الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1279

(2020/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – إدارة الهوية

إطار للاستيقان المعزز باستخدام القياسات البيومترية عن بُعد مع آليات الكشف عن حالات الانتحال

التوصية ITU-T X.1279

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 (1)	
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 (1)	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 (2)	
اتصالات الطوارئ	X.1309–X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1319–X.1310
أمن شبكة الكهرباء الذكية	X.1339–X.1330
البريد المعتمد	X.1349–X.1340
أمن إنترنت الأشياء (IoT)	X.1369–X.1360
أمن أنظمة النقل الذكية (ITS)	X.1389–X.1370
أمن سجل الحسابات الموزع	X.1429–X.1400
أمن سجل الحسابات الموزع	X.1449–X.1430
البروتوكولات الأمنية (2)	X.1459–X.1450
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
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680
الاتصالات الكمومية	
المصطلحات	X.1701–X.1700
مولّد الأعداد العشوائية الكمومية	X.1709–X.1702
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1711–X.1710
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1719–X.1712
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1729–X.1720
أمن البيانات	
أمن البيانات الضخمة	X.1759–X.1750
أمن شبكات الجيل الخامس	X.1819–X.1800

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

التوصية ITU-T X.1279

إطار للاستيقان المعزز باستخدام القياسات البيومترية عن بُعد مع آليات الكشف عن حالات الانتحال

ملخص

تقدم التوصية ITU-T X.1279 إطاراً معمارياً للاستيقان المعزز باستخدام القياسات البيومترية عن بُعد للكشف عن حالات الانتحال. وتحلل هذه التوصية التهديدات التي تواجهها حلول الاستيقان التقليدية باستخدام القياسات البيومترية عن بُعد وتوصف إطاراً معمارياً وتدفقات عملية الاستيقان والاعتبارات الأمنية للاستيقان المعزز باستخدام القياسات البيومترية عن بُعد مع آليات الكشف عن حالات الانتحال.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1279	2020-09-03	17	11.1002/1000/14261

مصطلحات أساسية

الكشف عن حالات الانتحال، الاستيقان المعزز، القياسات البيومترية عن بُعد.

* 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 "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" 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/.

© ITU 2021

جميع الحقوق محفوظة. لا يجوز استنساخ أي جزء من هذه المنشورة بأي وسيلة كانت إلا بإذن خطي مسبق من الاتحاد الدولي للاتصالات.

جدول المحتويات

الصفحة

مقدمة

تستخدم تكنولوجيا الاستيقان بالقياسات البيومترية عن بُعد كثيراً في مجالات مختلفة تتطلب مستوى رفيع من الموثوقية مثل الأعمال المصرفية الإلكترونية وخدمات المشتريات. ومن الضروري بذل الجهود من أجل تطوير نظام أمني يمكن أن يواكب بشكل استباقي التهديدات الأمنية المحتملة من أجل ضمان أمن بيانات القياسات البيومترية عن بُعد.

وتحلل هذه التوصية التهديدات التي تواجهها حلول الاستيقان التقليدية باستخدام القياسات البيومترية عن بُعد وتقترح إطاراً للاستيقان المعزز باستخدام القياسات البيومترية عن بُعد مع الكشف عن حالات الانتحال (ASD). ويرمي الكشف ASD إلى تحديد أن المستعمل الذي يرسل طلب الاستيقان بالقياسات البيومترية عن بُعد هو الشخص الفعلي الذي يمتلك البيانات البيومترية. ويمكن استخدام الكشف ASD جنباً إلى جنب مع التحقق باستخدام القياسات البيومترية عن بُعد لتعزيز الأمن وتجنب البيانات البيومترية المزيفة. ووظيفة الكشف ASD يمكن تصميمها بحيث تعزز الأمن وتمنع تسرب البيانات البيومترية.

التوصية ITU-T X.1279

إطار للاستيقان المعزز باستخدام القياسات البيومترية عن بُعد مع آليات الكشف عن حالات الانتحال

1 مجال التطبيق

تقدم هذه التوصية إطاراً معمارياً للاستيقان المعزز باستخدام القياسات البيومترية عن بُعد مع قدرات الكشف عن حالات الانتحال. وتحلل هذه التوصية التهديدات التي تواجهها حلول الاستيقان التقليدية باستخدام القياسات البيومترية عن بُعد وتوصف إطاراً معمارياً وتدفقات عملية الاستيقان والاعتبارات الأمنية للاستيقان المعزز باستخدام القياسات البيومترية عن بُعد مع آليات الكشف عن حالات الانتحال.

والإطار المعماري الموصف في هذه التوصية يمكن استخدامه كتوجيه للمساعدة في عمليات نشر حلول الاستيقان المعزز بالقياسات البيومترية عن بُعد باستخدام وظائف الكشف عن حالات الاحتيال.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل، من خلال الإشارة إليها في هذا النص، أحكاماً تتعلق بهذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية وقت نشر هذه التوصية. وبما أن جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، يُرجى من مستعملي هذه التوصية السعي إلى تقصّي إمكانية تطبيق أحدث طبعة للتوصيات وغيرها من المراجع الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات سارية الصلاحية. والإشارة إلى وثيقة في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T X.1086] التوصية ITU-T X.1086 (2008)، *إجراء الحماية البيومترية عن بُعد – الجزء 1: مبدأ توجيهي للتدابير التقنية والإدارية المضادة في أمن البيانات البيومترية*.

[ITU-T X.1087] التوصية ITU-T X.1087 (2016)، *التدابير التقنية والتشغيلية المضادة في تطبيقات القياس الحيوي التي تستخدم الأجهزة المتنقلة*.

[ISO/IEC 24745] المعيار ISO/IEC 24745:2011، *تكنولوجيا المعلومات – تقنيات الأمن – حماية المعلومات البيومترية*.

3 التعاريف

1.3 تعاريف معرفة في وثائق أخرى

تستخدم هذه التوصية التعاريف التالية المعرفة في وثائق أخرى:

1.1.3 الاستيقان [b-ISO/IEC 2382-37]: عملية إثبات أو بيان عدم الشك.

2.1.3 بيومترية (صفة) [b-ISO/IEC 2382]: تتعلق بمجال القياسات البيومترية.

3.1.3 الاستحواذ البيومتري [b-ISO/IEC 2382-37]: الحصول على والتسجيل، في صورة قابلة للاستعادة، إشارة (إشارات) ذات خاصية (خصائص) بيومترية من فرد (أفراد) مباشرة، أو من ممثل (ممثلين) للخاصية (الخصائص) البيومترية.

4.1.3 الخاصية البيومترية [b-ISO/IEC 2382-37]: خاصية بيولوجية أو سلوكية لفرد، يمكن تستخلص منها السمات البيومترية المتكررة المميزة لأغراض التعرف البيومتري.

5.1.3 البيانات البيومترية [b-ISO/IEC 2382-37]: عينة بيومترية أو تجميع لعينات بيومترية في مرحلة من مراحل المعالجة، مثل المرجع البيومتري، أو المسبار البيومتري، أو السمة البيومترية أو الخاصية البيومترية.

6.1.3 السمة البيومترية [b-ISO/IEC 2382-37]: أرقام أو رموز تستخلص من عينات بيومترية وتستخدم لأغراض المقارنة.

