أمن الاتصال الصوتي عبر الإنترنت

المهندس مصطفى قاسم السمارة* الدكتورة نداء سلمان الدكتور أحمد باسل الخشي*****

الملخص

عندما نتكلم عن الاتصال الصوتي فوق بروتوكول الإنترنت IP، فالكلام يتضمَّن أمرين اثنين، الأول هو إشارات التحكُّم والثاني هو تبادل معطيات الصوت. يتضمَّن الأمر الأول عملية تأسيس الاتصال الصوتي بين طرفين أو أكثر من خلال استخدام بروتوكول يتحكم بالاتصال، بينما يتضمَّن الأمر الثاني نقل معطيات الصوت، تمَّ التركيز في موضوع البحث على مرحلة تأسيس الاتصال، كون هذه المرحلة هي الأهم لأنّ عملية حماية رسائل التحكم تضمن حماية عملية تبادل المفاتيح المحمَّلة عليها في كثير من الأحيان وبالتالي سيتم توصيل هذه المفاتيح إلى الأطراف النهائية بشكل آمن، ومن ثم يكفي استخدام أحد بروتكولات حماية معطيات الصوت كالبروتوكول SRTP أو البروتوكول IPSec من أجل حماية معطيات الصوت. يهدف البحث إلى دراسة وتحليل ومقارنة جميع الحلول الأمنية الممكنة لحماية الاتصال الصوتي عبر بروتوكول الإنترنت، من حيث الأداء من خلال دراسة أثر تطبيق هذه الحلول على مقدار التأخير الحاصل في مرحلة تأسيس الاتصال، والفاعلية أثناء التعرض للهجمات المختلفة الممكن حدوثها ضمن بيئة الاتصال الصوتي بغية الوصول إلى حل متكامل ناتج عن تجميع ومواءمة مكونات مختلفة.

الكلمات المفتاحية: الاتصال الصوتي عبر الإنترنت، إشارات التحكم، معطيات الصوت، بروتوكول تحكم بالاتصال، تهديد، آليات الحماية، تأسيس اتصال آمن.

* أعد البحث في سياق رسالة الماجستير للمهندس مصطفى قاسم سمارة بإشراف الدكتور نداء سلمان والدكتور أحمد باسل الخشي

** أستاذ مساعد قسم النظم والشبكات الحاسوبية - كلية الهندسة المعلوماتية جامعة دمشق

*** وزارة الاتصالات والتقانة دمشق سورية

مقدمة

مع انتشار الإنترنت انتشاراً واسعاً وازدياد استخدامه بشكلٍ مطَّرد، ظهرت كثير من التّطبيقات والخدمات الشبكية الحديثة فلم يعد الأمر مقتصراً على البريد الكتروني (email) والتصفح، بل ظهرت خدمات جديدة، كالاتصال الصوتي عبر الإنترنت VoIP (Voice over Internet Protocol)، حيث كانت خدمات الصوت والصورة تُنقل على الشبكات الثابتة PSTN (Public Switched Telphoney Network) أمَّا الآن فأصبحت تُنقل على شبكات الإنترنت، ولذلك طُوِّعَتْ تقنيات نقل الصوت عبر الإنترنت لتصبح ملائمة للعديد من البيئات في المنزل وفي العمل.... إذْ إنَّها تقدِّم تكلفة اتصال أقل ومرونة أكبر. على أيَّة حال رغم كل الفوائد التي تقدِّمُها تقنية الاتصال الصوتي عبر الإنترنت، يواجه تنفيذ هذه التقنية العديد من الصعوبات والتحديات، كتحقيق أمن الاتصال الصوتي وأثره في جودة الخدمة.

نقدم في بداية هذه المقالة مناقشة للأعمال السابقة في هذا المجال لنبيّن مكانة البحث الحالي بين البحوث الحالية ومن ثمَّ نقدم تمهيدًا عن نظام الاتصال الصوتي عبر الإنترنت VoIP، وبروتوكول تأسيس الجلسة SIP(Session Initiation Protocol) الذي يعمل بالتعاون مع بروتوكول آخر مستخدم لوصف الجلسة SDP(Session Description Protocol). وفي **القسم الثاني** عُرِّفَتْ مجموعة من المتطلبات الأمنية الواجب تحقيقها لتحقيق أمن الاتصال الصوتي ومن ثم عرض لأهم الهجمات التي تتعرض لها رسائل البروتوكول SIP. وفي **القسم الثالث** تعرّفنا أهم بروتوكولات إدارة عملية تبادل المفاتيح ومقارنتها وكيفية تحقيق الوثوقية Authentication من خلالها. خُصِص **القسم الرابع** لعرض طرائق حماية رسائل البروتوكول SIP المطبقة حالياً ومقارنتها من أجل التغلُّب على التهديدات الأمنية من ناحية تحقيقها للمتطلبات الأمنيَّة المعرَّفة. في **القسم الخامس** يتم تقييم أثر تطبيق الحلول الأمنية المدروسة(والحل مؤلف من بروتوكول تبادل مفاتيح يتم تحميل رسائله على رسائل البروتوكول SIP فضلاً عن أحد بروتوكولات حماية رسائل البروتوكول SIP كاملةً) على جودة الخدمة من خلال إجراء تطبيق عملي لمنظومة مصغرة تُمثل نظام اتصال صوتي ضمن بيئة نظام التشغيل Linux وتجريب العديد من الحالات العملية ومقارنة مقدار التأخير الحاصل في كل حالة من الحالات المجربة وفق ثلاث مراحل يمر بها الاتصال الصوتي (1 - مرحلة التسجيل Registeration 2 - مرحلة الرنين Ringing 3 - مرحلة الإجابة Ansewring)؛ يفيد النظام الاختباري أيضاً في تجريب الحلول الأمنية ومدى تصديها للهجمات الممكنة من خلال تنفيذ هذه الهجمات وافتعالها ضمن بيئة النظام بشكل حقيقي.

دراسة مرجعية:

إنَّ آليات الحماية الموجودة حالياً تحدُّ أو تمنع بعض الهجومات التي تتعرَّض لها بيئة عمل SIP، ولذلك فمن الضرورة وجود آليات حماية إضافية مكمِّلة للآليات الحالية، وهذا ماتمَّ العمل عليه في المدة الأخيرة، إذ يقترح المرجع [2]-[1] إيجاد آليات حماية جديدة أو تحسين الآليات الحالية وفي كلتا الحالتين الهدف هو تحقيق المتطلبات الأمنيَّة للبروتوكول SIP. يعرف الباحثان Ono & Tachimoto[1] مجموعة من المتطلبات الأمنيَّة من أجل تقديم التكامليَّة والسريَّة لرسائل التحكُّم على طول المسار مع التأكيد أنَّ العقد الوسيطة الموثوق بها يسمح لها فقط بالوصول إلى المعطيات وهذا مايعرف باسم الأمن من نوع end-to

middle security على اعتبار أنَّه ليست كل العقد الوسيطة موثوقاً بها ويمكنها أن تعالج كل أنواع معلومات التحكُّم. يقترح بعض الباحثون إيجاد وسائل لتحسين خدمات الوثوقية كمحاولة لتخفيف تهديد انتحال الشخصية impersonation وبالنتيجة الحد من الهجومات على رسائل التحكُّم [4]-[3]، فعلى سبيل المثال، يركز كل من Cao & Jennings [3]على إيجاد طرائق لتأمين التكامليَّة والوثوقية لردود SIP وهذا الحل المقترح فعال في الحالات التي يقوم بها المخدِّم الوكيل المهاجم rouge SIP proxy بأداء دور الرجل بالوسط Man in the Middle والقيام بتوليد ردود مزوَّرة وتوجيهها إلى مستخدم غير مخوَّل. دراسة مشابهة قام بها كل من Geneiatakis & [5] Lambrinoudakis من أجل إيجاد طرائق لتأمين التكامليَّة والوثوقية لطلبات وردود SIP على طول مسار الرسالة. يقترح Yang et al[4] باستبدال آليَّة التوثُّق باستخدام HTTP digest والاعتماد على خوارزميَّة Diffie-Hellman للاتفاق على المفاتيح والقيم السريَّة الموزَّعة بشكل مسبق والهدف هو الحد من عيوب آليَّة HTTP digest. وتظهر دراسة أخرى قامت بمراقبة العديد من الأنظمة أنَّه يمكن كشف الهجومات على رسائل التحكُّم، ومن ثمَّ منع تعديل الآليَّة HTTP digest المدعومة من قبل أغلب الطرفيات SIP clients.

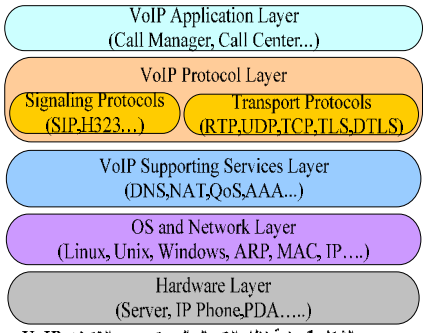
يقترح أيضاً الباحث Zhang et al[6] حلاً من أجل حماية مخدِّمات SIP الوكيلة من هجومات التطويف Flooding التي تحاول تزوير رسائل البروتوكول DNS وتضمينها بعناوين غير قابلة للحل من المهم أن نؤكد أنَّ أي تأثير في متاحية هذه الخدمات مثل parser, DNS look up, ... من شأنه أن يؤثِّر في بيئة عمل SIP. تركِّز بعض البحوث المقدمة في المرجع [7]-[2] على تعريف هجومات التطويف وتستهدف رسالة الدعوة invite وذلك بهدف حماية المخدِّمات الوكيلة. يقدِّم الباحثان Reynolds & Ghosal طريقة لقياس الترابط بين رسائل الدعوة والرد الموافق 200OK، وذلك من أجل كشف هجومات التطويف على مستوى التطبيق. في حين يعتمد الباحث Senger et al[8] على دراسة الترابط بين رسائل الدعوة ورسائل الردود 200Ok ورسائل الإنهاء Bye or Cancel وقياس مسافة Hellinger بين هذه الرسائل. تعتمد دراسات أخرى [9] أُجريَتْ في هذا المجال على دراسة الـ finit_stat_machine لمناقلات البروتوكول SIP. قدَّم الباحث Fiedler et al [2] بنية أمنيَّة معتمدة على البروتوكول SIP تُعرف باسم VoIP defender قادرة على معالجة أكثر من 50000 رسالة SIP بالثانية، وهي البنية الوحيدة التي تأخذ بالحسبان متطلبات الأداء بشكل جيد. يقترح المرجع [10] أن تتضمَّن رسائل SIP قيمة سريَّة cryptographic token ليتم التأكُّد من أنَّه قد تم التحقق من هوية المستخدم في الشبكة الموافقة. أثبتت دراسة أخرى مقترحة في المرجع [11] أجريت على الإجرائيات المتبعة للتوثُّق، أنَّ هذه الإجرائيات تؤثر في أداء المخدِّمات تأثيراً كبيراً. تتطلب هذه الخدمة حماية معلومات المستخدم الشخصية وعدم كشفها لكن لايمكن حجب كل الحقول إذ إنَّ بعضها كالحقل contact مستخدم من أجل القيام بعملية التوجيه، وكما هو مقترح في المرجع [10] أنَّ هذه الخدمة تتطلَّب دعماً وإنجازاً من قبل المخدِّمات الوكيلة. ركزت درسات أخرى[12] على المقارنة بين الحلول المطبقة من أجل حماية معطيات الصوت (SRTP vs IPSec).

