الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1332

(2020/03)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

التطبيقات والخدمات الآمنة (2) – أمن الشبكات الذكية

مبادئ توجيهية بشأن الأمن من أجل خدمات القياس الذكية في الشبكات الذكية

التوصية ITU-T X.1332

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 الشبكات 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 تكنولوجيا سجل الحسابات الموزع	X.1429-X.1400
أمن تكنولوجيا سجل الحسابات الموزع	X.1449-X.1430
البروتوكول الأمني (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	X.1729-X.1700

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

مبادئ توجيهية بشأن الأمن
من أجل خدمات القياس الذكية في الشبكات الذكية

ملخص

نُشرت خدمات القياس الذكي على نطاق واسع في جميع أنحاء العالم لجعل شبكات الكهرباء أكثر كفاءة وموثوقية من خلال جمع/توفير معلومات بشأن استخدام الكهرباء من/وإلى العملاء، على التوالي. ويمكن استخدام هذه المعلومات لتقدير طلبات العملاء من الكهرباء، ويمكن استخدام التقديرات لمواءمة الطلب أو لتغيير سلوك استهلاك العملاء للكهرباء من خلال تزويدهم بمعلومات عن استخدام الكهرباء. ومع ذلك، قد تتعطل خدمات القياس الذكي بسبب التهديدات المختلفة. وعلى سبيل المثال، يمكن أن تؤدي معلومات القياس غير الصحيحة إلى اتخاذ قرارات خاطئة بشأن إدارة الطلب، كما أن إساءة استخدام وظائف التحكم في الحمل يمكن أن تتسبب في أضرار اقتصادية ومادية للعملاء. وتقدم التوصية ITU-T X.1332 مبادئ توجيهية لأمن خدمات القياس الذكي من أجل تمكين موردي الخدمات من تنفيذ التدابير الأمنية المناسبة لضمان أمن خدماتهم. وتحدد هذه التوصية التهديدات الأمنية وأساليب الهجوم ضد خدمات القياس الذكي، وتحدد المتطلبات والقدرات الأمنية للتخفيف من هذه التهديدات والهجمات وفقاً لذلك.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1332	2020-03-26	17	11.1002/1000/14086

مصطلحات أساسية

بنية تحتية متقدمة للقياس، مبادئ توجيهية بشأن الأمن، شبكة ذكية، خدمة القياس الذكي.

* 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/.

جدول المحتويات

الصفحة

مبادئ توجيهية بشأن الأمن
من أجل خدمات القياس الذكية في الشبكات الذكية

1 مجال التطبيق

تقدم هذه التوصية مبادئ توجيهية لأمن خدمات القياس الذكي في أنظمة الشبكات الذكية. وتشمل ما يلي:

- تحديد التهديدات الأمنية والهجمات ضد خدمات القياس الذكي؛
- متطلبات الأمن لخدمات القياس الذكي؛
- مبادئ توجيهية لأمن خدمات القياس الذكي من أجل الوفاء بمتطلبات الأمن.

2 المراجع

لا توجد.

3 التعاريف

1.3 مصطلحات معرَّفة في وثائق أخرى

تستعمل هذه التوصية المصطلحات التالية المعرفة في وثائق أخرى:

1.1.3 الاستجابة للطلب (demand response) (DR) [b-ITU-T Y.2071]: ميزة من ميزات الشبكة الذكية تتيح للمستهلكين خفض أنماط استخدامهم للكهرباء أو تغيير أنماط الاستخدام أثناء ذروة الطلب، وعادةً ما تكون مقابل حافز مالي. وتتيح آليات وحوافز للمرافق والعملاء من الشركات التجارية والصناعية والسكان لخفض استخدام الطاقة في أوقات ذروة الطلب أو عندما تكون اعتمادية الطاقة على المحك. وتكون الاستجابة للطلب ضرورية لاستمثال التوازن بين العرض والطلب في مجال الطاقة.

2.1.3 مشغل نظام الطاقة الكهربائية (electric power system operator) [b-IEC 60050-617]: جهة مسؤولة عن التشغيل الآمن والموثوق لجزء من نظام الطاقة الكهربائية في منطقة معينة وعن التوصيل بالأجزاء الأخرى من نظام الطاقة الكهربائية.

3.1.3 نظام إدارة الطاقة (energy management system) (EMS) [b-ITU-T Y.2071]: نظام حاسوبي يتألف من منصة برمجية توفر خدمات الدعم الأساسية ومجموعة من التطبيقات التي توفر الوظائف اللازمة للتشغيل الفعّال لمنشآت التوليد والنقل بغية ضمان الأمن الكافي للإمداد بالطاقة بأقل تكلفة.

