- îşi setează pe laptop un IP din aceeaşi reţea
-accesează interfaţa grafică a generatorului de atacuri cibernetice
-selectează tipul de atac
-configurează parametrii atacului (opţional)
-porneşte atacul

În cadrul atacurilor de tip "Reconnaissance" hacker-ul etic 1 (atacatorul) trimite pachete în reţea, pentru a identifica IP-urile existente, serviciile expuse şi modul în care poate interacţiona cu ele. Acest tip de atac îl ajută să construiască o hartă e echipamentelor, inclusiv cu tipul şi versiunea acestora.

Prin atacurile de tipul "Command injection", hacker-ul etic 1 (atacatorul) poate trimite către echipamentul PLC pachete de reţea cu valori greşite ale parametrilor aerului, altele decât cele preluate de către senzor, astfel încât PLC-ul să acţioneze releele care pornesc sau opresc diferite dispozitive ce controlează parametrii aerului (bec, ventilatoare, umidificator). Echipamentul HMI va afişa valorile eronate introduse de către atacator.

Prin atacurile de tipul "Denial of Service", hacker-ul etic 1 (atacatorul) se poate îndrepta împotriva oricărui echipament din reţea (PLC, HMI, Arduino). El va genera foarte multe pachete TCP, care vor inunda echipamentul, făcându-l inaccesibil celorlalte echipamente cu care ar trebui să comunice în mod normal. Efectul vizibil este faptul că datele citite de la senzorul de pe Arduino nu ajung la PLC, HMI-ul afişează un mesaj de eroare, iar parametrii aerului nu mai sunt controlaţi de programul din PLC.

Indiferent de tipul de atac, analizorul de evenimente (actorul uman şi aplicaţia software A_3) le poate detecta şi eventual bloca.

Incinta B în care se găsesc echipamentele de comandă a parametrilor aerului, într-un exemplu de realizare, poate arăta ca în fig. 2, unde 1 estre o zonă de acces la cabluri UTP pentru conectarea PLC-ului şi a HMI-ului la switch-ul de reţea, 2 reprezintă o carcasă cu instrumente electronice cu modul convertor DC-DC cu reglare coborâre tensiune 12V-5V necesari umidificatorului, 3 - Arduino Uno – are rolul de a transmite date de la senzor către PLC, 4 clemă fixare şină DIN, 5 sursă de alimentare 12V pentru ventilatoare, 6 priza modulara montaj sina DIN pentru alimentare Arduino Uno 3, 7 - PLC Siemens S7 1212C – rulează programul de control al parametrilor aerului, 8 - acces cablu 230v AC pentru alimentare PLC, 9 - ecran afişare valori senzor preluate de la Arduino Uno 3, 10 - HMI Siemens KTP400 – interfaţă grafică de afişare a parametrilor aerului şi de modificare a limitelor acestora, 11 - fereastră de acces montare şi control echipamente.

Echipamentul Arduino Uno 3 este un echipament minimalist, care este conectat cu un senzor de temperatură şi umiditate şi un mic ecran de vizualizare a datelor de la senzor. Rolul principal al său este de a converti semnalul analogic/digital primit de la senzor în pachete Modbus TCP, ce pot fi trimise către PLC-ul ce le poate interpreta.
Echipamentul PLC 7 este elementul central şi interacţionează cu Arduino Uno 3, cu echipamentul HMI 10, cât şi cu actuatorii ce modifică parametrii aerului. El rulează programul ce îi spune în ce moment să acţioneze releele conectate la echipamentele ce pot modifica parametrii aerului.

Echipamentul HMI 10 are rolul de a afişa valorile curente ale parametrilor aerului, dar şi pragurile setate şi permite modificarea pragurilor, precum şi pornirea şi oprirea programului care rulează în PLC.

Incinta de control a parametrilor aerului, C , fig, 3, este compusă din 2 ventilatoare de 12V, 12 – acţionate pentru a dezumidifica aerul, dar şi pentru a-l răci, un umidificator de aer 13 , un soclu şi un bec de 12V cu incandescenţă 14 – este aprins pentru a încălzi aerul şi un senzor BME280 – 15 care preia parametrii de temperatură şi umiditate ai aerului şi îi transmite către Arduino Uno 3.

REVENDICĂRI

1 – Simulator şi analiză atacuri cibernetice în infrastructuri industriale, conform invenţiei, este format dintr-o singură platformă unitară (A) a unei incinte pentru simularea unui proces industrial (A_1), care include o serie de echipamente industriale similare cu cele dintr-o infrastructură de producţie, si care poate fi integrată în reţeaua echipamentelor industriale existente într-o companie, a unei aplicaţii software (A_2) prin intermediul căreia se pot genera şi gestiona diferite atacuri cibernetice împotriva infrastructurii industriale şi a unui software de analiză evenimente de securitate (A3) capabil să analizeze traficul Modbus şi Profinet pentru care se utilizează senzori de reţea configuraţi pentru a monitoriza şi captura traficul din reţea unde sunt incluse sistemele de detectare a intruziunilor, cu reguli special concepute pentru a detecta traficul acestora.