1 - تعريف الاتصال الصوتي عبر الإنترنت VoIP:[13]

يشير الاتصال الصوتي عبر الإنترنت VoIP تقنياً إلى عملية نقل الصوت بالزمن الحقيقي على شبكات المعطيات المعتمدة على البروتوكول IP. تتم عملية تأسيس الاتصال عن طريق بروتوكول تحكُّم signaling protocol خاص بتأسيس الجلسات، ومن أهم البروتوكولات المستخدمة للتحكم بالاتصال البروتوكول(Session Initiation Protocol) SIP H323 MEGACO. إحدى القضايا الحساسة في عملية نقل الصوت، هي تأمين عملية تأسيس الاتصال secure call establishment وحماية معطيات الصوت المتبادلة بين طرفي الاتصال وجودة الخدمة QoS.

أ- ما سبب اختيار البروتوكول SIP [14]

إنَّ نظام الاتصال الصوتي عبر الإنترنت VoIP هو خدمة اتصال ممكنة بالتعاون مع مجموعة من البروتوكولات نسميها بروتوكولات نظام الاتصال الصوتي (انظر الشكل 1) عبر الإنترنت VoIP Protocols، تشمل هذه الخدمة عملية نقل الصوت وإشارات التحكُّم الخاصة به. تم التركيز في هذه الدراسة على بروتوكول تأسيس الجلسات SIP لأنَّه بسيط وهو البروتوكول الواعد في المستقبل في هذا المجال، ويتمتَّع بتعقيد أقل من البروتوكول H.232 وقابليَّة للتوسع أكبر، وقد تم قبول هذا البروتوكول كمعيار 3GPP وكعنصر رئيسي ضمن النظام الفرعي المتعدد الوسائط IP Multimedia Subsystem (IMS) المعتمد على البروتوكول IP التي تعدُّ النواة الرئيسية في انطلاقة شبكات الجيل القادم Next Generation Network (NGN).

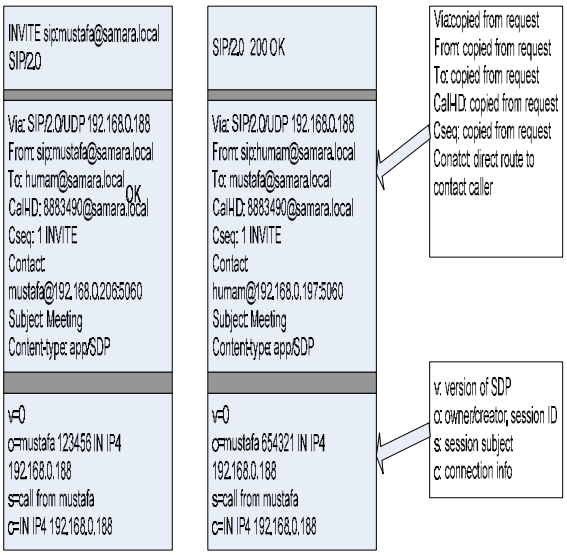


الشكل 1: بنية نظام الاتصال الصوتي عبر الانترنت VoIP

ب - بروتوكول تأسيس الجلسة SIP:[13],[14]

إن البروتوكول SIP هو بروتوكول نصي موصف ضمن المعيار RFC 3261، يمكن إرسال رسائل هذا البروتوكول فوق أحد بروتوكولات طبقة النقل كالبروتوكول TCP, UDP, TLS, SCTP, DTLS. لا يعدُّ البروتوكول SIP بروتوكول اتصال كامل، لكنَّه عنصر مهم في منظومة الاتصال الصوتي عبر الإنترنت VoIP. لذلك فهو بحاجة إلى التعاون مع بروتوكولات معيارية أخرى، كالبروتوكول RTP (Real Time Protocol) الذي يحمل معطيات الصوت في الزمن الحقيقي، يبيّن الشكل 1 موقع البروتوكول SIP ضمن بنية نظام الاتصال الصوتي. يحمل البروتوكول SIP معلومات بروتوكول آخر مستخدم لوصف جلسة الاتصال هو البروتوكول SDP (Session Descreption Protocol). يبيّن الشكل (2) موقع حقول البروتوكول SDP ضمن رسالة SIP. إنَّ الطرائق التي يتم من خلالها إرسال الوسائط تحتاج إلى الاتفاق والتفاوض (قبل بدء أي تواصل) على نمط الوسائط المرسلة ومع أي بروتوكول وإلى أي بوابة، وذلك عن طريق الخدمة التي يقدِّمها البروتوكول SDP لتحقق كل هذه المتطلبات. سنرى بعد عند مناقشة الحلول المتبعة لحماية الاتصال الصوتي، كيف سيشكل البروتوكول SDP خياراً جيداً لنقل المعاملات

المتعلقة بالتشفير من خلال حمل معطيات بعض بروتوكولات تبادل المفاتيح كالبروتوكول MIKEY والبروتوكول Sdesc.



الشكل 2: بنية الرسالة invite والرسالة 200OK

ج- وظائف بروتوكول تأسيس الجلسة SIP:

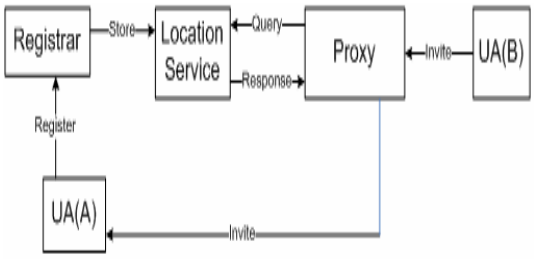
يقوم البروتوكول SIP بالتحكُّم بالاتصال من خلال تأسيس جلسات الوسائط المتعددة وإنهائها وإلغائها multimedia sessions(التي تتضمَّن الصوت والصورة والفيديو...) فضلاً عن دعم خدمة مطابقة الأسماء name mapping من خلال مقابلة العنوان بعنوان آخر من المفترض وجود الطرف الثاني للاتصال عنده، يشير العنوان الآتي:

(sip:alice@domain.com أو

sips:alice@domain.com إلى نطاق domain مرتبط بخدمة تحديد للموقع location service.

د - مكونات بيئة عمل البروتوكول SIP

نعدد فيما يأتي أهم المكونات الضرورية من أجل قيام هذا البروتوكول بعمله بشكل صحيح:عميل المستخدم User Agent المخدِّم الوكيل Proxy server، مخدِّم إعادة التوجيه Redirect server مخدِّم تحديد الموقع Location server المخدِّم المسجِّل Registrar server. يبيّن الشكل (3) مكونات بيئة عمل نظام الاتصال الصوتي.



الشكل 3: بيئة نظام الاتصال الصوتي

2 -التهديدات التي يتعرض لها بروتوكول SIP:

يتم التعرُّض لبروتوكول تأسيس الجلسة SIP من خلال استهداف رسائله، تُبعث رسائل البروتوكول SIP في أغلب الأحيان بشكل نصي غير مشفر، ولذلك يمكن تعديلها أو تزويرها أو الإضافة إليها، ومن ثمَّ يمكن القيام بالعديد من الهجمات على تطبيقات الاتصال الصوتي عبر الإنترنت، من خلال التعرُّض لهذه الرسائل. معظم هذه الهجمات ممكنة الحدوث وذلك لسببين: الأول هو أنَّ البروتوكول SIP يسمح بمعالجة أي طلب من دون التوثُّق منه، والسبب الثاني عدم وجود أي تدقيق على مصدر الرسالة. نورد فيما يلي وباختصار شديد أهم المتطلبات الأمنية لبروتوكول تأسيس الجلسة SIP والقيود الأمنية المفروضة عليه، ومن ثم تعرّف أهم الهجمات الممكنة التي يتعرض لها بروتوكول تأسيس الجلسة SIP ومدى تأثيرها في هذه المتطلبات:

أ- المتطلبات الأمنية للبروتوكول SIP: [15]

تُصنَّف المتطلبات الأمنية في الحالة العامة إلى أربعة تصنيفات السرية Confidentiality التكاملية Integrity المتاحية Availability والوثوقية

Authenticity ومن أجل عدم الفهم الخاطئ لكل من هذه المتطلبات لابد أن نقدم شرحاً بسيطاً لكل منها ضمن بيئة العمل المعتمدة على SIP:

- **السرية**: هي آلية لإخفاء المعلومات تضمن للكيانات المخولة فقط بقراءة هذه المعلومات أمَّا في بيئة عمل SIP فهي تضمن للكيانات المخولة(المخدمات الوكيلة، المخدمات المسجلة مخدمات إعادة التوجيه، الطرفية النهائية) فقط الوصول إلى إشارات أو رسائل التحكم.
- **التكاملية**: تضمن التكاملية أن الكيانات المخولة فقط يمكنها تعديل البيانات في أثناء النقل، أمَّا في بيئة عمل SIP فثمة العديد من المكونات تتطلب أن تصل إلى رسائل التحكم من أجل معالجتها وتوصيلها إلى وجهتها النهائية، فهي تضمن أن تتم معالجة رسائل التحكم من قبل الكيانات المخولة فقط وعلى طول مسار النقل وبالنمطين خطوة بخطوة وطرف لطرف وذلك نظراً إلى وجود عقد وسيطة على مسار النقل.
- **الوثوقية**: تضمن الوثوقية صحة مصدر المعطيات أمَّا في بيئة عمل SIP فهي تضمن أن المعطيات القادمة هي بالفعل المعطيات التي تم إرسالها من المصدر الحقيقي لها. توجد خدمة توثق خاصة بالبروتوكول SIP، لكنَّ استخدامها خياري. تقدِّم معظم أنظمة الاتصال الصوتي خدمة التوثُّق لبعض الرسائل في حين تسمح بعض الأنظمة بقبول الطلبات دون توثُّق، مما ينتج عن ذلك عواقب غير جيدة.
- **المتاحية**: تعني المتاحية في بيئة عمل SIP قدرة المستخدم على طلب الخدمات المعتمدة على SIP في أي لحظة.

