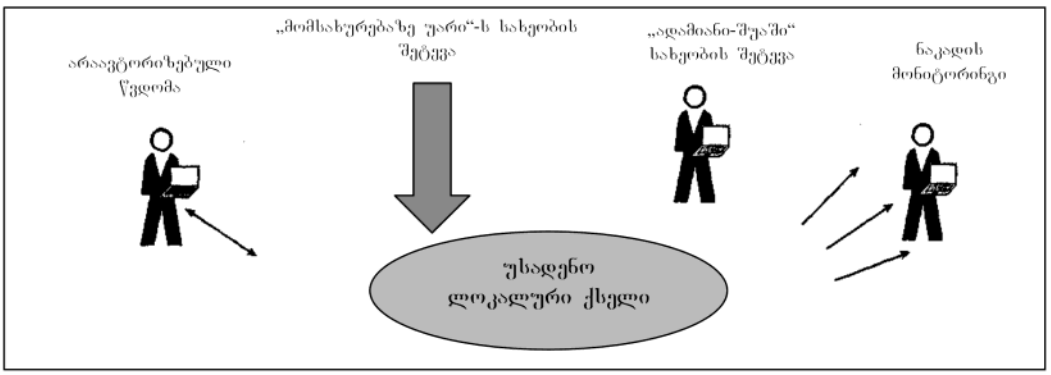
Sunday, July 01, 2012
12:00 PM

თინათინ კაიშაური
ოთარ შონია
ზებურ ბერიძე

# უსადენო ქსელების ინფორმაციული უსაფრთხოება და მათი ანალიზი

უსადენო ქსელებისათვის უსაფრთხოება და მომსახურების ხარისხი უაღრესად მნიშვნელოვანი საკითხია, ვინაიდან გარემოში გავრცელებული საკომუნიკაციო სიგნალები ხელმისაწვდომია დასაჭერად. აქედან გამომდინარე, კომპანიებმა და ინდივიდუალურმა მომხმარებლებმა უნდა შეიცნონ პოტენციურად არსებული პრობლემები და მიიღონ შესაბამისი ზომები.

ნებისმიერ სისტემას, რომელსაც დაცვა სჭირდება, გააჩნია ხარვეზები, რომელთა ნაწილს ან ყველას ერთად თავდამსმხმელი ობიექტად ამოირჩევს. შესაბამისად, სისტემის უსაფრთხოების მექანიზმების შექმნის ერთ-ერთი ვარიანტია იმ საფრთხეებისა და სავარაუდო თავდასხმების განხილვა, რომელთა წინაშეც დგას სისტემა. არსებობს უსადენო ქსელების გამოყენებასთან დაკავშირებული საფრთხეების ყველაზე გავრცელებული შემდეგი ფორმები (ნახ. 1).




*ნახ.1. უსადენო ქსელების გამოყენებასთან დაკავშირებული საფრთხეების სხვადასხვა ფორმები*

მაგალითად, ჰაკერებს (hackers) შეუძლიათ თავდასხმის შედეგად მოახდინონ არაავტორიზებული შეღწევა ქსელურ სისტემებში, ან დაარღვიონ ქსელის მუშაობა და მიიტაცონ კომპანიის ინფორმაცია. თავდასხმა წარმოადგენს კომპიუტერის უსაფრთხოების კონტროლის მექანიზმების გვერდის ავლის მცდელობას. თავდასხმის შედეგად შესაძლებელია უკანონო პრივილეგიების მიღების გზით მონაცემების მოპარვა, მცდარად შეტანა, ინფორმაციის მოდიფიცირება, ქსელის ნაკადის ანალიზი და ა.შ.

მაგალითად, გამოცდილ ჰაკერს ან სულაც შემთხვევით სნუპერს (Snooper – პირი, რომელსაც უყვარს ფარულად თვალთვალი) პროგრამული საშუალებების გამოყენებით შეუძლია ადვილად მოიძიოს უსადენო ქსელის დაუცველი პაკეტები და მთლიანად გახსნას მასში არსებული მონაცემები. სნუპერებს, რომლებიც იმყოფებიან იმ შენობიდან რამდენიმე ასეული მეტრის დაშორებით, სადაც ფუნქციონირებს უსადენო ლოკალური ქსელი, შეუძლიათ მოიძიონ ყველა ტრანზაქცია, რომელიც სრულდება უსადენო ქსელის ნაწილში. ძირითადი საფრთხე მდგომარეობს იმაში, რომ შეტევების შედეგად ვიღაცას შეიძლება ხელში ჩაუვარდეს ისეთი მნიშვნელოვანი ინფორმაცია, როგორიცაა მომხმარებლების სახელები და პაროლები, კრედიტ-ბარათების ნომრები და სხვა.

