Centar Informacijske Sigurnosti

Sigurnost pametnih kuća

travanj 2012.

CIS-DOC-2012-04-045

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

Pametne mreže (eng. *Smart Grid*) posljednjih godina izazivaju ogroman interes i danas predstavljaju jedno od glavnih područja istraživanja u elektroenergetici. Cilj pametnih mreža je poboljšati trenutni elektroenergetski sustav integracijom obnovljivih izvora energije i raznih informacijsko-komunikacijskih tehnologija. Jedna od osnovnih ideja je stvoriti uvjete za dvosmjernu komunikaciju između korisnika i električne mreže. Na taj bi se način moglo napraviti bolje predviđanje potrošnje u nekom razdoblju, brže otkriti razne kvarove, ali i optimirati mrežu ovisno o trenutnim potrebama korisnika.

Osnovna jedinica u pametnoj mreži je pametna kuća (eng. *Smart House*) ili pametna zgrada. Ranije spomenuta komunikacija između mreže i potrošača ostvaruje se preko pametnog brojila (eng. *Smart Meter*). Ono će biti detaljnije opisano u poglavlju 3.2, ali očito je potrebno osigurati sigurnost te komunikacije kako nitko ne bi mogao utjecati na rad pametnog brojila.

Osim pametnog brojila i komunikacije s mrežom, pametna kuća ima niz drugih sustava koji su umreženi i međusobno povezani. To ih čini potencijalno podložnim napadima i nužno je provjeriti i osigurati sigurnost tih sustava kako bi se ukućani osjećali sigurno u vlastitome domu. Osim samih ukućana u pametnoj kući, sigurnost njenih sustava svakako je važna i operatoru električne mreže kako ne bi došlo do manipulacije informacijama o potrošnji ili čak izazivanja kvara u mreži.

U poglavlju 2 ovog dokumenta ukratko će biti opisane ideje i princip rada pametne mreže. Poglavlje 3 bavit će se detaljnim opisom pametne kuće i tehnologijama koje se u njoj koriste, dok će u poglavlju 4 biti analizirana sigurnost pametne kuće.