ب -القيود الأمنية على البروتوكول SIP: [15]

1 - يجب أن تمتلك العقد الوسيطة سماحية الوصول إلى ترويسات رسائل SIP محددة من أجل أن تتمكن من معالجة رسائل التحكم وتوجيهها إلى وجهتها الصحيحة، لذلك فمن غير المقبول بشكل عام أن نشفر كامل رسالة التحكم (انظر الجدول 2 الذي يبيّن حقول البروتوكول SIP الممكن تعديلها).

الترويسة Header	Request URI	From	To	Via	Record Route	Record	Call Id	Cseq
التعديل المسموح	نعم	لا	لا	نعم	نعم	نعم	لا	لا

الجدول 2: القيود الموجودة على تعديل ترويسة رسالة SIP

2 - بعض رسائل التحكم مثل Cancel, Ack يجب أن لا يتم التوثق منها لأنها غير قابلة لإعادة الإرسال.

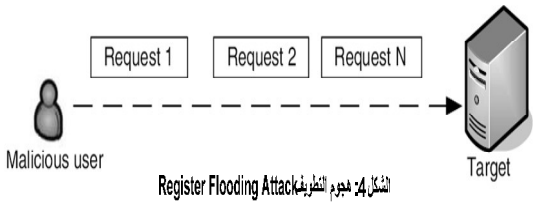
ج - الهجمات التي يتعرض لها بروتوكول تأسيس الجلسة SIP:

لنتعرف في مايأتي على أهم الهجمات التي تعترض رسائل التحكم التابعة لبروتوكول تأسيس الجلسة SIP:

- **التجسُّس: Eavesdropping:** يستهدف هذا الهجوم السريَّة والخصوصيَّة**[15]** من خلال الوصول إلى معطيات رسائل التحكُّم والاطلاع عليها وتعديلها أحياناً.
- **هجوم تزوير عملية التسجيل Registration Hijacking:**

تتمثل بتعديل بعض القيم ضمن حقول رسالة التسجيل **[17]** التي من شأنها أن تنهي تسجيل المستخدم أو أن تسبب رفضاً للخدمة DoS (Denail of Service) من طرف المستخدم أو من طرف المخدم الوكيل(انظر

الشكل 4 الذي يبيّن كيفية تطويف مخدم SIP الوكيل من خلال إرسال عدد كبير من الطلبات) ويمكن أيضاً لإضافة كود خبيث من شأنه أن يعدل معطيات التسجيل.



الشكل 4: هجوم التطويف Register Flooding Attack

- **هجوم إنهاء المكالمة: SIP BYE Attack**
- **هجوم إلغاء المكالمة: SIP CANCEL Attack**
- **هجوم انتحال الشخصية: Identity Spoofing attack**

يمكن تزوير تفاصيل رسالة الدعوة **[18]** كانتحال هوية المرسل caller ID ومن ثمَّ خداع الطرف المتَّصل وكشف معلوماته الشخصية، وهو يعتقد صحة قيمة معرِّف المتَّصل caller ID.

- **هجوم نقل المكالمات: Call Transfer Attacks**

يمكن تزوير الطلب SIP REFER request (الذي يُبعث إلى الطرفية) ونقل المكالمة إلى مكان آخر محدد برقم هاتف أو عنوان SIP مختلف تابع لمهاجم ما**[18]**. ومن ثمَّ كشف المعلومات السريَّة التي يتم تبادلها في أثناء المكالمة. الحالة الأصعب هي أن تبقى المكالمة الأصلية على حالها ومايفعله المهاجم هو أن يضيف نفسه إلى مؤتمر يخص المكالمة، من دون علم هذه الأطراف، وفي حال إخفاق هذه الحالة، فإنَّ مجرد توجيه المكالمة إلى طرف آخر بشكل عشوائي يعدُّ بحد ذاته هجوماً فعَّالاً لرفض الخدمة DoS.

تعرّفنا العديد من الهجمات، التي تتعرَّض لها رسائل بروتوكول تأسيس الجلسة SIP والتي من شأنها أن تؤثر في سرية وتكاملية هذه الرسائل وذلك كونها تُبعث بشكل واضح غير مشفر، فضلاً عن عدم القدرة على تشفير بعض الحقول، بسبب الحاجة إليها في عملية توجيه الرسائل. والأمر الآخر وهو عدم التوثُّق منها في كثير من الأحيان. نتعرض في القسم الثالث إلى كيفية تحقيق التوثُّق من خلال تعرّف بروتوكولات إدارة المفاتيح، أمَّا موضوع تأمين رسائل بروتوكول تأسيس الجلسة SIP والحفاظ على سريَّتها، فذلك سيمر معنا في القسم الرابع عندما سنتكلم عن طرق حماية بروتوكول تأسيس الجلسة SIP.

و - مقارنة التهديدات الأمنيَّة وآثارها:

نقدم في هذه الفقرة أهم التهديدات الأمنية ونقاط الضعف التي يمكن أن يستغلها المهاجم ومن ثمَّ القيام بالعديد من الهجمات التي من شأنها أن تؤثر في المتطلبات الأمنية التي تعرّفناها في بداية هذا الفصل نلاحظ هذه التهديدات مبينة في الجدول 3:

التأثير	الهجوم	نقطة الضعف	التهديد
سرية المعطيات	التجسس على رسائل التحكُّم	نقص آليات تحقيق السريَّة	الوصول غير المشروع للمعطيات
التكامليَّة والمتاحية	تزوير رسائل التحكُّم	سهولة الوصول إلى وسيط النقل و نقص آليات تحقيق التكامليَّة	التعديل غير المشروع للمعطيات
السريَّة والوثوقية	تزوير رسائل التحكم و هجومات على رسائل التحكم	سهولة الوصول إلى وسيط النقل و نقص آليات التوثُّق	انتحال شخصية الزبون
الوثوقية والتكامليَّة	هجومات على رسائل التحكم وهجوم الرجل بالوسط	نقص آليات التوثُّق من طرف المخدم	انتحال شخصية المخدِّم

الجدول 3: مقارنة بين التهديدات الأمنيَّة آثارها[15]

3 - بروتوكولات إدارة عملية تبادل المفاتيح Key Management Protocols

تحتاج عملية تأمين معطيات الصوت إلى تزويد طرفي الاتصال بالمفاتيح المطلوبة بشكل آمن وهذا يحدث في مرحلة تأسيس الاتصال، أي قبل أن تبدأ عملية تبادل الوسائط [تُستخدم هذه المفاتيح من قبل بروتوكولات حماية معطيات الصوت كالبروتوكول SRTP (Secure Real Time Protocol)]. إنَّ التوثُّق المتبادل Mutual Authentication هو الجزء الحسَّاس في هذه العملية وذلك بسبب ضرورة التوثُّق من الطرف الذي سيتم توصيل المفتاح إليه والتأكد من مصدر الرسالة، كما أنَّ دراسة عملية تبادل المفاتيح ضرورية من أجل تقدير قيمة التأخير الزمني الحاصل عن تطبيق الحلول الأمنية، والتي هي وكما ذكرنا تطبيق أحد بروتوكولات حماية رسائل التحكم(التي سنتعرّفها في الفقرة الرابعة) مع أحد بروتوكولات تبادل المفاتيح التي سنتعرّفها بشكل موجز في هذه الفقرة ومن ثم القيام بمقارنتها:

1 -بروتوكول تبادل المفاتيح MIKEY: [20][19][12]

هناك ثلاث طرائق من أجل توليد المفتاح الرئيسي ونقله Master Key بشكل آمن لكلا الطرفين A,B:

- **طريقة المفتاح المشترك السري الموزع بشكل مسبق (MIKEY / pre-shared secret key)**
- **طريقة التشفير بالمفتاح العام (MIKEY / PK public key encryption)**
- **طريقة ديفي هلمان (MIKEY / Diffie-Hellman) DH**

2 -البروتوكول Sdesc Security (SRTP Sdescriptions:[21][19]

3 -البروتوكولZRTP:[19][22]

أ- مقارنة بروتوكولات تبادل المفاتيح الثلاثة المستخدمة في MIKEY:

- **PSK:** هي أسهل وأسرع طريقة وتتطلب قدرات حسابية منخفضة لكنَّها غير قابلة للتوسع لذلك فهي مستخدمة في الحالات الآتية:
  - التواصل بين المخدِّم والزبون.
  - إعادة توزيع المفاتيح بعد استخدام الطريقة PK.
  - بشكل فردي يمكن تبادل المفاتيح بواسطتها.
  - تحقق خدمة الوثوقية بسبب وجود المفتاح المشترك الموزع مسبقاً.
- **PK:** وتقدِّم قدرة كبيرة على التوسُّع ضمن بيئة يكون فيها مستودع المفاتيح العامة المركزي متاحاً (بنية PKI) ويجب أن يكون موثوقاً به من قبل المستخدمين جميعهم. تدعم هذه الطريقة التواصل بين مجموعة مستخدمين group communication لكنَّها تتطلب موارد للمعالجة أكثر من الطريقة الأولى. يمكن استخدام هذه الطريقة لتخزين مفتاح متناظر ليستخدم لاحقاً في الطريقة الأولى وذلك لتحسن الكفاءة، كما أنها تحقق خدمة الوثوقية عن طريق الشهادات.
- DH: هذه الطريقة هي أكثر طريقة تستهلك موارد، لكنَّها الوحيدة التي تؤمن (PFS) تُستخدم هذه الطريقة في اتصالات من نمط ند للند peer-to-peer وغير مستخدمة في اتصالات المجموعة وتتطلَّب وجود بنية PKI. كما أنها تحقق خدمة الوثوقية عن طريق خوارزمية DH.

