الاتحـــــاد الدولـــــي للاتصـــــالات

ITU-T H.235.5

(2005/09)

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

السلسلة H: الأنظمة السمعية المرئية والأنظمـــة متعددة الوسائط

البنية التحتية للخدمات السمعية المرئية – جوانب الأنظمة

إطار الأمن H.323: إطار الاستيقان الآمن أثناء تبادل رسائل التسجيل والقبول والحالة (RAS) باستعمال أسرار متقاسمة ضعيفة

التوصيـــة ITU-T H.235.5

الاتحاد الدولي للاتصالات

توصيات السلسلة H الصادرة عن قطاع تقييس الاتصالات

الأنظمة السمعية المرئية والأنظمة متعددة الوسائط

خصائص أنظمة الهاتف المرئي	H.199 – H.100
البنية التحتية للخدمات السمعية المرئية	
مبادئ عامة	H.219 – H.200
تعدد الإرسال والتزامن في الإرسال	H.229 – H.220
جوانب الأنظمة	**H.239 – H.230**
إجراءات الاتصالات	H.259 – H.240
تشفير الصور المتحركة الفيديوية	H.279 – H.260
جوانب تتعلق بالأنظمة	H.299 – H.280
الأنظمة والتجهيزات المطرافية للخدمات السمعية المرئية	H.349 – H.300
معمارية خدمات الأدلة للخدمات السمعية المرئية والخدمات متعددة الوسائط	H.359 – H.350
معمارية جودة الخدمات السمعية المرئية والخدمات متعددة الوسائط	H.369 – H.360
خدمات تكميلية في تعدد الوسائط	H.499 – H.450
إجراءات التنقلية والتعاون	
لمحة عامة عن التنقلية والتعاون، تعاريف وبروتوكولات وإجراءات	H.509 – H.500
التنقلية لأغراض الأنظمة والخدمات متعددة الوسائط في السلسلة H	H.519 – H.510
تطبيقات وخدمات تعاون الوسائط المتعددة المتنقلة	H.529 – H.520
الأمن في الأنظمة والخدمات متعددة الوسائط المتنقلة	H.539 – H.530
الأمن في تطبيقات وخدمات تعاون الوسائط المتعددة المتنقلة	H.549 – H.540
إجراءات التشغيل البيني في التنقلية	H.559 – H.550
إجراءات التشغيل البيني في تعاون الوسائط المتعددة المتنقلة	H.569 – H.560
خدمات النطاق العريض وتعدد الوسائط ثلاثي الخدمات	
خدمات متعددة الوسائط بالنطاق العريض على خط المشترك الرقمي فائق السرعة (VDSL)	H.619 – H.610

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

إطار الأمن H.323: إطار الاستيقان الآمن أثناء تبادل رسائل التسجيل والقبول والحالة (RAS) باستعمال أسرار متقاسمة ضعيفة

ملخص

تتيح هذه التوصية الإطار اللازم للاستيقان المتبادل بين المشاركين أثناء تبادل رسائل التسجيل والقبول والحالة (RAS) H.225.0. وتسمح الأساليب القائمة على "إثبات الحيازة" الموصوفة بالاستعمال الآمن للأسرار المتقاسمة مثل كلمات السر، التي لو استعملت في حد ذاتها، لن تضمن أمناً كافياً.

كما يرد وصف تمديدات هذا الإطار الرامية إلى السماح بالمفاوضة الآنية لمعلمات أمن طبقة النقل لحماية قناة تشوير النداء اللاحقة.

وفي الصيغ السابقة للسلسلة الفرعية H.235، تم تعريف هذه الملامح في الملحق H بالتوصية H.235. وتبين التذييلات IV وV وVI بالتوصية H.235.0 التقابل بين كل الفقرات وكل الأشكال وكل الجداول في الصيغة 3 وفي الصيغة 4 من التوصية ITU-T H.235.

المصدر

وافقت لجنة الدراسات 16 (2005-2008) لقطاع تقييس الاتصالات بتاريخ 13 سبتمبر 2005 على التوصية ITU-T H.235.5 بموجب الإجراء الوارد في التوصية A.8.

العبارات الرئيسية

التصديق، كلمات السر، الأمن

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات. 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 رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

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

ملاحظـــة

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.

حقـــوق الملكيـــة الفكريـــة

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، كان 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 المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

المحتويات

الصفحة

مقدمة

يجوز، في تطبيقات كثيرة، لنقطة طرفية (أو لمستعملها وحارس بوابتها أن يتقاسما سراً "صغيراً" مثل كلمة السر أو "رقم التعرف الشخصي" (PIN). وهذا السر (الذي سيشار إليه فيما بعد بتعبير "كلمة السر") وأي مفتاح تجفير مشتق عنه يعتبر ضعيف من حيث الشيفرة. وتتيح آليات الاستيقان من نمط اختبار/استجابة، التي يرد وصفها في الفقرة 10، عينات لنصوص عادية والنصوص الشفرية المناظرة، وتتعرض بالتالي لهجمات قوى شرسة من قبل مراقب المعاملة قيد البحث حينما تجرى عمليات الاستيقان بواسطة عينات كلمات السر. وهكذا، يستطيع المراقب استرداد كلمة السر أو رقم التعرف الشخصي (PIN) بحيث يعتبر فيما بعد وكأنه النقطة الطرفية لكي يتمكن من الحصول على خدمة.

وتستعمل مجموعة من البروتوكولات المصنفة تحت عنوان تبادل مفاتيح التجفير سراً متقاسماً "لإخفاء" تبادل مفاتيح ديفي – هيلمان (Diffie-Hellman) بطريقة تسمح للمهاجم بتسوية مجموعة من مشاكل الخوارزميات المنتهية لإثبات هجوم قوى شرسة على السر المتقاسم. ويستعمل في تبادل مفاتيح التشفير (EKE) لبوليفان وميريت [B&M]، السر المتقاسم لتجفير المفاتيح العمومية ديفي – هيلمان وفقاً لخوارزمية متناظرة. ووفقاً لطريقة تبادل المفاتيح الأسي انطلاقاً من كلمة سرة بسيطة (SPEKE) لجابلون Jablon، يستعمل السر المتقاسم لانتقاء مولد آخر من مجموعة ديفي – هيلمان. وتجمع هذه البروتوكولات بين توفير الأمن لتبادل قوى لمفاتيح ديفي – هيلمان باستعمال السر المتقاسم بطريقة تمنع أي مهاجم من الحصول على النص العادي لاستعماله في هجوم لقوى شرسة ضد السر دون حل مشكلة الخوارزمية المنتهية ديفي – هيلمان بشدة فك تشفير مفتاح السر (أو العكس). ومن المثالب المحتملة أنها تخضع بشكل عام لحماية براءة الاختراع.

إطار الأمن H.323: إطار الاستيقان الآمن أثناء تبادل رسائل التسجيل والقبول والحالة (RAS) باستعمال أسرار متقاسمة ضعيفة

1 مجال التطبيق

يمكن استعمال هذه التوصية من قبل حارس بوابة أو نقطة طرفية باستعمال بروتوكول التسجيل والقبول والحالة الوارد في التوصية H.225.0.

2 المراجع

1.2 المراجع المعيارية

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 إلى المراجعة، فإن جميع المستعملين لهذه التوصية مدعوون إلى تطبيق أحدث طبعة للتوصيات والمراجع الواردة أدناه. وتُنشر بانتظام قائمة بتوصيات قطاع تقييس الاتصالات سارية الصلاحية. والإشارة إلى وثيقة في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

- التوصية ITU-T H.225.0 (2003)، *بروتوكولات تشوير النداء وترزيم التدفقات أحادية الوسائط لأنظمة الاتصالات متعددة الوسائط القائمة على الرزم.*
- التوصية ITU-T H.235.0 (2005)، *إطار الأمن H.323: أمن وتخفير المطاريف متعددة الوسائط من السلسلة H (المطاريف H.323 وغيرها من النمط H.245).*
- التوصية ITU-T H.235.1 (2005)، *إطار الأمن H.323: مظهر جانبي للأمن الأساسي.*
- التوصية ITU-T H.245 (2005)، *بروتوكول التحكم للاتصالات متعدد الوسائط.*
- التوصية ITU-T H.323 (2003)، *أنظمة الاتصالات متعددة الوسائط بأسلوب الرزم.*
- Federal Information Processing Standard FIPS PUB 180-2, *Secure Hash Standard*, U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, 1 August 2002.
- NIST Special Publication 800-38A 2001, *Recommendation for Block Cipher Modes of Operation – Methods and Techniques*. http://www.csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf.

