**Crypto-Gateway SİP Server (Cgs) istifadə edərək gözlənilməz yüksək SİP Server hücumlarının qarşısını almaq üçün SİP Privacy Gücləndirmə Framework ü**

**Annotasiya.** SIP server Session başlanğıc protokoluna gizli dinləmə hücumlarının qarşısını almaq üçün SIP serverləri üçün məxfilik artırma strategiyasını təqdim edirik. Bir SIP server Şəbəkə Ünvan Tərcümə və firewall'dan sonra olsa da, təcavüzkarlar SIP paketini təqlid və SIP istifadəçilərini taramaq kimi müxtəlif hücum texnikalarından istifadə edərək bu təhlükəsizlik xüsusiyyətlərini hədəfə ala bilər. Fırıldaqçı bir şəxsin orijinal SIP orqanı haqqında məlumat əldə etməsini asanlaşdırır və bu təfərrüatları daxil etmək üçün istifadə edir, buna görə axtarış aparır. Bu cür hücumlar, təşkilatlara və VoIP şirkətlərinə ciddi maliyyə itkiləri gətirə bilər, xüsusən SIP agenti digər VoIP təminatçıları ilə birlikdə dəyərli imkanlar təmin edərsə. Burada təklif olunan strategiya, SIP təhlükəsizlik qapısının sonuna SIP UA serverlərini gizli tətbiq etməklə SIP-ni həyata keçirir. Nəticələr göstərir ki, SIP üçün tətbiq olunan təhlükəsizlik siyasəti təhlükəsizlik problemlərinin həllində əhəmiyyətli üstünlüklər verir. Xüsusilə, təklif olunan proqram, SIP-ə hücum etmədən əvvəl təhlükəsizlik tədbirlərinin vaxtından əvvəl alınmasına icazə verir. Nəhayət, digər müvafiq təhlükəsizlik artırma metodları ilə birlikdə planı nəzərdən keçiririk və qiymətləndiririk. Bu metodların əksəriyyəti simulyasiya ilə təhlil edilmişdir, halbuki hazırkı işə baxılan sxemin məqsədəuyğunluğu bir iş nümunəsi ilə təsdiqlənmişdir.

Açar sözlər: SIP Gateway Server (SGS) ; RSA; Açıqlar, Ulduzlar

1. Giriş

Sessiya Başlatma Protokolu (SIP) İnternet Mühəndisliyi Task Force (IETF) tərəfindən təyin olunan protokolları elan etmək üçün istifadə olunan bir tətbiq təbəqəsidir. Media quruluşu üçün IETF artıq konkret Real Time Protokolu (RTP) hazırlamışdır. SIP mesajının ötürülməsi UDP və ya TCP üzərindəki SIP kimi IP protokolları üzərindən nəqliyyat qatı ilə ötürülməlidir.

Hipertext İşarələmə Dillərindən (HTML) əldə edildiyi üçün SIP əməliyyatları HTML-yə bənzəyir. (Şəkil 1) istifadəçi agenti "A" və "B" arasındakı əsas SIP zəng axınını göstərir. Aşağıdakı cədvəldə SIP tərəfindən istifadə olunan altı sorğu var. Cədvəl 1: “REGISTER, INVITE, ACK, CANCEL, BYE, and OPTION”. İstifadəçi agentləri “REGISTER” dən istifadə edərək cari IP ünvanını göstərirlər . Buna baxmayaraq, yalnız URL-lərin IP olmalı deyil, həm də kanonik telefon nömrəsi ola bilər, buna görə də PSTN ilə idarə edilə bilər. Yenə də SIP, digər şəbəkələrlə idarə etmək üçün əngəlsiz bir protokoldur

Hər SIP tələbi fərqli bir məna daşıyır və aşağıdakı kimi müəyyən edilir:

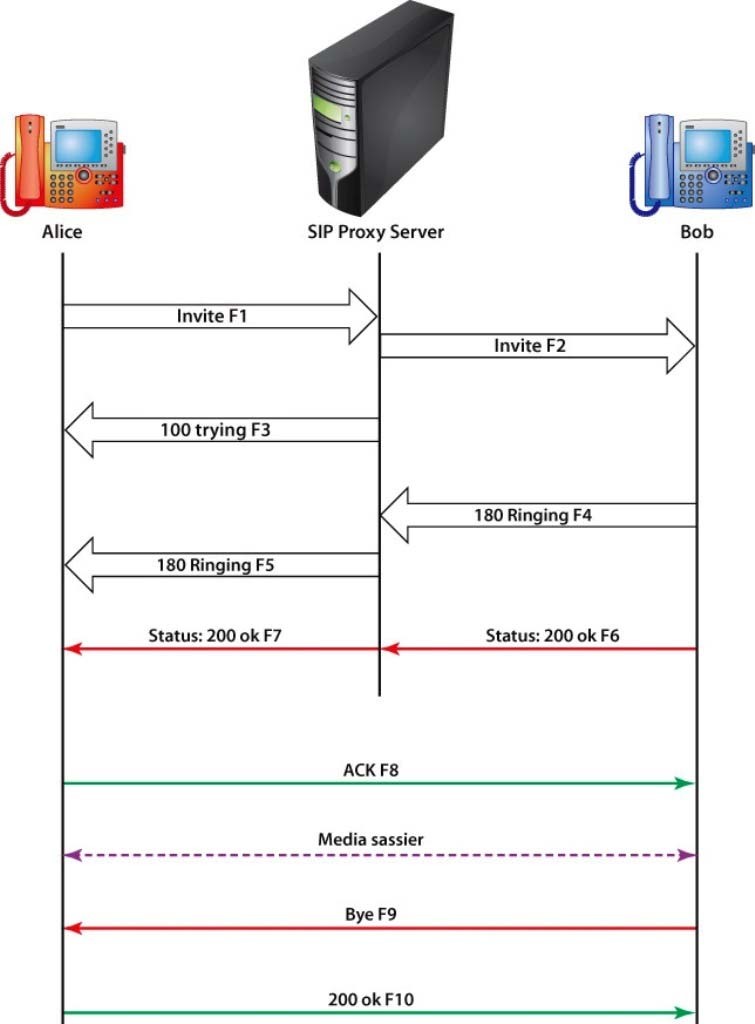
* INVITE: İstifadəçi agentləri (UA) arasında media sessiyası qurur
* ACK: SIP mesajları arasında görüş təsdiqləndikdən sonra zəng qurulacaq.
* CANCEL: Bir müştəri tərəfindən göndərilən hər hansı bir əvvəlki seansı nəzərdə tutur.
* BYE: İki istifadəçi arasındakı ümumi seansları bitir, məsələn, BYE sorğusu göndərərək konfrans sessiyasını bitirir.
* OPTIONS: İstifadəçi "invite" sorğusundan əvvəl proxy serverdən və ya digər istifadəçilərdən soruşur.

Bununla birlikdə, təhlükəsizlikdə hələ də qüsurlardır ki, bu da SIP əsaslı IP telefoniya xidmətinin təhlükəsizlik xüsusiyyətlərinə cavab vermədiyindən daha da yaxşılaşmağa təsir etdi. Bu protokol, mobil tətbiqetmə kimi digərlərindən daha çevik tətbiqləri dəstəkləyir və təhlükəsizlik problemlərindən əziyyət çəksə də müxtəlif simli və simsiz şəbəkələrdə tətbiq edilə bilər.

Cədvəl I SIP, cavab mesajlarının yeri

|  |  |  |
| --- | --- | --- |
| Təsvir | Status code | Nümunə |
| Məlumatlı | 1xx | 100 Trying |
| müvəffəqiyyət | 2xx | 200 Ok |
| İstiqamətləndirmə | 3xx | 300 Multiple choices |
| Müştəri xətası | 4xx | 400 Bad request |
| Server xətası | 5xx | 502 Bad geteway |
| Qlobal uğursuzluq | 6xx | 603 Decline |

Çərçivəmiz lokal şəbəkə şifrələmə / şifrəni açmaq üçün İnternetin onurğa sxeminə qoşulmuşdur; lakin, xarici şəbəkə üçün masanın digər tərəfində işləməyəcəyini düşünürük, çünki xarici şəbəkə üçün hansı alqoritm tətbiq olunduğunu heç bilmirik. Şəbəkə yolunun məqsədi ümumiyyətlə laboratoriya şəhərciyində qulaq asmağın qarşısını almaqdır.



