TEHNOLOŠKA REŠENJA I ZAKONSKA REGULATIVA ZA ZAŠTITU PRIVATNOSTI KORISNIKA NAPREDNIH ELEKTROENERGETSKIH MREŽA

Slobodan Bojanić, *Escuela Técnica Superior de Ing. de Telecomunicación, Universidad Politècnica de Madrid*
Srđan Đorđević, *Univerzitet u Nišu, Elektronski fakultet*

Sadržaj *– Rad daje širi pregled problematke zaštite podataka u naprednim elektroenergetskim mrežama. Na početku je dat prikaz postojećih tehničkih stadarda koji se odnose na informacionu bezbednost smart grida. Nakon toga razmotreni su pravni propisi kojima je regulisana zaštita privatnosti korisnika smart grida. Rad takođe opisuje primenu tehnologije bezbedne obrade signala u smart gridu.*

1. UVOD

Istraživanja smart grid sistema (SG) su veoma značajna i obuhvataju širok spektar raznovrsnih problema. Jedan od značajnih problema je obezbeđivanje informacione bezbednosti kao i zaštita privatnosti korisnika. Kada se razmatra informaciona bezbednost napredne elektroenergetske mreže moraju se uzeti u obzir ne samo namerni napadi već i greške korisnika, kvarovi na mreži, prirodne katastrofe.

Privatnost u smart grid mreži je intenzivno proučavana zbog značaja ove tematike. Detaljnim proučavanjem mernih podataka određenog naprednog brojila mogu se izvesti zaključci u vezi određenih obrazaca ponašanja potrošača.

U literaturi postoji više raznovrsnih tehničkih rešenja za problem zaštite privatnosti na smart gridu. Jedno od predloženih rešenja je filtriranje frekvencijskih komponenata male snage [1]. Drugi pristup ovom problemu je primena protokola koji se zasniva na nulto-znanje protokolu (zero knowledge proof) [2]. Na ovaj način omogućen je obračun potrošnje električne energije bez otkrivanja detalja o mernim podacima. Treće rešenje koje ovde navodimo je primena mehanizma kontrole pristupa [3]. Na ovaj način se pojedinim komponentama smart grida omogućava ili zabranjuje pristup podacima korisnika.

Savremeni razvoj informacionih i komunikacionih tehnologija dovodi do značajnih promena u svim oblastima društva. Jedan od aspekata ovih promena su povećane mogućnosti zloupotrebe tehnoloških dostignuća među koje spada i narušavanje privatnosti pojedinaca. Pravo na privatnost je jedno od osnovnih ljudskih prava zaštićeno nizom dokumenata uključujući i Univerzalnu deklaraciju Ujedinjenih nacija o ljudskim pravima. Pravo na privatnost se često u nacionalnim zakonodavstvima tumači kao pravo na privatnost podataka iako je to samo jedan od aspekata koncepta privatnosti.

Prvi deo rada daje pregled najznačajnijih standarda kojima se reguliše razmena podataka unutar napredne elektroenergetske mreže kao i neke pravce budućeg razvoja standarda u ovoj oblasti. Problem zaštite privatnosti korisnika smart grid mreže razmotren je u drugom poglavlju. Treće poglavlje posvećeno je bezbednosnim tehnologijama koje se primenjuju u naprednoj elektroenergetskoj mreži radi obezbeđivanja informacione sigurnosti.

2. TEHNIČKI STANDARDI ZA DEFINISANJE INFORMACIONE ZAŠTITE SMART GRIDA

Najznačajniji skup standarda kojima je definisana informaciona zaštita smartgrid-a u ovom trenutku sadržana je u sledećim dokumentima [4]:

- ISO/IEC 27001
- ISO/IEC 27002
- IEC 62351
- NERC CIP (US Standard)
- NISTIR-7628 (US Guidelines)

Ovi standardi su publikovani i široko prihvaćeni od strane aktera pametne elektroenergetske mreže kako u Evropi tako i u SAD. Očekuje se da će ovaj početni skup standarda vremenom nadograđivati.

