International Journal of Engineering and Management Sciences (IJEMS) Vol. 1. (2016). No.2.
DOI: 10.21791/IJEMS.2016.2.5.

A MODBUS RTU protokoll biztonságtechnikai vizsgálata, új kriptográfiai megoldások tesztelése
Security evaluation of MODBUS RTU protocol, testing new cryptographic methods

G. JAKABÓCZKI[1], P. T. SZEMES[2], É. ÁDÁMKÓ[3]

[1]Debreceni Egyetem, jakaboczkigabor@gmail.com
[2]Debreceni Egyetem, szemespeter@eng.unideb.hu
[3]Debreceni Egyetem, adamkoe@gmail.com

Absztrakt: Az elmúlt évtized alatt a SCADA, CIS, ICS és hasonló rendszerek elleni támadások száma nagyban megnövekedett, ezek a rendszerek egyre védtelenebbek. A dolgozat célja, hogy a MODBUS RTU protokoll biztonsági hiányosságaira megoldást jelentő új kriptográfiai megoldás implementációja során gyűjtött tapasztalatokat összegezze.

Kulcsszavak—biztonság; támadás; MODBUS RTU; kriptográfia

Abstract: In the late decade, the number of attacks against SCADA, CIS, or ICS systems had grown considerably. The purpose of this paper is to summarize the results of the implementation of a new cryptographic method on the MODBUS RTU line.

Keywords—security, attack, MODBUS RTU, cryptography

BEVEZETŐ

Ezen dolgozat célja, hogy egy gyakorlati alkalmazáson keresztül bemutassa az ipari terepi hálózatok biztonsági réseit, azok feltárásának technológiáját, valamint példával szolgáljon arra, miképpen tehetőek biztonságosabbá ezek a rendszerek.

Dolgozatomban két, az információ biztonságát növelő eljárás alkalmazásának hatását vizsgáltam az alkalmazott vezérlő programjának futási idejére, valamint a módszerek kommunikációra való kihatását. Az eredmények szerint a módszerek alkalmazása mellett a vezérlő eredeti funkcióit maradéktalanul betölti, tehát a protokoll alkalmazása nem csökkenti az eszköz alkalmazhatóságát.

DOI: 10.21791/IJEMS.2016.2.5.

1 Problémafelvetés – SCADA rendszerek elleni támadások történelme

1.1 Az egyik első ismert támadás

1982-ben Tobolsk városa mellet felrobbant a Transz-szibériai gázvezeték-hálózat egy része. Egyes források megerősítették, hogy a robbanás oka a vezérlőszoftverbe juttatott trójai program okozta. A robbanás ereje elérte a 3 kilo tonnát, az egyik legnagyobb ember okozta, nem nukleáris robbanás volt a földön.

1.2 Cél a károkozás

2008-ban Eric Forner és Brian Meixell kutatók egy szimulált olajfúró torony rendszerének támadhatóságát vizsgálták. Támadásuk alatt észrevétlenül átvették az irányítást több PLC felett, melyek a kőolaj kitermelését felügyelték. Valós környezetben egy hasonló támadás természeti katasztrófához vezetett volna. [1]

1.3 Az alkalmazott eszközök költségei rohamosan csökkennek

Ugyanebben az évben Lucas Apa és Carlos Penagos mexikói kutatók egy olyan 40 dollár összértékű készüléket építettek, mellyel egy vegyi üzem rádiófrekvenciás hőmérsékletszenzorinak jeleit olvasták, zavarták, valamint hamis adatokat juttattak a rendszerbe. [1]

1.4 Egész nemzetek megbénítása

2003 augusztusában az Egyesült Államok északkeleti részét és Ontario államot sújtotta áramszünet, mely a kritikus infrastruktúra rendszereinek teljes leállásához vezetett, közel 60 millió embert érintett. Eugen Kaspersky a Kaspersky Lab vezetője 2010-ben egy konferencián tartott előadásában beszélt következtetéseikről, melyek szerint az irányító rendszerbe juttatott malware okozta az áramkimaradásokat. [1]

