الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

# ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

# X.1331

(2018/03)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

التطبيقات والخدمات الآمنة (2) – أمن الشبكات الذكية

---

# المبادئ التوجيهية لأمن أجهزة الشبكات المنزلية (HAN) في أنظمة الشبكات الذكية

التوصية ITU-T X.1331

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 |
| 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 |

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

**التوصية ITU-T X.1331**

# المبادئ التوجيهية لأمن أجهزة الشبكات المنزلية (HAN) في أنظمة الشبكات الذكية


## ملخص

تشكل الشبكة المنزلية (HAN) في أنظمة الشبكات الذكية شبكة منشآت. وخلافاً للشبكات المنزلية التقليدية، تشمل الشبكات المنزلية في أنظمة الشبكات الذكية أجهزة الشبكات الذكية، كمصادر الطاقة الكهربائية الموزَّعة (DER) وشاحن المركبة الكهربائية (EV) وأنظمة إدارة الطاقة المنزلية (HEMS) وجهاز عرض نسبة استهلاك الزبون من الطاقة (CED). وتُوصَّل الحمولات الكهربائية ومصادر الطاقة الكهربائية الموزَّعة الخاصة بالزبائن بالشبكة المنزلية بحيث يتمكن الزبائن من تشغيل هذه الحمولات والمصادر أو إيقافها استناداً إلى المعلومات الواردة من شركة توزيع الكهرباء، من أجل رفع مستوى كفاءة استخدام الكهرباء إلى أقصى حد ممكن. وعادةً ما تكون الشبكة المنزلية موصّلة بالإنترنت، فيسهل، بالتالي، على المهاجمين النفاذ إلى الشبكة المنزلية وأجهزتها. ومن ثم، ينبغي أن تكون أجهزة الشبكات المنزلية قادرة على منع المهاجمين من الإضرار بهذه الشبكات وأجهزتها. وتعرض التوصية ITU-T X.1331 تحليلاً للتهديدات التي تتعرض الشبكة المنزلية في أنظمة الشبكات الذكية، والمتطلبات الأمنية، والوظائف الأمنية. ونظراً لاختلاف دور ووظائف كل جهاز من أجهزة الشبكات المنزلية، تعرض التوصية المتطلبات والوظائف الأمنية لكل جهاز.



## التسلسل التاريخي

| الطبعة | التوصية | تاريخ الموافقة | لجنة الدراسات | معرف الهوية الفريد* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1331 | 2018-03-29 | 17 | 11.1002/1000/13405 |



## مصطلحات أساسية

الشبكة المنزلية، المبادئ التوجيهية للأمن، المتطلبات الأمنية، الشبكة الذكية.


* للنفاذ إلى التوصية، اطبع العنوان الإلكتروني: http://handle.itu.int/ في حقل العنوان من متصفح الويب الذي تستعمله، متبوعاً بحرف الهوية الفريد للتوصية. ومثال على 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 "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

## حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

# جدول المحتويات

**الصفحة**

# المبادئ التوجيهية لأمن أجهزة الشبكات المنزلية (HAN) في أنظمة الشبكات الذكية

## 1 مجال التطبيق

تقدم هذه التوصية المبادئ التوجيهية لأمن أجهزة الشبكات المنزلية (HAN) في أنظمة الشبكات الذكية. وتتناول هذه التوصية ما يلي:

- المخاطر الأمنية التي تتعرض لها الأجهزة والاتصالات في الشبكة المنزلية؛
- المتطلبات الأمنية للأجهزة والاتصالات في الشبكة المنزلية؛
- الوظائف الأمنية للأجهزة والاتصالات في الشبكة المنزلية.

## 2 المراجع

لا توجد.

## 3 المصطلحات والتعاريف

### 1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

**1.1.3 السطح البيني لخدمات الطاقة (ESI)** [b-ITU-T Y.2071]: مجموعة من الوظائف تتكون من وظائف البوابة ووظائف مطلوبة لتطبيقات الشبكة الذكية من أجل مراقبة خدمات الشبكة الذكية وإدارتها في أماكن العملاء.

**2.1.3 نظام تخزين الطاقة (ESS)** [b-ITU-T L.1430]: الوحدة المادية أو المكون الذي يتمتع بالقدرة على تخزين أو تجميع الطاقة المنتجة بواسطة مولد الطاقة أو الطاقة التي يتم التقاطها من مستهلك الطاقة.

**ملاحظة** – يوفر نظام تخزين الطاقة وظائف تخزين الطاقة الكهربائية باستخدام أنواع مختلفة من البطاريات. ومن أمثلة استخدام تخزين الطاقة الاستجابة بفعالية لآليات أسعار دينامية من شبكة شركة توزيع الطاقة الكهربائية. وتُخزن الطاقة الكهربائية خلال فترة تكون فيها التكلفة منخفضة نسبياً بينما يمكن الاستعاضة عن الطاقة الكهربائية المخزنة بطاقة كهربائية ذات سعر أعلى من شبكة شركة توزيع الطاقة الكهربائية.

**3.1.3 شبكة منزلية (HAN)** [b-ITU-T G.9959]: شبكة قادرة على توصيل الأجهزة في المنشآت المنزلية.

**ملاحظة** – يتمثل كل كيان في هوية متكاملة واحدة تضم جميع عناصر المعلومات الممكنة التي تميز هذا الكيان (النعوت). بيد أن الهوية المتكاملة مسألة نظرية عصية على كل وصف واستعمال محلي لأن عدد النعوت الممكنة كلها لا نهائي.

**4.1.3 نظام إدارة الطاقة المنزلية (HEMS)** [b-ITU-T Y.4409]: نظام حاسوب يتألف من منصة برمجية توفر خدمات الدعم الأساسية ومجموعة من التطبيقات التي توفر الوظائف اللازمة لكفاءة تشغيل المعدات المنزلية كالأجهزة المنزلية وبطاريات التخزين بغية ضمان الأمن الكافي للإمداد بالطاقة بأقل تكلفة.

**ملاحظة** – يُشار إلى نظام إدارة الطاقة المنزلية بالشبكة المنزلية في الشبكة الذكية.

**5.1.3 عرض في المنزل (IHD)** [b-ITU-T Y.4409]: شاشة مستعمل لعرض المعلومات عن استهلاك الطاقة المنزلية. ويمكن للمستعملين التحكم بشكل اختياري في أجهزتهم المنزلية بواسطة السطح البيني للمستعمل الخاص بهم.

