BEZBEDNOST I RUKOVANJE PODACIMA U PAMETNIM MREŽAMA

V.Josipović JP „Elektromreža Srbije“, Srbija

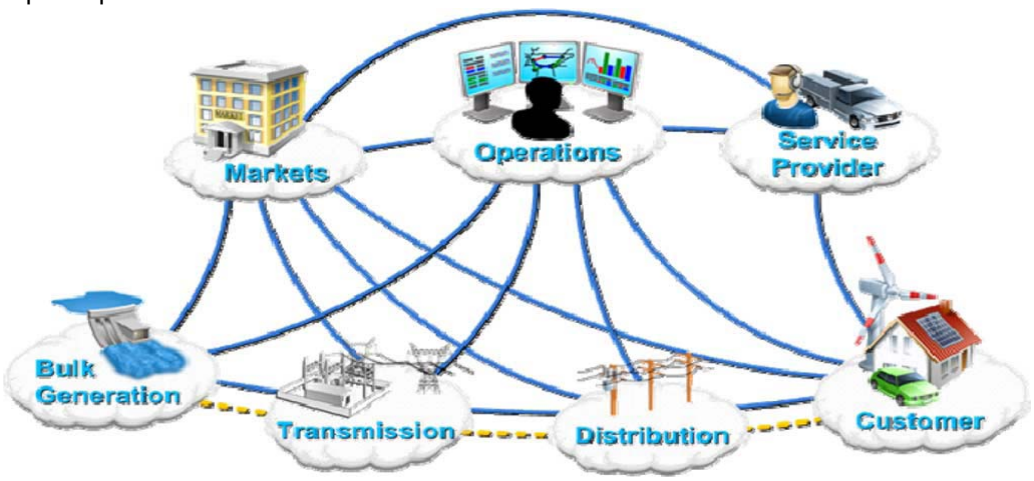
UVOD

Bezbednost i privatnost podataka u budućim pametnim mrežama je važna kako bi one bile prihvaćene od svih zainteresovanih strana. U svetu postoji saglasnost po pitanju potrebe da se unapredi prenosna mreža i to ka pametnim mrežama. Na tome se sistematski radi naročito u Severnoj Americi i Evropi. SAD su odredile vladine agencije i opredelile značajna sredstva u budžetu za razvoj standarda po kojima će se razvijati pametne mreže. U okviru već donetih standarda svoje mesto ima bezbednost podataka. EU u sklopu postavljenih ciljeva politike 2020 predviđa razvoj tehnologije za bezbednost podataka u pametnim mrežama.Pored standarda koji su već primenjeni u okviru postojećih pametnih mreža, u SAD postoje predlozi za uvođenje infrastrukture sa javnim ključem PKI (Public key infrastructure), kao tehnologije koja se već dokazala u poslovnom okruženju.

RAD

U poređenju sa sadašnjim mrežama pametne mreže se razlikuju po tome što povezuju elemente u mrežu sa dvosmernom komunikacijom. To pruža nove mogućnosti kao što je upravljanje tarifama, upravljanje opterećenjem, distribuirano skladištenje energije (npr. u električnim automobilima), i distribuirana proizvodnja energije (npr. iz obnovljivih izvora). Ova mreža se ostvaruje korišćenjem različitih medija počev od optičkih vlakana, klasičnih bakarnih provodnika do bežičnih mreža ZigBee i WLAN. Bežične mreže se štite tehnologijama koje obezbeđuju standardi kao što su 802.11i i 802.16e. Bežični protokoli imaju različite nivoe zaštite bezbednosnim mehanizmima. Žične mreže se štite firewall-om i virtualnim privatnim mrežama (VPN) tehnologijom kao što je IPSec. Viši nivoi bezbednosnih mehanizama kao što je Secure Shell (SSH) i SSL/TLS se takođe koriste.
Uzimajući u obzir potrebu za finom granularnošću nadgledanja pametnog merenja veoma je važna bezbednost infrastrukture naprednog merenja (AMI advanced metering infrastructure). Bezbednosni rizici i pretnje po pametnu mrežu se mogu identifikovati pristupom odozgo na dole(top-down) ili odozdo na gore(bottom-up) [2]. Top-down pristup analizira dobro definisani korisnički scenario kao što je automatsko očitavanje potrošnje (AMR automatic meter reading), obračun potrošnje, dok pristup odozdo na gore se fokusira na poznate bezbednosne atribute kao što je integritet, autentikacija, autorizacija, upravljanje ključevima i detekcija upada u mrežu. Klasifikacija rizika i pretnji u pametnim mrežama je objavljena od strane NIST [6].
Drugi korak u proceni bezbednosti pametne mreže je specifikacija bezbednosnih zahteva, na primer kakva je za AMI bezbednosne zahteve data od strane OpenSG. Međutim, nabrajanje svih mogućih