Şəkil 1. SIP əməliyyatı

* 1. Əlaqəli məsələlər

SIP təhlükəsizliyi IETF-in RFC 3329, 4189 və daha çox üzərində işlərini izah edir, bəziləri hələ də işləyir və yenilənir. Bununla birlikdə, parlaq işığda, uzantını özünə təmin etmək əvəzinə, bütün SIP server inkişaf etmiş və etibarlı bir görünüşə sahibdir, IETF artıq edilmişdir. SIP şifrələmə, bir bina təhlükəsizlik qapısı yaxşı əlaqəli bir iş şəbəkəsi təklif etdiyi üçün üçüncü tərəf dəstəyini şifrələyir. Xüsusilə əvvəlcədən paylaşılan açar və istifadə olunan Multimedia İnternet KEY (MIKEY) istifadə etdikdə. Digər hallarda, xüsusilə VoIP müəssisə şəbəkələrində təhlükəsizlik məsələlərini izləmək üçün qapı tülkülərinə yerləşdirmə. Digər araşdırmalar sip proxy serveri istifadəçi agenti serveri (UAs) və uzaq verilənlər bazası ilə korlamaqla sip proxylər arasında identifikasiyanı məcbur edir; identifikasiyası artırılması toplu Sip proxy üçün bir yerləşdirmə tələbi təşviq edəcək.

UA üçün çox səy tələb etməyən bir çağırış axınının bütövlüyünü təmin edəcək bir doğrulama mexanizmini təklif etmək üçün bir iş aparıldı. Bu mexanizm bizə sona çatmayan və istifadəçi səviyyəsində PKI olmadan zəng axınının bütövlüyünü təmin etməyə kömək edəcəkdir. Doğrulama mexanizmi SRTP üçün əsas danışıq protokoli olan ZRTP-də tətbiq edilir və təsdiqlənir.

SIP-ni TLS-ə yerləşdirmək üçün şəbəkə operatorları etibarlı əlaqələrin detallarını maksimum dərəcədə artırmağa çalışmalıdırlar ki, bunun üçün TLS bağlantısını yenidən qursunlar. Tez-tez telefonlar və şlüzlər arasında təhlükəsizliyi göstərən təkrar bir kalibrləmə bağlantısını məcbur etməyə çalışmaq çətin deyil. Bu bağlantı sıfırlamaq üçün təcavüzkar düzgün olmayan növ paketi göndərməli idi. Bu, telefon və zəng serveri arasındakı siqnal kanalını kəsəcəkdir. SIP şifrələməsinin yerləşdirilməsi üçün çoxsaylı təsirli qoruyucu gizlətmə texnikası; Hər ikisi üçün təsirli bir həll: Elliptik-Curve-Diffie-Hellman (ECDH) alqoritmi (açar yerləşdirmə üçün), açar nəsil funksiyası (KGF) (VoIP zəng sessiyasında açarı dinamik şəkildə dəyişdirmək üçün). Bu iki mərhələli keçid yerləşdirmə planı son çağırış sessiyaları zamanı VoIP səs paketləri üçün effektiv və güclü bir təhlükəsizlik təmin edir. Təklif olunan bu dizaynı sınamaq üçün, internetdəki test bazamızın açıq mənbəli SIP əsaslı telefonuna yerləşdirilmişdir. Bu təcrübənin nəticəsi test yatağına qoyulmuş itirilmiş paketin İnternet mexanikası tərəfindən sübut edildi: təklif olunan bu proqram ötürülən səs paketlərinin mükəmməlliyini qoruyaraq VoIP çağırışlarını daha az təmin edir. SIP təhlükəsizlik mexanizmləri; ucdan sona və hop-by-hop qorunması. Son nöqtəli mexanizmlər: zəng edən və / və ya SIP istifadəçi agenti adlandırılan və bu məqsədlə xüsusi olaraq hazırlanmış SIP protokolunun xüsusiyyətləri ilə həyata keçirilir (məsələn, SIP identifikasiyası və SIP mesajı body şifrələməsi). Hop-by-hop mexanizmləri siqnal mesajları yolunda iki ardıcıl SIP subyektləri arasında əlaqəni təmin edir. SIP tərəfindən hop-by-hop qorunması üçün təmin edilmiş xüsusi xüsusiyyətlər yoxdur, beləliklə IPsec kimi şəbəkə səviyyəsinə əsaslanır.

