الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1814

(2022/09)

السلسلة X: شبكات البيانات والاتصالات
بين الأنظمة المفتوحة ومسائل الأمن

أمن الاتصالات المتنقلة الدولية–2020

مبادئ توجيهية بشأن أمن أنظمة الاتصالات المتنقلة الدولية–2020

التوصية ITU-T X.1814

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
القياس الحيوي عن بُعد	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 (1)	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.1350
أمن أنظمة النقل الذكية (ITS)	X.1399–X.1370
أمن سجل الحسابات الموزع	X.1429–X.1400
أمن التطبيقات (2)	X.1459–X.1450
أمن شبكة الويب (2)	X.1489–X.1470
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
الدفاع السيبراني	X.1599–X.1590
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
مولِّد 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
حماية البيانات	X.1789–X.1770
أمن شبكات الاتصالات المتنقلة الدولية–2020	**X.1819–X.1800**

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

التوصية ITU-T X.1814

مبادئ توجيهية بشأن أمن أنظمة الاتصالات المتنقلة الدولية–2020

ملخص

تتطلب أجهزة إنترنت الأشياء (IoT) الموصولة وتطبيقاتها المتنقلة النفاذ إلى شبكة لاسلكية مرنة وآمنة وقادرة على حماية خصوصية الأفراد. وينبغي أن تكون أنظمة الاتصالات المتنقلة الدولية–2020 مصممة للوفاء بهذه المتطلبات بالغة الأهمية. وهناك حاجة إلى تحديد إطار أمني لأنظمة الاتصالات المتنقلة الدولية–2020 يمكن استخدامه كأساس لإعداد توصيات تقنية أكثر تفصيلاً بشأن مواضيع أمن الاتصالات المتنقلة الدولية–2020.

وتحدد التوصية ITU-T X.1814 جميع المكونات ذات الصلة بأمن أنظمة الاتصالات المتنقلة الدولية–2020، كما تحدد مبادئ توجيهية بشأن أمن أنظمة الاتصالات المتنقلة الدولية–2020. وتتضمن التوصية وصفاً لمعمارية عامة للاتصالات المتنقلة الدولية–2020 وميادينها، وتحدد التهديدات التي قد يتعرض لها كل مكون وتوصِّف المتطلبات بشأن القدرات الأمنية اللازمة مع أخذ الميزات التي تنفرد بها الشبكة في الاعتبار. وتستند هذه التوصية إلى المعمارية الأمنية للجيل الخامس لمشروع شراكة الجيل الثالث (3GPP).

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1814	2022-09-02	17	11.1002/1000/14992

مصطلحات أساسية

مقدرة، نظام الاتصالات المتنقلة الدولية–2020، حوسبة الحافة متعددة النفاذ، تقسيم الشبكة، التمثيل الافتراضي للشبكة، مبادئ توجيهية بشأن الأمن، تهديدات.

---

* 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 الأمم المتحدة المتخصصة 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/.

جدول المحتويات

الصفحة

الصفحة

التوصية ITU-T X.1814

مبادئ توجيهية بشأن أمن أنظمة الاتصالات المتنقلة الدولية–2020

1 مجال التطبيق

تقدم هذه التوصية مبادئ توجيهية بشأن أمن أنظمة الاتصالات المتنقلة الدولية–2020. وهي تحدد جميع المكونات المتعلقة بأمن نظام الاتصالات المتنقلة الدولية–2020، أي معدات المستعمل وشبكة النفاذ والشبكة الأساسية. وهي تصف معمارية عامة للاتصالات المتنقلة الدولية–2020 وميادينها. وتحدد أيضاً التهديدات التي قد يتعرض لها كل مكون وتوصِّف له القدرات الأمنية اللازمة مع أخذ الميزات التي تنفرد بها الشبكة في الاعتبار، مثل حوسبة الحافة ذات النفاذ المتعدد والتوصيل الشبكي المعرّف بالبرمجيات والتمثيل الافتراضي الدينامي لوظائف الشبكة وتقسيم الشبكة إلى شرائح. وتستند هذه التوصية إلى المعمارية الأمنية للجيل الخامس لمشروع شراكة الجيل الثالث (3GPP).

2 المراجع

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

[ITU-T X.800] التوصية ITU-T X.800 (1991)، *معمارية الأمن في التوصيل البيني للأنظمة المفتوحة من أجل تطبيقات اللجنة الاستشارية الدولية للبرق والهاتف*.

[ITU-T X.1038] التوصية ITU-T X.1038 (2016)، *المتطلبات الأمنية والمعمارية المرجعية للشبكات المعرّفة بالبرمجيّات*.

3 التعاريف

1.3 المصطلحات المعرَّفة في مراجع أخرى

1.1.3 تستخدم هذه التوصية المصطلحات التالية المأخوذة من التوصية [ITU-T X.800]:

- التحكم في النفاذ؛
- الاستيقان؛
- التيسر
- السرية؛
- سلامة البيانات؛
- الخصوصية
- التنصل؛
- خدمة الأمن

وبالإضافة إلى ذلك، تستعمل هذه التوصية المصطلحات الإضافية التالية المعرَّفة في مصادر أخرى:

2.1.3 التحكم (control) [b-ITU-T X.1408]: التدبير الذي يعدِّل المخاطر.

الملاحظة 1 – تتضمن عناصر التحكم أي عملية أو سياسة عامة أو جهاز أو ممارسة أو غيرها من الإجراءات التي تعدل المخاطر.

الملاحظة 2 – يجوز أن لا تمارس عناصر التحكم دائماً أثر التعديل المقصود أو المفترض.

3.1.3 هجوم الحرمان من الخدمة الموزَّع (distributed denial-of-service attack) (DDoS) [b-ITU-T Y.4807]: النفاذ غير المجاز إلى مورد من موارد النظام أو تأخير عمليات ووظائف النظام في سبيل الإضرار بأنظمة متعددة لإغراق عرض نطاق أو موارد النظام المستهدف، وما يترتب على ذلك من خسارة في التيسر للمستعملين المجازين.

4.1.3 المبدأ التوجيهي (guideline) [b-ITU-T X.1401]: وصف يوضح ما ينبغي عمله وكيف يمكن تحقيق الأهداف المحددة في السياسات المرعية.

5.1.3 وظيفة الشبكة (network function) [ITU-T Y.3100]: في سياق الاتصالات المتنقلة الدولية–2020، هي وظيفة المعالجة في الشبكة.

الملاحظة 1 – تشمل وظائف الشبكة على سبيل المثال لا الحصر وظائف عقدة الشبكة، مثل إدارة الدورة وإدارة التنقلية ووظائف النقل التي يعرّف سلوكها الوظيفي وسطوحها البينية.

الملاحظة 2 – يمكن تنفيذ وظائف الشبكة على عتاد مخصص أو كوظائف برمجيات ممثَّلة افتراضياً.

الملاحظة 3 – لا تعتبر وظائف الشبكة موارد وإنما يمكن تمثيل حالة أي من وظائف الشبكة باستعمال الموارد.

6.1.3 التمثيل الافتراضي لوظائف الشبكة (network function virtualization) [b-ITU-T X.1811]: التكنولوجيا التي تتيح إنشاء أقسام الشبكة المعزولة منطقياً عبر الشبكات المادية المشتركة بحيث يمكن للمجموعات غير المتجانسة من الشبكات الافتراضية المتعددة أن تتعايش في نفس الوقت عبر الشبكات المشتركة.

7.1.3 شريحة شبكة (network slice) [b-ITU-T Y.3100]: شبكة منطقية تقدم قدرات شبكية وخصائص شبكية محددة.

الملاحظة 1 – تمكِّن شرائح الشبكة من إنشاء شبكات مكيّفة حسب الطلب لتقديم حلول مرنة لسيناريوهات السوق المختلفة التي تتسم بمتطلبات متنوعة فيما يتعلق بالوظائف والأداء وتوزيع الموارد.

الملاحظة 2 – يجوز أن تتمكن شريحة شبكة من كشف قدراتها.

الملاحظة 3 – يتحقق سلوك شريحة شبكة عبر حالة (حالات) شريحة شبكة.

8.1.3 التنسيق (orchestration) [b-ITU-T Y.3100]: في سياق الاتصالات المتنقلة الدولية–2020 (IMT-2020)، العمليات الهادفة إلى أتمتة ترتيب الوظائف والموارد الشبكية في البنى التحتية المادية والافتراضية، على السواء، وأتمتة تنسيقها وإنشاء أمثلة لها واستخدامها، باستخدام معايير تحقق المستوى الأمثل لهذه العمليات.

9.1.3 القدرة الأمنية (security capability) [b-ISO 81001-1]: فئة واسعة من الضوابط التقنية والإدارية والتنظيمية لإدارة المخاطر المحيطة بسرية البيانات والأنظمة وسلامتها وتيسرها ومساءلتها.

10.1.3 المورِّد (supplier) [b-ISO 10393]: منظمة أو شخص يقدم منتجاً أو خدمة.

11.1.3 النظام (system) [b-ISO/IEC 27000]: تطبيقات أو خدمات أو أصول تكنولوجيا المعلومات أو غيرها من مكونات تداول المعلومات.

12.1.3 التهديد (threat) [b-ITU-T X.1406]: سبب محتمل لحادث غير مرغوب قد يُلحق ضرراً بالنظام أو المنظمة.

13.1.3 وظيفة افتراضية للشبكة (virtualized network function) A :[b-ITU-T Y.3150]: وظيفة شبكة تكون برمجيتها الوظيفية منفصلة عن العتاد وتعمل على آلة (آلات) افتراضية.

2.3 المصطلحات المعرَّفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 الميدان (domain): مجموعة من كيانات الشبكة طبقاً للجوانب المادية أو المنطقية ذات الصلة بشبكة الاتصالات المتنقلة الدولية–2020.

2.2.3 نظام الاتصالات للاتصالات المتنقلة الدولية–2020 (IMT-2020 communication system): نظام لإدارة عمليات الاتصالات المتنقلة الدولية–2020 لخدمات الاتصالات المتنقلة الدولية–2020.

الملاحظة 1 – يحال الجيل الخامس (5G) إلى الاتصالات المتنقلة الدولية–2020 في سياق قطاع تقييس الاتصالات.

الملاحظة 2 – نظام الاتصالات للاتصالات المتنقلة الدولية–2020 يطابق في هذه التوصية نظام الاتصالات المتنقلة الدولية–2020.

3.2.3 النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020 (IMT-2020 ecosystem): مجموعة من أصحاب المصلحة الذين يتفاعلون لتشكيل نظام مستقر عامل للاتصالات المتنقلة الدولية–2020.

ملاحظة – يعتمد ذلك بشكل أساسي على تكنولوجيا الاتصالات المتنقلة الدولية–2020، حيث يضم مجتمع الجهات الفاعلة فيه المنتجين والمستهلكين والموردين الذين يساهمون بكميات هائلة من المنتجات والتكنولوجيا والخبرات لكي يعمل نظام الاتصالات المتنقلة الدولية–2020 على مستويات مختلفة مثل البنية التحتية والشبكة والمنصة والخدمة والتطبيق.

4.2.3 خدمة الاتصالات المتنقلة الدولية–2020 (IMT-2020 service): منفعة يقدمها النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020.

5.2.3 هجوم فيض جدول التدفق (Flow table overflow attack): هجوم يستهلك جداول التدفق التي تعيد تسيير رزم التدفقات وتعالجها، مما لا يبقي أي فسحة أمام تدفقات أخرى لتثبيت قواعد التدفق ويؤدي بالتالي إلى الحرمان من خدمة الشبكة.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والمختزلات التالية:

4G الجيل الرابع من تكنولوجيا الاتصالات المتنقلة *(Fourth Generation of Mobile Communication Technology)*

AMF وظيفة إدارة النفاذ والتنقلية *(Access and Mobility Management Function)*

API السطح البيني لبرمجة التطبيقات *(Application Programming Interface)*

AUSF وظيفة مخدم الاستيقان *(Authentication Server Function)*

C-PDU وحدة بيانات بروتوكول التحكم *(Control Protocol Data Unit)*

CU/DU الوحدة المركزية/الوحدة الموزَّعة *(Central Unit / Distributed Unit)*

DCI التوصيل البيني لمراكز البيانات *(Data Centres Interconnect)*

DDoS الحرمان من الخدمة الموزَّع *(Distributed Denial-of-Service)*

DoS الحرمان من الخدمة *(Denial-of-Service)*

eMBB النطاق العريض المتنقل المعزَز *(Enhanced Mobile Broadband)*

FAT جدول توزيع الملفات *(File Allocation Table)*

IMSI الهوية الدولية للاشتراكات المتنقلة *(International Mobile Subscriber Identity)*

IMT-2020 الاتصالات المتنقلة الدولية–2020 *(International Mobile Telecommunications-2020)*

IoT إنترنت الأشياء *(Internet of Things)*

LTE التطور الطويل الأجل *(Long-Term Evolution)*

MAC شفرة استيقان الرسائل *(Message Authentication Code)*

MEC حوسبة الحافة ذات النفاذ المتعدد *(Multi-access Edge Computing)*

MEHW .أجهزة المعدات الإلكترونية *(Mobile Equipment Hardware)*

mIoT إنترنت الأشياء الكثيفة *(Massive Internet of Things)*

mMTC الاتصالات الكثيفة من آلة إلى أخرى *(Massive Machine-Type Communications)*

MNO مشغِّل شبكة اتصالات متنقلة *(Mobile Network Operator)*

NAS طبقة عدم النفاذ *(Non-Access Stratum)*

NF وظيفة الشبكة *(Network Function)*

NFV التمثيل الافتراضي لوظائف الشبكة *(Network Function Virtualization)*

NFVI *البنية التحتية للتمثيل الافتراضي لوظائف الشبكات*
(Network Functions Virtualization Infrastructure)

NRF وظيفة مستودع وظائف الشبكة *(Network Function Repository Function)*

OAM التشغيل والصيانة والإدارة *(Operation, Administration, and Management)*

O&M التشغيل والإدارة *(Operations and Management)*

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

PSK مفتاح مشترَك مسبقاً *(Pre-Shared Key)*

RA / CA سلطة التسجيل وسلطة إصدار الشهادات *(Registration Authority and Certification Authority)*

RRC التحكم في الموارد الراديوية *(Radio Resource Control)*

SBA معمارية قائمة على الخدمة *(Service-Based Architecture)*

SBI السطح البيني القائم على الخدمة *(Service-Based Interface)*

SDN التوصيل الشبكي المعرَّف بالبرمجيات *(Software-Defined Networking)*

SMF وظيفة إدارة الدورة *(Session Management Function)*

SQL لغة الاستجواب المهيكَلة *(Structured Query Language)*

SSL طبقة المقابس الآمنة *(Secure Sockets Layer)*

TA مصدر الثقة *(Trust Anchor)*

TLS أمن طبقة النقل *(Transport Layer Security)*

TMSI هوية مؤقتة لمشترك بالاتصالات المتنقلة *(Temporary Mobile Subscriber's Identity)*

TPM وحدة منصة موثوقة *(Trusted Platform Module)*

UDM إدارة البيانات الموحدة *(Unified Data Management)*

UE معدات المستعمل *(User Equipment)*

UICC بطاقة الدارات المتكاملة الشاملة *(Universal Integrated Circuit Card)*

URLLC اتصالات فائقة الموثوقية ومنخفضة الكمون *(Ultra-Reliable and Low-Latency Communications)*

USIM وحدة هوية المشترك العالمية *(Universal subscriber identity module)*

VM الآلة الافتراضية *(Virtual machines)*

VNF وظيفة الشبكة الافتراضية *(Virtual Network Function)*

VoIP الصوت عبر بروتوكول الإنترنت *(Voice over Internet Protocol)*

5 الاصطلاحات

في هذه التوصية، كلمة "ينبغي" تدل على مواصفة يوصى بها لكنها غير إلزامية في المطلق. وبالتالي لا يتعين توفر هذه المواصفة لزعم الامتثال.

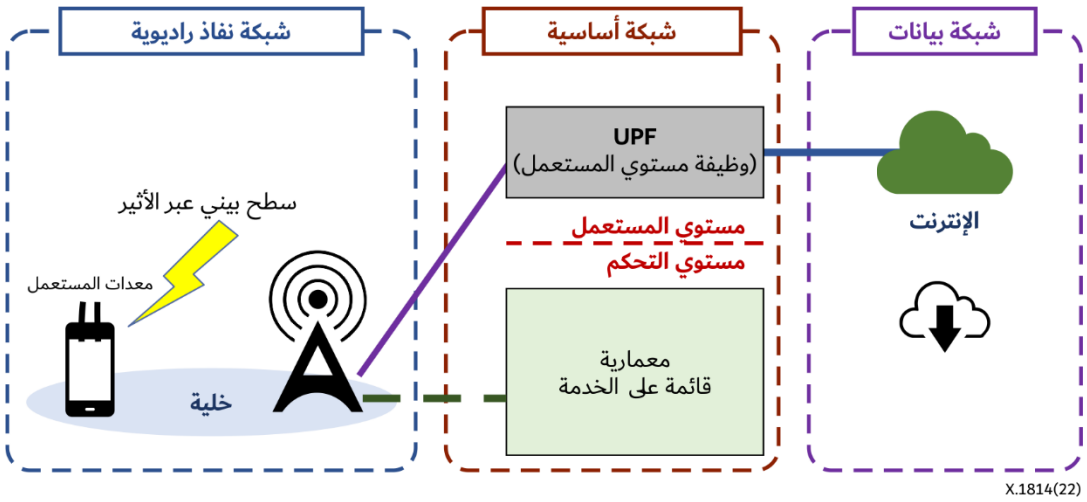
6 لمحة عامة عن أمن نظام الاتصالات المتنقلة الدولية–2020

1.6 المعمارية المبسطة للاتصالات المتنقلة الدولية–2020

تقدم هذه الفقرة لمحة عامة عن أمن نظام الاتصالات المتنقلة الدولية–2020. وتتطلب الأجهزة المتنقلة الموصولة وتطبيقاتها المتنقلة النفاذ إلى شبكة لاسلكية مرنة وآمنة وقادرة على حماية خصوصية الأفراد. وينبغي أن يكون نظام الاتصالات المتنقلة الدولية–2020 مصمماً للوفاء بهذه المتطلبات الإجمالية.