4.1.3 عداد ذكي (smart meter) [b-ITU-T X.1331]: جهاز مثبت في المنشآت لرصد ومراقبة استخدام الأجهزة المنزلية الذكية للطاقة الكهربائية استناداً إلى معلومات الاستجابة للطلب الخاصة بها.

2.3 المصطلحات المعرّفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 مركّز البيانات (data concentrator): جهاز وسيط يقع بين عداد ذكي وأنظمة شركات توزيع الكهرباء، ويكون الغرض الرئيسي منه جمع البيانات الواردة من العداد الذكي وإدارتها.

2.2.3 نظام إدارة بيانات العداد (meter data management system) (MDMS): يُجمّع نظام إدارة بيانات العداد ويتحقق من صحتها ويُقدّرها ويسمح بتعديلها، مثل استخدام الطاقة وتوليدها وسجلات العدادات. ويُخزن النظام MDMS هذه البيانات لفترة محدودة من الوقت قبل نقلها إلى مستودع بيانات مع إتاحتها للأنظمة المخوَّلة.

ملاحظة – مستمد من [b-ITU-T Y.2071].

3.2.3 خدمة القياس الذكي (smart metering service): خدمة تجمع بيانات استخدام الكهرباء من خلال العدادات الذكية، وتوفر المعلومات التي تم تحليلها للعملاء والمرافق؛ ويمكن للأطراف الثالثة من موردي الخدمات المشاركة في هذه الخدمة أيضاً لاستعمال بيانات استخدام الكهرباء من أجل توفير خدمة أو مجموعة من الخدمات للعميل.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

CDMA النفاذ المتعدد بتقسيم الشفرة *(Code-Division Multiple Access)*

DDoS رفض الخدمة الموزع *(Distributed Denial of Service)*

DoS رفض الخدمة *(Denial of Service)*

EMS نظام إدارة الطاقة *(Energy Management System)*

EUIS نظام معلومات استخدام الطاقة *(Energy Usage Information System)*

HMAC شفرة استيقان الرسالة القائمة على الاختزال *(Hash-based Message Authentication Code)*

IHD شاشة عرض في المنزل *(In-Home Display)*

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

MDMS نظام إدارة بيانات العداد *(Meter Data Management System)*

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

PLC الاتصالات عبر خطوط الطاقة *(Power Line Communication)*

QoS جودة الخدمة (*Quality of Service*)

TLS أمن طبقة النقل *(Transport Layer Security)*

VPN شبكة خاصة افتراضية *(Virtual Private Network)*

5 الاصطلاحات

لا توجد.

6 لمحة عامة

نُشرت خدمات القياس الذكي، وهي سمة أساسية في أي شبكة ذكية، على نطاق واسع في جميع أنحاء العالم لجعل شبكات الكهرباء أكثر كفاءة وموثوقية من خلال جمع/توفير معلومات بشأن استهلاك الكهرباء من/وإلى العملاء، على التوالي.

ويقيس العداد الذكي كمية الكهرباء التي يستهلكها العميل ويسجلها وينقلها. وترسل بيانات القياس بشكل دوري، كل 5 أو 15 دقيقة. وبناءً على هذه البيانات، يمكن لموردي خدمات القياس الذكي تقدير طلبات العملاء من الكهرباء. ووفقاً لهذه التقديرات، يمكن جعل شبكة الكهرباء أكثر موثوقية عن طريق مواءمة الطلب أو عن طريق تغيير سلوك العملاء فيما يتعلق باستهلاك الكهرباء.

ويمكن لموردي خدمات القياس الذكي تزويد العملاء بمعلومات عن استخدامهم للكهرباء، وأسعار الكهرباء في الوقت الفعلي أو الفواتير المقدرة أو البيانات الإحصائية أو اتجاهات الطلب. ويمكن للعملاء خفض استهلاكهم للكهرباء بشكل طوعي عبر استخدام هذه المعلومات. فعلى سبيل المثال، إذا طبق المورد تسعيراً ديناميكياً وغيّر السعر استناداً إلى الطلب على الكهرباء، فقد يؤخر العملاء أو يستبقون اتخاذ إجراء خاص بهم بشأن استهلاك الكهرباء..

ومع ذلك، توجد تهديدات قد تتسبب في تعطل الشبكات الذكية. فعلى سبيل المثال، يمكن أن تؤدي معلومات القياس غير الصحيحة إلى اتخاذ قرارات خاطئة فيما يتعلق بإدارة الطلب، كما أن إساءة استخدام وظائف التحكم في الحمل يمكن أن يتسبب في أضرار اقتصادية ومادية للعملاء. وعلاوة على ذلك، عندما يكون للأطراف الثالثة من موردي الخدمات الحق في النفاذ إلى معلومات القياس، يجب مراعاة مسألة حماية المعلومات المحدِّدة لهوية الشخص.