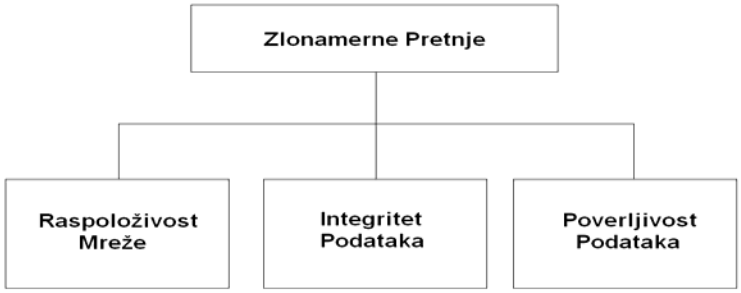
pretnji po pametnu mrežu nije praktično zbog sve veće kompleksnosti i nekih sofisticiranih napada koji još nisu identifikovani. Tako se zlonamerni napadi mogu prema top down pristupu po cilju podeliti na tri osnovne grupe. (i) dostupnost mreže, (ii) integritet podataka, (iii) poverljivost podataka. Zatim se može razmotriti uticaj i izvodljivost svakog od tih vrsta napada, a u isto vreme sumirati rad na svakom tipu napada protiv prenosne mreže.



Slika 1. Konceptualni model pametne mreže

Dostupnost mreže

Zlonamerni napadi koji za cilj imaju dostupnost mreže mogu se smatrati denial-of-service(DoS) napadima, kojima se pokušava usporiti, blokirati ili zauzeti mrežni resurs za prenos informacija sa namerom da se taj resurs učini nedostupnim za čvorove kojima je potrebna razmena informacija u okviru pametne mreže.
Pošto se očekuje da će bar deo, ako ne i sve pametne mreže koristiti IP bazirane protokole (npr. IEC 61850 je već usvojio TCP/IP kao deo svojih stek protokola) i TCP/IP je ranjiv na DoS napade, pa su sofisticirane i efikasne protivmere na DoS napade veoma važne za pametne mreže. DoS napadi na TCP/IP su dobro proučeni u literaturi u pogledu vrste napada zaštite i odgovora na njih. Posebno treba razmotriti potencijalne napade koji kao poseban cilj imaju raspoloživost energetske prenosne mreže. Pošto je glavna razlika izmedju interneta i pametne mreže to što se kod pametnih mreža više pažnje posvećuje kašnjenju poruke nego količini podataka koja se prenese kroz pametnu mrežu. Mrežni saobraćaj za prenos podataka u elektroenergetskim mrežama je generalno vremenski kritičan. Na primer ograničenje za kašnjenje u prenosu GOOSE poruka (GOOSE generic object oriented substation events) je 4 mS prema standardu IEC 61850. Takvo vremensko ograničenje omogućava pouzdano praćenje i kontrolu energetskih uređaja. Sa druge strane to postaje jedan od najranjivijih delova u energetskim mrežama na DoS napade. Još određenije, umesto da koristi ekstremne mere (npr.ometanje kanala), napadač može koristiti legitiman metod da namerno uspori prenos vremenski kritičnih poruka kako bi prekršio vremenska ograničenja. Na primer napadač se može fizički priključiti na komunikacioni kanal u okviru energetske mreže i generisati legitimni ali beskorisni saobraćaj čime zauzima kanal i tako usporava rad uređaja za kontrolu i upravljanje energetskom mrežom. Sve dok napadač samo treba da se konektuje na komunikacioni kanal a ne i da se priključi na mrežu koja ima autentikaciju u okviru pametne mreže, lako mu je da sprovede DoS napade protiv pametne mreže. Naročito je to lako kada su u pitanju bežične mreže koje su podložne DoS napadima.