ب - مقارنة بين طرائق إدارة عملية تبادل المفاتيح:

إنَّ إدارة المفاتيح عمليَّة ضروريَّة وإجباريَّة من أجل حماية تطبيقات الوسائط عبر الإنترنت مثل VOIP Conferencing Video on demand وغيرها من

التطبيقات. قمنا بتعرّف بروتوكولي تبادل المفاتيح MIKEY وSdescriptions وهما منجزان من قبل العديد من الشركات لتحقيق المتطلبات الأمنيَّة كالتوثُّق والسريَّة والتكامليَّة لقنوات الوسائط Media Streams. وتمَّ التعرُّض إلى ZRTP ومن المتوقَّع أن يصبح حلاً جيداً لتحقيق السريَّة من نوع ند لند peer to peer. يحقِّق MIKEY خاصية التوسُّع والمرونة لدعم العديد من الاتصالات من نوع Unicast، Multicast ولكنَّه أكثر تعقيداً من ناحية التنجيز بالمقارنة مع Sdescriptions. لكن كلا المفهومين يقدِّمان حلولاً لتبادل المفاتيح ودعم البروتوكول SRTP وتحقيق الحماية لقنوات الوسائط بين المشتركين. ونلاحظ أنَّ ZRTP يقدِّم مستوى من الشفافية transparency بالمقارنة مع MIKEY أو مع Sdescriptions لأنَّ ZRTP مستقل عن بروتوكولات التحكُّم بالاتصال ويتطلَّب تغييراً في البرنامج المنصب عند الأطراف النهائية ولكن لا يوجد تغيير في مكونات VoIP الرئيسية مثل SIP Proxy أو H.323 gate keeper.

كما هو مشار إليه في الـ RFC 3830 نجد أنَّ MIKEY مخصَّص للاستخدام من أجل حالة Peer-to-peer وفي الحالة one-to-many وضمن مجموعات متفاعلة ذات حجوم صغيرة. لذلك نعدُّ أنَّ إحدى النقاط التي يجب معالجتها ودراستها هي معرفة هل البروتوكول MIKEY يدعم عملية توزيع المفاتيح على نطاق واسع أي ضمن مجموعات كبيرة تتطلَّب خدمات وسائط (بث فيديوي لملايين المشتركين). لكن هذا القصور نظري بسبب عدم وجود أي حالة عملية كبيرة تستخدم البروتوكول MIKEY ضمن مجموعات ضخمة جداً.

4 - آليات حماية بروتوكول تأسيس الجلسة SIP

أحد أهم القضايا المهمة في موضوع أمن الاتصال الصوتي، هي عملية حماية رسائل التحكم المتبادلة بين المشتركين ومكونات بيئة عمل نظام الاتصال الصوتي وذلك لأنَّ هذه الرسائل مستهدفة كما رأينا في الفصل الثالث. تُستخدم هذه الرسائل من أجل تأسيس الاتصال الصوتي فضلاً عن أنها تحمل رسائل بروتوكولات تبادل وإدارة المفاتيح المستخدمة في حماية معطيات الصوت. تؤدي آليات حماية هذه الرسائل دوراً مهماً في صد العديد من الهجمات كالوصول غير المشروع والتجسس وتحويل المكالمات. نتعرف في هذا الفصل العديد من الآليات الأمنية المستخدمة لتحقيق المتطلبات الأمنية المعرفة في الفصل الثالث. لاتتضمَّن محددات البروتوكول SIP وفق المعيار RFC 3261 أي آليات أمنيَّة محددة، بدلاً من ذلك يشير المعيار إلى إمكانية استخدام الآليات الأمنيَّة المعروفة نفسها والمطبقة على مستوى الإنترنت، يمكن تحقيق أمن البروتوكول SIP إمّا من نوع خطوة بخطوة أو من نوع طرف لطرف. يمكن أن نستخدم العديد من البروتوكولات لتقدِّم كالسرية والتكاملية والوثوقية لرسائل بروتوكول تأسيس الجلسة SIP وذلك لصد العديد من الهجومات. يتطلب تحقيق هذه المتطلبات الأمنيَّة استخدام بروتوكولات أمنيَّة مثل: IPsec، S/MIME، TLS ومؤخراً DTLS. في البداية لابدَّ من تعرّف كيفية تحقيق الوثوقية بالاعتماد على البروتوكول HTTP Digest، ومن ثم تعرّف أهم البروتوكولات المستخدمة من أجل تحقيق الأهداف الأمنية السابقة.

- **HTTP Digest: [16][13][19]**

هو بروتوكول توثُّق معتمد على طريقة challenge-response مستخدم من أجل التوثُّق من الرسالة وصحة هويِّة المستخدم. تعدُّ هذه الطريقة عرضة لهجوم chosen plaintext attack وهجمات الرجل بالوسط وهجومات انتحال الشخصية Impersonation attack. أو القيام بعملية فتح الاتصال أو إنهائه من مستخدمين غير مخولين بذلك، إحدى الوسائل الممكنة للحماية من هذه الهجومات من خلال القيام بتشفير

رسائل التحكُّم للبروتوكول SIP باستخدام أحد البروتوكولات الأمنيَّة مثل IPsec، TLS، S/MIME أو القيام بالتوثُّق من الأجوبة SIP responses.

- **البروتوكول TLS :[23][19][13]**
- **البروتوكول DTLS :[19][24]**
- **البروتوكول S/MIME: [13][19][25]**
- **البروتوكول IPsec: [19]**

أ- مقارنة آليات حماية رسائل البروتوكول SIP:

نقدِّم في الجدول (4) مقارنة بين الحلول الأمنيَّة الممكن تطبيقها من أجل حماية عملية تأسيس الاتصال:

TLS	DTLS	S/MIME	IPSEC
دعم التوثُّق المتبادل (المخدم والزبون) باستخدام الشهادات	دعم التوثُّق المتبادل (المخدم والزبون) باستخدام الشهادات	دعم التوثق من نوع طرف لطرف	التوثُّق من مصدر المعطيات
إمكانية تطويع ونشر سهلة بسبب استخدام SSL	إمكانية تطويع ونشر سهلة بسبب استخدام SSL	صعوبة في النشر بسبب متطلبات بيئة العمل	
تأمين التكامليَّة والسريَّة (خطوة بخطوة)	تأمين التكامليَّة والسريَّة (خطوة بخطوة)	يؤمن السريَّة من نوع طرف لطرف والتكامليَّة وعدم النكران	يؤمن السريَّة(خطوة بخطوة) والتكامليَّة والوثوقية وعدم النكران
الحماية من الهجمات: كتزوير الرسائل والتجسس عليها وتعديلها	الحماية من الهجمات: كتزوير الرسائل والتجسس عليها وتعديلها	حماية قوية ضد العديد من الهجومات: كتزوير الرسائل والتجسس عليها وتعديلها وهجومات رفض الخدمة	حماية من الهجمات: كتزوير الرسائل والتجسس عليها وتعديلها
تأثير منخفض في الأداء وسهولة في التنجيز	تأثير منخفض في الأداء وسهولة في التنجيز	يتطلَّب درجة كبيرة من التعقيد من أجل تنجيزه بسبب بسبب حاجته إلى وجود بنية PKI كأحد متطلبات بيئة العمل	يتطلَّب درجة كبيرة من التعقيد من أجل تنجيزه بسبب بسبب حاجته إلى وجود بنية PKI كأحد متطلبات بيئة العمل
حماية عملية تبادل مفاتيح التشفير	حماية عملية تبادل مفاتيح التشفير	القدرة على حماية أجزاء من رسالة SIP	حماية رسائل تحكُّم SIP
يتطلَّب وجود بنية PKI من أجل تطبيق التوثُّق المتبادل	يتطلَّب وجود بنية PKI من أجل تطبيق التوثُّق المتبادل	يتطلَّب وجود بنية PKI من أجل تنجيزه	يتطلَّب وجود بنية PKI
مستخدم مع TCP أو مع STCP فقط	مستخدم مع UDP	مستخدم مع TCP أو مع UDP	يعمل في طبقة الشبكة لذلك فهو مستخدم مع SIP, RTP, UDP, TCP
تعرض TLS لهجوم رفض الخدمة: - TCP Flood - RST packet or TLS records Tampering	استخدام الـ cookies عديمة الحالة للحماية من هجومات رفض الخدمة DOS attacks		
	حل مشكلة عدم الموثوقية unreliability المتعلقة بالبروتوكول UDP من خلال تأمين المصافحة الموثوق بها وكشف التكرار		
		غير مطبق على نطاق واسع بسبب حاجته إلى وجود بنية PKI كأحد متطلبات بيئة العمل	مطبق على نطاق واسع لكنَّه غير قابل للتوسع بشكل جيد في الشبكات الموزَّعة وفي أثناء العمل بالتطبيقات الموزَّعة كالمؤتمرات الفيديوية
			يجب أن تكون المكونات الوسيطة موثوقة trusted.
قادر على حماية معطيات طبقة التطبيقات	قادر على حماية معطيات طبقة التطبيقات	قادرة على ترويسة رسالة SIP	قادر على حماية كامل طرد IP Packet طبقة الشبكة
قادر على حماية عملية التفاوض على مفاتيح التشفير المستخدمة من قبل بروتوكول التشفير SRTP لحماية معطيات الصوت		قادر على حماية عملية التفاوض على مفاتيح التشفير المستخدمة من قبل بروتوكول التشفير SRTP لحماية معطيات الصوت	

الجدول 4: مقارنة آليات حماية البروتوكول SIP

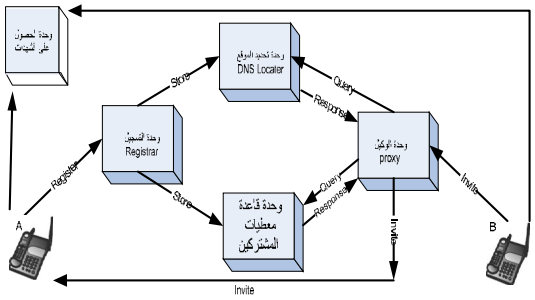
5 - تصميم وتحقيق النظام والنتائج العملية

نتعرف في هذا الفقرة على بنية النظام الاختباري الذي تم بناؤه وتصميمه من أجل اختبار الحلول الأمنية المدروسة (الحل الأمني عبارة عن تطبيق إحدى طرائق حماية رسائل التحكم مع برتوكول تبادل للمفاتيح) وتجريبها وإجراء مقارنة عملية لها، وذلك من خلال قياس أزمنة التأخير الناتجة عن تطبيق هذه الحلول ومقارنتها بالحالة الطبيعية لعملية تأسيس الاتصال من دون تطبيق أي حل أمني. واقتراح أفضل حل من خلال مفاضلة الخدمات الأمنية المحققة

لكل حل ونسبة التأخير الحاصل واختيار أفضل حل مأأمكن.