ويتألف نظام الاتصالات المتنقلة الدولية–2020 من أجهزة موصولة بشبكة نفاذ إلى الاتصالات المتنقلة الدولية–2020، موصولة بدورها ببقية النظام الذي يسمى الشبكة الأساسية للاتصالات المتنقلة الدولية–2020.

ويبين الشكل 1 معمارية مبسطة لنظام 3GPP 5G. وتتضمن شبكة النفاذ إلى الاتصالات المتنقلة الدولية–2020 محطات قاعدة راديوية مشمولة بمشروع الشراكة 3GPP و/أو شبكة نفاذ غير مشمولة بمشروع الشراكة 3GPP. وتتفوق معمارية الشبكة الأساسية للاتصالات المتنقلة الدولية–2020 كثيراً على شبكة الجيل الرابع من حيث قدرتها على دعم تنفيذ المنصات السحابية وإنترنت الأشياء، مع تحسينات كبيرة في تقسيم الشبكة إلى شرائح والمعمارية القائمة على الخدمة (SBA).

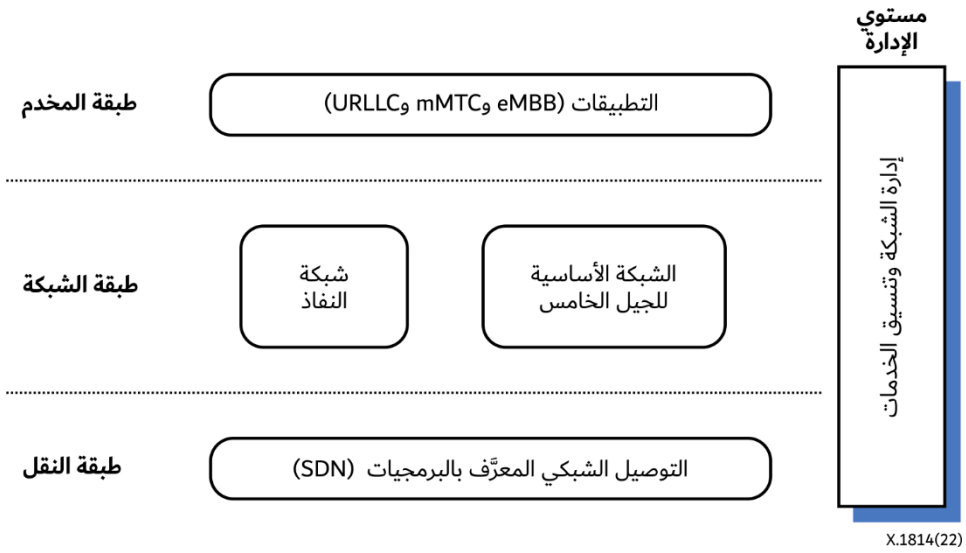


الشكل 1 – معمارية مبسطة للاتصالات المتنقلة الدولية–2020

2.6 المعمارية العامة لنظام الاتصالات المتنقلة الدولية–2020

يهدف نظام الاتصالات المتنقلة الدولية–2020 إلى تقديم مجموعة واسعة من الخدمات بمتطلبات أداء مختلفة. ويمكن تصنيف الخدمات المقدمة في شبكات الاتصالات المتنقلة الدولية–2020 إلى ثلاث فئات وفقاً لمواصفات مشروع الشراكة 3GPP: (1) يدعم النطاق العريض المتنقل المعزز (eMBB) معدلات بيانات أعلى وتنقلية أكبر للمستعمل من الجيل الرابع/التكنولوجيا طويلة الأجل (4G/LTE)؛ (2) توفر إنترنت الأشياء الكثيفة (mIoT) اتصالات كثيفة من آلة لآلة؛ (3) تدعم الاتصالات فائقة الموثوقية ومنخفضة الكمون (URLLC) خدمات المهام الحرجة التي تتطلب موثوقية أعلى وكمون أقل. ومن المزمع أن يكون نظام الاتصالات المتنقلة الدولية–2020 منصة مرنة تتيح حالات أعمال جديدة وتدمج المجالات التخصصية، مثل السيارات والتصنيع والطاقة والصحة الإلكترونية والترفيه. وعلاوةً على ذلك، سيكون نشر وصيانة نظام الاتصالات المتنقلة الدولية–2020 أسهل مقارنة بالأجيال السابقة من الشبكات المتنقلة. ولمواجهة هذه المتطلبات الصعبة، أدخل نظام الاتصالات المتنقلة الدولية–2020 عدداً من تكنولوجيات الابتكار، مثل تقسيم الشبكة إلى شرائح، والتمثيل الافتراضي لوظائف الشبكة (NFV)، والتوصيل الشبكي المعرَّف بالبرمجيات (SDN)، والمعمارية القائمة على الخدمة (SBA)، والفصل بين الوحدة المركزية/الوحدة الموزعة (CU/DU).

وتظهر في الشكل 2 المعمارية العامة لنظام الاتصالات المتنقلة الدولية–2020 [b-ITU-T X.1811] التي تتضمن طبقة النقل، وطبقة البنية التحتية؛ وطبقة الشبكة؛ وطبقة الخدمة ومستوي الإدارة، حسب الوظائف المطلوبة.



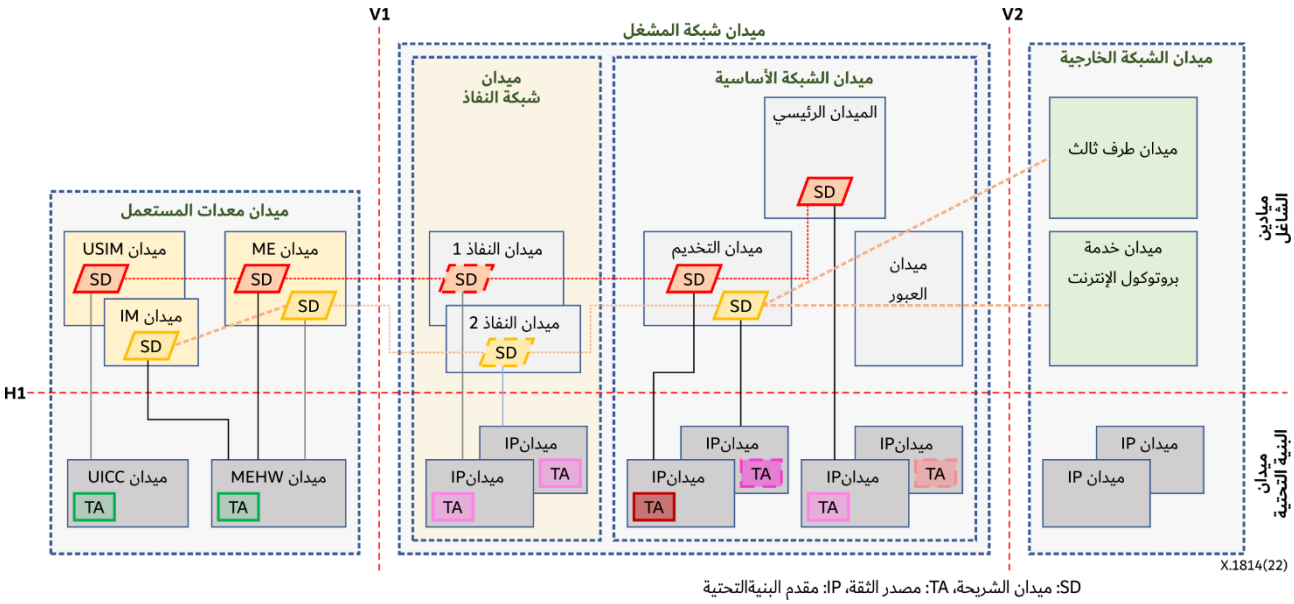
الشكل 2 – المعمارية العامة لنظام الاتصالات المتنقلة الدولية–2020 [b-ITU-T X.1811]، [b-TS 33.501]

- طبقة النقل: وهي تُستخدم لنقل الرزم بين المصدر والمقصد. وإلى جانب تكنولوجيات النقل التقليدية (مثل تبديل الوسم متعدد البروتوكولات (MPLS))، أدخل نظام الاتصالات المتنقلة الدولية–2020 تكنولوجيا التوصيل الشبكي المعرَّف بالبرمجيات (SDN) لزيادة سرعات النقل والتكيف السهل مع متطلبات الخدمة.
- طبقة الشبكة: وهي تضم شبكة النفاذ والشبكة الأساسية. وتمكن الأولى المعدة UE من النفاذ إلى شبكة من شبكات الاتصالات المتنقلة الدولية–2020. والثانية مصممة بمعمارية SBA للسماح بإمكانية التوسع والتبسيط. وهي تتكون من عدد من وظائف الشبكة لدعم توصيلية البيانات ونشر الخدمات. وتشمل الأمثلة على وظائف الشبكة وظيفة مخدم الاستيقان (AUSF) ووظيفة إدارة النفاذ والتنقلية (AMF) ووظيفة إدارة الدورة (SMF).
- طبقة الخدمة: وهي تتألف من التطبيقات التي تُشغل على قمة النظام IMT-2020، والتي قد تكون تطبيقات eMBB، وتطبيقات mMTC، وتطبيقات URLLC.
- مستوي الإدارة: وهو المسؤول عن إدارة الشبكة وتنسيق الخدمات.

3.6 ميادين نظام الاتصالات المتنقلة الدولية–2020

ينبغي تعريف أمن الاتصالات المتنقلة الدولية–2020 وفقاً للميادين والطبقات والمتطلبات الأمنية والقدرات الأمنية.

والميدان هو تجميع لكيانات الشبكة طبقاً للجوانب المادية أو المنطقية ذات الصلة بشبكة الاتصالات المتنقلة الدولية–2020. ويُستعمل مفهوم ميدان الشرائح لالتقاط جوانب تقسيم الشبكة إلى شرائح. ويمكن أن يمثل خواصاً وظيفية وخدمات وأطراف فاعلة مختلفة في شبكات الاتصالات المتنقلة الدولية–2020. ويعرض الشكل 3 ميدان الاتصالات المتنقلة الدولية–2020 النمطي.



الشكل 3 – الميادين النمطية للاتصالات المتنقلة الدولية–2020

تمثل عناصر الشبكة الموضوعة فوق الخط H1 في الشكل 3 جوانب الشبكة المنطقية المسماة ميادين الشاغل، وتمثل تلك الواقعة تحت الخط H1 جوانب الشبكة المادية المسماة ميادين البنية التحتية. ويفصل الخط V1 ميدان معدات المستعمل (UE) عن ميدان شبكة النفاذ، ويفصل الخط V2 ميدان الشبكة الأساسية عن ميدان الشبكة الخارجي، ومثال ذلك، خدمات بروتوكول الإنترنت التي تستعملها شبكة المشغل.

وتحتوي ميادين البنية التحتية على عناصر شبكة تنفَّذ بواسطة "عتاد" وبرمجيات تعمل كمقدم للبنية التحتية. ويشمل ذلك المشرفات على الآلات الافتراضية (البرمجيات التي تنشئ وتشغِّل آلات افتراضية)، وكذلك مصادر الثقة (كيان معتمَد تُفترض الثقة به ولا تُشتق منه) [b-ITU-T X.509].

وعلى جانب معدات المستعمل تحت الخط H1، تتألف ميادين معدات المستعمل من بطاقة دارة متكاملة شاملة (UICC)، تقدم وحدة مقاومة للعبث، وميدان عتاد المعدات المتنقلة (MEHW)، وتقدم دعماً للعتاد يشمل بيئة تنفيذ موثوقة.

وعلى جانب الشبكة. تحت الخط H1، يوجد ميدان مقدم البنية التحتية (IP)، يتألف من العتاد المحدد للنفاذ (الراديوي) وكذلك من عتاد الحوسبة والتخزين والتوصيل الشبكي المطلوب للخواص الوظيفية الأساسية.

وتُستخدم مصادر الثقة لتقديم ثقة للأنظمة الافتراضية. ويشمل ذلك ضمان سلامة ميدان الشاغل وتنفيذ ميدان الشاغل على بنية تحتية معينة وموثوقة. ويمكن أيضاً استعمال مصادر الثقة للتحقق من سلامة ميدان البنية التحتية وربط ميادين الشاغل بميادين البنية التحتية.

وتحتوي ميادين الشاغل على عدة ميادين منطقية تستعمل ميادين البنية التحتية، لتنفيذ وظائفها مثلاً. وهي تتألف، في جانب معدات المستعمل، من معدات متنقلة، ووحدة هوية المشترك العالمية (USIM)، وواحد من عدة تطبيقات برمجية موجودة في الجزء الخاص بالعتاد يدعى بطاقة الدارة المتكاملة الشاملة (UICC) التي تخزن المعلومات المتصلة بالمشترك وتنفذ الوظائف الأمنية الخاصة بالاستيقان والتشفير في جانب المستعمل وميدان إدارة الهوية. وتتكون ميادين الشاغل في جانب الشبكة من ميدان النفاذ (A) وميدان الخدمة (S) والميدان الرئيسي (H) وميدان العبور (T) وميدان الطرف الثالث (3P) وميدان خدمة بروتوكول الإنترنت وميدان الإدارة (M).

4.6 متطلبات وقدرات الأمن العامة

تلخص هذه الفقرة أبعاد الأمن العامة (المتطلبات) الموضحة في المعيار [b-ITU-T X.805]. والهدف من هذه الفقرة توفير الأساس للقدرة الأمنية لنظام الاتصالات المتنقلة الدولية–2020. ويقدم التذييل I معمارية أمن الشبكة العامة لتوفير أمن الشبكة من طرف إلى طرف.

تشير طبقة الأمن إلى تراتبية معدات الشبكة وتجميعات المرافق [b-ITU-T X.805]. وتتألف طبقة الأمن من مجموعة من البروتوكولات والبيانات والوظائف المتعلقة بجانب واحد من الخدمات التي يقدمها ميدان واحد أو أكثر من الميادين وتقدم طبقة معمارية أمن الاتصالات المتنقلة الدولية–2020 رؤية إجمالية للبروتوكولات والبيانات والوظائف المرتبطة بها بمعنى أنها معرضة لبيئة تهديدات مشتركة وتبدي متطلبات أمنية متماثلة. وتشمل التشويش الراديوي وهجمات محطات القاعدة الزائفة؛ وحقن بيانات مستوي المستعمل عبر الأثير، والرسائل المنتحَلة للتحكم في الموارد الراديوية (RRC) هي تهديدات شائعة للاتصالات بين معدات المستعمل وشبكة النفاذ الراديوي. ومن ناحية أخرى، فإن تتبع معرفات هوية الاشتراك، وانتحال رسائل مستوي التحكم، والتلاعب بالقدرات الأمنية، وما إلى ذلك، هي تهديدات شائعة للاتصالات بين معدات المستعمل والشبكة الأساسية. وتشمل بعض الأمثلة على التهديدات الشائعة لخدمات الإدارة في شبكات الاتصالات المتنقلة الدولية–2020، التعرض للتغييرات غير المجازة في التشكيلة، واختراق مفاتيح وشهادات الشبكة، وإضافة وظائف شبكية خبيثة على حين غرة. وتشمل طبقة الإدارة الجوانب المتصلة بالإدارة التقليدية للشبكة (التشكيلة وتحديثات البرمجيات وإدارة حسابات مستعملي النظام وجمع/تحليل السجلات، وما إلى ذلك). وعلى وجه الخصوص جوانب إدارة الأمن (تدقيق مراقبة الأمن، وإدارة المفاتيح والشهادات، وما إلى ذلك). وعلاوةً على ذلك، تنتمي إلى هذه الطبقة الجوانب المتعلقة بإدارة التمثيل الافتراضي وإنشاء/تكوين الخدمات (تنسيق وإدارة شرائح الشبكة، وإدارة العزل والآلات الافتراضية (VM)، وما إلى ذلك).

ومجال الأمن يوسع ميادين الأمن ويخضع لمتطلبات الأمن لطبقة أو ميدان أو أكثر من الطبقات أو الميادين.

وتُعرّف القدرة الأمنية عموماً على أنها فئة واسعة من الضوابط التقنية والإدارية والتنظيمية لإدارة المخاطر المتعلقة بسرية البيانات والأنظمة وسلامتها وتيسرها ومساءلتها [b-ISO 81001-1]. وهي تشير إلى مجموعة من وظائف وآليات الأمن (بما في ذلك الضمانات والتدابير المضادة) لجانب أمني واحد، من قبيل السلامة. وهي تحتوي على وظائف وآليات أمنية لتفادي المخاطر الأمنية التي تتعرض لها شبكات الاتصالات المتنقلة الدولية–2020، وكشفها وردعها والتصدي لها والتقليل منها إلى أدنى حد، ولا سيما المخاطر التي تهدد البنية التحتية المادية والمنطقية للشبكة وخدماتها ومعدات المستعمل والتشوير والبيانات. ويقدم الجدول 1 المتطلبات الأمنية لميادين الأمن.