Slika 2. Klasifikacija bezbednosnih pretnji u komunikacionim mrežama pametnih mreža

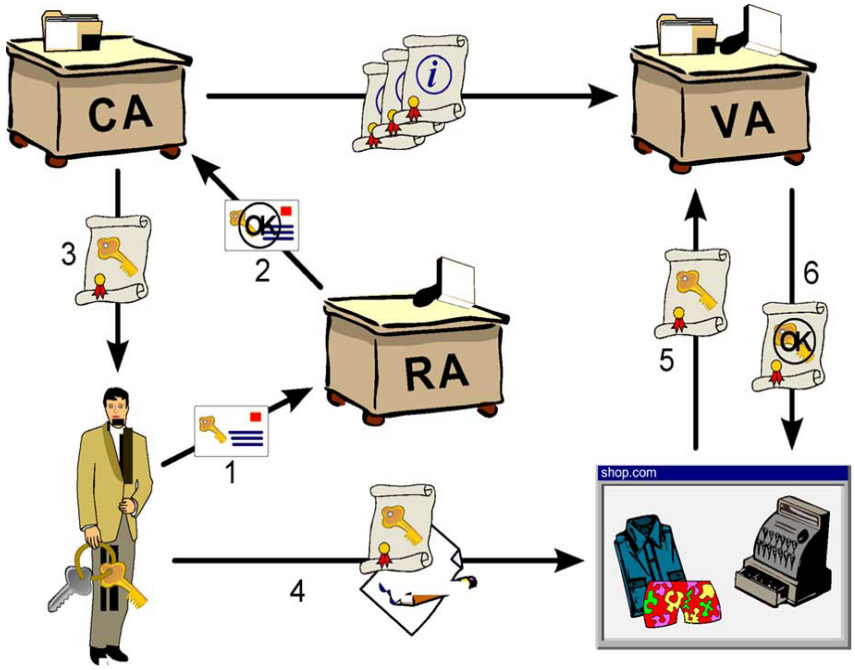
Integritet podataka i poverljivost podataka

Za razliku od napada koji za cilj imaju smanjenje dostupnosti mreže, napadi usmereni na integritet podataka su više sofisticirani. Cilj napada su neke informacije o korisniku (npr. cena ili račun nekog potrošača) ili neke informacije o radu energetske mreže (npr. očitavanje vrednosti napona, status opreme). Drugim rečima takvi napadi imaju za cilj namernu promenu informacija kako bi preuzeli razmenu kritičnih informacija za rad pametne mreže. Nasuprot tome napadač koji za cilj ima poverljivost podataka ne pokušava da modifikuje informacije koje se prenose kroz energetsku mrežu ali se trudi da prisluškuje komunikaciju kako bi prikupio informacije kao što su pretplatnički broj korisnika ili informacije o potrošnji. Takvi napadi se mogu smatrati kao zanemarljivi na funkcionalnost komunikacione mreže u okviru pametne mreže. U poređenju sa napadima koji za cilj imaju integritet podataka, napadi koji su usmereni na poverljivost podataka ne mogu prouzrokovati katastrofalne posledice, kao što je masovno isključenje (blackout). Rizik od napada koji za cilj imaju integritet podataka je iznenađujuće realan. Primer je rad koji govori o novoj vrsti napada, koji se nazivaju napad ubacivanja lažnih podataka, koji se primenjuje za napad na estimator stanja u okviru energetske mreže. U radu se predpostavljla da je napadač već kompromitovao jedno ili više merenja i ističe da napadač može iskoristiti pogodnosti konfiguracije energetskog sistema da sprovede napad ubacivanjem lažnih podataka u centar za nadgledanje, tako da oni mogu legitimno proći proceduru provere integriteta podataka koja se koristi u datom energetskom sistemu. Kao odgovor na to razvijene su metode koje estimatoru stanja omogućuju neosetljivost na napade ubacivanjem lažnih podataka. Ako želi da ostvari napad na integritet podataka ili da prikuplja podatke, napadač mora najpre da neopaženo uđe u računarski sistem ili neki od legitimnih čvorova mreže, ili da na neki od načina pristupi energetskoj mreži uz autentikaciju. Iz toga sledi da se protivmere za zaštitu od napada usmerenih na integritet i privatnost podataka sastoje od sledecih smernica:
1) Kreiranje protokola za autentikaciju. Autentikacija je važan problem za identifikaciju u okviru bilo koje komunikacione mreže. Jaka šema autentikacje je potrebna da bi se korisnicima i elektronskim uređajima obezbedilo komuniciranje sa potpunom bezbednošću i da zadovolje stroge zahteve komunikacione mreže u okviru pametne mreže, kao što su kašnjenje poruka i ograničenje potrošnje. Ograničenja u smisli kritičnog vremena dovode do sledećih zahteva prilikom kreiranja protokola za autentikaciju: (i) efikasnost algoritma sa ciljem smanjenja troškova procesorske snage (ii) niski komunikacioni overhead (iii) otpornost na napade.
2) Detekcija upada. Pametne mreže moraju imati sposobnost da detektuju pokušaje napadača da neovlašćeno pristupi računarskim sistemima. Neki radovi se bave tematikom upada u komunikacione mreže koja su u okviru energetskih mreža [8]. Može se reći da se ova pitanja uglavnom tretiraju u okviru sajber bezbednosti, i da su dovoljno zastupljena u literaturi.
3) Kreiranje firewall-a i gateway-a. Kao što je ranije spomenuto, za razliku od interneta pametne mreže imaju samo dva glavna toka informacija odozdo na gore i sa vrha ka dole. To dakle umnogome olakšava kontrolu toka saobraćaja koju vrši softver u gateway ili firewall-u u okviru pametne mreže i tako blokira neželjeni saobraćaj ili čak sumnjive tokove generisane od strane zlonamernoh čvorova. Može se reći da za napadača nije trivijalno da kompromituje legitimni čvor ili da pristupi energetskoj mreži uz autentikaciju. Pa ipak zbog velike rasprostranjenosti pametnih mreža, postoji mogućnost da

