الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

X.1582

(2014/01)

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

السلسلة X: شبكات البيانات والاتصالات
بين الأنظمة المفتوحة ومسائل الأمن

تبادل معلومات الأمن السيبراني – التبادل المضمون

بروتوكولات النقل المستعملة
لدعم تبادل معلومات الأمن السيبراني

التوصيـــة ITU-T X.1582

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
الدليـــل	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
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.

التوصيـــة ITU-T X.1582

بروتوكولات النقل المستعملة لدعم تبادل معلومات الأمن السيبراني

الملخص

تقدم التوصية ITU-T X.1582 لمحة عامة عن بروتوكولات النقل التي تم اعتمادها وتكييفها لاستعمالها في إطار تبادل معلومات الأمن السيبراني (CYBEX). وتلخص هذه التوصية خصائص تطبيقات النقل وبروتوكولات النقل فضلاً عن الاعتبارات الأمنية.

التسلسل التاريخي

الصيغة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الوحيد*
1.0	ITU-T X.1582	2014-01-24	17	11.1002/1000/12037

الكلمات الرئيسية

معلومات الأمن السيبراني، بروتوكولات تبادل المعلومات، نقل المعلومات.

* للنفاذ إلى التوصية، اطبع الرابط الإلكتروني http://handle.itu.int/ في حقل العنوان بمتصفح الويب الخاص بك، متبوعاً بمعرف الهوية الوحيد للتوصية. مثال: http://handle.itu.int/11.1002/1000/11830-en.

تمهيـــد

الاتحاد الدولي للاتصالات (ITU) 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 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.

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

جدول المحتـــويات

الصفحة

مقدمة

يوجد بالفعل عدد من آليات وبروتوكولات تبادل المعلومات وهي تُستعمل في تبادل معلومات الأمن السيبراني. ومع ذلك، فإن العديد من هذه الآليات إن لم يكن معظمها، مكرس إما للاستعمال الخاص وغير موثّق بصورة جيدة أو غير معروف على نطاق واسع، مما يجعل استعمالها في التبادل العالمي لمعلومات الأمن السيبراني صعباً. أضف إلى ذلك أن معظم تطبيقات التبادل الحالية متاحة بين عدد محدود من شركاء تبادل المعلومات وهي محدودة إما من حيث العدد أو من حيث مجال عمليات الأمن السيبراني.

وبغية دعم تبادل معلومات الأمن السيبراني على نحو أكثر عالمية وقابلية للتشغيل البيني بين مجموعة أوسع من مجالات التطبيق الممكنة، تقدم عملية *"تبادل معلومات الأمن السيبراني"* (CYBEX) لمحة عامة عن مجموعة من المواصفات المحددة حسب البروتوكول التي تدعم عولمة تبادل معلومات الأمن السيبراني بين أكبر مجموعة ممكنة من مجالات التطبيق.

التوصيـــة ITU-T X.1582

بروتوكولات النقل المستعملة لدعم تبادل معلومات الأمن السيبراني

1 مجال التطبيق

تقدم هذه التوصية لمحة عامة عن بروتوكولات نقل وتبادل المعلومات التي تم تقييسها من أجل و/أو في الاستعمال الحالي في مجال تطبيق نقل معلومات الأمن السيبراني وتبادلها والتي تم اعتمادها وتكييفها لاستعمالها في إطار سلسلة التوصيات ITU-T X.1500.

وتطبق هذه التوصية أساساً على مصممي ومنفذي التطبيقات الذين تقع عليهم مسؤولية تمكين نقل معلومات الأمن السيبراني وتبادلها على المستويات المحلية والإقليمية والعالمية.

2 المراجع

تحتوي التوصيات التالية الصادرة عن قطاع تقييس الاتصالات وغيرها من المراجع بعض الأحكام التي تشكل أحكاماً في هذه التوصية، بموجب الإحالة إليها في النص. ففي تاريخ نشر هذه التوصية كانت الطبعات المذكورة لا تزال صالحة. وبما أن جميع التوصيات والمراجع الأخرى تخضع للمراجعة، لذا يتعيَّن على مستعملي هذه التوصية السعي إلى تطبيق أحدث صيغ التوصيات والمراجع الأخرى الواردة أدناه. ويجري بانتظام نشر قائمة بالتوصيات السارية التي تصدر عن القطاع. والإحالة داخل هذه التوصية إلى وثيقة ما لا يضفي على هذه الوثيقة صفة توصية.