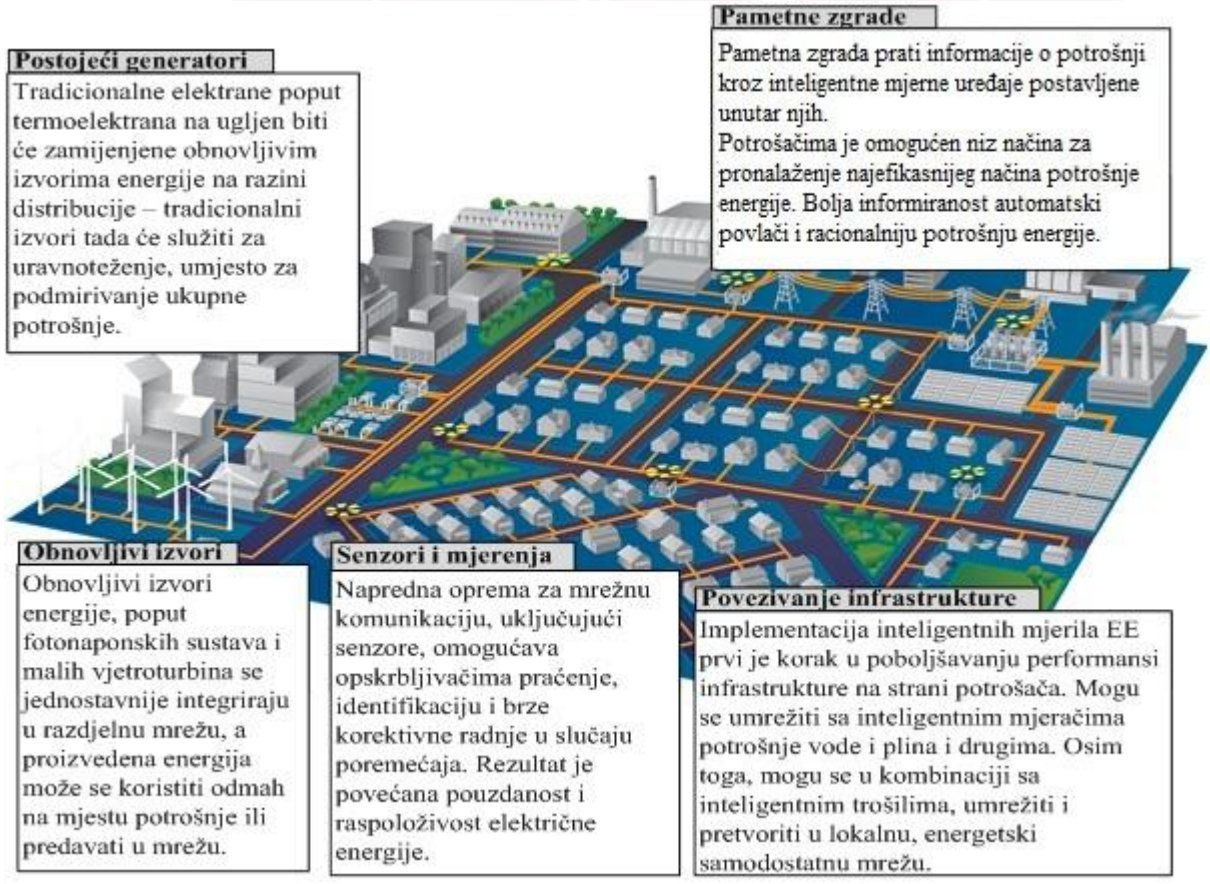
2. Pametna mreža

Kako bi se shvatila pozicija i uloga pametne kuće, u ovom će se poglavlju ukratko opisati ideje pametne mreže.

Glavna obilježja pametne mreže su:

- dvosmjerna komunikacija s potrošačima,
- lokalna i decentralizirana proizvodnja,
- jednostavna integracija malih obnovljivih izvora energije,
- veća učinkovitost u odnosu na klasičnu električnu mrežu,
- nadzor električne mreže u svim njenim čvorovima,
- aktivno uključenje potrošača u proizvodnju (preko malih obnovljivih izvora u pametnoj kući) i potrošnju električne energije,
- promjena cijene električne energije u stvarnom vremenu, ovisno o trenutnoj potrošnji u mreži, kako bi se uravnotežila dnevna krivulja potrošnje.

Slika 1 prikazuje osnovne koncepte pametne mreže [2]. Uz neophodnu integraciju obnovljivih izvora energije u postojeću električnu mrežu, pametna mreža podrazumjeva komunikaciju s potrošačima. Na taj se način osigurava veća učinkovitost te omogućuje upravljanje opterećenjem i potrošnjom u mreži. Osim toga, dvosmjerna komunikacija omogućuje proizvođaču i distributeru uvid u stanje mreže u svakom njenom čvoru te brzo otkrivanje potencijalnih problema. Osim obnovljivih izvora energije, osnovni elementi u pametnoj mreži su pametne kuće i zgrade te pametna električna brojila, koji će biti opisani u idućem poglavlju.



Slika 1. *Prikaz pametne mreže*
Izvor: *ieeeexplore.ieee.org*

Komunikacija između susjednih pametnih kuća u kombinaciji s malim obnovljivim izvorima energije u svakoj pametnoj kući vodi do stvaranja tzv. mikromreža. Ukoliko se dogodi nekakav kvar u mreži i izazove prekid dovoda električne energije, mikromreža se može sama izorganizirati tako da optimalno iskoristi izvore energije s kojima raspolaže i razdjeli električnu energiju među pametnim kućama.

3. Pametna kuća

Pojam pametne kuće (ili pametne zgrade) nastao je sedamdesetih godina prošlog stoljeća. Tada se pametnom kućom smatrala ona koja je bila sagrađena imajući na umu energetsku učinkovitost. Pojam pametne kuće od tada se mjenjao prateći razvoj tehnologije na tom području. Tako je tijekom osamdesetih godina pametna kuća bila ona u kojoj se s osobnog računala moglo upravljati raznim sustavima. Današnje poimanje pametne kuće predstavlja nadogradnju definicija iz prošlosti dodatkom podsustava za gospodarenje energijom i utjecaj na okoliš te primjenom raznih senzora i sustava za automatizaciju.

Tipične tehnologije i sustavi koji se koriste u pametnoj kući su:

