Зборник радова Факултета техничких наука, Нови Сад

UDK: 007.51
DOI: https://doi.org/10.24867/05TI02Tagliavia

СИГУРНОСТ И БЕЗБЕДНОСТ КОМУНИКАЦИЈЕ ИЗМЕЂУ КОНТРОЛНИХ ЦЕНТАРА НАДЗОРНО-УПРАВЉАЧКОГ СИСТЕМА

SECURE AND SAFE COMMUNICATION AMONG CONTROL CENTERS IN SCADA SYSTEM

Марко Таглиавиа, *Факултет техничких наука, Нови Сад*

Област – ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *У овом раду описана је реализација симулатора индустријског постројења, са комунукацијом преко ICCP протокола, развијеног ради тестирања SCADA система. Симулатор врши симулацију динамичких промена мерних величина, ишчитавање њихових вредности, али пре свега успоставу конекције између SCADA система и самог ICCP симулатора. Акценат је на безбедном успостављању комуникационог канала, као и на даљој безбедној комуникацији између два система.*

Кључне речи: *SCADA, ICCP, сигурност, безбедност*

Abstract –*This paper describes development of industrial plant simulator using ICCP protocol for purpose of testing of SCADA system. Simulator allows simulated dynamic changes of measured values, reading of their values, but first of all, establishing a connection between SCADA and ICCP simulator. The accent is on secure establishing of communication channel, and further secure communication between two systems, as well.*

Keywords: *SCADA, ICCP, safety, security*

1. УВОД

Данас је управљање помоћу рачунара неопходно у свим савременим индустријским постројењима и системима, и већина решења представља дистрибуирани управљачки систем са географски удаљеним и међусобно зависним деловима. Један тип таквих система су надзорно-управљачки системи (SCADA), који израстају у посебну категорију UMS (*Utility Management System*) намењену управљању у критичним инфраструктурним системима, попут система за снабдевање струјом, водом, гасом, телекомуникационих система, и сл. Контролни центри оваквих система су географски дислоцирани и управљање читавим системом се ослања на размену података између контролних центара. Изузетно је важно да ова комуникација буде безбедна како би се избегле несреће које могу настати. Стога, у данашњим дистрибуираним управљачким системима се велика пажња мора посветити сигурности и безбедности.

Cyber криминал је у последњој деценији у великој експанзији. Вредност информација је све већа, а самих информација је све више. Временом и ширењем, ствара се идеално окружење у којем *cyber* криминалци могу да украду податке или их учине невалидним и штетним. На пример, када би у систему критичне инфраструктуре само један параметар био погрешно прочитан, долази се до ситуације да оператер нема праву слику ситуације из реалног света. Тада он може издати команду која може угрозити људске животе. Да би се спречиле такве могућности, користе се безбедни комуникациони канали, а посебна пажња се посвећује безбедном преносу података кроз јавне комуникационе мреже, као и преносу података између удаљених делова, попут контролних центара. Постоје дефинисани комуникациони протколи који су погодни за комуникацију удаљених система.

ICCP (*Inter-Control Center Communication Protocol*) је протокол који се најчешће користи у поменуте сврхе. Поред безбедности, додатни проблем чине величина управљаног система, као и сложеност апликативне програмске подршке намењене управљању. У критичним инфраструктурама је захтевана висока расположивост надзорно-управљачких система, што резултује дугим и исцрпним тестирањима.

Могуће грешке настале током развоја или конфигурисања аквизиционо-управљачког система су недопустиве и треба их отклонити пре тестирања на реалном систему. Због тога се користе симулације, које се извршавају над програмским моделом физичког постројења. Оне се спроводе само у строго изолованим и контролисаним окружењима. Након успешне симулације долази се до пуштања система у погон.

Да би се решили претходно описани проблеми, овај рад предлаже употребу симулатора протокола који се користи за комуникацију између контролних центара у SCADA систему. Симулатор треба да обезбеди опонашање другог система у комуникацији, укључујући: иницијализацију, покретање комуникације са SCADA системом у складу са изабраним протоколом, подршку за руковање командама добијених од стране SCADA система и подршку за слање промена вредности тачака на удаљене уређаје. Посебан акценат решења ће бити стављен на безбедност саме комуникације.