7.1.3 التعرف البيومتري/القياسات البيومترية [b-ISO/IEC 2382-37]: التعرف الأوتوماتي على الأفراد استناداً إلى خصائصهم البيولوجية والسلوكية.

8.1.3 قاعدة البيانات المرجعية البيومترية [b-ISO/IEC 2382-37]: قاعدة بيانات لسجلات البيانات المرجعية البيومترية.

9.1.3 النموذج البيومتري [b-ISO/IEC 19784-1]: مجموعة من السمات البيومترية المخزنة التي تقارن مباشرةً بسمات بيومترية لعيِّنة تعرف بيومترية

10.1.3 التحقق البيومتري [b-ISO/IEC 2382-37]: عملية تأكيد ادعاء بيومتري من خلال مقارنة بيومترية

11.1.3 مقارنة (مواءمة) [b-ISO/IEC 19784-1]: تقدير أو حساب أو قياس التشابه أو الاختلاف بين عينات/سمات /نماذج/مراجع تعرف بيومترية.

12.1.3 قرار المقارنة [b-ISO/IEC 19784-1]: تحديد ما إذا كان لعينات ومراجع التعرف البيومتري نفس المصدر البيومتري استناداً إلى درجات المقارنة أو سياسات تحديد القرار، بما في ذلك العتبات، وربما مدخلات أخرى.

13.1.3 جهاز متنقل [b-ISO 18461]: جهاز حاسوبي محمول يتضمن عادةً شاشة باللمس، ووسيلة لإدخال البيانات، قلم و/أو لوحة مفاتيح وتوصيلة بالإنترنت.

14.1.3 مستعمِل [b-ISO/IEC 2382-37]: أي شخص أو منظمة يتفاعل أو تتفاعل بطريقة ما مع نظام بيومتري.

15.1.3 القياسات البيومترية عن بُعد [b-ITU-T X.1081]: تطبيق القياسات البيومترية في مجال الاتصالات.

2.3 تعاريف معرفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 الكشف عن حالات الانتحال: عملية كشف ومنع انتحال صفة نظام بيومتري من خلال إجراءات غير شرعية.

2.2.3 التمويه: تصرف متعمد لاستحداث شفرة مصدر أو آلة يصعب على الإنسان فهمها. وتعتمد هذه التقنية على مجموعة من التحولات التي تغير التشغيل الواضح للبرمجية دون تغيير النتائج. وينبغي للبرنامج المموه أن يعطي نفس النتائج تماماً كأي برنامج غير مموه.

ملاحظة – التمويه تقنية تستعمل عادةً لإخفاء معنى بعض البرمجيات بإعادة ترتيب العمليات، ولكنها يمكن أن تستعمل أيضاً لإضافة علامات مائية ضعيفة للشفرة. وفي الحالتين، تعتمد الخوارزميات على مجموعة من التحولات التي تغير التشغيل الواضح للبرمجية دون تغيير النتائج. وينبغي للبرنامج المموه أن يعطي نفس النتائج تماماً كأي برنامج غير مموه. [b-Disappearing Cryptography].

3.2.3 كشف الجودة: قياس لمدى قدرة عينة بيومترية على إنجاز أو تنفيذ قرار مقارنة بيومترية.

4.2.3 الانتحال: ادعاء كيان ما بأنه كيان مختلف، بتقديم صورة مسجلة أو عينة بيانات بيومترية أخرى أو خاصية بيومترية مشتقة اصطناعياً، من أجل انتحال شخصية فرد ما.

ملاحظة – تمت مواءمة هذا التعريف من التوصية [b-ITU M.3016.0].

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

ASD الكشف عن حالات الانتحال *(Anti-Spoofing Detection)*

PII المعلومات المحدِّدة لهوية الشخص *(Personally Identifiable Information)*

PKI البنية التحتية للمفاتيح العمومية *(Public Key Infrastructure)*

SMS خدمة الرسائل القصيرة *(Short Messaging Service)*

SRP كلمة مرور بعيدة مأمونة *(Secure Remote Password)*

5 الاصطلاحات

لا يوجد.

6 التهديدات الأمنية للاستيقان بالقياسات البيومترية عن بُعد والتدابير المضادة

1.6 معلومات أساسية

مع ظهور خدمات الإنترنت، لم تعد آليات الاستيقان القائمة على كلمة المرور التقليدية قادرة على الوفاء بمتطلبات تجارب المستعملين والقدرات الأمنية؛ وأصبحت آليات الاستيقان بالقياسات البيومترية عن بُعد تُستخدم الآن على نطاق أوسع لأسباب تتعلق بالملاءمة والأمن.

ومع ذلك، هناك تحديات ومخاطر في آليات الاستيقان بالقياسات البيومترية عن بُعد، مثلاً، يمكن للمهاجمين استعمال صورة فوتوغرافية أو صورة معدة حاسوبياً أو وجه في شاشة من أجل الاستيقان بالتعرف على الوجه، أو قد يستخدم أحد المستعملين نسخة من عينة بيومترية (مثل بصمة الأصابع أو قزحية العين أو بصمة الصوت) من أجل الاستيقان بالقياسات البيومترية عن بُعد.

2.6 أساليب الاستيقان المرجعية

بالنسبة إلى الاستيقان بالقياسات البيومترية عن بُعد على الأجهزة المتنقلة، هناك أسلوبان مرجعيان أساسيان للاستيقان:

1) أسلوب الاستيقان المحلي: تخزن البيانات البيومترية على جهاز متنقل ويجري التحقق من القياسات البيومترية على جانب الجهاز المتنقل. وترسَل نتائج التحقق من القياسات البيومترية إلى جانب المخدّم.

2) أسلوب الاستيقان عن بُعد: تخزن البيانات البيومترية على المخدّم ويجري التحقق من القياسات البيومترية على جانب المخدّم.

وتركز هذه التوصية على أسلوب الاستيقان عن بُعد.

3.6 التهديدات الأمنية

1.3.6 التهديدات الأمنية على جانب العميل

يواجه الاستيقان بالقياسات البيومترية عن بُعد التهديدات الأمنية التالية على جانب العميل:

- أن يكون العميل وكيلاً مزيفاً أو معدلاً بشفرة خبيثة.
- أن يحاول المهاجمون تعطيل تيسر العميل وسلامته.
- أن يحاول المهاجمون سرقة أو تعديل البيانات البيومترية الملتقطة للعميل.
- قد يستعمل المهاجمون صورة فوتوغرافية أو صورة معدة حاسوبياً أو وجه في شاشة من أجل الاستيقان بالتعرف على الوجه.

– قد يستعمل المهاجمون نسخة من البيانات البيومترية (مثل بصمة الأصابع أو قزحية العين أو بصمة الصوت) من أجل الاستيقان بالقياسات البيومترية عن بُعد.

2.3.6 التهديدات الأمنية على جانب المخدّم

يواجه الاستيقان بالقياسات البيومترية عن بُعد التهديدات الأمنية التالية على جانب المخدّم:

– يمكن للمهاجمين اقتحام المخدّم لتعطيل قاعدة بيانات المخدّم أو تطبيق المخدّم.

