Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 7-10 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

PRETTY GOOD PRIVACY (PGP)- გამოყენებასთან დაკავშირებული გამოწვევები

CHALLENGES OF USING OF PRETTY GOOD PRIVACY (PGP)

ზაალ ჯანიკაშვილი, სამეცნიერო კიბერუსაფრთხოების ასოციაცია
Z. Janikashvili, Scientific Cyber Security Association
ირმა ჩინჩალაძე, სამეცნიერო კიბერუსაფრთხოების ასოციაცია
I.Chinchiladze, Scientific Cyber Security Association

აბსტრაქტი: სტატიაში განხილულია PGP-ის ადრეული ისტორია, მუშაობის პრინციპი, წამოჭრილია ის პრობლემები რასაც ვაწყდებით მისი გამოყენებისას.

ABSTRACT: It is discussed and examined earlier history and working principles of PGP in this article. Also, we discuss challenges and problems we are faced while using PGP

საკვანძო სიტყვები: *კრიპტოგრაფია, PGP;*

KEYWORDS: *cryptography, PGP*

პგპ-ს ადრეული ისტორია

PGP გახლავთ ყველასთვის კარგად ცნობილი კრიპტოგრაფიული პროტოკოლი რომლის ძირითად მიზანს წარმოადგენს მომხმარებელთა ძირითადი მასის კონფიდენციალურობის უზრუნველყოფა. მისი თავდაპირველი სქემა, შექმნილი ფილიპ რ. ციმერმანის(Philip R. Zimmermann) მიერ, პირველად ინტერნეტში გამოქვეყნდა 1991 წელს, რომელიც ემსახურებოდა ელექტრონული შეტყობინებების დაშიფვრას. იმის გათვალისწინებით, რომ ღია გასაღების დაშიფვრისა და ხელმოწერის შესაქმნელად დამოკიდებული იყო RSA-ს საფუძვლებზე, სწრაფადვე მიიპყრო იმ კომპანიის ყურადღება, რომელსაც დაპატენტებული ჰქონდა RSA-ის თავდაპირველი ალგორითმები, და უფრო მეტიც PGP-თი დაინტერესდა შეერთებული შტატების მთავრობაც, კერძოდ, ციმერმანს ბრალს სდებდნენ კრიპტოგრაფიასთან დაკავშირებული გაშიფვრის აკრძალვის დარღვევაზე, რაც განაპირობა PGP-ის საწყისი კოდი ის გასაჯაროვებამ.[1]

საინტერესოა, რისთვის დაგვჭირდა და რამ გამოიწვია PGP ის შექმნა. მოგეხსენებათ, ჯერ კიდევ წინა საუკუნიდან მოყოლებული რამდენად სწრაფად მიიწევს წინ ციფრული ტექნოლოგიების განვითარება, აღნიშნული ფაქტის შედეგად, ადამიანთა უმრავლესობამ უარი თქვა ერთ დროს ძალიან გავრცელებულ საქმიანობებზე, მაგალითად, როგორიცაა ქაღალდზე წერა, ფოსტით შეტყობინებიბს გაგზავნა და ა.შ. და გადავიდნენ უფრო მეტად მოხერხებულ, მოქნილ და დღესდღეობით ფართოდ გავრცელებულ ელექტრონული ფოსტის სისტემაზე.

აღნიშნული წინსვლა, ერთი მხრივ, მოხერხებულობას სთავაზობდა კაცობრიობას, თუმცა, მეორე მხრივ, შეიქმნა უსაფრთხოების პრობლემაც [2], მაგალითად, როდესაც კონვერტით ხდებოდა შეტყობინების გაგზვნა, ამ დროს მომხმარებელი ბევრად უფრო დაცული იყო, რომ მის მიერ გაგზავნილ კონვერტს არავინ გახსნიდა, რადგან გახსნის მცდელობის შემთხვევაშიც კი კონვერტი დაზიანდებოდა და დანაშაულებრივი ქმედება გამოაშკარავდებოდა.

რაც შეეხება ჩვენს თანამედროვე რეალობაში მიმდინარე მოვლენებს, ყოველი დღის განმავლობაში იგზავნება მილიონობით მეილი, იქნება ეს პირადი თუ ოფიციალური ხასიათის, და ყოველთვის, როდესაც გამოიყენება ელექტრონულ ფოსტა, ამ გზით გაგზავნილი ყოველი შეტყობინება ავტომატურად ხდება მოწყვლადი. შეტყობინებები ვისთვისაცაა მოწყვლადი, უმეტეს შემთხვევაში არიან უცნობი ადამიანები, სისტემის ადმინისტრატორები რომელთაც დრო არ აქვთ უცხო ადამიანების პირადი შეტყობინებების საკითხად. მაგრად რა მოხდება თუ შენ ხარ ვიღაც ადამიანის ან ადამიანთა ჯგუფის სამიზნე და შენ აგზავნი ბიზენს მეილს, მათ შეუძლიათ წაიკითხონ შეცვალონ ან გამოიყენონ ეს ინფორმაცია შენ საზიანოდ.