الجدول 1 – المتطلبات الأمنية لكل مجال أمن

مجال الأمن	المتطلبات الأمنية
شبكة النفاذ	تحدد المتطلبات الأمنية ذات الصلة بطبقة وميدان النفاذ للتصدي للتهديدات ذات الصلة بهذا الميدان. ومن أمثلة هذه المتطلبات حماية سرية وسلامة بيانات مستوي المستعمل ومستوي التحكم والتنقلية الآمنة.
التطبيق أو الخدمة	المتطلبات الأمنية لطبقة التطبيق التي تقدم تطبيقات وخدمات المستعمل النهائي (مثل VoIP، VoLTE) للتصدي للتهديدات المتعلقة بهذا الميدان. ومن أمثلة هذه المتطلبات الاستيقان والتخويل للمستعمل من أجل استعمال تطبيق واكتشاف خدمة آمنة.
الإدارة	تحدَد المتطلبات الأمنية في طبقة الإدارة وميدان الإدارة للتصدي للتهديدات المتصلة بهذا الميدان، بما في ذلك إدارة الأمن (مثل عمليات الترقية الآمنة والتنسيق الآمن) وإدارة الأمن (أي المراقبة، وإدارة المفاتيح والنفاذ).
معدات المستعمل	تحدَد المتطلبات الأمنية ذات الصلة بميدان معدات المستعمل، بما في ذلك التحكم في النفاذ إلى الجهاز، من أجل التصدي للتهديدات ذات الصلة بهذا الميدان. ومن أمثلة هذه المتطلبات الاستيقان المتبادل مع الشبكة والتخزين الآمن لسياق الأمن.
الشبكة	تحدَد المتطلبات الأمنية ذات الصلة بالشبكة الأساسية والاتصالات بين الشبكة والشبكات الخارجية، بما في ذلك الجوانب المتعلقة بتبادل التشوير وبيانات المستعمل النهائي بشكل آمن بين العقد في ميدان المشغل وميدان الشبكة الخارجية. ومن أمثلة ذلك أمن الشبكة، وخصوصية المشترك، واستيقان المشترك.
البنية التحتية والتمثيل الافتراضي	تحدَد المتطلبات الأمنية لميدان مقدم البنية التحتية، على سبيل المثال، للإشهاد، والتقسيم إلى شرائح/العزل الآمن، وقضايا الثقة بين ميادين الشاغل، وبين ميادين الشاغل وميادين البنية التحتية.

ويصف الجدول 2 القدرات الأمنية لكل بعد أمني [b-ITU-T X.805]. وقد اعتُمد سبع منها من التوصية [b-ITU-T X.805]، وهي إدارة الهوية والنفاذ والاستيقان وعدم التنصل والسرية والسلامة والتيسر والخصوصية. أما الثلاث الأخرى، وهي المراجعة [b-ITU-T X.800] والثقة والضمان والامتثال، فهي أبعاد أمنية في معمارية أمن الاتصالات المتنقلة الدولية–2020.

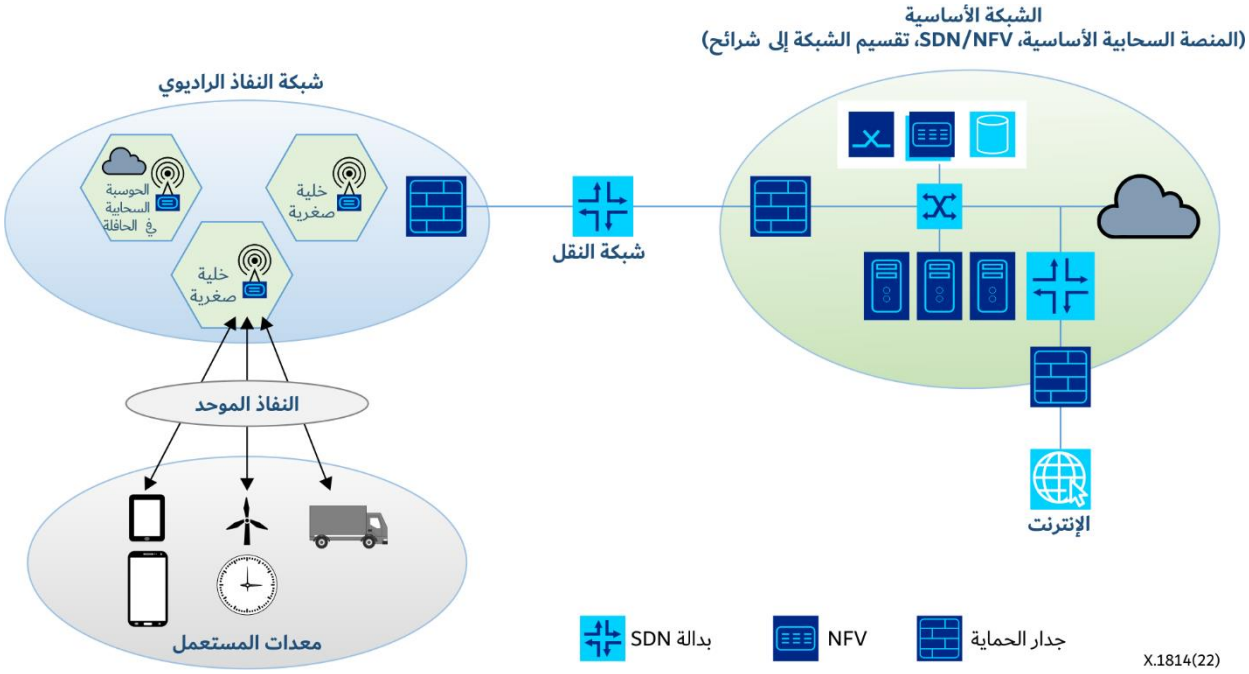
الجدول 2 – القدرات الأمنية

الأبعاد الأمنية	القدرة الأمنية
إدارة الهوية والنفاذ	تشير هذه القدرة الأمنية إلى مجموعة من وظائف وآليات الأمن (بما في ذلك الضمانات والتدابير المضادة) للتحكم في النفاذ وإدارة وبيانات الاعتماد والأدوار.
الاستيقان	تشير هذه القدرة الأمنية إلى مجموعة من الوظائف والآليات الأمنية (بما فيها الضمانات والتدابير المضادة) من أجل الاستيقان الذي يعمل على التحقق من صلاحية نعوت استيقان المستعمل، من قبيل الهوية المدعاة.
عدم التنصل	تشير هذه القدرة الأمنية إلى مجموعة من الوظائف والآليات الأمنية (بما فيها الضمانات والتدابير المضادة) لخدمة عدم التنصل التي تحمي من إنكار كاذب للضلوع في فعل معين.
السرية	تشير هذه القدرة الأمنية إلى مجموعة من الوظائف والآليات الأمنية (بما فيها الضمانات والتدابير المضادة) لخدمة السرية التي تحمي البيانات من الإفشاء غير المصرح به.
السلامة	تشير هذه القدرة الأمنية إلى مجموعة من الوظائف والآليات الأمنية (بما فيها الضمانات والتدابير المضادة) لخدمة السلامة التي تحمي البيانات من استحداث أو تعديل.
التيسر	تشير هذه القدرة الأمنية إلى مجموعة من الوظائف والآليات الأمنية (بما فيها الضمانات والتدابير المضادة) لتيسر الموارد، حتى في حال وجود هجمات. وترد في التصنيف آليات التعافي من الكوارث.
الخصوصية	تشير هذه القدرة الأمنية إلى مجموعة من الوظائف والآليات الأمنية (بما فيها الضمانات والتدابير المضادة) لخدمة خصوصية تتيح للكيانات الحق في تحديد الدرجة التي ستتناقل بها المعلومات المحددة لهويتها، وستتفاعل معها.
المراجعة	تشير هذه القدرة الأمنية إلى مجموعة من الوظائف والآليات الأمنية (بما فيها الضمانات والتدابير المضادة) لخدمة مراجعة تتيح استعراض وفحص سجلات النظام وأنشطته لتحديد مدى كفاية قدرة النظام وكشف الخروقات في أمن النظام وقدرته. كما يدرج تدقيق لجمع البيانات.
الثقة والضمان	تشير هذه القدرة الأمنية إلى مجموعة من الوظائف والآليات الأمنية (بما فيها الضمانات والتدابير المضادة) لخدمة الثقة والضمان التي تخدم نقل معلومات عن جدارة نظام ما بالثقة.
الامتثال	تشير هذه القدرة الأمنية إلى مجموعة من الوظائف والآليات الأمنية (بما فيها الضمانات والتدابير المضادة) لخدمة امتثال تسمح لكيان أو نظام بالإيفاء بالالتزامات التعاقدية أو القانونية.

7 مكونات الجدارة بالثقة في نظام الاتصالات المتنقلة الدولية–2020

1.7 مكونات الاتصالات المتنقلة الدولية–2020

تتطلب أجهزة إنترنت الأشياء الموصولة وتطبيقاتها المتنقلة النفاذ إلى شبكة لاسلكية مرنة وآمنة وقادرة على حماية خصوصية الأفراد. وينبغي تصميم نظام الاتصالات المتنقلة الدولية–2020 (IMT-2020) لتلبية المتطلبات المبينة في الفقرتين 8.7 و9.7 من التوصية [b-ITU-T Y.3101]. وتتألف شبكة الاتصالات المتنقلة الدولية–2020 من أربعة مكونات هي: معدات المستعمل (UE) وشبكة النفاذ الراديوي وشبكة النقل والشبكة الأساسية، وهي مبينة في الشكل 4.



الشكل 4 – شبكة الاتصالات المتنقلة الدولية–2020 (مقتبس من ورشة عمل الاتحاد الدولي للاتصالات)

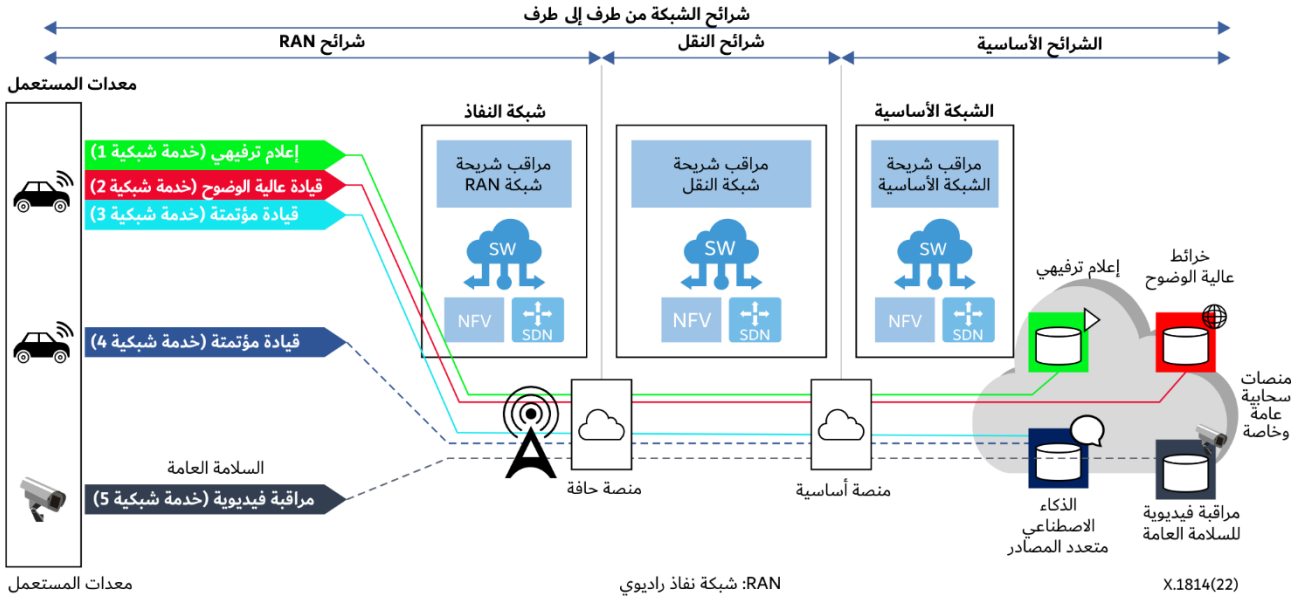
وسيبنى نظام الاتصالات المتنقلة الدولية–2020 على المنصات السحابية المتنقلة، والتوصيل الشبكي المعرَّف بالبرمجيات (SDN)، والتمثيل الافتراضي لوظائف الشبكة (NFV)، وتقسيم الشبكة إلى شرائح، لمواجهة تحديات التوصيلية الكثيفة، والمرونة، وتقليل التكلفة إلى أدنى حد. ولذلك، هناك حاجة إلى تحديد أمن الحوسبة السحابية للتمثيل الافتراضي لوظائف الشبكة وتقسيم وظائف الشبكة والحوسبة السحابية في الحافة.

ويفصل التمثيل الافتراضي لوظائف الشبكة وظائف الشبكة عن أجهزة العتاد المسجلة الملكية ويشغلها كبرمجيات في الآلات الافتراضية.

ووظيفة الشبكة الافتراضية (VNF) هي نتيجة منطقية للتمثيل الافتراضي لوظائف الشبكة، وهي وظيفة شبكية تُفصل برمجياتها الوظيفية عن العتاد وتعمل على آلة (آلات) افتراضية [b-ITU-T.Y.3100]. وتؤدي وظائف الشبكة الافتراضية وظائف شبكية محددة مثل جدران الحماية والتبديل وأنظمة كشف التسلل وأنظمة الحماية من التسلل.

وتقسيم الشبكة إلى شرائح هو شكل من معمارية الشبكة الافتراضية يستعمل المبادئ التي يقوم عليها التوصيل الشبكي المعرَّف بالبرمجيات والتمثيل الافتراضي لوظائف الشبكة في الشبكات الثابتة. وتنقسم شبكات الاتصالات المتنقلة الدولية–2020 (IMT-2020) فرعياً إلى شبكات افتراضية، يستمثل كل منها لحالة واحدة من حالات الأعمال، ويُعرف بشريحة الشبكة. ويمكنها أن تغطي ميادين متعددة للشبكة، بما في ذلك ميدان النفاذ والميدان الأساسي وميدان النقل، وأن تُنشر عبر مشغلين متعددين على النحو المبين في الشكل 5.

والتوصيل الشبكي المعرَّف بالبرمجيات (SDN) هو معمارية ترمي إلى جعل الشبكات سريعة ومرنة. والهدف من التوصيل الشبكي المعرَّف بالبرمجيات هو تحسين التحكم في الشبكة من خلال تمكين الشركات ومقدمي خدمات الشبكات من الاستجابة بسرعة لمتطلبات الأعمال المتغيرة.



الشكل 5 – شرائح شبكة الاتصالات المتنقلة الدولية–2020

وشبكة نقل الاتصالات المتنقلة الدولية–2020 هي بنية تحتية لنقل بروتوكول الإنترنت تقوم بإيصال الاتصالات المتنقلة الدولية–2020.

وتقدم حوسبة الحافة قدرات الحوسبة السحابية إلى حافة شبكة الاتصالات المتنقلة الدولية–2020. وحوسبة الحافة هي نموذج حوسبة موزع يجرى فيه معظم الحساب أو كله على عقد الأجهزة الموزعة المعروفة باسم الأجهزة الذكية أو أجهزة الحافة، بدلاً من إجرائه في بيئة سحابية مركزية. وتقرّب حوسبة الحافة المعالجة وتخزين البيانات إلى المعدات. وهذا يمكّن أجهزة إنترنت الأشياء من تقديم خدمتها بكمونات منخفضة.

