الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1362

(2017/03)

السلسلة X: شبكات البيانات والاتصالات، بين الأنظمة المفتوحة ومسائل الأمن

التطبيقات والخدمات الآمنة – أمن إنترنت الأشياء

إجراء تجفير بسيط من أجل بيئات إنترنت الأشياء (IoT)

التوصية ITU-T X.1362

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309–X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339–X.1310
التوصيات ذات الصلة بالبنية التحتية للمفاتيح العمومية	X.1349-X.1340
أمن إنترنت الأشياء	**X.1369-X.1360**
أمن أنظمة النقل الذكية	X.1379-X.1370
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أشكال أخرى لأمن الحوسبة السحابية	X.1699–X.1680

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1362

إجراء تجفير بسيط من أجل بيئات إنترنت الأشياء

ملخص

يُعتبر إنترنت الأشياء (IoT) من أهم المجالات المتعلقة بعملية التقييس في المستقبل. وتعرف إنترنت الأشياء، من منظور قطاع تقييس الاتصالات، بأنها بنية تحتية عالمية لمجتمع المعلومات تمكّن الخدمات المتطورة عن طريق التوصيل البيني للأشياء (المادية والافتراضية).

وفي بعض بيئات إنترنت الأشياء، ولا سيما بالنسبة إلى أجهزة إنترنت الأشياء، هناك شرط للمعالجة في الوقت الفعلي حيث تعالج المهام في غضون فترة زمنية محددة. ومن أجل ضمان حماية سرية البيانات وسلامتها، يعتبر تطبيق خوارزميات لتجفير البيانات والاستيقان منها أحد التدابير المضادة الأكثر شيوعاً. والمشكلة في التطبيقات القياسية لخوارزميات تجفير البيانات والاستيقان منها تتمثل في إمكانية عدم تحقيق هذا الشرط.

وتوصف التوصية ITU-T X.1362 التجفير ببيانات القناع المصاحب (EAMD) من أجل أجهزة إنترنت الأشياء. وتصف التجفير EAMD، وكيف أنه يوفر مجموعة من الخدمات الأمنية للحركة التي تستخدم التجفير EAMD.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1362	2017-03-30	17	11.1002/1000/13196

مصطلحات أساسية

تطبيق خوارزميات تجفير/استيقان البيانات، التجفير ببيانات القناع المصاحب (EAMD)، أجهزة إنترنت الأشياء، بيئات إنترنت الأشياء، شرط المعالجة في الوقت الفعلي.

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

مقدمة

تعتبر إنترنت الأشياء من أهم المجالات المتعلقة بعملية التقييس في المستقبل. وتُعرف إنترنت الأشياء، من منظور قطاع تقييس الاتصالات، بأنها بنية تحتية عالمية لمجتمع المعلومات تمكّن الخدمات المتطورة عن طريق التوصيل البيني للأشياء (المادية والافتراضية) استناداً إلى تكنولوجيات المعلومات والاتصالات القابلة للتشغيل البيني القائمة والمتطورة، الواردة في التوصية [b-ITU-T Y.2060]

وتعد شبكات أجهزة الاستشعار الشمولية (USN) من أهم المجالات المتعلقة بإنترنت الأشياء. وهي عبارة عن شبكات من عقد من أجهزة الاستشعار الذكية يمكن أن ينشرها "أي شخص وأي شيء، في أي مكان وأي وقت". ونحن نرى أن تقنيات الأمن المستخدمة لشبكات أجهزة الاستشعار الشمولية يمكن استخدامها في إنترنت الأشياء لتعدُّد القواسم المشتركة بين هذه الشبكات وإنترنت الأشياء بمعنى أنها تتعامل مع أجهزة من قبيل أجهزة الاستشعار والتفعيل. وفيما يخص أمن شبكات أجهزة الاستشعار الشمولية، فقد سبق أن نُشرت بشأنها توصيات مثل إطار الأمن [b-ITU-T X.1311] والمبادئ التوجيهية لأمن البرمجيات الوسيطة [b-ITU-T X.1312] ومتطلبات الأمن لتسيير شبكات أجهزة الاستشعار اللاسلكية [b-ITU-T X.1313]. ولكن لم يتم البحث في وضع توصية بشأن تقنيات حماية سرية البيانات وسلامتها تضمن أمن طبقة الأجهزة في شبكات أجهزة الاستشعار الشمولية. وبالتالي، يُعتبر أمن طبقة الأجهزة حلقة مفقودة في كل من شبكات أجهزة الاستشعار الشمولية وإنترنت الأشياء؛ ولذا، ينبغي التمحص في هذا المجال والتناقش بشأنه لأغراض التقييس في المستقبل.

ومن جهة أخرى، وفي بعض بيئات إنترنت الأشياء، ولا سيما أجهزة إنترنت الأشياء مثل أجهزة الاستشعار والتفعيل التي يمكن استخدامها في أنظمة التحكم الصناعية، هناك شرط يتمثل في المعالجة في الوقت الفعلي حيث تعالَج المهام في فترة زمنية محددة. ومن أجل ضمان حماية سرية البيانات وسلامتها يجوز اتخاذ تدبير مضاد من أبسط التدابير المضادة وهو استخدام خوارزميات لتجفير/استيقان البيانات. وتتمثل المشكلة في الخوارزميات القياسية لتجفير/استيقان البيانات في إمكانية عدم تحقيق هذا الشرط. وتكمن المشكلة الأخرى في دمج مستويات أمنية مختلفة: بمعنى أدق من أجل البيانات الموجودة في رزمة اتصال تتطلب، نظراً لاختلاف موقعها، مستويات مختلفة من الأمن من حيث الأهمية والنتائج المنشودة. ومن هنا، فإن تجفير البيانات الموجودة في موقع يدل على مستوى أمني منخفض هو عبارة عن زيادة في المعالجة لا ضرورة لها.

وكما ذُكر أعلاه، يتعيّن لتحقيق أمن بيئات إنترنت الأشياء، ولا سيما أجهزة إنترنت الأشياء، إيجاد تطبيق جديد لخوارزميات تجفير/استيقان البيانات يفي بشرط المعالجة في الوقت الفعلي ويتضمن مستويات أمنية مختلفة.

ولذلك، لا بد من اللجوء إلى التجفير ببيانات قناع مصاحبة لا يجفر إلا البيانات الموجودة في رزمة اتصال ما إذا اتسمت بمستوى أمني عال. وتُستخدم بيانات القناع المصاحبة للإشارة إلى مستوى أمن البيانات في كل موقع داخل أي رزمة من رزم الاتصال.

التوصية ITU-T X.1362

إجراء تجفير بسيط من أجل بيئات إنترنت الأشياء

1 مجال التطبيق

تنص هذه التوصية على إجراء تجفير لتحقيق أمن أجهزة إنترنت الأشياء. ويُعتزم إجراء هذا التجفير في بيئات إنترنت الأشياء، ولا سيما أجهزة إنترنت الأشياء التي تتسم بقدرات اتصال إلزامية وقدرات اختيارية للاستشعار والتفعيل وتخزين البيانات ومعالجتها. وتوصف هذه التوصية التجفير ببيانات القناع المصاحب (EAMD) من أجل بيئات إنترنت الأشياء. وتصف التجفير EAMD وكيف أنه يوفر مجموعة من الخدمات الأمنية للحركة التي تستخدم التجفير EAMD. وترد أيضاً في الملحق A أمثلة عملية عن ذلك.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع للمراجعة فإن على جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة من التوصيات والمراجع الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[IETF RFC 4303] IETF RFC 4303 (2005), *IP Encapsulating Security Payload (ESP)*

[IETF RFC 7296] IETF RFC 7296 (2014), *Internet Key Exchange Protocol Version 2 (IKEv2).*

[IETF RFC 7321] IETF RFC 7321 (2014), *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH).*

[ISO/IEC 10116] ISO/IEC 10116:2006, *Information technology – Security techniques –Modes of operation for an n-bit block cipher.*

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 المفعل (actuator) [b-ITU-T Y.4109]: جهاز يقوم بإجراءات فيزيائية بسبب إشارة دخل.

ملاحظة – من الأمثلة على ذلك، يمكن للمفعل أن يعمل على تدفق غاز أو سائل أو توزيع الكهرباء أو عبر عملية ميكانيكية. ومن أمثلة هذه المفعلات مخففات الأنوار والمرحلات. وقرار تنشيط المفعل قد يأتي من تطبيق من تطبيقات إدارة التغييرات (MOC) أو من الإنسان أو من أجهزة MOC وبوابات.

2.1.3 الحمولة النافعة الأمنية المغلّفة (encapsulating security payload) (ESP) [IETF RFC 4303]: بروتوكول أمني لبروتوكول الإنترنت (IPsec) يستخدم لتوفير السرية، والاستيقان من مصدر البيانات، والسلامة بدون توصيل، خدمة منع إعادة التشغيل (وهي شكل من أشكال السلامة الجزئية للتتابع)، وسرية تدفق الحركة (المحدودة). وتعتمد مجموعة الخدمات الموفرة على الخيارات التي تجرى عند استحداث رابطة الأمن (SA) وعلى موقع التنفيذ في طبولوجيا الشبكة.