- **obnovljivi izvori energije** – mikro vjetroturbine ili solarne ćelije, preko pametnog brojila usklađeni su s mrežom i šalju električnu energiju, ovisno o potrebi, u kuću ili u mrežu,
- **pametno brojilo** – služi za komunikaciju potrošača i mreže, nudi korisniku informaciju o trenutnoj cijeni električne energije u stvarnom vremenu,
- **mogućnost odabira tarife** – potrošačima se nudi mogućnost da izaberu između raznih tarifa, npr. 100% „zelene“ električne energije ili najjeftinije tarife,
- **električni automobil** – pametna kuća nudi mogućnost spajanja električnog automobila kao dodatnog spremnika električne energije koji se po potrebi može iskoristiti u razdoblju najveće potrošnje,
- **senzori** – mreža senzora postavljenih unutar kuće daje informaciju o trenutnom položaju ukućana te sukladno tome omogućuje automatsko upravljanje nekim sustavima (npr. gašenje nekih uređaja ili smanjenje grijanja/hlađenja u praznim prostorijama),
- **središnja jedinica –** služi za programiranje sustava u pametnoj kući,
- **pametni sustavi grijanja** – omogućuju djeljenje toplinske energije između susjednih kuća,
- **širokopojasna veza** – omogućuje komunikaciju senzora i sustava unutar kuće, ali i komunikaciju sa susjednim pametnim kućama i pametnom mrežom,
- **pametna trošila** – uređaji koji prate stanje u mreži te se mogu automatski paliti ili gasiti sukladno zadanim uvjetima.

Slika 2 prikazuje ilustraciju pametne kuće.

U nastavku će biti opisan rad nekih osnovnih komponenata pametne kuće: sustava za upravljanje trošilima, pametnih trošila te pametnog brojila. Ti su sustavi međusobno umreženi te povezani sa susjednim pametnim kućama i cijelom pametnom mrežom te predstavljaju i kritične točke što se tiče napada na pametnu kuću.

Slika 2. *Ilustracija pametne kuće*
Izvor: *worldchanging.com*

3.1. Sustav za upravljanje trošilima

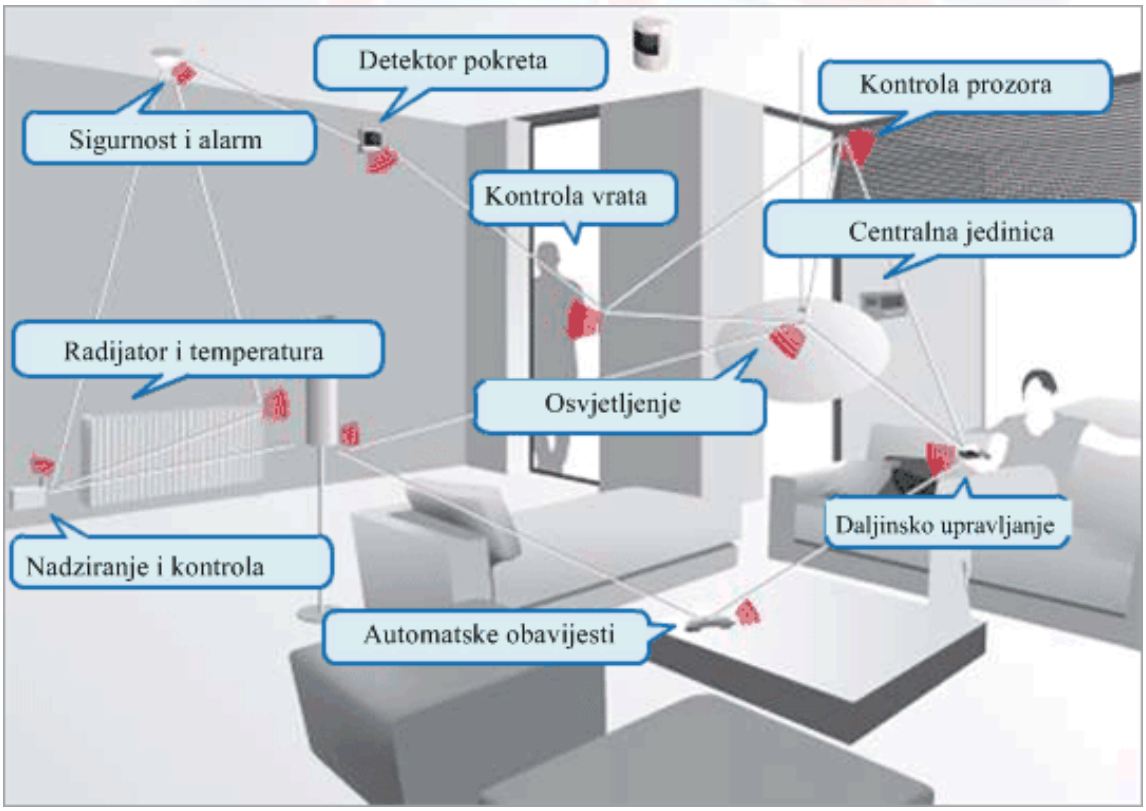
Kako bi se raznim uređajima u pametnoj kući moglo upravljati s jednog mjesta razvijen je sustav za upravljanje trošilima. On omogućuje korisniku da isprogramira rad trošila u kući ovisno o uvjetima u mreži. Primjerice, potrošač može odabrati nekoliko različitih postavki za termostat ili rasvjetu (ovisno o trenutnoj cijeni električne energije). Također, može odabrati kada će, ovisno o nekim uvjetima, raditi pametna trošila. Tipičan primjer je uključivanje perilica za rublje ili posuđe u trenutcima niže cijene električne energije.