أ- تصميم النظام الاختباري:

يتكون النظام من أربعة مكونات أساسية، كلٍ من هذه المكونات يمكن أن يوجد على مخدم مستقل ليحقق دور محدداً، ولمّا كانت هذه الأدوار منطقية أمكن تجميعها على مخدم وحيد(انظر الشكل 5).



الشكل 5: بنية النظام الاختباري

يشكل المخطط السابق بيئة العمل التي سنقوم بتنجيزها وهي البيئة التي سنجري عليها القياسات العملية ضمن شبكة محلية LAN. سنقدم في هذا الفصل شرحاً لهذه المكونات وكيفية تحقيقها بالاستعانة بمجموعة من البرمجيات مفتوحة المصدر:

أ - وحدة الوكيل Proxy: عندما يرد طلب الدعوة من الطرف B الذي يريد أن يتكلم مع الطرف A، تقوم وحدة الوكيل بالتخاطب مع وحدة قاعدة معطيات المشتركين ليحصل منه على العناوين الممكنة للطرف A وإيصال الطلب إليه، وذلك بحال كان الطرف A ضمن النطاق نفسه. لكن بحال كان الطرف A يتبع لنطاق آخر، تقوم وحدة الوكيل بإرسال الطلب إلى وحدة الوكيل الخاصة بذلك النطاق لتقوم بدورها بالتخاطب مع خدمة تحديد الموقع لمعرفة مكان وجود الطرف الثاني A وإيصال الطب إليه بشكل صحيح.

ب - وحدة التسجيل Registrar: تستقبل طلب التسجيل الوارد من الزبون ضمن رسالة Register وتتحقق منها كما رأينا في الفصل الرابع (HTTP Digest). وبعد نجاح عملية التحقق تُسَجَّلُ حالة المشترك ضمن قاعدة المعطيات على أنه مشترك شرعي وتكون له الوضعية Registered. يتم تحقيق هذه الوظيفة من خلال بناء المكتبات اللازمة.

ج - وحدة تحديد الموقع DNS Locator: عندما يرد طلب الدعوة من مشترك معين تقوم وحدة التسجيل بالتخاطب مع خدمة تحديد الموقع لمعرفة مكان وجود هذه المشترك ومن أجل تحقيق هذه الخدمة تم بناء وظيفة تحديد موقع المستخدم.

د - وحدة قاعدة معطيات المشتركين: من أجل تحقيق بنية قاعدة معطيات المشتركين تم العمل ضمن بيئة قواعد البيانات MYSQL DB التي تتطلب تجهيز مخدم قواعد البيانات MYSQL Server 5.0 والمكتبات الخاصة بها وتجهيز زبون قواعد البيانات والمكتبات الخاصة بها ومن ثم تجهيز الواجهة البيانية التي تسهل عملية إدارة قواعد البيانات وتعريف المشتركين ومن ثم إنشاء قاعدة بيانات جديدة مع تعريف الجداول اللازمة والخاصة بالمشتركين.

من أجل تحقيق هذه الوحدات جُهّزَ المخدم المطلوب الذي سيجمع هذه الوحدات معاً لتتفاعل وتعمل مع بعضها بعضاً كنظام اتصال صوتي موحد، بنظام تشغيل Linux kernel 2.6.28-18 Debian 5.0. مع بناء البرمجية الرئيسية Kamailio 1.5.3 server with TLS support التي تدعم الوحدات السابقة والتخاطب معها.

و- عميل المستخدم User Agent: يتألف من مكونين الأول هو عميل المستخدم الزبون user agent

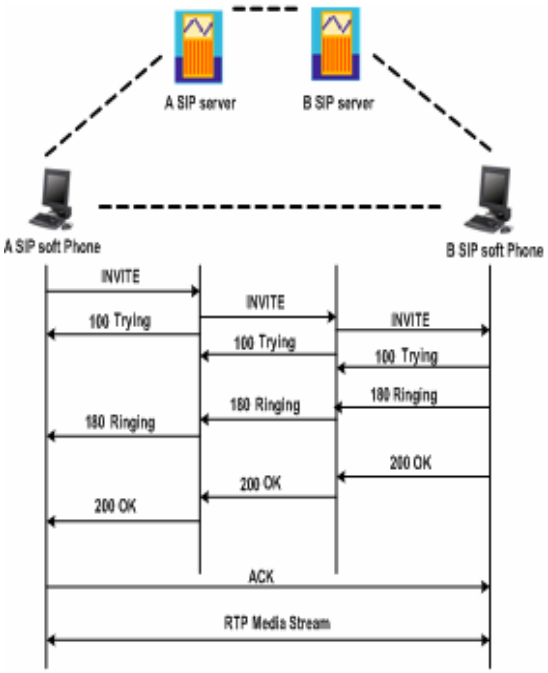
client، الذي يبعث رسائل SIP وعميل المستخدم المخدِّم user agent server، وهو الذي يجيب عنها. في أغلب الحالات يتوضع هذان المكونان في العميل نفسه. تمَّ بناء وتنصيب الهواتف البرمجية soft phones اللازمة للاختبار على الحواسب ضمن بيئة العمل فضلاً عن وضع الإعدادات اللازمة المتعلقة بالاتصال مع المخدم وتحديد بروتوكول النقل المستخدم TCP, TLS, UDP، والبوابة عند كل طرف بشكل مماثل للطرف الآخر.

ز - وحدة الحصول على الشهادات: تقوم بمنح شهادات للمستخدمين ولمكونات بيئة العمل وتوقيعها ذاتياً من قبل سلطة شهادات محلية معرفة ضمن هذه الوحدة.

- تم استخدام المكتبة openssl, ssl لتحقيق هذه الوظائف.

ب - عملية سير الاتصال في SIP:

من أجل تأسيس الاتصال بين الطرفين A,B (انظر الشكل 6)، يقوم الطرف الأول A بإرسال رسالة دعوة INVITE (وهي إحدى رسائل البروتوكول SIP) إلى المخدِّم الوكيل الموجود ضمن النطاق domain الخاص بالطرف A، يقوم المخدِّم الوكيل بالاتصال بالمخدِّم المسجِّل من أجل الحصول على كل العناوين الممكنة للطرف الثاني B المطلوب الاتصال به وبناءً على أولوية هذه العناوين، يقوم المخدِّم الوكيل بإرسال الطلب INVITE إلى الطرف B مباشرةً أو إلى مخدِّم وكيل آخر موجود ضمن النطاق domain الخاص بالطرف B. يقوم المخدِّم الوكيل عند الطرف B بإرسال رسالة إلى مخدِّم تحديد الموقع ضمن النطاق B ليحصل منه على موقع الطرف B، ومن ثمَّ إيصال الطلب إلى الطرف B، الذي سيقوم بدوره بالرد على الطلب الوارد من الطرف A.



الشكل 6: عملية سير الاتصال ضمن بيئة العمل

يجيب عميل الطرف B بالرسالة 100 Trying التي تشير إلى أنَّه يقوم بمعالجة طلب الدعوة ومن ثمَّ يبعث عميل الطرف B الرسالة 180 ringing التي تدلُّ على أنَّه يحاول الوصول إلى الطرف النهائي B يمكن للطرف B أن يقبل أو يرفض الاتصال، ولذلك يبعث عميل الطرف B الرسالة 200 OK التي تدل على قبول الاتصال، يستقبل الطرف A الجواب ويرسل رسالة إقرار ACK إلى الطرف B. عندما يستقبل الطرف B هذه الرسالة يقوم بتأكيد انتهاء مرحلة تأسيس الاتصال، ليتم بعدها تبادل الوسائط بين الطرفين عن طريق بروتوكول النقل في الزمن الحقيقي RTP. يتم التفاوض على موسطات الجلسة بين الطرفين من خلال الرسالتين INVITE, OK ومن أجل تغيير هذه الموسطات يمكن لأي طرف أن يرسل رسالة دعوة جديدة، لكي يتم الاتِّفاق على هذه

الموسطات مجدداً. يمكن إنهاء الجلسة من خلال إرسال الرسالة BYE من أحد الطرفين فضلاً عن رسالة إقرار 200 OK من الطرف الآخر.

ب - **أدوات الاختبار المستخدمة ضمن بيئة النظام:**

- ❖ Wireshark: هذه الأداة مستخدمة من أجل التقاط الطرود بشكل كامل وتحليلها وقياس أزمنة التأخير المطلوبة والتي سنتعرّفها في فقرة لاحقة.
- ❖ SIPP: هذه الأداة مستخدمة من أجل توليد حمل load ضمن بيئة العمل وذلك من خلال توليد رسائل تسجيل ودعوة وإرسالها إلى مخدم SIP الوكيل، كما تمكن هذه الأداة من رفع الحمل على المخدم بنسبة مئوية معينة بهدف محاكاة الحالة الطبيعية وهي ورود العديد من الاتصالات من قبل المستخدمين ضمن بيئة نظام الاتصال الصوتي وليس اتصالاً واحداً فقط بين مستخدمين اثنين. يُعدُّ SIPP أحد أهم أدوات قياس أداء البروتوكول SIP وتُتيح هذه الأداة تأسيس الاتصال بين طرفين وحمايته باستخدام IPSec أو TLS. تسمح هذه الأداة بتوليد مكالمات عشوائية ومن ثمَّ زيادة الضغط على مخدم SIP الوكيل.
- ❖ SIP Senario Generator: تسمح هذه الأداة بتوليد مخططات تدفقية لسير رسائل التحكم ضمن مكونات النظام الاختباري بشكل مشابه للشكل 6.
- ❖ Snom، Kphone، Zphone، Twinkle Minisip: هذه الأدوات تعمل كهواتف برمجية IP softphone مستخدمة من أجل الاتصال بين طرفين نهائيين.
- ❖ SIPsak (SIP Swiss Army Knife): أداة معتمدة على أوامر نصية موجهة للتطبيقات المعتمدة على بروتوكول تأسيس الجلسة SIP من أجل إجراء الاختبارات عليها.
- ❖ Protos: أداة تقوم بحق طرود مزورة ضمن بيئة الاتصال الصوتي بهدف القيام بالعديد من الهجمات.
- ❖ SiVus: هي أداة تعرض scan لنقاط الضعف التي تتعرض لها شبكات الاتصال الصوتي المعتمدة على SIP .
- ❖ Cain & apil: أداة معقدة من أجل التقاط كلمات السر المشفرة وغير المشفرة من خلال القيام بهجمات متعددة كالهجوم المعجمي dictionary attack وهجوم القوة المفرطة brute force attack فضلاً عن القيام بهجوم الرجل بالوسط.