3.1.3 مؤشر معلمات الأمن (security parameters index) (SPI) [b-IETF RFC 4301]: قيمة عشوائية من 32 بتة يستخدمها مستقبل لتحديد رابطة الأمن التي ينبغي أن تلتزم بها أي رزمة واردة.

4.1.3 البيانات المستشعرة (sensed data) [b-ITU-T F.4104]: بيانات تستشعر بجهاز استشعار موصول بعقدة أجهزة استشعار معينة.

5.1.3 جهاز الاستشعار (sensor) [b-ITU-T Y.4105]: جهاز إلكتروني يستشعر ظرفاً مادياً أو مركباً كيميائياً ويخرج إشارة كهربائية تتناسب مع الخاصية المرصودة.

6.1.3 رقم التتابع (sequence number) [IETF RFC 4303]: حقل من عدد غير جبري مكون من 32 بتة يحتوي على قيمة عداد تزداد برقم واحد مع كل رزمة مرسلة، أي رقم تتابع لكل رزمة من رزمات رابطة الأمن (SA).

2.3 مصطلحات معرفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 وحدة التحكم القابلة للبرمجة (programmable controller): جهاز إلكتروني للتحكم بالمفعلات استناداً إلى بيانات مستشعرة بواسطة أجهزة استشعار.

2.2.3 رابطة الأمن بقناع (security association with mask) (SAM): مجموعة من المعلمات المخصصة لبروتوكول الأمن. وتحدد الرابطة SAM الخدمات والآليات اللازمة لحماية الحركة بإجراء التجفير ببيانات قناع مصاحب (EAMD). ويشار إلى الرابطة SAM بالبروتوكول المرتبط بها، بحسب طبقات البروتوكول مثل طبقة النقل أو طبقة بروتوكول الإنترنت (IP). ويمكن أن تدرج ضمن هذه المعلمات معرفات هوية الخوارزميات، والأساليب، ومعرفات هوية الطبقات التي يطبق عليها التجفير EAMD، ومفاتيح التشفير.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

AES معيار تجفير متقدم *(Advanced Encryption Standard)*

CBC تسلسل فدرات التجفير *(Cipher Block Chaining)*

CMAC شفرة الاستيقان من الرسائل القائمة على التجفير *(Cipher-based Message Authentication Code)*

EAMD التجفير ببيانات قناع مصاحب *(Encryption with Associated Mask Data)*

EAMDSP الحمولة النافعة الأمنية القائمة على التجفير ببيانات قناع مصاحب *(EAMD Security Payload)*

ESP الحمولة النافعة الأمنية المغلّفة *(Encapsulating Security Payload)*

ICS نظام التحكم الصناعي *(Industrial Control System)*

IP بروتوكول الإنترنت *(Internet Protocol)*

IPSec أمن بروتوكول الإنترنت *(IP Security)*

IoT إنترنت الأشياء *(Internet of Things)*

IV متجه تدميث *(Initialization Vector)*

MAC شفرة الاستيقان من الرسائل *(Message Authentication Code)*

SA رابطة الأمن *(Security Association)*

SAM رابطة الأمن بقناع *(Security Association with Mask)*

SAMD قاعدة بيانات روابط الأمن بقناع *(SAM Database)*

SPI مؤشر معلمات الأمن *(Security Parameters Index)*

TCP بروتوكول التحكم في الإرسال *(Transmission Control Protocol)*

UDP بروتوكول مخطط بيانات المستخدم *(User Datagram Protocol)*

USN شبكات أجهزة الاستشعار الشمولية *(Ubiquitous Sensor Networks)*

XOR عملية الجمع المنطقية الحصرية *(Exclusive OR)*

5 الاصطلاحات

لا يوجد.

6 مقدمة للتجفير ببيانات القناع المصاحب (EAMD)

1.6 مواصفة إجراء التجفير EAMD

توجد مجموعة كبيرة من التهديدات الأمنية المحيطة ببيئات إنترنت الأشياء (IoT) [b-ZT]. وتركز هذه التوصية على التهديدات التالية:

1) الهجمات عن طريق انتحال الهويّة، التي تعترض بيانات سليمة أو تزيف بيانات غير سليمة، بما يؤدي إلى الكشف عن معلومات أو العبث بها.

2) الهجمات عن طريق التنصت، التي تلتقط الرزم من شبكة تبثها حواسيب الآخرين والتي تقرأ محتوى البيانات بحثاً عن أي معلومات سرية.

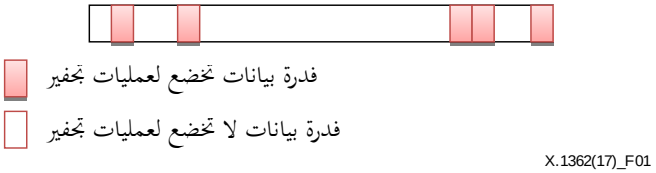
3) الهجمات المتحايلة، التي تتنكر في شكل مكون سليم للحصول على بيانات أو العبث بمعلومات.

وللتخفيف من حدة هذه التهديدات على بيئات إنترنت الأشياء، ولا سيما أجهزة إنترنت الأشياء، توصف هذه التوصية التجفير (EAMD) الذي يقوم بعمليات تجفير جزئية على رزم اتصالات خالصة مرسلة بين جهازين. وتشمل عمليات التجفير أعمال التجفير/فك التجفير، وتوليد شفرة الاستيقان من الرسائل (MAC)/التحقق منها، والتجفير المستيقن منه. ولا تدخل خوارزميات التجفير المستخدمة في التجفير ببيانات القناع المصاحب في نطاق هذه التوصية، بيد أن المعايير [b-ISO/IEC 9797] و[b-ISO/IEC 18033] و[b-ISO/IEC 19772] تعد مراجع جيدة لخوارزميات التجفير، والخوارزميات المتعلقة بشفرة الاستيقان من الرسائل، وخوارزميات التجفير المستيقن منه، على التوالي.

ويرجى ملاحظة أن البنية الموصوفة في هذا النص يمكن اعتبارها بروتوكولاً يستعمل التجفير–ثم–شفرة الاستيقان من الرسائل [b-ASIACRYPT] و[b-EUROCRYPT].

وفي رزمة الاتصال، يطلق على فدرات البيانات التي تخضع لعمليات التجفير اسم القناع.

ويفترض أن يكون المرسل على علم بخوارزمية التجفير، والمفتاح، ومتجه التدميث، والقناع من أجل تحقيق اتصال مؤمن بالتجفير EAMD، ويفترض أيضاً أن يكون المرسل والمستقبل على علم بمعرّف هوية الخوارزمية وبالمفتاح الخاص بالآخر. وفي ظل هذا الشرط، يتم الاتصال المؤمن بالتجفير EAMD من خلال الحصول على المعلومات لتجفيرها بالتجفير EAMD، على جانب المرسل، وتقديم معلومات التجفير إلى المستقبل. ويوضح الشكل 1 مجمل عملية التجفير EAMD.



الشكل 1 – رزمة اتصال مرسلة باستخدام التجفير EAMD

في أي عملية اتصال مؤمن بالتجفير EAMD، تجرى عملية معالجة البيانات الصادرة كالتالي:

1) إضافة تحشية ضرورية للتجفير.

2) استخلاص البيانات من أجل تجفيرها باستخدام قناع للتجفير، ونقل نسخة منها إلى الدارئ كي تستخدم للحسابات المؤقتة.

3) تجفير النتيجة في الدارئ باستخدام المفتاح وخوارزمية التجفير وأي بيانات مطلوبة.

4) استبدال النتيجة في الرزمة باستخدام القناع.

5) إدراج النتيجة في حقل الحمولة النافعة.

وفي حالة اختيار السلامة، تمر عملية المعالجة بالمراحل التالية:[1]