ამ პრობლემის გადაწყვეტის ერთ-ერთი გზაა იმ ინფორმაციის დაშიფვრა, რომელიც გადაიცემა უსადენო მოწყობილობებსა და საბაზისო სადგურებს შორის. დაშიფვრის პროცესის დროს მონაცემთა ბიტები იცვლება საიდუმლო გასაღების დახმარებით. რადგანაც გასაღები საიდუმლოა, ჰაკერს არ შეუძლია მონაცემების გაშიფვრა.

ანალოგიურად ნებისმიერს, რომელიც იმყოფება შენობის შორიახლოს, ყოველგვარი ძალისხმევის გარეშე შეუძლია მონიტორინგის ჩატარება უსადენო ქსელში არსებული სისტემების მიმართ, თუ არ არის მიღებული სიფრთხილის წინასწარი ზომები. მაგალითად, პირს, რომელიც იმყოფება შენობის მახლობლად მდგარ ავტომობილში, შეუძლია მიებას შენობაში განლაგებული საბაზისო

სადგურებიდან ერთ-ერთს. ასეთ პირს შეუძლია შეაღწიოს სერვერზე და კორპორატიულ ქსელში არსებულ სისტემებში.

სამწუხაროდ, კომპანიების უმრავლესობა უსადენო ქსელების გამართვის დროს იყენებს საბაზისო სადგურების კონფიგურაციას, რომელიც თავიდანვეა დაყენებული (default) და ვერ უზრუნველყოფს უსაფრთხოების საჭირო ზომებს. ოპერაციული სისტემა Windows საშუალებას იძლევა ადვილად დამყარდეს კავშირი უსადენო ქსელებთან, განსაკუთრებით საერთო კავშირის მქონე ქსელებთან. როდესაც ნოუთბუქი მიებმება უსადენო ლოკალურ ქსელს, მის მფლობელს შეუძლია შეაღწიოს ნებისმიერ სხვა ნოუთბუქში, რომელიც ჩართულია იმავე უსადენო ლოკალურ ქსელში. თუ არ არის გამოყენებული პერსონალური ბრანდმაუერი, ნებისმიერს შეუძლია გაეცნოს ასეთი ნოუთბუქის მყარ დისკზე არსებულ ყველა ინფორმაციას, რაც წარმოადგენს უზარმაზარ საფრთხეს.

ხშირად, როდესაც წვდომის წერტილში ამოქმედებულია დაცვის მექანიზმები, არსებულ საფრთხეს წარმოადგენს მიდგმული წვდომის წერტილის (rogue access point) ჩართვის შესაძლებლობა. ასეთი წერტილი ითვლება არაავტორიზებულ წვდომის წერტილად, რომელიც მიერთებულია ქსელში. მაგ.: რომელიმე მომსახურე პერსონალს შეუძლია შეიძინოს წვდომის წერტილი, არ გაითვალისწინოს ქსელის უსაფრთხოების ნორმები და დააყენოს იგი თავის ოფისში. ასევე ჰაკერს შეუძლია შენობაში განათავსოს წვდომის წერტილი, განზრახ შეაერთოს დაუცველი წვდომის წერტილი კორპორატიულ ქსელში.

მიდგმულ წვდომის წერტილში, როგორც წესი, არ არის აქტივირებული დაშიფვრის სისტემა. აქედან გამომდინარე, იგი წარმოადგენს ღია კარს მათთვის, ვინც კი მოინდომებს შენობის გარედან შეაღწიოს კორპორატიულ ქსელში. ამიტომ კომპანიებმა ყოველთვის უნდა შეამოწმონ მიდგმული წვდომის წერტილების არსებობა.