وعلاوةً على ذلك، عادةً ما تنقل معلومات استخدام الكهرباء والإحصاءات ومعلومات التكلفة إلى أجهزة العملاء الموصولة بالإنترنت مثل الهواتف الذكية أو أجهزة الحاسوب المحمولة باليد. وبالتالي، يمكن أن تؤثر جميع التهديدات التي قد تؤثر على الأجهزة المحمولة أيضاً على خدمات القياس الذكي.

وتبحث هذه التوصية التهديدات الأمنية في خدمات القياس الذكي، وتحدد المتطلبات والقدرات الأمنية لضمان أمن خدمات القياس الذكي.

7 معمارية خدمات القياس الذكي

قبل وصف أمن خدمات القياس الذكي، تُعرف معمارية لهذه الخدمات لتحديد جميع الكيانات المرتبطة بخدمة القياس الذكي من أجل توضيح العلاقة بينها.

ولتحديد نموذج عام لخدمة القياس، تتناول هذه التوصية حالات الاستعمال التالية:

- جمع بيانات استخدام الكهرباء من أجهزة القياس؛
- توفير اتجاهات استخدام الكهرباء للعملاء؛
- توفير معلومات استخدام الكهرباء للأطراف الثالثة من موردي الخدمات؛
- توفير معلومات استخدام الكهرباء لمشغلي أنظمة الطاقة الكهربائية.

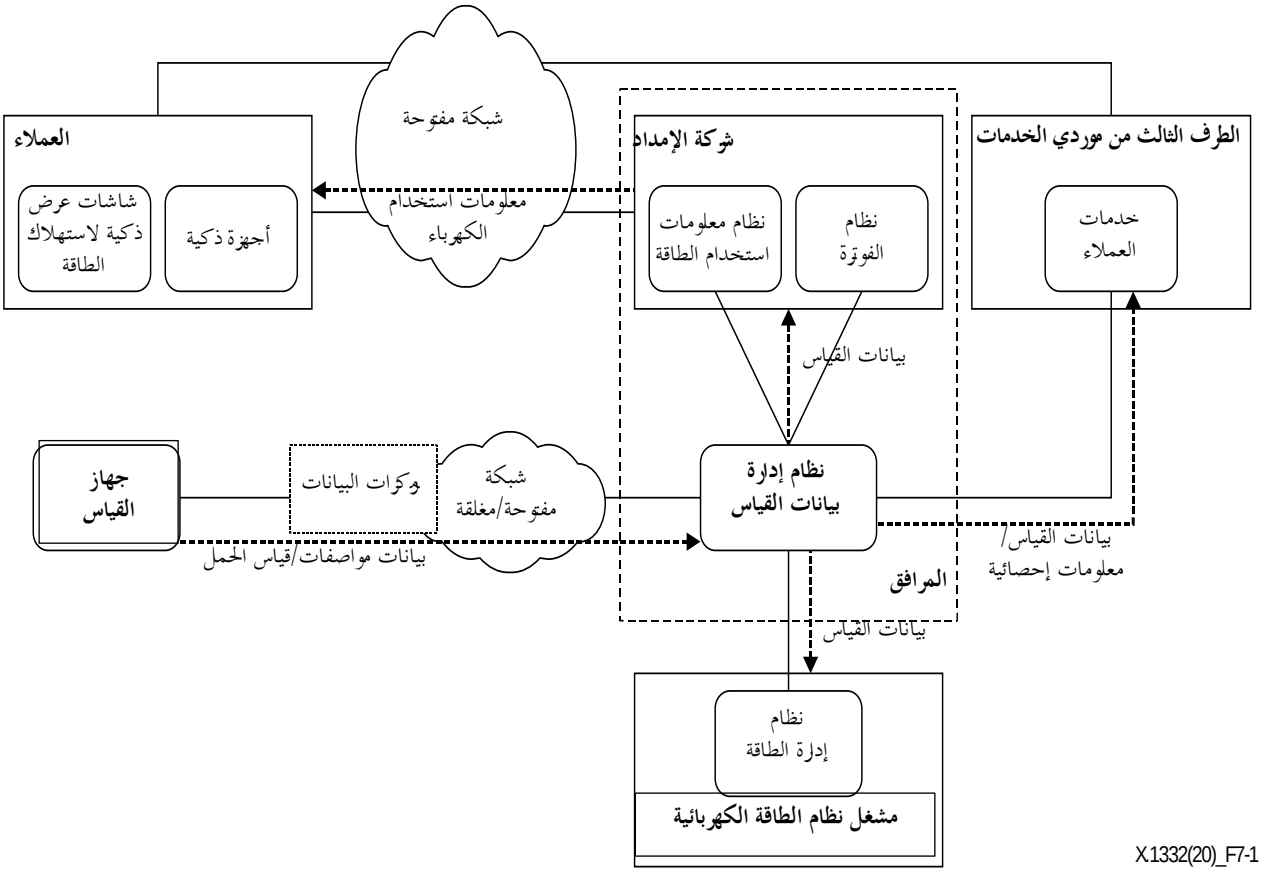
ويوضح الشكل 7-1 معمارية لخدمة القياس الذكي لحالات الاستعمال هذه. وتوجد في هذا النموذج ستة كيانات رئيسية: جهاز القياس، ومشغل نظام الطاقة الكهربائية، ونظام إدارة بيانات القياس (MDMS)، وشركة توزيع الكهرباء (النظام)، والأطراف الثالثة من موردي الخدمات والعملاء.

