Зборник радова Факултета техничких наука, Нови Сад

UDK: 004.41
DOI: https://doi.org/10.24867/13BE30Tosic

РАЗВОЈ И ИНТЕГРАЦИЈА *SIEM* СОФТВЕРСКОГ РЕШЕЊА У *SCADA* СИСТЕМЕ

DEVELOPMENT AND INTEGRATION OF SIEM SOFTWARE SOLUTION INTO SCADA SYSTEMS

Ђорђе Тошић, *Факултет техничких наука, Нови Сад*

Област – ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *У раду су описане сајбер претње по сигурност критичних инфраструктура са акцентом на SCADA системе. Поред теоријских основа рада, имплементирана је апликација која у себи садржи SIEM софтверско решење.*

Кључне речи: *Критичне инфраструктуре, SCADA, SIEM, DDoS, сајбер напади*

Abstract – *The paper describes cyber threats to the security of critical infrastructures with an emphasis on SCADA systems. In addition to the theoretical foundations of the work, an application containing a SIEM software solution has been implemented.*

Keywords: *Critical infrastructures, SCADA, SIEM, DdoS, cyber attacks*

1. УВОД

Сајбер систем представља кичму критичних инфраструктура, што значи да било какав компромис сајбер система могао би имати значајан утицај на поуздан и безбедан рад физичких система који се на њега ослањају. Фокус овог рада је на сајбер сигурности електроенергетских инфраструктура.

У раду су описани типични сајбер напади на критчне инфраструктуре, са акцентом на опис најучесталијих напада на *SCADA* системе. Задатак мастер рада јесте имплементација и интеграција *SIEM* софтвера у *DERMS* апликацији, која је имплементирана током мастер студија и њене фунционалности су укратко описане у овом раду.

За потребе тестирања симулирани су сајбер напади(*DDoS* напад, подметање неисправног модела). Циљ је имплементирати *SIEM* компоненту која ће бити способна да препозна такве нападе, и да обавести корисника путем корисничког интерфејса.

Пре саме имплементације *SIEM* компоненте, направљен је *threat model DERMS* апликације, како би се анализирале слабе тачке система и места која могу бити мета потенцијалних сајбер напада.

Напомена:
Овај рад је проистекао је из мастер рада чији ментор је био др Дарко Чапко, ванр. проф.

2. ОПИС КОРИШЋЕНИХ ТЕХНОЛОГИЈА И АЛАТА

У овом поглављу ће бити укратко описане коришћене технологије и алати.

• ***Microsoft Visual Studio*** је софтверско развојно окружење које омогућава развој апликација за све *Microsoft*-ове платформе. Садржи следеће алате: *code editor* за писање кода и аутоматско проналажење синтаксних грешака у коду, *debugger* за проналазак свих типова грешака у коду и њихово исправљање, *code profiler* алат за профајлирање кода(путем њега се може проверити како се рукује меморијом, какве су перформансе програма итд.) као и алате за дизајнирање и алате који помажу програмеру да се лакше снађе у *Visual studiu* попут *Solution Explorer-a, Object Browser* итд.

• ***C#*** је језик из фамилије *C* језика, који је у потпуности базиран на принципима ООП (Објектно орјентисаног програмирања).

•***XAML****(Extensible Application Markup Language)* је маркуп језик чија је намена поједностављење креирања *UI* за интеракцију са корисником у *.NET Framework* апликацијама. Погодан је за креирање и иницијализацију објеката. Поента *XAML-a,* је да омогући програмерима да раде са експертима из других области.

• ***.NET*** представља програмско окружење које служи за лакши развој програма. Садржи *CLR (Common Language Runtime)* који извршава написане програме, који брине о капацитету процесора, рукује заузећем меморије, управља изузецима и обезбеђује безбедност апликације.

• ***WPF****(Windows Presentation Foundation)* је графички подсистем за рендеровање корисничког интерфејса у апликацијама заснованим на *Windows-u.* Представља технологију за прављење клијентских апликација на *Windows* платформи, која нуди многобројне опције за подешавање изгледа апликације.