პგპ-ის მახასიათებლები

PGP დიდი უპირატესობა იმაში მდგომარეობს, რომ იგი უზრუნველყოფს უსაფრთხოების ოთხივე ასპექტს, კერძოდ: (1) კონფიდენციალურობას, (2) მთლიანობას, (3) აუთენთიფიკაციასა და (4) გაგზავნილი შეტყობინების ანულირებას.

ამასთანავე, იმისათვის, რომ PGP-ს ახასაითებდეს მთლიანობა, ავთენთიფიკაცია და ანულირება, იგი იყენებს ელექტრონული ხელმოწერის მეთოდს, უფრო კონკრეტულად, ჰეშ(hash) ფუნქციისა და ღია გასაღების(public key) დაშიფვრის მეთოდების კომბინაციას. რაც შეეხება კონფიდენციალურობის უზრუნველყოფას, ამისათვის პგპ-ის ფარგლებში სიმეტრიული (symmetric key) და ღია(public key) გასაღებების გაშიფვრის კომბინაცია.

როგორც უკვე ცნობილია, PGP-ის გამოყენება მეტად უსაფრთხოა, თუმცა ამასთანავე აღსანიშნია, რომ მისი მუშაობის სქემა საკმაოდ მარტივია. განვიხილოთ ნაბიჯები, რომლებიც მუშაობის პროცესში სრულდება:

თავდაპირველად გენერირდება საიდუმლო გასაღები(secret key) და ღია გასაღები(public key). საიდუმლო გასაღები არის შეტყობინების ადრესანტისთვის და ეს გასაღები უნდა ჰქონდეს მხოლოდ მას. ხოლო, რაც შეეხება, ღია გასაღებს, იგი არის ადრესატისთვის განკუთვნილი. ამის შემდეგ იწყება პირველი ბიჯი ხელის მოწერა. ადრესანტი აწერს ხელს მესიჯს თავისი საიდუმლო გასაღებით, იმის დასადასტურებლად, რომ ეს ნამდვილად მისი შეტყობინებაა.

(1) ხელმოწერა σ_m = SIGN(sk,m) სადაც sk არის საიდუმლო გასაღები(secret key).
(2) შემდეგ m იკუმშება ჰეშ(Hash) ფუნქციით და ხდება m`. ამ ბიჯშივე ხდება შეკუმშული შეტყჯობინება m`-ის კონკატენაცია მის ხელმოწერილ ვერსიასთან σ_m-თან.

მესამე ბიჯში გენერირდება ახალი სიმეტრიული გასაღები(symmetric key) k და შიფრავს მეორე ბიჯში მიღებულ შედეგს ანუ m`| σ_m.

(3) $c_m = E(k,m' |\sigma_m)$

მეოთხე ბიჯში ჩვენ ვშიფრავთ დაგენერირებულ სიმეტრიულ გასაღებს(symmetric key) ღია გასაღებით(public key).

(4) $c_k = E(pk, k)$.

საბოლოო ეტაპზე კი ჩვენი შიფრის დასრულებული ვერსია, წარმოდგენილია წინა ორ ეტაპზე მიღებული შიფრების კონკატენაციის შედეგად.

(5) $c = c_k \mid c_m$

სწორედ ამ სქემის გამო არის PGP ამ დროისთვის არსებული დაშიფვრის პროგრამებს შორის ყველაზე დაცული და უსაფრთხო. თუმცა, არსებობს მისი სხვა მხარეც, რის გამოც არ ვიყენებთ მას ყოველღიურად, მიუხედავად იმისა, რომ იგი ასეთ დაცულ სერვისს გვთავაზობს.

მინუსები და შეზღუდვები

სამწუხაროდ, PGP-ის აქვს როგორც ცალსახა მინუსები, ასევე შეზღუდვები, თუმცა ეს შეზღუდვები და მინუსები ერთმანეთთან მჭიდრო კავშირშია, ამიტომ განვიხილოთ ერთად, რომ მეტად გასაგები იყოს.

PGP-ზე საუბრისას, თავდაპირველად აუცილებლად უნდა აღინიშნოს, რომ ეს არაა მომხმარებელზე გათვლილი სისტემა. სისტემა ისეა შექმნილი და იმდენი ბიჯია შესასრულებელი შეტყობინების გასაგზავნად, რომ მომხარებელს ჭირდება საკმაოდ დიდი დრო და ცოდნა ამ ოპერაციის შესასრულებლად, თუმცა, თუ მომხმარებელს არ აქვს საკმარისი ცოდნა, უნარები და გამოცდილება, სავარაუდოა, რომ მან არათუ დიდი დრო მოანდომოს დაკისრებული დავალების შესრულებას, არამედ საერთოდაც ვერ გაართვას თავი. ამიტომაც მომხარებლების უმეტესობა ამჯობინებს გამოიყენოს ელექტრონული ფოსტის მარტივი სისტემა ყოველდღიური პირადი შეტყობინებებისთვის და ა.შ., მაგრამ როცა საქმე კომპანიების ოფიციალურ ბიზნეს მიმოწერას ეხება, აქ უკვე მომხმარებელს უწევს, გააკეთოს არჩევანი უსაფრთხოებასა და სისწრაფეს შორის და ბუნებრივია, აღარ არსებობს იმის ფუფუნება, რომ მოკლე დროში შესასრულებელი ოპერაცია იქცეს უპირატესად, ვიდრე უსაფრთხოება. ასეთ შემთხვევაში, საჭიროა დეველოპერთა ცალკეული ჯგუფის გამოყოფა, რომელიც შეძლებს და გააგზავნის შეტყობინებებს PGP -ს მეშვეობით. ეს გახლავთ ის ძირითადი ნაკლოვანება, რაც PGP-ის ახასიათებს.