2010-ben az Iráni atomenergia programban résztvevő urándúsító centrifugákat érte támadás, melynek során ezek közel 20 %-a megsemmisült. A támadás, mely STUXNET néven vált ismertté, a centrifugák motorjait vezérlő frekvenciaváltókat érte, melyek véletlenszerűen kezdték a fordulatszámokat változtatni, így komoly mechanikai károkat okozva a berendezésekben. [2]

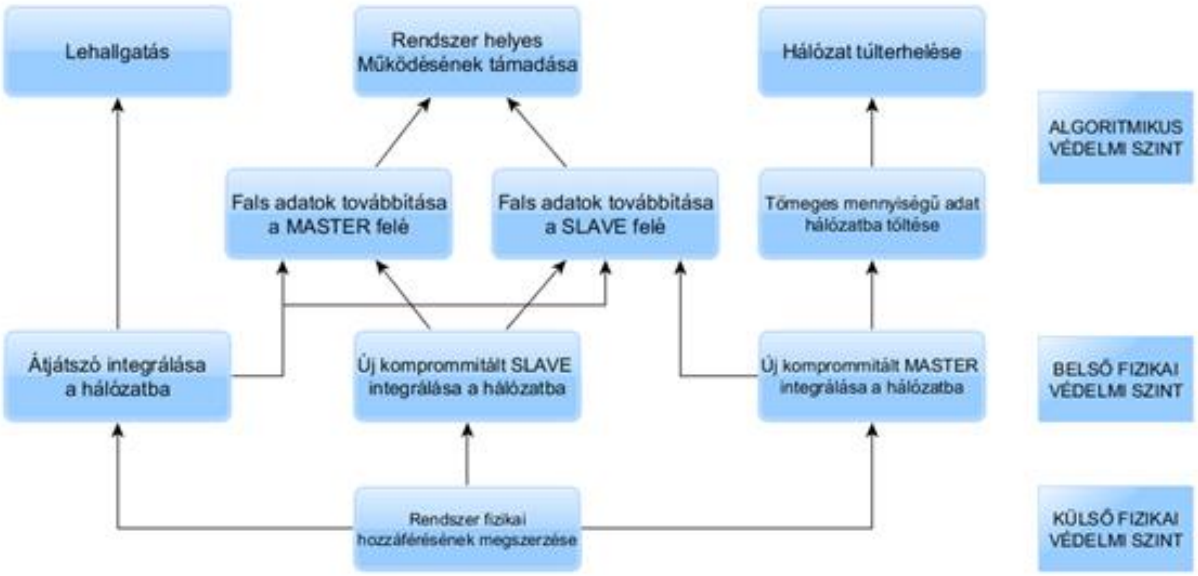
1.5 Ez is csak egy munka

A 2011-ben felfedezett Night Dragon néven elhíresült támadások nyugati (főleg európai és amerikai) cégek SCADA rendszereit célozták meg. Mivel a támadás nem kártékony jellegű volt, célja inkább az információszerzés lehetett, hónapokon át zavartalanul és észrevétlenül tevékenykedhettek résztvevői. A valószínűleg kínai eredetű támadás érdekessége, hogy a támadások helyi idő szerint 9-5 óra között folytak. [3]

DOI: 10.21791/IJEMS.2016.2.5.

2 A Modbus RTU protokoll biztonsági rései

Az ipari információs hálózatok biztonsági elemzése egyidős a hálózatokkal. Minden hálózat létrehozásakor felmerül a kérdés: Nem használják-e majd fel rendszerünket illetéktelen személyek, kártékony célok elérése érdekében? Ezen kérdések megválaszolására és a hálózat biztonsági réseinek felderítésére az úgynevezett ”támadási fa” (Attack Tree) eljárást választottuk, mely elemzést cikkünkben [4] részleteztük.



