TALLINNA TEHNIKAÜLIKOOL
Inseneriteaduskond
Virumaa kolledž
Reaal- ja tehnikateaduste keskus

Grigory Tureev

Android rakenduse loomine ARP protokolli haavatavuse ekspluateerimiseks

Rakendusinfotehnoloogia õppekava lõputöö

Juhendaja: L. Joonas, lektor

Kaasjuhendaja: N. Ivleva, lektor

Kohtla-Järve 2017

KOKKUVÕTE

Diplomitöös "Android rakenduse loomine ARP protokolli haavatavuse ekspluateerimiseks" vaadeldi juhtmevabade lokaalsete võrkude (WLAN) turvalisuse probleemi, konkreetselt ARP (AddressResolutionProtocol) protokolli turvalisust, mille suhtes saab teostada MITM (Man-in-the-middle) tüüpi rünnaku - ARP-spoofing ja mille abil saab üle võtta teiste seadmete võrguliiklust, millega saab oma äranägemisel manipuleerida.

Tuginedes erinevatele allikatele analüüsis autor 2016 aastal toimunud erinevaid võrgurünnakuid ning jõudis järeldusele, et TCP/IP protokollide komplektile, milles töötab ARP-protokoll, teostatud rünnakud on endiselt juhtpositsioonil. Ning kuna ARP-protokolli haavatavus ei ole endiselt lahendatud, siis on kaitse seda liiki rünnakute vastu eriti oluline.

Autor analüüsis ARP-protokolli ning ka ARP-protokolli haavatavust kasutavat rakendust ning valis selle alusel ARP-protokollile teostatavat populaarse rünnakutüübi – ARP-spoofing.

Kuna antud valdkonnas olid juba olema antud rünnaku teostamiseks vajalikud rakenduses, siis autor analüüsis neid ja valis nende hulgast välja need, mida saab kasutada omaenda Android rakenduses.

Selle valdkonnas on juba olemas Android rakendused, mis kasutasid ARP-protokolli haavatavust. Seetõttu analüüsis autor ka neid, mille alusel töötas välja omaenda Android rakenduse, mis kasutab tänapäevaseid teeke ja abirakendusi, mis vastavad tänapäevastele standarditele.

Autor töötas välja sellise Android rakenduse, mis kasutades ARP-protokolli haavatavaust, võimaldab WLAN võrgus sessioonide ülevõtmist ning nende avamist rakenduse brauseriga, mis võimaldab näitlikult demonstreerida ARP-protokolli kasutamist.

Autori Android rakendus töötati välja arvestades teise sarnase funktsionaalsusega Android rakenduste puudujääke – juurutati täiendavaid funktsioone, mis lihtsustavad rakendusega töötamist ning ka täiustavad seda.

Tänasel päeval eksisteerib mitmeid ARP-spoofing rünnaku vastaseid variante, mis võimaldavad hoida ära kurjategijate rünnakut. Kuid vaatamata sellel, ei ole need meetodid kardinaalseks lahenduseks, vaid võimaluseks sulgeda haavatavuse lõhe. Nad võimaldavad kaitsta edastatavaid andmeid seni, kuni ei töötata välja muud globaalset lahendust.

Autori arvates on kõige usaldusväärsemaks ja universaalsemaks kaitsevahendiks kas VLAN (VirtualLocalArea Network) tüüpi võrkude kasutamine või ruuteril staatilise ARP-tabeli kasutamine, mis võimaldab ARP-spoofing rünnaku täielikult ära hoida.

Käesolevas etapis töötas autor välja rakenduse, mis on võimeline üle võtma ainult HTTP-protokolli kasutatavaid sessioone, kuna see protokoll on võrreldes HTTPS-protokolliga oluliselt haavatavam. Kuid HTTPS-protokolli kasutatavaid sessioone ei ole seni õnnestunud üle võtta ning seetõttu oleks järgmiseks sammuks täiendavate tehnoloogiate juurutamine, mis võimaldaksid üle võtta HTTPS-protokolli kasutatavaid sessioone.

Lisaks sellele eeldab autor, et rakenduse töötamise ajaks tuleb juurutada võimalus seadme MAC-aadressi vahetamiseks. See võimaldaks ajutiselt varjata seadme MAC-aadressi ja raskendada selle jälitamist.

Autori arvates antud rakenduse arendamine jätkub, kuna kõikide täiendavate lahenduste realiseerimiseks on vaja oluliselt rohkem aega.