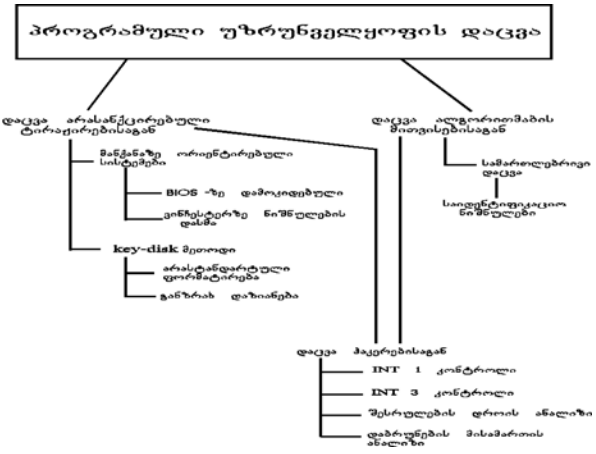
პროგრამული უზრუნველყოფა - დაცვა "პირატული" ტირაჟირებისაგან

კ.კახეთელიძე

მოხსენების მიზანია განხილულ იქნას პროგრამული უზრუნველყოფის დაცვის ძირითადი საშუალებანი, მათი დანიშნულება და ეფექტურობის შეფასება.



ნახაზზე ნაჩვენებია პროგრამული უზრუნველყოფის დაცვის საშუალებათა კლასიფიკაცია და მეთოდები, რომლებიც გამოიყენება თითოეული ტიპის დაცვაში. როგორც სქემიდან ჩანს, დაცვის სისტემები იყოფა გან-სხვავებული დანიშნულების მქონე ორ ქვეჯგუფად: I - დაცვა არასანქცი-რებული კოპირებისაგან და II - დადცვა ალგორითმების მითვისებისაგან.

პირველი ტიპის დაცვის სისტემებში ფართოდ გამოიყენება აპარატურაზე "მიბმული" პროგრამული უზრუნველყოფა და ე.წ. "დისკი-გასაღებები" (key-disks). აპარატურაზე "მიბმული" დაცვის მეთოდებიდან ფართო გავრცელება ჰპოვა BIOS-ზე დამოკიდებულმა სისტემებმა, თანაც საკმარისად ითვლება BIOS-ის გამომშვები ფარმის და გამოშვების თარიღის კონტროლი, თუმცა ეფექტურობის ასამაღლებლად ხშირად გამოიყენებენ მთელი BIOS-ის "საკონტროლო ჯამს". კიდევ უფრო მაღალი ეფექტურობით გამოირჩევა ხისტ დისკზე ("ვინჩესტერზე") ნიშნულების დასმის მეთოდი. MS-DOS სისტემაზე ბაზირებულ კომპიუტერებზე ჩვეულებრივ Partition Table-ს (cyl 0, hd 0, sec 1) და პირველი ლოგიკური დისკის Boot Record-ს (cyl 0, hd 0, sec 1) შორის არის გამოუყენებელ სექტორთა დიდი რაოდენობა (სამოცამდე), სადაც შეიძლება პროგრამისათვის აუცილებელი ინფორმაციის შენახვა. აქ ჩვენ ვაწყდებით ორ პრობლემას: ზოგიერთი Boot Manager-ი იყენებს ამ მოცულობას თავისი მიზნებისათვის და თანაც ვინჩესტერის ფიზიკური ფორმატირების შემთხვევაში იკარგება შენახული ინფორმაცია და პროგრამა

მოითხოვს რეინსტალაციას.

Key Disk -ების გამოყენებისას იგულისხმება რომ არ უნდა მოხდეს ამ დისკების კოპირება. ერთ-ერთი მისაღები ვარიანტია დისკების არასტანდარტული ფორმატირება; შესაძლებელია ბილიკების ნუმერაციის არევა, "უცნაურ" ნომრიანი სექტორების ჩამატება, სექტორების არაპროპორციული განლაგება და სხვა. თუმცა ოპერაციული სისტემის მეშვეობით ასეთი დისკების კოპირება შეუძლებელია, არსებობს სპეციალური პროგრამები, რომლებიც იძლევიან თითქმის ყველანაირი დისკების გადაწერის საშუალებას. უფრო ეფექტურია დისკის განზრახ დაზიანების მეთოდი, როდესაც დისკის მაგნიტური ზედაპირის გარკვეული უბანი ზიანდება ლაზერის სხივის ან თუნდაც უბრალო ნემსის მეშვეობით. ასეთ შემთხვევაში პრაქტიკულად შეუძლებელია კოპირებული დისკეტის ორიგინალთან იდენტურობის მიღწევა. "გასაღები" დისკების გამოყენების ძირითადი ნაკლია დისკეტების არასაიმედოობა და მათი დაზიანების დიდი ალბათობა. მეორე ტიპის დაცვაში (ე.ი. ალგორითმის მითვისებისაგან) დიდ როლს თამაშობს საავტორო უფლებებთან დაკავშირებული ვითარება ქვეყანაში. ამ განხრით პროგრამებში ხშირად იყენებენ შიფრირებულ საიდენტიფიკაციო ნიშნულებს, რომლებიც საკმარისი გარანტია საავტორო უფლების დასამტკიცებლად.

ორივე შემთხვევაში დიდ საშიშროებას წარმოადგენენ "ჰაკერები", რომლებსაც შეუძლიათ პირველ შემთხვევაში ამომიცნონ დაცვის ალგორითმი და გააუვნებელყოფონ იგი, ან, მეორე შემთხვევაში, გაარჩიონ თვითონ პროგრამის ალგორითმი რათა მითვისონ იგი. ჰაკერების ძირითადი "იარაღებია" ე.წ. დებაგერი და დიზასემბლერი, პირველი იძლევა პროგრამის ტრასირების - ნაბიჯ-ნაბიჯ შესრულების შესაძლებლობას, ხოლო მეორე - ასემბლერზე პროგრამის ტექსტის მიღების შესაძლებლობას. ტრასირებისაგან პროგრამის დაცვა შეიძლება, თუკი პროგრამა აკონტროლებს პროგრამულ წყვეტებს INT 1 და INT 3, რომლებსაც გამოიყენებს დებაგერი პირველს პროგრამის ნაბიჯ-ნაბიჯ შესრულებისას ხოლო მეორეს შეჩერების ადგილებში *(breakpoints)*. დებაგირებისაგან დაცვა ასევე შესაძლებელია კოდის შესრულების დროის ან დაბრუნების მისამართის ანალიზით. ალგორითმის დაცვა დიზასემბლირებისაგან შეიძლება პროგრამის კოდის შიფრაციით, ამ დროს ძირითადი მოდული ჩაიტვირთება და განიშიფრება მეორე, დამხმარე მოდულის მიერ.

ნებისმიერ შემთხვევაში იდეალური დაცვა არ არსებობს, შესაძლებელია ნებისმიერი დაცვის ამოცნობა და უვნებელყოფა. დაცვის სისტემის შეფასებაში ერთადერთ კრიტერიუმად შეიძლება გამოდგეს მისი სირთულე - თუ რა დანახარჯს მოითხოვს დაცვის უვნებელყოფის პროცესი. თუ ეს დანახარჯი მეტია ვიდრე პროგრამის მითვისებით მიღებული სარგებელი, ითვლება რომ დაცვა ეფექტურია.