ويقيس جهاز القياس استخدام العميل للكهرباء ويرسل بيانات القياس إلى النظام MDMS في شركة توزيع الكهرباء. وتوفر شركة توزيع الكهرباء نظام معلومات بشأن استخدام الطاقة (EUIS) لتقديم اتجاهات استخدام الكهرباء للعملاء. ويحصل النظام EUIS على بيانات القياس من النظام MDMS من أجل إعداد المعلومات الإحصائية. ويستخدم نظام الفوترة في شركة توزيع الكهرباء أيضاً بيانات القياس. وفي هذه المعمارية، يتم تصنيف النظام EUIS ونظام الفوترة كنظامين تابعين لشركة توزيع الكهرباء.

ويستخدم مشغل نظام الطاقة الكهربائية بيانات القياس لتقدير الوضع الحالي والمستقبلي لنظام الطاقة. ويستقبل نظام إدارة الطاقة (EMS) التابع لمشغل نظام الطاقة الكهربائية بيانات القياس من النظام MDMS، ويحلل اتجاهات الطلب على الكهرباء باستخدام هذه البيانات. وبناءً على الطلب المتوقع، يضبط المشغل كمية الإمداد بالكهرباء حتى يتمكن نظام الطاقة من تحقيق التوازن بين العرض والطلب.

ويمتلك العميل شاشات عرض ذكية أو أجهزة ذكية للطاقة تعرض إحصائيات عن استخدام الطاقة والتحكم في الأحمال موصولة بشبكات المباني الخاصة بهم. ويمكن للعملاء استخدام عدة أنواع من شاشات العرض، بما في ذلك الهواتف الذكية والأجهزة اللوحية وأجهزة التلفاز الذكية وأجهزة الحاسوب الشخصية وشاشات العرض المنزلية المتخصصة (IHD) للنفاذ إلى النظام EUIS التابع لشركة توزيع الكهرباء.

وتستخدم الأطراف الثالثة من موردي الخدمات بيانات القياس لتحسين جودة الخدمة. فعلى سبيل المثال، يمكن لشركة تلفزيون كبلي أن تبث إعلاناً تجارياً لأحد المنظفات لعميل معين، إذا كانت تعلم أن هذا العميل يقوم بغسل ملابسه.



الشكل 7-1 – معمارية خدمة القياس الذكي

تُراعى ست علاقات بين الكيانات في هذا النموذج المعماري: جهاز القياس والنظام MDMS، والنظام MDMS والنظام EMS، والنظام MDMS ونظام شركة توزيع الكهرباء، والنظام MDMS وأحد الأطراف الثالثة من موردي الخدمات، والعميل ونظام شركة توزيع الكهرباء، والعميل وأحد الأطراف الثالثة من موردي الخدمات.

ويتم توصيل جهاز القياس بنظام إدارة بيانات العداد عن طريق شبكة. ويمكن أن تكون الشبكة مفتوحة مثل التطور طويل الأجل أو النفاذ المتعدد بتقسيم الشفرة أو شبكة مغلقة مثل الاتصالات عبر الخطوط الكهربائية أو خط مؤجر. وبصرف النظر عن نوع الشبكة، ستُجمَع مركزات البيانات بيانات القياس في منطقة ما، وترسل البيانات المجمعة إلى النظام MDMS.

ويتواصل النطاقان MDMS وEMS مع بعضهما البعض عبر شبكة اتصالات ذات جودة خدمة مضمونة.

وعادةً ما يوجد النظام MDMS ونظام شركة توزيع الكهرباء في نفس الشبكة. وإذا لم يكن النظامان موصولين في نفس الشبكة، فعادةً ما يكونان موصولين بشبكة اتصالات ذات جودة خدمة مضمونة.

ويمكن توصيل النظام MDMS بالأطراف الثالثة من موردي الخدمات عبر استخدام شبكة اتصالات ذات جودة خدمة مضمونة.