• ***Microsoft Threat Modeling Tool*** је кључни елемент *Microsoft Security Development Lifecycle(SDL).* Омогућава софтвер архитектама да идентификују и ублаже потенцијалне сигурносне проблеме, пре него што дође до искоришћавања сигурносних проблема. Рано уочени проблеми у великој мери смањују укупне трошкове и време утрошено на развој софтвера.

3. ОПИС ОСНОВНИХ САЈБЕР НАПАДА НА КРИТИЧНЕ ИНФРАСТУКТУРЕ

Континуирано функционисање земаља, влада, међународних организација, корпорација и многих јавних служби често зависи од несметаности приступа критичној инфраструктури која може бити дефинисана као системи и имовина, физичка или виртуелна, која је толико витална, па би онеспособљеност ових система или уништавање имало велики утицај на националну, економску или оперативну сигурност, као и на јавно здравље или безбедност.

3.1. Сајбер напади на SCADA системе

Када је реч о нападима на критичне инфраструктуре, мета напада често представљају *SCADA* системи. Претње *SCADA* системима су класификоване као интерне и спољне претње[1]. Интерне претње вребају од људи који су запослени у организацији, који због тога имају већи физички приступ поверљивим и критичним информацијама *SCADA* система. Напади од стране нападача који немају приступ пословним објектима третирају се као спољне претње. Обе врсте претњи су једнако опасне.

Сигурност *SCADA* система зависи од слабих сигурносних тачки система. Уобичајена претња је убацивање малвера путем преносивих уређаја за складиштење и малициозним прилозима који се шаљу електронском поштом. Недовољно заштићене бежичне приступне тачке у систему су потенцијална улазна тачка. Већина *SCADA* мрежа повезана је са корпоративним мрежама помоћу *Virtual Private Networks (VPN).* Ако нападач има приступ корпоративној мрежи, он може приступити *SCADA* мрежи релативно лако. Зато је веома важно обезбедити корпоративну мрежу, како се њој не би могло приступити преко несигурних веза [2].

3.1.1. Сајбер напади на хардвер *SCADA* система

Претње по хардвер *SCADA* система јесу задобијање даљинске контроле над уређајима од стране нападача. Ови напади могу проузроковати да уређаји откажу при ниским вредностима, или да се неки аларм не укључи када би требао. Друга могућност напада јесте да нападач неовлашћено задобије приступ, и да након тога мења вредности које се приказују оператеру. У том случају могло би се десити да оператер не буде свестан да се одређени аларм упалио, и да указује на опасност, самим тим би изостала реакција оператера, што би могло да проузрокује хаварију система.

Главни проблем код превенције сајбер напада на хардвер *SCADA* система представља контрола приступа. Као један од напада који користе поменуту слабу тачку, и који се често догађају, јесу тзв. „*doorknob-rattling*“ напад. Нападач комбинује неколико уобичајених комбинација корисничког имена и лозинке, на неколико рачунара, што резултује врло малим бројем промашаја, и тако нападач не пробије дозвољени број покушаја, и приступи систему. Овај напад може остати непримећен, осим ако се подаци који се односе на пријаву не сакупљају и не проверавају на „*doorknob-rattling*“ напад.

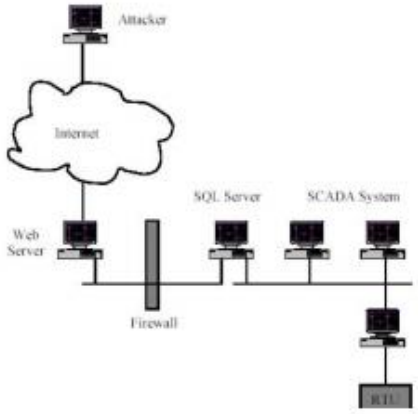
3.1.2. Сајбер напади на софтвер *SCADA* система

Buffer Overflow **–** многи напади се своде на то да проузрокују *Buffer Overflow* као средство које ће евентуално проузроковати неуобичајен рад програма. Неке опште методе за постизање *Buffer Overflow-a* су *stack smashing* и манипулација показивачем фунције.