2.2 المراجع البحثية

[AES] IETF RFC 3268 (2002), *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security*.

[B&M] BELLOVIN (S.), MERRITT (M.): U.S. Patent 5,241,599, August 31, 1993, originally assigned to AT&T Bell Laboratories, now assigned to Lucent Technologies.

[Jab] JABLON (D.): Strong Password-Only Authenticated Key Exchange, *Computer Communication Review*, ACM SIGCOMM, Vol. 26, No. 5, pp. 5-26, October 1996.

[NIST SP 800-57] NIST Draft Special Publication 800-57 (2005), *Recommendation for Key Management, Part 1: General Guideline*. http://www.csrc.nist.gov/publications/drafts/draft-800-57-Part1-April2005.pdf

[RFC2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication*.

[RFC2412] IETF RFC 2412 (1998), *The OAKLEY Key Determination Protocol*.
[RFC2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.
[RFC3546] IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*.

3 التعاريف

لا توجد تعاريف.

4 المختصرات

تستخدم التوصية الحالية المختصرات التالية:

ACF تأكيد القبول *(Admission Confirm)*
AES معيار تجفير متطور *(Advanced Encryption Standard)*
ARJ رفض القبول *(Admission Reject)*
ARQ طلب القبول *(Admission Request)*
CBC تشفير بتسلسل الأرتال *(Cipher Block Chaining)*
CTR أسلوب العداد (انظر NIST SP 800-38A) *(Counter Mode)*
D-H ديفي – هيلمان *(Diffie-Hellman)*
EKE تبادل مفاتيح التشفير *(Encrypted Key Exchange)*
GCF تأكيد حارس البوابة *(Gatekeeper Confirm)*
GK حارس البوابة *(Gatekeeper)*
GRJ رفض حارس البوابة *(Gatekeeper Reject)*
GRQ طلب حارس البوابة *(Gatekeeper Request)*
HMAC شفرة مظللة لاستيقان الرسالة *(Hashed Message Authentication Code)*
ICV قيمة التحقق من السلامة *(Integrity Check Value)*
ID معرّف *(Identifier)*
LCF تأكيد الموقع *(Location Confirm)*
LRJ رفض الموقع *(Location Reject)*
LRQ طلب تحديد الموقع *(Location Request)*
MIM مُعترض *(Man-in-the-middle)*
OID معرف الشيء *(Object Identifier)*
PIN رقم التعرف الشخصي *(Personal Identification Number)*
PRF وظيفة شبه عشوائية *(Pseudo-Random Function)*
RAS التسجيل والقبول والحالة *(Registration, Admission and Status)*
RCF تأكيد التسجيل *(Registration Confirm)*
RFC طلب الحصول على تعليقات *(Request for Comments)*
RRJ رفض التسجيل *(Registration Reject)*
RRQ طلب التسجيل *(Registration Request)*
SHA1 خوارزمية مظللة مؤمنة رقم 1 *(Secure Hash Algorithm 1)*
SPEKE تبادل المفاتيح الأسي انطلاقاً من كلمة سر بسيطة *(Simple Password Exponential Key Exchange)*
TLS أمن طبقة النقل *(Transport Layer Security)*
UDP بروتوكول وحدة بيانات مكتفية *(User Datagram Protocol)*

5 المصطلحات

تنطبق المصطلحات التالية في هذه التوصية:

- "يجب"، يشير إلى حكم إلزامي.
- "ينبغي"، يشير إلى إجراء مقترح لكن اختياري.
- "يجوز"، يشير إلى إجراء ممكن بالأحرى بدلاً من إجراء موصى به.

وللاطلاع على المصطلحات الأخرى، انظر الفقرة H.235.0/5.

6 الإطار الأساسي

1.6 قدرات محسنة للتفاوض في التوصية ITU-T H.235.0

تتيح التوصية ITU-T H.235.0 إطار الأمن هذا بإدراج العناصر النوعية التالية في المجال **ClearToken**:

- **ProfileInfo** هو تتابع لعناصر خاصة بملامح معينة، ويعرف كل عنصر بواسطة قيمته الخاصة على النحو المحدد بواسطة ملامح محددة يسيرها معرف الشيء OID في **ClearToken.tokenOID**.

تمرر في الأوصاف التالية عدة عناصر في **ProfileInfo**؛ وسوف يعطى كل عنصر من هذه العناصر اسماً بدلاً من قيمة معرفة، لتسهيل المناقشة.

2.6 الاستعمال بين النقطة الطرفية وحارس البوابة

يبدأ الإطار الأساسي، الذي يعتبر فيه الطالب بمثابة نقطة طرفية ترغب في التسجيل لدى حارس البوابة ويكون المستجيب هو حارس البوابة هنا بطريقة مباشرة. ويفترض فيما يلي ضمناً أن كل **ClearToken** مذكور يعرف بواسطة **TokenOID** لملامح الاستيقان. ومن المفترض تمديد المجال **ClearToken**. والعنصران **random** و/أو **random2** يجوز استعمالهما من قبل أحد الملامح بطريقتين مختلفتين: ويمكن إدراجهما في حساب مفتاح الاستيقان و/أو مجال **ClearToken** لملامح كل رسالة RAS لاحقة (أي RCF/RRQ) لتجنب التكرار ويبدأ التبادل لتسجيل النقطة الطرفية على النحو التالي:

1) تعلن النقطة الطرفية عن استعدادها للمشاركة في آلية أو أكثر من آليات الاستيقان أو المفاوضة الرئيسية وذلك بإدراج معرف الشيء أو معرفات الشيء الملائمة للملامح المنشودة في عناصر **authenticationMechanism.keyExch** لعنصر **authenticationCapability** لرسالة **G**atekeeper**ReQ**uest. ومن المفترض أن يعرف كل OID محدد بالكامل إجراءً للاستيقان من حيث نظام المفتاح العمومي (ديفي – هيلمان) أو منحنى إهليلجي مثلاً) ومجموعة محددة (أي إحدى مجموعات OAKLEY من RFC 2412)، وخوارزمية تشفير متناظرة (أي AES-128-CBC مع استخلاص نص مشفر) ووظيفة اشتقاق المفتاح (أي عن طريق الوظيفة شبه العشوائية الواردة في الفقرة 10 من التوصية H.235.0) وشفرة استيقان الرسالة ([RFC2104] HMAC-SHA1-96) والتتابع الذي تستعمل فيه. وتشمل النقطة الطرفية أيضاً واحداً أو أكثر من ملامح **ClearToken** في الطلب GRQ، يحمل كل منها المعرف OID للملامح المعنية، بالإضافة إلى بيانات المفتاح العمومة اللازمة بالشكل التالي:

أ) يحمل **TokenOID** معرف OID للملامح كما يرد في العنصر **authenticationCapability** لرسالة GRQ المغلفة.

ب) يجوز استعمال **timeStamp** لضمان التداول وتجنب التكرار.

ج) لا تستعمل **Password** لكلمة السر الحقيقية.

د) يحمل **dhkey** معلمات مفتاح ديفي – هيلمان، في حال استعمالها. ويشفر عنصر **halfkey** المدرج على النحو المحدد من قبل الملامح المختارة.

هـ) **challenge** غير مطلوب.

و) يقدم الطرف الممهد **random** ويستعمل لمنع تكرار الهجمات.

ز) يجوز استعمال **certificate** إذا كان تبادل الشهادات يشكل جزءاً من الملامح.

ح) يجوز استعمال **generalID** إذا طلبت الملامح ذلك.

ط) يحمل **eckasdhkey** معلمات مفتاح المنحنى الإهليلجي، إذا استعملته الملامح. وينبغي تشفير عنصر **public-key** المدرج على النحو المحدد من قبل الملامح.

ي) يجوز استعمال **sendersID** كما تحدده الملامح.

ك) يجوز تقديم العنصر **initVect**، **profileInfo** مصحوباً ببيانات (مشفرة) المفتاح العمومي **dhkey** أو **eckasdhkey**، إذا طلبت الملامح متجه تدميث للتشفير.