ونظراً لاستخدام العملاء لشبكة مفتوحة مثل الإنترنت، يتم توصيل كل من نظام شركة توزيع الكهرباء والطرف الثالث من موردي الخدمات بالعملاء عبر الشبكة المفتوحة. ويمكن للعملاء النفاذ إلى الشبكات عبر التكنولوجيات WiFi وLTE وBluetooth، وما إلى ذلك.

8 التهديدات الأمنية في خدمات القياس الذكي

1.8 التهديدات المتعلقة بالسطح البيني بين جهاز القياس والنظام MDMS

يستخدم السطح البيني بين جهاز القياس والنظام MDMS لجمع كم كبير من بيانات استخدام العملاء للكهرباء ومعالجتها، بما في ذلك بيانات العدادات ومواصفة الحمل وقياسات جودة الكهرباء. وتمثل البيانات المنقولة عبر هذا السطح البيني الهدف الرئيسي للمهاجمين. ويلحق المهاجمون أضراراً بخدمات القياس الذكي عن طريق اعتراض هذه البيانات وتزويرها وتكرارها.

ويستهدف المهاجمون أيضاً رفض خدمات القياس الذكي من خلال شن هجمات رفض الخدمة الموزع (DDoS) ضد نظام إدارة بيانات العداد.

ويتعرض السطح البيني بين جهاز القياس والنظام MDMS للتهديدات التالية:

- تسرب المعلومات: ترسل أجهزة القياس الذكي (أي العداد الذكي) بشكل دوري بيانات حمل الكهرباء (بيانات القياس) إلى النظام MDMS عبر مُركز بيانات. وفي الشبكات الذكية، تكون هذه الفترة قصيرة جداً (على سبيل المثال، 5 دقائق أو أقل). وعليه، يمكن للمهاجمين ملاحظة نمط حياة العملاء إذا كان بإمكانهم استشفاف بيانات القياس.
- تزوير بيانات القياس: يمكن للمهاجمين وقف بيانات القياس الفعلية، وإرسال بيانات قياس مزيفة إلى النظام MDMS بدلاً من ذلك. ويمكن أن تتسبب مثل هذه الهجمات في الفشل في تقدير الطلب عن طريق منع النظامين MDMS وEMS من النفاذ إلى بيانات القياس الفعلية المجمعة. ويمكن أن تؤدي مثل هذه الأعطال أيضاً إلى اختلال التوازن بين الطلب والعرض، مما يؤدي إلى انقطاع التيار الكهربائي.
- تزوير مواصفة الحمل: يمكن للمهاجمين إجراء تعديلات غير مصرح بها على مواصفة الحمل المخزنة في أجهزة القياس. وبما أن نظام الفوترة يفرض رسوماً على كل عميل بناءً على مواصفة الحمل الخاصة به، فقد يؤدي هذا التهديد إلى إصدار فواتير غير صحيحة للعملاء.
- رفض الخدمة (DoS): يمكن للمهاجمين تنفيذ هجوم رفض الخدمة لتشغيل شفرة خبيثة على عدد من أجهزة القياس أو مركزات البيانات وإغراق هدف (عادةً النظام MDMS) بكم كبير من البيانات أو عدد كبير من طلبات الخدمة. ويمكن أن يبطئ مثل هذا الهجوم خدمة القياس الذكي أو قد يتسبب في توقفها.

2.8 التهديدات على السطح البيني بين النظام MDMS وطرف من الأطراف الثالثة من موردي الخدمات

يتم استخدام السطح البيني بين النظام MDMS والأطراف الثالثة من موردي الخدمات لتبادل بيانات القياس حتى تتمكن هذه الأطراف من توفير خدمات مخصصة ومتنوعة لكل عميل. وبما أنه يمكن نقل المعلومات المحدِّدة لهوية الأشخاص عبر هذا السطح البيني، فإن المهاجمين يستهدفون هذه البيانات بشكل أساسي ويلحقون أضراراً بخدمات القياس الذكي عن طريق اعتراض هذه البيانات واستخدامها.

ويتعرض السطح البيني بين النظام والأطراف الثالثة من موردي الخدمات للتهديدات التالية:

- انتهاكات المعلومات المحدِّدة لهوية الأشخاص: يمكن للمهاجمين اعتراض المعلومات المحدِّدة لهوية الأشخاص عن طريق شن هجوم استشفاف أو تنفيذ شفرة خبيثة على الأنظمة الموصولة بالإنترنت التابعة للأطراف الثالثة من موردي الخدمات.