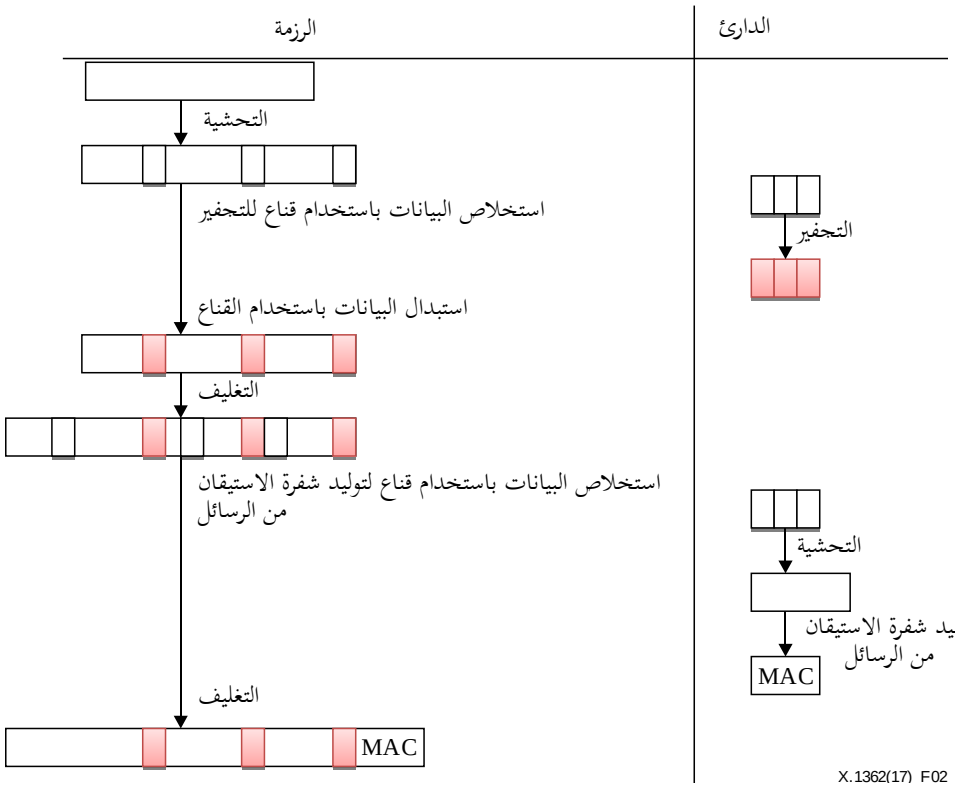
6) استخلاص البيانات لتوليد شفرة الاستيقان من الرسائل باستخدام قناع لتوليد هذه الشفرة، ونقل نسخة من البيانات إلى الدارئ.

7) إضافة تحشية ضرورية لتوليد شفرة الاستيقان من الرسائل.

8) توليد شفرة الاستيقان من الرسائل على النتيجة في الدارئ.

9) إضافة شفرة الاستيقان من الرسائل إلى الرزمة.

ويوضح الشكل 2 عملية معالجة البيانات الصادرة.



الشكل 2 – توليد رزمة باستخدام التجفير ببيانات القناع المصاحب خلال معالجة البيانات الصادرة

[1] ينبغي ضمان السرّية مع الاستيقان في حال استعمال تجفير مع بيانات قناع مصاحب ملتزمة بالبروتوكول IPsec.

في عملية اتصال مؤمن بالتجفير EAMD، تجرى عملية معالجة البيانات الصادرة كالتالي:

في حالة اختيار السلامة، تجرى الخطوات من 1 إلى 3 أدناه[1]:

1) استخلاص البيانات من الرزمة بدون شفرة الاستيقان من الرسائل، إلى الدارئ وفقاً للقناع الخاص بتوليد شفرة الاستيقان من الرسائل.

2) إضافة تحشية ضرورية لتوليد شفرة الاستيقان من الرسائل.

3) احتساب شفرة الاستيقان من الرسائل على البيانات التي جرى تحشيتها، باستخدام خوارزمية السلامة المحددة، والتحقق من تماثلها مع شفرة الاستيقان من الرسائل التي تحملها الرزمة. وإذا كانت الشفرة المحسوبة مطابقة للشفرة الواردة، تكون الرزمة سليمة ويتم قبولها. وإذا فشل الاختبار، يجب أن ينبذ المستقبل الرزمة الواردة باعتبارها غير صالحة.

4) إزالة الرأسية من الرزمة.

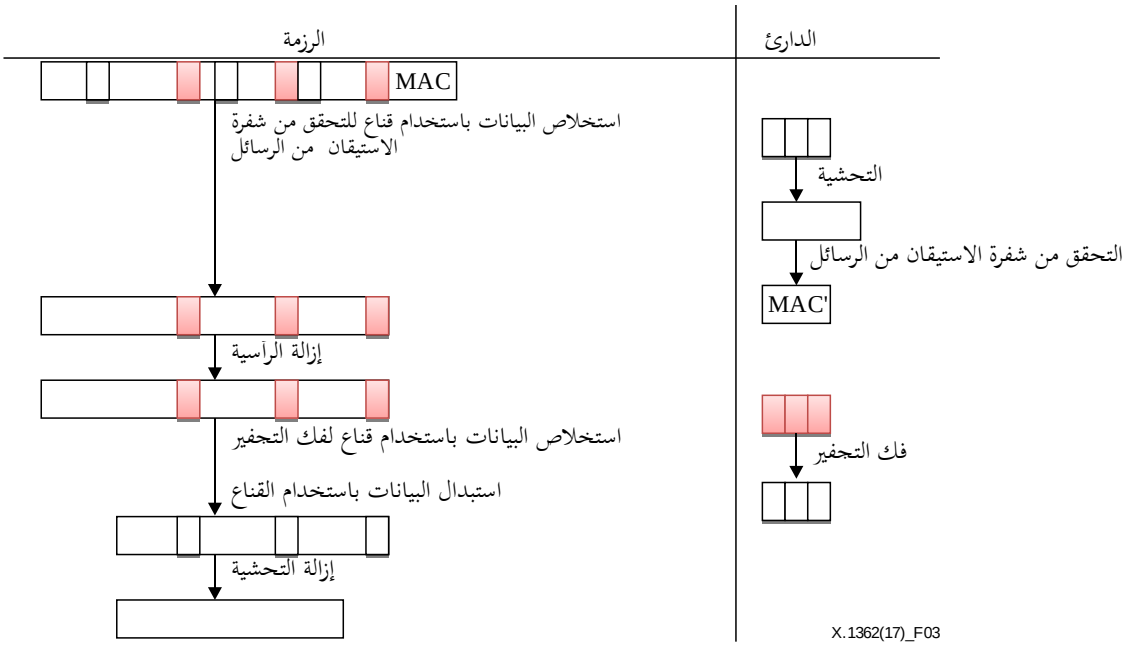
5) استخلاص البيانات من النتيجة إلى الدارئ وفقاً للقناع الخاص بفك التجفير.

6) فك تجفير النتيجة المستخلصة في الدارئ.

7) استبدال النتيجة في الدارئ إلى داخل الرزمة باستخدام القناع الخاص بفك التجفير.

8) إزالة تحشية التجفير من الرزمة.

ويبين الشكل 3 عملية معالجة البيانات الواردة.



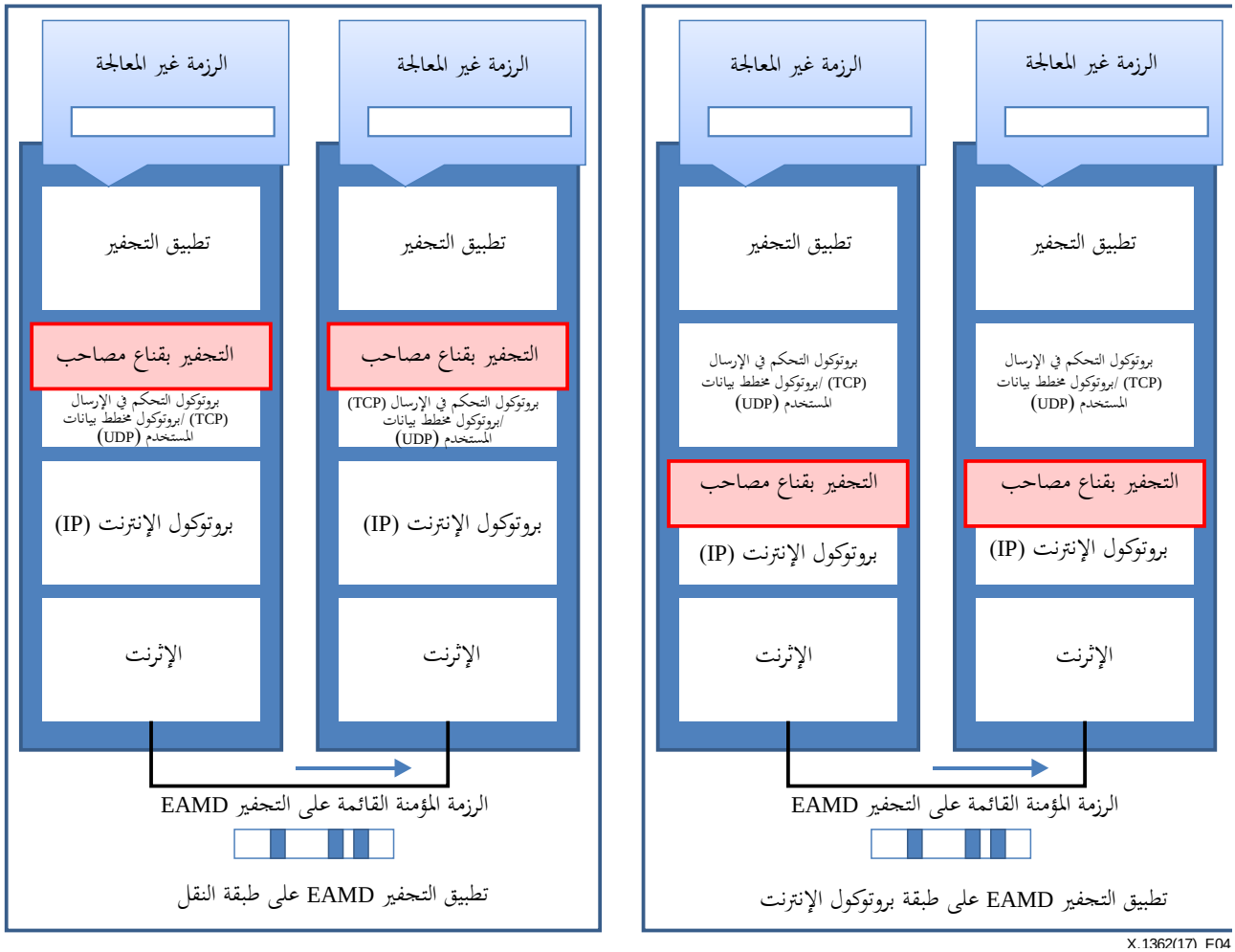
الشكل 3 – توليد رزمة باستخدام التجفير ببيانات القناع المصاحب أثناء عملية معالجة البيانات الواردة

2.6 قناع لاستخلاص البيانات المستهدفة من أجل إجراء تجفير ببيانات قناع مصاحب

في عمليات التجفير ببيانات القناع المصاحب، يُستخلص الهدف من دخل الفدرة في الخوارزمية ذات الصلة عن طريق تقسيم الرزمة إلى حجم الفدرة التي تستخدم خوارزمية التجفير وفقاً لمعلمات القناع.