Ефекти оваквих напада су ресетовање лозинки, модификација података, инсталирање малициозног кода и друге. *SCADA* уређаји који се налазе у пољу се јако ретко рестартују, због тога, посебно у застарелим мрежама долази до фрагментације меморије, која доводи до застоја програма [3].

SQL Injection – већина малих и индустријских база података користи *SQL* исказа за модификацију и манипулацију подацима. Данас када постоји приступ *SCADA* системима преко интернета, *SQL Injection*, као један од најчешћих напада на интернету, има велики утицај у креирању сигурности *SCADA* система [4].

SQL Injection напад дешава се када је нападачу омогућена модификација уноса података преко *Web* апликације, која не успе да препозна модификовани унос, и тако нападач убаци нежељене изразе у *SQL* упит. Намерне модификације базе података могу проузроковати катастрофалне последице. Пример *SQL Injection* напада приказан је на слици 1.



Слика 1. *SQL Injection напад*

3.1.3. Комуникациони сајбер напади на *SCADA* системе

Нападе на комуникациони стек, који могу нанети штету *SCADA* системима, можемо поделити на: нападе на мрежни слој, транспортни слој, апликативни слој и на нападе у зависности од протокола који *SCADA* системи користе.

Distributed Denial of Service (DDoS attack) – Напади који имају за циљ да преоптерете и тако онемогуће услугу сервера. Зарад ефикаснијих напада, користе се групе рачунара тзв. *„botnet“*. Термин *botnet* представља групу рачунара који су заражени малициозним садржајем, и под контролом су нападача. Методе на који се рачунари из *botnet* мреже заразе су: тројанац у комбинацији са *backdoor*, или путем социјалног инжењеринга.

Примери *DDoS* напада су [5]:

- *SYN Flood* – искориштава слабости *TCP three-way handshake* конекције. Сервер добија *SYN* поруку да започне „*handshake"*. Сервер затим узвраћа *ACK* поруку, страни која је иницирала почетак комуникације, која затим прекида комуникацију. Након тога страна која иницирала конекцију прекида комуникацију, а сервер остаје загушен истим захтевима, који резултују тајмаутом и тако загушују сервер.
- *Zero-day DDoS attack* – искориштава рањивости система, слабе тачке, за које још увек нису направљене закрпе.
- *Ping of Death* – манипулише *IP* протоколом, шаље пингове, са циљем да онеспособи сервер. У прошлости је био заступљен, данас се ретко среће.
- *Smurf Attack* - манипулише *IP* протоколом и *ICMP* протоколом користећи малициозни софтвер звани *Smurf*. Лажира *IP* адресу, и помоћу *ICMP* протокола шаље пингове.

3.2. Најпознатији напади на критичне инфраструктуре

У данашњици веома моћно оружје у сукобима између држава постали су сајбер напади. Најпознатији напади на критичне инфраструктуре у скоријој историју су [6]:

***Heartland Payment Systems* 2008. године** – хакереска група „*Shadowcrew fame*" која је починила многобројна дела из групе сајбер криминала, украла је око 100 милиона бројева кредитних картица, чиме је нанела штету од 140 милиона долара.

***Stuxnet* 2010. године** - Прво сајбер оружје које је способно да изазове напад који изазива кинетичко дејство јесте вирус назван *Stuxnet*, који је развијен и изграђен у информатичким лабораторијама *NSA*, у сарадњи *CIA* и израелске обавештајне службе. Био је намењен да физички уништи опрему иранског нуклеарног објекта у Натанзу.

Под маском да преузима индустријску контролу над системом *SCADA*, софистицирани црв требало је да оштети око хиљаду центрифуга за обогаћивање нуклеарног материјала.

***Night Dragon* 2011. године** - У фебруару 2011. године компанија која се бави производњом антивирусног софтвера (*McAfee*) објавила је да су пет међународних енергетских и нафтних компанија биле мете комбинованих напада укључујући социјални инжењеринг, тројанце и друге нападе. Потврђено је да су напади под називом „*Night* Dragon" трајали више од две године и верује се да су усмеравани из Кине.