ل) إذا رغب الممهد في استعمال بيانات المفتاح المستمدة من التبادل السابق، ينبغي أن يدرج الممهد عنصر **profileInfo**، الذي يطلق عليه **sessionID**، متضمناً المعرف الموزع أثناء التبادل السابق. وفي هذه الحالة ينبغي عدم إدراج **dhkey**، **eckasdhkey** و/أو **initVect**.

م) إذا رغب الممهد في إنشاء دورة أمن طبقة النقل (TLS) لتوصيلة تشوير النداء، يجوز للممهد أن يدرج عنصر **profileInfo** يتضمن تتابعات مشفرة TLS؛ وتتضمن الرسالة تتابع تشفير واحد فقط (الذي سبق التفاوض بشأنه) إذا كان عنصر **sessionID** موجوداً.

ن) إذا رغب الممهد في إنشاء دورة TLS لتشوير النداء، يمكن أن يتضمن عنصر **profileInfo** قائمة طرائق الانضغاط؛ وتدرج طريقة انضغاط واحدة (التي سبق التفاوض بشأنها) إذا كانت **sessionID** موجودة.

س) يجوز استعمال عناصر **profileInfo** أكثر لأي معلمات إضافية مطلوبة للإجراءات ذات الصلة بالملامح.

2) وعندما يستقبل الطلب GRQ، ينتقي حارس البوابة الملامح **AuthenticationMechanism** من القائمة المتوفرة، ويولد مفتاحاً خاصاً مناسباً، ويحسب المفتاح العمومي المناظر، ويولد متجه تدميث عند الضرورة للتشفير المتناظر باستعمال كلمة السر، ويشفر المفتاح العمومي، ويولد معرف ID دورة وحيدة، ويولد كمية عشوائية، وتشفر جميعها في **ClearToken**، ويجرى الاستعمال التالي لعناصر **ClearToken**، ويتوقف ذلك على الملامح التالية:

أ) يحمل **tokenOID** معرف OID للملامح، على النحو الذي انتقى به من العنصر **authenticationMethod** لرسالة GCF مغلفة.

ب) يجوز استعمال **timeStamp** لضمان التداول وتجنب التكرار.

ج) لا تستعمل **password** لكلمة السر الحقيقية.

د) يحمل **dhkey** معلمات مفتاح ديفي – هيلمان، في حال استعمالها. ويشفر عنصر **halfkey** على النحو المحدد من قبل الملامح المختارة.

هـ) يستعمل **challenge** لحمل متجه التدميث، إذا كان مطلوباً لتشفير المفتاح على النحو المحدد في الملامح، أو يمكن استعماله لحمل سلسلة عشوائية التي ينبغي أن تعيدها النقطة الطرفية لتجنب تكرار الهجمات.

و) يمكن أن يتضمن **random** قيمة وحيدة غير متوقعة يقدمها الطالب لمنع تكرار الهجمات.

ز) يجوز استعمال **certificate** إذا كان تبادل الشهادات يشكل جزءاً من الملامح.

ح) يجوز استعمال **generalID** إذا طلبت الملامح ذلك.

ط) يحمل **eckasdhkey** معلمات مفتاح المنحنى الإهليلجي، إذا استعملته الملامح. وينبغي تشفير عنصر **public-key** المدرج على النحو المحدد من قبل الملامح.

ي) يجوز استعمال **sendersID** على النحو المحدد في الملامح.

ك) ينبغي أن يتضمن **random** (أو عنصر **profileInfo** إضافي، يطلق عليه **random2**، إذا طلبت الملامح بقاء الرقمين العشوائيين أثناء تبادل الرسالة) قيمة وحيدة غير متوقعة من المستجيب للحماية من هجمات متكررة.

ل) يقدم **initVect** إلى جانب بيانات المفتاح العمومي (المشفرة) (**dhkey** أو **eckasdhkey**) إذا تطلبت الملامح متجه تدميث للتشفير.

م) **sessionID** هو بمثابة معرف وحيد (لحارس البوابة) يستعمل لتحديد دورة التسجيل هذه. ويمكن أن يفيد، في إطار بعض الملامح، كمعرف لدورة بروتوكول TLS من أجل إنشاء سريع لقناة تشوير نداء محمية بواسطة TLS.

ن) يجوز استعمال **profileInfo** لأي معلمة إضافية مطلوبة للإجراءات ذات الصلة بالملامح.

ثم يحسب حارس البوابة السر المتقاسم أو المفتاح الشامل باستعمال مفتاحه الخصوصي والمفتاح العمومي (المشفر) انطلاقاً من الرسالة GCF، ويشتق من المفتاح الشامل مفاتيح التجفير، ومفاتيح الاستيقان والبيانات الأخرى اللازمة، وفقاً للملامح. ويرد المجال **ClearToken** الموصوف أعلاه ضمن رسالة **G**atekeeper**C**on**F**irm. وينبغي التحقق من سلامة الرسالة **GCF** واستيقانها بواسطة مفتاح الاستيقان المحسوب ثم ترسل إلى النقطة الطرفية. ويمكن إرسال نتائج التحقق من الاستيقان والسلامة بأساليب مختلفة، على النحو المحدد من قبل الملامح؛ بوساطة عنصر **profileInfo** الخاص، أو بواسطة أسلوب من الأساليب المحددة في التوصية ITU-T H.235.1.

3) تفحص النقطة الطرفية العنصر **authenticationMechanism.keyExch** المختار من الرسالة GCF وتستخلص المعلمات من **ClearToken** المحدد بواسطة معرف **tokenOID** المناظر. ثم تختار النقطة الطرفية مفتاحها الخاص، وتحسب المفتاح العمومي المناظر، وتختار أي معلمات أخرى تطلبها الملامح. ثم تحسب النقطة الطرفية السر المتقاسم أو المفتاح الشامل باستعمال المفتاح الخاص بها والمفتاح العمومي (المشفر) من الرسالة GCF، وتشتق مفاتيح التجفير مفاتيح الاستيقان وغيرها من البيانات اللازمة، وفقاً للملامح. ثم تتحقق النقطة الطرفية من سلامة الرسالة GCF. وإذا كانت نتيجة هذا التحقق غير صحيحة، ينبغي أن تزيل النقطة الطرفية الرسالة GCF وكل البيانات الرئيسية المشتقة منها، وتواصل الانتظار لرسالة GRQ صحيحة. وسيترتب على استرداد RAS المعيارية إلى إعادة إرسال GRO، واستقبال رسالة GFC سليمة، على وجه الاحتمال. وإذا اخفقت عدة إرسالات في إنتاج استجابة ناجحة، ينبغي أن تتوقف النقطة الطرفية عن محاولة التسجيل وتبلغ مستعملها بافتقاد شيء ما. ويجدر ملاحظة أن كل رسالة GRO ترسل تعطي خادم البوابة فرصة إضافية لمحاولة تخمين كلمة سر المستعمل وتقر صلاحية هذا التخمين بواسطة قبول الرسالة GRO. وإذا نجح التحقق من سلامة الرسالة GCF، تثبت النقطة الطرفية صحة حارس البوابة، ويمكن أن تسجل نفسها وتثبت صحتها لدى حارس البوابة أثناء هذه العملية.

4) ثم تقوم النقطة الطرفية بملء المجال **ClearToken** بواسطة الملامح **tokenOID** بطريقة مماثلة للطريقة المستعملة من أجل حارس البوابة الموصوفة أعلاه. وبمجال كل فيشة واضحة للرسالة GCF تعتبرها الملامح بمثابة اختبار ينبغي أن يرد في المجال **ClearToken**. وينبغي أن يشتمل المجال **ClearToken** على عناصر **random** و**random2** للرسالة GFC المستقبلة، إذا حددتها الملامح لتجنب التكرار. ثم يوضع المجال **ClearToken** في رسالة **R**egistration **ReQ**uest لكي يرسل إلى حارس البوابة. ثم تثبت النقطة الطرفية صحة الرسالة RRQ الكاملة وترسلها إلى حارس البوابة. وانطلاقاً من هذه النقطة، ينبغي ألا تقبل النقطة الطرفية أو ترسل الرسائل RAS التي لم يتم استيقانها بواسطة الملامح المتفق عليها وذلك باستعمال مفتاح الاستيقان المشتق من بيانات المفتاح المتقاسم.