7 التجفير ببيانات القناع المصاحب

تصف هذه الفقرة كيفية توفير مجموعة من الخدمات الأمنية للحركة في كل طبقة من الطبقات. وتصف هذه التوصية عملية اتصال مؤمنة باستخدام التجفير EAMD المستند إلى حمولة نافعة أمنية لهذا التجفير (EAMDSP). ويعرض الشكل 4 لمحة عامة عن عملية الاتصال هذه. وفيما يلي وصف مفصل لتدفق الاتصال الآمن القائم على التجفير EAMD:



الشكل 4 – لمحة عن عملية اتصال تستخدم التجفير ببيانات القناع المصاحب

1.7 رابطة الأمن بقناع (SAM)

تعرَّف رابطة الأمن بقناع (SAM) على أنها مجموعة من المعلمات المخصصة لبروتوكولات الأمن. وتحدد الرابطة الخدمات والآليات اللازمة لحماية الحركة بإجراء التجفير EAMD. ويشار إلى الرابطة بالبروتوكول المرتبط بها، وبحسب طبقات البروتوكول مثل طبقة النقل أو طبقة بروتوكول الإنترنت (IP). ويمكن أن تدرج ضمن المعلمات معرفات هوية الخوارزميات، والأساليب، ومعرّف هوية الطبقة التي يجرى فيها التجفير EAMD، والمعلمات الخاصة بالطبقات مثل عنوان بروتوكول الإنترنت ومنفذه، ومفاتيح التجفير. وتتضمن الرابطة SAM معلمات CryptCtx بوصفها مجموعة من معلمات التجفير. وترد بيانات الحالة المرتبطة بالرابطة SAM في قاعدة بيانات الروابط SAM (SAMD).

وفيما يخص هذا النسق، يرد في الجدول 1 وصف لكل معلمة من المعلمات الإلزامية.

الجدول 1 – المعلمات الإلزامية في معلمات CryptCtx في رابطة الأمن (SA)

الرقم	المعلمة	المعنى
1	encAlg	معرف هوية خوارزمية التجفير
2	encKey	مفتاح التجفير
3	encMask	الحيز الذي يجري تجفيره

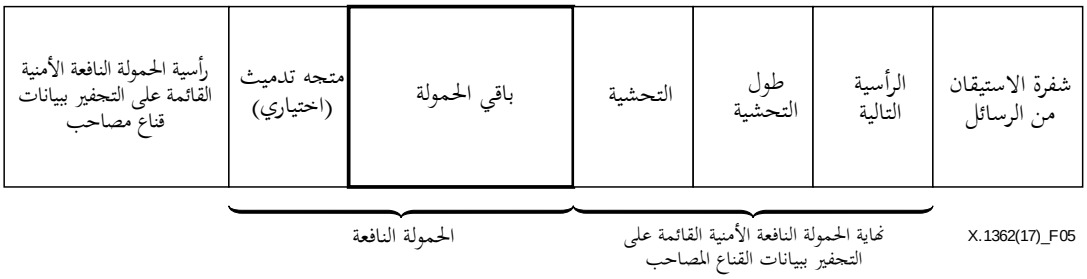
ويرد في الجدول 2 وصف لكل معلمة من المعلمات الاختيارية.

الجدول 2 – المعلمات الاختيارية في معلمات CryptCtx في رابطة الأمن

الرقم	المعلمة	المعنى
1	encRoundKey	مفتاح دورة للتجفير
2	decRoundKey	مفتاح دورة لفك التجفير
3	encIV	متجه تدميث (IV) للتجفير
4	macRoundKey	مفتاح دورة لشفرة الاستيقان من الرسائل
5	macK1	مفتاح فرعي للمفتاح K1 لشفرة الاستيقان من الرسائل القائمة على التجفير (CMAC)
6	macK2	مفتاح فرعي للمفتاح K2 لشفرة الاستيقان من الرسائل القائمة على التجفير
7	KeyStream	أرقام عشوائية مولَّدة مسبقاً
8	KeyStreamHead	مؤشر لرأسية الأرقام العشوائية غير المستخدمة
9	KeyStreamTail	مؤشر لذيل الأرقام العشوائية غير المستخدمة
10	EncIVTail	متجه تدميث لتوليد أرقام عشوائية
11	macAlg	معرف هوية خوارزمية شفرة الاستيقان من الرسائل
12	macKey	مفتاح شفرة الاستيقان من الرسائل
13	macMask	حيز يستخدم لتولد خوارزمية معينة شفرة الاستيقان من الرسائل

2.7 نسق رزمة الحمولة النافعة الأمنية القائمة على التجفير ببيانات القناع المصاحب (EAMDSP)

يعرض الشكل 5 نسقاً لرزمة حمولة نافعة أمنية قائمة على التجفير EAMD. وتبدأ الرزمة برأسية الحمولة EAMDSP، متغيرة الطول. ويلي هذا الحقل بياناتُ الحمولة النافعة التي تتضمن بنية فرعية تتوقف على اختيار خوارزمية التجفير وأسلوبه. ويلي بيانات الحمولة حقلا التحشية وطول التحشية ثم حقل الرأسية التالية. وتنتهي الرزمة بالحقل الاختياري لشفرة الاستيقان من الرسائل. وتتألف نهاية الحمولة EAMDSP من حقول التحشية وطول التحشية والرأسية التالية.



الشكل 5 – نسق رزمة الحمولة النافعة الأمنية القائمة على التجفير ببيانات قناع مصاحب (EAMDSP)

وتتألف نهاية الحمولة الأمنية (المرسلة) القائمة على التجفير ببيانات قناع مصاحب من حقول التحشية وطول التحشية والرأسية التالية. ويُدرَج في احتساب السلامة بيانات ضمنية إضافية (غير مرسلة) لنهاية الحمولة النافعة الأمنية القائمة على التجفير ببيانات قناع مصاحب.

وعند اختيار خدمة السلامة، يتضمن احتساب السلامة رأسية الحمولة EAMDSP، وبيانات الحمولة النافعة، ونهاية الحمولة الأمنية EAMDSP. وعند اختيار خدمة السرية، يتألف نص التجفير من بيانات الحمولة النافعة (فيما عدا بيانات التزامن التجفيري التي قد يتضمنها) ونهاية الحمولة EAMDSP.

وتورد الفقرات التالية وصفاً للحقول التي يتضمنها نسق الرأسية. وصفة "اختياري" تعني أن الحقل سيحذف إن لم يستعمل الخيار المعني، أي أنه سيُحذَف من الرزمة المرسلة ومن الرزمة المنسَّقة لاحتساب شفرة الاستيقان من الرسائل. وتحدد الخيارات المستعملة في إطار إنشاء الرابطة (SAM). وبالتالي، فإن نسق رزم الحمولة EAMDSP لرابطة SAM هو نسق ثابت طوال مدة الرابطة. وعلى النقيض من ذلك، فإن الحقول "الإلزامية" تكون موجودة دائماً في نسق رزم الحمولة EAMDSP لجميع الروابط SAM.

1.2.7 بيانات الحمولة النافعة

بيانات الحمولة النافعة عبارة عن حقل متغير الطول يتضمن بيانات (من الرزمة الأصلية) يرد وصفها بواسطة حقل الرأسية التالية. ويُعتبر حقل بيانات الحمولة النافعة حقلاً إلزامياً ويحدَّد من حيث الطول بعدد صحيح من البايتات. وإذا تطلبت الخوارزمية المستخدمة لتجفير الحمولة النافعة بيانات للتزامن التجفيري، مثل متجه التدميث (IV)، فإن هذه البيانات تحمل صراحة في حقل الحمولة النافعة، ولكن لا يستدعي ذلك اعتبار هذا الحقل حقلاً مستقلاً في الحمولة EAMDSP، بمعنى أن إرسال متجه IV صريح يكون غير مرئي بالنسبة للحمولة EAMDSP.