[ITU-T X.1500] التوصية ITU-T X.1500 (2011)، *نظرة عامة على تبادل معلومات الأمن السيبراني (CYBEX)*.

3 التعاريف

1.3 مصطلحات معرَّفة في وثائق أخرى

تستعمل هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 الأمن السيبراني [التوصية b-ITU-T X.1205]: مجموع الأدوات والسياسات ومفاهيم الأمن وتحفظات الأمن والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وآليات الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية وأصول المؤسسات والمستعملين. وتشمل أصول المؤسسات والمستعملين أجهزة الحوسبة الموصولة بالشبكة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات ومجموع المعلومات المنقولة و/أو المحفوظة في البيئة السيبرانية. ويسعى الأمن السيبراني إلى تحقيق خصائص أمن أصول المؤسسة والمستعملين والحفاظ عليها وحمايتها من المخاطر الأمنية ذات الصلة في البيئة السيبرانية. وتضم الأهداف العامة للأمن التيسر والسلامة (التي قد تضم الاستيقان وعدم الرفض والسرية).

ملاحظة – (ليست جزءاً من التوصية [b-ITU-T X.1205]) قد تفرض بعض اللوائح والتشريعات الوطنية المحددة استعمال آليات لحماية المعلومات التي تؤدي إلى تعرف هوية أصحابها.

2.1.3 بروتوكول التبادل [ITU-T X.1500]: مجموعة من القواعد والأنساق التقنية تعمل على تنظيم تبادل المعلومات بين كيانين أو أكثر.

2.3 مصطلحات معرَّفة في هذه التوصية

تعرف هذه التوصية المصطلح التالي:

1.2.3 كيان الأمن السيبراني: أي كيان يملك معلومات الأمن السيبراني أو يسعى إلى الحصول عليها.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

BEEP بروتوكول تبادل موسع الفدرات *(Blocks Extensible Exchange Protocol)*

CAPEC تعداد نماذج الاعتداءات الشائعة وتصنيفها *(Common Attack Pattern Enumeration and Classification)*

CYBEX تبادل معلومات الأمن السيبراني *(Cybersecurity Information Exchange)*

DDoS الرفض الموزع للخدمة *(Distributed Denial of Service)*

EVCERT شهادة الصلاحية الممتدة *(Extended Validation Certificate)*

HTTP بروتوكول نقل النص المترابط *(Hypertext Transfer Protocol)*

HSTS أمن نقل صارم لبروتوكول نقل النص المترابط *(Hypertext transfer protocol Strict Transport Security)*

IODEF نسق تبادل وصف الشيء العرضي *(Incident Object Description Exchange Format)*

MIME تمديدات بريد الإنترنت متعدد الأغراض *(Multi-purpose Internet Mail Extensions)*

RID الدفاع بين الشبكات في الوقت الفعلي *(Real-time Inter-network Defense)*

RSS طريقة بسيطة لنشر المعلومات *(Really Simple Syndication)*

SCTP بروتوكول إرسال التحكم في قطار البتات *(Stream Control Transmission Protocol)*

SOAP بروتوكول النفاذ البسيط إلى الأشياء *(Simple Object Access Protocol)*

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

TLS أمن طبقة النقل *(Transport Layer Security)*

UDP بروتوكول وحدات نقل بيانات المستعمل *(User Datagram Protocol)*

URI معرف الموارد الموحد *(Uniform Resource Identifier)*

XML لغة الوسم القابلة للتمديد *(extensible Markup Language)*

5 الاصطلاحات

لا توجد.

6 بروتوكولات النقل المستعملة لدعم تبادل معلومات الأمن السيبراني

1.6 تطبيق النقل

يشمل تبادل معلومات الأمن السيبراني طائفة واسعة من سيناريوهات الاستعمال التي يمكن تنفيذها مع العديد من بروتوكولات النقل، مع خصائص فريدة لكل منها. ومن أجل التمييز بين هذه الخصائص، يرد فيما يلي وصف لأربعة تطبيقات تمثيلية للنقل.