5) يستلم حارس البوابة الرسالة RRQ ويستعمل بيانات المفتاح المتقاسم للاستيقان من سلامة الرسالة RRQ بالنسبة للعنصر المدرج للاستيقان والتحقق من السلامة. وإذا أخفق التحقق من السلامة، يتجاهل حارس البوابة الرسالة RRQ المستلمة وينتظر رسالة RRQ يمكن التحقق منها. وإذا لم تصل أي رسالة من هذا القبيل، من المحتمل أن تتخلى النقطة الطرفية عن التسجيل وتعود إلى البحث عن حارس البوابة. وإذا نجحت عملية التحقق من السلامة، يقوم حارس البوابة بإعداد رسالة Registration ConFirm لإرسالها إلى النقطة الطرفية. ووفقاً للملامح المستعملة، يمكن أن تتضمن الرسالة RCF مجالاً **ClearToken** يتضمن عناصر **random** و**random2** و/أو **challenge** لمجال **ClearToken** من ملامح الاستيقان المتاحة في الرسالة RRQ. وينبغي أن تشتمل رسائل RCF وجميع رسائل RCF اللاحقة على عنصر استيقان والتحقق من السلامة يمكن التحقق منه بحسب بواسطة مفتاح خوارزمية الاستيقان المتفاوض بشأنها.

6) عندما تستلم نقطة طرفية رسالة RCF، تتحقق النقطة الطرفية من السلامة بواسطة عنصر الاستيقان والتحقق من السلامة المدرج. وإذا كانت نتيجة هذا التحقق غير صحيحة، ترفض الرسالة RCF؛ وإذا لم تستلم رسالة RCF صالحة، حتى بعد إعادة إرسال الرسالة RRQ، ينبغي التخلي عن الدورة وتعود النقطة الطرفية إلى البحث عن حارس بوابة جديد. وإذا كانت نتيجة التحقق من سلامة الرسالة RCF صحيحة، يجوز استخلاص دورة ID وتتابع التشطير، في حال وجودهما، من المجال **ClearToken** من أجل الاستعمال اللاحق أثناء إنشاء قناة تشوير نداءات آمنة.

3.6 استعمال الملامح بين حراس البوابات

يجوز استعمال الإجراء ذاته أساساً بين حراس البوابات في تبادل الرسالتين LRQ/LCF. وفي هذه الحالة، لا يمكن إجراء انتقاء صريح للملامح، يقوم حارس بوابة المصدر باقتراح واحد أو أكثر من الملامح وذلك بإدراج المجال أو المجالات **ClearToken** المناسبة على النحو الموصوف أعلاه للرسالة **GRQ**. ويستطيع حارس البوابة المستجيب انتقال أحد الملامح المقترحة وينبغي أن يعيد إرسال المجال **ClearToken** المناظر على النحو الموصوف أعلاه للرسالة **GCF**. ومن الجدير الملاحظة في هذه الحالة أن حارس البوابة الطالب لا يستيقن لحارس البوابة المستجيب إلى أن ينشئ قناة لتشوير النداء نحو حارس البوابة ذاك.

ويمكن استعمال هذا الإجراء في أسلوب البث المتعدد إذا تقاسمت مجموعة من حراس البوابات سراً واحداً يتعين استعماله لهذا الغرض. وسوف تستند الراسلة LRQ متعددة البث إلى هذا السر؛ وسوف يستعمل حراس البوابات الذين يستجيبون بواسطة الرسالة LCF هذا المفتاح لفك تشفير المفتاح العمومي ديفي – هيلمان ويقوم كل منهم باختيار **nonce** الخاص به والمفتاح الخصوصي ديفي – هيلمان لاستجاباتهم. وستكون مفاتيح الدورة الناتجة خاصة بالزوج النهائي من حراس البوابات.

4.6 تجفير واستيقان قناة التشوير

إذا دعم حارس البوابة تسيير حارس البوابة، يمكن استعمال بيانات المفتاح الشامل المتفاوض بشأنها حديثاً ومعلمات التجفير المحددة لاستيقان قناة تشوير النداء وتأمينها، وذلك بإنشاء دورة TLS لتشوير النداء. وإذا تعين استعمال دورة TLS، ينبغي أن يدرج حارس البوابة العنصرين **cipherSuite** و**compress** المختارين في الملامح المرسلة **ClearToken**.

7 ملامح أمن محددة (SP1)

تتيح هذه الفقرة ملامح أمن معيارية من المتوقع أن توفر سراً متقاسماً مناظراً لرقم عشوائي من 80 بتة (انظر [NIST SP 800-57]). وتتألف هذه الملامح مما يلي:

- معرف الشيء لهذه الملامح (يطلق عليه "SP1") {itu-t (0) recommendation (0) h (8) 235 version (0) 3 60}.

- التفاوض بشأن المفتاح الشامل K_m، تبادل مفاتيح ديفي – هيلمان بواسطة المجموعة المعروفة 2 OAKLEY [RFC 2412]، يعقبها SHA1 [FIPS PUB 180-1] تخفيض مظلل لسر ديفي – هيلمان: K_m = SHA1 (السر المتقاسم ديفي – هيلمان).

- خوارزمية التجفير المتناظر: ينبغي أن تكون خوارزمية AES-128 بأسلوب عداد مقطع بطرف مميز من 2 أثمونة D، ومتجه تدميث من 12 أثمونة، IV، ومجال عداد من 2 أثمونة C، بحيث يكون العداد مساوياً لـــ C || IV || D وC = 0 في البداية. انظر [NIST SP 800-38A] للحصول على وصف لأسلوب CTR. يضبط مميز الطرف D على 3636 × 0 عندما يولد IV الطرف الذي أصدر GRQ/RRQ أو LRQ، ويضبط على 5c5c × 0 عندما يولد IV بواسطة الطرف المستجيب بالرسالة GCF/RCF أو LCF. وينبغي أن يتأكد كل طرف من أن المتجه الذي يولده يعتبر وحيد؛ ويمكن أن يستعمل طريقته الخاصة لضمان هذا الطابع الوحيد.

- تجفير مفتاح ديفي – هيلمان: يجب أن يستعمل أسلوب العداد المقطع AES-128 لتجفير المفتاح الشامل ديفي – هيلمان (الذي يمثل في شكل سلسلة أثمونية وفقاً لترتيب الأثمونات في الشبكة)؛ ويحمل متجه التدميث في المجال **ClearToken.initVect**، ويجب إنشاء المفتاح من 16 أثمونة، K_p، في شكل 128 بتة أكثر وزناً من قيمة التظليل SHA1 لكلمة سر المستعمل: K_p = Trunc(SHA1 user password), 16 ، حيث Trunc(x,y)، تبتر سلسلة الأثمونات x إلى y أثمونة. ويجدر ملاحظة أن هذا المفتاح يعتبر عموماً مفتاحاً ضعيفاً.

- منع التكرار: يجب على كل طرف أن يقدم رقماً "عشوائياً" من 32 بتة (يمكن أن يتضمن مجال عداد لضمان الطابع الوحيد)؛ وتستعمل الأرقام العشوائية صراحة في حساب المفاتيح المشتقة، وبالتالي فهي ترسل مرة واحدة لكل منها.

- اشتقاق مفتاح الاستيقان، K_a،: باستعمال PRF المحددة في الفقرة 10 من التوصية H.235.0، التي يطلق عليها PRF(*in_key*, *label*, *outkey_len*) مع k_m = *key* و*label* = "auth_key" || R_e || R_g أو R_e هي **nonce** أمكن الحصول عليه انطلاقاً من عنصر **ProfileElement** من الرسالة GRQ، R_g هو **nonce** أمكن الحصول عليه انطلاقاً من الصفر **ProfileElement** للرسالة GCF و*outkey_len* = 128.

- وظيفة استيقان الرسالة وسلامتها: بواسطة مجال **ClearToken** يضبط بمعرفة **tokenOID** على "SP1" ويضبط العنصر **ProfileElement.octets** على قيمة التظليل HMAC-SHA1-96 المحسوبة على الرسالة بأسرها على النحو الموصوف في التوصية ITU-T H.225.0؛ ويطبق هذا الإجراء على جميع رسائل RAS ورسائل تشوير النداء (باستثناء الرسالة GRQ أو LRQ التي لا تتضمن معرف **sessionID**).