არაავტორიზებული შეღწევის საწინააღმდეგოდ უსადენო ქსელში გამოიყენება ურთიერთქმედებითი აუტენტიფიკაცია, რომელიც ხორციელდება ქსელის მოწყობილობებსა და წვდომის წერტილებს შორის. აუტენტიფიკაციის დროს მოწმდება მომხმარებლის ან მოწყობილობის იდენტურობა. უსადენო ქსელში უნდა გამოიყენებოდეს მეთოდები, რომლის საშუალებითაც ხდება საბაზისო სადგურის დარწმუნება ქსელის მოწყობილობის იდენტურობაში და პირიქით. ეს აუცილებელია იმისთვის, რომ მოხდეს ლეგიტიმურ საბაზისო სადგურებსა და მოწყობილობებს შორის კავშირი. წვდომის წერტილები უნდა გადიოდნენ აუტენტიფიკაციის პროცედურებს კომპუტატორზე, რაც ქსელში გამორიცხავს მიდგმული წვდომის წერტილების გამოჩენას.

აუტენტიფიკაციისა და დაშიფვრის მექანიზმების გამოყენების წყალობით იზრდება უსადენო ქსელების უსაფრთხოება, მაგრამ გამოცდილი ჰაკერები ძებნიან სუსტ მხარეებს, იციან რა, თუ როგორ მუშაობს ქსელის ოქმები. განსაკუთრებულ საშიშროებას წარმოადგენს «ადამიანი შუაში» (man-in-the-middle attacks) სახეობის შეტევები. ჰაკერი განათავსებს ფიქტიურ მოწყობილობას ლეგალურ მომხმარებლებსა და უსადენო ქსელს შორის. მაგალითად, სტანდარტული «ადამიანი შუაში» სახეობის შეტევის განხორციელების დროს გამოიყენება მისამართების გარდამქმნელი პროტოკოლი (Address resolution protocol - ARP), რომელიც გამოიყენება ყველა TCP/IP (Transmission Control Protocol/Internet Protocol – გადაცემის მართვის პროტოკოლი/ინტერნეტპროტოკოლი) ქსელში. ჰაკერს, რომელიც შეიარაღებულია აუცილებელი პროგრამული საშუალებებით, ARP-ს გამოყენებით შეუძლია დაამყაროს კონტროლი უსადენო ქსელზე.

ARP ნებას რთავს შესრულდეს მთავარი ფუნქცია, რისთვისაც იგზავნება მოთხოვნა უსადენო ან სადენიანი ქსელის ინტერფეისის პლატის მიმართ იმ მიზნით, რომ გამოვლინდეს პლატის ფიზიკური მისამართი – ეს იგივეა, რაც MAC (Media Access Control – წვდომის მართვის საერთო ოქმი) მისამართი, რომელიც მინიჭებულია პლატაზე მისი მწარმოებელის მიერ და განსხვავდება ქსელის სხვა ნებისმიერი კომპონენტის მისამართისგან, ანუ ის უნიკალურია. აქედან გამომდინარე, გადამცემმა ქსელის ინტერფეისის პლატამ უნდა იცოდეს მიმღების MAC-მისამართი. ეს პლატა ამოიცნობს და რეაგირებას ახდენს მხოლოდ ფიზიკურ MAC-მისამართზე.

გამოყენებით პროგრამებს, რომლებიც საჭიროა მონაცემების გადასაცემად, უნდა გააჩნდეს მიმღების IP (Internet Protocol) მისამართი, ხოლო გადამცემი ქსელის ინტერფეისის პლატა იყენებს ARP ოქმს იმისათვის, რომ გამოავლინოს შესაბამისი ფიზიკური მისამართი. ის იღებს მისთვის საჭირო მისამართს, აგზავნის ARP პაკეტებს, სადაც ცხადდება მიმღების ქსელის ინტერფეისის პლატის IP მისამართი. ყველა სადგურს აქვს შეხება მოთხოვნასთან და სადგურმა შესაბამისი IP მისამართით უნდა დააბრუნოს პასუხის პაკეტი ARP ოქმით, რომელიც შეიცავს MAC და IP მისამართებს. შემდეგ გადამცემი სადგური ჩართავს MAC-მისამართს გადასაცემ ფრეიმში, როგორც მიმღების მისამართს. რაღაც პერიოდის განმავლობაში ცხრილის სახით ინახავს შესაბამის MAC და IP მისამართებს (ინახავს მანამ, სანამ სადგური არ მიიღებს სხვა ARP პასუხს იმ სადგურისგან, რომელსაც გააჩნია ეს IP მისამართი).