1.1.6 نشر المعلومات

يمكن لكيانات الأمن السيبراني أن تنشر المعلومات على أساس غير تمييزي. ويمكن تحقيق ذلك من خلال البروتوكولات المتاحة على نطاق واسع من أجل التغذية بالبيانات مثل الطريقة البسيطة لنشر المعلومات (RSS). ولأغراض نشر المعلومات هذه، يمكن تقديم مجموعة المعلومات ذاتها إلى أي شخص بدون ترشيح البيانات أو تكييفها لكي تناسب طرفاً بعينه.

2.1.6 انشر–اشترك

يمكن لأحد كيانات الأمن السيبراني أن يشترك لدى مقدم معلومات معين على أساس ثنائي، ويمكن لمقدم المعلومات أن يوفر بيانات ذات صلة مكيفة خصيصاً للطرف الطالب المحدد. وفي مثل هذا السيناريو، يمكن لمقدم الخدمة أن يتصرف كوسيط بين ناشر المعلومات (مثلاً، موردو البرمجيات) والمشترك. وتتطلب خدمات انشر–اشترك هذه الترشيح على مستوى الوسيط الذي يتطلب بدوره التعداد والاستعلام مثل تعداد الأصول أو الاستعلام للحصول على المعلومات ذات الصلة.

3.1.6 تبادل مضمون للمعلومات

يمكن لكيانات الأمن السيبراني ذات القدرات المتماثلة أن تتبادل المعلومات فيما بينها من أجل زيادة التغطية أو التعجيل بالاستجابة للحوادث. ويمثل النسق الخاص بتبادل وصف الشيء العرضي (IODEF) [b-ITU-T X.1541] والدفاع بين الشبكات في الوقت الفعلي (RID) [b-ITU-T X.1580] بروتوكولين للإبلاغ عن التفاصيل. وستحدد كيانات الأمن السيبراني النقاط الطرفية المشاركة في الاتصال وستحتاج إلى الاستيقان والضمان فيما بينهما. ولأغراض هذا التبادل المضمون، قد يتعين على كل كيان أمن سيبراني بدء الاتصال بالكيانات الأخرى. ويمكن تحقيق ذلك من خلال بروتوكولات النقل ثنائي الاتجاه.

4.1.6 إثبات حيازة المعلومات

قد ترغب كيانات الأمن السيبراني في الاتصال بالأطراف المعنية التي رصدت أحد الأحداث أو الحوادث العرضية، دون الكشف عن التفاصيل لكيانات مجاورة أخرى غير متأثرة. ويمكن تحقيق ذلك من خلال نوع من أنواع بروتوكولات التجفير، مثلاً من خلال تقاطع مجموعات الحفاظ على السرية [b-Kissner]. ويقوم بروتوكول التجفير هذا أساساً بتبادل إثبات حيازة المعلومات بدون تبادل المعلومات ذاتها، مما يضمن سرية المعلومات الحساسة. ويمكن تنفيذ بروتوكولات التجفير هذه على رأس بروتوكولات النقل ثنائي الاتجاه.

2.6 اعتبارات بروتوكولات النقل

يمكن للنقاط الطرفية للاتصال أن تعمل على أساس لا تناظري أو كأقران تبعاً للأدوار المسندة إلى كيانات الأمن السيبراني.

وفي حالة نموذجية حيث يكون دورا كل من النقطتين الطرفيتين ثابتين بطريقة لا تناظرية، تعتبر بروتوكولات "الطلب – الاستجابة" مناسبة نظراً لأن أحد طرفي الاتصال هو الذي يستهل الاتصال دائماً. وعندما تعمل النقطتان الطرفيتان كأقران، يمكن لكلتا النقطتين بدء الاتصال، ومن ثم تعتبر البروتوكولات ثنائية الاتجاه مناسبة.

1.2.6 بروتكولات الطلب–الاستجابة

في بروتوكولات الطلب–الاستجابة، يكون العميل هو بادئ التوصيل ويكون المخدم هو المستجيب. وفي هذه الحالة، يكون تدفق المعلومات غير ملائم من حيث التمييز بين العميل والمخدم؛ إذ يمكن للعميل أن يوفر المعلومات أو أن يكيف المعلومات اعتماداً على فصل الأدوار.