3.8 التهديدات على السطح البيني بين نظام توزيع شركة الكهرباء والعميل

يوفر السطح البيني بين نظام توزيع شركة الكهرباء والجهاز المتعلق بمقر العميل أنواعاً مختلفة من المعلومات التي تشجع العملاء على المشاركة في الاستجابة للطلب. وتشمل المعلومات اتجاهات استخدام العميل للكهرباء، وأسعار الكهرباء في الوقت الفعلي، واتجاهات الطلب، والفواتير، والبيانات الإحصائية. ويمكن للمهاجمين خداع العميل بإيهامه بالوقوع في استهلاك زائد للكهرباء من خلال تزوير المعلومات المنقولة. وهجوم رفض الخدمة هو تهديد آخر خطير محتمل لنظام توزيع شركة الكهرباء الموصول بأجهزة العملاء الموجودة في مقراتهم.

وتتعرض السطوح البينية بين نظام توزيع شركة الكهرباء وجهاز العميل للتهديدات التالية:

- تزييف السعر في الوقت الفعلي: يمكن للمهاجمين تزييف السعر المرسل في الوقت الفعلي من نظام توزيع شركة الكهرباء إلى العملاء للإيقاع بهم. وإذا كان السعر المزيف أقل من السعر الفعلي، فيمكن لأجهزة العملاء (مثل شاشة العرض الذكية الخاصة باستهلاك الطاقة) أن تجعل جهازاً مستهلكاً للكهرباء (على سبيل المثال السيارة الكهربائية) يستهلك قدراً أكبر من الكهرباء. وعلى النقيض من ذلك، إذا كان السعر أعلى من السعر الفعلي، فقد يفقد العميل فرصة تخزين الكهرباء بتكلفة منخفضة.
- رفض الخدمة: يمكن للمهاجمين تنفيذ هجوم رفض الخدمة لتشغيل شفرة خبيثة على عدد من أجهزة العملاء وإغراق هدف (عادة ما يكون نظام EUIS) بطلبات خدمة كثيفة. ويمكن أن يبطئ هذا الهجوم خدمة القياس الذكي أو يتسبب حتى في توقفها.
- انتهاك المعلومات المحدِّدة لهوية الأشخاص: يمكن للمهاجمين اعتراض المعلومات المحدِّدة لهوية الأشخاص من خلال شن هجوم استشفاف أو تنفيذ شفرة خبيثة على جهاز عميل موصول بالإنترنت.

9 متطلبات أمنية لخدمات القياس الذكي

1.9 متطلبات أمنية لقياس استخدام الكهرباء

يعد قياس استخدام الكهرباء أهم سمة لخدمات القياس الذكي. وعندما يعمل القياس بشكل صحيح، يمكن للنظام MDMS جمع المعلومات اللازمة لتحديد اتجاهات استخدام الكهرباء، ونمط استخدام كل عميل، وفواتير شركة توزيع الكهرباء، وما إلى ذلك. وعلاوة على ذلك، يمكن لكيانات أخرى في خدمة القياس الذكي استخدام هذه المعلومات للاضطلاع بدورها بشكل صحيح. وبالتالي، تعد سلامة بيانات القياس ومصداقيتها وسريتها هي المتطلبات الأمنية الرئيسية في عملية جمع المعلومات.

وللاستجابة بشكل صحيح للتهديدات المتعلقة بالسطح البيني للاتصالات بين العدادات الذكية والنظام MDMS، يجب مراعاة المتطلبات الأمنية التالية.

- ينبغي ضمان سرية البيانات المنقولة من طرف إلى طرف عبر السطح البيني للاتصالات بين أي عداد ذكي والنظام MDMS.
- ينبغي ضمان سلامة رسائل الاتصالات من طرف إلى طرف بين أي عداد ذكي والنظام MDMS لمنع التعديل غير المرخص للبيانات.
- ينبغي حماية بيانات القياس ومعلومات الاستيقان المخزنة في أجهزة مثل العدادات الذكية ومركزات البيانات والنظام MDMS من النفاذ غير المرخص.
- ينبغي ضمان استيقان المرسل في كل عملية اتصالات.

2.9 المتطلبات الأمنية للمعلومات التي يستخدمها العميل

نظراً لإمكانية نفاذ أجهزة العملاء إلى نظام شركة توزيع الكهرباء بالموصول بالجزء الخلفي لنظام الطاقة الكهربائية، فهي تشكل الهدف الرئيسي للهجوم على خدمات القياس الذكي. وبالتالي، يجب حماية البيانات والتطبيقات في أجهزة العملاء فيما يتصل بهذا الجزء من خدمة القياس الذكي.

وتخفيفاً للآثار الجانبية المحتملة من التهديدات المتعلقة بالسطح البيني للاتصالات بين نظام شركة توزيع الكهرباء والعميل، ينبغي مراعاة متطلبات الأمن التالية.