1. ábra: A MODBUS RTU protokoll támadási fája

A fenti ábrán látható támadási fában az alábbi listában felsorolt három gyökérelem a cél, vagyis ez a három elem írja le a Modbus RTU kommunikációs protokoll [a protokoll működésével a 4.3 fejezet foglakozik] legfőbb biztonsági réseit. Ezek a következők:

- Az adatforgalom lehallgatása, jogosulatlan hozzáférés az adatokhoz.
- A rendszer helyes működésének támadása, módosítása (eszközök szerepének átvétele, a helyes adatok módosítása)
- A hálózat túlterhelése, Denial Of Service támadás

Jelen dolgozatban a külső fizikai védelmi szinttel nem foglalkoztam, az e szintet áttörő módszerek büntető törvénykönyvbeli tételek, például illetéktelen behatolás fizikai vagy kevésbé radikális esetben ”social engineering” eszközök (az emberi erőforrások kihasználásán alapuló támadási módszer) segítségével. A legfelső (a célokhoz legközelebb eső) védelmi szint, az úgynevezett algoritmikus védelem biztosítására kerestem megoldást. A dolgozatban végül a “Secure protocol for Modbus RTU” cikkben [5] ismertetett protokollok felhasználásával kapott eredményeket dolgoztam fel.

DOI: 10.21791/IJEMS.2016.2.5.

3 A rendszer bemutatása

A választott eszköz melyen keresztül az eljárás bemutatásra kerül, egy egyszerűbb mérési-adatgyűjtő és szabályzó eszköz, mely a Debreceni Egyetem Műszaki Kar Villamosmérnöki és Mechatronikai tanszék épületében került fejlesztésre. A készülék RTD (termoellenállás) szenzorcsatornával, digitális bemenetekkel és analóg kimenetekkel rendelkezik. A mérések során a mérőeszköz nyolc darab PT100 típusú hőmérőszenzor adatait gyűjtötte, melyek a Hallgatói labor hőmérsékletét mérték.

Az eljárás bemutatására választott rendszer terepi vezérlője és a számítógép között az adatkapcsolatot 2-vezetékes RS485 buszon keresztül ModBus RTU protokoll valósítja meg. Választásunk a Modbus RTU protokollra esett, mivel a szabványt birtokló Schneider Electric cég nagyfokú eszköz- és mérnöktámogatást nyújt tanszékünknek az ott létrehozott tudásközponton keresztül.

Az általunk vizsgált példa épületmechatronikai rendszerben az egyszerűség kedvéért PTC szenzorok adatait gyűjtjük. Ezek a szenzorok platinából készült, 100 Ω névleges ellenállású eszközök, áramgenerátoros meghajtásuk konstans 1 mA áramot enged folyni a mérőkapcsolásban.

4 Megoldások

4.1 Üzenetek entrópiájának növelését célzó protokoll

A standard Modbus RTU üzenet maximális hossza 252 bájt (126 regiszter), ám ezt a hosszt nem minden eszköz és nem minden esetben használja ki. Az első protokoll esetén a fent említett cikkben feltételeztük, hogy a megfigyelő nem ismeri a lekérdezett adatok sorrendjét, illetve az adatok milyenségét. Így ha megnöveljük az üzenetek entrópiáját (minden üzenetben a maximális számú regisztert kérdezzük le) a hasznos információk megtalálása is nehezebb. A protokoll megszorításokat tesz a véletlenül generált adatok milyenségére is. Ennek megfelelően amennyiben hőmérséklet típusú a kért adat, akkor az entrópiát úgy növeljük, hogy a szabad regisztereket is hőmérséklet típusú véletlen adatokkal töltjük fel. Tehát az első megoldásban ezt az entrópia növelő módszert implementáltam.

A véletlenszerűen generált adatokat egy analóg csatorna pillanatnyi értékéből kaptam, mely értékeket úgy alakítottam, hogy nagyságrendi egyezés legyen köztük és a hasznos hőmérsékletadatok között.