ومع بروتوكولات الطلب–الاستجابة، قد لا يكون بوسع المخدمات نشر المعلومات للعملاء في الوقت المناسب، إلا إذا استمر العملاء في استطلاع وضع المخدمات. وبعبارة أخرى، فإن العميل هو بادئ عملية تبادل المعلومات والمخدم هو الطرف المستجيب لتبادل المعلومات.

ويلخص الجدول 1 بروتوكولات الطلب–الاستجابة المتاحة.

الجدول 1 – بروتوكولات الطلب–الاستجابة المتاحة لنقل المعلومات وتبادلها

اسم البروتوكول	الخصائص	المراجع
بروتوكول نقل النص المترابط (HTTP)	يوفر بروتوكول نقل النصوص المترابطة آليات أساسية لاسترجاع المعلومات من المستجيب أو إرسالها إليه. ويمكن استعمال هذا البروتوكول لتبادل أي نوع من المعلومات التي يمكن تحديدها بواسطة معرفات الهوية الموحد للموارد (URI) والتي يمكن تحديد نمطها بأنماط تمديدات بريد الإنترنت متعدد الأغراض (MIME).	[b-IETF RFC 2616]
بروتوكول النفاذ البسيط إلى الأشياء (SOAP)	يقوم بروتوكول النفاذ البسيط إلى الأشياء على بروتوكول نقل النصوص المترابطة لتيسير نقل أزواج النعوت–القيم. ويستعمل مخطط لغة الوسم القابلة للتمديد (XML) لتحديد نمط النعوت والقيم.	[b-SOAP]

2.2.6 البروتوكولات ثنائية الاتجاه

في البروتوكولات ثنائية الاتجاه، يمكن لكلا الطرفين أن يتصرفا بصفة الطرف البادئ بتبادل المعلومات. ويمكن أن يكون هذا البروتوكول لا تناظري أي أن يعتبر أحد الطرفين عميلاً ويتعين عليه بدء التوصيل. ويمكن أن يكون البروتوكول تناظرياً، أيضاً أي أن كلا الطرفين يمكن لهما بدء التوصيل حسب رغبة كل منهما.

ومع البروتوكولات ثنائية الاتجاه، يكون تبادل المعلومات في الوقت المناسب ممكناً بدون أن ينطوي ذلك على نفقات كبيرة في عمليات الاستطلاع الدورية. وفوائد البروتوكولات ثنائية الاتجاه لا تقتصر على حالات الاستعمال التناظري حيث تتبادل كيانات متعددة للأمن السيبراني المعلومات فيما بينها؛ حيث توجد هناك فوائد من حيث إمكانية التوسع عندما يتعين نشر المعلومات عبر عدد كبير من عقد العملاء.

ويمكن أيضاً إنشاء توصيل ثنائي الاتجاه من زوج من توصيلي طلب–استجابة مستقلين. ويتطلب هذا التركيب أن تعمل كلتا النقطتين الطرفيتين كعميل ومخدم، مما قد يؤدي إلى ظهور قضايا إضافية بخصوص تنفيذ البرمجيات.

ويلخص الجدول 2 البروتوكولات ثنائية الاتجاه المتاحة.

الجدول 2 – البروتوكولات ثنائية الاتجاه المتاحة لنقل المعلومات وتبادلها

اسم البروتوكول	الخصائص	المراجع
بروتوكول تبادل موسع الفدرات (BEEP)	بروتوكول التبادل موسع الفدرات قادر على استيعاب النقاط الطرفية التناظرية واللا تناظرية. ويمكن لكلا الطرفين أن يتصرفا بصفة بادئ التوصيل والمستجيب.	[b-IETF RFC 3080]
WebSocket	يقوم بروتوكول WebSocket على بروتوكول نقل النصوص المترابطة، ومن ثم، يكون العميل هو بادئ التوصيل دائماً. وعلى الرغم من التمييز بين العميل والمخدم، يمكن للمخدم أن يباشر تفاعل البروتوكول من خلال التوصيل بمبادرة من العميل.	[b-IETF RFC 6455]