- ينبغي ضمان سرية البيانات للسطح البيني للاتصالات بين العميل ونظام شركة توزيع الكهرباء.
- ينبغي ضمان سلامة البيانات لرسائل الاتصالات بين العميل ونظام شركة توزيع الكهرباء لمنع التعديل غير المرخص للبيانات.
- ينبغي ضمان استيقان المرسل في كل عملية اتصالات.
- ينبغي حماية المعلومات المخزنة في جهاز العميل ونظام شركة توزيع الكهرباء من النفاذ غير المرخص.
- ينبغي مراعاة سلامة التطبيقات في جهاز العميل.

3.9 المتطلبات الأمنية للمعلومات المستخدمة من جانب الأطراف الثالثة من موردي الخدمات

إن الشاغل الرئيسي في هذه المسألة هو معالجة بيانات المعلومات المحدِّدة لهوية الأشخاص وانتهاكها بين الأطراف الثالثة من موردي الخدمات والنظام MDMS.

ولمعالجة التهديدات المتعلقة بالسطح البيني للاتصالات بين النظام MDMS والأطراف الثالثة من موردي الخدمات بشكل صحيح، ينبغي مراعاة المتطلبات الأمنية التالية.

- ينبغي ضمان سرية البيانات للسطح البيني للاتصالات بين النظام MDMS والأطراف الثالثة من موردي الخدمات.
- ينبغي ضمان سرية البيانات لرسائل الاتصالات بين النظام MDMS والأطراف الثالثة من موردي الخدمات لمنع التعديل غير المرخص للبيانات.
- ينبغي ضمان استيقان المرسل في كل عملية اتصالات.
- ينبغي التعامل مع بيانات المعلومات المحدِّدة لهوية الأشخاص بشكل صحيح بحيث يتم الكشف عنها فقط بموافقة العميل من أجل تنفيذ الخدمات الشخصية.
- فيما يتعلق بالخدمات التي لا تستخدم المعلومات المحدِّدة لهوية الأشخاص، ينبغي عدم تقديم هذه المعلومات المتعلقة بالقياس.

4.9 المتطلبات الأمنية للمعلومات المستخدمة من جانب مشغل نظام الطاقة الكهربائية

لمنع التهديدات المتعلقة بالسطوح البينية للاتصالات بين النظام MDMS ومشغل نظام الطاقة الكهربائية بشكل صحيح، ينبغي مراعاة المتطلبات الأمنية التالية.

- ينبغي ضمان سرية البيانات للسطح البيني للاتصالات بين النظام MDMS ومشغل نظام الطاقة الكهربائية.
- ينبغي ضمان سلامة البيانات لرسائل الاتصالات بين النظام MDMS ومشغل نظام الطاقة الكهربائية لمنع التعديل غير المرخص للبيانات.
- ينبغي السماح للكيانات المصرح لها فقط بالنفاذ إلى السطح البيني للاتصالات بين النظام MDMS ومشغل نظام الطاقة الكهربائية.
- ينبغي عدم تقديم المعلومات المحدِّدة لهوية الأشخاص المتعلقة بالقياس.

10 المبادئ التوجيهية لأمن خدمات القياس الذكي

1.10 الضوابط الأمنية لقياس استخدام الكهرباء

للوفاء بالمتطلبات الأمنية الخاصة بقياس استخدام الكهرباء، ينبغي النظر إلى الضوابط الأمنية التالية باعتبارها قدرات تتعلق بكل كيان من أجل قياس الكهرباء.

- ينبغي تطبيق التحكم في النفاذ إلى بيانات القياس على أجهزة القياس ومركزات البيانات والنظام MDMS. وينبغي السماح للكيانات المرخص لها فقط بالنفاذ إلى بيانات استخدام الكهرباء.
- ينبغي استخدام آلية الاستيقان المتبادل بين جهاز القياس والنظام MDMS لضمان استيقان المرسل.
- ينبغي اتخاذ تدابير لاستيقان الرسائل من أجل حماية سلامة بيانات استخدام الكهرباء المنقولة إلى النظام MDMS. فعلى سبيل المثال، قد تكون شفرات استيقان رسائل التشفير مثل شفرة استيقان الرسالة القائمة على الاختزال خياراً في هذا الصدد.
- يمكن النظر في تشفير البيانات كإجراء أمني لحماية البيانات المتعلقة بالفواتير.
- ينبغي إجراء الكشف عن الأضرار التي تلحق بسلامة البيانات وفك تشفير البيانات المشفرة في النظام MDMS.
- ينبغي اعتماد آلية آمنة لإدارة المفاتيح في أجهزة القياس ومركزات البيانات والنظام MDMS العداد لإنشاء مفاتيح التشفير والموافقة عليها وتخزينها وتحديثها بشكل آمن.
- ينبغي استخدام آلية لحماية البيانات لضمان سرية بيانات القياس المخزنة في النظام MDMS وسلامتها.
- يمكن اعتماد تدبير أمني للتخفيف من حدة هجمات رفض الخدمة في النظام MDMS.