**ملاحظة** – يتم تحويل المعلومات المتعلقة بالمراقبة والاستخدام في بيئة نظام الاتصالات للشبكة الذكية. ويمكن أن تكون شاشة المستعمل أيضاً عبارة عن هاتف محمول أو هاتف ذكي (بروتوكول الإنترنت) أو جهاز تلفزيون، أو هاتف فيديوي موصول بالإنترنت، أو حاسوب شخصي أو حاسوب لوحي أو شاشة جدارية.

**6.1.3 شبكة منطقة واسعة (WAN)** [b-ITU-T Y.4409]: شبكة اتصالات قائمة على بروتوكول الإنترنت تغطي منطقة جغرافية واسعة بما في ذلك الإنترنت وتستوعب أجهزة وشبكات محلية.

### 2.3 المصطلحات المعرفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

**1.2.3 مركبة كهربائية (EV)**: مركبة بمحرك يمكن إعادة شحنها من أي مصدر كهربائي خارجي ويمكن أن تعمل في الوقت نفسه كنظام لتوفير الطاقة.

وتشمل أمثلة ذلك المركبات التي تعمل بالكهرباء كلياً والمركبات الكهربائية التي تعمل بالبطارية والمركبات الكهربائية الهجينة القابلة للشحن والمركبات التي يمكن أن تُحوّل من مركبات كهربائية قابلة للشحن إلى مركبات هجينة. ويشار أحياناً إلى المركبة الكهربائية القابلة للشحن كمركبة مدعومة بالشبكة أو مركبة قابلة للشحن إلكترونياً.

**2.2.3 شبكة مجاورة (NAN)**: شبكة نفاذ تسمح بتوصيل الأجهزة الطرفية للشبكة الذكية والشبكات المنزلية بشبكة منطقة واسعة (WAN).

**ملاحظة** – مقتبس من [b-Smart-O-33].

**3.2.3 عدّاد ذكي**: جهاز مثبت في المنشآت لرصد ومراقبة استخدام الطاقة الكهربائية للأجهزة المنزلية الذكية استناداً إلى معلومات الاستجابة للطلب الخاصة بها.

**ملاحظة** – مقتبس من [b-ITU-T Y.4409].

## 4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

AMI البنية التحتية المتقدمة للقياس *(Advanced Metering Infrastructure)*

CED جهاز عرض نسبة استهلاك العميل من الطاقة *(Customer Energy Display)*

DER مصدر الطاقة الكهربائية الموزعة *(Distributed Electricity Resource)*

DG مولِّد موزَّع *(Distributed Generator)*

DoS منع الخدمة *(Denial of Service)*

DTLS أمن طبقة نقل وحدة البيانات *(Datagram Transport Layer Security)*

ESI السطح البيني لخدمات الطاقة *(Energy Services Interface)*

ESS نظام تخزين الطاقة *(Energy Storage System)*

EV مركبة كهربائية *(Electric Vehicle)*

G/W بوابة *(Gateway)*

HAN شبكة منزلية *(Home Area Network)*

HEMS نظام إدارة الطاقة المنزلية *(Home Energy Management System)*

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

ID معرِّف الهوية *(Identifier)*

IP بروتوكول الإنترنت *(Internet Protocol)*

IHD عرض في المنزل *(In-Home Display)*

NAN شبكة مجاورة *(Neighbourhood Area Network)*

TLS أمن طبقة النقل *(Transport Layer Security)*

WAN شبكة منطقة واسعة *(Wide Area Network)*

WAP نفاذ Wi-fi محمي *(Wi-Fi Protected Access)*

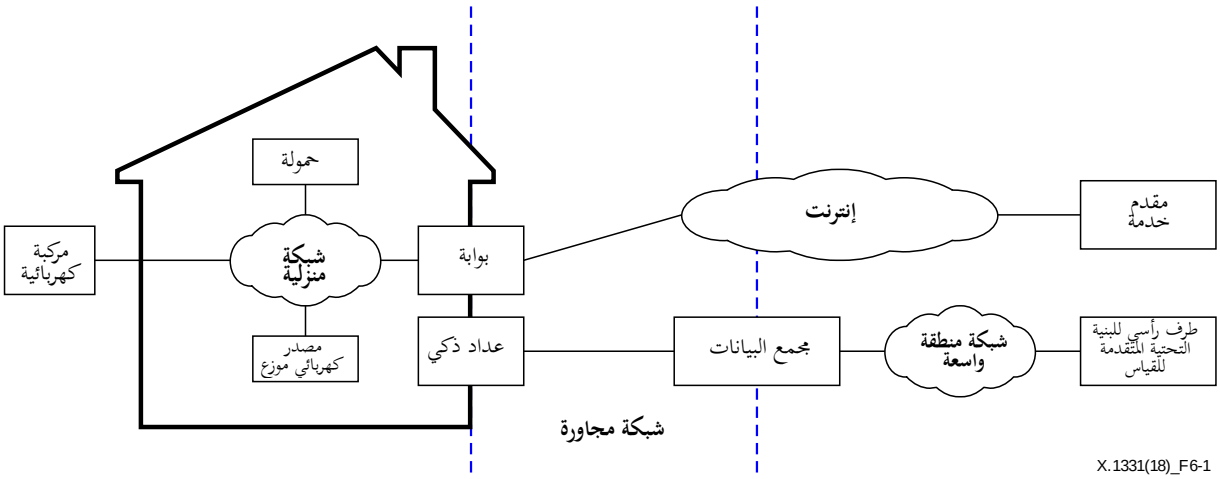
## 5 الاصطلاحات

لا توجد.

## 6 النموذج العام لشبكة منزلية في شبكة ذكية

الشبكة الذكية هي شبكة طاقة ذكية مجهزة بتكنولوجيات المعلومات والاتصالات. وبواسطة الشبكة الذكية، تستطيع شركات توزيع الكهرباء تقدير الطلب على الكهرباء استناداً إلى المعلومات المتعلقة باستهلاك العميل للكهرباء التي تُجمّع من عدادات ذكية. ونتيجةً لذلك، يمكن لشركات توزيع الكهرباء مراقبة حالة الحمولة في أوقات الذروة استناداً إلى التقدير. وقبل بلوغ الحمولة الكهربائية ذروتها، تُخفض شركة توزيع الكهرباء استخدام العميل للطاقة أو تجعله يقوم بالتغيير إلى مصادر بديلة تُولد من مصدر كهربائي موزع (DER) في أماكن العميل، كالأجهزة القطبية الضوئية على السطح أو متاجر الكهرباء أو المركبات الكهربائية. وعلاوةً على ذلك، يمكن للعميل أن يقوم بتأخير أو تقديم استعمال الكهرباء بناءً على معلومات أوقات حمولة الذروة التي تتيحها شركة توزيع الكهرباء.