– يمكن استبدال البيانات البيومترية أو بيانات النموذج الملتقطة وتسريبها بصورة غير قانونية أو سرقتها أو تبديلها.

– يمكن استبدال البيانات البيومترية أو بيانات النموذج الملتقطة وتسريبها بصورة غير قانونية عند نقل البيانات الملتقطة.

– قد يُستعمل برنامج غير قانوني للمقارنة.

3.3.6 التهديدات الأمنية على قناة الإرسال بين العميل والمخدّم

يواجه الاستيقان بالقياسات البيومترية عن بُعد التهديدات الأمنية التالية على قناة الإرسال بين العميل والمخدّم:

– قد يقوم المهاجمون بالتنصت على الرسائل بين العميل والمخدّم أو تعديلها.

– قد تتعرض البيانات البيومترية للسطو أو التعديل أثناء إرسالها من العميل إلى المخدّم.

4.6 التدابير المضادة

للحد من هذه التهديدات التي تعرقل الاستيقان بالقياسات عن بُعد، يستخدم عادة الكشف عن حالات الانتحال (ASD) جنباً إلى جنب مع التحقق من القياسات البيومترية عن بُعد لأغراض الاستيقان.

وينبغي تنفيذ الكشف ASD في إطار للاستيقان بالقياسات البيومترية عن بُعد. ويمكن استخدام وظيفة الكشف ASD لتحديد أن المستعمل الذي يرسل طلب الاستيقان بالقياسات البيومترية عن بُعد هو الشخص الفعلي الذي يمتلك البيانات البيومترية. ومن شأن ذلك أن يمنع الحالات التي قد يستخدم فيها مستعمل غير قانوني بيانات بيومترية مزيفة أو مستنسخة من أجل الاستيقان بالقياسات البيومترية عن بُعد.

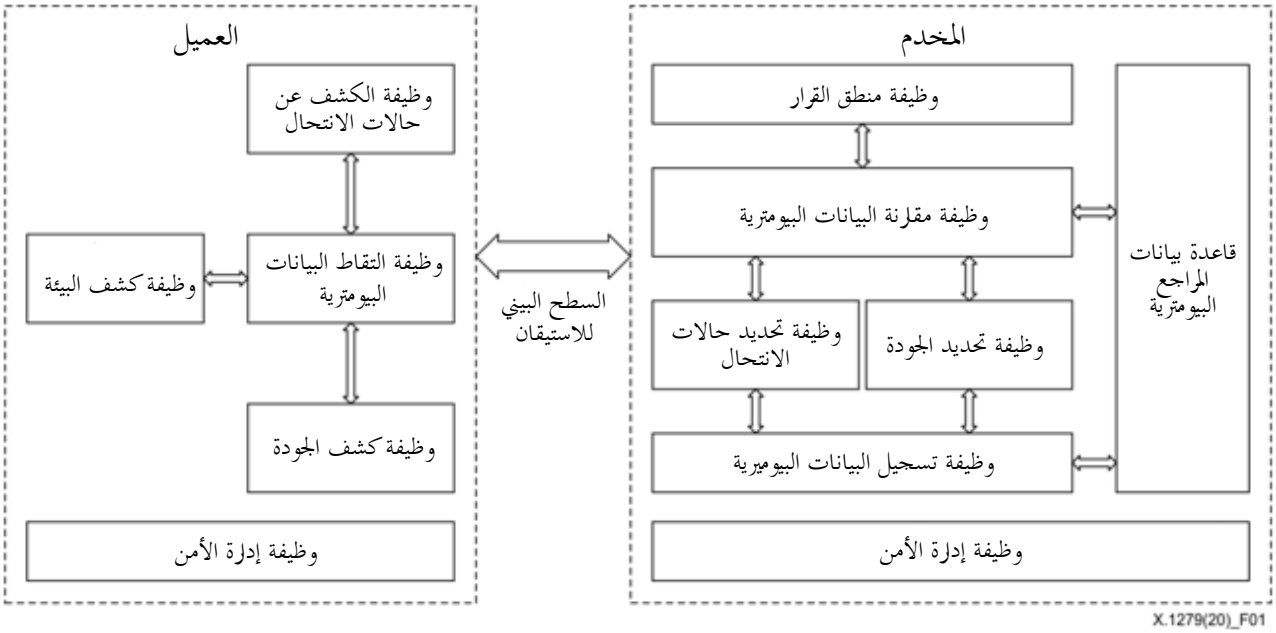
ويمكن استخدام الكشف ASD إلى جانب التحقق من القياسات البيومترية عن بُعد لتعزيز الأمن ومنع الحالات البيومترية المزيفة. فعلى سبيل المثال، يمكن التطبيق المتنقل أن يطلب من المستعمل الإيماء أو هز الرأس أو الغمز أو فتح الفم وما إلى ذلك للتحقق من أن المستعمل هو الشخص الفعلي الذي تقدم بطلب الاستيقان.

وترد في التوصيتين [ITU-T X.1086] و[ITU-T X.1087] تهديدات أمنية وتدابير مضادة إضافية.

7 الإطار المعماري

1.7 المخطط المعماري

يعرض في الشكل 1 المخطط المعماري للاستيقان المعزز باستخدام القياسات البيومترية عن بُعد مع آليات الكشف عن حالات الاحتيال.



الشكل 1 – المخطط المعماري للاستيقان المعزز باستخدام القياسات البيومترية عن بُعد مع آليات الكشف عن حالات الانتحال

ويرد الوصف التفصيلي للوظائف المبينة في هذا المخطط المعماري في الفقرتين 2.7 و3.7.

2.7 وظائف جانب العميل

1.2.7 وظيفة كشف البيئة

هذه الوظيفة هي المسؤولة عن كشف الخصائص البيومترية والظروف الخاصة بالبيئة. فمثلاً، هي تحدد ما إذا كانت خصائص الوجه تفي بشروط الجمع أم لا وما إذا كانت البيئة تفي بشروط جمع البيانات أم لا.

2.2.7 وظيفة التقاط البيانات البيومترية

تستعمل هذه الوظيفة لالتقاط البيانات البيومترية للمستعملين ثم إرسالها إلى وظيفة كشف الجودة المحلية ووظيفة الكشف ASD لمعالجتها وإرسالها بعد ذلك إلى المخدّم عبر السطح البيني للاستيقان من أجل الاستيقان عن بُعد.

3.2.7 وظيفة الكشف عن حالات الانتحال (ASD)

تستعمل هذه الوظيفة لكشف التحركات المتوقعة طبقاً لاستراتيجيات المخدّم أو سياساته مثل الإيماء وهز الرأس والغمز وفتح الفم وما إلى ذلك.

بالرغم من أنه يمكن استخدام الكثير من الطرق للكشف ASD، فإن الكشف عن الجوانب الحية هو الأكثر ملاءمة إلى حدٍ كبير للاستيقان بالقياسات البيومترية عن بُعد على الأجهزة المتنقلة. ويمكن استخدام الاستجابة للتحديات كأداة لتحديد ما إذا كان للعرض الشخصي خواص حياتية يمكن أن تعرض في عمليات الالتقاط للأنظمة الفرعية لالتقاط البيانات البيومترية. فمثلاً، يتوقع للإيماءات البشرية الحية أن تستجيب للتغيرات في شدة إضاءة الضوء المرئي (التحدي) بتغيرات في حجم حدقة العين (الاستجابة المتوقعة إذا كانت حية).