ت - **محددات آداء الاتصال الصوتي عبر الإنترنت:**

يوجد العديد من العوامل التي تحدد أداء الاتصال الصوتي، نذكر منها مقدار التأخير delay والتغير في مقدار التأخير Jitter وغيرها. رُكِّزَ في هذا البحث على مقدار التأخير الحاصل عن تطبيق الحلول الأمنية مقارنةً بالحالة الطبيعية من دون تطبيق أي حل أمني ومن هنا تم التركيز على ثلاثة أزمنة مهمة متعلقة بموضوع البحث من أجل دراسة مقدار الزيادة في التأخير بعد تطبيق الحلول الأمنية وهي:

- ➢ زمن الرنين Ringing Delay: وهو الزمن الفاصل من لحظة طلب الطرف A رقم الطرف الثاني B حتى يصله تنبيه بأنَّ وكيل الطرف الثاني يرن.
- ➢ زمن الإجابة Answering Delay: وهو الزمن الفاصل من لحظة قبول الطرف الثاني للاتصال(رفع السماعة) إلى لحظة وصول الإقرار ACK إليه من الطرف الأول.
- ➢ زمن التسجيل Registering Delay: هو الزمن الفاصل من لحظة إرسال الطرف A الرسالة register إلى لحظة وصول الرسالة 200 OK إلى

الطرف A (يتضمَّن هذا الزمن زمناً آخرَ هو الزمن اللازم من أجل فتح اتصال TCP أو TLS).

ويكون زمن تأسيس الاتصال call delay مساوياً لمجموع الأزمنة السابقة:

زمن تأسيس الاتصال = زمن الرنين + زمن الإجابة + زمن التسجيل

بعد تعريف هذه الأزمنة لابدَّ من تعريف مقدار التأخير الممكن التسامح به بشكل تقريبي والقيم المقبولة كحد أعلى وحد أدنى فكما هو وارد في توصيات منظمة الاتصالات الدولية ITU-T في الجزء p.800 الخاص بالاتصال الصوتي عبر الإنترنت (e.g. P.862).

Factor	Good	Acceptable	Poor
Delay	< 150 ms	...	> 400 ms

وكما هو وارد في المرجع [3] أن القيمة المحدد صناعياً والتي يمكن أن نتسامح بها وعدّها مقبولة بالنسبة إلى المستخدم النهائي يجب أن تكون أقل من 200 ميلي ثانية. يمكن أن نقارن القيم التي حصلنا عليها في السيناريوهات المختبرة بهذه القيم المرجعية.

ج - سيناريوهات العمل المختبرة:

في هذه الفقرة سنقدم العديد من السناريوهات التي اختُبِرَتْ ضمن بيئة النظام سنقوم بقياس التأخير الحاصل في مرحلة تأسيس الاتصال لكل من رسائل التسجيل Register (زمن التسجيل) والدعوة Invite (زمن الرنين + زمن الاستجابة)، يشير العمود الأول في الجداول التالية إلى بروتوكول النقل المستخدم في حين يدل العمود الثاني على الحل الأمني المطبق متمثلاً ببروتوكول تبادل المفاتيح المستخدم مع تشفير إشارات التحكم أو من دونها. يدل العمود الثالث على مقدار التأخير الحاصل لعملية التسجيل وفي العمود الرابع نجد مقدار التأخير الحاصل لعملية الرنين وفي العمود الخامس نجد مقدار التأخير الحاصل لعملية الاجابة.

ونلاحظ أن القيم الواردة في الجداول التالية هي قيمة الوسطي لمجموعة من القياسات بالميلي ثانية مطبقة على كل حالة من الحالات المذكورة في كل سطر. ونشير إلى أنَّ بروتوكول حماية معطيات الصوت المستخدم هو البروتوكول SRTP:

- **تأسيس اتصال VoIP بين الطرفين A,B دون تطبيق أي حل أمني:**

هنا يتم تأسيس الاتصال بين الطرفين باستخدام Minisip أو Snom 320 أو أي هاتف آخر من دون تطبيق أي حل أمني أو أي طريقة لتبادل المفاتيح، كما أنَّ بروتوكول تبادل معطيات الصوت المستخدم هو البروتوكول RTP. حصلنا على النتائج الآتية كماهي موضحة بالجدول رقم (5):

Protocol	Security	Registration delay(ms)	Calling delay(ms)	Answering delay(ms)
UDP	NO	0.001	0.0034	0.009
TCP	NO	0.004	0.08	0.01

الجدول رقم 5

نلاحظ أن القيم الواردة في الجدول متوافقة مع القيم المرجعية المقبولة وبذلك يمكن تكرار التجارب لكن مع تطبيق الحلول الأمنية المدروسة.

- **تأسيس اتصال VoIP باستخدام Minisip بين الطرفين A,B مع تشفير رسائل التحكُّم:**

يمكن لـ Minisip أن يؤسس اتصالات VoIP آمنة ومحمية باستخدام مايأتي:

1 -استخدام البروتوكول MIKEY من أجل تبادل المفاتيح والموسطات الأمنيَّة للبروتوكول SRTP وفق الحالات الآتية:

- استخدام خوارزميَّة DH.
- استخدام مفتاح موزع بشكل مسبق PSK .
- استخدام تقنية المفتاح العام PK.

2 -استخدام الطريقتين PSK و PK معاً.

3 -استخدام SIP over TLS or SIPS من أجل حماية رسائل تحكُّم البروتوكول SIP، ومنه تتم حماية المفاتيح المتبالة ضمن هذه الرسائل.

4 -استخدام SRTP لحماية الوسائط المتبادلة. انظر الجدول رقم (6)

Protocol	MIKEY Authentication	Registration delay(ms)	Calling delay(ms)	Answering delay(ms)
UDP	PSK	0.005	0.005	0.01
	PK	0.007	0.012	0.009
	DH	0.006	0.02	0.011
	PK + PSK	0.006	0.012	0.011
TCP	PSK	0.009	0.03	0.01
	PK	0.009	0.08	0.02
	DH	0.008	0.09	0.03
	PK + PSK	0.009	0.05	0.02
TLS	PSK	0.11	0.07	0.02
	PK	0.11	0.09	0.01
	DH	0.12	0.09	0.03
	PK + PSK	0.13	0.1	0.01

الجدول رقم 6

تأسيس اتصال VoIP باستخدام snom 360 بين الطرفين A,B مع تشفير رسائل التحكُّم :

يمكن لـ snom 360 أن يؤسِّس اتصالات VoIP آمنة ومحمية باستخدام مايأتي:

1 -استخدام البروتوكول Sdescription من أجل تبادل المفاتيح والموسطات الأمنيَّة للبروتوكول SRTP

2 -استخدام SIP over TLS or SIPS من أجل حماية رسائل نحكم البروتوكول SIP ومنه تتم حماية المفاتيح المتبادلة ضمن هذه الرسائل.

3 -SRTP لحماية الوسائط المتبادلة. انظر الجدول رقم (7)

Protocol	Security / Sdesc	Registration delay(ms)	Calling delay(ms)	Answering delay(ms)
UDP	Sdesc	0.002	0.11	0.01
TCP	Sdesc	0.006	0.17	0.01
TCP + TLS	Sdesc	0.13	0.24	0.226

الجدول رقم 7

ملاحظة: عند تطبيق الحلول الأمنيَّة TLS, MIKEY نحتاج إلى وجود بنية PKI infrastructure وكحل بديل قمنا بتوليد مجموعة من الشهادات الموقعة ذاتياً self signed certificates ومن أجل توليدها يتم استخدام المجتزأ module المرافق مع Kamailio واستخدام المكتبة OpenSSL, LibSSL وذلك من خلال توليد سلطة شهادات جذرية موقعة ذاتياً RootCA ومن ثم توليد مجموعة من الشهادات لكل من الطرفين A,B والمخدِّم الوكيل موقعة من سلطة الشهادات المذكورة.

تأسيس الاتصال بين الطرفين A,B مع وجود بنية IPSec:

يمكن تأسيس اتصالات VoIP آمنة ومحمية باستخدام IPSec يتم تنجيزه على مستوى نواة نظام التشغيل Linux، لذلك يمكن استخدام أي هاتف. يتم تأسيس قناة IPSec

بين الطرفين A,B وبين كل طرف مع المخدم الرئيسي كل على حدة. باستخدام مجموعة من المكتبات أهمها:

- المكتبة Racoon المستخدمة من أجل إدارة الاتصال وحساب قيم الارتباط الأمني Security Association SA.
- المكتبة IPSec-tools المستخدمة من أجل تعريف الاتصال بين كل طرفين سيتصلان ببعض وتعريف قيم السياسة الأمنيَّة IPSec Policy.
- البروتوكول IKE مستخدم من أجل تبادل المفاتيح.

