Mobilna SCADA aplikacija u virtuelizovanom okruženju

Nikola Milutinović, Nikola Popović

***Apstrakt* — U radu se opisuju iskustva u virtuelizaciji SCADA aplikacije velikog obima. Virtuelizovanjem je postignuta mogućnost uvida u sve delove aplikacije izvan procesa upravljanja što znači korišćenje u svrhe analiziranja, testiranja i edukacije. U virtuelnom okruženju napravljen je jedinstven mobilni izvršni fajl korišćenjem VMware ThinApp programa. Ovako virtuelizovana EPKS R310 SCADA sistem može da se izvršava bez uobičajenog procesa instalacije, samo kopiranjem izvršnog fajla na neki od medija: fiksni disk ili eksterni, izmenljivi disk. Istestirano je i pokazano da aplikacija efikasno radi i direktno sa skladišnih medija odnosno eksternog diska čime je postignuta mobilnost aplikacije. Tretiran je aspekt sigurnosti kao faktor od bitnog interesa za funkcionisanje programskih sistema upravljanja u naftnoj industriji.**

***Ključne reči* — Virtuelizacija, virtuelna mašina, SCADA, zaštita informacija.**

I. Uvod

Svrha metoda i sredstava virtuelizacije možda najbolje može da sagleda u ovom trenutku kada je virus pod nazivom "Stuxnet" "napao" sisteme za upravljanje industrijskim procesima [1]. Prvi put su ugrožene instalacije čije oštećenje može da izazove posledice velikih razmera - u već poznatim slučajevima porede se sa efektima upotrebe atomskog oružja. Drugi, jednako značajan aspekt problema je da se više ne pominju talentovani hakeri ili teroristi kao pojedinci ili vrlo male grupe. Sada se već govori o upotrebi jedinica za informaciono ratovanje koje se obično organizuju na državnom nivou.

Oskudne i površne informacije koje većinom potiču iz štampe ukazuju da je Internet odigrao svoju negativnu ulogu. Uglavnom su napadnuti računari menadžera u postrojenjima što može da bude indikacija da su ipak imali pristup internetu. Nisu jasne ni informacije da su napadnuti i računari u drugim zemljama [2] a pominje se cifra reda 30.000 računara. Teško je prihvatiti stav da je virus koji napada SCADA sisteme predvidjen i za napad na računare no-name korisnika. U tekstu [2] ne daje se detaljnija specifikacija kakvi računari odnosno sistemi su napadnuti, niti je to moguće da se proveri. Pretežno su napadnuti sistemi u nerazvijenim zemljama što može da se tumači ili kao problem niskog nivoa znanja osoblja na industrijskim instalacijama ili kao posledica isporuke zastarele opreme. Nije neopravdana pretpostavka da se takvim (dez)informacijama maskiraju stvarni pravci i obim napada na veći broj industrijskih postojenja za koje će tek da se sazna (da li su uopšte i napadnuti drugi računarski sistemi?). U pitanju su investicije izuzetno velikog obima i izuzetno velikog značaja. Virus za napad na softverski kompleks kakav je SCADA u svakom slučaju ne može da bude malog fizičkog obima. Na osnovu vremena koje je proteklo od detekcije anomalija (jun 2010) može se pretpostaviti da je u pitanju distribuirani sistem - virus čije su komponente manjeg obima dislocirane i skrivene na više mesta sa namerom da se u zadatim periodima reorganizuju u kompletan virus. Jedan nemački stručnjak ispravno kaže da se ne treba plašiti "Stuxnet-a" već "sledeće generacije".

Treći aspekt koji mora da se ponovo oceni je sistem zaštite informacija i informacione infrastrukture industrijskih postrojenja. I u ovom slučaju su zatajili sistem administratori i administratori mreža. Ponovo se pokazuje da je čovek najslabija karika u lancu zaštite.