Prvi dokument koji čini sveobuhvatan skup zahteva za postizanje visokog stepena sigurnosti svih mogućih aspekata SG izadat je od strane NIST pod nazivom „NIST IR 7628 smernice za informacionu bezbednost smart grida".

NERC CIP standardi nisu direktno namenjeni aplikacijama u SG već se prvenstveno odnose na postrojenjima za generisanje i transmisiju električne energije.

Problemom razvoja standarda za razmenu informacija elektroenergetskih i drugih srodnih sistema bavi se više radnih grupa u okviru tehničkog komiteta IEC TC57 u okviru Međunarodne elektrotehničke komisije (*International Electrotechnical Commission* IEC). Standard pod oznakom IEC 62351 razvijen je od strane radne grupe WG15 da bi se obezbedila informaciona sigurnost TC57 protokola. Ovim standardom se obezbeđuje i sigurnost komunikacija u elektroenergetskom sistemu. Cilj preporuka IEC 62351 je usavršavanje postojećih standarda sa tehnološkog aspekta čime se izlazi u susret novijim tehnološkim inovacijama i podržava dalji razvoj SG.

Serija standarda ISO/IEC 27000 obuhvata međunarnodne standarde informacione sigurnosti koje su objavile Međunarodna organizacija za standardizaciju (*International Organization for Standardization* - ISO) i Međunarodna elektrotehnička komisija (*International Electrotechnical Commission* - IEC). Standard ISO/IEC 27001 formalno specificira sistem upravljanja koji je namenjen obezbeđivanju informacione sigurnosti pod eksplicitnom kontrolom upravljanja (*Information security management systems* - ISMS). Standard ISO/IEC 27002 sadrži preporuke namenjene osobama odgovornim za pokretanje, uvođenje ili održavanje ISMS (*Information security management systems* - ISMS). Informaciona sigurnost je u ISO/IEC 27002 standardu definisana u kontekstu C-I-A trijade (*Confidentiality-Integrity-Availability*): očuvanje tajnosti (osigurati da informacija bude dostupna samo entitetima koji su autorizovani), integriteta (potrebno je obezbediti tačnost i

kompletnost informacija kao i metoda procesiranja) i dostupnosti (obezbediti da autorizovani korisnici imaju pristup informacijama i odgovarajućim sredstvima).

Jedan od pravaca daljeg razvoja standarda za informacionu sigurnost smart grida je prilagođenje standarda ISO/IEC 27002 specifičnim primenama. Prvi pokušaj da se reši ovaj problem je bio uvođenje standarda DIN 27009.

Radna grupa za informacionu sigurnost smart grida unutar Evropske komisije pod standardizacijskim mandatom M/490 izdala je poseban dokument u cilju podrške razvoju Evropske napredne elektroenergetske mreže [4]. Cilj ovog mandata je razvoj ili ažuriranje niza konzistentnih standarda za primenu u Evropskoj elektroenergetskoj mreži. Ovim standardima bi trebalo da se odgovori tehničkim i organizacioni potrebama za održivu informacionu sigurnost, kao i zaštitu podataka i privatnosti.

Institut inženjera elektrotehnike i elektronike [5] (Institute of Electrical and Electronics Engineers - IEEE, www.ieee.org) i Američki nacionalni institut za standarde i tehnologije [6] (National Institute of Standards and Technology - NIST, www.nist.gov) razvili su konceptualni model naprednih elektroenergetskih mreža. Ovaj model zasniva se sledećim domenima: masovna proizvodnja, transmisija, distribucija, klijenti, usluge, operacije, tržišta. Svaki od ovih domena se može sagledati na različitim fundamentalnim nivoima: nivou energije, komunikacija, informacijsko-informatičkom. Namena ovog modela je da omogući predstavljanje trenutnog stanja implementacije elektroenergetske mreže kao i da posluži kao smernica za dalji razvoj smartgrida. Kranji cilj daljeg razvoja standarda SG sistema je obezbeđivanje zadovoljavajućeg nivoa bezbednosti u svim domenima i slojevima napredne elektroenergetske mreže.