تأسيس الاتصال باستخدام Twinkle بين الطرفين A,B:

يمكن تأسيس اتصالات VoIP آمنة ومحمية باستخدام البروتوكول ZRTP الذي يستخدم البروتوكول SRTP من أجل حماية الوسائط المتبادلة وبروتوكول DH من أجل تبادل المفاتيح اللازمة مع استخدام SAS (Short Authentication String) method من أجل الحماية من هجوم رفض الخدمة DoS الذي من الممكن أن يتعرض له البروتوكول DH. كذلك نحتاج إلى أداة مساعدة من أجل تطبيق ZRTP بين الطرفين النهائيين وهي zfone.انظر الجدول (8)

Protocol	Security	Registration delay(ms)	Calling delay(ms)	Answering delay(ms)
TCP	ZRTP (DH+ SAS)	0.8	0.12	0.02

الجدول رقم 8

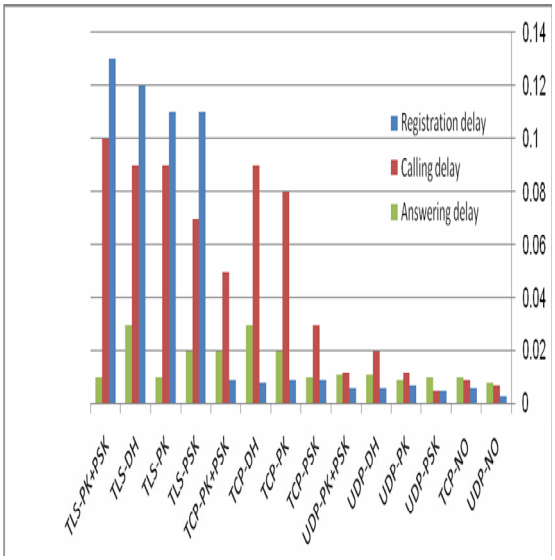
تأسيس الاتصال مع تطبيق طرائق مختلفة للتوثق:

نطبق في هذه الحالة المختبرة طريقة التوثق HTTP Digest المعتمدة على تقديم اسم مستخدم وكلمة سر من قبل الطرفية النهائية إلى المخدم الوكيل. والحالة الثانية تحقيق التوثق عن طريق استخدام TLS باتجاه وحيد وباتجاهين. انظر الجدول رقم (9).

Protocol	Security Authentiaction method	Authentication Delay(ms)
TCP	HTTP Digest	0.14
TCP	TLS one way auth	0.17
TCP	TLS mutual auth	0.25

الجدول رقم 9

نجد في الشكل (7) مقارنة عملية بين طرق الحماية المستخدمة:



الشكل 7: مقارنة القياسات باستخدام هواتف مختلفة

وكما هو ملاحظ أنَّ هذه الأزمنة الناتجة منخفضة نسبياً ومتقاربة من بعضها مع وجود بعض الفروقات الصغيرة، ولكنها أزمنة مقبولة على خلاف قيم التأخير الحاصلة من استخدام IPSec وهذا هو سبب استبعاد هذا البروتوكول من المقارنة كما هو موضح في الفصل الرابع(سنقوم بضمه للمقارنة بشرط أن تكون قناة IPSec مؤسسة مسبقاً).

ث - مناقشة النتائج وبناء الحل المفضل:

يمكن استخدام أحد البروتوكولات المبينة في الجدول (10) من أجل حماية رسائل التحكم والمفاتيح المتبادلة، ونلاحظ من الجدول أنَّ زمن تأسيس الاتصال الناتج عن استخدام TLS مقبول كما هو مبين في الفقرة 6-5 في حين نجده يتجاول القيم المسموحة عند استخدام البروتوكول TLS، إلا بحالة خاصة جداً وهي أن تكون القناة مؤسسة مسبقاً. وبذلك يمكن استبعاد IPSec بسبب التأخير غير المسموح الذي ينتج عنه واستبعاد S/MIME بسبب تعقيده.

Protocol	Call delay
TLS	0.24 ms
IPSec	2 second
IPSec pre-established (ESP)	0.12 ms
S/MIME	تنجيزه معقد جداً

الجدول رقم 10

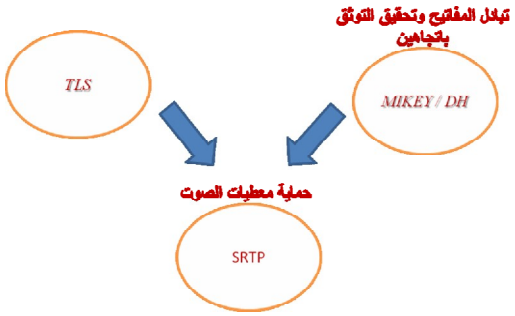
نحتاج أيضاً استخدام بروتوكول لتبادل المفاتيح وكما هو مبين في الجدول رقم 11 يمكن استخدام أحد هذه البروتوكولات إذ إنَّها تعطي زمن تأخير مقبولاً. وكما ذكرنا سابقاً إنَّ رسائل هذه البروتوكولات تحتاج حماية. ونلاحظ أنَّ طريقة تبادل المفاتيح المعتمدة على المفتاح الموزع مسبقاً هي طريقة قديمة نوعاً ما ولايمكن الاعتماد عليها، أمَّا الطريقة المعتمدة على المفتاح العام فهي بحاجة لوجود بنية PKI ولايمكن الاعتماد عليها أيضاً، وبالنسبة إلى الطريقتين Sdesc, ZRTP فهما لاتحققان خاصية التوثق في مرحلة تأسيس الاتصال. ومنه نستنتج أن أفضل طريقة يمكن استخدامها هي MIKEY/DH لكنها عرضة لهجوم الرجل بالوسط كما نعلم، لكن يمكن التغلب على هذا الهجوم من خلال تشفير رسائل هذه الطريقة.

Key Exchange	Call delay
MIKEY/PSK	0.11
MIKEY/PK	0.12
MIKEY/DH	0.16
Sdesc	0.14
ZRTP (DH & SAS)	0.10

الجدول رقم 11

وبذلك قمنا باستخدام المكونات الآتيـــة لبنـــاء الحـــل المفضل:

- MIKEY/DH من أجل نقل المفاتيح اللازمة لعمل SRTP.
- DH من أجل تحقيق التوثق المتبادل.
- TLS من أجل حماية رسائل التحكم وعملية تبادل المفاتيح.
- SRTP من أجل حماية معطيات الصوت. فالحـــل ناتج عن تطبيق عدة حلول مع بعضها كمـــا هـــو مبين في الشكل (8):



الشكل 8: الحل الأمني المفضل

ج- خصائص الحل:

1 - سيتم تأسيس الاتصال مع الطرف المطلوب تماماً، حتى يتأكد الطرف A من أنه يتكلم مع الطرف B فعلاً فنحن بحاجة إلى تحقيق الوثوقية مـــن نـــوع طرف لطرف، وهذا محقق باستخدام البروتوكـــول MIKEY مع خوارزميَّة DH من أجـــل تبـــادل المفاتيح والموسطات الأمنيَّة الخاصة بالبروتوكول SRTP، كما يُفضل استخدام TLS من أجل حماية عملية تبادل المفاتيح.

2 - الاتصالات غير المرغوب بها محجوبـــة وذلـــك لتجنب الاتـــصالات مجهولـــة المـــصدر VOIP Spamming، علـــى أيـــة حـــال تُحقِّـــق عمليـــة

المصافحة عند تأسيس الاتصال إمكانية رفض مثل هذا الاتصالات آلياً وذلك بالاعتماد على معلومات المستخدم User Preferences.

3 - معطيات الصوت محمية من التجسس eavesdropping فإذا بدأ الطرف A اتصاله الآمن فهو يتوقع أن يتكلم مع الطرف B بشكل خاص وغير مكشوف للآخرين. إن الحاجة لهذه الخدمة في حالة الاتصال الصوتي عبر الإنترنت VOIP أكبر من الحاجة لها في شبكات الهاتف الثابتة PSIN لأن إمكانية تعرض الاتصال الصوتي IP call للتجسس أكبر.

5 - يجب أن تكون المعلومات عن هوية الطرف B غير مكشوفة، وبكلام آخر من يُكلِّم الطرف A. ولتحقيق هذا المطلب الأمني يجب تشفير رسائل البروتوكول SIP في مرحلة تأسيس الاتصال. لكن تبقى الفرصة متاحة للمهاجم لمعرفة هوية الطرف الآخر من خلال متابعة الطرود المارة على مخدم الأسماء DNS وذلك بحال كان الطرف الآخر B ضمن نطاق domain خاص به ومستقل عن النطاق الذي يتبع له الطرف A، أو من خلال مراقبة تدفق معطيات البروتوكول RTP (وذلك بحال كان للطرف B عنوان IP ثابت لا يتغير).

6 - عدم كشف معرِّف المتَّصل (الطرف A) من خلال التجسس، إن هذا المطلب صعب التحقيق، لكن ربما لا يكون له أهمية بالنسبة إلى المستخدمين، إذ إنَّه حتى لو تمكنا من حماية كل رسائل التحكم للبروتوكول SIP، ثمة العديد من الطرائق الأخرى المتاحة للمهاجم ليتمكن من كشف هوية الطرف A، ربما ذلك يكون من خلال مراقبة المعطيات الأخرى التي يتم إرسالها واستقبالها من قبل الطرف A.

إن عنونة الخاصية (1) والخاصية (2) ممكنة من خلال إجراء توثق متبادل بين الطرفين A، B في مرحلة تأسيس الاتصال، فالوثوقية وكما ذكرنا جزء مهم من بروتوكول تبادل المفاتيح ، المستخدم لتأسيس ارتباط أمني security Association بين الطرفين A B، والمقصود بذلك: معلومات التشفير التي سيتم استخدامها وخلق المفتاح الرئيسي Master key المستخدم في الجلسة فضلاً عن معلومات أخرى... يمكن استخدام هذا السياق الأمني بعد تأسيس الاتصال من أجل تحقيق سرية وتكاملية معطيات الصوت الخاصة بالمستخدم أي عنونة الخاصية 3 يتم ذلك من خلال تشفير الصوت نفسه باستخدام SRTP. من أجل عنونة الخاصية 4 والخاصية 5 يجب أن تكون رسائل البروتوكول SIP مؤمنة خطوة بخطوة hop-by-hop يتم ذلك باستخدام البروتوكول TLS بين مكونات بيئة العمل الرئيسية، على الأقل المسار من الطرف A إلى المخدم الوكيل الذي يتبع له. يتَّبع البرتوكول TLS المستخدم لحماية رسائل تحكم SIP محددات البروتوكول Secure SIP URI (SIPS) نفسه.

على الرغم من أن استخدام SIPS-URI يضمن أن كل العقد بين مكونات بيئة عمل البروتوكول SIP (ربما ما عدا آخر عقدة بين المخّدم الوكيل الذي يتبع له الطرف B والطرف B ذاته) يجب أن تكون محميَّة باستخدام البروتوكول TLS، لابدَّ من ملاحظة أن SIPS URI لا يقدّم وثوقية من نوع طرف لطرف، أو تشفيراً لمعطيات الصوت بل فقط يحقق حماية من نوع خطوة بخطوة hop-by-hop لرسائل تحكم البروتوكول SIP.