Neophodno je da se pristupi veoma obimnim i detaljnim ispitivanjima kapaciteta procesa virtuelizacije i svih virtuelizovanih segmenata. Naime, pretpostavka je da su proizvođači virtuelnih mašina testiranja izvodili na najmasovnije korišćenim periferijama i respektivnim drajverima [3]. Industrijska elektronika i informatika je srazmerno specifična i virtuelizovane aplikacije tek moraju da prođu sveobuhvatne faze testiranja pre aktiviranja u pogonu. Naprimer, Xenocode model virtuelizacije [4], virtuelizuje samo user-mode karakteristike operativnog sistema što obezbeđuje kompaktne, efikasne virtuelizovane aplikacije koje bi odgovarale SCADA real-time režimu rada. Medjutim, SCADA po definiciji zahteva čitav spektar drajvera za različite uređaje i/ili drugi non-user-mode softver tako da je nužna primena modela hardverske virtuelizacije.

Dosadašnji hardversko-softverski sistemi zaštite su se uglavnom zasnivali na primeni slojeva više različitih operativnih sistema [5] kao i naravno na serijama firewall i drugih odgovarajućih konstrukcija zaštite [6]. Poslednjih godina standardizacija virtuelnih mašina i metoda izrade virtuelizovanih aplikacija formira suštinski novi zaštitni sloj nezavisno od njihove osnovne namene. U ovom tekstu se daje skica procedura koje se testiraju u cilju razvoja novih metoda povećanja bezbednosti SCADA sistema i testiranja raspoloživih aktuelnih softverskih alata.

Nikola Milutinović, Vlatacom d.o.o.; (telefon: +381-11-3771113, e-mail: nikola.milutinovic@vlatacom.com).

Nikola B. Popović, Ministarstvo spoljnih poslova Republike Srbije, Kneza Miloša 24-26, 11000 Beograd, Srbija; (e-mail: nipopo@afrodita.rcub.bg.ac.rs, nikola.popovic@mfa.rs).

II. OPIS SISTEMA

Informaciona infrastruktura industrijskih postrojenja je u većini slučajeva statična odnosno odnosno uklapa se u fizičku strukturu postrojenja. Novija tehnička rešenja koja se oslanjaju na WEB tehnologije su sa nešto većim kapacitetom mobilnosti. Uvodjenje virtuelnih mašina daje mogućnost za suštinski veći stepen mobilnosti softverskog dela sistema upravljanja procesima. Naime hardverski sloj koji je vezan za fizičke uređaje i dalje ostaje statičan ali se zato povećavaju kapaciteti pristupa tim uredjajima sa različitih lokacija i izborom različitih informacionih puteva (wireless networks itd.).

Za eksperiment virtuelizacije izabrana je Honeywell-ova SCADA aplikacija Experion Process Knowledge System - EPKS R310 (Slika 1.). U pitanju je integrisano programsko i konfiguraciono okruženje uključujući, servere, radne stanice i kontrolere C300 i Series C I/O. Po saznanju autora, instaliran je vrlo uspešno u mnogobrojnim zemljama širom sveta posebno u regionima Bliskog Istoka, Severna Afrike i Kine, uglavnom na postrojenjima za eksploataciju nafte i gasa. Radi se o vrlo značajnom i prestižnom proizvodjaču kontrolnih sistema i opreme, kako hardvera tako i softvera a trenutno je najzastupljeniji u oblasti eksploatacije nafte.