وبغية تبادل المعلومات بين شركة توزيع الكهرباء والعميل، ينبغي أن يكون التقدير أو نظام إدارة الطلب لشركة توزيع الكهرباء موصولاً بالأجهزة الموجودة في أماكن العميل مثل نظام إدارة الطاقة المنزلية (HEMS) أو جهاز عرض نسبة استهلاك العميل من الطاقة (CED). ويعرض الشكل 6-1 شبكات مختلفة في بيئة شبكة ذكية. ويمكن أن يتم التوصيل عبر عدة شبكات مثل الشبكة المنزلية أو شبكة النفاذ (المعروفة أيضاً باسم الشبكة المجاورة) أو شبكة منطقة واسعة على النحو الموضح في الشكل.



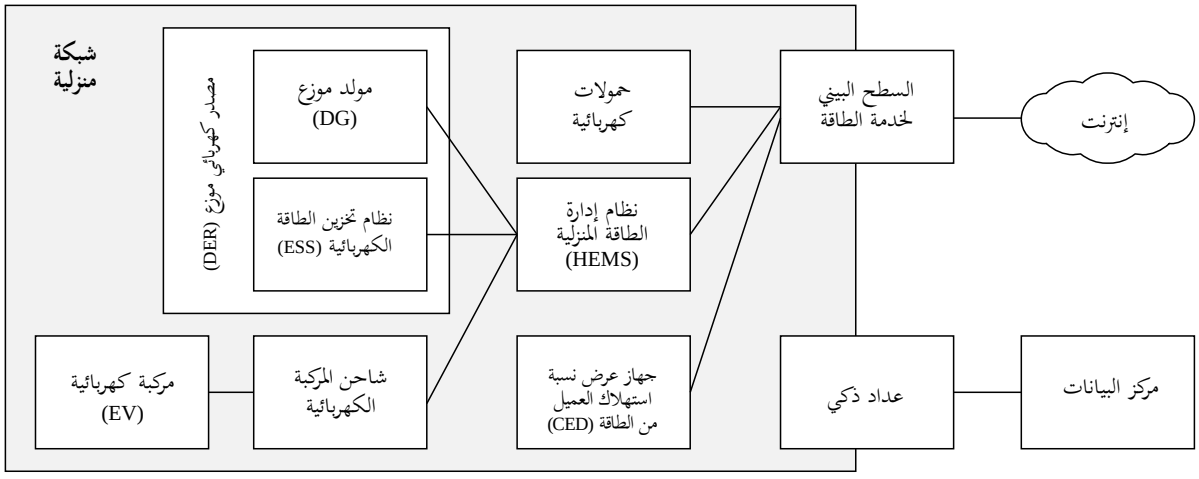

**الشكل 6-1 – الأنواع المختلفة للشبكات في شبكة ذكية**

تربط الشبكة المنزلية بين الحمولات الكهربائية والمصادر الكهربائية الموجودة في أماكن العميل. وينبغي لجميع المعلومات الصادرة من أجهزة الشبكة المنزلية أن تتدفق أولاً إلى نظام الطرف الخلفي لشركة توزيع الكهرباء مثل الطرف الرأسي للبنية التحتية المتقدمة للقياس (AMI)، من الشبكة المنزلية، وينبغي إيصال جميع المعلومات المقدمة من شركات توزيع الكهرباء إلى أجهزة العميل عبر الشبكة المنزلية.

وبما أن الشبكة المنزلية غالباً ما تكون موصولة بالإنترنت، فإنها قابلة للنفاذ من الإنترنت. وبمجرد أن يتمكن مستعمل ماكر من النفاذ إلى الشبكة المنزلية، يمكن أن تتعرض الأجهزة الموصولة بهذه الشبكة للخطر ويمكن أن يغير المهاجم المعلومات عمداً مثل المعلومات المتعلقة بالحمولات الكهربائية. وفي هذه الحالة، يستطيع المهاجم التحكم في أجهزة الشبكة المنزلية كما يرغب. ولذلك، ينبغي النظر في اتخاذ تدابير أمنية فيما يتعلق بالأجهزة الموصولة بالشبكة المنزلية والاتصالات الخاصة بها.

وقبل وصف التهديدات والمتطلبات والتكنولوجيات الأمنية، ينبغي وضع نموذج عام للشبكة المنزلية في الشبكة الذكية. وينبغي أن يحدد هذا النموذج جميع الكيانات والسطوح البينية للاتصالات المرتبطة بها لتوضيح الترابط فيما بينها.

يبين الشكل 6-2 نموذجاً عاماً لشبكة منزلية في شبكة ذكية. وفي هذه الشبكة المنزلية، هناك العديد من العناصر مثل الحمولة الكهربائية والمصدر الكهربائي الموزع (DER) ونظام إدارة الطاقة المنزلية (HEMS) وجهاز عرض نسبة استهلاك العميل من الطاقة (CED) [المعروف أيضاً بالعرض في المنزل (IHD)] والسطح البيني لخدمات الطاقة (ESI) والعداد الذكي.




