NASTAVNO-NAUČNOM VEĆU ELEKTROTEHNIČKOG FAKULTETA U BEOGRADU

Komisija za drugi stepen studija Elektrotehničkog fakulteta u Beogradu imenovala nas je za članove Komisije za pregled i ocenu master rada kandidata **Stefane Krivokuće** pod naslovom **„Analiza rada sistema pametne distribucije vode sa aspekta sajber sigurnosti“**. Nakon pregleda rada podnosimo Nastavno-naučnom veću sledeći

IZVEŠTAJ

1. Biografski podaci

Stefana Krivokuća je rođena 30.11.1996. godine u Beogradu. Završila je osnovnu školu "Filip Kljajić Fića" u Beogradu kao vukovac. Upisala je Trinaestu beogradsku gimnaziju u Beogradu koju je završila sa odličnim uspehom. Elektrotehnički fakultet upisala je 2015. godine. Diplomirala je 2019. godine na odseku za Telekomunikacije i informacione tehnologije, smer Sistemsko inženjerstvo. Diplomski rad „Frekvencijsko planiranje radio-relejne mreže na teritoriji grada Beograda“ odbranila je u septembru 2019. godine sa ocenom 10. Diplomske akademske – master studije na Elektrotehničkom fakultetu u Beogradu, na Modulu za sistemsko inženjerstvo i radio komunikacije, upisala je u oktobru 2019. godine. Položila je sve ispite sa prosečnom ocenom 10.

2. Predmet master rada

Sistemi za distribuciju vode svakim danom postaju sve automatizovaniji. Kako se složenost ovih sistema brzo povećava, pojavljuju se novi izazovi po pitanju bezbednosti. Pored složenog funkcionisanja, savremeni sistemi zahtevaju i mehanizme koji mogu otkriti sajber napade i pokrenuti odgovarajuću reakciju ukoliko je potrebno. Način borbe protiv pojedinaca sa lošim namerama napadača je korišćenje dodatnih elemenata koji će pokušati da obezbede sigurnost u sistemu.

Sistem za pametnu distribuciju vode predstavlja kolekciju rezervoara, pumpi, ventila i cevi koje isporučuju pitku vodu krajnjim korisnicima. Različite vrste pametnih uređaja se dodaju ovim sistemima, uključujući senzore koji mogu da mere kvalitet vode, nivo vode u rezervoaru ili pritisak u cevi i kontrolere (*Programmable Logic Controllers*) koji, na primer, mogu automatski uključiti pumpu kad je rezervoar blizu praznog, itd. Takođe postoje SCADA (*Supervisory Control And Data Acquisition*) sistemi koji nadgledaju i kontrolišu uređaje širom mreže. Iako sve ove inovacije mogu omogućiti sistemu da radi pouzdanije i efikasnije, oni takođe izlažu sistem potencijalnim napadima. Napadi sežu od jednostavne krađe podataka do oštećenja opreme, prekida dovoda vode ili čak puštanja tosičnih hemikalija u vodu. Da bi se sprečili ovi napadi i da bi se moglo brzo reagovati na njih, ako se oni dogode, važno je implementirati sigurnost od faze dizajniranja sistema, čineći sistem otpornim na napade u što većoj meri.

U tipičnom sistemu za distribuciju vode glavna briga distributera je obezbeđivanje čiste vode i obezbeđivanje odgovarajuće količine vode. Imajući u vidu ove aspekte sistema distribucije vode, u ovom radu je napravljena formalna analiza za scenario zagađenja vode i scenario prelivanja vode u rezervoaru. Prvi korak u obezbeđivanju bezbednosti sistema je otkrivanje koje su slabosti arhitekture i beleženje načina na koje se te slabosti mogu iskoristiti za ostvarivanje napada. Procesom modelovanja pretnji sistema u alatu *Microsoft Threat Modeling Tool* dobija se lista relevatnih pretnji čijom analizom se ustanovljavaju slabosti sistema.