# Framework Hədəfləri

# SIP, Brute Force hücumlarına həssas olan HTTP Digest Doğrulamasından endirildi. Lüğətlərdən istifadə edərək, zəif şifrələr istifadə olunan xülasə alqoritminin nəticələrini müqayisə edərək müəyyən edilə bilər. Ən çox tətbiqetmənin HTTP Digest Doğrulanmasından istifadə etməsinin səbəbi asan tətbiq olunması və əla performansdır. Altı saat davamlı hücumda SIP çağırışlarında artım gördük. Qanuni istifadəçi ilə görüşürük və o bizə göstərdiyimiz anda zəng etmədiyini və hücumun vaxtının bitdiyini göstərdi. Ulduz hesabatlarına dərindən getdik. SIP uzantısının bu planetin hər hansı bir nöqtəsinə hücum edildiyini və istifadə etdiyini gördük. Bir neçə nömrənin tez-tez çağırıldığı görünürdü. Beləliklə, kriptovalyutası və şifrələmə və şifrəni açmaq üçün yeni bir düstur kimi çıxış edən Openis kimi açıq mənbə materialları. Bundan əlavə, istifadəçi müştəri serveri kimi fəaliyyət göstərən Asterisk, şifrələmə üçün istifadə olunan üsullar RSA-dan asılıdır - kağızda təsvir olunan 256 bayt düymənin uzunluğu.

# Framework anlayışları

# Təhlükəsizliyin qiymətləndirilməsi və seçimi müxtəlif SIP zəifliklərinə qarşı tədbir görülməli olan Sessiya Başlatma Protokolu (SIP) prosesi üçün vacib bir prosedur olacaqdır. İstifadəçi Agent Müştərisinə (UAC), İstifadəçi Agent Serverinə (UAS) və ya SIP Gateway-ə hücum üsulları zamanla dəyişir. Təhlükəsizlik boşluqlarının qorunması və hücum metodlarının qarşısının alınması müxtəlif təhlükəsizlik mexanizmlərinin tətbiqi ilə də təkmilləşdirilir. TLS'nin SIP şlüzləri, proxylər, yönləndirici serverlər və ya qeydlər vasitəsilə həyata keçirilməsi, SIP komponentləri arasında güclü identifikasiya və şifrələmə təmin etməklə SIP siqnalları üçün daha yaxşı bir təhlükəsizlik təmin edir. Bununla birlikdə, düzgün olmayan konfiqurasiya və aşağı təhlükəsizlik tətbiqi İstifadəçi Agent Serverini güzəştə və ya istifadəçi giriş məlumatlarını icazəsiz əldə etməyə səbəb olacaqdır. Bunun səbəbi məlumat oğurluğu və ya kredit xərclərinin baha olması ilə nəticələnəcək. Şəkil 2-də göstərildiyi kimi SİP şəbəkə infrastrukturu təklif olunur. SIP mühitində ortaq komponentin əksəriyyəti təşkilat tətbiq edəcəyi və VoIP provayderinə qoşulacağı. Əməliyyat sistemi, SIP xidmətləri və asılılıq paketləri və ya tətbiqlərini fərdiləşdirən əməliyyat sistemi və ya istehsalçı müstəqil bir sistem olan İstifadəçi Agent Server. Bu, qeyri-vacib xidmətlər və ya tətbiqlərdən alınan və əsas sistemdə SIP siqnal emalına maksimum giriş olan xüsusi əməliyyat sistemi tərəfindən emal yüklərini azaldacaqdır. İstifadəçi Agent Server həm də son nöqtələr arasında SIP trafikini / siqnallarını şifrələmək üçün Nəqliyyat Layer Təhlükəsizlik (TLS) daxildir; İstifadəçi Agent Server və İstifadəçi Agent Müştəri. TLS SIP komponentləri arasında güclü identifikasiya və şifrələməni təmin etsə də, mövcud SIP hücum / infiltrasiya metodları xüsusi olaraq qaçırma və şlüz / proxy emulyasiya, TLS etibarlılığı təşkilatı və VoIP təminatçıları üçün xüsusi metodlar hazırlamışdır. Təklif olunan yeni şifrələmə alqoritmi şifrləmə axını şifrələmə (CSC) alqoritminə əsaslanır. Əslində, uzun məlumat axınlarını kollektiv şəkildə şifrələmək üçün hazırlanmışdır. Məlumat şifrələməsində daha səmərəli və daha sürətli olacaqdır. Təklif olunan həllində, CSC mexanizmi İstifadəçi Agent Serverində TLS şifrələməsi vasitəsilə həyata keçirilir. Beləliklə, şifrələmə və şifrələmə prosesi Cədvəl 2-də göstərildiyi kimi müxtəlif İstifadəçi Agent Müştəri identifikasiyası prosesində baş verəcəkdir.