Osnova sustava za upravljanje trošilima je središnja jedinica. Primjer središnje jedinice prikazuje Slika 3. Središnja jedinica povezana je s pametnim brojilom i tako dobiva informacije o trenutnom stanju u mreži i cijeni električne energije. Dobiva i informaciju o vremenu koja se također može iskoristiti kod programiranja rada različitih uređaja, što je posebno korisno kod termostata i rasvjete.

Slika 3. *Središnja jedinica sustava za upravljanje trošilima*
Izvor: *impactlab.net*

Središnja jedinica povezana je i s raznim senzorima koji su postavljeni u pametnoj kući. Na taj način trošilima se može upravljati i ovisno o položaju ukućana ili informaciji o trenutno otvorenim prozorima i vratima u kući.

Slika 4 prikazuje vezu između raznih sustava koji zajedno čine sustav za upravljanje trošilima [2].



Slika 4. *Sustav za upravljanje trošilima*
Izvor: *ieeeexplore.ieee.org*

3.1.1. Pametna trošila

Pametna trošila imaju mogućnost spajanja sa sustavom za upravljanje trošilima ili pametnim brojilom, a samim time povezani su i s cijelom pametnom mrežom.

Općenito, pametna trošila podržavaju tri različita načina rada:

- potpuno automatizirano, trošilo radi prema zahtjevima korisnika ili mreže, ne može se koristiti drugačije,
- djelomično automatizirano, trošilo radi kao i u prvom slučaju, ali moguće ga je izvanredno uključiti i u drugim situacijama (npr. za vrijeme skupe struje),
- individualan način rada, u kojem korisnik može podesiti vremenske periode u kojem će trošilo raditi automatski (npr. dok nema nikoga doma).

Slika 5 opisuje kako rade pametni grijači vode, perilica posuđa, perilica rublja i hladnjak [2].

Slika 5. *Primjer rada nekih pametnih trošila*
Izvor: *ieeeexplore.ieee.org*

3.2. Pametno brojilo

S elektroenergetskog stajališta, pametno brojilo je osnovna komponenta u pametnoj kući. Klasična brojila nemaju mogućnost komunikacije s mrežom, a mjere samo ukupnu potrošnju. To znači da se njima ne može za svakog potrošača odrediti dnevna krivulja potrošnje električne energije. Pametna brojila prate potrošnju svaki sat i odmah šalju informaciju operatoru mreže i samom potrošaču. Ono što je bitno sa stajališta sigurnosti je to da operator mreže može preko pametnog brojila isključiti korisnika iz mreže. To otvara mogućnost potencijalnom napadaču da učini isto [8].

Slika 6 prikazuje pametno brojilo. Pametno brojilo predstavlja glavnu sigurnosnu prijetnju u pametnoj kući, o čemu će biti više govora u idućim poglavljima.

Slika 6. *Pametno brojilo*
Izvor: *wikipedia*

Veliki problem kod pametnih brojila predstavlja odabir tehnologije za komunikaciju. Pametno brojilo mora neprestano biti povezano s mrežom, tj. ne smije doći do prekida. Zbog toga odabir korištene tehnologije ovisi i o mjestu na kojoj se pametno brojilo ugrađuje.

Najčešće korištena žičana tehnologija je komunikacija preko električne mreže (eng. *Power Line Communication*). Ta tehnologija kao prijenosni medij iskorištava električne vodove. Signal koji prijenosi podatak dodaje se 50 hercnom signalu napona te se na prijemnoj strani izdvaja filtracijom.

Kod bežičnih prijenosa koriste se globalni sustav za mobilnu komunikaciju (eng. *Global System for Mobile Communication,* GSM), bežične lokalne mreže (eng. *Wireless Local Area Network,* WLAN) ili sve češće WiMAX (eng. *Worldwide Interoperability for Microwave Access*).

4. Sigurnost pametne kuće

Većina sustava u pametnoj kući radi bez prestanka, a cijelo vrijeme postoji i komunikacija s mrežom. Nužno je osigurati sigurnost sustava u pametnoj kući i zaštititi ih od napada.

4.1. Sigurnosni sustavi u pametnoj kući

U ovom će se poglavlju ukratko opisati dva karakteristična sustava u pametnoj kući koji služe za fizičku zaštitu kuće.