يمكن إجراء الكشف عن الجوانب الحية بالخطوات التالية التي تماثل عمليات التعرف البيومتري:

- التقاط البيانات الخام من أجل الكشف ASD من شخص يستخدم نظاماً فرعياً لالتقاط البيانات البيومترية؛
- استخلاص السمات من بيانات الكشف ASD؛
- مقارنة سمات الكشف ASD بالمعايير.

4.2.7 وظيفة كشف الجودة

تستخدم هذه الوظيفة من أجل التحديد الأولي لجودة البيانات البيومترية طبقاً لاستراتيجيات المخدّم أو سياساته. وتجري هذه الوظيفة تقييماً للجودة على البيانات البيومترية. وتستعمل هذه الوظيفة عادة مع وظيفة الكشف ASD ووظيفة التقاط البيانات البيومترية لإنتاج أفضل البيانات البيومترية من أجل نمذجة هذه البيانات والحكم عليها.

5.2.7 وظيفة إدارة الأمن

وظيفة إدارة الأمن على جانب العميل هي المسؤولية عن إدارة بيانات الاعتماد والبيئة الموثوقة وما إلى ذلك.

3.7 وظائف جانب المخدّم

1.3.7 وظيفة تسجيل البيانات البيومترية

هذه الوظيفة مسؤولة عن القيام بتسجيل البيانات البيومترية. ويمكن تجميع تسجيل البيانات البيومترية من عميل أو دفعة من البيانات تستورد أو تجمع مباشرة من قنوات أخرى مثل قاعدة بيانات وظيفة للهويات ويمكن تحقيق ذلك من نموذج تسجيل بيانات بيومترية.

2.3.7 وظيفة تحديد حالات الانتحال

تُستخدم هذه الوظيفة لتحديد ما إذا كانت البيانات البيومترية مزيفة أو مستنسخة. ويجري المخدّم عملية تحديد متعمقة لحالات الانتحال استناداً إلى نتائج الكشف الأولي من جانب العميل وإلى استراتيجيات المخدّم وسياساته.

ويمكن للمخدم أن يشير على العميل بالكشف عن التحركات المتوقعة طبقاً لاستراتيجيات المخدّم أو سياساته. مثل الإيماء وهز الرأس والغمز وفتح الفم وما إلى ذلك. ويستقبل المخدّم بيانات الخصائص البيومترية المستخلصة من العميل ويستعمل مراجعه البيومترية والاستراتيجية المحددة سلفاً لتحديد ما إذا كان لعرض الشخص خواص تتعلق بالجوانب الحية.

3.3.7 وظيفة تحديد الجودة

تستعمل هذه الوظيفة لتحديد جودة البيانات البيومترية استناداً إلى نتائج الكشف الأولي المأخوذة من جانب العميل وإلى استراتيجيات المخدّم وسياساته. وتقوم وظيفة تحديد الجودة بإجراء تقييم للجودة على البيانات البيومترية المستقبلة. وإذا لم تصل الجودة إلى العتبة المطلوبة، يرفض المخدّم البيانات البيومترية المستقبلة ويطلب من العميل التقاط البيانات البيومترية مجدداً. وإذا ما وافقت الجودة العتبة المطلوبة، ترسل البيانات البيومترية إلى وظيفة مقارنة البيانات البيومترية لإجراء المقارنة.

وقد تختلف قدرات التقاط البيانات البيومترية باختلاف الأجهزة ويمكن تحسين جودة البيانات البيومترية حسب اختلاف الأجهزة. وقد يطلب المخدّم من المستعمل استخدام أجهزة متعددة لالتقاط البيانات البيومترية لتحسين الجودة. إذا تم التقاط المرجع البيومتري من أنواع أجهزة مختلفة ينبغي للمخدم تخزين المراجع البيومترية المختلفة واستعمالها لأنواع الأجهزة المختلفة.

4.3.7 وظيفة مقارنة البيانات البيومترية

تدعم هذه الوظيفة المقارنة والتحقق بين السمات البيومترية المستخلصة من عميل ما والمراجع البيومترية المخزنة على جانب المخدّم. والمراجع البيومترية المخزنة في قاعدة بيانات للمراجع البيومترية تتولد من عملية تسجيل البيانات البيومترية.

5.3.7 وظيفة منطق القرار

تشمل هذه الوظيفة الوسائل المنطقية للقرار من أجل إجراء عمليات الاستيقان المختلفة والتعليق على الإرشادات ذات الصلة للعميل بتنفيذ عمليات الاستيقان المختلفة. ويُتخذ القرار استناداً إلى بيانات إدارة المخاطر، بما في ذلك معلومات برمجيات وعتاد الجهاز المتنقل وبيانات المستعمل. فمثلاً، طبقاً لتحليل البيانات، إذا كان المستعمل النهائي يشكل مخاطر كبيرة، تَطلب وظيفة منطق القرار من العميل إجراء كشف ASD إضافة إلى عمليتي الالتقاط والمقارنة الأساسيتين للبيانات البيومترية.

6.3.7 قاعدة بيانات المراجع البيومترية

تستخدم قاعدة بيانات المراجع البيومترية لتخزين البيانات البيومترية وبيانات إدارة المخاطر واسم المستعمل وهويته وما إلى ذلك.

7.3.7 وظيفة إدارة الأمن

تُستخدم هذه الوظيفة من أجل ضمان التنفيذ المأمون لوظائف المخدّم والتخزين المأمون لقاعدة بيانات المراجع البيومترية، وذلك لتفادي التلاعب في البيانات أو النماذج البيومترية أو سرقتها.