***BlackEnergy* напад на електоенергетску мрежу Украјине 2015. године** – Напад је изведен тако што су нападачи слали *mail*-ove, са *Microsoft Office* документима, који када се отвори аутоматски зарази корисника. Напад је проузроковао да 1,4 милиона корисника остане без напајања електричном енергијом.

Сајбер напад на болницу у Лос Анђелесу 2016. године – Нападачи су успоставили контролу над базом података болнице, у којој су се налазиле информације о пацијентима, њихова историја болести, терапије које су примали.
Нападачи су шифровали податке и доктори нису могли да приступе бази без кључа. Нападачи су тражили 3,6 милиона долара за кључ.

4. МЕТОДИ ЗАШТИТЕ КРИТИЧНИХ ИНФРАСТРУКТУРА ОД САЈБЕР ПРЕТЊИ

Сајбер сигурност је најкритичнији аспект технолошки заснованог света. Све технологије које се заснивају на комуникационим и информационим системима зависне су од сајбер сигурности.
Јавни и приватни сектор сваке године троше огромне своте новца на технологије, сигурносне софтвере и хардвер уређаје који ће повећати сајбер сигурност у њиховим компанијама, али су ти системи и даље рањиви.

4.1. *SIEM* софтвер

SIEM систем је сложена група технологија, дизајнирана да пружи визију и јасан преглед система у којем се користи. Од велике је користи аналитичарима сигурности система и *IT* администраторима.
Пружа холистички поглед на оно што се дешава на мрежи у реалном времену, и помаже *IT* тимовима да буду активнији у решавању сигурносних претњи.

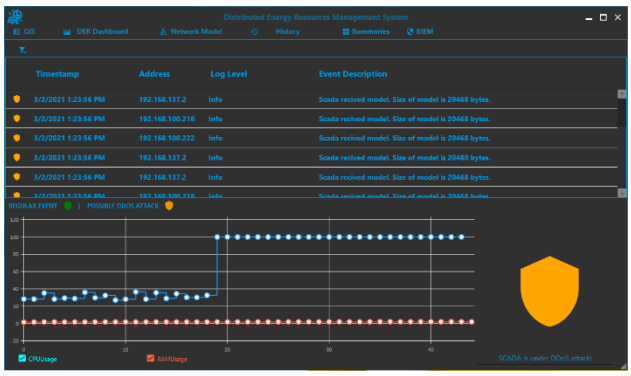
Неке од основних функционалности су:
- *Log management*
- *IT regulatory compliance*
- *Event correlation*
- *Active response*
- *Endpoint security*

5. ИМПЛЕМЕНТАЦИЈА И ИНТЕГРАЦИЈА *SIEM* ПРОГРАМСКОГ РЕШЕЊА У *DERMS* АПЛИКАЦИЈУ

У овом поглављу биће описано *SIEM* програмско решење и његове фунционалности у оквиру *DERMS* апликације. *SIEM* компонента прикупља лог фајлове у које се бележи рад осталих сервиса, прикупљене податке анализира и по унапред дефинисаним правилима проверава да ли је дошло до неког сајбер напада, или неке друге неуобичајене активности.

5.1. Детекција и последице *DDoS* напада

На слици 2. приказано је стање *SCADA* сервиса током *DDoS* напада. *SIEM* компонента функционише тако што на одређени временски период чита информације из лог фајлова.
Пошто се подаци уписују у логове константно, и после гашења апликације, информације у логовоима остају трајно у њима. Зарад тога учитавају се информације из логова, само које су уписане у току рада апликације.



Слика 2. *Детекција DDoS напада*

Као што је приказано на слици 2, на графику на којем се приказује оптерећеност *CPU* и *RAM*, уочава се период пре почетка *DDoS* напада и након почетка симулације *DDoS* напада. Пре напада процесор није много оптерећен, и те промене оптерећености процесора не варирају много кроз време. Након покретања симулације *DDoS* напада, *SIEM* компонента региструје велики број конекција са различитих машина, које у истом тренутку шаљу податке на *SCADA* сервис. У том тренутку оптерећеност процесора расте на 100%, и *SIEM* компонента, путем корисничког интерфејса алармира корисника да је у току *DDoS* напад.