4.1.1. Sustavi za kontrolu pristupa

Ovaj se sustav sastoji od sigurnosnih kamera, detektora pokreta i raznih sličnih mehanizama zaštite i detekcije uljeza u kući i oko nje. U slučaju kad je netko od ukućana kod kuće, takav će ga sustav upozoriti da se približava nepoznata osoba. Ako pak nema nikoga kod kuće, sustav se može programirati da, primjerice, pošalje ukućanima poruku da je nepoznata osoba blizu njihove kuće ili im čak pošalje video koji trenutno snima sigurnosna kamera. Kako bi se raspoznalo radi li se doista o nepoznatoj osobi (i potencijalnom uljezu), koriste se informacije sa sigurnosnih kamera i algoritmi za prepoznavanje lica. U slučaju da uljez pokuša provaliti u kuću, pametna će kuća automatski uputiti poziv policiji.

4.1.2. Sustav za zaštitu od požara

Ovaj sigurnosni sustav pametne kuće mnogo je više od običnog dimnog alarma. Ovaj sustav prati sve prostorije u kući i u njima mjeri razinu ugljičnog monoksida i temperaturu. Na taj način može ne samo otkriti požar, već i točnu lokaciju na kojoj je požar izbio i automatski proslijediti tu informaciju vatrogascima.

4.2. Sigurnosni modeli za zaštitu od računalnih napada

S aspekta računalne sigurnosti sustava pametne kuće moguće je napraviti podjelu na tri različita modela, ovisno o tome tko se brine za sigurnost sustava (vlasnik kuće ili vanjski pružatelj usluge) te o broju sustava koji su nadzirani (jedna pametna kuća ili više njih) [1]:

- **Sustav nadziran od strane vlasnika kuća** (eng. *Owner Supported Single Smart House System,* OSS) – u ovom, najjednostavnijem, modelu vlasnik kuće (i njeni ostali ukućani) održavaju sustave u pametnoj kući. Ovakav model često nije primjeren jer samo mali broj ljudi posjeduje dovoljno znanja za samostalno održavanje sustava i brigu o sigurnosti. Zbog toga bi bolji izbor bio model u kojem je briga za sigurnost prepuštena profesionalcima što je ideja idućeg modela.
- **Sustav nadziran izvana** (eng. *Externally Supported Single Smart House System,* ESS) – u ovom se modelu za informacijsko-komunikacijske tehnologije (eng. *Information and Communication Technologies,* ICT), a posebice za osiguranje njihove sigurnosti, prepušta pružatelju ICT usluga koji osigurava prikladan odabir sigurnosnih metoda te njihovu ispravnu provedbu i održavanje.
- **Više sustava zajednički nadzirani izvana** (eng. *Externally Supported Multiple Smart House System*, ESM) – ideja ovog modela i razlika u odnosu na prethodni jest u tome što bi u ESM modelu postojao pružatelj usluga pametne kuće preko kojega bi išla sva komunikacija te bi tako sigurnost sustava bila povećana.

4.3. Analiza računalnih sigurnosnih prijetnji

U ovom će se poglavlju opisati neki mogući napadi na sustave pametne kuće i analizirati njihove potencijalne posljedice. Isto tako, vidjet će se za koji su od ranije spomenutih sigurnosnih modela pojedine vrste napada najkritičnije.

Pametnu je kuću potrebno zaštiti od neovlaštenog pristupa sustavu, bilo neovlaštenih korisnika ili neovlaštenih vanjskih sustava. Neovlaštene korisnike možemo podijeliti u aktivne (imaju mogućnost čitanja i promjene podataka u sustavu) i pasivne (mogu samo čitati podatke). Potonji su također vrlo opasni jer mogu, primjerice, dobiti informaciju iz kućnih senzora i na taj način saznati gdje se ukućani nalaze u kojem trenutku ili jesu li uopće kod kuće. Aktivni neovlašteni korisnik je još puno opasniji jer može manipulirati sustavom (ili nekim njegovim dijelovima), izvoditi naredbe umjesto pravog korisnika ili u sustav ubaciti trojanskog konja (eng. *Trojan horse*). Neovlašteni pristup predstavlja najveću opasnost u pametnoj kući.

Opasnost od neovlaštenog pristupa postoji u sva tri sigurnosna modela. Ipak, problemi vezani uz privatnost korisnika veći su u modelima ESS i EMS budući da tamo korisnik nije jedini koji ima pristup sustavu. Zbog toga bi organizacije koje korisniku održavaju sustav morale imati ograničen pristup kako ne bi mogle pristupiti privatnim informacijama.