3.6 الاعتبارات الأمنية

من بين بروتوكولات نقل معلومات الأمن السيبراني، ينبغي أن تخضع البروتوكولات المدعومة بمتصفحات الويب إلى تحليل أمني دقيق قبل اعتمادها نظراً لأن بعض متصفحات الويب توفر مستويات بدائية للفصل بين المخطوطات المنفذة عبر المواقع الإلكترونية والتي غالباً ما تكون ذات مستويات متفاوتة من حيث جدارتها بالثقة. وبينما قد يستخدم أحد كيانات الأمن السيبراني الصالحة متصفحات ويب لتبادل المعلومات، يمكن استخدام نفس المتصفح للتنقل عبر مواقع إلكترونية

غير موثوق بها، قد تستضيف شفرة يُحتمل أن تكون ضارة بالنسبة لنقطة طرفية CYBEX معنية. ومن بين هذه التهديدات، تزوير الطلب عبر المواقع (CSRF)؛ (Cross-Site Request Forgery؛ CAPEC ID 62) ودس مخطوطات مغرضة في مواقع الويب (XSS) (Cross Site Scripting؛ CAPEC ID 63) وهما من المظاهر المعروف عنها حالياً أنها تغير بشكل فعال مبدأ الفصل بين المواقع الإلكترونية ذات مستويات الثقة المختلفة.

وتتاح التدابير المضادة لهذه التهديدات كتمديدات لبروتوكول نقل النصوص المترابطة (HTTP)، على النحو الملخص في الجدول 3. وقد تختلف التمديدات المدعومة تبعاً للعلامة التجارية لمتصفحات الويب وإصدارها.

الجدول 3 – التمديدات المتاحة للبروتوكول HTTP لتحسين الأمن

اسم البروتوكول	الخصائص	المراجع
سياسة أمن المحتوى (CSP)	يمكن لبروتوكول سياسة أمن المحتوى أن يقصر مصادر الأشياء المدمجة، بما في ذلك تنفيذ مخطوطات بشكل دينامي، على مجموعة محددة مسبقاً من المواقع الإلكترونية.	[b-CSP]
أمن النقل الصارم للبروتوكول HTTP (HSTS)	يمكن لأمن النقل الصارم لبروتوكول نقل النصوص المترابطة أن يقصر تفاعلات البروتوكول اللاحقة على قناة آمنة مثل أمن طبقة النقل (TLS) لفترة معينة من الوقت.	[b- IETF RFC 6797]
HttpOnly	تقيد برمجية HttpOnly البرامج المشغلة ضمن متصفحات الويب من النفاذ إلى بيانات اعتماد الاستيقان، مثلاً استعمال بصمات "cookies".	[b- IETF RFC 6265]
بصمات المصدر	تمنع بصمات المصدر مواقع إلكترونية أخرى من تدمير البصمات التي يضعها مخدم الويب المصدر؛ وتكون بصمات المصدر قابلة للتعديل من مصدر دقيق فقط.	[b-Bortz]

يمكن أن تتعرض بروتوكولات طبقة التطبيق الأخرى لتهديدات شبيهة، نظراً لتمكن متصحفات الويب الحديثة من تنفيذ برامج اعتباطية داخل البرامج المساعدة المرتبطة بالمتصفح مثل برامج Java وFlash scripts، التي يمكن أن تُستخدم بدورها لتحقيق تفاعلات البروتوكول. وهكذا، ينبغي للنقاط الطرفية CYBEX أن تتفادى استضافة وتشغيل برمجيات من مصادر غير موثوقة، بما في ذلك تلك المتاحة في المواقع الإلكترونية. وفي حال اعتُبر إنفاذ النقطة الطرفية CYBEX الأخرى غير واقعي بسبب الطابع غير التمييزي لتطبيق معين، يلزم قياس المخاطر الجارية والتحكم فيها.

4.6 اعتبارات النقل وطبقة الدورة

نظراً لأنه يتعين على النقاط الطرفية CYBEX حماية سلامة قناة الاتصال، يُشجع استخدام بروتوكول التحكم في الإرسال (TCP) أو بروتوكول إرسال التحكم في قطار البتات (SCTP) [b-IETF RFC 4960]. وإضافة إلى ذلك، ينبغي للمسؤولين عن تنفيذ النقاط الطرفية CYBEX النظر في الحماية من هجمات رفض الخدمة بواسطة مجموعة متنوعة من الوسائل مثلاً من خلال بصمات SYN [b-IETF RFC 4987] (SYN Cookies) وغيرها من التدابير المضادة لهجمات الرفض الموزع للخدمة (DDoS) [b-Mirkovic]. ويمكن للمسؤولين عن التنفيذ زيادة تعزيز سلامة قناة الاتصال من خلال شفرات استيقان الرسائل على النحو المبين في خيار استيقان بروتوكول التحكم في الإرسال (TCP) [b-IETF RFC 5925] والقطع المستيقن منها (Authenticated Chunks) لبروتوكول إرسال التحكم في قطار البتات (SCTP) [b-IETF RFC 4895].