2.2.7 التحشية (للتجفير)

إذا استُخدمت خوارزمية تجفير تتطلب أن يكون النص الخالص أحد مضاعفات عدد معين من البايتات، مثلاً حجم فدرة التجفير، فإن حقل التحشية يستخدم لملء النص الخالص (الذي يتألف من حقول بيانات الحمولة النافعة، والتحشية، وطول التحشية، والرأسية التالية) حسب الحجم الذي تقتضيه الخوارزمية.

3.2.7 طول التحشية

يشير حقل طول التحشية إلى عدد بايتات التحشية التي تسبقه مباشرة في حقل التحشية. ويُعتبر حقل طول التحشية إلزامياً.

4.2.7 الرأسية التالية

يُعتبر حقل الرأسية التالية إلزامياً. ويحدد هذا الحقل نوع البيانات الموجودة في حقل بيانات الحمولة النافعة، مثل رأسية للطبقة التالية والبيانات.

5.2.7 شفرة الاستيقان من الرسائل

شفرة الاستيقان من الرسائل عبارة عن حقل متغير الطول يحتسب على البيانات التي يشير إليها القناع لتوفير الحماية من منظور السلامة. وتدرَج في احتساب شفرة الاستيقان من الرسائل الحقول الضمنية لنهاية الحمولة EAMDSP مثل التحشية لتوليد شفرة الاستيقان من الرسائل. وحقل شفرة الاستيقان من الرسائل اختياري. ولا يوجد إلا عند اختيار خدمة السلامة، وتوفره إما خوارزمية مستقلة للسلامة أو خوارزمية بأسلوب مدمج تستخدم شفرة الاستيقان من الرسائل. وتحدد خوارزمية السلامة التي اختيرت طول الحقل

وترتبط برابطة SAM. وتحدد مواصفة خوارزمية السلامة طول شفرة الاستيقان من الرسائل، وقواعد المقارنة، وخطوات المعالجة من أجل التحقق.

3.7 معالجة الرزمة

1.3.7 معالجة رزمة البيانات الصادرة

تجرى معالجة البيانات الصادرة التي تستخدم التجفير EAMD كالتالي:

1) البحث عن الرابطة SAM:

قبل تطبيق الحمولة EAMDSP على رزمة صادرة، فإن الرابطة SAM ذات الصلة التي تتطلب معالجة هذه الحمولة تحدد بناء على بعض المعلومات مثل معرف هوية الطبقة والمعلمة الخاصة بالطبقات مثل عنوان بروتوكول الإنترنت أو رقم منفذه في الرزمة. وتشير الرابطة SAM إلى المفتاح والأقنعة المتعلقين بالتجفير وبتوليد شفرة الاستيقان من الرسائل.

2) تحويل البيانات باستخدام التجفير EAMD الذي يرد وصفه في الفقرة 1.6.

3) إرسال الرزمة:

تضاف الرأسية الأصلية إلى الرزمة المحمولة بالتجفير EAMD، وترسل الرزمة الناجمة عن ذلك إلى الشبكة.

2.3.7 معالجة رزمة البيانات الواردة

تجرى معالجة البيانات الواردة التي تستخدم التجفير EAMD كالتالي:

1) البحث عن الرابطة SAM:

عند استقبال رزمة تتضمن رأسية حمولة EAMDSP، يحدّد المستقبل الرابطة SAM الملائمة من خلال البحث في قاعدة بيانات الروابط SAM (SAMD). ويشير مدخل SAM في قاعدة البيانات هذه أيضاً إلى الطبقة التي يطبَّق عليها التجفير EAMD خلال معالجة البيانات الصادرة والمعلمة الخاصة بالطبقة مثل عنوان بروتوكول الإنترنت أو رقم منفذه في الرزمة، وما إذا كان ينبغي لحقل شفرة الاستيقان من الرسائل أن يكون موجوداً. وإضافةً إلى ذلك، يحدّد مدخل قاعدة البيانات هذه الخوارزميات والمفاتيح التي ينبغي استخدامها لفك التجفير والتحقق من شفرة الاستيقان من الرسائل (إن وجدت).

2) التحقق من بيانات رأسية الحمولة EAMDSP:

يمكن التحقق من بيانات رأسية الحمولة EAMDSP باستخدام بعض القيم في رأسية هذه الحمولة، ويتم ذلك قبل التحقق من السلامة وفك التجفير. وإذا فشلت عملية التحقق هذه، تنبذ الرزمة.

ويرد في الفقرة 1.6 وصف تحويل البيانات باستخدام التجفير EAMD.

8 التجفير ببيانات القناع المصاحب باستخدام خوارزمية تجفير مستيقن منها

1.8 رابطة الأمن بقناع (SAM)

في حالة استخدام التجفير EAMD لخوارزمية تجفير مستيقن منها، تحدد رابطة الأمن بقناع كما هي معرفة في الفقرة 1.7.

وفيما يخص هذا النسق، يرد وصف كل معلمة من المعلمات الإلزامية في الجدول 3.

الجدول 3 – المعلمات الإلزامية في معلمات CryptCtx في رابطة الأمن (SA)

الرقم	المعلم	المعنى
1	auencAlg	معرف هوية خوارزمية التجفير المستيقن منها
2	auencKey	مفتاح التجفير المستيقن منه
3	encMask	الحيز الذي يجري تجفيره

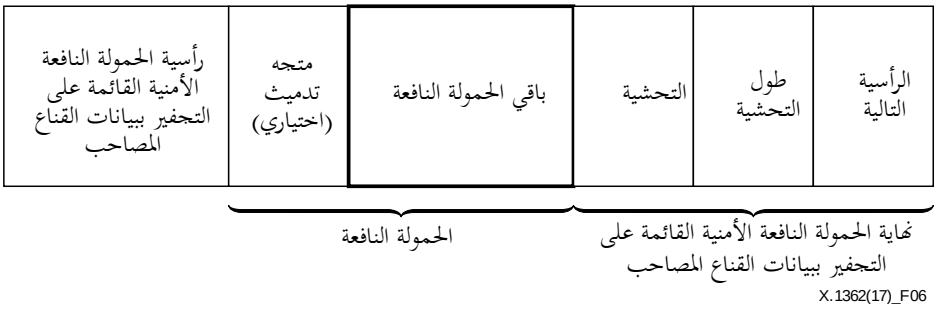
ويرد في الجدول 4 وصف لكل معلمة من المعلمات الاختيارية.

الجدول 4– المعلمات الاختيارية في معلمات CryptCtx في رابطة الأمن (SA)

الرقم	المعلمة	المعنى
1	auencRoundKey	مفتاح دورة للتجفير المستيقن منه
2	audecRoundKey	مفتاح دورة لفك التجفير
3	IV	متجه تدميث للتجفير المستيقن منه
4	Nonce	مفتاح دورة للتجفير المستيقن منه

2.8 نسق رزمة الحمولة النافعة الأمنية القائمة على التجفير ببيانات القناع المصاحب (EAMDSP)

يعرض الشكل 6 نسقاً لرزمة حمولة نافعة أمنية قائمة على التجفير ببيانات قناع مصاحب. وتبدأ الرزمة برأسية الحمولة EAMDSP متغيرة الطول. ويلي هذا الحقل بياناتُ الحمولة النافعة التي تتضمن بنية فرعية تتوقف على اختيار خوارزمية التجفير وأسلوبه. وبعد بيانات الحمولة يأتي حقلا التحشية وطول التحشية ثم حقل الرأسية التالية. وتتألف نهاية الحمولة EAMDSP من حقول التحشية وطول التحشية والرأسية التالية.



الشكل 6 – نسق رزمة الحمولة EAMDSP (للتجفير المستيقن منه) من دون شفرة للاستيقان من الرسائل

وتتألف نهاية الحمولة EAMDSP (المرسلة) من حقول التحشية وطول التحشية والرأسية التالية. ويُدرَج في احتساب السلامة بيانات ضمنية إضافية (لا ترسل) عن نهاية الحمولة EAMDSP.

وفي حالة اختيار خدمة السلامة، يتضمن احتساب السلامة رأسية الحمولة EAMDSP، وبيانات الحمولة النافعة، ونهاية الحمولة EAMDSP. وعند اختيار خدمة السرية، يتألف نص التجفير من بيانات الحمولة النافعة (فيما عدا بيانات التزامن التجفيري التي قد تتضمنها) ونهاية الحمولة الأمنية EAMDSP.

وتورد الفقرات التالية وصفاً للحقول التي يتضمنها نسق الرأسية. وصفة "اختياري" تعني حذف الحقل إن لم يحدد الخيار المعني، أي يحذف من الرزمة المرسلة ومن الرزمة المنسَّقة لاحتساب شفرة الاستيقان من الرسائل. وتحدد الخيارات المستخدمة في إطار إنشاء الرابطة SAM. وبالتالي، فإن نسق رزم الحمولة EAMDSP لرابطة SAM معيّنة هو نسق ثابت طوال مدة الرابطة. وعلى النقيض من ذلك، فإن الحقول "الإلزامية" تكون موجودة دائماً في نسق رزم الحمولة EAMDSP في جميع الرابطات SAM.