Prijetnju za sustav predstavljaju i zloćudni programi (eng. *Malware*). Oni mogu utjecati na rad programa u sustavu i tako ugroziti ili prekinuti rad sustava. Napadi uskraćivanja usluga (eng. *Denial of Service, DoS*) također mogu izazvati prekid rada u sustavu.

4.4. Sustavi za zaštitu od računalnih napada

Kao mjera zaštite od ranije spomenutih sigurnosnih prijetnji provode se neke tehnološke (npr. antivirusni alati, vatrozidi i sl.) te proceduralne zaštitne mjere (npr. ažuriranje programa). U ovom će poglavlju biti opisane neke od sigurnosnih mjera koje se primjenjuju u pametnim kućama kao zaštita od sigurnosnih prijetnji.

4.4.1. Kontrola pristupa

U prošlom je poglavlju neovlašteni pristup označen kao najveća opasnost u pametnoj kući. Najbolju obranu od njega pruža dobro izvedena kontrola pristupa sustavima pametne kuće.

Osnova kontrole pristupa je dodjela različitih prava pristupa različitim korisnicima. Neke funkcije (npr. kontrola rasvjete) mogu se dodjeliti svim korisnicima, ali nekim je korisnicima (djeci, posjetiteljima) moguće ograničiti određene funkcije. Također, u prvom sigurnosnom modelu (OSS) važno je napraviti posebni administratorski korisnički račun koji će se koristiti samo kod administracije sustava.

Postupak autentifikacije i provjere identiteta korisnika koji se prijavljuje u sustav treba biti što jednostavniji, ali dovoljno siguran. Dugačke lozinke nisu prikladne jer se korisnicima ne da svaki puta ih unositi. Dobro rješenje za taj problem je biometrijska zaštita otiskom prsta. S obzirom na tipično malen broj korisnika u pametnoj kući moguće je napraviti vrlo učinkovito prepoznavanje otisaka prstiju. Međutim, takav sustav zaštite nije prikladan kod pristupa na daljinu koji je često dio pametne kuće.

4.4.2. Vatrozid i antivirusni alat

Vatrozid se koristi u sustavu kako bi kontrolirao odlazni i dolazni mrežni promet te spriječio napade na mrežu. Problem je što vatrozidi nisu dovoljna zaštita od naprednijih napada uskraćivanja usluga, iako nude određenu razinu zaštite. Kao zaštitu od zloćudnih programa pametna kuća koristi neki od antivirusnih alata.

4.4.3. Povrat podataka

Povremeno će sigurno doći do greške i prekida rada u sustavu. To se ne mora nužno dogoditi kao posljedica napada, već jednostavno kao posljedica činjenice da sustav radi neprestano. U takvoj se situaciji sustav mora moći resetirati te učitati najnovije spremljene postavke programa.

4.5. Sigurnost pametnog brojila

Pametna brojila već se i danas ugrađuju u mnoga kućanstva u nekim zemljama i nude operateru mogućnost neprestanog praćenja potrošnje te isključenja korisnika na daljinu. Integracijom u pametnu kuću pametno će brojilo biti povezano sa svim ostalim pametnim uređajima te će tako predstavljati još veću sigurnosnu prijetnju.

Pametno brojilo možemo razdvojiti u dva sustava.

Prvi je onaj koji radi samo mjerenje potrošnje električne energije, odnosno ima istu funkcionalnost kao stara, analogna brojila. Taj dio sadrži i informaciju o trenutnoj cijeni električne energije. Ako bi napadač mogao pristupiti tome dijelu pametnog brojila, mogao bi manipulirati iznosom potrošene električne energije. Naravno, to bi u većini slučajeva bilo na štetu dobavljača električne energije, odnosno potrošač bi pokušao postaviti nižu cijenu u pametno brojilo. Trenutno ne postoje dokazi da je nekome to pošlo za rukom.

Drugi dio pametnog brojila je zapravo „pametni“ dio. On uključuje memoriju u kojoj se spremaju podaci, vezu s ostalim sustavima u kući i mrežom te mikrokontroler koji svime upravlja. Napadi na taj dio pametnog brojila obično se temelje na izravnom priključivanju na brojilo i ispitivanjem signala u njemu.

Napad koji predstavlja možda najveću prijetnju zbog relativne jednostavnosti je analiza potrošnje električne energije. Na prvi pogled ne radi se o napadu u pravom smislu te riječi, ali iz tih se podataka može saznati mnogo o dnevnim navikama ili trenutnom položaju ukućana. Za dobivanje informacije o potrošnji dovoljno je poznavati MAC (eng. *Media Access Control*) adresu pametnog brojila, a iz dobivenih podataka moguće je čak, primjerice, odrediti koji tv program ukućani trenutno gledaju [8].

