უსაფრთხოების ანალიზი და ნდობის მოდელები უსადენო ქსელებში

ლელა მირცხულავა

lela.mirtskhulava@tsu.ge

კომპიუტერული მეცნიერებების დეპარტამენტი

ზუსტ და საბუნებისმეტყველო მეცნიერებათა ფაკულტეტი

ივ. ჯავახიშვილის თბილისის სახელმწიფო უნივერსიტეტი

უნივერსიტეტის ქ. 13, თბილისი

ნაშრომში მოცემულია უსადენო WPA2 (Wi-Fi Protected Access 2) პროტოკოლის სერიოზული სისუსტეები, რომელიც აღმოჩენილ იქნა 2017 წლის ოქტომბერში კომპიუტერული მეცნიერებების სფეროში მომუშავე მეცნიერების მიერ. განხორციელებულ იქნა KRACK (Key Reinstallation Attack) შეტევა WPA2-ზე კრიპტოგრაფიულ პროტოკოლებში არსებული შეცდომების აღმოსაფხვრელად, რათა მოხდეს უკვე გამოყენებული გასაღების ხელახალი ინსტალაცია. მათ მოახერხეს აგრეთვე Wi-Fi-ის რამოდენიმე „ხელის ჩამორთმევის ოთხი გზის“ სისტემაზე შეტევა. არსებობს ნდობის სხვადასხვა ფორმები ქსელური უსაფრთხოების აღმოსაფხვრელად და განსაზღვრული რისკების შესამცირებლად.

მოცემულ სტატიაში განიხილება სხვადასხვა სახის ნდობის მოდელები, რომლებსაც იყენებენ სხვადასხვა კრიპტოგრაფიული სისტემები: ა) ნდობის ქსელი, რომელიც იყენებს “საიმედო კონფიდენციალობას (Pretty Good Privacy (PGP)), სადაც მომხმარებლები იყენებენ საკუთარ სანდო გასაღებებს, ბ) Kerberos - საიდუმლო გასაღებების განაწილების სქემა მესამე სანდო მხარის გამოყენებით, გ) სერტიფიკატები, რომლებიც მესამე სანდო მხარეებს და მომხმარებლებს ერთმანეთის აუტენტიფიკაციის საშუალებას აძლევენ. ყველა ზემოთ მოცემული მოდელი განსხვავდება სირთულის, მოცულობის, მასშტაბურობის და საერთო გამოყენების მიხედვით. მოცემული სტატია კი განიხილავს თუ რომელი მოდელი შეიძლება შეირჩეს მოცემული პრობლემის მოსაგვარებლად. მოცემულ სტატიაში, ამასთანავე, აღწერილია უსაფრთხოების ძირითადი პრობლემები და ნდობის მოდელების აგების მეთოდები ქსელის ქცევის მონიტორინგის მეშვეობით. მოცემული პრობლემის გადასაწყვეტად მოცემულია სწრაფი კრიპტოგრაფიული გადაწყვეტილება Wi-Fi ქსელებისათვის, რისთვისაც გამოიყენება NTRU კრიპტოსისტემა ღია გასაღებით (open source public-key), რომელიც იყენებს მესერზე დაფუძნებულ კრიპტოგრაფიას (lattice-based cryptography). NTRU-ს შეუძლია NTRUEncrypt ღია გასაღების დაშიფვრის ალგორითმის რეალიზება Java-ს გამოყენებით. NTRUEncrypt არის მესერზე დაფუძნებული და ცნობილია, როგორც შეუვალი და მიუღწეველი კვანტური კომპიუტერების მხრიდანაც. ხოლო კრიპტოსისტემები, როგორიცაა RSA ან ECC, ხშირად გამოიყენება და მათი გატეხვა თავისუფლად შეუძლიათ კვანტური კომპიუტერებს. აქედან გამომდინარე, NTRU მნიშვნელოვნად უფრო სწრაფია ვიდრე სხვა კრიპტოსისტემები ღია გასაღებით.