ز - تحليل نتائج التأخير:

1 -يُهمل التأخير الناتج عن انتشار الإشارة ضمن الشبكة ضمن بيئة الاختبار لأنَّ المسافة بين

مكونات SIP خطوة hop واحدة وهذا يعني أنَّه في الحالات الحقيقية يجب أن يؤخذ هذا التأخير بالحسبان وتجب إضافته.

2 -تأخير ناتج عن فتح اتصال TCP فكما هو معلوم تتطلب العملية إرسال مجموعة من الطرود قبل أن تبدأ عملية التسجيل ممايزيد التأخير في عملية التسجيل.

3 -تأخير ناتج عن نظام حل نطاقات الأسماء DNS فكما هو موضح بالشكل 6 يتم الاستعلام عن العنوان من خلال عملية DNS lookup في كل مكون من مكونات بيئة العمل من أجل مقابلة الاسم بعنوان IP. من الأفضل إعادة إقلاع خدمة التسمية بعد كل محاولة وذلك من أجل صحة القياسات بسبب التخبئة caching

4 -تأخير ناتج عن التوثق من المستخدم النهائي من بسبب الاتصال بقاعدة بينات المشتركين كما هو متَّبع في طريقة HTTP Digest المعتمدة على نموذج تحدي/جواب.

5 -تتم عملية تأسيس اتصال TLS في بداية عملية التسجيل register للزبون مع المخدِّم الموافق مما ينتج عنه تأخير إضافي في عملية التسجيل كما هو موضح في جداول النتائج، وهذا ناتج عن عمليات تبادل الشهادات وعمليات التشفير الحاصلة.

6 -ينتج عن عملية استخدام IPSec بدلاً من SRTP تأخير إضافي ناتج عن استدعاءات النظام (التي تعدُّ عمليات مستهلكة للوقت) الحاصلة من أجل حساب قيم الارتباط الأمني وقيم السياسة الأمنيَّة IPSec Policy.

7 -يُستخدم IPSec من أجل حماية المعطيات المتبادلة بشكل عام لكن SRTP مفضَّل من أجل تطبيقات نقل الصوت عبر الإنترنت VoIP وذلك للأسباب الآتية:

أ- عند استخدام IPSec نحتاج إلى التخاطب مع بعض البرمجيات التي تدعم IPSec على مستوى نواة نظام التشغيل، وهذا يتطلَّب سماحيات privileges خاصة للتخاطب مع النواة فضلاً عن الحاجة إلى التواصل بين فضاء النواة kernel space وفضاء المستخدم user space (وهذا التعقيد غير موجود في SRTP).

ب - تأخير ناتج عن كتابة قيم الارتباط الأمني وقيم السياسة الأمنيَّة في نواة نظام التشغيل.

ت - يحمي IPSec المعطيات المتبادلة بالنمط طرفية لطرفية ولاتعدُّ هذه الحماية من النمط تطبيق لتطبيق

8 - تتكامل SRTP بشكل أفضل مع التطبيق فضلاً عن سهولة تنجيزها واستقلاليتها عن بنية نظام التشغيل نسبياً.

9 - ثمة تأخير حاصل من توليد الرسائل الخاصة بالبروتوكولين MIKEY, Sdesc وحساب التوقيع الإلكتروني لـ MIKEY والتحقق من رسائل MIKEY المبعوثة والردود الموافقة.

10 -على الرغم لما للبروتوكول S/MIME من فوائد أمنية مهمة كحماية أجزاء انتقائية من رسالة التحكم للبروتوكول SIP من نوع طرف لطرف وهذا ما لايحققه TLS or IPSec. إلا أنَّ هذا البروتوكول له تعقيد كبير جداً وهذا سبب ابتعاد مطوري منتجات VoIP عن تنجيز هذا البروتوكول وهذا هو سبب عدم وجود أي

منتجات VoIP clients تدعمه. ونجد أنَّ معظم المنتجات تتجه نحو SIPS/SRTP أو IPSec.

الخاتمة والآفاق المستقبلية:

بعد دراسة هذه القضايا الأمنيَّة المتعلقة بالبروتوكول SIP وتحليلها، نتبين أنَّه من الضروري لمزودات خدمة SIP أن تأخذ بالحسبان وبشكل جدي التهديدات والمخاطر التي تعتري بيئة عمل SIP التي يمكن أن يستغلَّها المهاجم لشن هجوم ما، ومن أجل تخفيف أثر هذه التهديدات من المهم جداً تعريف المتطلبات الأمنيَّة الفعلية وتحقيقها من خلال تطبيق الآليات الأمنيَّة المناسبة، وكما هو مبيّن سابقاً لا يوجد أي من هذه الآليات تحقق المتطلبات الأمنيَّة كلّها وبالنتيجة نقول: إنَّه يجب على مزودي خدمة SIP أن يراقبوا الآليات الأمنيَّة المطورة حديثاً كمحاولة لإيجاد طرائق لدمجها مع الآليات الأمنيَّة الحالية. تفتح المناقشة الحاصلة في البحث الباب للعديد من الموضوعات للغوص فيها وإكمال الطريق إما لتنجيز الحل المفضل في البحث أو تنجيز حلول أخرى مازالت في طور البناء ولم تصدر مسودة الإنترنت الخاصة بها كالحل المعتمد على استخدام ZRTP والذي من المتوقع أن يستبدل كل الحلول الحالية أو تنجيز البروتوكول DTLS ليعمل مع البروتوكول UDP كونه يعطي أداء أفضل من البروتوكول TCP عندما يعمل مع البروتوكول TLS. يمكن أيضاً إكمال الطريق لموضوع أوسع انتشاراً وهو موضوع أمن النظام الفرعي متعدد الوسائط IP Multi Media Subsystem Security كون هذا النظام يشكل البنية الأساسية للجيل الجديد من الشبكات وفيها نُعنى بنقل الوسائط المتعددة كالصوت والصورة والفيديو، وموضوع حمايتها ضروري جداً بسبب وجود العديد من التهديدات الأمنية التي تعتريها كتلك الموجودة في بيئة نظام الاتصال الصوتي وغيرها من التهديدات الجديدة. يمكن أيضاً التطرق إلى موضوع أمن الاتصال الصوتي في شبكات الند للند P2P VoIP Security وهو موضوع شائك وأكثر تعقيداً. أيضاً يمكن تمديد موضوع أمن الاتصال الصوتي ليشمل الشبكات اللاسلكية(Wireless & Ad Hoc Networks).

المراجع

[1]: Requirements for End-To-Middle Security for the Session Initiation Protocol, Ono, K., and S. Tachimoto, RFC 4189, 2005

[2]: VoIP defender: Highly scalable SIP-based security architecture, Fiedler, J., T. Kupka, S. Ehlert, T. Magedanz, and D. Sisalem, Principles, Systems and Applications of IP Telecommunications (IPTComm). New York, USA. 2007

[3]: Providing response identity and authentication in IP telephony, Cao, F., and C. Jennings, In Proceedings of the First International Conference on Availability, Reliability and Security, 2006.

[4]: Secure authentication scheme for session initiation Protocol, Yang, C., R. Wang, and W. Liu, Computers & Security 24 (5): 381–86, 2005.

[5]: A lightweight protection Mechanism against signaling attacks in a SIP-based VoIP environment, Telecommunication Systems, 36(4): 153–59, Geneiatakis, D., and C. Lambrinoudakis, 2007.

[6]: Denial of service attack and prevention on SIP VoIP infrastructures using DNS flooding. Principles, Systems and Applications of IP Telecommunications (IPTComm2007), Zhang, G., S. Ehlert, T. Magedanz, and D. Sisalem, 2007.

[7]: Secure IP telephony using multilayered protection, Reynolds, B., and D. Ghosal, In Proceedings of the Network and Distributed System Security Symposium (NDSS), 2003.

[8]: Fast detection of denial-of-service attacks on IP telephony, Sengar, H., H.Wang, D. Wijesekera, and S. Jajodia, In Proceedings of 14th IEEE International Workshop on Quality of Service, 199–208. 2006.

[9]: Detecting DoS attacks on SIP systems, Chen, E. Y., In Proceedings of 1st IEEE workshop on VoIP Management and Security. 3: 53–58. 2006.

[10]: Enhancements for authenticated identity management in the session initiation protocol (SIP), Peterson, J.

[11]: SIP Security Issues: The SIP authentication procedure and its processing load, Salsano, S. Veltri, L. and Papalilo D., IEEE Network.

[12]: Secure VoIP: call establishment and media protection, Johan Bilien, Erik Eliasson, Joachim Orrblad, Jon-Olov, Vatn, Royal Institute of Technology (KTH) Stockholm, Sweden, 2006.

[13]: RFC 3261 SIP Session Initiation Protocol, http://www.ietf.org/rfc/rfc3261.txt, The Internet Society, 2002.

[14]: Security_of_VoIP_in_enterprise master thesis, Christina Chalastanis, University of Stuttgart, 2005-2006.

[15]: SIP Hand Book Services, Technologies, and Security of Session Initiation Protocol, Syed A. Ahson Mohammad Ilyas, CRC Press Taylor &. Francis Group Boca Raton London New York, 2009

[16]: RFC 2617, HTTP Authentication: Basic and Digest Access Authentication,

[17]: 8: Thermos, P. Two attacks against VoIP. Retrieved April, 2006 at http://www.securityfocus.com/infocus/1862/1.

[18]: Reviewing the VoIP Threat Landscape white paper, Border Ware Technologies Inc, 2006.

[19]: securing VoIP networks, Peter Thermos and Ari Takanen, Addison wesly, 2009.

[20]: RFC 3835 MIKEY, http://www.ietf.org/rfc/rfc3830.txt

[21]: RFC 4568 Sdescription, http://www.ietf.org/rfc/rfc4568.txt

[22]: Internet Draft, http://tools.ietf.org/html/draft-zimmermann-avt-zrtp-17

[23]: RFC 2246 The TLS Protocol Version 1.0, www.ietf.org/rfc/rfc2246.txt

[24]: RFC 4347 DTLS

[25]: S/MIME Version 3 Message Specification, www.ietf.org/rfc/rfc2633.txt, RFC 3851, RFC 3853, RFC 3852

www.ietf.org/rfc/rfc2617.txt

تاريخ ورود البحث إلى مجلة جامعة دمشق 2010/11/14.