8 تدفقات عملية الاستيقان

1.8 أنواع الرسائل

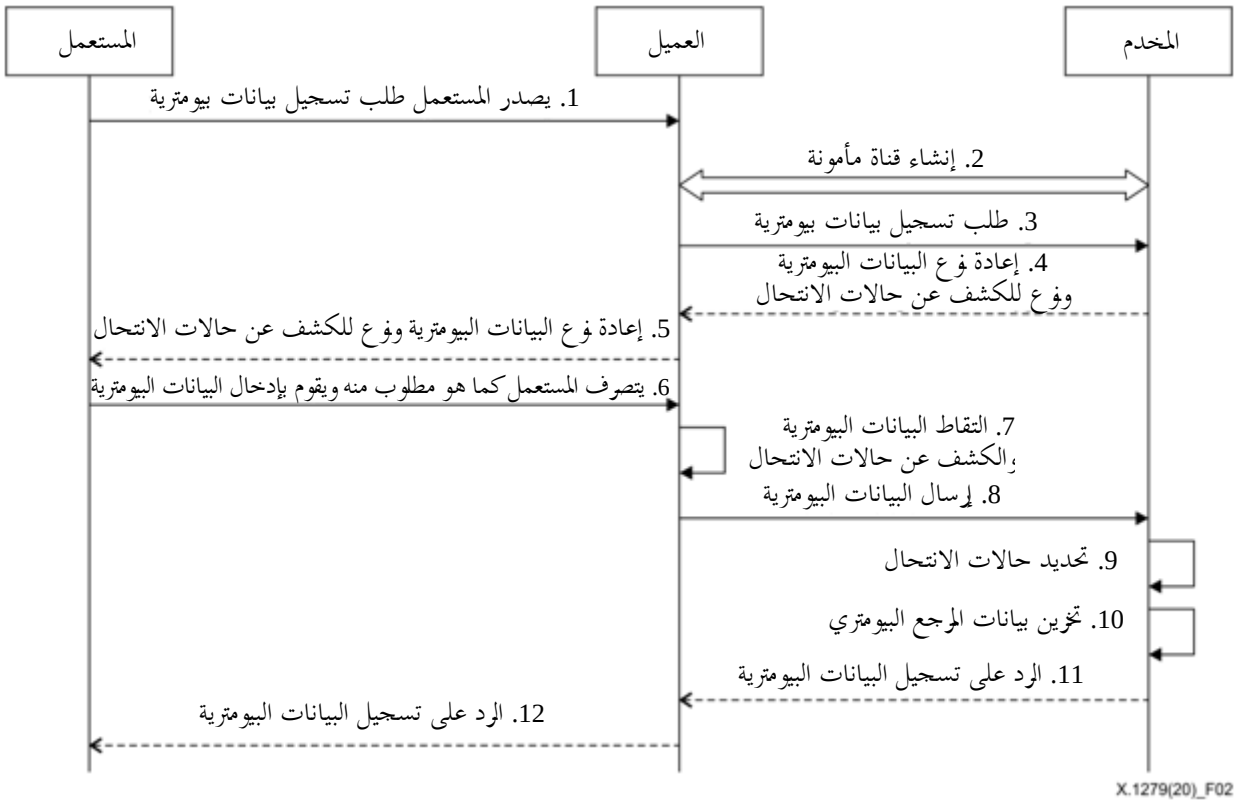
في كدسة بروتوكول الاستيقان بالقياسات البيومترية عن بُعد على الأجهزة المتنقلة، هناك على الأقل ثلاثة أنواع من الرسائل في المراحل المختلفة:

- التسجيل: يسجل المخدّم معلومات تسجيل المستعمل ونمط الاستيقان طبقاً لمفاوضات بين المستعمل والمخدّم.
- الاستيقان: يقارن المخدّم البيانات البيومترية المستقبلة بمرجع بيومتري مسجل.
- إلغاء التسجيل: يُلغى تسجيل المستعمِل من المخدّم. يحذف المخدّم بيانات تسجيل المستعمل.

ملاحظة – هذه التوصية تركز على التحقق عن بُعد. ويقوم العميل بتسجيل مرجع بيومتري في المخدّم. وبعد استلام طلب التحقق، يقارن المخدّم البيانات البيومترية المستقبلة بالمرجع البيومتري المسجَّل.

2.8 تدفقات العمليات

1.2.8 تدفقات عملية التسجيل



الشكل 2 – تدفقات عملية التسجيل

يعرض الشكل 2 تدفقات عملية التسجيل. وفيما يلي أدناه شرح لهذه التدفقات بالتفصيل:

شرط مسبق: يستيقن المستعمل بنجاح مع المخدّم عبر آليات استيقان أخرى مثل معرّف هوية حساب المستعمل/كلمة المرور وشفرة تحقق عبر خدمة الرسائل القصيرة (SMS).

1 يستخدم المستعمل معرّف هوية الحساب/كلمة المرور لتسجيل الدخول وإطلاق طلب تسجيل بيانات بيومترية للعميل؛

2 ينشئ العميل قناة مأمونة مع المخدّم لحماية الدورة وإرسال البيانات، مثلاً: باستخدام بروتوكول كلمة المرور البعيدة المأمونة (SRP)؛

3 يرسل العميل طلب تسجيل البيانات البيومترية مع معرّف هوية حساب المستعمل وبيانات إدارة المخاطر إلى المخدّم؛

4 تعيد وظيفة منطق القرار في المخدّم نوع البيانات البيومترية ونوع الكشف ASD السليمين إلى العميل استناداً إلى تحليل بيانات المخاطر ومنطق الأعمال؛

5 يطلب العميل من المستعمل القيام بالإجراءات المحددة لالتقاط البيانات البيومترية؛

6 يتصرف المستعمل حسب المطلوب منه ويقوم بإدخال البيانات البيومترية الواردة من العميل؛

7 تقوم وظيفة التقاط البيانات البيومترية في العميل بالتقاط البيانات البيومترية ويقوم الكشف ASD بالكشف عن التحركات المتوقعة للمستعمل؛

8 يستخلص العميل السمات البيومترية ويرسلها إلى المخدّم كمرجع بيومتري في القناة المأمونة المنشأة؛

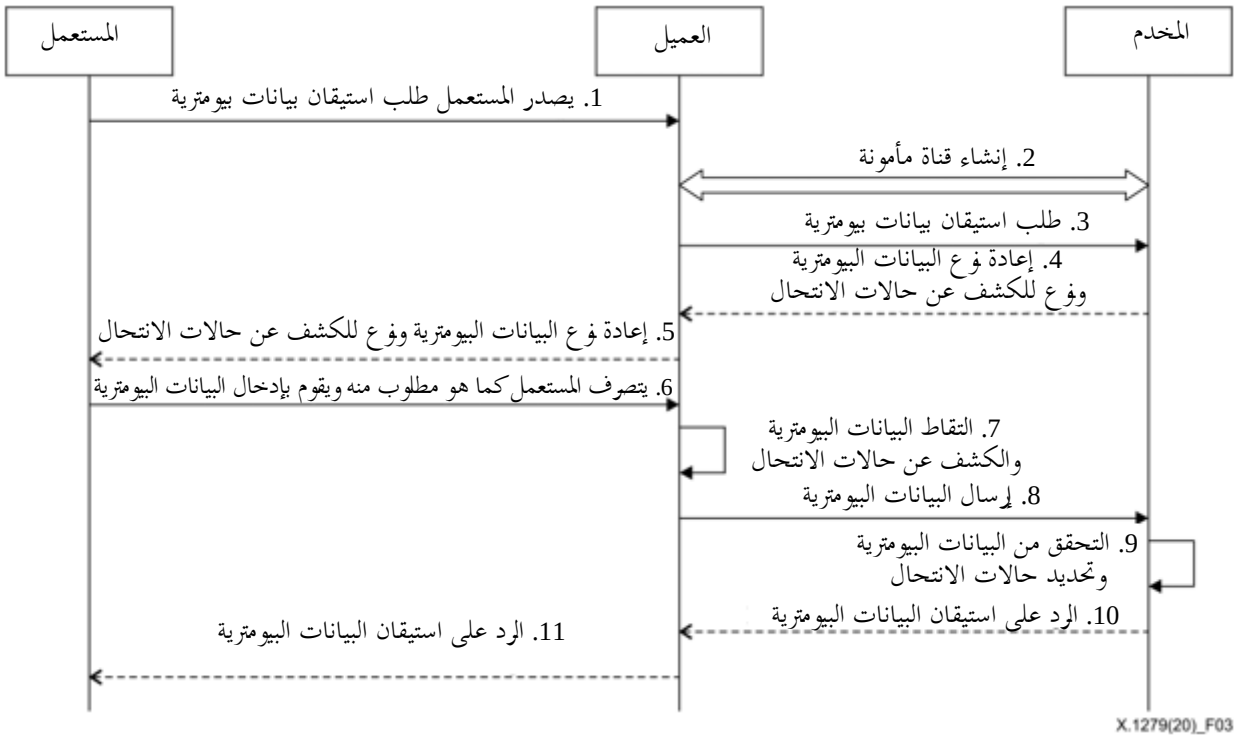
9 يربط المخدّم البيانات البيومترية بمعرّف هوية حساب المستعمل ويقوم بإجراء الكشف ASD؛

10 يخزن المخدّم المرجع البيومتري المستقبل في قاعدة بيانات المراجع البيومترية؛

11 يعيد المخدّم نتائج تسجيل البيانات البيومترية إلى العميل؛

12 يخطر العميل المستعمل بنتائج عملية التسجيل.