- مفتاح تجفير العنصر، K_e: يمكن تجفير العناصر المختارة لرسائل تشوير النداء (أو العناصر النفقية الواردة فيها) باستعمال AES-128 بأسلوب العداد المقطع باستعمال المفتاح K_e = PRF(K_m, "encrypt_key" || R_e || R_g, 128). ويمكن استعمال هذا المفتاح مثلاً لتجفير دورة الوسائط من أجل توزيعها في العناصر **h235Key** على النحو المستعمل في إجراءات التوصيل السريع و/أو H.245. وفي هذه الحالة، يستعمل "SP1" بوصفه معرفاً OID لخوارزمية التجفير.

وتستعمل هذه الملامح **ProfileElement** المحددة في الجدول 1. وتسير هذه العناصر في تتابع العناصر **ClearToken.profileInfo** على النحو المحدد في التوصية ITU.T H.235.0.

الجدول H.235.5/1 – عناصر الملامح

اسم العنصر (المستعمل في النص)	قيمة معرف العنصر ID	اختيار العنصر (الطول)	وصف العنصر
initVect	1	أثمونة (12)	متجه التدميث للتجفير EKE
nonce	2	أثمونة (أي رقم)	قيمة وحيدة غير متوقعة
cipherSuite	3	أثمونة (2)	تتابع تشفير TLS
compression	4	أثمونة (1)	خوارزمية انضغاط TLS
sessionID	5	أثمونة (1)	عنصر وحيد يمكن أن يناظر معرف دورة TLS
integrityCheck	6	أثمونة (12)	قيمة التحقق مسحوبة بواسطة مفتاح

ويتألف تتابع التسجيل مما يلي:

- ترسل النقطة الطرفية الطلب GRQ مصحوباً بالعنصر **authenticationCapability** الذي يتضمن **AuthenticationMechanism.keyExch** والذي يشتمل على معرف OID "SP1" ومجال **ClearToken** مناظر مع **tokenID** = "SP1" و **dhkey** يتضمن مفتاح عمومي مجفر من 1024 بتة باستعمال **initVect** بوصفه موجهاً IV والمفتاح المحسوب انطلاقاً من كلمة سر المستعمل، و**nonce** = الرقم العشوائي من 32 بتة الذي اختارته النقطة الطرفية.

- ويرد حارس البوابة بواسطة الرسالة GCF بعنصر **authenticationMode** يكون مساوياً لعنصر **AuthenticationMechanism.keyExch** يتمضن معرف OID "SP1" ومجال **ClearToken** مع **tokenID** = "SP1" ومجال **dhkey** يتضمن مفتاح عمومي غير مجفر من 1024 بتة، و**nonce** = رقماً عشوائياً من 32 بتة يختاره حارس البوابة، إلى جانب **integrityCheck** يتضمن قيمة مظللة للاستيقان محسوبة باستعمال مفتاح الاستيقان المشتق K_a. ويجدر ملاحظة أنه ليس من الضروري أن يقوم حارس البوابة بتجفير نصف مفتاحه ديفي – هيلمان في الرسالة GCF في هذه الملامح لأن الأمر يتعلق بأول مشارك في الاستيقان يبين قدرته على استيقان الرسالة GCF بواسطة مفتاح الاستيقان المشتق، وتسمح هذه الطريقة لحارس البوابة بإعادة استعمال مفاتيحه الخاصة ديفي – هيلمان بعدة نقاط طرفية. انظر الفقرة 5.10.

- يجب أن ترد النقطة الطرفية بواسطة رسالة RRQ تتضمن قيمة استيقان ومراقبة السلامة في العنصر **ProfileElement** مع المجال **elementID** المضبوط على **integrityCheck** و**element** المضبوط على القيمة المحسوبة انطلاقاً من مفتاح الاستيقان المشتق، K_a.

- يجب استيقان ومراقبة سلامة رسائل RAS اللاحقة، بما في ذلك الرسالة RCF، بواسطة الإجراء ذاته والمفتاح ذاته. ويجب الاستيقان من رسائل تشوير النداء في H.225.0 (ورسائل H.245 النفقية، إذا كانت موجودة) وذلك بواسطة المجال **ClearToken** والمجال **tokenOID** المضبوط على "SP1"، والذي يتضمن عنصر **profileInfo** **ProfileElement** مع المجال **elementID** المضبوط على **integrityCheck** والمجال **element** المضبوط على القيمة المحسوبة.

- ويمكن استعمال مفتاح التجفير K_e، وكذلك خوارزمية التجفير AES-128 بأسلوب العداد المقطع، من قبل حارس البوابة والنقطة الطرفية وذلك لتجفير معلومات مختارة تنقل بواسطة بروتوكول RAS، وبروتوكول تشوير النداء أو بروتوكول H.245. ويجوز لحارس البوابة، مثلاً، أن يوزع مفاتيح تجفير الوسائط المحمية بواسطة المفتاح K_e وخوارزمية تجفير الملامح.

- وإذا طُلب من نقطة طرفية التسجيل، مع الاحتفاظ بهوية الدورة الأصلية والسر الشامل الأصلي، ينبغي أن تحاول النقطة الطرفية التسجيل بإدراج معرف الدورة صراحة في الرسالة GRQ (بدون إدراج نصف مفتاح ديفي – هيلمان) في رسالته GRQ.
- يمكن استعمال هذه الملامح بين حراس البوابات (انظر الفقرة 3.6).

8 ملامح أمن محسنة (SP2)

تحدد هذه الفقرة ملامح أمن جديدة تستند إلى الملامح الأصلية SP1. وهي محددة بطريقة غير رسمية بالرمز SP2 وبطريقة رسمية بمعرف OID {itu-t (0) recommendation (0) h (8) 235 version (0) 4 62}. وهذه الملامح مماثلة لملامح SP1، باستثناء ما هو محدد في الفقرات التالية. وتشمل التحسينات المحددة ما يلي:

- التحسينات المتعلقة بإسناد أرقام التتابع لرسائل تشوير النداء للتصدي لهجمات متكررة.
- تمليح مفتاح التجفير المولد انطلاقاً من كلمة السر باستعمال استعارة النقطة الطرفية للتصدي للهجمات المعجمية.
- يزاد حجم القيمة الحاضرة ويصبح متغيراً.
- يشتق مفتاح تمليح لكي يستعمل مع متجه تدميث التجفير.
- يكفل نقل أكثر فعالية للملامح **ClearToken** باستعمال **genericData**.

تستعمل الملامح SP2 عناصر الملامح الواردة في الجدول 1 بالإضافة إلى عناصر الملامح الإضافية الموصوفة في الجدول 2:

الجدول H.235.5/2 – عناصر الملامح الإضافية من أجل ملامح SP2

اسم العنصر (المستعمل في النص)	قيمة معرف العنصر ID	اختيار العنصر (الطول)	وصف العنصر
seqNumber	7	أثمونات (4)	رقم تتابع من 32 وفقاً لترتيب الأثمونات في الشبكة
connectID	8	أثمونات (2)	معرف توصيل التشوير (اختياري، قيمة بالتغيب = 0)
endpointID	9	أثمونات (متغير)	ASN.1 – عنوان مستعار مشفر مرتبط بالنقطة الطرفية وكلمة السر الخاصة بها. (اختياري)

1.8 رقم تتابع تشوير النداء

لا تتضمن رسائل تشوير النداء الواردة في H.225.0 رقماً للتتابع إذ إنها تنقل عبر وصلة موثوقة (TCP) تكون مسؤولة عن وضع التتابع. بيد أن الافتقار إلى معرف رسالة وحيد على مستوى التطبق لا يعرض تشوير النداء للهجمات أو الهجمات الانعكاسية. ويمكن التصدي لهذه المشكلة بإضافة رقم تتابع ومعرف توصيل اختياري لكل رسالة تشوير للنداء. ومن الملاحظ أن هذه التقنية لا تمنع الهجمات أو الهجمات الانعكاسية تماماً ولكنها تخفض إلى حد كبير فرص نجاح المهاجم.