Formalna verifikacija predstavlja proces dokazivanja ispravnosti sistema ispitivanjem da li se isti ponaša u skladu sa projektovanim dizajnom. Ovim postupkom je omogućena identifikacija nedostataka, koji se mogu prevazići redizajniranjem sistema. Jedan od načina postizanja formalne verifikacije je apstrakcija sistema i stvaranje matematičkog modela sa ciljem dobijanja merljivih rezultata. Tokom modelovanja sistema uzete su u obzir slabosti, dobijene po završetku procesa modelovanja pretnji, način funkcionisanja sistema kao i ponašanje napadača koje je nedeterminističke prirode. U slučaju napada, napadač će doći do svog cilja manipulacijom određenih segmenata sistema, odnosno, eksploatacijom postojećih slabosti. Podrazumeva se da je napadač svestan slabosti sistema i da je izbor slabosti koji će eksploatisati nepredvidiv odn. slučajan. Takođe, imajući u vidu da mogućnosti napadača nisu neograničene, uvrštena je granica u broju slabosti koje mogu biti eksploatisanje u okviru napada. Pored modelovanja sistema potrebno je definisati napade, odn. preduslove koji, kada su ispunjeni, predstavljaju prisustvo napada. Model sistema se zatim testira naspram potencijalnih napada korišćenjem alata *PRISM model checker*. Za svaki od pomenutih scenarija se vrši opisana analiza i po završetku procesa dolazi se do saznanja koje konfiguracije sistema su pogodnije sa aspekta sajber sigurnosti, odn. koje su otpornije na sajber napade.

Konačni rezultati analize pružaju uvid u to koje elemente treba uvrstiti u sistem i na šta treba obratiti pažnju tokom dizajniranja sistema kako bi se ispoštovali zahtevi po pitanju sigurnosti, posebno u *Security-by-design* pristupu.

3. Osnovni podaci o master radu

Master rad kandidata Stefane Krivokuća **„Analiza rada sistema pametne distribucije vode sa aspekta sajber sigurnosti“**, obuhvata 61 stranu štampanog teksta sa 9 slika, 9 tabela i 18 referenci. Rad je napisan na engleskom jeziku i organizovan je tako da sadrži uvod, pet poglavlja, zaključak, spisak literature, spisak slika, spisak tabela i prilog.

4. Sadržaj i analiza rada

U uvodnom poglavlju razmatrani su razlozi za izradu teze i dat je pregled poglavlja rada.

U drugom poglavlju iznesena su prethodna istaživanja vezana za sajber sigurnost sistema distribucije vode, kao i istraživački pristup korišćen u radu.

U trećem poglavlju predstavljena je arhitektura sistema pametne distribucije vode kao i scenariji od interesa za dalju analizu.

U četvrtom poglavlju opisan je proces modelovanja pretnji sistema korišćenjem alata *Microsoft Threat Modeling Tool* i kao rezultat ovog procesa izdvojene su slabosti komunikacione arhitekture sistema.

U petom poglavlju izvršeno je modelovanje sistema pametne distribucije vode za analizu rizika od sajber napada, procesom formalne verifikacije i korišćenjem alata *PRISM model checker*.

U šestom poglavlju prikazani su rezultati analize rizika i relevantna diskusija.

U sedmom poglavlji su izneti zaključci do kojih se došlo tokom izrade master rada kao i predlog mogućnosti daljih tokova rada.

Osmo poglavlje predstavlja spisak korišćene literature.

5. Zaključak i predlog

Master rad Stefane Krivokuća prikazuje rezultate analize rizika od sajber napada u sistemu pametne distribucije vode procesom formalne verifikacije, gde su u obzir uzeti scenariji zagađenja vode i prelivanja rezervoara. Najvažniji doprinosi master rada su sledeći:

- Kreiran je adekvatan model sistema i isti je ispitan s aspekta sajber napada korišćenjem alata *PRISM model checker*, dok je proces detekcije slabosti sistema automatizovan korišćenjem alata *Microsoft Threat Modeling Tool*.
- Na osnovu dobijenih rezultata postale su dostupne preporuke koje elemente uvrstiti i kako dizajnirati sistem da bude obezbeđen što veći nivo sigurnosti, odnosno, kako smanjiti šanse za realizovanje uspešnog sajber napada.

Na osnovu izloženog, članovi Komisije predlažu Nastavno-naučnom veću Elektrotehničkog fakulteta u Beogradu da rad Stefane Krivokuće, pod naslovom **„Analiza rada sistema pametne distribucije vode sa aspekta sajber sigurnosti“**, prihvati kao master tezu i da kandidatu odobri javnu usmenu odbranu.

Beograd, 28.08.2020.

Članovi komisije:

Dr Nataša Nešković, redovni profesor

Dr Aleksandar Nešković, redovni profesor