1.2.8 بيانات الحمولة النافعة

بيانات الحمولة عبارة عن حقل متغير الطول يتضمن بيانات (من الرزمة الأصلية) توصف بواسطة حقل الرأسية التالية. ويُعتبر حقل بيانات الحمولة حقلاً إلزامياً ويحدَّد من حيث الطول بعدد صحيح من البايتات.

ويمكن التعبير عن نسق رزمة الحمولة النافعة للأمن المغلّفة بالطريقة التالية: ESP = SPI || Sequence Number || IV || C، حيث يشكل C نص التجفير الذي تنتجه خوارزمية التجفير المستيقن منها. وفي هذه الحالة، يتضمن النص التجفير C وَسْم الاستيقان.

2.2.8 التحشية (للتجفير المستيقن منه)

إذا استُخدمت خوارزمية تجفير مستيقن منها تتطلب أن يكون النص غير المعالج أحد مضاعفات عدد معين من البايتات، مثلاً حجم فدرة التجفير، يستخدم حقل التحشية لملء هذا النص (الذي يتألف من حقول بيانات الحمولة النافعة، والتحشية، وطول التحشية، والرأسية التالية) حسب الحجم الذي تقتضيه الخوارزمية.

3.2.8 طول التحشية

يشير حقل طول التحشية إلى عدد بايتات التحشية التي تسبقه مباشرة في حقل التحشية. ويُعتبر حقل طول التحشية إلزامياً.

4.2.8 الرأسية التالية

يُعتبر حقل الرأسية التالية إلزامياً. ويحدد هذا الحقل نوع البيانات الموجودة في حقل بيانات الحمولة النافعة مثل رأسية الطبقة التالية والبيانات.

3.8 معالجة الرزمة

1.3.8 معالجة رزمة البيانات الصادرة

تجرى معالجة البيانات الصادرة بالتجفير EAMD كالتالي:

1) البحث عن الرابطة SAM:

قبل تطبيق الحمولة EAMDSP على رزمة صادرة، فإن الرابطة SAM ذات الصلة التي تتطلب معالجة هذه الحمولة تحدّد بناءً على بعض المعلمات مثل معرف هوية الطبقة والمعلمة الخاصة بالطبقة مثل عنوان بروتوكول الإنترنت (IP) أو رقم منفذه في الرزمة. وتشير الرابطة SAM إلى المفتاح والأقنعة المتعلقين بالتجفير المستيقن منه.

2) تحويل البيانات باستخدام أسلوب التجفير EAMD المستيقن منه

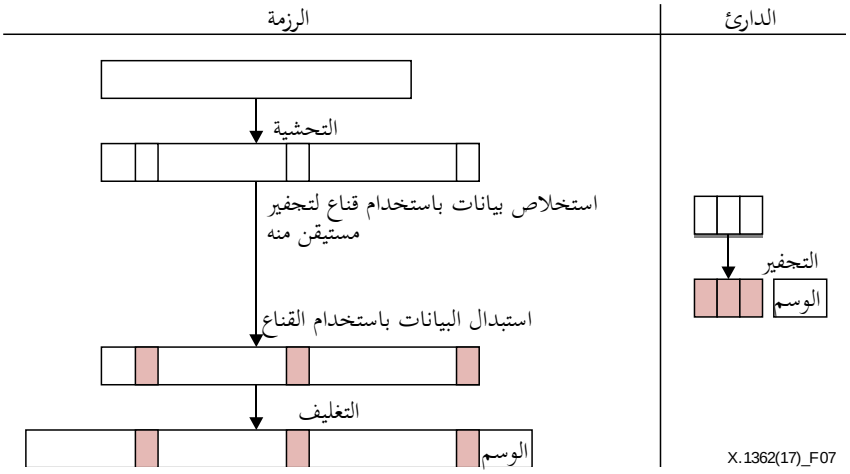
1) إضافة تحشية ضرورية للتجفير.

2) استخلاص بيانات من أجل التجفير باستخدام قناع للتجفير، ونقل نسخة منها إلى الدارئ الذي يستخدم للحسابات المؤقتة.

3) تجفير النتيجة في الدارئ باستخدام المفتاح وخوارزمية التجفير وأي بيانات لازمة.

4) استبدال النص المجفر في الرزمة باستخدام القناع.

5) إضافة وَسْم الاستيقان إلى الرزمة بوصفه شفرة الاستيقان من الرسائل.



الشكل 7 – معالجة رزمة البيانات الصادرة فيما يخص أسلوب التجفير المستيقن منه

3) إرسال الرزمة:

تضاف الرأسية الأصلية إلى الرزمة المحولة بالتجفير EAMD، وترسل الرزمة الناجمة عن ذلك إلى الشبكة.

2.3.8 معالجة رزمة البيانات الواردة

تجرى معالجة البيانات الواردة بالتجفير EAMD كالتالي:

1) البحث عن الرابطة SAM:

عند استقبال رزمة تتضمن رأسية حمولة EAMDSP، يحدد المستقبل الرابطة SAM الملائمة من خلال البحث في قاعدة بيانات الروابط SAM. ويشير المدخل الخاص بالرابطة SAM في قاعدة بيانات الروابط (SAMD) أيضاً إلى الطبقة التي طبق عليها التجفير EAMD خلال معالجة البيانات الصادرة والمعلمة الخاصة بالطبقة مثل عنوان بروتوكول الإنترنت أو رقم منفذه في الرزمة. وإضافة إلى ذلك، يحدد هذا المدخل الخوارزميات والمفاتيح التي ينبغي استخدامها لفك التجفير والتحقق من الوسم.

2) التحقق من بيانات رأسية الحمولة النافعة الأمنية EAMDSP:

يمكن التحقق من بيانات رأسية الحمولة EAMDSP باستخدام بعض القيم في رأسية هذه الحمولة، وذلك قبل التحقق من السلامة وفك التجفير. وإذا فشلت عملية التحقق هذه، تنبذ الرزمة.

3) تحويل البيانات باستخدام أسلوب فك التجفير EAMD المستيقن منه

1) إزالة الرأسية من الرزمة.

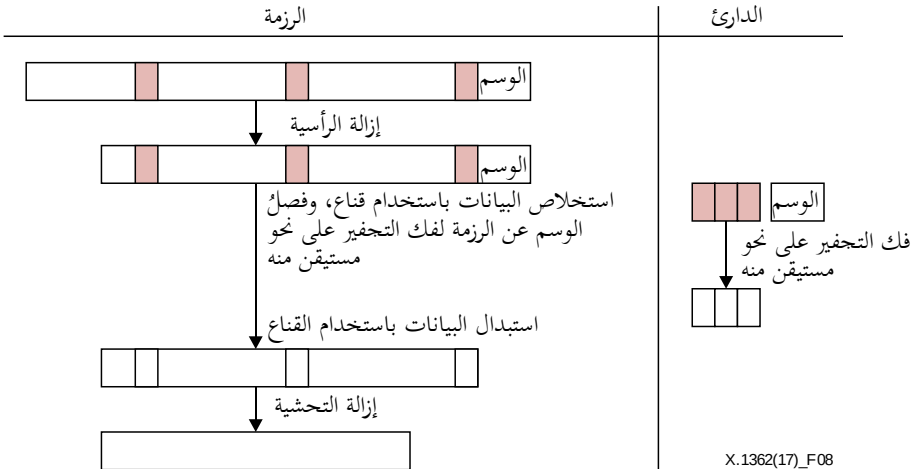
2) استخلاص البيانات لفك التجفير باستخدام القناع الخاص بفك التجفير، ونقل نسخة منها إلى الدارئ الذي يستخدم للحسابات المؤقتة.

3) فصل وَسْم الاستيقان عن الرزمة ونقله إلى الدارئ.

4) فك تجفير النتيجة في الدارئ باستخدام المفتاح وخوارزمية فك التجفير وأي بيانات أخرى لازمة.

5) استبدال نتيجة فك التجفير في الرزمة باستخدام القناع إذا لم يتعذر فك التجفير.

4) إزالة تحشية التجفير من الرزمة.



الشكل 8 – معالجة رزمة البيانات الواردة باتباع أسلوب فك التجفير على نحو مستيقن منه

9 الإرشادات والقيود

1.9 إرشادات بشأن إنشاء رابطة الأمن بقناع

فيما يخص طريقة تقنيع التجفير EAMD، جدير بالإشارة أنه إذا تمكن كيان خبيث من تعديل القناع، فيمكنه أن يضع قيمة للقناع تحول دون تجفير أي من البيانات. وعند تغيير القناع على هذا النحو، فإن بيانات الجهاز ترسل في صورة "صريحة" (أي غير مجفرة). ويمثل هذا الأمر موطن ضعف كبيراً في نظام الأمن.

ومن أجل حل هذه المشكلة، ينبغي تناول المسائل التالية:

1) اتصالات أمن القناع

من أجل استهلال وتحديث مواد الإبراق مثل مفاتيح التشفير، ومتجهات التدميث، ومعلمات الأمن الأخرى، هناك عدد من بروتوكولات إنشاء المفاتيح من قبيل الإصدار الثاني من بروتوكول تبادل مفاتيح الإنترنت (IKEv2) [IETF RFC 7296]، واتفاق المفاتيح، ونقل المفاتيح.