ARP ოქმთან დაკავშირებული პრობლემა არის ის, რომ დაცვის სისტემისთვის ის წარმოადგენს

საფრთხეს, ვინაიდან ადგილი აქვს სპუფინგის (spoofing – კავშირის იმიტაცია, წვდომის მიღება მოტყუებითი გზით) შესაძლებლობას. ჰაკერს შეუძლია შუალედური მოწყობილობის საშუალებით სადგურს გაუგზავნოს ფიქტიური ARP-პასუხი, რომელიც შეიცავს ლეგიტიმური ქსელური მოწყობილობის IP მისამართს და შუალედური მოწყობილობის MAC მისამართს და სადგური შეიყვანოს შეცდომაში. ყველაფერი ეს მიიყვანს იქამდე, რომ ყველა ლეგიტიმური ქსელის სადგური ავტომატურად განაახლებს თავიანთ ARP-ცხრილებს, სადაც შეიტანება მცდარი მონაცემები. შედეგად სადგურები დაიწყებს პაკეტების გადაცემას შუალედური მოწყობილობის მისამართით და არა ლეგიტიმური წვდომის წერტილისკენ. სწორედ ეს არის კლასიკური შეტევა «ადამიანი შუაში», რის შედეგადაც ჰაკერი იღებს იმის შესაძლებლობას, რომ მართოს მომხმარებელთან დაკავშირებული სეანსები. ის მიიღებს პაროლებს, მნიშვნელოვან მონაცემებს და შეძლებს კორპორატიულ სერვერებთან ურთიერთქმედებას ისე, რომ თითქოს ის არის ლეგიტიმური მომხმარებელი.

შეტევების თავიდან აცილების მიზნით ARP მომწოდებლები გვთავაზობენ დაცულ ARP-ს (secure ARP, SARP). ასეთი გაუმჯობესებული ARP უზრუნველყოფს სპეციალურ დაცულ გვირაბს ყველა მომხმარებელსა და წვდომის წერტილებს ან მარშრუტიზატორებს შორის, რომელიც იგნორირებას უკეთებს ყველა იმ ARP-პასუხს, რომლებიც დაკავშირებული არაა იმ მომხმარებლებთან, რომლებიც იმყოფებიან გვირაბის მეორე ბოლოში. მაშასადამე, მხოლოდ ლეგიტიმური ARP-პასუხები მოემსახურება ARP-ცხრილების განახლების დაფუძნებას. სადგურებს, რომლებიც იყენებს SARP ოქმებს, მიდრეკილება არა აქვთ სპუფინგისადმი.

SARP ოქმის გამოყენებისთვის საჭიროა, რომ ყველა სამომხმარებლო მოწყობილობაზე დაყენდეს სპეციალური პროგრამული უზრუნველყოფა, ამიტომ SARP არ გამოიყენება საერთო კავშირის მქონე ქსელებისთვის. მაგრამ საწარმოებს თავიანთ სამომხმარებლო მოწყობილობებზე შეუძლიათ დააყენონ SARP, რათა თავი დაიცვან «ადამიანი შუაში» სახეობის შეტევისაგან.

«მომსახურებაზე უარი» სახეობის შეტევა (Denial of service, DoS) არის თავდასხმა, რის შედეგადაც უსადენო ქსელი ხდება გამოუსადეგარი ან მისი მუშაობა იბლოკება. ასეთი შეტევის შესაძლებლობა უნდა გაითვალისწინოს ყველამ, ვინც გამართავს უსადენო ქსელს. აუცილებელია დაფიქრება იმაზეც, თუ რა მოხდება, როდესაც ქსელი გახდება მიუწვდომელი განუსაზღვრელი დროით.

DoS შეტევის სერიოზულობა დამოკიდებულია იმაზე, თუ რა შედეგს გამოიწვევს უსადენო ქსელის მწყობრიდან გამოსვლა. მაგალითად, ჰაკერს შეუძლია გახადოს მიუწვდომელი უსადენო ლოკალური ქსელი, რომელიც გამართულია სახლში, ხოლო ამის შედეგი იქნება მხოლოდ სახლის მეპატრონის შეწუხება, მაგრამ საწარმოს ინვენტარიზაციის უსადენო სისტემის მწყობრიდან გამოსვლა მნიშვნელოვან ფინანსურ დანაკარგებს გამოიწვევს.

DoS შეტევის სახესხვაობიდან ერთ-ერთს წარმოადგენს მეთოდი «უხეში ძალა» (brute-force attack). ინფორმაციული პაკეტების მასიური გაგზავნის დროს ამოქმედებულია ქსელის ყველა რესურსი და შედეგად ქსელი წყვეტს მუშაობას – ეს არის DoS შეტევის ვარიანტი, რომლის შესრულება ხდება მეთოდით «უხეში ძალა».