4.6. Preporuke za sigurnost pametne kuće

Ovisno o korištenom sigurnosnom modelu, postoje određene preporuke kako bi se povećala sigurnost pametne kuće. OSS model pametne kuće, u kojem ukućan sam održava sustave i brine se za sigurnost mreže, preporuča se samo korisnicima koji imaju dovoljno znanja za to. Ostalima se preporuča korištenje drugog ili trećeg modela, u kojima će sigurnost sustava pametne kuće biti u rukama profesionalaca. Važno je detaljno proučiti kakvo osiguranje nudi organizacija kojoj namjeravaju povjeriti sigurnost svoje pametne kuće.

Isto kao i kod osobnih računala, preporuka je često raditi *backup* podataka kako bi se po potrebi uvijek mogao napraviti uspješan povrat podataka i ponovno pokretanje sustava. Korisnicima se preporuča detaljno proučavanje potrebe svakog od ukućana kako bi se adekvatno definirala kontrola pristupa sustavu. Prava dodjeljena osobama koje samo privremeno borave u kući (gosti, podstanari) potrebno je ukinuti čim te osobe napuste kuću.

Konačno, najvažnije je da svi ukućani razumiju potencijalnu sigurnosnu prijetnju te da savjesno rukuju sustavima pametne kuće.

5. Studije o sigurnosti pametnih kuća i budućnost

Problem u trenutnoj procjeni sigurnosti pametnih kuća predstavlja činjenica da nema ozbiljnih studija koje bi detaljno analizirale sve potencijalne napade. Zasad su sve informacije o potencijalnim napadima na hipotetskoj razini i nije poznato koji je napad najučinkovitiji niti što se sve točno može postići uspješnim napadom na neki od sustava pametne kuće.

Jedan od razloga što je trenutno stanje takvo je i taj što je tehnologija pametnih kuća (pametno brojilo i ostali sustavi) relativno nova i još uvijek slabo zastupljena u kućanstvima. Kako će se pametne kuće širiti, sigurno će se povećati interes za napadima na njih, a samim time i za detaljnijom analizom sigurnosti.

S obzirom na potencijalno veliku štetu koju bi mogao izazvati uspješan napad, proizvođači sustava koji se koriste u pametnim kućama, a posebice pametnih brojila moraju i u budućnosti vrlo ozbiljno shvatiti sigurnost svojih proizvoda. Ukoliko se pronađe sigurnosna rupa u, primjerice, pametnom brojilu koje je ugrađeno u milijune kućanstava, posljedice bi mogle biti ogromne. Zbog toga je i nužno redovito provođenje ispitivanja sigurnosti sustava kako bi se osiguralo da se stvarni napadi (barem oni koji bi izazvali veliku štetu) nikada ne dogode.

6. Zaključak

Broj pametnih kuća danas je, pogotovo u Hrvatskoj, prilično malen. Međutim, trenutni je trend u elektroenergetici intenzivno istraživanje i razvoj pametnih mreža koje su, po svemu sudeći, budućnost elektroenergetskog sustava. To će potaknuti i sve veći broj ljudi da svoju kuću pretvore u pametnu kuću.

Opasnost od napada na pametnu kuću je velika zbog činjenice da mnogi sustavi u kući međusobno komuniciraju, što znači da napadač može dobiti mnoge informacije. Druga velika opasnost proizlazi iz veze pametne kuće s drugim kućama i električnom mrežom, što napadač također može potencijalno iskoristiti.

Međutim, ne postoji nikakva ozbiljna studija koja bi pokazala koliko je strah od napada na pametnu kuću i pametno brojilo opravdan. U Sjedinjenim Američkim Državama trenutno traje prijelaz na pametna brojila što je izazvalo strah od mogućih napada na privatnost potrošača. Mediji su prenijeli vijesti o tome kako je pametna brojila moguće hakirati zbog čega se pojavila dodatna sumnja u njihovu sigurnost, ali još uvijek nije prikazano na koji se način to može postići i kakva se točno šteta može nanijeti. Trenutno je sve još uvijek na hipotetskoj razini.

Ipak, potencijalna šteta od napada na pametnu kuću je velika. Zbog toga ne treba čekati da se stvarni napad dogodi i zatim sanirati štetu, već je potrebno detaljno analizirati i osigurati sigurnost svih sustava u pametnoj kući. Nažalost, čini se da se trenutno premalo radi na tom području i da ne postoji dovoljno informacija i testova koji bi pokazali koliko su ti sustavi danas sigurni.