ახლა კი განვიხილოთ მისი შეზღუდვები. მომხმარებელს რაგინდ დიდი სურვილი ჰქონდეს, რომ დაცული იყოს და იყენებდეს PGP-ის, მას საშუალება აქ გააგზავნოს შეტყობინება მხოლოდ მასთან, ვინც ასევე PGP-ის მომხარებელია. ამასთანავე, შეუძლებელია მომხმარებელმა გაიგოს, მისი შეტყობინება მივიდა თუ არა ადრესატამდე.

გარდა ამისა, PGP ის საიდუმლო გასაღები (secret key) უნდა იყოს დაცული და არახელმისაწვდომი. თუმცა მისი დაკარგვის შემდეგ თქვენ არ გაქვთ არანაირი ბერკეტი, რომ იქამდე გაუშიფრავი შეტყობინებები გაშიფროთ, ამის გამო შეიძლება ძალიან დაზარალდეთ, ამიტომ უნდა არსებობდეს, საიდუმლო გასაღების ასლი გაუთვალისწინებელი

შემთხვევებისთვის. აქვე თავს იჩენს ასლის შენახვის პრობლემა რადგან საიდუმლო გასაღები(secret key) უნდა იყოს დაცული.

ასევე, დიდი ორგანიზაციის შემთხვევაში საჭიროა, დიდი ფაილების დაშიფვრა ამაშიც აქვს PGP-ის შეზღუდვა. ამიტომ სხვა ხერხია მოსაფიქრებელი ამ დროს, მაგალითად ფაილის დაყოფა და ა.შ.

ამასთანავე, მომხარებელს არ შეუძლია შეამოწმოს, გახსნამდე მოსული შეტყობინება ხომ არ შეიცავს რაიმე მავნე ფაილს, ვირუსს. ამ პრობლემის გადაჭრის ერთ-ერთი საშუალებაა, შეტყობინება გაიხსნას ჯერ სატესტო გარემოში(ვირტუალური მანქანა,sandbox) და შემოწმების შემდეგ თუ ფაილი ან შეტყობინება დავირუსებული არაა, გადავიტანოთ რეალურ გარემოში. ეს პრობლემას არ წარმოადგენს კომპანიებისთვის, მათ ამისთვის საკმარისი შესაძლებლობა, უნარი და რესურსი გააჩნიათ, მაგრამ როცა ვლაპარაკობთ ერთეულ მომხმარებლებზე, მათთვის ეს მოუხერხებელი და არაპრაქტიკული მიდგომაა.

და ბოლოს, რასაც მინდა შევეხო, ესაა ანონიმურობა. ჩვეულებრივი ელექტრონული შეტყობინების გამოყენებისას თქვენ შეგიძლიათ გამოიყენოთ, VPN მაგალითად რომ დამალოთ თქვენი ადგილმდებარეობა. PGP -ის გამოყეენებისას კი ადრესატმა ზუსტად იცის ვისგან და შეუძლია დაადგინოს, საიდან მიიღო შეტყობინება.

რომ შევაჯამოთ, არსებობს უამრავი აპლიკაცია- სხვადასხვა სისტემისთვის ინდივიდუალური, არსებობს ელქტრონული შეტყობინებები, რომელთაც PGP ჩაშენებული აქვთ მაგალითად ProtonMail. თუმცა უამრავი აპლიკაციისა და სხვადასხვა ელექტრონული შეტყობინების არსებობის მიუხედავად, ჩვეულებრივ მომხარებელს უფრო მეტად აბნევს, უჭირს გადაწყვეტილების მიღება, რომელ აპლიკაციას ენდოს და რომელს- არა, იმის გათვალისწინებით, რომ არსებობს ამდენი შეზღუდვა. სწორედ ამ და სხვა მიზეზების გამო, არსებობს მრავალი საკითხი, რაზე მუშაობაც და გამოსწორებაც საჭიროა PGP-ს ფუნქციონირებისა და გამოყენებადობის დასახვეწად.

გამოყენებული ლიტერატურა

1. Harry Halpin, “SoK: Why Johnny Can’t Fix PGP Standardization”, *ACM, 2020.*
2. Garfinkel, Simson. *PGP: Pretty Good Privacy*. United States of America: O’Reilly & Associates, Inc., 1995