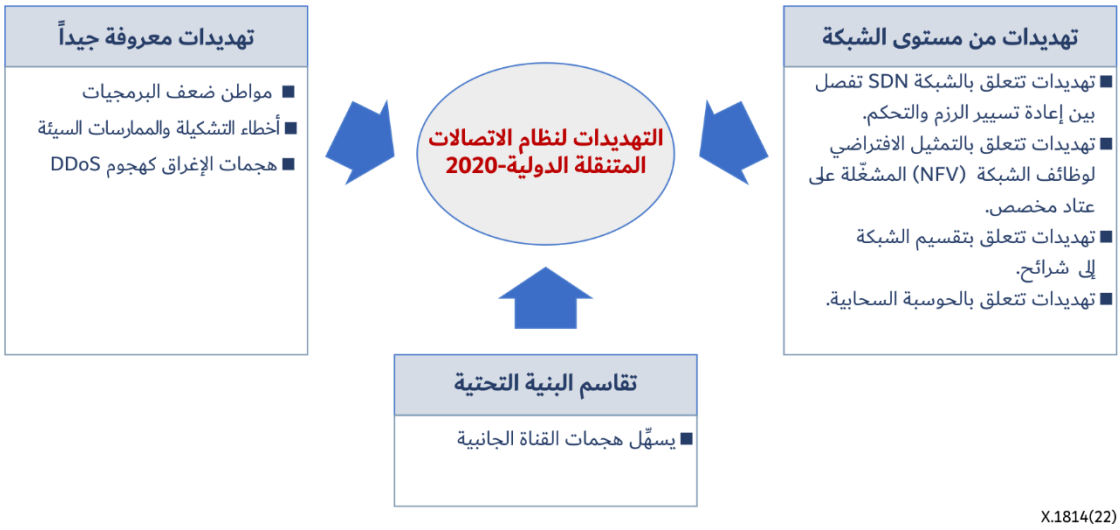
2.7 جدارة نظام الاتصالات المتنقلة الدولية–2020 بالثقة

تَنتج جدارة نظام الاتصالات المتنقلة الدولية–2020 (IMT-2020) بالثقة عن خمس خصائص هي: الصمود، وأمن الاتصالات، وإدارة الهوية، وحماية المعلومات المحددة لهوية شخص (PII) وضمان الأمن:

- الصمود: هو قدرة المنظمة على مقاومة التأثر بالأعطال. ويمكن لمجموعة متنوعة من الميزات التكميلية والمتداخلة جزئياً في الاتصالات المتنقلة الدولية–2020 أن تساعد على تحقيق قدرة نظام الاتصالات المتنقلة الدولية–2020 على الصمود أمام الهجمات السيبرانية والحوادث غير الخبيثة.
- أمن الاتصالات: يطبق هذا الأمن على اتصالات البيانات في الاتصالات المتنقلة الدولية–2020. وتعد الاتصالات الآمنة للأجهزة ولبنيتها التحتية الخاصة أمراً حيوياً في نظام للاتصالات المتنقلة الدولية–2020.
- إدارة الهوية: عمليات وسياسات تتعلق بإدارة دورة الحياة والقيمة والنوع والبيانات الشرحية الاختيارية في هويات معروفة في نظام الاتصالات المتنقلة الدولية–2020. وينبغي تقديم إدارة هوية آمنة لتعرف واستيقان المشتركين أو التجوال أو عدمه، وضمان أن يقتصر النفاذ إلى خدمات الشبكة على المشتركين الحقيقيين. وينبغي أن تبنى هذه الإدارة على بدائيات تجفيرية وخصائص أمنية قوية.
- الخصوصية: تعرّف حرمة البيانات في المعيار [b-ISO/TS 21719-2] بأنها حقوق والتزامات الأفراد والمنظمات فيما يتعلق بجمع المعلومات الشخصية واستعمالها والاحتفاظ بها والإفصاح عنها والتخلص منها. وتنطوي الخصوصية على حماية المعلومات المحددة لهوية شخص على حماية المعلومات التي يمكن أن تستعملها أطراف غير مخولة لتحديد هوية المشتركين.
- ضمان الأمن: يقدم ضمان الأمن أسباباً للثقة المبررة بأن الادعاء بشأن تحقيق أهداف الأمن قد تحقق أو سيتحقق. وضمان الأمن هو وسيلة لضمان تلبية معدات الشبكة لمتطلبات الأمن وتنفيذها باتباع عمليات آمنة للتطوير ودورة حياة المنتج.

8 التهديدات للمكونات والوظائف

يوضح الشكل 6 أمثلة على التهديدات في أنظمة الاتصالات المتنقلة الدولية–2020. وهي تصنف ضمن ثلاث فئات: تهديدات معروفة جيداً من مواطن ضعف البرمجيات، وأخطاء التشكيلة وهجمات الإغراق، وتهديدات من تقاسم البنية التحتية وتهديدات من مستوى الشبكة، مثل التهديدات المتعلقة بالتوصيل الشبكي المعرَّف بالبرمجيات (SDN) والتمثيل الافتراضي لوظائف الشبكة (NFV) وتقسيم الشبكة إلى شرائح والحوسبة السحابية.



الشكل 6 – التهديدات النموذجية في الاتصالات المتنقلة الدولية–2020 [ورشة العمل b-ITU]

1.8 التهديدات العامة

حدد المرجع [b-ENISA] التهديدات العامة التالية:

- **الحرمان من الخدمة (DoS)** [b-ENISA]: يسعى هذا الهجوم إلى جعل مورد الشبكة غير متيسر للمستعملين المستهدفين من خلال التدخل المؤقت أو غير المحدود في خدمة الشبكة أو تعطيلها بإغراقها بعدد هائل من الطلبات. وقد يؤدي تعدد أنواع هذه التهديدات إلى الحرمان من الخدمة من قبيل هجمات الإغراق والتكبير وعاصفة التشوير والتشبع. ويشمل الحرمان من الخدمة الشائع (1) الهجمات الطافحة للدارئ. ويتمثل المفهوم في إرسال حركة إلى عنوان شبكي تفوق قدرة النظام على التعامل معها وفق تصميم مبرمجيه له. وهي تتضمن الهجمات المدرجة أدناه، بالإضافة إلى هجمات أخرى مصممة لاستغلال مواطن الخلل الخاصة ببعض التطبيقات أو الشبكات. (2) إغراق بروتوكول رسالة التحكم في الإنترنت (ICMP) – يستفيد من أجهزة الشبكة المشكَّلة بشكل خاطئ عن طريق إرسال رزم منتحَلة تسبر كل حاسوب على الشبكة المستهدفة، بدلاً من الاكتفاء بسبر آلة واحدة محددة. ثم تُطلَق ردود الشبكة لتضخيم الحركة. ويُعرف هذا الهجوم أيضاً باسم هجوم السنافر أو السبر المميت. (3) الإغراق برزم التزامن (SYN) – يرسل طلباً للتوصيل بمخدم، ولكنه لا يستكمل التعارف. ويمعن في ذلك إلى أن تتشبع جميع المنافذ المفتوحة بالطلبات بحيث لا يبقى أي من المنافذ متاحاً للمستعملين الشرعيين للتوصيل بها.
- **هجوم الحرمان من الخدمة الموزَّع (DDoS)** [b-ENISA]: يقع هجوم الحرمان من الخدمة الموزَّع عندما تستهدف أنظمة متعددة نظاماً واحداً بهجوم الحرمان من الخدمة (DoS)، منسقةً هجوم حرمان من الخدمة متزامناً على هدف واحد. والفرق الأساسي هو أن الهدف يتعرض للهجوم من مواقع عديدة في وقت واحد بدلاً من أن يتعرض للهجوم من موقع واحد.
- **انتهاك البيانات وتسريبها وسرقتها وإتلافها والتلاعب بالمعلومات** [b-ENISA]: يشمل ذلك سرقة المعلومات المحددة لهوية شخص (PII) من خلال النفاذ غير المخول إلى الأنظمة و/أو الشبكة والنفاذ غير المخول إلى البيانات الشخصية/البيومترية/الطبية أو المعلومات السرية للمنظمة أو المعلومات المتصلة بالحكومة/الدولة واحتمال نشرها. وفي شن

أنواع مختلفة من الهجمات يمكن أن يستفيد المهاجمون أيضاً من سرقة أو خرق أو تسرب أنواع أخرى من البيانات مثل بيانات اعتماد المستعمل ومفاتيح التجفير وسجلات أمن الشبكات وتشكيلة البرمجيات وما إلى ذلك.

- **التنصت** [b-ENISA]: هو مصطلح يُستعمل لوصف اعتراض المعلومات غير المجاز. وهو تهديد يسعى فيه الدخيل إلى العبث بطبقات التطبيق والاتصالات لمختلف عناصر شبكة الاتصالات المتنقلة الدولية–2020 (وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات، ووظيفة الشبكة، وعقدة الحافة، ومنسق التمثيل الافتراضي). وهو يشمل التنصت على بيانات المشتركين والمعلومات المكتومة ووقت النظام وموقع المشترِك والرسائل الإلكترونية وإشارة البيانات المرحَّلة عبر الشبكة. وتقوم الجهة المهدِّدة بمراقبة المنظمات و/أو التجسس و/أو التنصت عليها لتتبع المواقع أو النفاذ إلى المعلومات الحساسة.
- **استغلال مواطن ضعف البرمجيات والعتاد** [b-ENISA]: يمكّن هذا النوع من التهديدات مهاجماً خبيثاً من استغلال عيوب البرمجيات أو العتاد أو العيوب المجهولة (لدى البائع والمستعمل) أو العيوب المعروفة ولكنها غير المصححة لشن هجوم. ومن أمثلة ذلك استغلال عيوب العتاد والبرمجيات المعروفة مثل الانهيار والفيض في الدارئ. ومنها أيضاً استغلال نقاط الضعف الأخرى المعروفة المتعلقة بأجيال سابقة للاتصالات المتنقلة.
- **شفرة أو برمجية خبيثة** [b-ENISA]: الشفرة الخبيثة هي المصطلح المستعمل لوصف أي شفرة في أي جزء من نظام برمجيات أو تعليمات برمجية تنفيذية الغرض منها إحداث تأثيرات غير مرغوبة أو خروقات أمنية أو الإضرار بالنظام. ويشمل التهديد تركيب وتوزيع البرمجيات الضارة أو دس شفرة أو برمجيات معينة داخل منتج أو تحديثات. ومن أمثلة البرمجيات الخبيثة، البرمجيات الضارة وبرمجيات طلب الفدية والفيروسات والديدان البرمجية وبرمجيات طروادة وبرمجيات حقن لغة الاستعلام المهيكلة (SQL) [b-SQL] وبرمجيات الأمن المنفلتة والبرمجيات الخبيثة وبرمجيات التبرعات الخيرية. ومن أمثلة البرمجيات الخبيثة في سياق الاتصالات المتنقلة الدولية–2020 (IMT-2020)، استعمال وظيفة شبكية افتراضية (VNF) غير مجازة يمكنها أن تثبت وتسجل نفسها على نحو مسيء في الشبكة الأساسية لكشف السطوح البينية الخبيثة لبرمجة التطبيقات.
- **اختراق سلسلة التوريد والبائعين ومقدمي الخدمات** [b-ENISA]: في حال اختراق سلسلة التوريد والبائعين ومقدمي الخدمات، فهذا يمكِّن البائعين من إدخال عتاد مخفي وبرمجيات خبيثة وعيوب برمجية في المنتج. ويمكِّنهم أيضاً من تنفيذ تحديثات برمجية غير مضبوطة ومن التلاعب بالخواص الوظيفية، بما في ذلك وظائف تجاوز آليات المراجعة والنفاذ عبر أبواب خلفية.

  وإذا شارك الموظفون غير الموثوقين من أطراف ثالثة أثناء اختبار المنتج وصيانته وتشكيله وتشغيله، فسيتمكنون من النفاذ إلى مرافق إدارة الشبكة (محلياً وكذلك عبر السطح البيني عن بُعد) للقيام بأنشطة الصيانة وتقديم الدعم التقني. ويتيح هذا النفاذ المميّز إلى التشغيل والإدارة والصيانة (OAM) في الشبكة فرصة لهؤلاء الموظفين للنفاذ إلى أنواع مختلفة من البيانات مثل بيانات تشكيلة المشترك والنظام والشبكة والقياس عن بُعد.
- **التهديدات المستهدِفة** [b-ENISA]: تأتي التهديدات المستهدِفة من البرمجيات الضارة الموجهة نحو منظمة أو صناعة محددة. وبوصفها نوعاً من أنواع برمجيات الجريمة، تثير هذه التهديدات المخاوف لأنها مصممة لاستخلاص معلومات حساسة. وقد تستهدف الهجمات عالية التعقيد أو التهديدات المتقدمة المستمرة معلومات حساسة أو تيسُّر الخدمات الحساسة والحرجة.
- **استغلال العيوب في إجراءات الأمن والإدارة والتشغيل** [b-ENISA]: رغم أن هذا التهديد لا يتعلق مباشرة بالاتصالات المتنقلة الدولية–2020، فإنه سيكون ذا أهمية عند التعامل مع تعقيد التكنولوجيا والحاجة إلى وضع إجراءات تشغيلية لإدارة الشبكة. ويشمل هذا التهديد، على سبيل الذكر لا الحصر، استغلال العيوب في الإدارة التشغيلية والأمنية للشبكة والتشكيلة والتحديث وإدارة الترقيع التصحيحي للبرمجيات. وقد تترتب على الأخطاء الناجمة عن نقص أو ضعف تصميم الإجراءات التشغيلية والأمنية عواقب على سلامة الشبكة وتيسرها.
- **إساءة استعمال الاستيقان** [b-ENISA]: قد يؤثر هذا التهديد على نقاط دخول متعددة إلى الشبكة مثل معدات المستعمل (الأجهزة المتنقلة وإنترنت الأشياء) والسطوح البينية للتشغيل والإدارة والتجوال والخدمات التخصصية. وتتصل

هذه التهديدات بسرقة بيانات اعتماد المستعمل، واستنفاد كل الاحتمالات لكشف أرقام حسابات المستعمل وكلمة المرور، وحجب هوية المستعمل، وتعطيل استيقان تجمعات إنترنت الأشياء، كتقنيات تستعملها الأطراف المهدِّدة لإساءة استعمال أنظمة استيقان الاتصالات المتنقلة الدولية–2020.

- **سرقة الهوية أو انتحالها** [b-ENISA]: سرقة الهوية هي الاستعمال المتعمد لهوية كيان آخر. وقد يشكل ذلك تهديداً عندما يحدد مهاجم خبيث بنجاح هوية كيان مشروع ثم ينتحلها لشن المزيد من الهجمات. ويشير انتحال الهوية إلى اتخاذ هوية كيان آخر ثم استعمال هذه الهوية لتحقيق هدف ما. ويمثل انتحال الهوية تهديداً يمكن أن يؤثر على أي مكون برمجي أو وكيل بشري. وفي هذا الهجوم، ينتحل المهاجم هوية المتحكم المشروع ويتفاعل مع وظائف الشبكة التي يتحكم فيها المتحكم المشروع (أي عناصر مستوي البيانات) لشن عدة أنماط أخرى من الهجمات (تحريك تدفقات الشبكة وتحويل الحركة وما إلى ذلك). ويمكن أيضاً استعمال الهندسة الاجتماعية واستنفاد كل الاحتمالات لكشف أرقام حسابات المستعمل/كلمة المرور كتقنية لانتحال أو سرقة بيانات اعتماد المستعمل. فمثلاً، يمكن استعمال هجمات التقاط هوية مشترك في الخدمة المتنقلة الدولية (IMSI) لكشف هوية المشترك عن طريق التقاط هوية IMSI الخاصة بمشترك من معدات المستعمل. ويمكن أيضاً شن هذه الهجمات بإنشاء محطة قاعدة مزيفة تعتبر محطة القاعدة المفضلة لمعدات المستعمل التي فقدت النفاذ إلى هوية مؤقتة للمشترك في الخدمة المتنقلة (TMSI). وسيجيب المشترك بهوية IMSI الخاصة به. وعلاوةً على ذلك، فإن لشبكات IMT-2020 أطراف فاعلة مختلفة مثل مشغلي شبكة الاتصالات المتنقلة الافتراضية (VMNO) ومقدمي خدمات الاتصالات (CSP) ومقدمي البنية التحتية للشبكات.

2.8 التهديدات لمعدات المستعمل

حُددت التهديدات الأمنية التالية لمعدات المستعمل:

- **إصابة ببرمجيات خبيثة** [b-ENISA]: في حال تركيب برمجيات خبيثة على جهاز المستعمل، قد يستفيد المهاجم من جهاز المستعمل المصاب لإطلاق نوع من الهجمات مثل سرقة البيانات الشخصية داخل جهاز المستعمل، أو إطلاق هجوم الحرمان من الخدمة الموزَّع (DDoS) أو محاولة إصابة معدات المستعمل الأخرى. وتشمل أمثلة البرمجيات الخبيثة برمجيات ضارة وبرمجيات طلب الفدية والفيروسات والديدان البرمجية وبرمجيات طروادة وبرمجيات الأمن المنفلتة. وحالما تصيب البرمجيات الخبيثة معدات المستعمل، تُدرج النقطة الطرفية المتنقلة في شبكة برمجيات روبوتية.
- **تهديد من البرمجيات الروبوتية** [b-Khan]: البرمجيات الروبوتية هي نوع من البرمجيات الضارة التي يمكنها التحكم في مجموعة من الأجهزة الموصولة بالإنترنت. ويمكن للبرمجيات الروبوتية المتنقلة أن تستهدف العديد من النقاط الطرفية المتنقلة لشن طائفة متنوعة من الهجمات تلقائياً (مثل: هجوم الحرمان من الخدمة (DoS) على أنظمة الاتصالات المتنقلة الدولية–2020. وإذ توصل الاتصالات المتنقلة الدولية–2020 بين الهواتف المتنقلة بقدرة حوسبة عالية، تزداد هذه التهديدات. وبالإضافة إلى ذلك، يفتح توصيل أجهزة إنترنت الأشياء أنواعاً جديدة من التهديدات. ونتيجة لذلك، تتعرض أجهزة إنترنت الأشياء لهجمات الشبكات الروبوتية على إنترنت الأشياء. ومن الأمثلة على ذلك الشبكة الروبوتية Mirai التي أثرت على الملايين من كاميرات بروتوكول الإنترنت في عام 2016.
- **تهديدات من البرمجيات الضارة المتنقلة** [b-Khan]: يمكن للبرمجيات الضارة المتنقلة أن تسمح للمهاجمين بسرقة بيانات المعلومات المحددة لهوية شخص (PII) المخزنة في الأجهزة المتنقلة أو حتى بشن هجمات (مثل هجمات الحرمان من الخدمة) ضد كيانات أخرى مثل معدات المستعمل الأخرى وشبكات النفاذ المتنقلة والشبكات الأساسية لمشغل الاتصالات المتنقلة.
- **نفاذ غير مجاز إلى بيانات المستعمل والتشوير أو إتلافها أو إفشائها أو تعديلها:** يمكن لمهاجم الحصول على نفاذ غير مجاز إلى بيانات المستعمل والتشوير المتداولة بين جهاز المستعمل وعقدة الجيل التالي B أو إتلافها أو إفشائها أو تعديلها.
- **التلاعب ببيانات اعتماد الاشتراك:** يمكن لمهاجم التلاعب ببيانات اعتماد الاشتراك التي تُستعمل للاستيقان والسرية.