# Şəbəkə Ünvan Tərcümə (NAT) fərqli şəbəkə memarlıqlarını nəzərdən keçirdikdən sonra tövsiyə olunur. Şəbəkə arxitekturası, Xüsusi İstifadəçi Server Server şəbəkəsini etibarlı şəbəkələrdən və İnternetdən qoruyur. NAT və Firewall imkanları, trafik axını, qanuni əlaqə və ya sessiya və məlumatların monitorinqi və idarəetmə bacarığı olan SIP Gateway digər şəbəkə memarlıq tətbiqləri ilə müqayisə edilə bilər.

# CƏDVƏL II. Şifrləmə və DeŞifrələmə Prosesi

|  |  |  |  |
| --- | --- | --- | --- |
| İstifadəçi Agent Müştəri | | SIP Gateway | User Agent Server |
| Qlobal, Etibarsız, İnternet Şəbəkəsi | IP PBX | SIP Gateway Server (SGS) | SIP Server |
| SIP Phone |
| VoIP Provider |
| Private Network | SIP Phone | - | SIP Server |

1. Tətbiq və nəticələr

SIP, TLS dəstəyi, STUN dəstəyi (NAT dəstəyi) və TLS dəstəyi üzərindən CSC xüsusiyyətlərinin daxil edilməsi tələb olunan İstifadəçi Agent Müştərisinə gəldikdə. CSC istifadəçi agenti serveri tərəfindən təsdiqlənə bilən şifrələmə açarı ilə təyin edilmişdir. Bu xüsusiyyət, təsdiqlənmiş İstifadəçi Agent Müştəri cihazlarına (SIP Telefonlar) TLS və CSC şifrəli SIP siqnallarını, məsələn, cüt şifrələmə xüsusiyyətləri kimi İstifadəçi Agent Serverinə göndərməyə imkan verir. İstifadəçi Agent Müştəri və İstifadəçi Agenti Server arasında qeyd edildikdən sonra TCP Handshake və TLS Handshake kimi bir danışıq mesajı icra olunur. Bu iki SIP komponenti arasında təsdiqlənmiş şifrələmə açarını doğrulamaq üçün İstifadəçi Agent Müştəri və Kriptoqrafiya axını şifrəsi (CSC) Handshake ilə İstifadəçi Agent Server arasında əlavə bir mesajla yüksək bir inkişaf əldə edildi. İstifadəçi Agent Müştəri giriş məlumatları, məsələn bir uzatma nömrəsi və şifrə, şifrəli mesajlarla qorunur. Bu, etibarlı olmayan bir şəbəkədə və ya İnternetdə SIP Telefonlar, IP PBX, Yumşaq telefonlar, VoIP Provayderi (magistral rejimi) və başqaları kimi müxtəlif İstifadəçi Agent Müştərilərinə də aiddir. Buna görə açıq açar şifrələmə sistemlərinin məqsədi hər bir müştərinin səlahiyyətli SIP server tərəfindən yaradılan iki açıq (Kpub) və Şəxsi (KPR) açarlarının olmasıdır. Beləliklə, ümumi açarlar SIP serverindəki bir verilənlər bazasında saxlanılır və hər bir müştəri də öz xüsusi açarlarına sahibdir. Diskret logaritmanın çətin probleminə əsaslanan RSA şifrələmə sistemi qurulmuş və şifrələmə n (Kpub) kök modulunun nəticəsi olan C = m ^ (K\_ Pub) (rejim n) alınması kimi təyin edilmişdir. iki iri ədədi çoxaltmaq (n = p × q). Eyni şəkildə, C dəyəri = C ^ (K\_Pr) (rejimi n) ilə həll edilə bilər. İki müştəri istifadəçisi arasındakı RSA alqoritmindən istifadə edərək doğrulama etibarlı olacaq və eyni zamanda müştərilər identifikasiya prosesini başa vurduqdan sonra qarşı tərəfin Pub düyməsini istəyərək etibarlı əlaqə qura bilərlər.