2. РЕФЕРЕНТНА РЕШЕЊА

Свакако највећа несрећа која се догодила у предходних неколико деценија је она у Чернобилу. То је најупечатљивији пример SCADA система чији је квар изазвао катастрофу и енормне штете. Често се помиње као светски најгори нуклеарни инцидент.

НАПОМЕНА:
Овај рад проистекао је из мастер рада чији ментор је био др Александар Ердељан, ред. проф.

Један од фактора који стоји иза овог инцидента 1986. године јесте тим инжењера који су управљали системом.

Нешто скорији пример несреће у SCADA системима је Stuxnet. Овај чувени напад се десио у нуклеарној електрани у Ирану. Stuxnet је као мету имао специфичне SCADA системе које производи Siemens. Stuxnet напад је искористио 5 приступних тачака које су имале слабости [3].

Превенција оваквих догађаја је кључна. *Penetration* тестирање је један вид превенције испада, где се подразумева коришћење алата као што су: Nessus, Metasploit, Core IMPACT и сл. Њихова улога је да омогуће инжењерима задуженим за безбедност система да изведу тестне нападе на SCADA системе, односно да покушају да искористе њихове познате слабости. Поред наведених, у индустрији се користе и друга сложена софтверска решења, попут SIEM софтвера који у себи имају Anti-Virus, Firewall, IDS, IPS као и подршку за конфигурацију права приступа, слабости система итд.

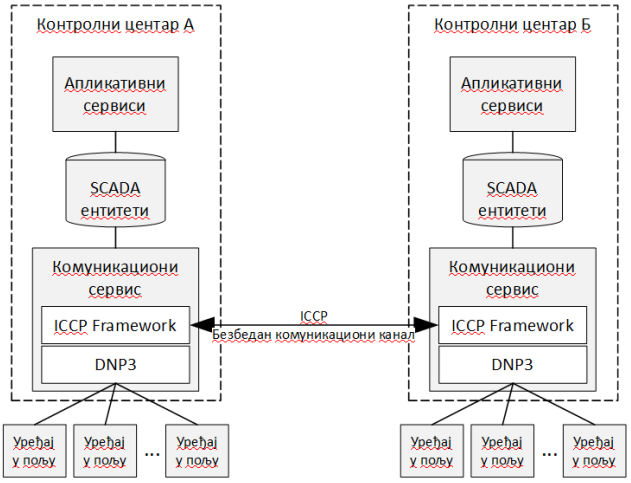
SCADA системи имају своје специфичности где је битна и ефикасност система. Нови начин за управљање криптографским кључевима који повећава ефикасност и сигурност комуникације надзорно управљачког система је описан у [2]. У предложеном решењу представљена је шема управљања кључем, где се користе две кључне фазе ажурирања: ажурирање кључа сесије и мастер освежавање кључа.

3. SCADA СИСТЕМ

SCADA је систем који служи за аутоматизацију општих процеса, односно који се користи за прикупљање података са сензора и инструмената лоцираних на удаљеним станицама и за пренос и приказивање тих података у централној станици у сврху надзора или управљања. Прикупљени подаци се обично посматрају на једном или више SCADA рачунара. SCADA систем у реалности може да прати и управља и до стотинама хиљада улазно-излазних вредности. Уобичајени аналогни сигнали које SCADA систем надзире (или управља) су нивои, температуре, притисци, брзине протока и брзине мотора. Типични дигитални сигнали за надзор (управљање) су прекидачи нивоа, прекидачи притиска, статус генератора, релеји и мотори. Целокупна опрема која се физички налази на мерним местима се назива поље. Сви сигнали који могу да буду мерени се везују за једну „тачку“, па се у даљем току комуникације размењују подаци о променама на тачкама за које су везани сигнали који мере неку вредност.

Прокотол представља скуп правила и конвенција за слање информација преко мреже. Посредством комуникационих протокола обезбеђује се успешна интеракција између удаљених процеса. Основне функције комуникационих протокола су контрола грешака и управљање током података у мрежи.