უსადენო ქსელების მუშაობის გაჩერების სხვა ხერხს წარმოადგენს მეთოდი «შეგრძნების აღმოჩენა» (carrier sense access), სადაც გამოიყენება მძლავრი რადიოსიგნალი, რომელიც ახშობს სხვებს და აკეთებს ისე, რომ წვდომის წერტილები და ქსელის ინტერფეისის რადიოპლატები გამოუსადეგარი ხდება.

გარდა ამისა, Dos შეტევას ხელს უწყობს დაცვის ზოგიერთი მექანიზმი. მაგალითად, WPA (დაცული წვდომა Wi-Fi-სადმი, Wi-Fi Protected Access) მექანიზმმა შეიძლება გამოიწვიოს «მომსახურებაზე უარი» სახეობის შეტევა. WPA ქსელის მომხმარებლები აუტენტიფიკაციისათვის იყენებენ მათემატიკურ ალგორითმებს. თუ რომელიმე მომხმარებელი შეეცდება მიიღოს მისადმი წვდომა და ერთი წამის განმავლობაში გააგზავნის არაავტორიზებული მონაცემების ორ პაკეტს, WPA ჩათვლის, რომ გახდა შეტევის ობიექტი და ქსელი მუშაობას შეწყვეტს.

Dos შეტევის წინააღმდეგ შედარებით მოქმედ დაცვას წარმოადგენს უსაფრთხოების მკაცრი წესების შემუშავება და შესრულება, მაგალითად, როგორიც არის ბრანდმაუერების სისტემების დაყენება და განახლება, ანტივირუსული სისტემების მუდმივად განახლება, სიმბოლოების დიდი რაოდენობით გამოყენება პაროლებში, არაგამოყენებადი ქსელური მოწყობილობების ქსელიდან გათიშვა და სხვა ყველა ის ქმედება, რომლებიც მკაცრად უნდა დაიცვას უსადენო ქსელის ყველა მომხმარებლებმა.

უსადენო ქსელის დაცვა გარეთა რადიოსიგნალების შეღწევისაგან შესაძლებელია შენობის წინააღმდეგობის გაწევის უნარის გაზრდის გზით. არსებობს ზოგიერთი რეკომენდაცია, რომლის საშუალებითაც შესაძლებელია შენობაში რადიოსიგნალების ნაკადის შემცირება: შენობის შიდა კედლებს უნდა გააჩნდეს ლითონის გამძლე ზედაპირი, სასურველია მოხდეს მისი დამიწება; დაყენდეს თერმოიზოლაციის მქონე ფანჯრები და მოხდეს მისი ქრომირება; შენობის შიდა და გარე კედლებზე გამოყენებულ იქნას ლითონის მინარევის საღებავი; გადამცემის სიმძლავრის დარეგულირება მოხდეს ისეთი სახით, რომ მთლიანად გამოი-

რიცხოს სიგნალის გაჟონვა ან მისი დონე დაიწიოს ისეთ მნიშვნელობამდე, რომ შესაძლებელი იქნეს ჰაკერის ადვილად გამოვლინება.

**TINATIN KAISHAURI**
**OTAR SHONIA**
**ZEBUR BERIDZE**

**INFORMATIONAL SACURITY OF WIRELESS NETWORKS AND THEIR ANALYSIS**

Summary

Wireless networks, the related security issues and their analysis are provided in the present paper. The most widely spread threats, related to the application of wireless networks are presented in the form of drawing. Each of them is characterized with its properties and several recommendations are provided for the purpose of security.

გამოყენებული ლიტერატურა:

1. ჩოგოვაძე გ., გოგიჩაიშვილი გ., სურგულაძე გ., გ. შეროზია გ., მართვის ავტომატიზებული სისტემების დაპროექტება და აგება, სტუ, თბ., 2003 .
2. შონია ო., ნარეშელაშვილი გ., ქართველიშვილი ი. უმავთულო ქსელების უსაფრთხოება. საქართველოს ტექნიკური უნივერსიტეტი, თბ., 2009.
3. Мерритт М., Поллино Д.. Безопасность беспроводных сетей. М., 2004.
4. Козил Д., Логфилд Д., Еител Д., Енли К. Ерен С., Мехта Н., Хасель Р. Искусство взлома и защиты систем. Питер, 2006, 417 стр.