Prilikom razmatranja informacione sigurnosti smart grida pojavila se potreba da se klasifikuju rizici prema posledicama koje mogu da imaju na Evropsku elektroenergetsku mrežu. Posebna radna grupa zadužena za informacionu sigurnost pod nazivom SGIS definisala je pet nivoa sigurnosti kojima se praktično povezuju informaciona bezbednost sa funkcionisanjem elektroenergetske mreže. Prilikom implementacija SG neophodno je razmotriti zahteve koje treba ispuniti da bi se postigao odgovarajući nivo bezbednosti. Neki od ovih zateva se mogu izostaviti ukoliko se proceni da nisu od značaja. Način na koji su sigurnosne mere implementirane je veoma kritičan sa stanovišta interoperabilnosti sistema. Evropska SG mreža još uvek nije fizička realnost tako da ne postoji usvojena arhitektura. Problem bezbednosti SG dodatno komplikuje veliki broj raznovrsnih tehnologija koje međusobno interaguju kao i različite moguće arhitekture za pojedine domene smartgrida. Definisanje smernice za detaljniju tehničku implementaciju je u ovom trenutku veoma komplikovano, skoro i neizvodljivo.

3. ZAŠTITA PRIVATNOSTI

Zaštita privatnosti prema definiciji koju daje Džozef Kantači znači zaštitu pojedinca od zloupotrebe ili neadekvatne upotrebe ličnih podataka od strane nekog lica, privatne organizacije ili države [7]. Jedan od problema u sankcionisanju povrede privatnosti je uspostavljanje ravnoteže između prava pojedinca na privatnost i prava javnosti da budu informisana.

Stalnim razvoj informacionih i komunikacionih tehnologija povećava se mogućnost njihove zloupotrebe. Kao jedan od vidova ove zloupotrebe pojavilo se i pitanje zaštite pojedinačnog ličnog prava - prava na privatnost. Međunarodna i nacionalna pravna regulativa moraju da budu veoma fleksibilne i da prate svakodnevni razvoj tehnologije i inovacija.

Vezano za zaštitu privatnosti otvara se niz pitanja funkcionalnog, organizacionog i bezbednosnog karaktera kao što su: mere obezbeđenja hardvera i softvera, ograničavanje raspolaganja određenim informacijama, obaveštavanje građana o njihovim podacima, davanje informacija državnim organima itsl.

Konvencija Saveta Evrope o visokotehnološkom kriminalu iz 2001 godine ne reguliše posebno pitanje privatnosti i zaštite podataka u virtuelnom prostoru ili kompjuterskim komunikacijama. Sankcioniše se nedozvoljeni pristup računarskiim podacima ili njihovo falsifikovanje. Može se reći da je regulativa više vezana za tehnička a ne suštinska pitanja zaštite od kriminalnih ponašanja.

Analizom podataka finih granualarnih SG merenja mogu se pratiti aktivnosti građana (njegovo prisustvo i odsustvo, svakodnevno kretanje ili ponašanje) kao i donositi neke zaključke u vezi njegovog ličnog života (broj članova domaćinstva, religijska ili grupna pripadnost).

Evropska unija i Kanada primenjuju takozvani horizontalni režim zaštite podataka prema kojem je uspostavljen skup zakona i propisa čije se mere odnose na obradu bilo koje vrste privatnih podataka. Vremenom su odredbe ovih zakona postale primenjive i na podatke koji se prenose naprednom elektroenergetskom mrežom. Federalno zakonodavstvo SAD još uvek ne poseduje pravne propise kojima je regulisana zaštita prava na privatnost korisnika smart grida. Uprkos ovoj činjenici niz saveznih država SAD uključujući Kaliforniju, Kolorado, Ohajo i Oklahomu usvojilo je zakone koji regulišu zaštitu privatnosti u ovoj oblasti.