На пример, комуникациони протоколи у домену SCADA система у електроенергетици који се највише користе су DNP3, Modbus, IEC60870-5-104, и ICCP. Такви SCADA системи могу имати више контролних центара који покривају велику територију, те они размењују податке. Уређаји у пољу се деле по географски најближим контролним центрима. Типично, један контролни центар може другом да пошаље вредности својих сигнала, као и да прими команде из другог центра. На слици 1 је приказана архитектура SCADA система са два контролна центра.

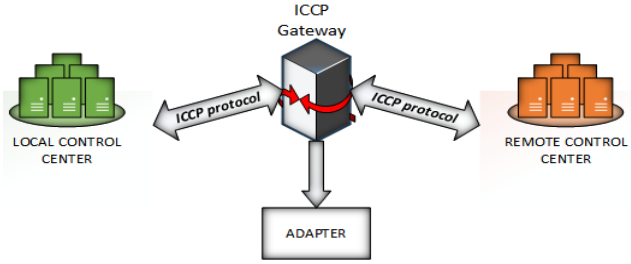


Слика 1. *SCADA систем са два контролна центра*

Видимо да два контролна центра имају своје апликативне и комуникационе сервисе, као и своје архитектуре база података. Контролни центри управљају уређајима у пољу који се налазе географски распоређени најближе њима. Два контролна центра успостављају комуникацију путем комуникационих сервиса при чему се отвара безбедан комуникациони канал. Путем овог канала се размењују поруке које су усклађене са ICCP стандардом.

4. ICCP ПРОТОКОЛ

ICCP (Inter-Control Center Communications Protocol) је међусистемски протокол који као учеснике комуникације има више контролних центара (може се наћи и под другим називима: IEC 60870-6 и TASE.2). Типично се употребљава за повезивање контролних центара аутономних SCADA система [1]. У једном једноставном примеру таквог система, локални и удаљени контролни центар су у комуникацији (слика 2). Они користе ICCP протокол како би свој саобраћај усмерили ка ICCP *Gateway*-у. Он има информације на коју адресу треба да проследи саобраћај. Поред тога, може постојати и *Adapter* који се користи да прилагоди поруке формату ICCP протокола.



Слика 2. ICCP *везе између* SCADA *система*

ICCP је базиран на архитектури *Client – Server*. Уколико имамо више контролних центара који комуницирају, у сваком моменту, сваки од њих може се

понашати као клијент и сервер. Сав пренос података потиче од захтева једног контролног центра који је у улози клијента, другом контролном центру који је у улози сервера, који поседује и управља подацима.

5. СИГУРНОСТ И БЕЗБЕДНОСТ SCADA СИСТЕМА

Са теоријског становишта, сигурност представља степен отпорности или заштите од „повреде“, односно нежељене ситуације. Постизањем довољно високог нивоа сигурности доводимо ресурсе од важности у стање где они нису угрожени и где не постоје претње по њих. Када говоримо о системима који користе рачунаре као управљачку подршку, ресурси представљају податке и физичке ентитете у систему.

Постизањем довољно високог нивоа сигурности долазимо у безбедно стање. Другим речима, безбедност представља стање заштићености од отказа, претње, грешке, незгоде, или повреде. Безбедношћу постижемо контролу над идентификованим опасностима са циљем достизања одговарајућег нивоа ризика.

Постоје бројне врсте безбедности, али су од највеће важности мере које треба предузети да би се умањиле потенцијалне физичке претње, као и дигиталне претње, које су са развојем технологије све учесталије. Највећи број напада на електроенергетске системе се дешава управо овим путем. Методе којима је могуће зауставити овакве претње или их ублажити су безбедни комуникациони канали, криптографија, Triple A, дигитални потписи и сертификати као и безбедносни протоколи.