ويجب أن تكون أرقام التتابع وحيدة في كل اتجاه لمنع الانعكاس. ويمكن تحقيق ذلك، ضمن حدود عملية، بمطالبة مُصدر الرسالة GRQ (النقطة الطرفية) أو رسالة LRQ (حارس البوابة) ببدء رقم تتابع رسائل تشوير النداء المرسلة من صفر (0) لرقم تتابع رسائل تشوير النداء المرسلة إلى 2^{31} لرقم تتابع الرسائل المستقبلة، مع سلوك مقابل لحارس البوابة المُستقبل. ويوفر هذا وقتاً طويلاً جداً قبل إمكانية حدوث أي تراكب (حوالي 600 ساعة بمعدل غير معتاد فعلاً قدره رسالة واحدة كل واحد من الألف من الثانية). أما فيما يتعلق بالنداءات المتتالية التي تستعمل المعرف ذاته sessionID، يجدر استعمال رقم التتابع غير المستعمل التالي في كل اتجاه. (ولمراعاة الرسائل التي يحتمل فقدانها على التوصيلات المعيبة، ينبغي أن يقبل المستقبل الرسائل الموجودة في نافذة صغيرة (من 5 إلى 10 مثلاً) تلي رقم التتابع الأخير المستلم والاستمرار انطلاقاً من هناك). ويمكن للتجهيزات التي تدعم عدة توصيلات لتشوير النداء الآنية مع معرف الدورة ذاته، أن تستعمل معرف **connectID** الاختياري لتحديد أماكن رقم التتابع المنفصل لمختلف النداءات. وإذا لم تحدد، يفترض أن تكون قيمة معرف **connectID** مساوية لصفر (0).

2.8 توليد مفتاح تجفير ضعيف انطلاقاً من كلمة السر

ولتجنب الهجمات المعجمية التي يخمن فيها رقم التعرف الشخصي (PIN) المستعمل لتجفير مفتاح عمومي D-H المطبق على التوالي على استعارات النقطة الطرفية المعروفة، من المطلوب "تمليح" مفتاح التشفير المستعار ذاته. وبوجه خاص، ينبغي حساب المفتاح القائم على كلمة السر، K_p، من تسلسل كلمة السر ومعرف **endpointID** المقدم :

$$K_p = \text{Trunc}(\text{SHA1}(\text{user password} \,||\, \textbf{endpointID}), 16)$$

وسيكون **AliasAddress** في **endpointID** عادة أحد الأسماء المستعارة المدرجة في العنصر **endpointAlias** لرسالة GRQ، ولكن ذلك ليس ضرورياً. وعلى سبيل المثال، **endpointID** يمكن أن يحدد بوابة تدعم نقاط طرفية كثيرة ترد مستعاراتها في **endpointType**.

3.8 الحجم الحاضر (nonce)

تتطلب ملامح الأمن 1 أن يقوم كل طرف بتقديم قيمة حاضرة من 4 أثمونات (32 بتة) كجزء من بروتوكول التفاوض بشأن المفتاح. وعندما تقدم القيمة الحاضرة أثناء التفاوض بشأن المفتاح الأولي، قد تكون 32 بتة كافية لضمان أن تكون القمية الحاضرة جديدة تماماً في حالة ما إذا قام حارس البوابة المستجيب بإعادة استعمال المفتاح العمومي ديفي – هيلمان ويولد الطالب مفتاحاً جديداً. بيد أنه، عند التفاوض بشأن مفاتيح دورة جديدة انطلاقاً من مفتاح شامل ثم التفاوض بشأنه من قبل، قد لا يسمح الطول الكلي من 64 بتة بوجود فرق كافٍ بين كل مجموعة من المفتاح المشتقة. ويقترح أن يكون الحجم الحاضر متغيراً، بحد أدنى 4 أثمونات وبحد أقصى 16.

4.8 تمليح متجه التدميث

وكإجراء إضافي للتعتيم، يحسب مفتاح تمليح دورة من 112 بتة، K_s، على النحو التالي انطلاقاً من المفتاح الشامل المتفاوض بشأنه:

$$K_s = \text{PRF}(K_m, \text{"salting\_key"} \,||\, R_e \,||\, R_g, 112).$$

ويتم بناء عداد AES-128-CM الأولي لتشفير وفك التشفير على النحو التالي:

العداد = C || $(K_s \,\hat{}\, (D \,||\, IV))$ حيث C مجال عداد من 16 بتة، كانت صفراً في البداية.

5.8 تشفير ClearToken

تستعمل ملامح الأمن 1 تتابع **ClearToken** لحمل معلمات الملامح. وتتضمن كل رسالة **H.225.0** تتابع **ClearToken**، باستثناء اختيار **empty** في **h323-message-body**؛ وتحمل جميع الرسائل **genericData**. وتسمح بنية إجراءات SP1 ببنية منتظمة نسبياً للمجال **ClearToken**، التي يمكن تشفيرها مقدماً وإرسالها بوصفها معلمة **raw** مع ضبط **id.standard** على 1 في عنصر **GenericData** المحدد بواسطة معرف SP2 OID. ويسمح هذا الشكل بتحديد **ClearToken** بواسطة

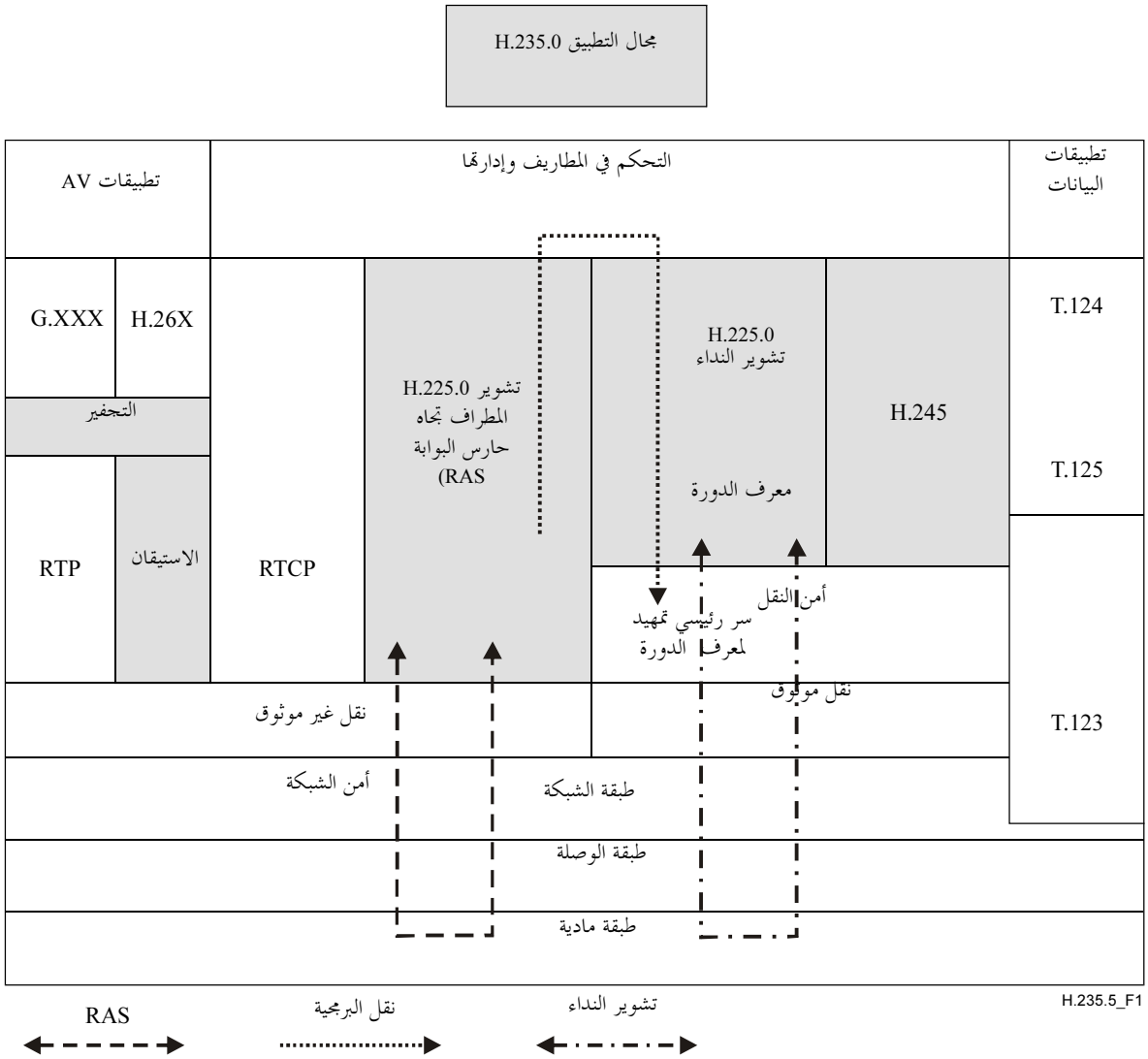
"null" {0,0} OID. والأهم، أنه يسهل تحديد موقع الفيشة وكذلك قيمة التحقق الواردة فيها، لأن الشكل المشفر **ClearToken** يصبح وحده متاحاً كجزء من عملية التشفير وفك التشفير العادية. وهكذا، من الأسرع تحديد موقع integrityCheck ضمن مجال **ClearToken** المشفر في كامل الرسالة المشفرة.