3.8 التهديدات لشبكات النفاذ

حُددت التهديدات الأمنية التالية لشبكات النفاذ:

- **حركة خبيثة أو عَرَضية عالية** [b-NGMN]: بازدياد سعة الشبكة وعدد بنود معدات المستعمل، يزداد خطر حدوث تغييرات كبيرة في أنماط حركة الشبكة العارضة أو الخبيثة بسبب الأحداث الكبيرة. وبهذا المقياس، يتعذر تمييز القصد من شطحات الشبكة، وبالتالي فإن منع الأحداث الخبيثة هو الهدف الرئيسي، ولكنه يشمل كلا السيناريوهين.
- **تسرب المفاتيح بين وصلات المشغل** [b-NGMN]: يُحسب مفتاح التجفير (والسلامة أحياناً) للسطح البيني الأثيري من الشبكة الأساسية المحلية ثم يُرسَل إلى الشبكة اللاسلكية التي يزورها عبر وصلة إشارة مثل نظام التشوير رقم 7 (SS7) [b-ITU-T Q700] أو بروتوكول القطر [b-RFC 3588]. وهذه نقطة واضحة للتعرض وتُظهر كيفية تسرب المفتاح.
- **الإخلال بسلامة مستوي المستعمل** [b-NGMN]: هناك تهديد باعتراض الدورة بأكملها واستعمالها لإدراج بيانات فاسدة في التوصيل المتنقل (أو لأن تُهدر البيانات بتمرير البيانات إلى النقطة الطرفية للخدمة المهدورة).
- **التنفيذ الأمني الاختياري** [b-Khan] و[b-NGMN]: يأتي هذا التهديد من التنفيذ الأمني الاختياري. وهناك العديد من الأحكام الأمنية التي لا تؤثر على قابلية التشغيل البيني (معظمها قابلية التشغيل البيني مع معدات المستعمل)، وقد عوملت هذه الخيارات تاريخياً على أنها خيارات للنشر. ويمكن أن يؤدي هذا الاختيار إلى مخاطر تهدد المشغِّل حتماً جراء إجراءات مشغلين آخرين (دون أن يتعرضوا للوم عليها). وهو يخل أيضاً بافتراضات الأمن على مستوى النظام. وبدون خطوة الاستيقان هذه، لا يمكن لطبقة المفاتيح أن تحقق أحد أهداف التصميم، أي حماية العملاء من محطات القاعدة المعطوبة.
- **التهديد المستند إلى تقارير حالة الدارئ الكاذبة** [b-Khan]: يمكن لمهاجمين استغلال تقارير عن حالة الدارئ في مكونات شبكة النفاذ، مثل محطات القاعدة، للحصول على معلومات مثل خوارزميات الجدولة الزمنية للرزم وموازنة الحمولة، والتحكم في القبول لتحقيق مقاصدهم الخبيثة. ثم يمكن للمهاجم إرسال تقارير زائفة عن حالة الدارئ بالتظاهر بأن معدات المستعمل مشروعة لإلحاق الضرر بالعمليات.
- **تهديدات إدراج الرسائل** [b-Khan]: يمكن لحقن الرسائل أن يطلق هجمات الحرمان من الخدمة على شبكات الاتصالات المتنقلة الدولية–2020. فعلى سبيل المثال، يمكن تحميل جهاز التوصيل الشبكي المعرَّف بالبرمجيات ذي التحديث غير الصحيح لجدول التدفق فوق طاقته. ويمكن للمهاجم أيضاً أن يحقن وحدات بيانات بروتوكول التحكم (C-PDU) في النظام خلال وقت التنشيط لشن هجمات الحرمان من الخدمة على معدات المستعمل الجديدة الواردة.
- **التهديدات من خلية صغرية** [b-Khan]: التهديدات من خلية صغرية [b-Khan]: انخفض الحجم المادي لمحطات القاعدة انخفاضاً حاداً ووُضعت في مواقع داخل المباني مثل مراكز التسوق والأماكن العامة والملاعب والمستشفيات. وبالإضافة إلى ذلك، فإن استعمال ترددات جديدة مثل تردد الموجات المليمترية سيسهل أيضاً استعمال محطات القاعدة الصغرية هذه. بيد أنها غير آمنة من الناحية المادية كمحطات قاعدة ماكروية مستعملة في شبكات ما قبل الاتصالات المتنقلة الدولية–2020. وعلاوةً على ذلك، فإن زيادة عدد محطات القاعدة ستزيد من مواطن الضعف المحتملة في شبكات الاتصالات المتنقلة الدولية–2020.
- **اختطاف الدورة** [b-ENISA]: اختطاف الدورة، الذي يتعلق بالسطح البيني الأثيري، هو هجوم يستولي فيه المهاجم على دورة مستعمل. وفي حال الاستيلاء على دورة مستيقَنة مشروعة، يتحكم المهاجم في كامل دورة حركة معينة لشن نوع آخر من الهجمات.
- **التهديدات من شبكة نفاذ مزيفة** [b-ENISA]: إذا تعرضت محطة قاعدة للاختراق، يمكن للمهاجم انتحال صفة محطة قاعدة مشروعة وشن هجمة اعتراض وسيط أو تعديل حركة الشبكة. ويؤدي هذا التهديد إلى العبث بالاتصالات بين جهاز المستعمل المتنقل والشبكة لإطلاق الإجراء الآخر.
- **التلاعب ببيانات تشكيلة شبكة النفاذ** [b-ENISA]: في حال اختراق عنصر شبكة النفاذ مثل محطة قاعدة، يمكن للمهاجم تزوير بيانات التشكيلة وشن هجمات أخرى (مثل الحرمان من الخدمة (DoS)).

- **التهديدات الناجمة عن التقاط الهوية (IMSI)** [b-ENISA]: إذا استُغلت بروتوكولات الاستدعاء الخلوي، يمكن لمهاجم أن يربط الهوية البرمجية للضحية مع مناسبة الاستدعاء. ويمكن للمهاجم الخبيث أن يتحقق من معلومات موقع الضحية وأن يحقن رسائل استدعاء مصطنعة وأن يشن هجمات الحرمان من الخدمة.
- **تعطُّل الخدمة جراء التلاعب بطلب توصيل التحكم في الموارد الراديوية (RRC)**: إذا تلاعب المهاجم بطلب توصيل التحكم في الموارد الراديوية (RRC) المرسَل بنص عادي، يمكن عندئذ استعمال معلومات الهوية المؤقتة للضحية لمنع توصيل شبكة الضحية. ويرد وصف سيناريو الهجوم المفصل في التذييل II.

4.8 التهديدات للتوصيل الشبكي المعرَّف بالبرمجيات

يرد وصف للتهديدات التي يتعرض لها التوصيل الشبكي المعرَّف بالبرمجيات في التوصية [ITU-T X.1038].

5.8 التهديدات للشبكة الأساسية

تحدَد التهديدات الأمنية التالية للشبكة الأساسية:

- **الحرمان من الخدمة الموزع (DDoS)** [b-Khan]: يمكن استهلال هجمات الحرمان من الخدمة الموزع في شكل تضخيم التشوير وتشبُّع وظيفة مخدم الاستيقان (AUSF) وإدارة البيانات الموحدة (UDM) باستعمال شبكات روبوتية تتحكم بعدة معدات مستعملين مصابة.
- **تهديدات تتعلق بأمن طبقة النقل (TLS)/طبقة المقابس الآمنة (SSL)** [b-Khan]: إن الاتصالات القائمة على أمن طبقة النقل (TLS)/طبقة المقابس الآمنة (SSL) المستعملة في الشبكات الأساسية القائمة على التوصيل الشبكي المعرَّف بالبرمجيات (SDN) معرضة لهجمات مثل بروتوكول التحكم في الإرسال (TCP)/الحرمان من الخدمة الموزع (DDoS) المتزامن (SYN)، وانحيازات تشفير التكرار بعامل 4 (RC4) في أمن طبقة النقل (TLS)، وهجوم استغلال المتصفح ضد طبقة مقابس الأمن/أمن طبقة النقل (BEAST)، وهجوم بنسبة الضغط المسهِّلة لتسريب المعلومات (CRIME)، وهجوم 13 **المحظوظ** (LUCKY 13) [b-Goodin] وهجوم تحشية خوارزمية oracle للتجفير التقليدي المخفَّض (POODLE) [b-Möller].
- **ماسح التوصيل الشبكي المعرَّف بالبرمجيات** [b-Khan]: يمكن لمهاجم تحليل حركة التوصيل الشبكي المعرَّف بالبرمجيات وجمع معلومات عن الشبكة يدوياً مثل بروتوكول البنية التحتية وعناصر شبكة المفاتيح لوحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات. ويمكن استعمال المعلومات المجمعة لتنفيذ مختلف الهجمات مثل هجمات الحرمان من الخدمة وإعادة ضبط بروتوكول التحكم في الإرسال وهجمات التكرار والانتحال.
- **تحويل وجهة الحركة الخبيث** [b-ENISA]: يسمح اختراق عنصر الشبكة للمهاجمين بتحويل وجهة تدفقات الحركة والتنصّت على حركة الشبكة. ويشكل تحويل وجهة الحركة تهديداً يتعلق بعناصر شبكة مستوي البيانات. والمثال النمطي لتحويل وجهة الحركة في الشبكات الافتراضية هو التجاوز على شريحة من شرائح الشبكة. وقد يحدث هذا التهديد عندما يُخترق العزل بين الشرائح في أي عقدة نشيطة أو عند تجاوز أو إساءة تشكيل إنفاذ النفاذ إلى شريحة في معدات الحافة.
- **إساءة استعمال أدوات المراجعة** [b-ENISA]: يستعمل مشغلو الشبكات أدوات المراجعة لمراقبة نشاط الشبكة والحصول على معلومات يمكن استعمالها لأغراض متعددة كالاستمثال أو الأمن أو لأغراض تجارية. وقد يسمح هذا النوع من الأدوات البرمجية للمهاجمين الخبثاء بالقيام بأنشطة استطلاع لشن هجوم. ويستعمل المهاجم الخبيث عادة مصادر عليمة بدخائل مشغل الشبكة المتنقلة (MNO) وتتمتع بنفاذ مميز إلى هذه الأدوات لاستخلاص معلومات حساسة.
- **تسرب المفتاح طويل الأجل لبيانات استيقان/تخويل المستعمل** [b-ENISA]: يتعلق هذا التهديد بإفشاء مفاتيح طويلة الأجل للاستيقان وضوابط الأمن الذي يقوم به الموظفون الداخليون أو المعادون أو غير الموثوق بهم العاملون في الشبكة الأساسية.
- **استغلال أنظمة/شبكات سيئة أو رديئة التشكيلة** [b-ENISA]: إذا كانت الأنظمة والشبكات مشكَّلة تشكيلةً رديئة أو سيئة، يمكن للمهاجمين النفاذ إلى أصول حرجة. واستغلال نظام مشكَّل تشكيلةً سيئة عن غير قصد يتيح فرصة

للمهاجم للوصول إلى الأصول الحرجة في الشبكة. وقد تحدث أخطاء التشكيلة في مختلف مراحل دورة حياة تنفيذ الحلول مثل تركيب المنتج وصيانته.

- **استشفاف الحركة** [b-ENISA]: يستعمل المهاجمون أداة الاستشفاف لاعتراض حركة الشبكة وبياناتها ولتسجيلها وتحليلها وهي إما كأداة برمجيات أو كأداة عتاد. ومن خلال الاستشفاف، يستطيع المهاجم أيضاً التنصت على البيانات من عناصر الشبكة أو ربط المعلومات الحساسة وسرقتها. ويمكن للاستشفاف أن يحدث في أي مكان توجد فيه حركة مستمرة.
- **تسجيل وظائف الشبكات الخبيثة** [b-ENISA]: يظهر هذا التهديد عند نشر الوظائف الشبكية الخبيثة في شبكات الاتصالات المتنقلة الدولية–2020. ويمكن بشكل مسيء تثبيت وظيفة شبكية غير مخوَّلة أو وظيفة تقوم بإدخال برمجية طروادة إلى الشبكة بواسطة عامل داخلي (بالنسبة إلى مشغل شبكة الاتصالات المتنقلة) أو بائع/مقدم خدمة، في المعمارية القائمة على الخدمة (SBA) وتسجيلها في الشبكة الأساسية عبر وظيفة مستودع وظائف الشبكة (NRF)، من أجل الانكشاف لسطوح بينية خبيثة أخرى لبرمجة التطبيقات. ومن خلال تثبيت أو تفعيل وظيفة شبكية (NF) غير مخوَّلة، قد يتمكن المهاجم من النفاذ إلى أصول حساسة في الشبكة لشن أنواع أخرى من الهجمات مثل الحرمان من الخدمة وتوزيع البرمجيات الخبيثة أو سرقة المعلومات الحساسة.
- **انكشاف وظائف الشبكة غير الآمنة لوظائف تطبيق طرف ثالث** [b-Ta-Hao Ting]: يقدم انكشاف وظيفة الشبكة بين الشبكات الداخلية والخارجية نشراً دينامياً ومرناً للاتصالات المتنقلة الدولية–2020. وإذا انتُحلت الرسالة أو تعرضت للتلاعب، فإنها ستلحق ضرراً بالشبكة الأساسية بأكملها.
- **سطح بيني غير آمن قائم على الخدمة** [b-TS 33.501]: تُنتحل رسالة بين عناصر الشبكة من خلال السطح البيني القائم على الخدمة (SBI) أو تتعرض للتلاعب ويمكن تعديلها وإفشاؤها.

6.8 التهديدات لتقسيم الشبكة إلى شرائح

تحدَد التهديدات التالية لتقسيم الشبكة إلى شرائح:

- **التهديدات للاتصالات بين شرائح الشبكة** [b-Khan]: يمكن للمهاجم تعطيل الاتصالات بين الشرائح لمنع الإدارة السليمة لدورة حياة الشرائح.
- **هجوم انتحال صفة** [b-Khan]: يمكن لمهاجم أن ينتحل صفة منصة مضيف مادية لتوزيع موارد غير متاحة. وعلاوة على ذلك، يمكن للمهاجم انتحال صفة مدير شريحة شبكة لسرقة معلمة إنشاء شريحة شبكة.
- **عدم تطابق سياسات الأمن** [b-Khan]: إن تغاير السياسات الأمنية والبروتوكولات الأمنية للشرائح المختلفة يسمح للمهاجمين بالنفاذ إلى نظام تقسيم الشبكة إلى شرائح والنفاذ إلى كيانات التحكم عبر شريحة أقل أمناً.
- **الحرمان من الخدمة (DoS)** [b-Khan]: يشن المهاجم هجوم حرمان من الخدمة إما على شبكة افتراضية أو على موارد مادية لاستنفاد موارد الشبكة المتاحة لشرائح أخرى.
- **القناة الجانبية** [b-Khan]: يتمكن المهاجم من النفاذ إلى شريحة واحدة ويهاجم مجموعة من الشرائح تتقاسم نفس العتاد الأساسي.
- **تسرب الخصوصية** [b-Khan]: يسرق مقدمو البنية التحتية أو موردو وظائف الشبكة الافتراضية (VNF) معلومات المستعمل عبر الشرائح.
- **التهديدات المتعلقة بالمشرف على الآلات الافتراضية** [b-Khan]: الهجمات ضد المشرف على الآلات الافتراضية لتعريض التمثيل الافتراضي للموارد للخطر. وتشمل هذه الهجمات أخطاء البرمجيات في المشرف على الآلات الافتراضية والدخول من الباب الخلفي عبر نظام التشغيل المضيف وهجمات الحرمان من الخدمة وهجمات على موارد العتاد.