X.1331(18)_F6-2

**الشكل 6-2 – نموذج عام لشبكة منزلية في شبكة ذكية**

- تنتج الحمولات الكهربائية عن الأجهزة التي تستهلك الكهرباء كالأجهزة المنزلية ومكيفات الهواء ومضخات المياه. والحمولات بشكل عام نوعان: ذكية وتقليدية. تشمل الحمولات الذكية قدرات الاتصال والقياس التي لا توجد في الحمولات التقليدية. ومع ذلك، يمكن التحكم في استهلاك الكهرباء الناتج عن الحمولات التقليدية عن طريق نظام إدارة الطاقة المنزلية إذا كان الجهاز موصولاً بمقبس من خلال مقبس ذكي يتمتع بقدرات الاتصال والتبديل. ومن ثم، تنظر هذه التوصية في كل من الحمولات الذكية والمقابس الذكية كحمولات كهربائية.
- المصادر الكهربائية الموزعة التي تشمل المولدات الموزعة (DG) وأنظمة تخزين الطاقة الكهربائية (ESS) هي أجهزة تزود الحمولات بالكهرباء. وتستخدم المصادر الضوئية القطبية المولدات الموزعة بصورة واسعة في الشبكات المنزلية.
- تستطيع المركبة الكهربائية أن تعمل كحمولة وكمصدر كهربائي موزع على السواء. ويشكل شحن المركبة الكهربائية حمولة في الشبكة المنزلية بينما يزود الأجهزة المنزلية بالكهرباء كمصدر كهربائي موزع.
- يراقب نظام إدارة الطاقة المنزلية قدرات الحمولات والمصادر الكهربائية الموزعة إما بالاستناد إلى جدول تسجيل العملاء أو إلى شروط محددة مسبقاً. وتشمل المعايير الرئيسية للشروط سعر الكهرباء وإشارة الاستجابة للطلب.
- يبين جهاز عرض نسبة استهلاك العميل من الطاقة الإحصاءات المتعلقة بالاستعمال الكهربائي الحالي ومعلومات الأسعار الحالية، بحيث يمكن للعملاء التقليل من استهلاكهم للطاقة أو تغيير خطتهم بشأن استهلاك الكهرباء.

## 7 التهديدات الأمنية ضد الشبكات المنزلية

تعرض هذه الفقرة التهديدات الأمنية الرئيسية التي تتعرض لها الشبكة المنزلية. ويرجى ملاحظة أن هذه الفقرة لا ترمي إلى تحديد تصنيف التهديدات وإنما عرض التهديدات التي تتطلب الحد الأدنى من النظر من جانب مشغلي الشبكات المنزلية.

### 1.7 تسرب البيانات

عُرف الكشف عن البيانات المخزنة أو المبلغة بأنه تهديد ضد الشبكات والأجهزة على نطاق واسع. وبإمكان المهاجم التنصت بفعالية على البيانات المرسلة أو النفاذ مادياً إلى الجهاز للحصول على البيانات من ذاكرته. وإذا كانت البيانات غير محمية، يمكن للمهاجم أن يكشف عنها.

ونظراً لاستخدام الاتصالات اللاسلكية على نطاق واسع في الشبكة المنزلية، يمكن بسهولة التنصت داخل الشبكة المنزلية أو خارجها. وعلاوةً على ذلك، بما أن الكيانات موصولة بالإنترنت في الشبكة المنزلية في كثير من الحالات، بمقدور كيان بعيد النفاذ إليها. وتبعاً لذلك، يمكن لمهاجم غير مخوّل النفاذ إلى البيانات المبلغة والمخزنة في بيئة الشبكة المنزلية.

وفي الشبكة المنزلية، تُخزن أنواع مختلفة من البيانات المتصلة بالخصوصية مثل معلومات استهلاك الكهرباء ومعلومات الفوترة وخطة استعمال الكهرباء في نظام إدارة الطاقة المنزلية، أو في جهاز عرض نسبة استهلاك العميل من الطاقة أو في العداد الذكي. ويمكن تحويل هذه البيانات الخاصة من أو إلى نظام إدارة الطاقة المنزلية وجهاز العرض CED عن طريق السطح البيني لخدمة الطاقة. ويمكن أن يؤثر الكشف عن البيانات تأثيراً سلبياً خطيراً على خصوصية العميل، إذ من خلال هذه البيانات، يستطيع المهاجم أن يطّلع على نمط الحياة اليومية للعميل.

وبالإضافة إلى ذلك، يمكن تحويل أوامر التحكم في تشغيل الحمولات أو المصادر الكهربائية الموزعة أو أجهزة شحن المركبة الكهربائية من النظام HEMS وجهاز العرض CED عبر شبكة الاتصالات. ومن خلال النفاذ إلى البيانات، يستطيع المهاجم تحديد كيفية التحكم في الحمولات والمصادر الكهربائية الموزعة في الشبكة المنزلية. ويمكن أن يفضي هذا الاطلاع على البيانات إلى تهديد آخر مثل حقن البيانات الخبيثة الوارد وصفه في الفقرة 2.7.

### 2.7 تزوير البيانات أو حقن البيانات الخبيثة

يستطيع مهاجم غير مخوّل إدخال أو تغيير أو حذف المعلومات المرسلة بين الكيانات في الشبكة المنزلية أو المخزنة في كيان الشبكة المنزلية. ويمكن أن يكون المهاجم شخصاً أو برنامجاً أو كياناً من كيانات الشبكة المنزلية. وبمجرد حدوث هذا النوع من التهديد، يمكن أن يلحق الضرر بسلامة البيانات. وبالإضافة إلى ذلك، فالإضرار بسلامة البيانات يمكن أن يؤدي إلى تعطل الجهاز.

ونظراً لاستطاعة أي كيان مجهول النفاذ إلى شبكة الاتصالات اللاسلكية، يمكن لكيان مجهول أن يرسل بيانات خبيثة إلى كيانات الشبكة المنزلية. وبالإضافة إلى ذلك، يستطيع المهاجم إضافة بيانات إلى توصيل موجود بهدف اختطاف التوصيل أو إرسال بيانات بطريقة خبيثة. وعلاوةً على ذلك، يستطيع المهاجم النفاذ إلى ذاكرة كيان الشبكة المنزلية كالنظام HEMS وتغيير البيانات المخزنة أو إدخال بيانات خبيثة في الذاكرة.

إذا أظهرت الإشارة زيادة في أسعار الكهرباء، يستطيع النظام HEMS الحد من استهلاك الكهرباء ضد رغبة العميل. وعلاوةً على ذلك، بإمكان المهاجم إرسال رسالة تحكم تسفر عن تفريغ المركبة الكهربائية أو نظام تخزين الطاقة الكهربائية. ومن الأمثلة الأخرى بهذا الشأن، إرسال أعداد كبيرة من الطلبات إلى الكيان مما يؤدي إلى منع الخدمة (DoS) عن الكيان أو تغيير القيم الموجودة في ملف البيانات أو تغيير البرنامج بحيث يعمل كيان الشبكة المنزلية بشكل مختلف.