2.2.8 تدفقات عملية الاستيقان



الشكل 3 – تدفقات عملية الاستيقان

يعرض الشكل 3 تدفقات عملية الاستيقان. ويرد فيما يلي وصف التدفقات بالتفصيل:

1 يطلق المستعمل طلب استيقان بيانات بيومترية للعميل مصحوباً بمعرّف هوية كلمة المرور المستعمل؛

2 ينشئ العميل قناة مأمونة مع المخدّم لحماية الدورة وإرسال البيانات، مثلاً: باستخدام بروتوكول كلمة المرور البعيدة المأمونة (SRP)؛

3 يرسل العميل طلب استيقان البيانات البيومترية مع معرّف هوية حساب المستعمل وبيانات إدارة المخاطر؛

4 تعيد وظيفة منطق القرار في المخدّم نوع البيانات البيومترية ونوع الكشف ASD السليمين إلى العميل استناداً إلى تحليل بيانات المخاطر ومنطق الأعمال؛

5 يطلب العميل من المستعمل القيام بالإجراءات المحددة لالتقاط البيانات البيومترية؛

6 يتصرف المستعمل حسب المطلوب منه ويقوم بإدخال البيانات البيومترية الواردة من العميل؛

7 تقوم وظيفة التقاط البيانات البيومترية في العميل بالتقاط البيانات البيومترية ويقوم الكشف ASD بالكشف عن التحركات المتوقعة للمستعمل؛

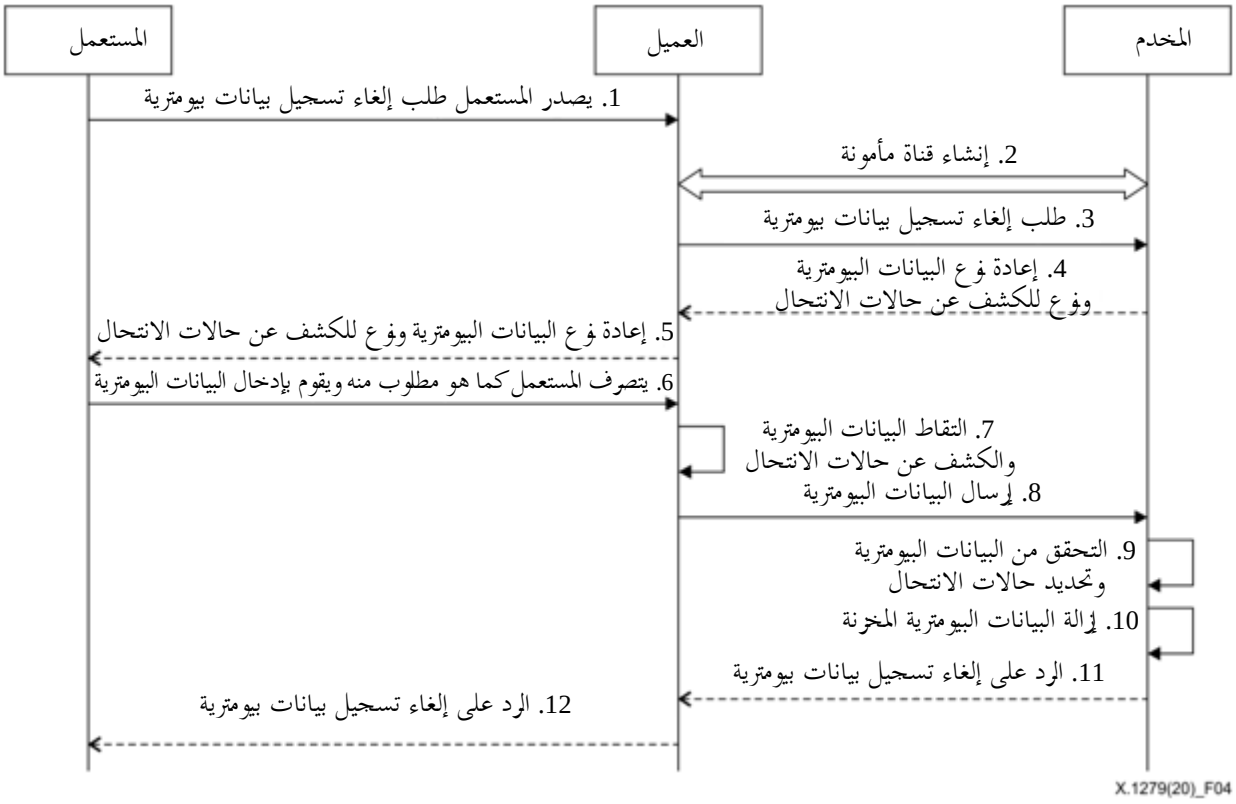
8 يستخلص العميل السمات البيومترية ويرسلها إلى المخدّم كمرجع بيومتري في القناة المأمونة المنشأة؛

9 يجري المرسل عملية التحقق من البيانات البيومترية بين السمة البيومترية المستخلصة والمرجع البيومتري ويقوم بالكشف ASD؛

10 يعيد المخدّم نتائج استيقان البيانات البيومترية إلى العميل؛

11 يخطر العميل المستعمل بنتائج استيقان البيانات البيومترية.

3.2.8 تدفقات عملية إلغاء التسجيل



الشكل 4 – تدفقات عملية إلغاء التسجيل

يعرض الشكل 4 تدفقات عملية إلغاء التسجيل. وفيما يلي وصف التدفقات بالتفصيل:

شرط مسبق: يستيقن المستعمل بنجاح مع المخدّم عبر آليات استيقان أخرى مثل معرّف هوية حساب المستعمل/كلمة المرور وشفرة تحقق عبر خدمة الرسائل القصيرة (SMS).