Prvi pokušaj da se u našoj zemlji pravno reguliše zaštita privatnosti je *Zakon o zaštiti podataka o ličnosti* („Sl. List SRJ“ br. 24/98) iz 1998. godine. Može se reći da ovaj zakon nije zaživeo u praksi jer nije zabeležen ni jedan pokušaj njegove primene od strane nadležnih organa ili pojedinaca. Usled nastojanja da se domaće zakonodavstvo uskladi sa Evropskim stadardima, Srbija je 2008 godine usvojila novi *Zakon o zaštiti podataka o ličnosti* („Sl. glasnik RS“ br. 98/2008). Najznačajniji pravni okvir za donošenje ovog zakona je Konvencija Saveta Evrope broj 108 o zaštiti lica u odnosu na automatsku obradu ličnih podataka iz 1981 koju je Srbija potpisala 2005 godine.

4. BEZBEDNOSNE TEHNOLOGIJE

U SG nije moguće sprečiti odavanje poverljivih informacija širenjem svesti kod građana na koji način zaštiti poverljive podatke za razliku od nekih drugih on-line sistema u kojima takođe postoji problem zaštite privatnosti (internet, društvene mreže). Problem zaštite privatnosti se može rešiti pravnom regulativom ili razvojem bezbednosnih tehnologija. Poslednjih godina se za ovu namenu primenjuje tehnologija

pod nazivom *Bezbedna obrada signala* (*Secure Signal Processing* SSP) [8]. Ovaj mehanizam zaštite treba da obezbedi da entiteti koji su nepouzdani nemaju pristup privatnim podacima pri čemu komunalne službe pružaoca usluga *(utility provider* UP) mogu nesmetano da primene obradu merenih rezulata naprednih brojila. Radi postizanja ovog cilja merni podaci koje napredna brojila šalju komunalnim službama pružaoca usluga radi obračuna potrošnje ili analize podataka se enkriptuju. Iako su podaci pojedinačnih brojila skriveni za UP obrada merenih podataka se obavlja nesmetano zahvaljujući primeni unapred definisanih protokola komunikacije između naprednih brojila i UP.

Postoje tri najznačajnije pretpostavke za realizaciju SSP:

1. Raspoloživost komunikacione mreže kako između UP i naprednih brojila tako i između pojedinih broijla (Bluetooth ili ZigBee),
2. Validni sertifikat za svako brojilo,
3. Usvojene kriptografske operacije se mogu izvršiti primenom ograničenih hardverskih resursa.

Radi sprovođenja ovog cilja primenjuju se homomorfna enkripcija (*homomorphic encryption*) kao i tehnike bezbednog izračunavanja sa više učesnika (*secure multi-party computation* ili *multi-party computation* (MPC)). Homomorfno šifriranje je vrsta enkripcije za koju važi da se nakon sprovođenja specifičnih funkcija nad kriptovanim tekstom i njegovog dekriptovanja dobija rezultat koji odgovaraju primeni tih istih funkcija nad otvorenim tekstom.

Procedura prikupljanja podataka primenom homomorfne enkripcije zahteva da svi entiteti koji šalju podatke primenjuju isti ključ. Proizilazi da je za primene ove šeme šifrovanja u naprednoj elektroenergetskoj mreži neophodno uvesti dodatne tehnike jer bi deljenjem ključa između brojila bila narušena tajnost merenih podataka.