ويرد في المعيار [b-IETF RFC 5062].التهديدات المعروفة ضد البروتوكول SCTP إلى جانب التدابير المضادة المرتبطة بها. وينبغي ألا يُستعمل البروتوكول UDP من أجل الحد من مخاطر الهجمات الانعكاسية [b-Paxson].

وبغية تحقيق سرية الاتصالات، يُشجع استعمال أمن طبقة النقل [b-IETF RFC 5246] و[b-IETF RFC 3436]. وإذا اعتُبر أن ضمان هوية النقطة الطرفية ضرورياً، يُشجع استعمال شهادة الصلاحية الممتدة (EVCERT) [b-EVCERT].

بيبليوغرافيـــا

[b-ITU-T X.1205] Recommendation ITU-T X.1205 (2008), *Overview of cybersecurity.*

[b-ITU-T X.1541] Recommendation ITU-T X.1541 (2012), *Incident object description exchange format.*

[b-ITU-T X.1544] Recommendation ITU-T X.1544 (2013), *Common attack pattern enumeration and classification.*

[b-ITU-T X.1580] Recommendation ITU-T X.1580 (2012), *Real-time inter-network defense*.

[b-Bortz] Andrew Bortz, Adam Barth and Alexei Czeskis, Origin Cookies: Session Integrity for Web Applications, W2SP 2011.

[b-CSP] W3C, Content Security Policy 1.0.
http://www.w3.org/TR/CSP/

[b-EVCERT] CA/Browser Forum, *Guidelines for the Issuance and Management of Extended Validation Certificates*, Ver. 1.3.

[b-IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol* – HTTP/1.1.

[b-IETF RFC 3080] IETF RFC 3080 (2001), *The Blocks Extensible Exchange Protocol Core*.

[b-IETF RFC 3436] IETF RFC 3436 (2002), *Transport Layer Security over Stream Control Transmission Protocol*.

[b-IETF RFC 4895] IETF RFC 4895 (2007), *Authenticated Chunks for the Stream Control Transmission Protocol*.

[b-IETF RFC 4960] IETF RFC 4960 (2007), *Stream Control Transmission Protocol*.

[b-IETF RFC 4987] IETF RFC 4987 (2007), *TCP SYN Flooding Attacks and Common Mitigations*.

[b-IETF RFC 5062] IETF RFC 5062 (2007), *Security Attacks Found Against the Stream Control Transmission Protocol (SCTP) and Current Countermeasures*.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

[b-IETF RFC 5925] IETF RFC 5925 (2010), *The TCP Authentication Option*.

[b-IETF RFC 6265] IETF RFC 6265 (2011), *HTTP State Management Mechanism*.

[b-IETF RFC 6455] IETF RFC 6455 (2011), *The WebSocket Protocol*.

[b-IETF RFC 6797] IETF RFC 6797 (2012), *HTTP Strict Transport Security*.

[b-Kissner] Lea Kissner and Dawn Song, *Privacy-Preserving Set Operations*, CRYPTO 2005.

[b-Mirkovic] Jelena Mirkovic and Peter Reiher, *A Taxonomy of DDoS Attack and DDoS Defense Mechanisms*, ACM SIGCOMM Computer Communication Review, 34(2), April 2004.

[b-Paxson] Vern Paxson, *An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks*, ACM SIGCOMM Computer Communication Review, 31(3), July 2001.

[b-SOAP] W3C, *Simple Object Access Protocol*.
SOAP Version 1.2 Part 1: Messaging Framework (2007).
SOAP Version 1.2 Part 2: Adjuncts (2007).

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 تلفزيونية وبرامج صوتية 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 البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2014