### 3.7 انقطاع الاتصالات

من أمثلة انقطاع الاتصال التشويش الذي يحدث عندما يؤدي تداخل مقصود أو غير مقصود إلى التشويش على مرسِل وصلة الاتصال أو مستقبِلها مما يجعل الاتصال بلا جدوى. ومثال آخر على انقطاع الاتصال هو الإفراط في استهلاك عرض نطاق الاتصال عن طريق إرسال كميات هائلة من البيانات.

في شبكة منزلية، ينبغي أن يقوم النظام HEMS بجمع المعلومات عن حالة الحمولات والمصادر الكهربائية الموزعة المتصلة باستخدام الكهرباء وتلقي الأسعار وإشارات التحكم الواردة من شركة توزيع الكهرباء أو مقدم الخدمة من أجل الاستجابة لطلبات التعديل المطلوبة. وهكذا ينبغي صيانة قدرات الاتصال لدى الشبكة المنزلية بشكل صحيح لكي تعمل على نحو جيد.

### 4.7 النفاذ غير المخوّل

يمكن أن يطرأ النفاذ غير المخوّل عند اكتساب المهاجم للنفاذ إلى الكيانات، مثل المصادر الكهربائية الموزعة أو أنظمة إدارة الطاقة الكهربائية أو أجهزة عرض نسبة استهلاك العميل من الطاقة عن طريق التخفي في صورة مستعمل حقيقي. وبمجرد نجاح محاولة النفاذ غير المخوّل، يستطيع المهاجم النفاذ إلى أجهزة أخرى أيضاً.

وتحقيقاً لذلك، يجب تعرّف هوية المهاجم واستيقانه. ولأجل ذلك، يمكن للمهاجم أن يشن هجوم مسح المنْفَذ الذي يتم تنفيذه لتحديد المنافذ الضعيفة المفتوحة في جهاز الشبكة المنزلية. وفي حال وجود منافذ ضعيفة مفتوحة، يمكن للمهاجم أن يستغل نقاط ضعف جهاز الشبكة المنزلية. وبالإضافة إلى ذلك، يستطيع المهاجم كسب النفاذ غير المخوّل إلى الخدمة "المنيعة" عن طريق شن هجوم تخمين كلمة السر.

تعد البرمجيات الخبيثة من التهديدات الرئيسية أيضاً. ويمكن للبرمجية الخبيثة أن تصيب جهاز الشبكة المنزلية كجهاز عرض نسبة استهلاك العميل من الطاقة عن طريق البريد الإلكتروني أو خدمة الويب ويمكن أن تنتشر بعد ذلك لتصيب أجهزة أخرى في الشبكة المنزلية. وبمجرد تثبيت البرمجية الخبيثة في جهاز الشبكة المنزلية، يمكن الحصول على النفاذ غير المخوّل لموارد الجهاز الذي ربما يؤدي إلى خلل أو ضرر أو تعطل في الجهاز.

### 5.7 النكران

يمكن أن يحدث هذا التهديد عندما ينكر المهاجم، سواء المرسِل أو المستقبِل، حقيقة قيامه بإرسال رسالة أو استقبالها. ولا يؤدي هذا الأمر إلى أي ضرر أو خلل في أجهزة الشبكة المنزلية ولكن يمكن أن ينشب نزاع عند وقوع ذلك. وتبعاً لطبيعة النزاع، قد يتعذر تحديد سبب عطل الخدمة أو خللها بشكل صحيح.

### 6.7 العلاقة بين التهديدات الأمنية والشبكة المنزلية

تظهر التهديدات الأمنية الوارد وصفها في الفقرات من 1.7 إلى 5.7 في كيان أو اتصال محدد في النموذج العام للشبكة المنزلية. ويبين الجدول 7-1 العلاقات بين التهديدات الأمنية وكيانات الشبكة المنزلية، حيث ترمز الدائرة المفتوحة في الخلية إلى وجود تهديد معين بالنسبة إلى كيان محدد.

**الجدول 7-1 – العلاقة بين التهديدات الأمنية والشبكة المنزلية**

| الكيانات | الكشف | | تعديل/حقن | | انقطاع الاتصال | نفاذ غير مخوّل | نكران |
|---|---|---|---|---|---|---|---|
| | بيانات مخزنة | بيانات مبلغة | بيانات مخزنة | بيانات مبلغة | | | |
| حمولة | | ○ | | ○ | ○ | | |
| مصدر كهربائي موزع | | ○ | | ○ | ○ | ○ | ○ |
| شاحن المركبة الكهربائية | | ○ | | ○ | ○ | | ○ |
| نظام إدارة الطاقة المنزلية | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| جهاز عرض نسبة استهلاك العميل من الطاقة | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| السطح البيني لخدمة الطاقة | | | | | ○ | ○ | |
| الاتصال | | ○ | | ○ | ○ | | |

## 8 المتطلبات الأمنية للشبكة المنزلية

تصف هذه الفقرة المتطلبات الأمنية عالية المستوى من حيث أربعة جوانب أمنية رئيسية هي التيسر والسرية والسلامة وعدم النكران.

### 1.8 التيسر

يضمن التيسر عدم رفض النفاذ المخوّل إلى عناصر الشبكة والمعلومات المخزنة وتدفق المعلومات والخدمات والتطبيقات نتيجة أحداث تؤثر على الشبكة. وبعبارة أخرى، إذا رغب كيان في شبكة منزلية الحصول على معلومات عن جهاز آخر مع إذن، ينبغي أن يكون الكيان قادراً على النفاذ إلى الجهاز مباشرةً.

ينبغي أن تقوم الشبكة المنزلية في الشبكة الذكية بمراقبة استعمال حمولات الكهرباء أو توليده أو تخزينه بواسطة المصادر الكهربائية الموزعة تبعاً لطلبات الشبكات. وعند تقدير شركات توزيع الكهرباء أن هناك طلب الذروة، ينبغي أن يُحول طلب تخفيض الاستهلاك أو إشارة السعر المقرر حديثاً إلى نظام إدارة الطاقة المنزلية أو جهاز عرض نسبة المستهلك من الطاقة، بحيث يتسنى لها إدارة طلبات أجهزة العملاء من الكهرباء. ويمكن تحديد ما إذا كان الطلب قد تم قبوله استناداً إلى الشروط التي يسجلها العميل.

ويجب في المقام الأول ضمان تيسر وظائف كيانات الشبكة والشبكة المنزلية فيما يخص هذا السيناريو. وإذا كانت الشبكة المنزلية غير متيسرة عند وقوع طلب الذروة، من المحتمل ألا يتلقى نظام إدارة الطاقة المنزلية أي إشارة من شركة توزيع الكهرباء مما يؤدي إلى ارتفاع التكاليف التي يتحملها العميل.