2 - Simulator şi analiză atacuri cibernetice în infrastructuri industriale, conform revendicării 1, caracterizat prin aceea că incinta pentru simularea unui proces industrial (A1), include o serie de echipamente industriale similare cu cele dintr-o infrastructură de producţie, sau poate fi integrată în reţeaua echipamentelor industriale existente într-o companie, cuprinde o incintă cu senzori care monitorizează valori precum temperatură şi umiditate, dar şi actuatori de tipul on/off (încălzitor, ventilator, umidificator), care vor fi comandaţi atunci când se ating anumite valori prag ale valorilor.

3 - Simulator şi analiză atacuri cibernetice în infrastructuri industriale, conform revendicărilor 1 şi 2, caracterizat prin aceea că prin intermediul aplicaţiei software (A_2) se pot genera diferite atacuri cibernetice împotriva infrastructurii industriale, monitorizează şi raportează progresul atacurilor cibernetice, oferă posibilitatea de a selecta componentele specifice ale sistemului infrastructură critică din laborator împotriva cărora sunt atacurile cibernetice, astfel utilizatorii pot selecta configuraţii specifice şi pot ajusta parametrii de atac pentru a se potrivi obiectivelor lor de instruire sau validare a securităţii componentelor infrastructurii testate, aplicaţia software poate încărca şi stoca fişiere de captură trafic de tip PCAP, aplicaţia software (A_2) oferă datele de intrare pentru analizorul de evenimente de securitate cibernetică (A_3).

4 – Simulator şi analiză atacuri cibernetice în infrastructuri industriale, conform revendicărilor 1, 2 şi 3, caracterizat prin aceea că analizorul de evenimente de securitate cibernetică (A_3) ce detectează şi alertează utilizatorii cu privire la activitatea suspectă din infrastructura de reţea a laboratorului, analizează traficul Modbus şi Profinet utilizând

senzori de rețea care sunt configurați pentru a monitoriza și captura traficul din rețea și sunt incluse sistemele de detectare a intruziunilor cu reguli special concepute pentru a detecta traficul Modbus și Profinet.

32

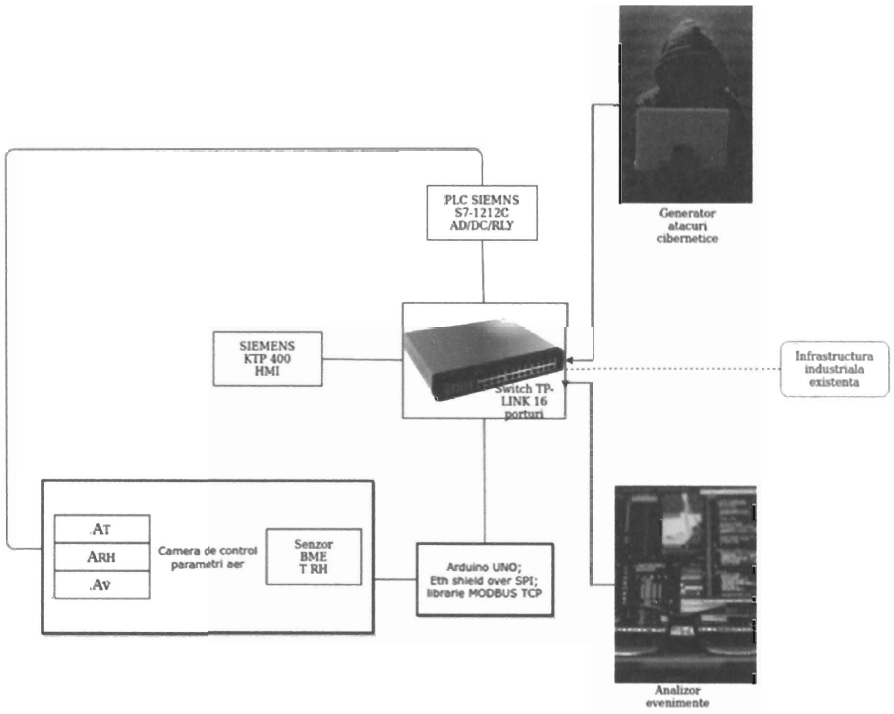
PLC SIEMNS
S7-1212C
AD/DC/RLY
Generator
atacuri
cibernetice
SIEMENS
KTP 400
HMI
Switch TP-
LINK 16
porturi
Infrastructura
industriala
existenta
AT
ARH
Av
Camera de control
parametri aer
Senzor
BME
T RH
Arduino UNO;
Eth shield over SPI;
librarie MODBUS TCP
Analizor
evenimente