se zlonamerni napadač može na neki od načina konektovati na energetsku mrežu i izvršiti napad na integritet podataka ili poverljivost podataka.

PKI standard i mogućnost primene u pametnim mrežama

Na osnovu bezbednosnih zahteva koji se javljaju u pametnim mrežama i na osnovu poznatih i dostupnih tehnologija u SAD postoje predlozi da se PKI (Public Key Infrastructure) koristi kao najefektivnija tehnologija za upravljanje ključevima, čime bi se ostvarila bezbednost podataka u pametnim mrežama. PKI je više od hardvera i softvera u sistemu. On uključuje politiku i procedure, kojima se opisuje uspostavljanje, upravljanje, obnavljanje i povlačenje certifikata koji su ključni elemenat PKI sistema. PKI povezuje javni ključ korisnika sa njegovim identitetom korišćenjem digitalnog certifikata. U veoma velikim sistemima PKI je značajno efikasniji od sistema sa deljenim ključevima po pitanju uspostavljanja i održavanja. To je zbog činjenice da svaki entitet treba da bude konfigurisan sa sopstvenim sertifikatom. U poređenju sa simetričnim sistemom šifrovanja u kojem je potrebno obezbediti po jedan par ključeva za svaki bezbednu vezu. Osnovna funkcija sistema sa javnim ključevima je pouzdano uspostavljanje digitalnog identiteta subjekata u okviru računarske mreže. U savremenim sistemima zaštite, osnovni nosioci digitalnog identiteta su digitalni sertifikati. Digitalni sertifikati predstavljaju jednoznačne identifikacione parametre subjekata u komunikaciji. Infrastruktura sistema za primenu javnih ključeva predstavlja kombinaciju hardverskih i softverskih elemenata za realizaciju funkcija sistema sa primenom javnih ključeva. Postoji više mogućih načina da se realizuje PKI . Njegova osnovna uloga je pouzdano uspostavljanje digitalnog identiteta subjekata u okviru mreže, baziranog na upotrebi digitalnih sertifikata. Time se stvara bezbedno okruženje za realizaciju drugih bezbednosnih servisa, prvenstveno onih kod kojih je od značaja autentičnost subjekata koji komuniciraju. Drugim rečima, uspostavljanje infrastrukture sistema sa javnim ključevima je osnovni preduslov za realizaciju sistema zaštite. Usluge PKI sistema se koriste na svim nivoima zaštite računarskih resursa i mreža. Primeri aplikacija zaštite zasnovanih na PKI sistemima su formiranje virtualne privatne mreže (VPN - Virtual Private Network) formiranje pouzdanog sistema zaštite na transportnom nivou u računarskoj mreži. Infrastruktura sistema za primenu javnih ključeva sastoji se iz sledećih funkcionalnih komponenti: sertifikacionog tela (Certification Authority, CA), koje