Kontrolni sistem za vodjenje LPG (Liquid Petrol Gas) postrojenja u Zueitina Oil Company, Libya je od skora Honeywell EPKS R310. Sastoji se od redundantnih kontrolera, servera i više konzola i radnih stanica, Fault Tolerant Ethernet-a i druge opreme. Na servere su povezani i nezavisni sistemi drugih proizvodjača kao Enraf sistem za merenje nivoa i drugih parametara u tankovima za odlaganje tečnog gasa, Daniel-Emerson Metering System za precizno merenje isporučenih količina gasa ka tankerima i nezavisni Emergency Shut Down system za bezbedno zaustavljanje pogona u havarijskim uslovima. U sistemu je aktivno vise od 3000 tagova. U toku razvoja sistema i sada u toku održavanja kao nezaobilazna alatka koristi se virtuelizacija. Prethodni kontrolni sistem ORSI CUBE zamenjen je u toku 4 meseca “on line” za koje vreme je postrojenje neprekidno radilo. To znači da svi razvoji i testovi i dileme nisu mogli da budu probani i razvijani na licenciranom i instaliranom EPKS softveru koji je svo vreme vodio postrojenje u početku u manjem procentu paralelno a ORSI Sistemom, a kasnije u potpunosti. Svi testovi i razvoji programa su vršeni isključivo na identičnom softveru instaliranom u okviru jedne VM jer nije bilo moguće napraviti identičnu instalaciju realnog softvera na oskudnom hardveru i u okviru jedne licence sem u VM. U okviru te instalacije nalazila se i simulacija kontrolera, a simulacija I/O varijabli vršila se dodatnim CM (Control Module), SIMULINK-om kroz mrežu itd. Danas, u periodu kada sistem pripada održavanju kompanije, sve promene, dorade ili otlkanjanje bagova prvo se pažljivo ispitaju na istoj VM sa EPKS instalacijom i realnim projektom . Ovakve situacije nakon isporuke i prijema (commissioning) sistema su mnogobrojne u prvih godinu dana i ne postoji drugi način da se to efikasno uradi sem na VM.

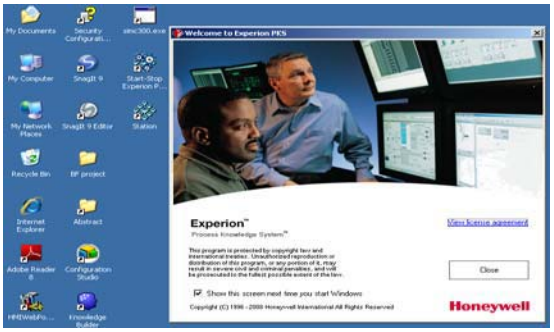
Objedinjeno upravljačko oruđe, programsko okruženje je Configuration studio. Glavne komponente su Control Builder za razvoj kontrolnih modula za pojedinačne tagove - pointe i HMIWeb Display Builder za razvoj grafičkog upravljačkog interfejsa (Slika 2.). Tu je smeštena konfiguracija servera i radnih stanica različitih tipova. U osnovnoj Experion sistemskoj topologiji serveri i procesni kontroleri dele jednu globalnu bazu.

Podržava redundansu servera, mreže i kontrolera. FTE - Fault Tolerant Ethernet je Honeywell-ov koncept redundantne mreže.

Interfejs prema širokoj paleti kontrolera i protokola drugih proizvođača. Allen Bradley, Siemens, Modicon. EPKS uključuje Honeywell-ove C200, C300 i ACE kontrolere. ACE - Application Control Environment je tipično eksterni kompjuter koji zamenjuje funkcije kontrolera. EPKS može takođe uključivati i SCADA uređaje koji mogu sadržavati serijske konekcije RS232, RS485, ControlNet konekcije, Ethernet interfejs, na primer MODBUS TCP. Quick Builder u okviru Configuration Studija omogućava integraciju SCADA tagova sa uređaja drugih proizvođača u jednu globalnu bazu.

Simulaciono upravljačko okruženje (SCE) omogućava razvoj upravljačkog sistema bez prisustva potrebne hardverske opreme, kontrolera i konekcija ka procesu.