### 2.8 السرية

تضمن سرية البيانات عدم تمكن كيانات غير مخوّلة من قراءة محتوى البيانات. وحتى في حالات اعتراض بعض البيانات عن طريق التصنت عبر الاتصالات اللاسلكية، لا يمكن ضمان سرية البيانات إلا إذا تعذر على المهاجم الكشف عنها.

والسرية مطلوبة للكيانات وبيانات الاتصالات الحساسة، سواء فيما يخص تخزينها أو إرسالها. وتشمل البيانات الحساسة في الشبكة المنزلية معلومات قياس استخدام الكهرباء ورسائل التحكم التي تراقب تشغيل الحمولات والمصادر الكهربائية الموزعة وإشارات الأسعار أو طلبات تعديل الطلب من شركة توزيع الكهرباء ومعلومات محددة لهوية الشخص المخزنة في جهاز عرض نسبة استهلاك العميل من الطاقة.

### 3.8 السلامة

تضمن السلامة عدم اختلاف البيانات، عند تحويلها، عن تلك المتاحة في المصدر. وتم مؤخراً توسيع معنى السلامة ليشمل حالة نظام أو جهاز يجب ألا تتغير عن التشكيلة الأساسية. وبالمثل، يجب ألا تتغير البيانات الأصلية المخزنة بعد المناولة المصرح بها.

وينبغي ضمان سلامة أوامر التحكم ومعلومات الحالة المنقولة بين نظام إدارة الطاقة المنزلية والكيانات الأخرى التي تشمل الحمولات والمصادر الكهربائية الموزعة. وبالإضافة إلى ذلك، ينبغي حماية سلامة البيانات التي تُنقل من أو إلى جهاز العرض CED. وعلاوةً على ذلك، بغية ضمان الأداء الوظيفي، ينبغي حماية سلامة قائمة البرامج المثبتة في كل جهاز HAN وكذلك تلك الخاصة بالبرامج نفسها.

### 4.8 عدم النكران

ينطوي عدم النكران على منع شخص أو كيان من إنكار قيامه بإجراء معين يتعلق بالبيانات من خلال إتاحة إثبات رقمي لهذا الإجراء.

وفي الشبكة المنزلية، تشمل الإجراءات التي يُحتمل أن تؤدي إلى نزاع، التحكم في المصادر الكهربائية الموزعة والحمولات واستقبال إشارات الأسعار وطلبات تعديل الطلب فضلاً عن تسجيل جدول استخدام الكهرباء عن طريق الجهاز CED. ومن ثم، ينبغي لكيانات الشبكة المنزلية ذات الصلة بهذه الإجراءات أن تفي بمتطلبات عدم النكران. ومع ذلك، وفي حالات الحمولات قد لا يكون عدم النكران ممكناً بسبب أداء الحمولات. فعلى سبيل المثال، يعد المقبس الذكي جهازاً مقيّداً لا يتمتع بما يكفي من الذاكرة والقدرة الحاسوبية.

### 5.8 العلاقة بين المتطلبات الأمنية والشبكات المنزلية

يبين الجدول 8-1 العلاقة بين المتطلبات الأمنية والتهديدات الأمنية حيث تشير دائرة مفتوحة في الخلية إلى ضرورة استيفاء الشرط الأمني من أجل إزالة تهديد محدد أو التخفيف من حدته.

**الجدول 8-1 – العلاقة بين المتطلبات الأمنية والتهديدات الأمنية**

| | | | التهديدات الأمنية | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | الكشف | | تعديل/حقن | انقطاع | نفاذ غير مخوّل | نكران |
| | | | بيانات مخزنة | بيانات مبلغة | بيانات مخزنة | بيانات مبلغة | | |
| المتطلبات الأمنية | السرية | بيانات مخزنة | ○ | | | | | |
| | | بيانات مبلغة | | ○ | | | | |
| | السلامة | بيانات مخزنة | | | ○ | | ○ | |
| | | بيانات مبلغة | | | | ○ | ○ | |
| | التيسر | | | | | ○ | | |
| | عدم النكران | | | | | | | ○ |

نظراً إلى أن الجدول 7-1 يعرض التهديدات لكل كيان في الشبكة المنزلية والجدول 8-1 يعرض المتطلبات الأمنية الخاصة بكل تهديد، يمكن توفير المتطلبات الأمنية لكل كيان في الشبكة المنزلية من خلال الربط بين هذين الجدولين. ويبين الجدول 8-2 توزيع المتطلبات الأمنية للكيانات في الشبكة المنزلية، حيث تشير دائرة مفتوحة في الخلية إلى ضرورة استيفاء كل كيان لشرط أمني محدد من أجل إزالة تهديد محدد أو التخفيف من حدته.

**الجدول 8-2 – توزيع المتطلبات الأمنية للكيانات في الشبكات المنزلية**

| | | المتطلبات الأمنية | | | | | |
|---|---|---|---|---|---|---|---|
| | | التيسر | السرية | | السلامة | | عدم النكران |
| | | | بيانات مخزنة | بيانات مبلغة | بيانات مخزنة | بيانات مبلغة | |
| الكيانات | حمولة | ○ | | ○ | | ○ | |
| | مصدر كهربائي موزع | ○ | | ○ | | ○ | ○ |
| | شاحن المركبة الكهربائية | ○ | | ○ | | ○ | ○ |
| | جهاز عرض نسبة استهلاك العميل من الطاقة | ○ | ○ | ○ | ○ | ○ | ○ |
| | نظام إدارة الطاقة المنزلية | ○ | ○ | ○ | ○ | ○ | ○ |
| | السطح البيني لخدمة الطاقة | ○ | | | | ○ | |
| | اتصالات | ○ | | ○ | | ○ | |

## 9 العلاقة بين المتطلبات الأمنية والوظائف الأمنية

ينبغي تطبيق الوظائف الأمنية للوفاء بالمتطلبات الأمنية للشبكة المنزلية وأجهزتها. وتشمل هذه الوظائف الأمنية التجفير أو فك التجفير والتوقيع الرقمي واستيقان الرسالة واستيقان الكيان والإذن ومراقبة النفاذ وتدبير مكافحة هجوم رفض الخدمة وأمن التدقيق والأمن المادي. ويصف الجدول 9-1 كيفية استيفاء المتطلبات الأمنية عن طريق الوظائف الأمنية. وتشير دائرة مفتوحة في الخلية إلى إمكانية اعتماد وظيفة أمنية محددة للوفاء بمتطلبات أمنية محددة. ويرجى ملاحظة أن الفقرة 10 ستصف كل وظيفة أمنية مذكورة في الجدول 9-1.