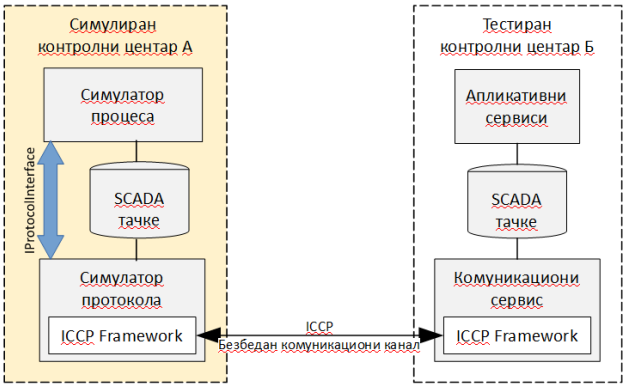
Безбедност контролног центра подразумева читав инжењерски тим који је посвећен само безбедности. Поред раније наведених метода, неопходно је и физички заштитити контролни центар постављањем баријера, надзорних камера, чувара и сл. и успоставити адекватне безбедносне процесе.

6. ПРЕДЛОГ РЕШЕЊА

Да би се SCADA систем са више контролних центара пустио у употребу неопходно је исцрпно тестирати целокупно решења укључујући и комуникацију између контролних центара. Стога се предлаже употреба симулатора надзираног и управљаног процеса, као и симулатора протокола да би се благовремено проверили конфигурација решења и очекивана функционланост. Стога су основне софтверске компоненте предложеног решења: симулатор процеса и симулатор протокола. Они симулирају понашање једног контролног центра са становишта другог (посматраног) контролног центра. Тиме се омогућава тестирање функционалности посматраног контролног центра пре него се успостави веза са стварним центром, укључујући и тестирање сигурности и безбедности система.

Симулатор процеса има улогу симулирања понашања дела система који се надзире из контролног центра, и у основи треба да израчуна вредности за тачке које реалан центар прикупља. Рад тог симулатора се заснива на симулационом моделу надзираног система, и он није предмет овог рада.

Симулатор протокола је заснован на ICCP протоколу, где су имплементиране методе за комуникацију тако да користе услуге симулатора процеса и формирају одговоре на ICCP упите из другог система. За имплементацију самог протокола је употребљена ICCP *Framework* библиотека. Поред интефејса за комуникацију ка другим контролним центрима, симулатор има додатни интерфејс за везу ка корисничком апликацијом, која има графички кориснички интерфејс да би се тестирале саме методе које обухватају првенствено иницијализацију, покретање и стопирање симулације.



Слика 3. *Архитектура решења*

Најбитније функционалности симулатора протокола су:

- конфигурисање симулатора
- креирање апликације која учитава ICCP функционалности из ICCP симулатора за потребе тестирања
- иницијализација ICCP*Framework*-а покретање и заустављање ICCP услуге
- читање локалних вредности
- приказ информација о локалним уређајима
- приказ информација о клијентским тачкама
- управљање клијентским уређајим
- механизми за безбедну иницијализацију и успоставу конекције
- механизми за безбедну комуникацију и размену саобраћаја између контролних центара
- моделске могућности за конфигурацију параметара који се тичу безбедности
- конфигурација сертификата и алгоритама који ће се користити приликом енкриптовања, дектриптовања и иницијалног *handshake*-а

Да би се размена података између контролних центара учинила сигурном и безбедном, успоставља се безбедан комуникациони канал, где се размењене поруке енкриптују и декриптују. Такав комуникациони канал је означен стрелицама са обе стране (Слика 3.).

У оквиру решења користе се дигитални сертификати, енкрипција, декрипција, Triple A, иницијални *handshake* као и TLS/SSL сигурносни протоколи. Читав процес потпомаже протокол библиотека која се налази у позадини ICCP *Framework*-а. Аутентификација, енкрипција, декрипција и иницијални *handshake* су ослоњени на успешну иницијализацију дигиталних сертификата.

Предложено решење се заснива на присутности три типа сертификата: *Root*, *Intermediate* и *Personal* (*End-entity*), где је *Root* сертификат увезан са *Intermediate*, док се *Personal* сертификат ослања на важећи *Root* сертификат. Ако било који од ова три сертификата није валидан, комплетна иницијализација комуникације није успешна, тако да постојање сва три исправна сертификата у оба система је оно што комуникацију између њих чини безбедном. Сертификати дефинишу алгоритме и механизме који ће бити коришћени у даљем току комуникације.