Virtualizacija EPKS softverskog paketa omogućava mobilnost celokupnog Experion programskog okruženja nezavisno od operativnog sistema, kontrolera i procesa (Slika 1.). U okviru EPKS obavezno je instaliran simulacioni paket R300 za simulaciju C300 kontrolera i distribuiranih I/O kartica Honeywell serije C. Dodatno je instaliran i OperTune paket za podešavanje PID petlji, a koji se ponaša kao OPC klijent. EPKS server ima bidirekcionu vezu, razmenu podataka izmedju EPKS dB i sistema drugih proizvodjača. OPC server omogućava pristup Honeywell dB (ERDB/EMDB). OPC Integrator mapira tagove u lokalnoj dB ka drugim OPC serverima radi čitanja i upisivanja.

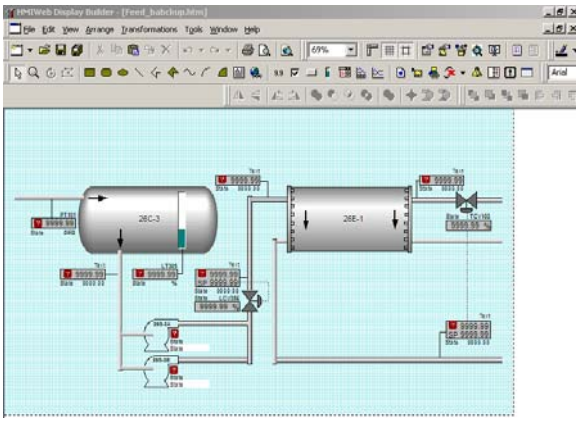


Slika 1. Uvodni ekran SCADA aplikacije startovan u sklopu virtuelne mašine Windows Server 2003

Primećena su pojedina ograničenja nastala uvođenjem simulacije kao na primer da se ne može koristiti redundantna topologija. Ali obzirom da je simulacija namenjena isključivo za treniranje i offline razvoj i provere to i nije ograničenje. Zatim u realnom sistemu se mogu uvoditi više kontrolera koji dele procesne ulaze i

izlaze što u simulaciji nije podržano.

Naravno posebna pažnja posvećena je simulaciji procesa odnosno ulaznih i izlaznih varijabli. To je ostvareno tako što su I/O blokovi digitalni ili analogni zamenjivani posebnim kontrolnim modulima ili posebnim funkcionalnim blokovima u okviru određenog kontrolnog modula. Ovi funkcionalni blokovi uvodili su matematičke formule, izraze koji su pretstavljali simulaciju realnih protoka, promene nivoa, pritisaka i temperatura kao i procenat otvorenosti kontrolnih ventila u kontrolnim PID petljama. Takođe dodavani su flagovi i dodatne veze koje su omogućavale automatsko uključivanje i isključivanje pumpi, kompresora ili otvaranje i zatvaranje ventila. Posebno je probana i simulacija procesnih varijabli pomoću MatLab SIMULINK-a. Pri tome SIMULINK nije obavezno instaliran u okviru jedne VM. U našem slučaju instalacija i konekcija je bila eksterna sa host kompjuter, a za povezivanje je korišćena OPC integracija. U ovom slušaju u EPKS Control Builderu nije potrebno raditi izmene zato što se spoljna simulacija procesnih varijabli konektuje direktno sa/na SIMULINK na I/O analogne ili digitalne ulaze EPKS hardvera.



Slika 2. Prikaz segmenta Display Buildera sa modelom

Formiranje virtuelne mašine izvršeno je programom firme VMware Inc. - VMware v.6.5.2. Za rad aplikacije pod virtuelnom mašinom korišćen je operativni sistem Windows Server 2003. U okruženju virtuelne mašine instaliran je SCADA softver firme Honeywell Experion PKS R301 a zatim formirana virtuelizovana aplikacija primenom programa Vmware ThinApp v.4.1.