4.2 Statikusan titkos kulccsal rendelkező titokmegosztáson alapuló kriptográfiai protokoll

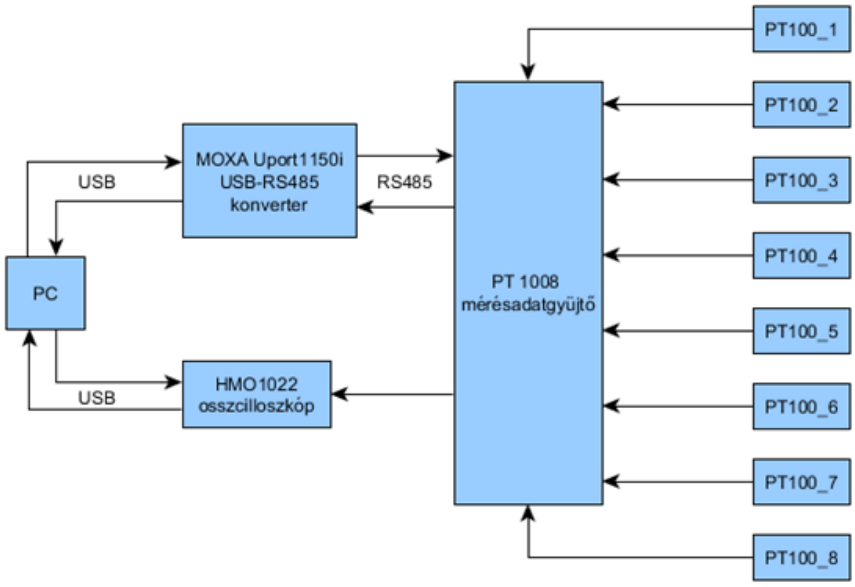
A Modbus RTU protokoll által szolgáltatott adat a soros csatornán normál esetben mindenféle titkosítás nélkül jelenik meg, így lehallgatás esetén egyértelműen olvasható, vagy módosítható. Ebben a protokollban viszont az adatok a titokmegosztás módszerével darabokra szedve, majd a darabok szimmetrikus titkosító segítségével elfedve közlekednek a kommunikációs csatornán.
A szimmetrikus kulcsú titkosításnál a küldő és fogadó felek birtokában vannak egy közös titoknak (kulcsnak), melynek segítségével fenn tudnak tartani egy biztonságos csatornát. A második protokoll alkalmazásánál feltételezzük, hogy az említett kulcsot, mely egy 128 bit hosszú véletlenszerűen generált szám, csak az általunk telepített eszközök ismerik, mivel a protokoll előírásait figyelembe

DOI: 10.21791/IJEMS.2016.2.5.

véve ez a rendszer kiépítésénél generálódik, valamint a Master és Slave eszközök nem tartalmazzák közvetlenül, tehát belőlük ki nem olvasható. Ennek részletes

megoldása a protokollt leíró cikkben olvasható. A titokmegosztás módszere pedig azon az elven működik, hogy egy titkot a részeiből csak akkor tudunk visszaállítani, ha tudjuk, hogy pontosan hány darabból áll (n), és rendelkezünk e darabok közül legalább n-1 darabbal. Így amennyiben a lehallgató megszerzi akár az összes regiszter tartalmát, és még dekódolni is képes, mert valamilyen támadás során birtokába került a titkos kulcs, még mindig meg kell birkóznia azzal, hogy a részekből visszaállítsa a titkot, a titok visszaállításához szükséges titokrészek számával azonban nincs tisztában.

5 Mérések



2. ábra: A mérőkapcsolás blokkvázlata

Az első referenciamérést a kommunikáció indítása nélkül végeztem, így meghatározva a program rendes lefutásának idejét. A vezérlő a referenciamérés közben 8 darab Platina 100 ellenállás-hőmérő adatait gyűjtötte. A program futása közben, minden funkció végén egy 10 μs idejű késleltetés került a programba, mely előtt a vezérlő egyik digitális kimenete logikai „1”-ből logikai „0”-ba váltott, majd a késleltetés után vissza. Az oszcilloszkóp az ezen a lábon történő feszültségváltozást mérte. A késleltetésre a mérés pontosságának növelése miatt volt szükség.

Az oszcilloszkóp és a számítógép között USB kapcsolaton keresztül mentettem a kapott adatokat (*.csv* formátumban), melyeket később az Excel program segítségével dolgoztam fel. Feltételezve, hogy a legkisebb mérendő időintervallum 10 μs, a mintavételezés frekvenciáját 400 *kHz*-re választottam, mely a mérési adatok alapján teljesítette a Nyquist-féle mintavételezési-kritériumot.