**الجدول 9-1 – العلاقة بين المتطلبات الأمنية والوظائف الأمنية**

| | | | الوظائف الأمنية | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | تجفير/ فك التجفير | توقيع رقمي | استيقان | | مراقبة النفاذ | هجوم رفض الخدمة | تدقيق | أمن مادي |
| | | | | | الرسالة | الكيان | | | | |
| المتطلبات الأمنية | السرية | بيانات مخزنة | ○ | | | | | | | |
| | | بيانات مبلغة | ○ | | | | | | | |
| | السلامة | بيانات مبلغة | | ○ | ○ | | ○ | | | |
| | | بيانات مبلغة | | ○ | ○ | | ○ | | | |
| | التيسر | | | | | ○ | | ○ | ○ | ○ |
| | عدم النكران | | | ○ | | | | | ○ | ○ |

# 10 المبادئ التوجيهية لأمن أجهزة الشبكات المنزلية في أنظمة الشبكات الذكية

## 1.10 الوظائف الأمنية للحمولات

يعرض الجدول 10-1 الوظائف الأمنية للحمولات في الشبكة المنزلية. ويبين التقابل بين المتطلبات الأمنية والوظائف الأمنية، ويعرض كذلك تفاصيل القدرات اللازمة لتنفيذ الوظائف الأمنية.

**الجدول 10-1 – الوظائف الأمنية للحمولات في الشبكة المنزلية**

| المتطلبات الأمنية | الوظائف الأمنية | الوصف |
|---|---|---|
| التيسر | تدبير مكافحة هجوم رفض الخدمة | ينبغي النظر في القدرة على كشف هجوم رفض الخدمة والتخفيف من حدته. |
| | الأمن المادي | ينبغي النظر في القدرة على منع النفاذ المادي غير المخوّل من أجل منع المستعملين غير المخوّلين من التلاعب بالحمولات أو تشكيلها. |
| السلامة | استيقان الرسالة | ينبغي النظر في القدرة على توليد بيانات سلامة التجفير والتحقق منها من أجل ضمان سلامة رسائل الإبلاغ والتحكم. ويمكن توليد بيانات سلامة التجفير بواسطة آليات شفرة استيقان الرسالة القائمة على الاختزال (HMAC). |
| السرية | التجفير أو فك التجفير | ينبغي النظر في القدرة على فك تجفير رسالة التحكم المجفرة من نظام إدارة الطاقة المنزلية. |

## 2.10 الوظائف الأمنية لمصادر الطاقة الموزعة

يعرض الجدول 10-2 الوظائف الأمنية لمصادر الطاقة الموزعة في الشبكة المنزلية. ويبين التقابل بين المتطلبات الأمنية والوظائف الأمنية، ويعرض كذلك تفاصيل القدرات اللازمة لتنفيذ الوظائف الأمنية.

**الجدول 10-2 – الوظائف الأمنية لمصادر الطاقة الموزعة في الشبكة المنزلية**

| المتطلبات الأمنية | الوظائف الأمنية | الوصف |
|---|---|---|
| التيسر | تدبير مكافحة هجوم رفض الخدمة | ينبغي النظر في القدرة على كشف هجوم رفض الخدمة والتخفيف من حدته. |
| | الأمن المادي | ينبغي النظر في القدرة على منع النفاذ المادي غير المخوّل من أجل منع المستعملين غير المخوّلين من التلاعب بالحمولات أو تشكيلها |
| السلامة | استيقان الرسالة | ينبغي النظر في القدرة على توليد بيانات سلامة التجفير والتحقق منها من أجل ضمان سلامة رسائل الإبلاغ والتحكم. ويمكن توليد بيانات سلامة التجفير بواسطة آليات شفرة استيقان الرسالة القائمة على الاختزال (HMAC). |
| | استيقان الكيان | • ينبغي النظر في القدرة على استيقان المطاريف البعيدة التي ترسل رسائل التحكم. ويمكن اعتبار التحقق من إثباتات التجفير أو الشهادة كأسلوب استيقان.<br>• ينبغي النظر في القدرة على استيقان المستعملين الذين يحاولون تشكيل مصادر الطاقة الموزعة أو التلاعب بها. والتحقق من كلمة السر وسيلة نموذجية لاستيقان المستعمل. ويمكن للقياسات البيومترية كبصمات الأصابع أن تكون أحد الحلول البديلة. |
| | مراقبة النفاذ | ينبغي النظر في القدرة على السماح للمستعملين المخوّلين فقط بتغيير تشكيلة المصدر الكهربائي الموزع ومناولته. |
| السرية | التجفير أو فك التجفير | ينبغي النظر في القدرة على فك تجفير رسالة التحكم المجفرة من نظام إدارة الطاقة المنزلية. |
| عدم النكران | توقيع رقمي | ينبغي النظر في القدرة على التحقق من التوقيع الرقمي الذي تتضمنه رسالة التحكم. |
| | تدقيق | ينبغي النظر في القدرة على إنشاء سجلات تدقيق والاحتفاظ بها بغية ضمان المساءلة. ويمكن اعتبار شحن نظام تخزين الطاقة الكهربائية أو تفريغه إجراء هاماً ينبغي تسجيله. |

### 3.10 الوظائف الأمنية لأجهزة شحن المركبة الكهربائية

يعرض الجدول 10-3 الوظائف الأمنية لأجهزة شحن المركبة الكهربائية في الشبكة المنزلية. ويبين التقابل بين المتطلبات الأمنية والوظائف الأمنية، ويعرض كذلك تفاصيل القدرات اللازمة لتنفيذ الوظائف الأمنية.