Među trenutno predloženim realizacijama bezbedne obrada signala (SSP) u naprednoj elektroenergetskoj mreži ističu se četiri rešenja. Svako od ovih rešenja primenjuje posebne tehnike obrade signala koje se mogu opisati na sledeći način:

1. Homomorfna enkripcija i deljive tajne (*Homomorphic Encryption and Secret Sharing*) [9],
2. Maskiranje i dešifrovanje primenom "grube sile" (*Masking and brute forcing*) [10],
3. Modifikovana homomorfna enkripcija (*Modified homomorphic encryption*) [11],
4. Maskiranje i diferencijalna privatnost (*Masking and differential privacy*) [12].

Enkripcioni protokol kod kojeg se primenjuje deljiva tajna započinje tako što svako od brojila deli merne podatke na više delova čiji broj odgovara broju brojila nad kojima se sprovodi protokol pri čemu je svaki od ovih delova posvećen određenom brojilu odnosno enkriptuje se javnim ključem odgovarajućeg brojila. Na ovaj način enkriptovani podaci šalju se UP. Nakon što prikupi podatke od svih brojila UP objedinjuje sve one delove podataka koji su kriptovani istim javnim ključem koristeći se svojstvima homomorfne enkripcione šeme. Na ovaj način obrađene podatke UP šalje odgovarajućem brojilu koje ih dekriptuje svojim tajnim ključem i pridodaje deo podataka koji nije bio poslat. Tokom sledećeg koraka protokola svako od brojila objedinjuje sve delove mernih podataka koji su posvećeni tom brojilu i šalje ih u formi otvorenog teksta UP. Na osnovu primljenih podataka UP jednostavno dobija ukupnu potrošnju skupa potrošača.

Autori protokola koji se zasniva na primeni maskiranja i dešifrovanja primenom "grube sile" (brute forcing) predlažu dve procedure za bezbedan proračun ukupne potrošnje. Jedan od ta dva protokola pod nazivom agregacioni protokol primenjuje maskiranje mernih podataka pojedinih brojila na takav način da ukupna suma svih maskiranih podataka daje ukupnu potrošnju. Suština postupka je da se prilikom sumiranja uzajamno potiru maskirne vrednosti. Drugi predloženi protokol pod nazivom poredbeni protokol polazi od pretpostavke da UP može grubo proceniti vrednost zbirne potrošnje određene grupe brojila. Upoređivanjem niza proračunatih vrednosti primenom stepenovanja sa vrednostima dobijenim od pojedinih brojila dolazi se do zaključka kolika je vrednost zbirne potrošnje.

Modifikovana homomorfna enkripcija primenjuje modifikovanu verziju Paillier-ovog kriptosistema. Da bi ova tehnika mogla da se primeni neophodno je da brojila primenjuju prilikom enkripcije istu slučajnu vrednost. Autori ove procedure predviđaju tri šeme protokola: prostorna kojom se proračunava zbirna potrošnja određenog broja korisnika u zadatom vremenskom intervalu, vremenska kojom se proračunava ukupna potrošnja jednog korisnika u toku određenog vremenskog intervala i na kraju prostorno vremenska-šema koja predstavlja kombinaciju prethodne dve.

Protokol koji se zasniva na maskiranju i primeni diferencijalne privatnosti primenjuje aditivnu homomorfnu enkripcionu šemu. Procedura započinje tako što napredna brojila nasumično biraju niz brojila iz okruženja sa kojima se uparuju bidirekciono. Svaka dva međusobno povezana napredna brojila generišu zajedničku slučajnu vrednost koja odgovara toj vezi. Prilikom enkripcije podatak u brojilu mernim podacima se dodaje se ili oduzima slučajna vrednost koja odgovara svakoj od veza. Pri tome se striktno vodi račun da se mernim podacima jednog od dva međusobno povezana brojila doda a drugom oduzme slučajna vrednost.

Svako od brojila iz grupe brojila za koju se proračunava zbirna potrošnja istovremeno deli i ključ sa UP. Kada se saberu merni podaci svih brojila u UP se dobija ukupna zbirna potrošnja jer dolazi do međusobnog potiranja svih slučajnih vrednosti.