Fig. 1

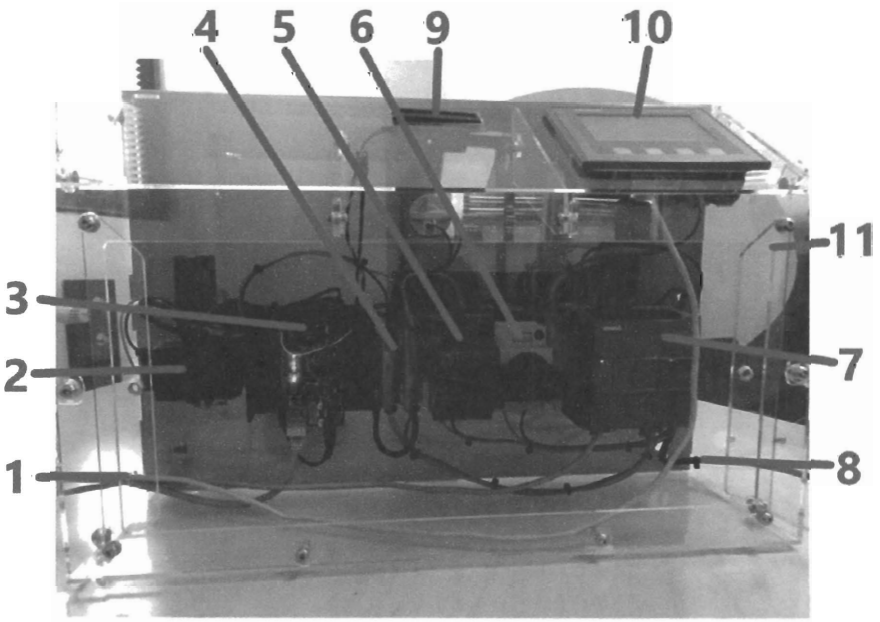
4
5
6
9
10
11
3
2
7
1
8

Fig. 2

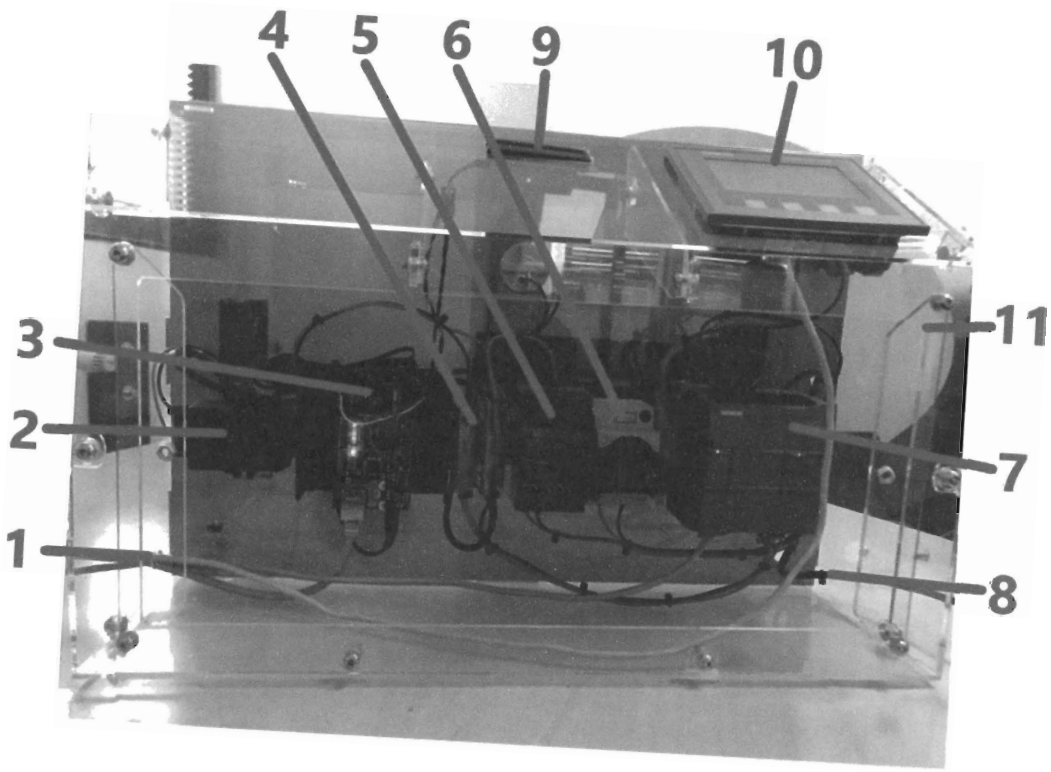

Fig. 3