9 تمديدات الإطار (على سبيل الإعلام)

يمكن إدارج العناصر التالية في ملامح الأمن المحددة في هذا الإطار.

1.9 استعمال المفتاح الشامل لتأمين قناة تشوير النداء بواسطة بروتوكول TLS

يمكن استعمال بيانات المفتاح المتفاوض بشأنها أثناء تبادل RAS لاشتقاق مفاتيح الدورة لحماية قناة تشوير النداء بموجب بروتوكول النقل TLS (RFC-2246)، (RFC-3546). وفي الواقع، يحل التفاوض RAS محل بروتوكول التصافح الأولي TLS. ولا يكون ذلك معقولاً بالطبع إلا إذا كان تشوير النداء موجهاً إلى حارس البوابة. وهذا مفيد بشكل خاص للاستيقان ومن التشوير بين حراس البوابات عن طريق تبادل الرسالتين LRQ/LCF. وفي هذه الحالة لا توجد رسالة ثالثة RAS يستطيع عن طريقها حارس البوابة الطالب الاستيقان لدى حارس البوابة المطلوب انطلاقاً من بيانات المفتاح المتفاوض بشأنه، ولكن يمكن التحقق من الطالب ضمناً من خلال قدرته على إنشاء قناة تشوير النداء مزودة بمعلمات دورة TLS صحيحة. يبين الشكل 1 تدفق المعلومات قيد البحث: يستعمل RAS للتفاوض بشأن المفتاح الشامل للدورة، ويوزع معرف الدورة وسر الاختبار الشامل المناظر على برمجية بروتوكول TLS، ويستعمل معرف الدورة من قبل طبقة تشوير النداء لإنشاء قناة تشوير النداء عن طريق بروتوكول TLS. والطريقة التي ينقل بها السر تتوقف على التنفيذ وتتجاوز نطاق هذه التوصية. ويجدر ملاحظة أن هذه التوصية تحدد المنفذ 1300 باعتباره منفذ الاستماع TLS بالتغيب لتشوير النداء. ويجب على النقطة الطرفية أن تستعمل عنواناً واحداً لنقل تشوير النداء المقدم من حارس البوابة.



الشكل H.235.5/1 – تدفق المعلومات من أجل ملامح الأمن وبروتوكول TLS

تصف الفقرة التالية مختلف خطوات الإطار الأساسي الواردة في الشكل 1.

1.1.9 تسجيل النقطة الطرفية

يمكن لأي نقطة طرفية أن تختبر قدرة حارس بوابة معين على دعم تشوير نداء محمي بواسطة بروتوكول TLS وذلك بإدراج عنصر أو أكثر من عناصر **cipherSuite** وعنصر أو أكثر من عناصر **compression** في المجال **ClearToken** لملامح الرسالة GRQ المرسلة إلى الخطوة 1 أعلاه. وإذا رغبت النقطة الطرفية استعمال دورة متفاوض بشأنها مسبقاً، ينبغي أن تدرج النقطة الطرفية أيضاً **sessionID** في **ClearToken** (وتحدد فقط شفرة التتابع وطريقة الانضغاط الوحيد التي تتطابق مع الدورة المطلوبة). وإذا كان التفاوض يستند إلى دورة TLS القائمة، لا يتطلب الأمر بيانات شفرية في ملامح **ClearToken** بخلاف **nonce**.

وإذا كانت الدورة المطلوبة غير قائمة، يقوم حارس البوابة باختبار ملامح استيقان أخرى (إذا تيسر ذلك) أو يعيد رسالة GRJ مع **GatekeeperRejectReason.resourceUnavailable**. وإذا كانت الدورة المطلوبة غير قائمة، يتم الحصول على بيانات المفتاح الشامل انطلاقاً من دورة TLS، وتستعمل (مع العنصر **random** لرسالة GRQ والعنصر **random2** المولد بواسطة حارس البوابة) لحساب مفتاح الاستيقان لتبادل RAS. ويعاد معرف **sessionID**، و**cipherSuite** وطريقة **compress** و**nonce** حارس البوابة إلى ملامح **ClearToken** لرسالة GCF.

وإذا كان في إمكان حارس البوابة دعم تفاوض دورة TLS، ينبغي أن يوقم حارس البوابة بحساب بيانات المفتاح الشامل كما هو محدد في الملامح، ويوزع معرف جديد للدورة ويرسله إلى ملامح **ClearToken** في **sessionID**. وتتضمن ملامح **ClearToken** أيضاً معلمات الأمن المطلوبة من الخطوة 2 أعلاه، إلى جانب تتابع واحد تشفير **cipherSuite**، وطريقة واحدة **compress** مختارة، و**sessionID** غير صفري. ويجدر ملاحظة أن طريقة تبادل المفتاح للتتابع الشفري المختار ليست ذات أهمية. وإذا وافق حارس البوابة على حماية TLS لتشوير النداء، ينبغي حماية جميع عناوين نقل تشوير النداء المتبادلة في الرسالتين اللاحقتين RRQ/RCF أو ARQ/ACF بواسطة بروتوكول TLS.

وإذا لم يدعم حارس البوابة تفاوض الدورة TLS و/أو تحرير حارس البوابة، عندئذ لا تعاد أي معلمة من معلمات TLS، ولكن يمكن أن تستمر إجراءات الاستيقان من الخطوة 3، على النحو الموصوف أعلاه. وتقرر النقطة الطرفية ما إذا كانت مستعدة للاستمرار دون حماية TLS لتشوير النداء، ويمكنها أن تختار أن تفعل ذلك مع الاستمرار في استعمال ملامح الاستيقان.

وبناءً على الاستكمال الناجح لتتابع التسجيل، تتيسر دورة TLS للاستعمال للقيام بإنشاء سريع لتوصيلة أو عدة توصيلات لتشوير النداء في اتجاه حارس البوابة، دون أن تعيد التفاوض بشأن بيانات المفتاح بواسطة الطرائق المطبقة على المفاتيح العمومية.

ولدورات TLS أجل محدود. وبالتالي، قد يكون من الضروري أن تعيد النقطة الطرفية التفاوض بشأن معلمات الدورة للحصول على معرف جديد للدورة. ويمكن إنجاز ذلك عن طريق تبادل عناصر **ClearToken** اللازمة على النحو الموصوف أعلاه في شكل تتابع تسجيل مبسط ("للبقاء على قيد الحياة"). ولا يؤثر هذا التتابع على مفتاح استيقان RAS.

2.9 استعمال الشهادات لاستيقان حارس البوابة

قد يكون من غير العملي تبادل سلاسل الشهادات التي يمكن التحقق منها في RAS (والسبب في ذلك هو الحجم المحدود لرزم UDP)، إلا أن من الممكن أن يقوم مخدم ما بالتيقن بنفسه أمام النقطة الطرفية إذا تمكنت النقطة الطرفية من الحصول على نسخة موثوقة من المفتاح العمومي للمخدم عن طريق وسائل أخرى. ويمكن للمخدم أن يدرج ببساطة، في الرسالة GCF، عنصر **CryptoH323Token.cryptoGKCert** يكون مُعرفه **ClearToken.tokenOID** مضبوطاً على معرف OID لملامح الأمن المختارة.