7. Leksikon pojmova

MAC protokol – komunikacijski protokol za pristup mediju

Media Access Control (MAC) je protokol za komunikaciju podacima, također poznat kao Medium Access Control protokol (protokol upravljanja pristupom mediju). On omogućuje mehanizme adresiranja i kontrole pristupa kanalima koji služe za komunikaciju terminala, odnosno čvorišta, s mrežom koja ima više pristupnih točaka.

http://ahyco.ffri.hr/ritehmreze/teme/mac.htm

Autentikacija - Autentikacija je proces potvrđivanja identiteta podatka ili osobe.

Autentikacija je proces određivanja identiteta nekog subjekta, najčešće se odnosi na fizičku osobu. U praksi subjekt daje određene podatke po kojima druga strana može utvrditi da je subjekt upravo taj kojim se predstavlja. Najčešći primjeri su: uz korištenje kartice na bankomatu i upisivanje PIN-a, ili upisivanje (korisničkog) imena i zaporke.

http://searchsecurity.techtarget.com/definition/authentication

Virus - Računalni virus

Virusi su programi koji se mogu kopirati i zaraziti računalo bez znanja ili dopuštenja korisnika. Računalo se može zaraziti na razne načine preko Internet-a, CD-a, USB-a... Virusi dolaze većinom sa drugim programima, kao što su npr. Trojanski konji kako bi maskirali svoj rad i kako bi ih bilo još teže za otkriti. Namjene virusa su različite, mogu služiti samo kako bi radili štetu no neki su manje štetni i samo usporavaju računalo i smetaju korisniku u radu. Virusi se spremaju u memoriju računala i pokreću se s operacijskim sustavom i inficiraju programe koji se pokreću.

http://www.ust.hk/itsc/antivirus/general/whatis.html

Trojanski konj - Zloćudni program koji se pretvara kao legitimna aplikacija

Trojanski konj je oblik zloćudnog programa koji se pretvara kao legitimna aplikacija. U početku se pretvara kao da obavlja korisnu funkcionalnost za korisnika, no u pozadini izvodi štetne radnje (na primjer, krađa informacija). Za razliku od crva, ovaj oblik zloćudnih programa se ne širi samostalno.

http://www.webopedia.com/TERM/T/Trojan_horse.html

WiMax - Worldwide Interoperability for Microwave Access

WiMax je bežična mreža za širokopojasni pristup Internetu za fiksne ili mobilne korisnike. Trenutačna inačica WiMax standarda omogućuje brzine do 40 Mbit/s.

http://info.biz.hr/Typo3/typo3_01/dummy-3.8.0//index.php?id=485

WLAN - Wireless Local Area Network

WLAN služi za bežično povezivanje dva ili više računala u lokalnu mrežu, a omogućuje i pristup Internetu preko bežične pristupne točke. Najrašireniji standard u WLAN mrežama je standard 802.11 ili Wi-Fi.

http://searchmobilecomputing.techtarget.com/definition/wireless-LAN

8. Reference

[1] CENELEC Workshop Agreement – SmartHouse Code of Practice

[2] Boran Morvaj – Završni rad, Simulacija interakcije potrošača i operatora sustava u pametnoj mreži

[3] Wikipedia – Smart Grid,
http://en.wikipedia.org/wiki/Smart_grid, travanj 2012.

[4] Wikipedia – Smart Meter,
http://en.wikipedia.org/wiki/Smart_meter, travanj 2012.

[5] Wikipedia – Home Automation,
http://en.wikipedia.org/wiki/Home_automation, travanj 2012.

[6] Erica Naone – Hack Meters for the Smart Grid,
http://www.technologyreview.com/read_article.aspx?id=23179&ch=computing&a=f&pw7=T, travanj 2012.

[7] Dario Carluccio, Stephan Brinkhaus – Smart hacking for privacy,
http://www.youtube.com/watch?v=YYe4SwQn2GE&lr=1&uid=wBVURsT1hSnFT8vGO6vSqw, travanj 2012.

[8] Ken Kalthoff – Smart Meters Can Be Hacked: Security Experts,
http://www.nbcdfw.com/news/local/Smart-Meters-Can-Be-Hacked-Security-Experts-59943982.html, travanj 2012.

[9] Victoria NIcks – Artificial Intelligence Programs Improve Home Automation Technology,
http://victoria-nicks.suite101.com/ai-enhances-the-smart-home-security-system-a136697, travanj 2012.

[10] Chester Wisniewski – Smart meter hacking can disclose which TV shows and movies you watch,
http://nakedsecurity.sophos.com/2012/01/08/28c3-smart-meter-hacking-can-disclose-which-tv-shows-and-movies-you-watch/, travanj 2012.