7.8 التهديدات لحوسبة الحافة ذات النفاذ المتعدد

حُددت التهديدات التالية لحوسبة الحافة:

- **مسيِّر حوسبة الحافة ذات النفاذ المتعدد (MEC) الزائف أو المنفلت** [b-ENISA]: يمكن للطبيعة المفتوحة لمسيِّرات الحافة أن تستحدث سيناريو هجومي يمكن فيه للمهاجمين نشر أجهزة المسيِّر الخاصة بهم. ويؤدي هذا التهديد إلى نفس تأثير هجوم الاعتراض الوسيط.
- **زيادة حمولة عقدة الحافة** [b-ENISA]: إذا بدأت تطبيقات متنقلة أو أجهزة معينة لإنترنت الأشياء بإغراق عقدة الحافة بطلبات أو حركة موجهة إلى هذا المكون، قد تحدث زيادة حمولة عقدة الحافة على مستوى محلي أو مستوى الخدمة. ويأتي هذا الهجوم من شبكات الحافة المكونة من أجهزة إنترنت الأشياء القائمة بتعطيل العقد المجاورة للشبكة المتأثرة.
- **إساءة استعمال السطوح البينية المفتوحة لبرمجة التطبيقات في الحافة** [b-ENISA]: إذا استُغلت مواطن الضعف في التطبيقات من نوع حوسبة الحافة ذات النفاذ المتعدد (MEC)، فقد يُساء استعمال السطوح البينية المفتوحة لبرمجة التطبيقات في عقد حوسبة الحافة ذات النفاذ المتعدد. والحاجة إلى سطوح بينية مفتوحة لبرمجة التطبيقات في حوسبة الحافة ذات النفاذ المتعدد تتمثل أساساً في تقديم الدعم للخدمات والتفاعلات الاتحادية مع مختلف مقدمي الخدمات ومنشئي المحتوى. ويمكن أن يرتبط هذا التهديد بالحرمان من الخدمة والاعتراض الوسيط وتسربات الخصوصية والتلاعب في الآلات الافتراضية.
- **العبث المادي بالأجهزة**: الأرجح أن يكون العبث المادي بالأجهزة ممكناً نظراً لأن الموارد الحاسوبية في معمارية حوسبة الحافة أقرب إلى المهاجمين. ويمكن للمهاجم أن يدمر عقد الحافة، وأن ينال بدوره من فعالية الشبكة بأكملها.

8.8 التهديدات للتمثيل الافتراضي لوظائف الشبكة

حُددت التهديدات التالية للتمثيل الافتراضي لوظائف الشبكة:

- **إساءة استعمال بروتوكول التوصيل البيني لمراكز البيانات (DCI)** [b-ENISA]: في حال استغلال مواطن ضعف بروتوكولات DCI، يمكن للمهاجم أن ينشئ حركة منتحَلة. وفي حال نشر الأنظمة الافتراضية ضمن مراكز البيانات، قد يولد ذلك تهديدات أمنية لمراكز البيانات يتعين النظر فيها.
- **إساءة استعمال الموارد الحاسوبية السحابية** [b-ENISA]: إذا استعمل المهاجم عملية تسجيل بسيطة لدى مقدم خدمة الحوسبة السحابية، تمكن إساءة استعمال البنية التحتية الحاسوبية القوية، بما فيها مكونات البرمجيات والعتاد معاً. ويستغل المهاجمون قدرة الحوسبة السائدة للشبكات السحابية ويستطيعون بدء الهجمات في وقت قصير جداً. فعلى سبيل المثال، يمكن للمهاجم أن يشن هجمات مستنفدة لجميع الاحتمالات وهجمات الحرمان من الخدمة من خلال إساءة استعمال قوة الحوسبة السحابية.
- **التجاوز على التمثيل الافتراضي للشبكة** [b-ENISA]: يمكن للإشكالات المتعلقة بسوء تنفيذ تقسيم الشبكة إلى شرائح والتشكيلة غير السليمة أو العزل غير السليم أن تتسبب في فقدان سرية البيانات/الخصوصية (اعتراض كيانات الشرائح الأخرى للبيانات/الحركة). وتحتاج الشبكة التي يستعملها مختلف الشاغلين إلى ضمان حصر الدخول إلى شريحة الشبكة أو مغادرتها في الحركة المشروعة، ولكن أيضاً ضمان قيام أي عنصر تبديل بالتحقق من الحركة وإنفاذ عزلها عن طريق تركيب قواعد تدفق مشروعة تمنع التجاوز على الشرائح. وعلى مستوى الشبكة الأساسية، فإن مهاجماً معادياً من شأنه أن يستغل نقاط ضعف المشرف على الآلات الافتراضية وتشكيلة قاعدة التدفق ليتجاوز على عزل الشرائح ويفشي بيانات تخص شاغلين آخرين.
- **إساءة استعمال المضيف الافتراضي** [b-ENISA]: إذا كانت التطبيقات تعمل على مضيفين افتراضيين، فقد يتسبب ذلك في إساءة استعمال الموارد المشتركة من بيئة افتراضية. وفي البيئات الافتراضية، التي تكون فيها الموارد المادية مشتركة بين الشاغلين، قد تكون هناك مجموعة من السلوكيات التي تؤدي إلى انكشاف معلومات حساسة. فعلى سبيل المثال، يكون التعرض جراء النبش في بيئات افتراضية أكثر خطورة مما يحدث في الأنظمة المادية. وفي حين أن الاعتراض يشكل

تهديداً شائعاً في الأنظمة المادية (مثل بيئات التوصيل الشبكي)، يستفحل تأثيره في البيئات الافتراضية لأنه يسمح بالتفحص المتقاطع لتدفق بيانات مختلف الشاغلين فضلاً عن الاستدلال الطوبولوجي، الأمر الذي يمكن تسخيره لشن هجوم الحرمان من الخدمة.

- **تهديد سلامة البنية التحتية** [b-Alwakeel]: ينتحل المهاجم هوية مقدم الخدمة ليظهر جزءاً من الخدمات الحقيقية للتمثيل الافتراضي لوظائف الشبكة من أجل النفاذ إلى بيانات المستعمل.
- **إساءة استعمال الموارد** [b-Alwakeel]: يُخلي المهاجم بعض الموارد ويستعملها لفائدته.
- **تغيير تعريف وظيفة التمثيل الافتراضي لوظائف الشبكة (NFV)** [b-Alwakeel]: يقوم المهاجم بتعديل بعض العمليات في الخواص الوظيفية للتمثيل الافتراضي لوظائف الشبكة أو تعريفها، أو حتى بالتسبب بالحرمان من الخدمة (DoS). ويجري ذلك عادة عن طريق الحقن.
- **تعديل الامتياز** [b-Alwakeel]: يغير المهاجم امتيازات المستعملين في هجوم البيانات غير ذات الصلة بالتحكم، من خلال ترقية أو تنحية نفاذها إلى كيانات النظام بطريقة غير مجازة.
- **هجوم على السرية على أساس الموارد المشتركة** [b-Alwakeel]: يمكن للمهاجمين، باستعمال هجوم على القنوات الجانبية، سحب بعض المعلومات الخاصة عن مستعملين آخرين باستعمال خدمة مشتركة بطريقة غير مجازة.
- **عامل داخلي خبيث** [b-Alwakeel]: يستعمل الأعضاء الموثوق بهم من داخل منظمة سلطاتهم للنفاذ إلى البيانات الخاصة للمستعملين بطريقة غير مجازة.

9.8 التهديدات للإدارة

حُددت التهديدات التالية التي تتعرض لها الإدارة:

- **سطح بيني غير آمن للإدارة** [b-TR 33.811]: يظهر هذا التهديد عندما لا يكون السطح البيني مأموناً. وهو يمكِّن المهاجمين من النفاذ إلى قدرات إدارة الشبكة دون تخويل ومن إنشاء حالات لشرائح الشبكة تتطلب موارداً كبيرة من الشبكة، أو عدداً كبيراً من حالات شرائح الشبكة.
- **انكشاف بيانات الإشراف والإبلاغ ذات الصلة بوظيفة الإدارة** [b-TR 33.811]: يظهر هذا التهديد عندما لا تكون بيانات الإشراف والإبلاغ محمية بطريقة ملائمة. ويؤدي ذلك إلى عبث المهاجم بنتائج الإشراف/الإبلاغ وتنصته على إرسال بيانات الإشراف والإبلاغ واستخلاصه المعلومات الحساسة التي يمكن استعمالها لتنفيذ هجمات لتشغيل حالات شرائح الشبكة.
- **النفاذ غير المجاز إلى السطح البيني لانكشاف الإدارة** [b-Ta-Hao Ting]: إذا تعرض السطح البيني للاختراق بنفاذ غير مجاز، يمكن أن تتعرض وظائف الشبكة مثل التوصيل الشبكي المعرَّف بالبرمجيات (SDN) والتمثيل الافتراضي لوظائف الشبكة (NFV) وشريحة الشبكة لحالات خلل غير ملائمة مثل التغييرات غير المجازة في وظائف الشبكة واستحداث تشكيلات شبكية غير مناسبة وتعديل وظيفة الشبكة.

9 متطلبات القدرات الأمنية المتصلة بالمكونات والوظائف

1.9 القدرات الأمنية المتصلة بمعدات المستعمل

ينبغي دعم القدرات الأمنية التالية لمعدات المستعمل:

- **القدرة على مكافحة البرمجيات الخبيثة لتأمين معدات المستعمل**: مكافحة البرمجيات الخبيثة هي نوع من البرمجيات المصممة لمنع البرمجيات الضارة (البرمجيات الخبيثة) في معدات المستعمل وكشفها وإزالتها. وتُستعمل ثلاثة أساليب، هي كشف البرمجيات الخبيثة القائمة على التوقيع وكشف البرمجيات الخبيثة القائمة على السلوك ومنصات التجارب، لحماية معدات المستعمل من الإصابة بالبرمجيات الخبيثة.

- **القدرة الأمنية لهوية مشترك في الخدمة المتنقلة الدولية (IMSI) لتأمين هوية المشترك (IMSI) عن طريق التجفير:** ينبغي تجفير هوية مشترك في الخدمة المتنقلة الدولية (IMSI) بمفتاح تجفير سريع الزوال باستعمال خوارزمية تجفير متناظرة مثل الخاصة به والمفتاح اللاتناظري العمومي للشبكة المحلية وأن يكون لكل مشغل اتصالات متنقلة (يسمى هنا "الشبكة المحلية") زوج المفتاحين غير المتناظرين العمومي/الخاص. ويُفترض بالشبكة المحلية الحفاظ على سرية المفتاح اللاتناظري الخاص بها، في حين يهيَأ المفتاح اللاتناظري العمومي للشبكة المحلية مسبقاً في الأجهزة المتنقلة إلى جانب الهويات IMSI الخاصة بالمشترك.
- **قدرة التحقق من الهوية:** تتحقق من هوية المستعمل لخدمات التجوال والخدمات السحابية.
- **قدرة إدارة المفاتيح:** تدعم التحقق من هوية المستعمل والاستيقان المتبادل بين جهاز المستعمل وعنصر الشبكة.
- **قدرة أمن الموقع:** تضمن أمن موقع المستعمل.
- **استيقان الشبكة المخدِّمة:** ينبغي أن يستيقن جهاز المستعمل معرّف هوية الشبكة المخدِّمة عن طريق استيقان المفتاح ضمنياً، أي: أن الاستيقان يتحقق من خلال الاستعمال الناجح للمفاتيح الناتجة عن الاستيقان واتفاق المفتاح في إجراءات لاحقة.
- **سرية وسلامة بيانات المستعمل وبيانات التشوير** [b-ITU-T X.1811]: لدى معدات المستعمل القدرة على دعم سرية البيانات من خلال خوارزميات تجفير، ودعم حماية سلامة بيانات المستعمل وحمايتها من التكرار بين معدات المستعمل وعقد الشبكة.
- **قدرة التخزين والمعالجة الآمنة لبيانات اعتماد الاشتراك** [b-Craven]: لدى معدات المستعمل القدرة على تقديم حماية سلامة بيانات الاعتماد ومفاتيحها طويلة الأجل عن طريق العتاد المقاوم للعبث. وينبغي ألا تتاح المفاتيح طويلة الأجل غير المجفرة خارج العتاد المقاوم للعبث. وينبغي تشغيل البرنامج في العتاد المقاوم للعبث باستعمال خوارزمية استيقان وبيانات اعتماد الاشتراك.

2.9 القدرات الأمنية المتصلة بشبكة النفاذ

ينبغي دعم القدرات الأمنية التالية لشبكة النفاذ:

- **قدرة أمن الوصلة:** تقدم سرية الاتصالات وسلامتها لقنوات التحكم وقنوات حركة المستعمل مع معدات المستعمل.
- **قدرة استيقان معدات المستعمل:** ينبغي أن تستيقن الشبكة المخدِّمة معرف الهوية الدائم للاشتراك في عملية الاستيقان واتفاق المفاتيح بين جهاز المستعمل والشبكة.
- **قدرة تخويل معدات المستعمل** [b-Craven]: ينبغي للشبكة المخدِّمة أن تخوِّل جهاز المستعمل باستعمال البيانات الوصفية للاشتراك المحصَّلة من الشبكة المحلية.
- **قدرة الشبكة المحلية على التخويل للشبكة المخدِّمة** [b-Craven]: ينبغي ضمان أن يكون جهاز المستعمل موصولاً بشبكة خدمة تسمح بها الشبكة المحلية.
- **قدرة تخويل شبكة النفاذ** [b-Craven]: ينبغي أن تخول الشبكة المخدِّمة لشبكة النفاذ بتقديم الخدمات لمعدات المستعمل.
- **قدرة سرية بيانات المستعمل والتشوير** [b-Craven]: ينبغي أن تدعم شبكة النفاذ تجفير بيانات المستعمل العابرة ولتشوير التحكم في الموارد الراديوية (RRC).
- **قدرة سلامة بيانات المستعمل والتشوير** [b-Craven]: ينبغي للعُقد، مثل معدات المستعمل، أن تدعم حماية سلامة بيانات المستعمل وحمايتها من تكرار التشغيل بين جهاز المستعمل والعقدة التالية B.
- **قدرة الإعداد والتشكيل** [b-Craven]: عند إعداد وتشكيل أنظمة التشغيل والإدارة (O&M)، ينبغي استيقان العقدة التالية B والتخويل لها من سلطة تسجيل وسلطة إصدار الشهادات (RA/CA) بحيث يعجز المهاجمون عن تعديل الإعدادات وتشكيلات البرمجيات الخاصة بالعقدة B التالية.

- **قدرة إدارة المفاتيح داخل العقدة B التالية** [b-Craven]: تدعو الحاجة لحماية العناصر المختلفة لمفاتيح التشفير التي تقدمها شبكة IMT-2020 الأساسية للعقدة التالية B.
- **قدرة معالجة بيانات مستوي المستعمل ومستوي التحكم** [b-Craven]: هي قدرة لإدارة المفاتيح مماثلة لتلك الخاصة بمعالجة بيانات مستوي المستعمل ومستوي التحكم للعقدة B التالية.
- **قدرة تهيئة بيئة آمنة** [b-Craven]: تخضع البيئة الآمنة التي تعمل بها جميع هذه البيانات غير المجفَّرة لمتطلبات أيضاً. وينبغي أن تدعم التخزين الآمن من خلال أسرار التجفير الطويلة الأجل وبيانات التشكيلة الحيوية على سبيل المثال.
- **القدرة على التصدي لتهديدات تعطل الخدمة الناجمة عن طلبات توصيل التحكم في الموارد الراديوية (RRC)**: لمنع تهديد طلب توصيل التحكم في الموارد الراديوية، يتعين على محطة القاعدة الحفاظ على توصيل التحكم في الموارد الراديوية مع المستعمل القائم لفترة أطول من الوقت. ويؤدي ذلك لاحتفاظ محطة القاعدة بالتوصيل لفترة أطول من مؤقت الانتظار لتوصيل التحكم في الموارد الراديوية القائم. وبالإضافة إلى ذلك، ينبغي استعمال معلمتي "تقييد الوقت" و"تقييد التعداد" في محطة القاعدة والتحقق عبر عملية المراقبة مما إذا كان هذا الهجوم يُشَن أم لا. ويرد وصف سيناريو الهجوم المفصل في التذييل II.