A második, illetve harmadik referenciamérés célja a kommunikáció paramétereinek vizsgálata volt, valamint a kommunikáció visszahatása a ciklusidőkre. A lekérdezések 100 ms időközönként ismétlődtek, egy lekérdezés 20 regiszter értékét érintette.

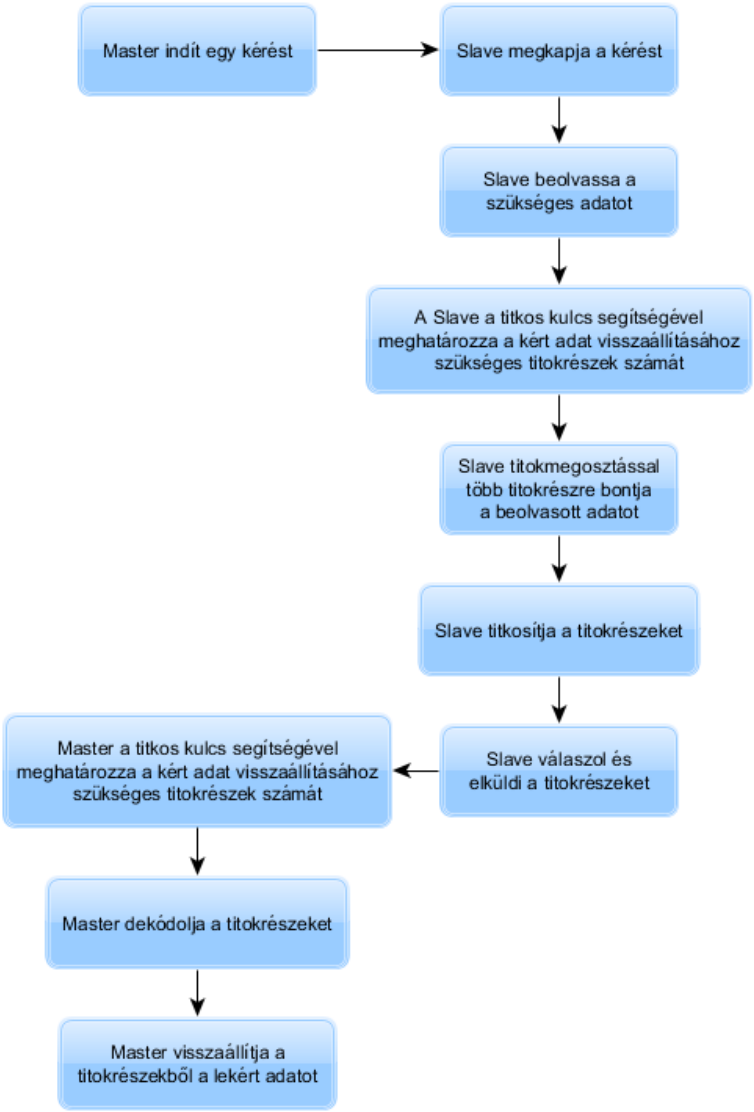
DOI: 10.21791/IJEMS.2016.2.5.

Az üzenet entrópiájának növelését célzó eljárás lényege, hogy az üzenet ne csak a hasznos adatokat tartalmazza, hanem olyan regisztereket is, melyek nem valós értékeket tartalmaznak. Az üzenet entrópiáját nem csak a lekérdezett regiszterek számának megnövelésével értem el, hanem ezekbe a regiszterekbe generált véletlenszerű adatokkal is. Ezek az adatok ugyan hasonlítanak a valós hőmérsékletadatokra, ám értékük nagyban eltérhet azoktól.

Az utolsó mérés tárgya a statikusan titkos kulccsal rendelkező titokmegosztáson alapuló kriptográfiai protokoll működése, illetve a kriptográfiai eljárás a program-futásidőre való kihatását vizsgálta

6 A mérések kiértékelése

A mérési adatokból kiderül, hogy az entrópia megnövelésével és a kriptográfiai protokoll alkalmazásával a ciklus futási ideje megötszöröződött.