Slika 3. Osnovna PKI arhitektura

izdaje digitalne sertifikate i reguliše način njihove upotrebe, registracionih tela (Registration Authority, RA), koja predstavljaju interfejs za podnošenje zahteva za izdavanje sertifikata, komunikacionog sistema za razmenu podataka između registracionog i sertifikacionog tela distribuciju zahteva za

izdavanje sertifikata i slanje digitalnih sertifikata, kriptografskih aplikacija za realizaciju funkcija PKI sistema, subjekata koji komuniciraju u mrežnom okruženju, na bazi izdatih digitalnih sertifikata. Sertifikaciono telo je autoritet sa najvećim stepenom poverenja u PKI sistemu. Sertifikacioni autoritet svojim digitalnim potpisom garantuje asocijaciju odgovarajućeg subjekta i njegovog javnog ključa. Neke od osnovnih funkcija CA su: Izdavanje digitalnih sertifikata, publikovanje sertifikata na X500/LDAP serveru, upravljanje rokom važnosti, upravljanje procedurom povlačenja sertifikata.

ZAKLJUČAK

Kao kritični elemenat infrastrukture, pametna mreža zahteva najviši nivo bezbednosti. Neophodno je od samog početka primene pametnih mreža izgraditi svobuhvatnu arhitekturu sa ugrađenom bezbednošću. Bezbednosne pretnje po komunikacione mreže u okviru pametnih mreža se mogu podeliti na tri grupe zavisno od ciljeva. To se odnosi na dostupnost mreže, integritet podataka i privatnost podataka. Bezbednosno rešenje za pametne mreže zahteva holistički pristup uključujući i moguću primenu elemente PKI tehnologije zasnovane na industrijskim standardima. PKI je poznata tehnologija koju treba prilagoditi specifičnostima pametnih mreža. Po pitanju zaštite privatnosti podataka, na šta je javnost sve osetljivija, jedno od rešenja su procedure za anonimno predstavljanje podataka o trenutnom opterećenju u mreži.

LITERATURA

1. A.R. Metke and R.L. Ekl, 2010, „Security Technology for a Smart Grid Networks“, „IEEE Transactions on Smart Grid“.“Vol.1.No.1.
2. Zhuo Lu, Xiang Lu, Wenye Wang, and Cliff Wang, October-November 2010,"Review and Evaluation of Security Threats on the Communication Networks in the Smart Grid", in Proc. of IEEE Military Communications Conference (Milcom' 10).
3. V.K.Sood, D.Fischer, J.M.Eklund, T.Brown, 2009 „Developing a Communication Infrastructure for the Smart Grid“, „IEEE Electrical Power Energy Conference EPEC (2009) Vol.:4, Issue:10, IEEE“, 1-7
4. C.Efthymiou, G.Kalogridis, 2010, „Smart Grid Privacy via Anonymization of Smart Metering Data“, IEEE, Pages: 238-24
5. T.Baumeister, 2010, “Literature Review on Smart Grid Cyber Security”,University of Hawai`i Honolulu, HI, 26-27
6. A. Lee, 2009, „Smart Grid Cyber Security Strategy and Requirements”, NIST
7. Y. Liu, P. Ning, and M. Reiter, 2009, “False data injection attacks against state estimation in electric power grids,” in *Proc. of ACM Conference on Computer and Communications Security (CCS ’09)*.
8. M. LeMay and C. A. Gunter, 2009,“Cumulative attestation kernels for embedded systems,” in *Proc. of the European Symposium on Research in Computer Security (ESORICS ’09)*.

Vladan Josipović, JP EMS Bore Baruha 13, 14000 Valjevo, Srbija