3.9 القدرات الأمنية المتصلة بالتوصيل الشبكي المعرَّف بالبرمجيات

ينبغي دعم القدرات الأمنية التالية للتوصيل الشبكي المعرَّف بالبرمجيات [ITU-T X.1038]:

- **قدرة استيقان** تطبيق التوصيل الشبكي المعرَّف بالبرمجيات (SDN) لاستيقان وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات/المستعمل/المدير؛
- **قدرة التخويل** لتطبيق التوصيل الشبكي المعرَّف بالبرمجيات (SDN) من أجل تخويل المستعمل/المدير بالنفاذ إلى معلومات النظام؛
- **قدرة سرية بيانات** تطبيق التوصيل الشبكي المعرَّف بالبرمجيات (SDN) لتقديم حماية لسرية معلومات النظام المخزنة في منصة التطبيق ولإجراء حماية لسرية نقل البيانات عبر السطح البيني للتحكم في التطبيق؛
- **قدرة إدارة مفتاح/شهادة** تطبيق التوصيل الشبكي المعرَّف بالبرمجيات (SDN)، لدعم إدارة المفتاح/الشهادة؛
- **قدرة إدارة أمن** تطبيق التوصيل الشبكي المعرَّف بالبرمجيات لدعم السجل والمراجعة؛
- **قدرة حماية تطبيق** التوصيل الشبكي المعرّف بالبرمجيات لدعم الدفاع عن مواطن ضعف التطبيق؛
- **قدرة سلامة بيانات** تطبيق التوصيل الشبكي المعرَّف بالبرمجيات (SDN)، لدعم أداء حماية السلامة لنقل البيانات عبر السطح البيني للتحكم في التطبيق؛
- **قدرة الاستيقان** في وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات لاستيقان المديرين/تطبيق التوصيل الشبكي المعرَّف بالبرمجيات/بدالة التوصيل الشبكي المعرَّف بالبرمجيات؛
- **قدرة التخويل** لوحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) من أجل التخويل للمديرين/تطبيق التوصيل الشبكي المعرَّف بالبرمجيات لإدارة وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات؛
- **قدرة الاستيقان وإدارة الأمن** لوحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) لدعم حماية مكافحة الحرمان من الخدمة (DoS)؛
- **قدرة سلامة بيانات وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات** للقيام بحماية سلامة بيانات التشكيلة المخزنة في وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات، وللقيام بحماية سلامة بيانات المستعمل المخزنة في وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات، وللقيام بحماية سلامة نقل البيانات عبر السطح البيني للتحكم في التطبيق، وللقيام بحماية سلامة نقل البيانات عبر السطح البيني للتحكم في الموارد؛

- **قدرة إدارة المفاتيح/الشهادات** في وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) كي تقوم بإدارة المفاتيح/الشهادات؛
- **قدرة سرية بيانات وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات** للقيام بحماية سرية بيانات التشكيلة المخزنة في وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات، وللقيام بحماية سرية بيانات المستعمل المخزنة في وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات، وللقيام بحماية سرية نقل البيانات عبر السطح البيني للتحكم في التطبيق، وللقيام بحماية سرية نقل البيانات عبر السطح البيني للتحكم في الموارد؛
- **قدرة مناعة نظام التشغيل في وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات** لدعم الخواص الوظيفية لمناعة نظام التشغيل؛
- **قدرة استيقان طبقة موارد التوصيل الشبكي المعرَّف بالبرمجيات** لاستيقان المديرين/وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات؛
- **قدرة التخويل في طبقة موارد التوصيل الشبكي المعرَّف بالبرمجيات** للتخويل للمديرين/وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات؛
- **قدرة إدارة أمن طبقة موارد التوصيل الشبكي المعرَّف بالبرمجيات** لدعم السجل والمراجعة؛
- **قدرة سلامة بيانات طبقة موارد التوصيل الشبكي المعرَّف بالبرمجيات** للقيام بحماية سلامة بيانات التشكيلة المخزنة في بدالة التوصيل الشبكي المعرَّف بالبرمجيات، وللقيام بحماية سلامة نقل بيانات بدالات التوصيل الشبكي المعرَّف بالبرمجيات/للقيام بحماية سلامة نقل البيانات عبر السطح البيني للتحكم في الموارد؛
- **قدرة إدارة المفاتيح/الشهادات لطبقة موارد التوصيل الشبكي المعرَّف بالبرمجيات (SDN)** كي تقوم بإدارة المفاتيح/الشهادات؛
- **قدرة سرية بيانات طبقة موارد التوصيل الشبكي المعرَّف بالبرمجيات** للقيام بحماية سرية بيانات التشكيلة المخزنة في بدالة التوصيل الشبكي المعرَّف بالبرمجيات، وللقيام بحماية سرية نقل بيانات بدالات التوصيل الشبكي المعرَّف بالبرمجيات/للقيام بحماية سرية نقل البيانات عبر السطح البيني للتحكم في الموارد؛
- **قدرة منع فيض جدول التدفق في طبقة موارد التوصيل الشبكي المعرَّف بالبرمجيات.** تحتاج وحدة تحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) للحفاظ على جدول التدفق دينامياً بإدراج وحذف إدخالات التدفق.

4.9 القدرات الأمنية المتصلة بالشبكة الأساسية

ينبغي دعم القدرات الأمنية التالية:

- **قدرة كشف الحرمان من الخدمة (DoS) والحرمان من الخدمة الموزَّع (DDoS) وقدرة الحماية** لحماية نقطة التحكم المركزية في التوصيل الشبكي المعرَّف بالبرمجيات؛
- **قدرة التحقق من التشكيلة** للتحقق من قواعد التدفق في عنصر شبكة التوصيل الشبكي المعرَّف بالبرمجيات (SDN)؛
- **قدرة التحكم في النفاذ** للحد من النفاذ إلى شبكة التوصيل الشبكي المعرَّف بالبرمجيات وعناصر الشبكة الأساسية.

وينبغي دعم القدرات الأمنية التالية لوظيفة انكشاف الشبكة والسطح البيني القائم على الخدمة:

- **قدرات انكشاف وظائف الشبكة الآمنة** [b-TS 33.501]: ينبغي إجراء استيقان متبادل قائم على شهادتي العميل والمخدِّم بين وظيفة انكشاف الشبكة ووظيفة تطبيق وظائف تطبيق طرف ثالث خارج ميدان مشغل الاتصالات المتنقلة الدولية–2020، التي يقدمها نفق آمن مثل أمن طبقة النقل (TLS). وينبغي استعمال الحركة بين وظيفة انكشاف الشبكة (NEF) ووظيفة التطبيق لتقديم حماية السلامة وحماية التكرار وحماية السرية.

- **سرية وسلامة البيانات واستيقان عناصر الشبكة من خلال سطح بيني قائم على الخدمة** [b-TS 33.501]: ينبغي للحركة بين عناصر الشبكة من خلال السطح البيني القائم على الخدمة (SBI) أن تقدم حماية سلامة البيانات وحماية التكرار وحماية سرية البيانات واستيقان عناصر الشبكة من خلال نفق آمن مثل أمن طبقة النقل.

5.9 القدرات الأمنية المتصلة بتقسيم الشبكة إلى شرائح

ينبغي دعم القدرات الأمنية التالية المتعلقة بدورة حياة الشريحة [b-Olimid]:

- **القدرة الأمنية لدورة حياة الشريحة:** ينبغي إنفاذ الأمن في المراحل الأربع كلها لأن نقطة الضعف في مرحلة ما يمكن أن تسبب نقاط ضعف في المراحل الأخرى.
- **قدرة التسجيل والمراجعة الملائمة:** ينبغي تنفيذ مستويات مختلفة للتسجيل في شرائح شبكة متمايزة تبعاً لعوامل مختلفة مثل اللوائح (من قبيل متطلبات الاعتراض المشروع)، ومستوى الأمن المستهدف للخدمات المستهلكة، والنوع المخصص من أجهزة العملاء وتنبغي حماية نتائج السجلات والتقارير، لأن انكشافها من شأنه أن يسرب معلومات حساسة.
- **القدرة الأمنية لنموذج شريحة الشبكة المعياري:** تنبغي حماية السرية والسلامة في الإرسال والتخزين، وينبغي استيقان مصدر النموذج المعياري.
- **قدرة تنسيق الأمن:** ينبغي تنسيق ونشر الخدمات الأمنية المكيفة حسب الطلب وفقاً للمتطلبات الأمنية لمختلف الصناعات التخصصية [b-ITU-T X.1047].
- **قدرة عزل الشرائح:** ينبغي تأمين العزل عند إنشاء الشرائح ومراقبته وتحديثه، إذا اقتضى الأمر، خلال وقت التنفيذ [b-ITU-T X.1047].
- **القدرة الأمنية للسطح البيني لبرمجة التطبيقات (API):** ينبغي أن تكون السطوح البينية لبرمجة التطبيقات آمنة من حيث النفاذ وحقوق التشغيل وألا تكشف بيانات الحركة؛ وينبغي للسطوح البينية لبرمجة التطبيقات ألا تسمح بقدرات ونفاذ إلى بيانات إلا على النحو المتفق عليه بين الأطراف بوسائل قانونية.
- **قدرة السحب من الخدمة:** ينبغي إتلاف البيانات الحساسة عند سحبها من الخدمة (أو تخزينها بطريقة آمنة على أساس كل حالة على حدة) وينبغي عندئذ إخلاء الموارد ووظائف الشبكة.

وينبغي دعم القدرات الأمنية التالية المتعلقة بالأمن داخل الشريحة:

- **القدرات الأمنية من طرف إلى طرف:** تمثل الشرائح شبكات منطقية من طرف إلى طرف، ولذلك ينبغي النظر في الأمن من طرف إلى طرف [b-ITU-T X.1047]؛
- **قدرة الاستعمال الملائم لآليات الأمن:** جميع الاتصالات (كتلك بين الشريحة وطبقة الموارد، وبين الشريحة ومدير الشريحة، وبين الشرائح الفرعية للشريحة، وبين جهاز العميل ونقطة النفاذ في الشبكة) ينبغي أن تستعمل آليات كافية لضمان المستوى الأمني المستهدف؛ وينبغي أن تتضمن المتطلبات الدنيا سرية وسلامة واستيقان البيانات والاستيقان المتبادل بين النظراء؛
- **قدرة استيقان معدات المستعملين (UE):** ينبغي التشدد في استيقان أجهزة عملاء الاتصالات المتنقلة الدولية-2020 عن طريق الاستيقان الأولي والمفضل على أساس ثانوي؛
- **القدرة المستهلكة للخواص الوظيفية الآمنة للموارد:** ينبغي تأمين جميع الموارد ووظائف الشبكة التي تستهلكها شريحة ما؛
- **قدرة أمن الشاغلين:** ينبغي تأمين المرافق الجديدة التي يدخلها الشاغلون (من قبيل وظائف الشبكة والتشكيلات والخدمات) وتكاملها بطريقة ملائمة لمنع زيادة استغلال مواطن الضعف؛
- **قدرة أمن الهوية:** تنبغي حماية المعرفات الحساسة وينبغي عدم تسريب أي ترابط بين المعرفات؛
- **الاعتراض القانوني:** ينبغي أن يكون النفاذ إليه متاحاً في طبقتي الشريحة والخدمة؛

- **قدرات النفاذ والحقوق والتشكيلة:** ينبغي أن تطابق هذه القدرات الاتفاقات القانونية المبرمة بين الأطراف.

وينبغي دعم القدرات الأمنية التالية المتعلقة بالاتصالات بين الشرائح:

- ينبغي منح حد أدنى من المستوى الأمني لكل شريحة؛
- **قدرة عزل الشرائح:** ينبغي أن يكون العزل بين الشرائح قوياً بما يكفي لمنع الهجمات عبر الشرائح الأقل أمناً [b-ITU-T X.1047]؛
- **قدرة الحد الأدنى من أمن الاتصالات:** ينبغي خفض الاتصالات بين الشرائح إلى أدنى حد وتعريفها بقواعد صارمة وتنفيذها عبر قنوات مؤمنة؛
- **قدرة إدارة المفاتيح:** ينبغي عدم تناقل مفاتيح التجفير (ومعلمات حساسة أخرى) بين الشرائح؛
- **الحد الأدنى من قدرة توزيع الموارد:** ينبغي أن يضمن توزيع الموارد مستوى أدنى من التوفر لكل شريحة؛ وعلى وجه الخصوص، ينبغي لآليات الأمن أن تكون قادرة على العمل بغض النظر عن استهلاك الموارد؛
- ينبغي للشرائح ذات الفرق الكبير في مستويات الأمن ألا تتقاسم الموارد أو وظائف الشبكة، وعلى وجه الخصوص، عدم تشغيل الشرائح بأسلوب الاختبار مع شرائح في مرحلة التشغيل؛
- **قدرة أمنية مستقلة:** ينبغي أن تكون آليات الاستيقان والتخويل والتحكم في النفاذ مستقلة في كل شريحة.

6.9 القدرات الأمنية المتصلة بحوسبة الحافة ذات النفاذ المتعدد

ينبغي دعم القدرات الأمنية التالية:

- **قدرة تخفيف الحرمان من الخدمة الموزَّع (DDoS)** لحماية خدمات الإنترنت السحابية؛
- **قدرة التحكم في النفاذ** للحد من عناصر شبكة حوسبة الحافة ذات النفاذ المتعدد؛
- **قدرة التحقق من السلامة** لتأمين البيانات ونظام التخزين في الحوسبة السحابية؛
- **قدرة التحكم في النفاذ إلى الخدمة** للحد من عنصر الحوسبة السحابية القائم على الخدمة؛
- **قدرة أمن مادية:** ينبغي الإيفاء بالأمن المادي لأي عقد حافة لا تقع في مراكز بيانات الحافة الآمنة للغاية، كتلك التي تستعمل تقنيات حماية مادية إضافية أثناء تصنيع أو تنفيذ آليات إقفال وغيرها من الضمانات المادية في الميدان.

7.9 القدرات الأمنية المتصلة بالتمثيل الافتراضي لوظائف الشبكة

ينبغي دعم القدرات الأمنية التالية:

- **قدرة عزل الحركة:** وهي لضمان الشرائح الافتراضية ووظائف الشبكة الافتراضية.
- **قدرة منع هجوم الحرمان من الخدمة** [b-Alwakeel]: ينبغي استعمال عناصر الشبكة، من قبيل جدران الحماية وموازِنات الحمولة، للتخفيف من هجمات الحرمان من الخدمة (DoS)/ الحرمان من الخدمة الموزَّع (DDoS).
- **قدرة سلامة البنية التحتية** [b-Alwakeel]: ينبغي استعمال سلسلة من الثقة ووحدة منصة موثوقة (TPM) لضمان أمن مختلَف مقدمي خدمات وظائف الشبكة الافتراضية (VNF).
- **قدرة التخفيف من سوء استعمال الموارد** [b-Alwakeel]: ينبغي تقديم جدول مواعيد المشرف على الآلات الافتراضية المتقدم الذي يقوم بتوزيع الحصص العادل بين العمليات وبتحديد القدر الأقصى المسموح به لكل خدمة افتراضية.
- **قدرة الحماية من تغيير تعريف وظيفة الشبكة الافتراضية (NFV)** [b-Alwakeel]: ينبغي الاحتفاظ بنسخة من الخدمات الافتراضية للمستعمل في تخزين منفصل لمنع هجمات حقن البرمجيات الضارة. ويُستعمل جدول توزيع الملفات (FAT) الذي يحتوي على معلومات عن الخدمات والبرمجيات التي ينفذها المستعمل.

- **قدرة منع تعديل الامتياز** [b-Alwakeel]: ينبغي تقديم حماية كيان التمثيل الافتراضي من النفاذ غير المخوَّل، وذلك بإضافة سياسات تقييدية للنفاذ إلى الموارد.
- **قدرة تخفيف الموارد المشتركة** [b-Alwakeel]: ينبغي استعمال قدرة تخفيف هجمات القنوات الجانبية لتقييد النفاذ إلى مكونات صور الآلة الافتراضية والبنية التحتية للتمثيل الافتراضي لوظائف الشبكة (NFVI) والتحكم في استعمال الموارد. ويمكن تحقيق ذلك باستعمال جدار حماية افتراضي لمنع النفاذ غير المجاز إلى النظام.
- **قدرة تخفيف العامل الداخلي الخبيث** [b-Alwakeel]: يمكن التخفيف من هجمات عامل داخلي باستعمال عدة قدرات يقوم أحدها بتسجيل عمليات النفاذ في بيئة التمثيل الافتراضي لوظائف الشبكة والتي يمكن بعد ذلك استعمالها لعمليات المراجعة الداخلية لكشف النشاط المشبوه. وتتمثل آلية أخرى في وضع سياسات صارمة بشأن الاستيقان والتخويل للمستعملين القادرين على النفاذ.

8.9 القدرات الأمنية المتصلة بوظيفة الإدارة

ينبغي دعم القدرات الأمنية التالية [b-TR 33.811]:

- **قدرة الاستيقان المتبادل** بين مستهلك خدمة الإدارة ومنتِج خدمة الإدارة باستعمال نفق آمن مثل أمن طبقة النقل (TLS) استناداً إما إلى (1) شهادتي العميل والمخدمات أو (2) المفاتيح المشتركة مسبقاً (PSK) مع TLS-PSK؛
- **قدرة حماية السلامة وحماية التكرار وحماية السرية** للسطح البيني بين منتِج خدمة الإدارة ومستهلك خدمة الإدارة الكائن خارج ميدان الثقة لأمن طبقة النقل (TLS) لدى مشغِّل مشروع شراكة الجيل الثالث (3GPP)؛
- **قدرة أمن المعلومات المحدِّدة لهوية شخص (PI) في السطح البيني للإدارة**: ينبغي للسطوح البينية لبرمجة التطبيقات (API) أن تكون آمنة من حيث النفاذ والحقوق التشغيلية وألا تكشف بيانات الحركة، وينبغي لسطوح التماس لبرمجة التطبيقات مع السطح البيني للإدارة ألا تسمح إلا بالقدرات والنفاذ إلى البيانات على النحو المتفق عليه بين الأطراف بالوسائل القانونية.

الملحق A

معمارية أمن نظام الاتصالات المتنقلة الدولية–2020 (IMT-2020)

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية.)

يقدم الشكل 4-1 الوارد في [b-TS 33.501] لمحة عامة عن معمارية أمن نظام الاتصالات المتنقلة الدولية–2020.