3.9 استعمال آليات بديلة لأمن التشوير

والمعلمات المتفاوض بشأنها كجزء من ملامح الأمن بموجب هذه التوصية يمكن استعمالها في آليات الأمن على مستوى النقل و/أو مستوى التطبيق كما تحددها الملامح المحددة. وتم إضافة التتابع **profileInfo** إلى **ClearToken** H.235 لاستعمال من هذا القبيل، حسب الحاجة.

10 التهديدات (على سبيل الإعلام)

1.10 الهجمات السلبية

لا يتعرض المخطط الموصوف أعلاه، في الوقت الراهن، للتأثر بسبب الهجمات السلبية، شريطة ألا تكون المفاوضة ديفي – هيلمان هي ذاتها معرضة للتأثر من هذه الهجمات

2.10 هجمات حجب الخدمة

يخضع هذا المخطط لهجمات نشيطة لحجب الخدمة يستجيب فيها طرف ثالث لرسالة GRQ الأولية برسالة GRJ هامشية. ويمكن أو لا يمكن تعرف هوية هذا النوع من الهجمات، وإذا كان حارس البوابة الرافض مشروعاً، ويعرف السر المتقاسم (حارس البوابة هو حارس بوابة النقطة الطرفية والعنصر **rejectReason** له القيمة **resourceUnavailable**)، عندئذ يمكن أن يستكمل حارس البوابة المفاوضة بشأن المفتاح ويستقين الرسالة GRJ، بأن يرسل في هذه الرسالة، العناصر ذاتها الموصوفة للرسالة GCF (باستثناء أن المعرف OID المرسل في العنصر **authenticationMode** للرسالة GCF سيرسل في العنصر **ClearToken.profileInfo** للرسالة GRJ). ويتوقف ذلك على تعريف الملامح المحددة.

وإذا لم يتم استيقان GRJ، يمكن أن تكون الرسالة من مهاجم. وقبل التصرف في الرسالة GRJ (أي البحث عن حارس بوابة بديل)، ينبغي أن تنتظر النقطة الطرفية الاستلام المحتمل لرسالة أخرى GRJ أو رسالة GCF ثبتت صحتها ومستلمة من حارس بوابة صحيح. وخلاف ذلك، ينبغي أن تحاول النقطة الطرفية كل حارس بوابة مقترح في أي **altGKInfo** مستلمة في جميع الرسائل GRJ (يفترض في واحدة منها أن تكون مشروعة). وفي جميع الأحوال، لا يستطيع سوى حارس البوابة الصحيح (الذي يعرف السر المتقاسم) إعادة إرسال رسالة GCF مستيقنة.

3.10 هجمات المعترض

من المغري التفكير كأسلوب للتبادل، تبادل مفاتيح ديفي – هيلمان غير المشفرة، مع استعمال كلمة السر أو رقم التعرف الشخصي (PIN) لحساب مفاتيح الدورة انطلاقاً من سر ديفي – هيلمان. غير أن هذا الشكل من أشكال التبادل يخضع لهجمة معترض يمكن استعمالها للكشف عن السر المتقاسم "الصغير" بواسطة قوى شرسة عن طريق قيمة التحكم في السلامة التي يوفرها حارس البوابة المشروع في الرسالة GCF.

ويمكن لأي معترض، بالطبع، أن يتلاعب في أي رسالة مستيقنة لضمان نبذ الرسالة بسبب الإخفاق في التحقق من سلامتها. وإذا أمكن التلاعب في جميع الرسائل، يمكن حجب الخدمة.

4.10 تخمين الهجمات

يستطيع أن مهاجم أن ينتحل إما مركز نقطة طرفية مشروعة أو حارس بوابة مشروع، أو كلاهما (المعترض) وأن يحاول التنبؤ بالسر المتقاسم بطريقة تجريبية. ويستطيع المهاجم مثلاً (الذي يفترض معرفته لبيانات ملامح الاستيقان وجهله للسر المتقاسم) التنبؤ بالسر المتقاسم ويحاول تسجيله عن طريق إرسال رسالة GRQ انطلاقاً من هذا الافتراض. وبشكل عام، سيستجيب حارس البوابة لهذه المحاولة بواسطة رسالة GCF تتضمن المفتاح العمومي لحارس البوابة (مشفرة بواسطة السر المتقاسم الحقيقي) والقيمة ICV محسوبة باستعمال المفتاح المشتق الذي يعتمد على فك تجفير حارس البوابة للمفتاح العمومي المشفر

بواسطة المهاجم. ويمكن للمهاجم أن يستعمل هذه المعلومة للتحقق من مدى افتراضه للسر المتقاسم. وإذا أكد هذا الافتراض قيمة IVC للرسالة GCF، فمن المحتمل أن يناظر السر المتقاسم الحقيقي، ويمكن تأكدي ذلك بمواصلة تتابع التسجيل. وإذا تعذر استعمال الافتراض لاستنساخ القيمة ICV للرسالة GCF، ينبغي أن يصدر المهاجم افتراضاً آخر ويجري محاولة أخرى. ومع ترك حيز صغير لمفتاح السر المتقاسم، قد لا يكون عدد الافتراضات للبحث عن القوى الشرسة كبيراً. وتتطلب هذه الهجمة مشاركة نشيطة من حارس البوابة (أو النقطة الطرفية إذا انتحل المهاجم مركز حارس البوابة). والطريقة التقليدية المستعملة للتصدي لهذا الهجوم تتمثل في مراقبة عدد المحاولات الفاشلة، وعند بلوغ عتبة معينة، تعامل جميع المحاولات التالية باعتبارها صالحة (لفترة محددة على الأقل) ويطلق الإنذار، لكن هذه الإجراءات تتوقف على التنفيذ.

5.10 نصف مفتاح غير مشفر لحارس البوابة

وكما ذكر أعلاه، يمكن أن يبقى تبادل مفاتيح التشفير مأموناً في ظل ظروف معينة، إذا لم يقم حارس البوابة المستجيب بتشفير نصف مفتاحه ديفي – هيلمان. وينبغي أن يكون حارس البوابة، بوجه خاص، أول مشارك في إثبات أنه يعرف السر المتقاسم (رقم PIN) بواسطة القيمة ICV. وإذا لم يكن الأمر كذلك، يستطيع حارس البوابة (أو أي دخيل ينتحل مركز حارس البوابة) ببساطة محاولة جميع أرقام PIN الممكنة لفك تشفير نصف مفتاح ديفي – هيلمان للنقطة الطرفية، ويحسب السر المتقاسم ديفي – هيلمان الناتج، ويحسب مفتاح الاستيقان ويختبر قياساً على القيمة ICV التي تتيحها النقطة الطرفية. ويتعذر ذلك إذا استطاعت النقطة الطرفية مراقبة القيمة ICV التي يوفرها حارس البوابة أولاً، وترفض مواصلة التسجيل إذا كانت القيمة ICV ليست القيمة المتوقعة.

يعتبر استعمال نصف مفتاح غير مشفر مفيداً لحارس البوابة حيث يستطيع هذا الأخير إعادة استعمال المفتاح الخصوصي المناظر مع نقاط طرفية متعددة. وقد يستحيل ذلك إذا وزع المفتاح ذاته بطريقة مشفرة بواسطة أسرار متقاسمة عديدة أو بأرقام PIN. ويمكن لمراقب طرف ثالث أن يجمع أمثلة لنصف المفتاح المشفر بواسطة رقمين PIN مختلفين، ثم يبحث عن تركيبات ممكنة لرقمين PIN لكي يتبين الزوج الذي سمح بالحصول على نصف المفتاح ذاته بعد فك تشفيره. وَلْنَقُلْ إن هناك 10^8 أرقام PIN ممكنة، عندئذ توجد 10^{16} تركيبات ممكنة يتوجب محاولتها. وهي مشكلة مكافئة للبحث عن رقم عشوائي من 54 بتة، وهي ليست متعذرة على الإطلاق وحتى وإن أمكن الحصول على حلول ممكنة عديدة، يمكن تحديد الحل الصائب بسرعة باستعمال ملاحظة ثالثة.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
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 البرامج الإذاعية الصوتية والتلفزيونية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) 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
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التلماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات المعطيات على الشبكة الهاتفية
السلسلة X	شبكات المعطيات والاتصالات بين الأنظمة المفتوحة والأمن
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	لغات البرمجة والخصائص العامة للبرمجيات في أنظمة الاتصالات

طبعت في سويسرا

جنيف، 2006