1 يستخدم المستعمل معرّف هوية الحساب/كلمة المرور لتسجيل الدخول وإطلاق طلب إلغاء تسجيل بيانات بيومترية للعميل؛

2 ينشئ العميل قناة مأمونة مع المخدّم لحماية الدورة وإرسال البيانات، باستخدام البروتوكول SRP، على سبيل المثال؛

3 يرسل العميل طلب إلغاء تسجيل البيانات البيومترية مصحوباً بمعرّف هوية حساب المستعمل وبيانات إدارة المخاطر إلى المخدّم؛

4 تعيد وظيفة منطق القرار في المخدّم نوع البيانات البيومترية ونوع الكشف ASD السليمين إلى العميل استناداً إلى تحليل بيانات المخاطر ومنطق الأعمال؛

5 يطلب العميل من المستعمل القيام بالإجراءات المحددة لالتقاط البيانات البيومترية؛

6 يتصرف المستعمل حسب المطلوب منه ويقوم بإدخال البيانات البيومترية الواردة من العميل؛

7 تقوم وظيفة التقاط البيانات البيومترية في العميل بالتقاط البيانات البيومترية ويقوم الكشف ASD بالكشف عن التحركات المتوقعة للمستعمل؛

8 يستخلص العميل السمات البيومترية ويرسلها إلى المخدّم كمرجع بيومتري في القناة المأمونة المنشأة؛

9 يجري المخدّم عملية التحقق من البيانات البيومترية بين السمة البيومترية المستخلصة والمرجع البيومتري المخزن ويجري الكشف ASD؛

10 يزيل المخدّم المرجع البيومتري الخاص بالمستعمل من قاعدة بيانات المراجع البيومترية؛

11 يرسل المخدّم نتائج إلغاء تسجيل البيانات البيومترية إلى العميل؛

12 يخطر العميل المستعمل بنتائج إلغاء تسجيل البيانات البيومترية.

9 مبادئ توجيهية أمنية

1.9 أمن العميل

ينبغي تحديث نظام تشغيل الجهاز المتنقل حسب أحدث نسخة مؤمنة في حينه.

ينبغي للعميل التوقيع لتحديد مصدر العميل.

ينبغي حماية العميل من التعديل أو التحديث غير المخول.

ينبغي تعزيز حماية الشفرة والبيانات من عمليات الهندسة العكسية في العميل، مثل التموين.

ينبغي تنفيذ الاستحواذ على البيانات في العميل في بيئة موثوقة لضمان سرية البيانات المجمَّعة وسلامتها.

2.9 أمن المخدّم

ينبغي تنفيذ سياسات صارمة للتحكم في النفاذ في المخدّم، وينبغي استيقان أي عملية تشغيل للمخدّم والتصريح بها أولاً.

ينبغي أن يكون المخدّم قادراً على تحديد هوية العميل.

ينبغي حماية الاتصالات بين المخدّم والعميل من هجمات إعادة التشغيل، مثل استعمال بيانات دينامية في الرسائل مثل قيمة ظرفية أو سؤال تحقق أو خاتم توقيت.

ينبغي الاحتفاظ بسجلات للعمليات التي تتم على المخدّم، مع حماية سلامة هذه السجلات.

3.9 أمن التخزين

شهادات التوصية ITU-T X.509 والمفاتيح الخاصة، ينبغي تخزينها بأمان مع وضع سياسات صارمة للتحكم في النفاذ.

ينبغي تخزين المفاتيح الخاصة بنص مشفر وينبغي أن تكون خوارزمية التجفير على مستوى عال من الأمن لمنع عمليات الفك.

ينبغي أن تكون البيانات البيومترية المخزنة في المخدّم، وينبغي أن تكون خوارزمية التجفير على مستوى عال من الأمن لمنع عمليات الفك.

ينبغي أن تكون البيانات البيومترية المخزنة في المخدّم سمة بيومترية مستخلصة يتعذر إعادتها إلى البيانات الأصلية.

وهناك مزيد من التفاصيل عن أمن التخزين ينبغي أن تفي بالمتطلبات الواردة في المعيار [ISO/IEC 24745].

4.9 أمن الاتصالات

قبل أي اتصالات بين العميل والمخدّم، ينبغي إنشاء قناة مأمونة، مثل البروتوكول https، الذي يعد مناسباً لأغراض أمن الاتصالات.

وينبغي توفير آلية للتبادل المأمون للمفاتيح في الاستيقان بين العميل والمخدّم، مثل كلمة المرور البعيدة المأمونة التي يمكن استخدامها كآلية للتبادل المأمون للمفاتيح.

وينبغي الحيلولة دون اعتراض المفتاح المستخدم في التفاوض بشأن القناة المأمونة، كأن تستخدم كلمة المرور البعيدة المأمونة للتفاوض بشأن القناة المأمونة دون نقل المفتاح.

المعلومات التي على شاكلة البيانات البيومترية المعالجة ونتائج مكونات القرار ينبغي تشفيرها من أجل الإرسال وينبغي التحقق من سلامتها بوظيفة وحيدة الاتجاه مثل دالة الاختزال أو البنية التحتية للمفاتيح العمومي (PKI) التي تمنع أي تعديل للبيانات أثناء الإرسال.

وينبغي إزالة حساسية البيانات البيومترية المعالجة وتجفيرها من أجل الإرسال وينبغي أن يكون مفتاح التجفير مختلفاً باختلاف العميل وأن يستعمل المخدّم مفتاح فك تجفير متوائم لفك التجفير.

وهناك المزيد من التفاصيل عن أمن الاتصالات ينبغي أن تفي بالمتطلبات الواردة في المعيار [ISO/IEC 24745].

5.9 اعتبارات أمنية أخرى

إلى جانب أمن التخزين وأمن الاتصالات، هناك الكثير من جوانب الأمن الأخرى التي يجب مراعاتها، مثل أمن المعالجة وحماية المعلومات المحددة لهوية لأشخاص وما إلى ذلك. وهناك المزيد من تفاصيل التقنيات الأمنية لحماية المعلومات البيومترية ينبغي أن تفي بالمتطلبات الواردة في المعيار [ISO/IEC 24745].

التذييل I

حالات وسيناريوهات الاستعمال

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

1.I دراسة حالة استعمال لخدمات السداد بالاتصالات المتنقلة

أليس واحدة ممن يستخدمون تطبيقاً يسمى "المحفظة المتنقلة" من أجل عمليات السداد باستغلال الاتصالات المتنقلة. ويرد وصف الخطوات كالتالي:

1) استخدمت أليس في المرة الأولى اسم المستعمل وكلمة المرور الخاصة بها لتسجيل الدخول في تطبيق المحفظة المتنقلة. وهي لم تكن ترغب في إدخال كلمة المرور الخاصة بها في كل مرة تجري بها عملية سداد، وكانت خائفة أيضاً من نسيان كلمة المرور الخاصة بها. لذا، فهي تقوم بالنقر على زر "تسجيل السداد بالتحقق عن طريق الوجه" في تطبيق المحفظة المتنقلة.

2) يطلب تطبيق المحفظة المتنقلة من أليس فتح الكاميرا والإيماء نحوها.

3) تتلقى أليس رسالة من تطبيق المحفظة المتنقلة "لقد تم تسجيلك بنجاح".

4) تشتري أليس قدحاً من القهوة في مقهى ستارباكس وتستعمل تطبيق المحفظة المتنقلة للدفع. وتفتح أليس تطبيق المحفظة المتنقلة وتتلقى رسالة مستعد للدفع ويطلب التطبيق المتنقل من أليس فتح الكاميرا والإيماء نحوها. وتجد أليس متعة كبيرة في هذه التجربة.