يوضح الشكل 4-1 ميادين الأمن التالية:

- أمن النفاذ إلى الشبكة (I): مجموعة الميزات الأمنية التي تمكن معدات المستعمل من الاستيقان وخدمات النفاذ عبر الشبكة بصورة آمنة، بما في ذلك عبر شبكة النفاذ الموصَّفة في مشروع شراكة الجيل الثالث (3GPP) وشبكة نفاذ غير الموصَّفة في مشروع شراكة الجيل الثالث، وبوجه خاص، للحماية من الهجمات على السطوح البينية (الراديوية). وبالإضافة إلى ذلك، فهي تشمل إيصال سياق الأمن من الشبكة المخدِّمة (SN) إلى شبكة النفاذ (AN) من أجل أمن النفاذ.
- أمن ميدان الشبكة (II): مجموعة الميزات الأمنية التي تمكن عُقد الشبكة من تبادل بيانات التشوير وبيانات مستوي المستعمل بشكل آمن.
- أمن ميدان المستعمل (III): مجموعة الميزات الأمنية التي تضمن نفاذ المستعمل إلى المعدات المتنقلة.
- أمن ميدان التطبيق (IV): مجموعة الميزات الأمنية التي تمكن التطبيقات في ميدان المستعمل وفي ميدان مقدم الخدمة من تبادل الرسائل بشكل آمن. ولا يندرج أمن ميدان التطبيق ضمن مجال تطبيق هذه التوصية.
- أمن ميدان المعمارية القائمة على الخدمة (SBA) (V): مجموعة الميزات الأمنية التي تمكن وظائف الشبكة في المعمارية القائمة على الخدمة من الاتصال الآمن ضمن ميدان الشبكة المخدِّمة ومع الميادين الأخرى للشبكة. وتشمل هذه الميزات جوانب الأمن المتعلقة بالتسجيل والاكتشاف والتخويل في وظائف الشبكة، فضلاً عن حماية السطوح البينية القائمة على الخدمة. وأمن ميدان المعمارية القائمة على الخدمة هو ميزة أمنية جديدة مقارنةً مع المعيار [b-TS 33.401].
- قابلية رؤية وقابلية تشكيل الأمن (VI): هي مجموعة الميزات التي تمكّن المستعمل من الاطلاع على ما إذا كانت ميزة أمنية قيد التشغيل أم لا.

التذييل I

معمارية أمن الشبكة العامة لتقديم أمن الشبكة من طرف إلى طرف

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

يصف هذا التذييل معمارية أمن الشبكة العامة لتقديم أمن الشبكة من طرف إلى طرف، ويرد وصفها في التوصية [b-ITU-T X.805]، وهي أساس لهذه التوصية.

ويرد في التوصية [b-ITU-T X.805] تعريف معمارية أمن لتقديم أمن الشبكة من طرف إلى طرف. ويمكن تطبيق هذه المعمارية على مختلف أشكال الشبكات حيث يكون الأمن من طرف إلى طرف مصدر قلق ويعمل بشكل مستقل عن التكنولوجيا التي تقوم عليها الشبكة. وتعرّف التوصية [b-ITU-T X.805] العناصر المعمارية العامة المتعلقة بالأمن اللازمة لتقديم الأمن من طرف إلى طرف. والهدف من التوصية [b-ITU-T X.805] هو أن تكون أساساً لوضع توصيات مفصلة بشأن أمن الشبكة من طرف إلى طرف.

وتعرّف التوصية [b-ITU-T X.805] ثمانية أبعاد أمنية:

1) التحكم في النفاذ؛
2) الاستيقان؛
3) عدم التنصل؛
4) سرية البيانات؛
5) أمن الاتصالات؛
6) سلامة البيانات؛
7) التيسر؛
8) الخصوصية.

وتعرِّف التوصية [b-ITU-T X.805] أيضاً ثلاث طبقات أمنية تقوم على بعضها البعض لتقديم حلول قائمة على الشبكة:

1) طبقة أمن البنية التحتية؛
2) طبقة أمن الخدمات؛
3) طبقة أمن التطبيقات.

وبالإضافة إلى ذلك، تعرّف التوصية [b-ITU-T X.805] ثلاثة مستويات أمنية:

1) مستوي الإدارة؛
2) مستوي التحكم؛
3) مستوي المستعمل النهائي.

التذييل II

تهديد تعطُّل الخدمة جراء التلاعب بطلب توصيل التحكم في الموارد الراديوية (RRC) وقدرته

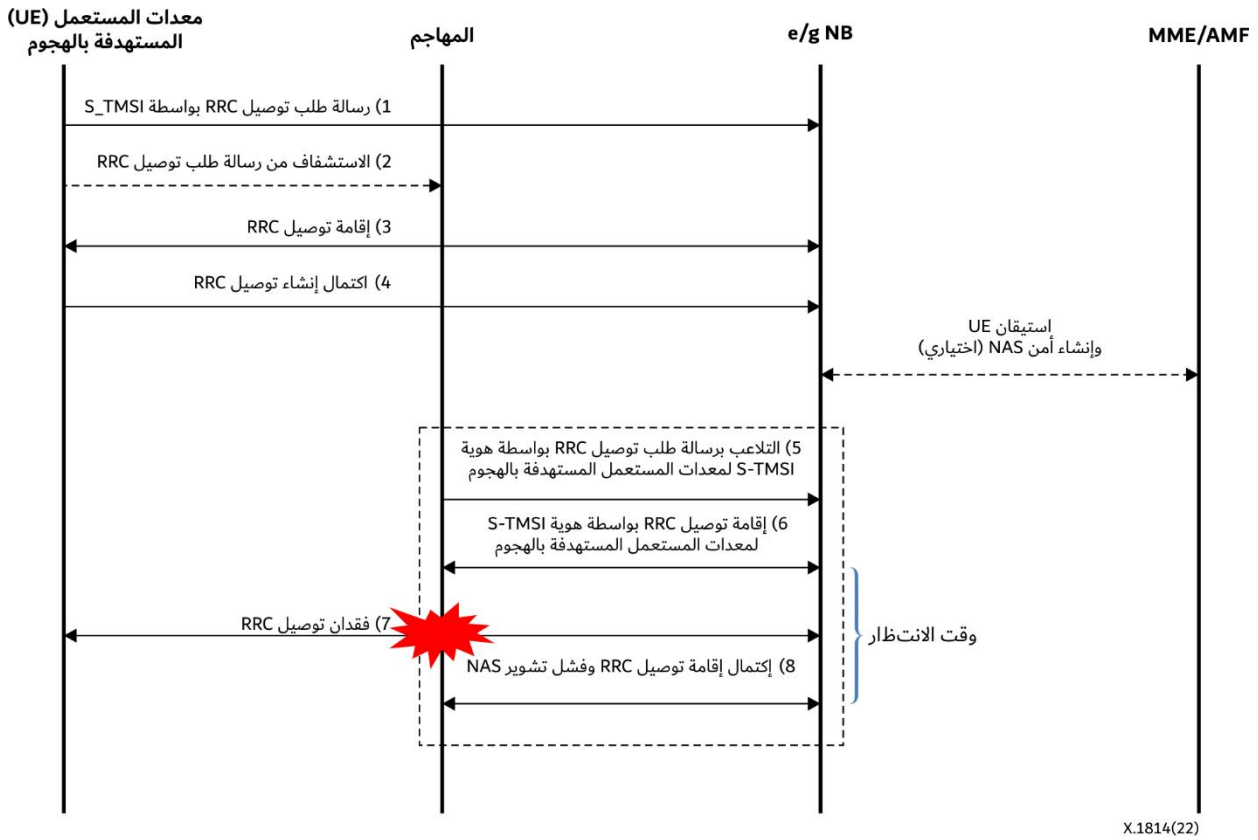
(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

1.II لمحة عامة

إن طلب توصيل التحكم في الموارد الراديوية (RRC) هو رسالة تُرسَل عندما ينفذ جهاز المستعمل إلى شبكة، وتُرسَل بنص واضح. وهي تشمل هوية مؤقتة فريدة عالمياً (GUTI) أو هوية مؤقتة مخدِّمة للمشترك في الخدمة المتنقلة (S-TMSI)، وهي معلومات تعريف مؤقتة لمعدات المستعمل. وهناك عدة طرق للعثور على معلومات الهوية المؤقتة لمستعمل معين. وعندما يلتقط مهاجم طلب توصيل التحكم في الموارد الراديوية ويعدل هذه الرسالة المرسلة بنص واضح في الخطوة السابقة، يمكن عندئذٍ استعمال معلومات التعرف المؤقت للضحية لمنع التوصيل الشبكي للضحية.

2.II سيناريو الهجوم

يمكن لمهاجم أن يعترض رسالة طلب توصيل التحكم في الموارد الراديوية (RRC) المرسَلة بنص واضح ويتعرف على هوية مؤقتة فريدة عالمياً (GUTI) أو هوية مؤقتة مخدِّمة للمشترك في الخدمة المتنقلة (S-TMSI)، توفر معلومات تعرُّف هوية مؤقتة. وعند إرسال رسالة مزوَّرة لطلب توصيل التحكم في الموارد الراديوية، يسيء المهاجم استعمال معلومات تعرف الهوية المؤقتة ويُظَّن خطأً أن رسالته مرسَلة من معدات المستعمل (UE) المستهدَفة بالهجوم. وعلى الرغم من فك توصيل طلب توصيل التحكم في الموارد الراديوية من المهاجم بسبب عدم الاستيقان بشفرة استيقان الرسالة (MAC) أثناء التشوير في طبقة عدم النفاذ (NAS)، يستطيع المهاجم أن يمنع باستمرار التوصيل الراديوي للضحية بإرسال نفس الرسالة المزيفة مرة أخرى. وبالإضافة إلى ذلك، تُستحدث مجدداً معلومات مؤقتة لتعرف الهوية على فترات منتظمة وفقاً لقواعد محددة تستند إلى هوية مشترك في الخدمة المتنقلة الدولية (IMSI). وإذا تغيرت الهوية المؤقتة المخدِّمة للمشترك في الخدمة المتنقلة، عندئذ يمكن للمهاجم أن يكشف التغيير وأن يرسل رسالة هجوم مرة أخرى. ولمنع معدات المستعمل المتضررة من النفاذ الراديوي، يحتاج المهاجم إلى إرسال رسالة مزوَّرة لطلب توصيل التحكم في الموارد الراديوية. وهناك شرطان مسبقان لهذا الهجوم: (1) يحتاج المهاجم إلى وضع جهازه المتنقل في نفس الخلية كتلك الخاصة بمعدات المستعمل المستهدَفة بالهجوم لالتقاط الحركة الراديوية؛ (2) يمتلك المهاجم معدات مستعمل يمكنها إرسال رسالة مزوَّرة.



الشكل II.1 – سيناريو الهجوم بالتلاعب بطلب توصيل التحكم في الموارد الراديوية (RRC)

II.3 العواقب

جراء نقطة الضعف هذه، وبغياب التحقق مما إذا كانت الرسالة قد تعرضت للعبث، تقطع معدات الشبكة الراديوية (محطة القاعدة e/gNodeB) التوصيل القائم مع معدات المستعمل المستهدَفة بالهجوم وفقاً للرسالة المرسَلة من المهاجم ويُوصل معدات المستعمل الخاصة بالمهاجم. وقد تظل معدات المستعمل المستهدَفة بالهجوم في حالة تعجز فيها عن النفاذ إلى الشبكة بشكل طبيعي.

II.4 التدابير المضادة

يتمثل التدبير المضاد الأبسط والأكثر فعالية في أن تحتفظ محطة القاعدة بتوصيل التحكم في الموارد الراديوية (RRC) مع المستعمل الموجود لفترة معينة من الزمن. وبعد قيام المهاجم بإنشاء توصيل التحكم في الموارد الراديوية باستعمال معرِّف الهوية المسروق للضحية، سيُفك التوصيل عند فشل عملية تشوير في طبقة عدم النفاذ (NAS). وبالتالي، في حال الحفاظ على التوصيل القائم للضحية إلى أن فك توصيل التحكم في الموارد الراديوية للمهاجم، يمكن الحفاظ على التوصيل الراديوي. وعادة ما يقابل الوقت، الذي يحاول فيه المهاجم إقامة توصيل التحكم في الموارد الراديوية وحتى فك هذا التوصيل بسبب فشل عملية تشوير في طبقة عدم النفاذ، المدة التي تقوم فيها محطة القاعدة بإرسال إعدادات توصيل التحكم في الموارد الراديوية وتنتظر اكتمال هذا التوصيل. وبالتالي ينفَّذ "مؤقِّت الانتظار"[1] في محطة القاعدة e/gNodeB لحساب الوقت المستغرَق من اللحظة التي ترسِل فيها إنشاء توصيل التحكم في الموارد الراديوية إلى معدات المستعمل حتى تَستقبل اكتمال إنشاء هذا التوصيل. وتنبغي إضافة عملية بحيث تحتفظ محطة القاعدة بتوصيل لفترة أطول من مؤقت انتظار توصيل التحكم في الموارد الراديوية القائم الذي يرسل الآن طلباً بمعرف هوية مزدوج ويحافظ على التوصيل القائم عند فك توصيل جديد خلال الوقت المقابل. ويجب اختصار وقت الصيانة إلى أدنى حد نظراً لتأثيره على خدمة الاتصالات وأداء المعدات.

---

1 من قبيل مؤقت T352 على النحو المعرَّف في المواصفة التقنية 3GPP TS 25.331.

وبالإضافة إلى ذلك، يمكن للمهاجم تكرار إرسال طلبات توصيل التحكم في الموارد الراديوية (RRC) إلى المحطة القاعدة لإدامة حالة تعطل الخدمة عن الجهة المتضررة. وللتخفيف من حدة هذه الحالة، ينبغي ضبط "زمن الحد" و"عداد الحدود" في محطة القاعدة e/gNodeB إذا أجري توصيل التحكم في الموارد الراديوية وفكه بشكل متكرر ضمن المهلة الزمنية وعبر عدد من حدود التعداد، فتضاف عملية تنذر فيها محطة القاعدة مشغِّل الشبكة كي يراقب الهجمات.

بيبليوغرافيا

[b-ITU-T Q.700] Recommendation ITU-T Q.700 (1993), *Introduction to CCITT Signalling System No. 7*.

[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.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

[b-ITU-T X.1047] Recommendation ITU-T X.1047 (2021), *Security requirements and architecture for network slice management and orchestration*.

[b-ITU-T X.1401] Recommendation ITU-T X.1401 (2019), *Security threats of distributed ledger technology*.

[b-ITU-T X.1406] Recommendation ITU-T X.1406 (2021), *Security threats to online voting systems using distributed ledger technology*.

[b-ITU-T X.1408] Recommendation ITU-T X.1408 (2021), *Security threats and requirements for data access and sharing based on the distributed ledger technology*.

[b-ITU-T X.1811] Recommendation ITU-T X.1811 (2021), *Security guidelines for applying quantum-safe algorithms in IMT-2020 systems*.

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network*.

[b-ITU-T Y.3101] Recommendation ITU-T Y.3101 (2018), *Requirements of the IMT-2020 network*.

[b-ITU-T Y.3150] Recommendation ITU-T Y.3150 (2020) *High-level technical characteristics of network softwarization for IMT-2020*.

[b-ITU-T Y.4807] Recommendation ITU-T Y.4807 (2020) *Agility by design for telecommunication/ICT systems security used in the Internet of things*.

[b-ITU workshop] Third annual ITU IMT-2020/5G Workshop and Demo Day (July 18, 2018), *5G security activities and future plan in ITU-T SG17*.

[b-ISO 10393] ISO 10393:2013, *Consumer product recall – Guidelines for suppliers*.

[b-ISO 81001-1] ISO 81001-1:2021, *Health software and health IT systems safety, effectiveness and security – Part 1: Principles and concepts.*

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/TS 21719-2] ISO/TS 21719-2: 2018, *Electronic fee collection – Personalization of on-board equipment (OBE) – Part 2: Using dedicated short-range communication*.

[b-RFC 3588] IETF RFC 3588 (2003), *Diameter base protocol*.

[b-TR 33.811] 3GPP TR 33.811 (2018), *Study on security aspects of 5G network slicing management*.

[b-TS 33.401] 3GPP TS 33.401 (2021), *3GPP System Architecture Evolution (SAE); Security architecture*.

[b-TS 33.501] 3GPP TS 33.501 (2022), *Security architecture and procedures for 5G System*.

[b-Alwakeel] Alwakeel, A.M., Alnaim, A., and Fernández, E.B., *A Survey of Network Function Virtualization Security*, IEEE Southeast Conf. 2018.
https://www.researchgate.net/publication/328146655_A_Survey_of_Network_Function_Virtualization_Security

[b-Craven] Craven, C., *5G Security Standards: What Are They?* 10 June 2020.
https://www.sdxcentral.com/5g/definitions/5g-security-standards/

[b-ENISA] European Union Agency for Cybersecurity (ENISA) (2019), *ENISA Threat Landscape for 5G Networks*.

[b-Goodin] Goodin, D. (2013), *Lucky Thirteen attack snarfs cookies protected by SSL encryption* Ars Technica.
https://arstechnica.com/security/2013/02/lucky-thirteen-attack-snarfs-cookies-protected-by-ssl-encryption/

[b-Khan] Khan, R., Kumar, P., Jayakody, D.N.K, and Liyanage, M. (2019), *A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions*, IEEE Communications Surveys and Tutorials, Vol. 22, No. 1, July, pp. 196-248.

[b-Möller] Möller, B, Duong, T, and Kotowicz, K. (2014), *This POODLE Bites: Exploiting The SSL 3.0 Fallback*.
https://www.openssl.org/~bodo/ssl-poodle.pdf

[b-NGMN] The Next Generation Mobile Networks Alliance (NGMN Alliance) (2016), *5G security recommendations package*.

[b-Olimid] Olimid, R., and Nencioni, G. (2020) *5G Network Slicing: A Security Overview*, IEEE Access, Vol. 8, June, 99999-100009.

[b-SQL] OWASP, *SQL injection.*
https://owasp.org/www-community/attacks/SQL_Injection

[b-Ta-Hao Ting] Ta-Hao Ting, Tsung-Nan Lin, Shan-Hsiang Shen, and Yu-Wei Chang (2019), *Guidelines for 5G end to end architecture and security issues*.
https://arxiv.org/abs/1912.10318

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، 2022