2.10 الضوابط الأمنية للمعلومات المستخدمة من جانب العميل

للوفاء بالمتطلبات الأمنية الخاصة بالمعلومات المستخدمة من جانب العميل، ينبغي النظر إلى الضوابط الأمنية التالية باعتبارها قدرات تتعلق بكل كيان:

- ينبغي تطبيق تدابير للاتصالات الآمنة مثل أمن طبقة النقل على الاتصالات بين جهاز العميل ونظام شركة توزيع الكهرباء. وينبغي توفير الاستيقان المتبادل واستيقان بيانات الاتصالات والتشفير بين جهاز العميل ونظام شركة توزيع الكهرباء.
- ينبغي تطبيق استيقان المستعمل والتخويل للنفاذ إلى معلومات استخدام الكهرباء على التطبيقات التي توفر هذه المعلومات. وينبغي أن يمنح نظام شركة توزيع الكهرباء الترخيص للمستعملين للنفاذ إلى البيانات الخاصة بهم فقط.
- ينبغي أن تخزن بيانات استيقان المستخدم ومفاتيح التشفير الخاصة باستيقان المستعمل والاتصالات الآمنة وكذلك المعلومات المحدِّدة لهوية الأشخاص بشكل آمن في جهاز العميل.
- ينبغي البدء في إجراءات التحقق من السلامة للكشف عن تزوير أي من التطبيقات كلما تم تشغيلها على جهاز العميل.

3.10 الضوابط الأمنية للمعلومات المستخدمة من جانب الأطراف الثالثة من موردي الخدمات

للوفاء بالمتطلبات الأمنية الخاصة بالمعلومات المستخدمة من جانب الأطراف الثالثة من موردي الخدمات، ينبغي النظر إلى الضوابط الأمنية التالية باعتبارها قدرات تتعلق بكل كيان:

- يمكن استخدام خط مؤجر لمنع المستعملين غير المخوَّلين من للنفاذ إلى الاتصالات بين النظام MDMS والطرف الثالث من موردي الخدمات.
- ينبغي تطبيق تدابير الاتصالات الآمنة مثل الشبكة الخاصة الافتراضية (VPN) على الاتصال بين جهاز العميل ونظام شركة توزيع الكهرباء. وينبغي توفير الاستيقان المتبادل واستيقان بيانات الاتصالات والتشفير بين جهاز العميل ونظام شركة توزيع الكهرباء.

- ينبغي تطبيق عملية حماية المعلومات المحدِّدة لهوية الأشخاص طوال دورة حياتها بأكملها في حالة نفاذ طرف من الأطراف الثالثة من موردي الخدمات إلى المعلومات المحدِّدة لهوية الأشخاص [b-GAO-08-343]. وقد يكون إلغاء تعرف الهوية قابلاً للتطبيق إذا لم تكن الأطراف الثالثة من موردي الخدمات في حاجة إلى بيانات تعرف الهوية.

4.10 الضوابط الأمنية للمعلومات المستخدمة من جانب مشغل نظام الطاقة الكهربائية

للوفاء بالمتطلبات الأمنية الخاصة بالمعلومات المستخدمة من جانب مشغل نظام الطاقة الكهربائية، ينبغي النظر إلى الضوابط الأمنية التالية باعتبارها قدرات تتعلق بكل كيان:

- ينبغي استخدام خط مؤجر لتقليل مخاطر النفاذ غير المخوَّل إلى الاتصالات بين النظام MDMS ومشغل نظام الطاقة الكهربائية.
- ينبغي تطبيق تدابير الاتصالات الآمنة مثل الشبكة الخاصة الافتراضية على الاتصالات بين النظام MDMS ومشغل نظام الطاقة الكهربائية. وينبغي توفير الاستيقان المتبادل واستيقان بيانات الاتصالات والتشفير بين النظام MDMS ومشغل نظام الطاقة الكهربائية.
- قد يكون إلغاء تعرف الهوية قابلاً للتطبيق إذا لم يكن مشغل نظام الطاقة الكهربائية في حاجة إلى بيانات تعرف الهوية.

بيبليوغرافيا

[b-ITU-T X.1331] Recommendation ITU-T X.1331 (2018), *Security guidelines for home area network (HAN) devices in smart grid systems.*

[b-ITU-T Y.2071] Recommendation ITU-T Y.2071 (2015), *Framework of a micro energy grid.*

[b-GAO-08-343] United States Government Accountability Office, GAO-08-343:2008, *Information Security: Protecting Personally Identifiable Information.*
https://www.gao.gov/new.items/d08343.pdf

[b-IEC 60050-617] IEC 60050-617:2009, *International Electrotechnical Vocabulary – Part 617: Organization/Market of electricity.*

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، 2020