وينبغي التأكد من تدميث القناع وتحديثه بالارتباط مع تدميث وتحديث مواد الإبراق أثناء عملية الاتصال بين الكيانات ذات الصلة باستخدام هذه البروتوكولات. فعلى سبيل المثال، فإنه أثناء عملية الاتصال الخاصة بإنشاء المفتاح، فإن مواد الإبراق المشار إليها أعلاه ينبغي لها أن تتضمن أيضاً القناع من أجل ضمان سلامة وسرية القناع بواسطة خوارزميات التجفير وخوارزميات شفرة الاستيقان من الرسائل، المستخدمة في هذه البروتوكولات.

2) عمليات تخزين أمن القناع

بمجرد وجود القناع في الجهاز، ينبغي التأكد من عدم وجود بروتوكول يتيح لأجهزة أخرى قراءة القناع.

ويمكن اقتراح الوسائل التالية لتحقيق هذا الغرض.

تتمثل الوسيلة الأولى في تصميم نظام مؤمن يخصص مكونات النظام بحيث لا تتصل الأجهزة التي يطبق عليها التجفير EAMD اتصالاً مباشراً بكيان من خارج النظام، رغم اتصال هذا الكيان بمكون بوابة مؤمنة يتسم بقدرة حوسبية عالية.

وتتمثل الطريقة الثانية في حماية الجهاز بواسطة تجهيزات مقاومة للعبث أو بواسطة طريقة التمويه البرمجية التي تستحدث شفرة مموهة يصعب على البشر فهمها.

2.9 إرشادات بشأن الاستخدام الأمثل لمتجهات التدميث والقيم الظرفية

توفر هذه الفقرة إرشادات بشأن الاستخدام الأمثل لمتجهات التدميث (فضلاً عن أساليب تجفير الفدرات والتحشية). ويعتبر الاستخدام غير المناسب لمتجهات التدميث أو التحشية من العيوب الشائعة التي تفسح المجال للقيام بهجمات على البروتوكولات. ومن المرجح جداً أن يكون لمتجه التدميث أو القيمة الظرفية دور حاسم في أمن البروتوكول.

ومن أجل استخدام أسلوب تسلسل فدرات التجفير (CBC) [ISO/IEC 10116] لتجفير يقوم بالجمع بين فدرات النص غير المعالج وفدرات النص المجفر من قبل، ينبغي إجراء الخطوات التالية:

عند استخدام أسلوب تسلسل فدرات التجفير بوصفه الأسلوب المتبع لتجفير الفدرات، ينبغي النظر في ضمان الأمن ضد الهجمات التي تستخدم تحشية الرسائل المجفرة في [b-CBCPADD]. ويتطلب هذا الأسلوب الجمع بين متجه تدميث مع فدرة النص غير المعالج الأول. ولا ينبغي أن يكون متجه التدميث سرياً، ولكن يتعين أن يكون التنبؤ به أمراً متعذراً.

ومن أجل استخدام خوارزمية تجفير مستيقن منه بصورة مؤمنة، ينبغي اتباع الخطوات التالية:

إذا تعذر على تطبيق الوفاءُ بشرط التفرد عند توليد القيم الظرفية، فعليه أن يستخدم قيمة ظرفية يبلغ طولها صفراً. واستخدام الخوارزميات المرتبة عشوائياً أو التي تحافظ على الحالة [b-IETF RFC 5116] هو استخدام مناسب مع هذه التطبيقات. وإلا، فينبغي أن يستخدم التطبيقُ قيمة ظرفية يبلغ طولها اثني عشر أثموناً.

وعند تكرار القيم الظرفية أو متجهات التدميث، تتعرض العديد من المخططات لهجمات عملية تفصح، مثلاً عن حصرية أو (عملية XOR) بين الرزمتين. وبالتالي، يوصى بشدة أن يتم ضمان تفرد متجه التدميث أو القيمة الظرفية.

3.9 قيود استخدام التجفير ببيانات القناع المصاحب (EAMD)

يقيد استخدام التجفير EAMD بشروط الأداء في الوقت الفعلي للنظام.

وتستمثل مزايا التجفير EAMD في النظام عندما يتسم المرسل والمستقبل بمستوى معين من القدرة الحوسبية، أن تكون معمارية وحدة المعالجة المركزية (CPU) من 16 بتة أو 32 بتة مع تردد (مئات الميغاهيرتزات) وذاكرة معقولين، مثلاً.

وجدير بالذكر أن التجفير EAMD قد لا يكون حلاً جيداً للنظم التي تقتضي قيوداً بالنسبة للقدرة لأن استهلاك القدرة نتيجة عملية التخزين المرتبطة بالتجفير EAMD قد يؤدي إلى كثرة المعلومات الإضافية.

وجدير بالذكر أن القناع يتسم بحساسية عالية مثله مثل مفتاح التشفير، كما ذكر أعلاه، وبالتالي، فيمكن تطبيق التجفير EAMD فقط على افتراض أن القناع محمي ومدار بصورة مؤمنة.

الملحق A

الروابط مع البروتوكولات القائمة

(يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

من أجل القيام باتصالات مؤمنة باستخدام التجفير ببيانات القناع المصاحب (EAMD)، يجب أن تكون الطبقة التي يطبق عليها التجفير ثابتة. وهناك عدة طبقات يمكن أن يحدث فيها ذلك منها طبقة النقل وطبقة بروتوكول الإنترنت وغيرهما. ويصف هذا الملحق كيفية ربط التجفير EAMD بالبروتوكولات القائمة. واستخدام التجفير EAMD مع الالتزام بالبروتوكول IPsec يتعين أن يوفر السرية والاستيقان. وينبغي ضمان السرية مع الاستيقان [IETF RFC 7321].

1.A الربط مع بروتوكول الحمولة النافعة الأمنية المغلفة لأمن بروتوكول الإنترنت IETF RFC 4303

1.1.A نسق رابطة الأمن بقناع (SAM)

تحدد رابطة الأمن الخدمات والآليات اللازمة لحماية الحركة بالتجفير EAMD. ويرد في الشكل 1.A وصف للرابطة (SAM) عند تطبيق هذا التجفير على طبقة الشبكة.

```
SecurityAssertion ::= SEQUENCE {
  layerIdentifier OCTET STRING (SIZE(1)),
  SPI             OCTET STRING (SIZE (4)),
  ipAddr          OCTET STRING (SIZE (4)),
  cryptCtx        CryptCtx
}
CryptCtx ::= SEQUENCE {
  encAlg    OCTET STRING (SIZE (4))
  encKey    OCTET STRING (SIZE (keySizeMax)),
  encMask   OCTET STRING (SIZE (maskLength))
}
keySizeMax INTEGER ::= 64
maskLength INTEGER ::= 16
```

الشكل 1.A – نسق رابطة الأمن بقناع (SAM) من أجل طبقة الشبكة

2.1.A نسق الرزمة

يعرض الشكل 2.A مثالاً لنسق رزمة الحمولة EAMD. وتبدأ الرزمة برأسية الحمولة (EAMDSP) متغيرة الطول. ويلي هذا الحقل بياناتُ الحمولة النافعة التي تتضمن بنية فرعية تتوقف على اختيار خوارزمية التجفير وأسلوبه. وبعد بيانات الحمولة يأتي حقلا التحشية وطول التحشية ثم حقل الرأسية التالية. وينهي الرزمة الحقل الاختياري لشفرة الاستيقان من الرسائل. وتتألف نهاية الحمولة EAMDSP من حقول التحشية وطول التحشية والرأسية التالية. ونظراً إلى حجم الحركة الناجمة عن عمليات احتساب شفرة الاستيقان من الرسائل الخاصة بالتجفير EAMD وعن التجفير EAMD، في مثال لنسق آخر، يمكن أن يبلغ طول رقم التتابع 8 بايتات وأن يوضع حقل الرأسية التالية في رأسية الحمولة EAMDSP.

الشكل 2.A – مثال لنسق رزمة الحمولة EAMDSP لربطها ببروتوكول الحمولة الأمنية المغلفة لأمن بروتوكول الإنترنت

1) مؤشر معلمات الأمن (SPI):

مؤشر معلمات الأمن عبارة عن قيمة عشوائية من 32 بتة يستخدمها أي مستقبل لتحديد رابطة الأمن التي ترتبط بها الرزمات الواردة. وحقل المؤشر SPI إلزامي. ويُحمل المؤشر في البروتوكول ليتسنى للنظام المستقبل اختيار شفرة للاستيقان من الرسائل تعالج ضمنها الرزمة الواردة.

2) رقم التتابع:

يحتوي هذا الحقل غير الجبري المكون من 32 بتة أو 64 بتة على قيمة عداد تزداد برقم واحد مع كل رزمة ترسل، أي رقم تتابع لكل رزمة من رزم رابطات الأمن، أو بدلاً من ذلك، قيمة تولَّد استناداً إلى قاعدة لا لبس فيها.