Addım 1: İstifadəçi "A" Agent Müştəri istifadəçi agenti serverinin açıq açarını əldə etməyi xahiş edir.

Addım 2: Server İstifadəçi Agent Serverinin açarını İstifadəçi Agent Müştərisinə geri göndərir. (Kpub-S)

Addım 3: İstifadəçi "A" öz istifadəçi açarı (Kpub-S) ilə "B" istifadəçisinin VOIP-identifikatorunu şifrələyir və İstifadəçi Agent Serverinə göndərir.

### **C = E (Void-IP-B, Kpub-S)**

Addım 4: İstifadəçi Agent Server, tələb olunan tərəfi müəyyənləşdirmək üçün şifrəli VOID-IP şifrəsini açır.

**Void-IP-B =D(C, Kpr-S)**

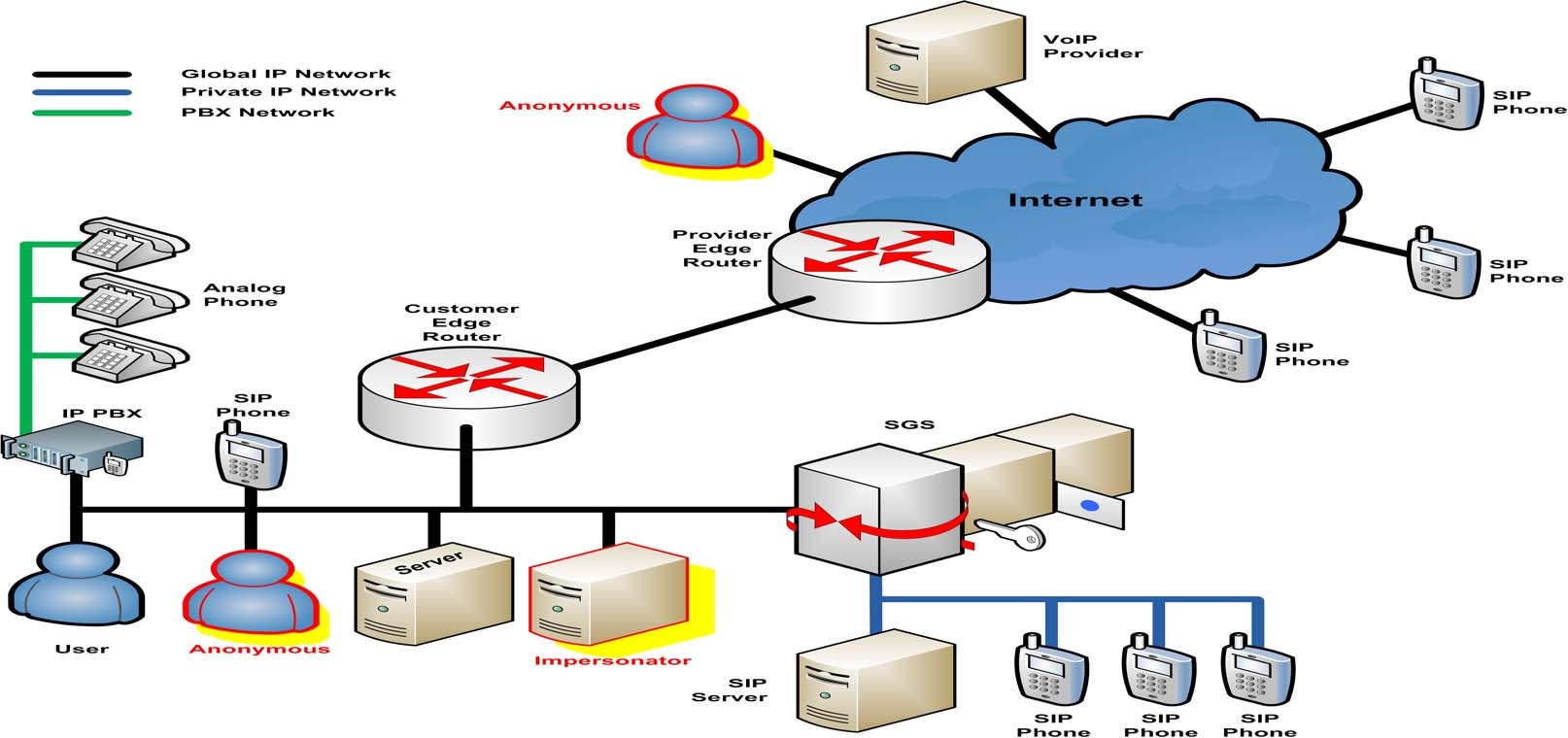
Addım 5: İstifadəçi Agent Server VOID-IP-A-nı B (Kpub-B) açıq açarı ilə şifrələyir və İstifadəçi B-yə kimin zəng etmək istədiyini müəyyən etmək üçün B İstifadəçisinə göndərir.