Osnovni podaci o dimenzijama virtuelizovane aplikacije su sledeći:

- Virtuelna mašina sa instaliranom aplikacijom zauzima oko 18 GB
- Aplikacija u okviru virtuelne mašine zauzima oko 7.5 GB

Testiranja instalacije su izvršena na standardnoj radnoj stanici kao i na prenosnom računaru. Preporučljiva je RAM memorija od barem 4 GB. Virtuelizovana aplikacija može da se pokrene i na notebook računaru Sony VAIO sa 1GB RAM ali je rad značajno usporen. U ovom slučaju smo uočili i određene probleme u startovanju potrebnih servisa (sa prefiksom Experion). Naime iako su svi dodatni servisi podešeni za automatsko startovanje 8 servisa se nije startovalo već su morali da budu startovani naknadno. Ove anomalije zahtevaju dodatna testiranja i ispitivanja uzroka problema – da li je u pitanju uzrok vezan za rad pod virtuelnom mašinom ili potiče iz same aplikacije.

O širem korišćenju virtuelizovanih aplikacija, u operativnom okruženju, još uvek ne postoji dovoljno preciznih informacija. Verovatni uzrok je u tome što u slučaju desktop virtuelne mašine postoji određeno kašnjenje koje zavisi kako od vrste hardvera (procesora) tako i od same vrste virtuelne mašine (hardverska virtuelizacija itd.). Same virtuelne mašine su u ovom trenutku projektovane prema domenu opšte primene računara a SCADA aplikacije spadaju u znatno uži domen industrijskih upravljačkih sistema.

III. POUZDANOST SISTEMA I ZAŠTITA SISTEMA

Pošto je u pitanju softverska aplikacija koja se koristi u fizički velikim objektima podrazumeva se korišćenje računarskih mreža u različitim formama. Takodje se u procesu implementacije i održavanja prirodno pojavljuje veliki broj izvođača i podizvođača. Pomenuti napad na SCADA sistem [2] ostavlja utisak prisutnosti grešaka u upravljanju projektom posmatrane instalacije.

Podaci iz literature [6] (stanje iz 2006 godine) pokazuju da broj prijavljenih napada na SCADA sisteme raste sa 2 u 2001 godini, na 10 objavljenih incidenata u 2003 godini. Za razmišljanje je procena istraživača da se samo jedan od 10 SCADA bezbednosnih incidenata prijavljuje. U većini slučajeva, organizacije ne prijavljuju napade da bi se izbegao loš publicicte i gubljenje poverenja u sposobnost upravljanja posmatrane organizacije.

Istraživanja [6] (str. 99) ukazuju na povećanje broja bezbednosnih incidenata iz spoljašnjih izvora kroz korišćenje IT tehnologija i standard kao što su Microsoft Windows, Ethernet, Web servisi i uspostavljanje konekcija između SCADA mreže i poslovnog IT okruženja. Glavni elementi rizika za SCADA sistema su sledeći:

- Konekcije na dodatne , moguće bezbednosno rizične mreže
- Korišćenje standardnih hardverskih platformi sa poznatim bezbednosnim rizicima
- Korišćenje standardnog softvera sa poznatim bezbednosnim rizicima
- Ostale spoljašnje tj udaljene moguće rizične konekcije
- Deterministički zahtevi u domenu obrade podataka u realnom vremenu koji su protivrečni sa kontrolama informacione bezbednosti a koje izazivaju kašnjenja u obradi (delay time)

Nezavisno od tekućih ograničenja virtuelnih mašina specifičnosti SCADA sistema su takve da je primena virtuelnih mašina neminovnost u ovoj oblasti. Osnovne specifičnosti su:

- SCADA system nužno mora da neprekidno

funkcioniše u zadatom opsegu vremena tj. sve dok traje process kojim upravlja

- Modeli koje koriste SCADA sistemi zasnivaju se na centralizovanoj bazi podataka. Replikacije baza podataka i recovery funkcije su veoma složene operacije u real-time aplikacijama.