5. ZAKLJUČAK

Problemu zaštite privatnosti korisnika napredne elektroenergetske mreže pristupa se sa dva aspekta. Sa jedne strane rešenje se traži u razvoju odgovarajuće zakonske regulative kojom bi se sprečila svaka vrsta zloupotrebe merenih podataka a sa druge strane u razvoju tehnologija čijom bi se primenom onemogućilo bilo kojem entitetu koji je nepouzdan da pristupi merenim podacima naprednih brojila.

Postojećim tehničkim standardima uspostavljene su osnove informacione bezbednosti smart grid mreže. Radi regulisanja nekih specifičnih zahteva koje treba da ispuni smart grid neophodno je unapređenje postojećih i uvođenje novih standarda. Primenom tehnologije Bezbedne obrade signala SSP u naprednoj elektroenergetskoj mreži se u

značajnoj meri doprinosi rešavanju problema zaštite privatnosti merenih podataka.

6. LITERATURA

[1] S. R. Rajagopalan, L. Sankar, S. Mohajer, and H. V. Poor, „Smart meter privacy: A utility-privacy framework," *IEEE SmartGridComm* 2011, To appear. Available at http://arxiv.org/abs/1108.2234

[2] A. Rial and G. Danezis, „Privacy-preserving smart metering," technical Report MSR-TR-2010-150, Microsoft Research, 2010.

[3] R. Bobba , H. Khurana , M. AlTurki , F. Ashraf, „PBES: a policy based encryption system with application to data sharing in the power grid," Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, Sydney, Australia, March 10-12, 2009.

[4] „CEN-CENELEC-ETSI Smart Grid Coordination Group Smart Grid Information Security" CEN-CENELEC-ETSI Smart Grid Coordination Group, November 2012.

[5] Institute of Electrical and Electronics Engineers, Approved IEEE Smart Grid Standards, http://smartgrid.ieee.org/standards/approved-ieee-smart-grid-standards.

[6] National Institute of Standards and Technology, NIST & the Smart Grid, www.nist.gov/smartgrid/nistandsmartgrid.cfm.

[7] J. A. Cannataci, „Privacy and Data Protection Law: International Development and Maltese Perspectives," Complex, Norwegian research center for computers and law, 1987.

[8] Erkin, Z. Troncoso-Pastoriza, J.R. ; Lagendijk, R.L. ; Perez-Gonzalez, F, „An Overview of Privacy-Preserving Data Aggregation in Smart Metering Systems," IEEE Signal Processing Magazine, vol. 30, Issue: 2, March 2013.

[9] F. D. Garcia and B. Jacobs, „Privacy-friendly energy-metering via homomorphic encryption," In J. C. et al., editor, 6th Workshop on Security and Trust Management (STM 2010), volume 6710 of Lecture Notes in Computer Science, pp. 226–238. Springer Verlag, 2010.

[10] K. Kursawe, G. Danezis, and M. Kohlweiss, „Privacy-friendly aggregation for the smart-grid," In PETS, pp. 175–191, 2011.

[11] Z. Erkin and G. Tsudik, „Private computation of spatial and temporal power consumption with smart meters," In International Conference on Applied Cryptography and Network Security, pp. 561–577. Springer-Verlag, June 26-29 2012.

[12] G. Acs and C. Castelluccia „I have a DREAM! (Differentially PrivatE smart Metering) ," In Information Hiding Conference, LNCS, pages –Springer, May 18-20 2011.

Abstract – This paper provides an overview of problems associated with protecting privacy in smart grids. First we review technical standards which establish the basic of the Smart grid information security. Then we consider available legislation governing data privacy in the Smart grids. We also give a survey of privacy-preserving data aggregation in smart metering systems.

TECHNOLOGY SOLUTIONS AND REGULATIONS FOR PRIVACY PROTECTION OF THE SMART GRID USERS

Slobodan Bojanić, Srđan Đorđević