**C1 =E(Void-IP-A, Kpub-B).**

Addım 6: İstifadəçi B agenti müştəri tələb olunan tərəfi müəyyən etmək üçün C1 şifrəsini açır.

**Void-IP-A =D(C1, Kpr-B)**

Təcavüzkarın (Anonim) perspektivi mesajları deşifr edə bilməz və ya SIP şifrələmə düymələrini (Açıq və Şəxsi) orijinal mesajlara deşifr etməsini tələb edən SIP siqnallarını deşifr edə bilməz. SIP Gateway Server-də tövsiyə olunan əlavə tələblər Gələn və Gedən trafikin izlənməsi, SIP trafikinin gecikməsini, qeyd qaçırılması və ya digər müdaxilə metodlarını və digər zəruri tətbiqləri izləmək üçün nəzarət alətləridir.



1. Nəticələr

SIP siqnalında tətbiq ediləcək təhlükəsizlik xüsusiyyətlərini inkişaf etdirmə prosesində yeni bir framework quruldu. Təklif olunan həll SIP trafikinin və ya sessiyanın bütövlüyünü və məxfiliyini hücum edən şəxsdən qoruyacaqdır.

Framework, korrelyasiya addımına sahib olmaq və genişləndirilə bilən ümumi bir rəhbər olmaq məqsədi daşıyır. Təklif olunan framework-ün digər üstünlükləri ondan ibarətdir ki, yaxşı, güclü və gələcək iş üçün tətbiq oluna bilən bir təhlükəsizlik sistemi olan Təhlükəsizlik Gateway serverini tətbiq edirik. Şifreleme axını şifrələmə alqoritminin firewall qabaqcıl qayda dəsti, SIP Gateway-də Şəbəkə Ünvanı Tərcümə (NAT) və İstifadəçi Agent Serverində TLS şifrələmə və şifrələmə xüsusiyyətləri ilə hazırkı tətbiqdə qulaq asmaq və SIP siqnallarına hücum etmə üsulları ilə müqayisədə təhlükəsizlik və etibarlılığı artıracaqdır.

1. İstinadlar
2. J. Rosenberg , H. Schulzrinne , G. Camarillo , A. Johnston , J. Peterson , R. Sparks , M. Handley , E. Schooler, SIP: Session Initiation Protocol, RFC Editor, 2002 Schulzrinne, H., Casner, S., Frederick, R., Jacobson, V. (2003) RTP: A Transport Protocol for Real-Time Application.
3. J. Arkko , V. Torvinen , G. Camarillo , A. Niemi , T. Haukka, Security Mechanism Agreement for the Session Initiation Protocol (SIP), RFC 3329, 2003 K. Elissa. K. Ono and S. Tachimoto, “Requirements for End-to-Middle Security for the Session Initiation Protocol (SIP),” RFC 4189,Oct. 2005
4. Perez-Botero, D.; Donoso, Y.; , "VoIP Eavesdropping: A Comprehensive Evaluation of Cryptographic Countermeasures," Networking and Distributed Computing (ICNDC), 2011 Second International Conference on , vol., no., pp.192-196, 21-24 Sept. 2011.
5. Nassar, M., Niccolini, S., State, R., Ewald, T.Holistic VoIP intrusion detection and prevention system (2007) Proceedings of the 1st International Conference on Principles, Systems and Applications of IP Telecommunications, IPTComm '07, pp. 1-9.
6. Takahara, H.; Nakamura, M.; , "Enhancement of SIP Signaling for Integrity Verification," Applications and the Internet (SAINT), 2010 10th IEEE/IPSJ International Symposium on , vol., no., pp.289-292, 19-23 July 2010
7. ]El Sawda, S., Urien, P., El Sawda, R. A trust communication with SIP protocol (2010) 2010 ACS/IEEE International Conference on Computer Systems and Applications, AICCSA 2010, art. no. 5587028, .