Предложено решење подржава све TLS/SSL верзије од 1.3 па на ниже (TLS верзија 1.3 је из 2018. године), тако да се могу повезати контролни центри у којима постоје и старији SCADA системи. При успостави конекције са симулатором протокола, користи се најнижа верзија коју обе стране подржавају.

Са становишта аутентификације, предложено решење омогућава успостављање конекције на три начина. То су: конекција са SSL аутентификацијом, MACE аутентификацијом и без аутентификације. Ако се користе прве две, саобраћај аутоматски мора бити енкриптован и декриптован од стране другог система. Конекција без аутентификације се користи само у тестне сврхе и ретко се налази у продукционим системима.

Када говоримо о ауторизацији, долазимо до специфичности саме имплементације решења. Приликом имплементације се врши имперсонификација у корисника који има права приступа за све акције у тестне сврхе. У продукционом систему, овакав вид ауторизације није дозвољен, те *security* тим има задатак да на рачунарима које запослени користе подеси само неопходна права приступа да могу успешно да заврше своје радне задатке.

Поред аутентификације и ауторизације, бележење историје акција чини безбедносни механизам Triple A. У оквиру овог решења, критичне акције се логују у посебне текстуалне фајлове на предефинисаним локацијама.

С’ обзиром на то да су приликом комуникације између два контролна центра овим решењем уведена многа проширења у комуникацији, неизбежан је пад перформанси по питању брзине комуникације. Са узорком од 100 секунди, просечан број промена вредности сигнала је износио 30000 по секунди док је највећи број промена у некој секунди био 52000. Када је симулатор покренут без подешених безбедносних механизама, број промена је износио 28500 по секунди док је највећи број промена био 50000. Уочавамо да је пад перформанси око 5%. У оквиру овог мерења коришћени су рачунари са 128 GB RAM меморије и Intel Xeon процесором E5-2680 који ради на 2.4 GHz радног такта са 32 виртуелна језгра процесора.

7. ЗАКЉУЧАК

У овом раду је представљен концепт и описана реализација ICCP протокол симулатора у циљу тестирања комуникационих веза између командних центара унутар SCADA система. Акценат комуникације је на сигурности и безбедности и стога симулатор протокола нуди решење ослоњено на успоставу безбедног комуникационог канала између два система. Решење користи дигиталне сертификате као и механизаме који чине комуникацију безбедном.

Још једна велика корист оваквог протокол симулатора је што може да се користи за тестирање самог надзорно управљачког система, да провери све подржане функционалности, да ли раде како би иначе требало. Од критичног је значаја верификовати да све функционалности у тестном окружењу раде како је предвиђено. ICCP као симулатор протокола**,** може опонашати уређаје, односно стање на терену и да, користећи симулатор, комуницира са надзорно управљачким системом. Кроз то ће указати да ли постоје евентуалне грешке у истом и може користити за обуку корисника.

8. ЛИТЕРАТУРА

[1] Бранислав Атлагић, „*Софтвер са критичним одзивом – Пројектовање SCADA система*“, ФТН издаваштво, Нови Сад, 2015.

[2] Abdalhossein Rezai, Parviz Keshavarzi, Zahra Moravej, „Secure SCADA communication by using a modified key management scheme”, *ISA Transactions*, Vol. 52, Issue 4, pp. 517-524, July 2013

[3] "STUXNET Malware Targets SCADA Systems". Trend Micro. 2012., http://about-threats.trendmicro.com/us/webattack/54/STUXNET%20Malware%20Targets%20SCADA%20Systems (приступљено у јулу 2019.)

Кратка биографија:

Марко Таглиавиа рођен је 1. маја 1995. У Руми. Завршио је средњу електротехничку школу „Михајло Пупин“, смер рачунарство у Новом Саду 2014. године. Факултет техничких наука у Новом Саду је уписао 2014. године, смер Рачунарство и аутоматика. Четврту годину студија завршио је на смеру Примењено софтверско инжењерство. Дипломирао је 15.07.2018. године. У октобру 2018. године, уписао је мастер академске студије, смер Информациони инжењеринг. Добитник је „Доситејеве награде“ фонда за младе таленте Републике Србије за школску 2017/18. и 2018./19.