5) تتلقى أليس إخطاراً من تطبيق المحفظة المتنقلة: "لقد قمت بالدفع بنجاح ، شكراً لك".

6) بعد مضي بعض الوقت، لم تعد أليس في حاجة إلى استعمال هذه الوظيفة مجدداً، وبالتالي، تقوم بالنقر في زر لإغلاق خيار أسلوب السداد هذا.

2.I دراسة حالة استعمال لخدمات التجارة الإلكترونية

يمتلك بوب متجراً يبيع الملابس ويرغب في فتح متجر إلكتروني على منصة للتجارة الإلكترونية. وفيما يلي وصف للإجراءات:

1) يقوم بوب في المرة الأولى بتسجيل نفسه على منصة التجارة الإلكترونية ويتقدم بطلب لفتح متجر إلكتروني. يدخل بوب اسم المستعمل وكلمة المرور الخاصة به على منصة التجارة الإلكترونية من تطبيق للتجارة الإلكترونية على جهازه المتنقل.

2) يطلب تطبيق التجارة الإلكترونية الموجود على جهاز بوب المتنقل منه أن يفتح الكاميرا أو أن يقوم بالعدد من الأعمال على التوالي، مثل فتح الفم وهز الرأس والغمز بالعين والإيماء في الكاميرا.

3) يتلقى بوب رسالة من التطبيق المتنقل للتجارة الإلكترونية "لقد تم تسجيلك بنجاح".

4) بعد مرور بعض الوقت، يرغب بوب في الإعلان عن بعض الملابس من متجره وتطلب منصة التجارة الإلكترونية من بوب فتح الكاميرا أو القيام بالعديد من الأعمال على التوالي، مثل هز الرأس والغمز بالعينين وفتح الفم والإيماء في الكاميرا.

5) يتلقى بوب إخطاراً من منصة التجارة الإلكترونية "لقد سجلت للدخول بنجاح".

6) بعد مرور بعض الوقت، لا يرغب بوب في استعمال هذه الوظيفة مجدداً وينقر على زر لغلق خيار الاستيقان هذا.

التذييل II

كلمة المرور البعيدة المأمونة (SRP)

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

كلمة المرور البعيدة المأمونة (SRP) هي وسيلة استيقان للهوية على أساس كلمة المرور وبروتوكول لتبادل المفاتيح. وتتمثل ميزة كلمة المرور SRP في أن النص العادي للمفاتيح ليس ظاهرة نقل في عملية الاستيقان، حيث لا يحتاج المستعملون إلا إلى الاحتفاظ بكلمة المرور. وإلى جانب ذلك، لا يخزن المخدّم كلمات مرور المستعملين ولكنه يخزن المعلومات ذات الصلة حتى وإن التقط المخدّم أحد الخصوم؛ حيث لا يستطيع هذا الخصم استحداث عميل شرعي (لأنه يتعذر الحصول على كلمة المرور).

ويمكن الاطلاع على تفاصيل البروتوكول SRP في المعيار [b-RFC 2945].

ويمكن استخدام البروتوكول SRP في إنشاء قنوات مأمونة بين العميل والمخدّم في عملية تسجيل البيانات البيومترية وعملية استيقان البيانات البيومترية وعملية إلغاء تسجيل البيانات البيومترية. ويمكن استخدام البروتوكول SRP في التفاوض بشأن التوصيلات المأمونة باستخدام كلمة مرور مقدمة من المستعمل، مع القضاء على المشكلات الأمنية المرتبطة تقليدياً بكلمات المرور القابلة لإعادة الاستعمال. ويمكن استخدام البروتوكول SRP أيضاً في إجراء تبادل مأمون للمفاتيح في عملية الاستيقان، مما يمكن من تفعيل طبقات الأمن (حماية الخصوصية و/أو السلامة) أثناء الدورة.

التذييل III

أمثلة على الكيفية التي يُجري بها المخدّم الكشف عن حالات الانتحال (ASD) في التعرف عن طريق الوجه

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

تشمل الأمثلة على الكيفية التي يجري بها المخدّم الكشف عن حالات الانتحال (ASD) في التعرّف عن طريق الوجه ما يلي، على سبيل الذكر وليس الحصر:

1) باتباع بعض الملاحظات والإرشادات من المخدّم، يمكن للمستعمل القيام بإجراء محدد ويكتشف المخدّم الإجراء من صورة الوجه.

2) ينبغي أن يكون بمقدور المخدّم اكتشاف زاوية الوجه والكاميرا واكتشاف الجسم الحي من خلال تغيير زاوية الوجه في العملية.

3) ينبغي أن يكون للمخدّم القدرة على اكتشاف استمرارية إجراء الوجه ومنع تشغيل الشرائح ومنع الأفراد من التغيير أثناء العملية.

4) ينبغي أن يكون للمخدّم القدرة على اكتشاف إعادة تشغيل الفيديو الخاص بإجراء الوجه.

5) ينبغي أن يكون للمخدّم القدرة على منع الهجمات بصورة الوجه.

6) ينبغي أن يكون للمخدّم القدرة على اكتشاف استخدام نماذج الوجه ثلاثية الأبعاد المعدة بواسطة تكنولوجيا الغرافيك على الحاسوب.

بيبليوغرافيا

[b-ITU-T M.3016.0] Recommendation ITU-T M.3016.0 (2005), *Security for the management plane: Overview.*

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*

[b-ITU-T X.1081] Recommendation ITU-T X.1081 (2011), *The telebiometric multimodal model - A framework for the specification of security and safety aspects of telebiometrics*.

[b-ITU-T X.1085] Recommendation ITU-T X.1085 (2016) | ISO/IEC 17922:2017, *Information technology - Security techniques – Telebiometric authentication framework using biometric hardware security module.*

[b-ITU-T X.1089] Recommendation ITU-T X.1089 (2008), *Telebiometrics authentication infrastructure (TAI).*

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions.*

[b-ITU-T X.1254] Recommendation ITU-T X.1254 (2012), *Entity authentication assurance framework.*

[b-ISO 18461] ISO 18461:2016, *International museum statistics.*

[b-ISO/IEC 19784-1] ISO/IEC 19784-1:2018, *Information technology –Biometric application programming interface – Part 1: BioAPI specification*

[b-ISO/IEC 19792] ISO/IEC 19792:2009, *Security evaluation of biometrics.*

[b-ISO/IEC 19989] ISO/IEC 19989, *Evaluation of presentation attack detection for biometrics.*

[b-ISO/IEC 2382] ISO/IEC 2382:2015, *Information technology – Vocabulary*

[b-ISO/IEC 2382-37] ISO/IEC 2382-37:2017, *Information technology – Vocabulary – Part 37: Biometrics*

[b-ISO/IEC 24761] ISO/IEC 24761:2009, *Information technology – Security techniques – Authentication context for biometrics.*

[b-ISO/IEC 30107] ISO/IEC 30107:2017, *Information technology – Biometric presentation attack detection.*

[b-ISO/IEC 30125] ISO/IEC 30125:2016, *Biometrics – Biometrics used with mobile devices.*

[b-RFC 2945] RFC 2945, *The SRP Authentication and Key Exchange System*

[b-Disappearing Cryptography] Disappearing Cryptography (Third Edition), 2009, Pages 355-364.

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، 2021