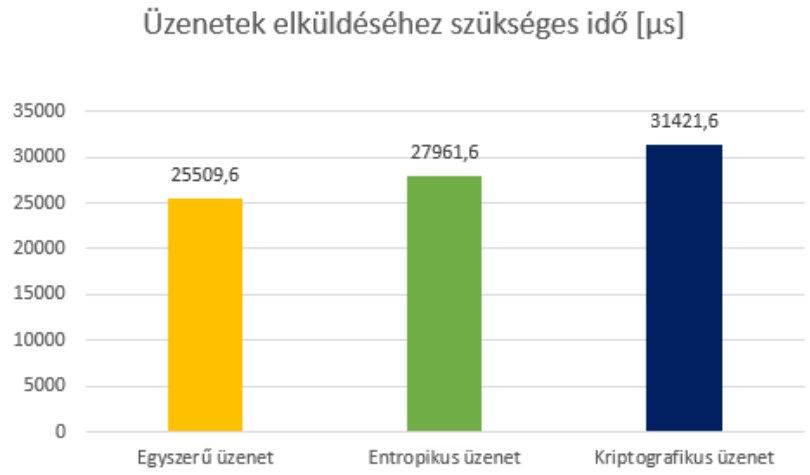


3. ábra: A kriptográfiai protokoll működése a slave oldaláról

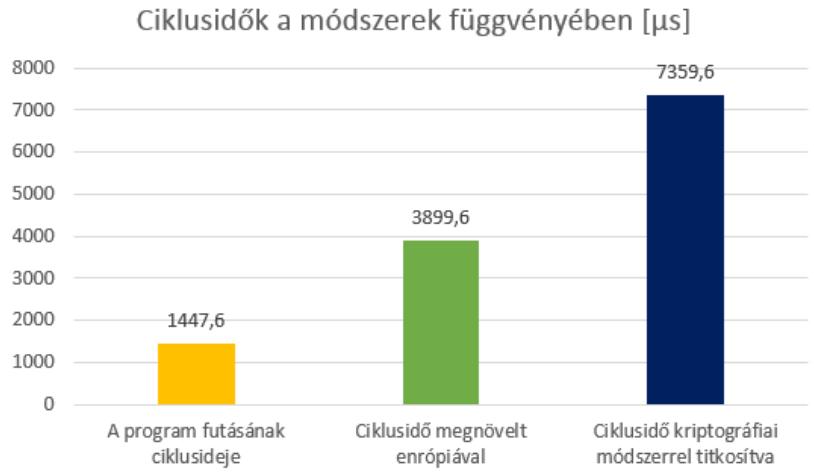
DOI: 10.21791/IJEMS.2016.2.5.

Az adatokat tartalmazó üzenet hossza 23%-os növekedést mutat, mely az entrópia növelését célzó eljárás és a kriptográfiai titkosítás futási idejének felel meg.

A fenti adatok tükrében elmondhatjuk, hogy bár a ciklus lefutásának ideje, illetve a válaszüzenetek összeállításához szüksége időtartam nagymértékben megnőtt, az eszköz képes volt feladatának zavartalan ellátására. A kommunikációs csatornán zavart nem tapasztaltam, a hibás üzenetváltások aránya 1:15000.



4. ábra: A program egyszeri lefutásának ideje a három verzió esetén



5. ábra: Az üzenetek elküldéséhez szüksége idő a három verzió esetén

Hivatkozások

[1] Ackerman, Robert K. ”SCADA Systems Face Diverse Software Attack Threats” (July 31, 2013).

[2] Albright, David, Paul Brannan, and Christina Walrond.”Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?”. Institute for Science and International Security, (2010).

DOI: 10.21791/IJEMS.2016.2.5.

[3] Keizer, Gregg. "'Sloppy'Chinese hackers scored data-theft coup with 'Night Dragon'." Computerworld, February 11 (2011).

[4] É. Ádámkó, G. Jakabóczki: Security Analysis of Modbus RTU (2015), kiadatlan.

[5] É. Ádámkó, G. Jakabóczki: Secure protocol for Modbus RTU, kiadatlan..