6. МАШИНСКО УЧЕЊЕ У *SIEM* СИСТЕМИМА

Машинско учење се односи на грану вештачке интелигенције. Машинско учење користи алгоритме вештачке интелигенције за учење из својих искустава током времена након почетног уноса података. Стога, машинско учење у *SIEM* системима узима правила и податке о сајбер сигурности, како би олакшало аналитику података о сигурности. Као резултат, може смањити напор или време утрошено на базичне задатке или чак и на оне софистицираније. Уколико се правилно конфигурише, машинско учење заправо може доносити одлуке на основу података које прима и у складу са тим променити понашање [7].

Машинско учење у *SIEM* системима може омогућити аналитику претњи и створити обавештења о ризику у реалном времену.

7. ЗАКЉУЧАК

Сајбер напади на критичне инфраструктуре су са дигитализацијом тих система постали свакодневница. Последице сајбер напада на критичне инфраструктуре могу бити катастрофалне. Поред огромне финансијске штете коју сајбер напади изазивају, постоји опасност и по људске животе, животну средину и друге аспекте живота. Из тих разлога неопходно је сигурност система подићи на највиши ниво. Софтверско решење *SIEM* се последњих две деценије истиче као моћан алат за детекцију и превенцију сајбер претњи, као и мониторинг целокупног система.

У раду је описан утицај *DDoS* напада на перформансе система и функционалност апликације. Након симулације напада уочава се пораст оптерећења процесора, док се оптерећење *RAM* меморије незнатно повећава. У току напада основне функционалности апликације било је отежано извршавати, команде које се шаљу на сервис погођен *DDoS* нападом нису успешно извршаване.

За разлику од *DDoS* напада, подметање неисправног модела није значајно утицало на перформансе система. Рад апликације, што се перформанси тиче, настављао се неометано. Последице напада огледале су се у различитим резултатима за исте елементе система, што јасно указује да модел није валидан, јер се резултати не подударају.

За даље усавршавање апликације засноване на *SIEM* софтверском решењу, алгоритми машинског учења би се могли имплементирати у такве системе. Тако би систем, на основу претходних сајбер напада, могао да детектује нове сајбер претње, без претходног дефинисања услова који асоцирају на поједини сајбер напад.

8. ЛИТЕРАТУРА

[1] W. T. Shaw, „Cybersecurity for SCADA Systems“, 2008.

[2] Siddharth Sridhar, G. Manimaran, “Data Integrity Attacks and their Impacts on SCADA Control System”, Department of Electrical and Computer Engineering Iowa State University, 2010.

[3] Siddharth Sridhar, G. Manimaran, „Data Integrity Attacks and their Impacts on SCADA Control System“, Department of Electrical and Computer Engineering Iowa State University

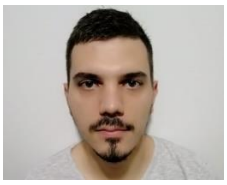
[4] T. Paukatong, „SCADA Security: A New Concerning Issue of an In-house EGAT-SCADA“, IEEE/PES Transmission and Distribution Conference & Exhibition: Asia and Pacific Dalian, China, 2005.

[5] Douligeris, Christos, and Aikaterini Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art." Computer Networks, 2004.

[6] Kim Zetter "Everything We Know About Ukraine's Power Plant Hack“. Wired, 2016.

[7] Anumol, E. T. "Use of machine learning algorithms with SIEM for attack prediction." Intelligent Computing, Communication and Devices. Springer, New Delhi, 2015.

Кратка биографија:



Ђорђе Тошић рођен је у Сремској Митровици 1996. године. Дипломирао је 2019. године на Факултету техничких наука, смер Примењено софтверско инжењерство, на којем исте године уписује мастер студије.