3) بيانات الحمولة النافعة:

بيانات الحمولة النافعة عبارة عن حقل متغير الطول يتضمن بيانات (من الرزمة الأصلية) يصفها حقل الرأسية التالية. ويُعتبر حقل بيانات الحمولة النافعة إلزامياً ويحدَّد من حيث الطول بعدد صحيح من البايتات. وإذا تطلبت الخوارزمية المستخدمة لتجفير الحمولة النافعة بيانات للتزامن التجفيري، مثل متجه التدميث، تحمل هذه البيانات صراحة في حقل الحمولة النافعة، ولكن لا يستدعي ذلك اعتبار هذا الحقل حقلاً مستقلاً من الحمولة EAMDSP، بمعنى أن إرسال متجه تدميث صريح يكون غير مرئي بالنسبة للحمولة EAMDSP.

4) التحشية (للتجفير):

قد تكون التحشية أيضاً مطلوبة، بغض النظر عن متطلبات خوارزمية التجفير، للتأكد من انتهاء نص التجفير الناجم عنها بحد بايتات يبلغ أربعة. وبوجه خاص، يجب أن يكون حقلا طول التحشية والرأسية التالية متراصفين ضمن كلمة من أربعة بايتات، كما تعرضه الأشكال أعلاه الخاصة بنسق رزمة الحمولة EAMDSP لضمان تراصف حقل شفرة الاستيقان من الرسائل (إن وجد) ضمن حد من 4 بايتات.

5) طول التحشية:

يشير حقل طول التحشية إلى عدد بايتات التحشية التي تسبقه مباشرة في حقل التحشية. وتتراوح القيم الصالحة بين صفر و255، وتشير القيمة صفر إلى عدم وجود بايتات تحشية. ويُعتبر حقل طول التحشية إلزامياً.

6) الرأسية التالية:

يُعتبر حقل الرأسية التالية إلزامياً، وهو حقل من 8 بتات يحدد نوع البيانات الموجودة في حقل بيانات الحمولة النافعة، مثل رأسية الطبقة التالية والبيانات.

7) شفرة الاستيقان من الرسائل:

شفرة الاستيقان من الرسائل عبارة عن حقل متغير الطول يحتسب على البيانات التي يشير إليها القناع لتوفير الحماية من منظور السلامة. وتدرَج في احتساب شفرة الاستيقان من الرسائل الحقول الضمنية لرأسية الحمولة EAMDSP مثل التحشية اللازمة لتوليد شفرة الاستيقان من الرسائل. وحقل شفرة الاستيقان من الرسائل اختياري.

3.1.A معالجة الرزمة

تجرى عملية معالجة البيانات الصادرة بالتجفير EAMD كالتالي:

1) البحث عن الرابطة SAM:

تحدد الرابطة SAM ذات الصلة التي تتطلب معالجة الحمولة EAMDSP بناءً على معلومات مثل معرف هوية الطبقة والمعلمة الخاصة بالطبقة مثل عنوان بروتوكول الإنترنت أو رقم منفذه في الرزمة.

2) تحويل البيانات باستخدام التجفير EAMD:

يُجرى التجفير وتوليد شفرة الاستيقان من الرسائل باستخدام التجفير EAMD وفقاً للعملية التي يرد وصفها في الفقرة 1.6.

3) إرسال الرزمة:

تضاف الرأسية الأصلية إلى الرزمة المحولة بالتجفير EAMD، وترسل الرزمة الناجمة عن ذلك إلى الشبكة.

وتجرى عملية معالجة البيانات الواردة باستخدام التجفير EAMD كالتالي:

1) البحث عن الرابطة SAM:

تُحدد الرابطة SAM ذات الصلة التي تتطلب معالجة الحمولة EAMDSP بناءً على بعض المعلومات مثل معرف هوية الطبقة الذي يحدد طبقة النقل وعنوان بروتوكول الإنترنت ورقم منفذه في الرزمة.

2) التحقق من رقم التتابع:

يتم التحقق من رقم التتابع باستخدام قيمة رقم التتابع في رأسية الحمولة EAMDSP، وذلك قبل التحقق من السلامة وفك التجفير. وإذا فشلت عملية التحقق هذه، تنبذ الرزمة.

3) تحويل البيانات باستخدام التجفير EAMD:

يتم التحقق من شفرة الاستيقان من الرسائل وفك التجفير باستخدام التجفير EAMD وفقاً للعملية التي يرد وصفها في الفقرة 1.6.

4.1.A قناع لاستخلاص البيانات المستهدفة من أجل إجراء التجفير ببيانات قناع مصاحب

في عمليات التجفير ببيانات قناع مصاحب، يستخلص الهدف من مدخلات الفدرات إلى الخوارزمية المقابلة بتقسيم الرزمة إلى حجم الفدرة خوارزمية التجفير المستخدمة وفقاً لمعلمات القناع. فعلى سبيل المثال، عند التجفير EAMD باستخدام معيار تجفير متقدم (AES)، تقسَّم الحمولة النافعة إلى كلّ 128 بتة لأن طول فدرة معيار التجفير المتقدم يبلغ 128 بتة. في حين يستخلص الهدف من فدرة فك التجفير بتحديد الفدرة استناداً إلى القناع. وبعد ذلك، تولد البيانات المستهدفة للعملية من تسلسل هدف فدرة فك التجفير. ويرد وصف نسق القناع في الشكلين 3.A و4.A. وتظهر هذه المعلمة الفدرة التي ينبغي تجفيرها أو فك تجفيرها في حال تقسيم الحمولة النافعة إلى حجم فدرة خوارزمية تجفير المستخدمة.

```
MaskFormat ::= SEQUENCE {
  encryptionArea OCTET STRING (SIZE (12))
  reserved OCTET STRING (SIZE (4))
}
```

الشكل 3.A – نسق القناع

الشكل 4.A – نسق مفصل لمعلمة القناع

تعني معلمة القناع هذه، في هذه الحالة، تجفير الفدرة الأولى فقط لأن البتة الأولى من معلمة القناع حقيقية. ويتطلب تجفير بعض المقاطع تغيير بعض بتات معلمة القناع من زائفة إلى حقيقية.

5.1.A خوارزمية التحشية

يمكن وصف خوارزمية التحشية على النحو التالي:

- إلحاق '0x80' في آخر الحمولة النافعة.
- إذا بلغ طول الحمولة النافعة أحد مضاعفات طول فدرة خوارزمية التجفير، توقف التحشية.

إذا **لم** يكن طول الحمولة النافعة أحد مضاعفات طول فدرة خوارزمية التجفير، تلحق '0x00' بآخر الحمولة النافعة إلى أن يصبح طول الحمولة أحد مضاعفاته.

بيبليوغرافيا

[b-ITU-T F.4104] Recommendation ITU-T F.4104/F.744 (2009), *Service description and requirements for ubiquitous sensor network middleware.*

[b-ITU-T X.1311] Recommendation ITU-T X.1311 (2011) | ISO/IEC 29180:2012, *Information technology – Security framework for ubiquitous sensor networks.*

[b-ITU-T X.1312] Recommendation ITU-T X.1312 (2011), *Ubiquitous sensor network middleware security guidelines.*

[b-ITU-T X.1313] Recommendation ITU-T X.1313 (2012), *Security requirements for wireless sensor network routing.*

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.

[b-ITU-T Y.4105] Recommendation ITU-T Y.4105/Y.2221 (2010), *Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment.*

[b-ITU-T Y.4109] Recommendation ITU-T Y.4109/Y.2061 (2012), *Requirements for the support of machine-oriented communication applications in the next generation network environment.*

[b-IETF RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol.*

[b-IETF RFC 5116] IETF RFC 5116 (2008), *An Interface and Algorithms for Authenticated Encryption.*

[b-ISO/IEC 9797] ISO/IEC 9797-1:2011, *Information technology – Security techniques –Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher.*

[b-ISO/IEC 18033] ISO/IEC 18033-3:2010, *Information technology – Security techniques –Encryption algorithms – Part 3: Block ciphers.*

[b-ISO/IEC 19772] ISO/IEC 19772:2009, *Information technology – Security techniques – Authenticated encryption.*

[b-ASIACRYPT] Bellare, M., and Namprempre, C. (2000), *Authenticated encryption:* Relations *among notions and analysis of the generic composition paradigm*, in Tatsuaki Okamoto, editor, ASIACRYPT 2000, Vol. 1976 of LNCS, Springer, December, pp. 531-545.

[b-CBCPADD] Vaudenay, S. (2002), *Security Flaws Induced by CBC Padding Applications to SSL, IPSEC, WTLS*, EUROCRYPT 2002.

[b-EUROCRYPT] Namprempre, C., Rogaway, P., and Shrimpton, T. (2014), *Reconsidering generic composition*, in Phong Q. Nguyen and Elisabeth Oswald, editors, EUROCRYPT 2014, Vol. 8441 of LNCS, Springer, May, pp. 257-274.

[b-ZT] Li, Zhang, and Xin, Tong (2013), *Threat Modeling and Countermeasures Study for the Internet of Things*, Journal of Convergence Information Technology (JCIT), Vol. 8, No. 5, March.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2018