Virtuelni serveri omogućavaju povoljniju organizaciju procesa kroz postojanje više paralelnih softverskih mašina. Prebacivanje radnih procesa sa jedne na drugu mašinu u slučaju potrebe je suštinski kraće. Primena virtuelnih desktop aplikacije je korisna u smislu potencijalnog odvajanja aplikacije od kontrolne sobe SCADA sistema. Kontrolna soba je sa stanovišta bezbednosti visoko rizična lokacija pošto integriše celinu svih funkcije SCADA sistema. "Virtuelizovana" kontrolna soba bi u principu omogućavala upravljanje celinom sistema sa terena odnosno relaksiranje veze upravljačkih funkcija i fizičke infrastrukture.

Sa aspekta bezbednosti virtuelizacija SCADA aplikacija može da komplikuje napad na zadati sistem. Mobilnost aplikacije omogućava odvajanje od zadate fizičke lokacije u računarskoj mreži). To je razlog zbog koga je ovaj rad posebno vezan za korišćenje desktop virtuelnih mašina. Uvođenje novog međusloja – operativnog sistema virtuelne mašine - koji se do sada uglavnom obezbeđivao slojeve mašina sa različitim operativnim sistemima (UNIX i Windows). Slično tome omogućeno je i uvođenje virtuelnih računarskih mreža u sklopu postojećih klasičnih računarskih mreža.

IV. ZAKLJUČAK

Sa aspekta namene SCADA sistema koncept virtuelizacije aplikacija predstavlja mogućnost za suštinsko povećanje bezbednosti ali i fleksibilnosti odnosno pouzdanosti sistema. Mobilnost ovakvih aplikacija olakšava upravljanje procesima u industriji koji se odvijaju na skupu složenih objekata, prostorno lociranih na različitoj udaljenosti od komandne sobe i servera. Potreba za potpuno bezbednim radom i očuvanjem podataka neophodnih za neprekidan tok procesa uslovljava virtuelizaciju kao nezaobilaznu tehnologiju u korišćenju SCADA aplikacija u naftnoj industriji. Mobilnom virtuelizovanom SCADA-om obavlja se lakše i bezbednije testiranje vrednosti parametara sistema, proučavanje funkcionisanja pojedinih rizičnih komponenti, detektovanje i otklanjanje grešaka i saniranje otkaza. Dalje istraživanje u domenu fault tolerant sistema je u toku..

REFERENCE

[1] Nicolas Falliere, Stuxnet Introduces the First Known Rootkit for Industrial Control Systems, Symantec Corporation, 06.08.2010, dostupno na: http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices

[2] Jarrad Shearer, W32.Stuxnet, Symantec Corporation, 17.09.2010, dostupno na: http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

[2] Nikola Milutinović, Nikola Popović, Posebne pogodnosti u radu sa perifernim uredjajima u VMware okruženju, 17. Telekomunikacioni forum Telfor 2009, nov. 2009, Beograd

[3] Xenocode app virtualization technology, Xenocode Inc., 2009, dostupno na: http://www.xenocode.com/Technology/

[4] Nikola Popović, Julijana Mirčevski, Odnos host i guest operativnih sistema u VMware okruženju, 17. Telekomunikacioni forum Telfor 2009, nov. 2009, Beograd

[5] R.R. Krutz, *Securing SCADA Systems,*Indianapolis, Wiley Publishing, Inc., 2006,

THE MOBILE SCADA APPLICATION IN THE VIRTUALIZED ENVIRONMENT

***Abstract* — In the paper the experiences in virtualization of the large scale SCADA application are described. Through virtualization the introduction possibility in all part of application without control process that mind the using in analyzing, testing and education purpose was reached. In virtual environment it is build the single executable file by using VMware ThinApp program. Such virtualized EPKS R310 SCADA system can be executed without usual installation process, only with the executable file copyng into storage media, such as: HDD or removable disc. It is proved and shown that the application is running efficently directly from storage devices i.e. external disc and with that is realized the application mobility. The security aspect is considered also as a significant factor of the control program system in oil industry.**

***Keywords* — Virtualization, virtual machine, SCADA, information security**