**الجدول 10-3 – الوظائف الأمنية لأجهزة شحن المركبة الكهربائية في الشبكة المنزلية**

| المتطلبات الأمنية | الوظائف الأمنية | الوصف |
|---|---|---|
| التيسر | تدبير مكافحة هجوم رفض الخدمة | ينبغي النظر في القدرة على كشف هجوم رفض الخدمة والتخفيف من حدته. |
| | الأمن المادي | ينبغي النظر في القدرة على منع النفاذ المادي غير المخوّل من أجل منع المستعملين غير المخوّلين من التلاعب بالحمولات أو تشكيلها. |
| السلامة | استيقان الرسالة | ينبغي النظر في القدرة على توليد بيانات سلامة التجفير والتحقق منها من أجل ضمان سلامة رسائل الإبلاغ والتحكم. ويمكن توليد بيانات سلامة التجفير بواسطة آليات شفرة استيقان الرسالة القائمة على الاختزال (HMAC). |
| | استيقان الكيان | • ينبغي النظر في القدرة على استيقان المطاريف البعيدة التي ترسل رسائل التحكم. ويمكن اعتبار التحقق من إثباتات التجفير أو الشهادة كأسلوب استيقان.<br>• ينبغي النظر في القدرة على استيقان المستعملين الذين يحاولون تشكيل مصادر الطاقة الموزعة أو التلاعب بها. والتحقق من كلمة السر وسيلة نموذجية لاستيقان المستعمل. ويمكن للقياسات البيومترية كبصمات الأصابع أن تكون أحد الحلول البديلة. |
| | مراقبة النفاذ | ينبغي النظر في القدرة على السماح للمستعملين المخوّلين فقط بتغيير تشكيلة المصدر الكهربائي الموزع ومناولته. |
| السرية | التجفير أو فك التجفير | ينبغي النظر في القدرة على فك تجفير رسالة التحكم المجفرة من نظام إدارة الطاقة المنزلية. |
| عدم النكران | توقيع رقمي | ينبغي النظر في القدرة على التحقق من التوقيع الرقمي الذي تتضمنه رسالة التحكم. |
| | تدقيق | ينبغي النظر في القدرة على إنشاء سجلات تدقيق والاحتفاظ بها بغية ضمان المساءلة. ويمكن أن يكون شحن نظام تخزين الطاقة الكهربائية أو تفريغه إجراء هاماً يتعين تسجيله. |

### 4.10 الوظائف الأمنية لأجهزة عرض نسبة استهلاك العميل من الطاقة

يعرض الجدول 10-4 الوظائف الأمنية لأجهزة عرض نسبة استهلاك العميل من الطاقة في الشبكة المنزلية. ويبين التقابل بين المتطلبات الأمنية والوظائف الأمنية، ويعرض كذلك تفاصيل القدرات اللازمة لتنفيذ الوظائف الأمنية.

**الجدول 10-4 – الوظائف الأمنية لأجهزة عرض نسبة استهلاك العميل من الطاقة في الشبكة المنزلية**

| المتطلبات الأمنية | الوظائف الأمنية | الوصف |
|---|---|---|
| التيسر | الأمن المادي | ينبغي النظر في القدرة على منع النفاذ المادي غير المخوّل من أجل منع المستعملين غير المخوّلين من استخدام أجهزة عرض نسبة استهلاك العميل من الطاقة. |
| السلامة | استيقان الرسالة | ينبغي النظر في القدرة على توليد بيانات سلامة التجفير والتحقق منها من أجل ضمان سلامة معلومات الحالة الواردة من النظام HEMS ورسالة التحكم المرسلة إلى هذا النظام. ويمكن توليد بيانات سلامة التجفير بواسطة شفرة استيقان الرسالة القائمة على الاختزال (HMAC) أو آلية التوقيع الرقمي. |
| | استيقان الكيان | • ينبغي النظر في القدرة على استيقان النظام HEMS. ويمكن اعتبار التحقق من إثباتات التجفير أو الشهادة كأسلوب استيقان.<br>• ينبغي النظر في القدرة على استيقان المستعملين الذين يحاولون استعمال الأجهزة CED. والتحقق من كلمة السر وسيلة نموذجية لاستيقان المستعمل. ويمكن للقياسات البيومترية كبصمات الأصابع أن تكون أحد الحلول البديلة. |
| | مراقبة النفاذ | ينبغي النظر في القدرة على السماح للمستعملين المخوّلين فقط بتغيير تشكيلة الجهاز CED أو استعمال وظائفه. |

**الجدول 10-4 – الوظائف الأمنية لأجهزة عرض نسبة استهلاك العميل من الطاقة في الشبكة المنزلية**

| المتطلبات الأمنية | الوظائف الأمنية | الوصف |
|---|---|---|
| | سلامة التطبيق | ينبغي النظر في القدرة على ضمان سلامة التطبيق من أجل الكشف عن التطبيقات التي تتعرض للإصابة بالبرمجيات الضارة أو للتعديل من جانب المهاجمين. وقد يقوم المهاجمون عمداً بتغيير أو حذف الملفات القابلة للتنفيذ أو المكتبات، مما يؤدي إلى عدم استقرار التطبيق. ومن خلال هذه المقدرة، تستطيع أجهزة الشبكة المنزلية تحديد ما إذا كان التطبيق قد تغير أم لا. ويمكن أن يكون التحقق من شفرة سلامة التجفير الخاصة بالتطبيق التي تُولد عند تثبيت التطبيق أو تحديثه مثالاً لمنهج هذه المقدرة. |
| السرية | التجفير أو فك التجفير | • ينبغي النظر في القدرة على تجفير أو فك تجفير الرسائل الموجهة من أو إلى النظام HEMS من أجل حماية رسائل التحكم أو الرسائل التي تتضمن المعلومات المحددة لهوية الشخص.<br>• ينبغي النظر في القدرة على تجفير أو فك تجفير البيانات المخزنة في الجهاز CED من أجل حماية المعلومات المحددة لهوية الشخص في هذا الجهاز. |
| عدم النكران | توقيع رقمي | ينبغي النظر في القدرة على التحقق من التوقيع الرقمي الذي تتضمنه رسالة التحكم. |
| | تدقيق | ينبغي النظر في القدرة على إنشاء سجلات تدقيق والاحتفاظ بها بغية ضمان المساءلة. |

## 5.10 الوظائف الأمنية لنظام إدارة الطاقة المنزلية

يعرض الجدول 10-5 الوظائف الأمنية لنظام إدارة الطاقة المنزلية (HEMS) في الشبكة المنزلية. ويبين التقابل بين المتطلبات الأمنية والوظائف الأمنية، ويعرض كذلك تفاصيل القدرات اللازمة لتنفيذ الوظائف الأمنية.

**الجدول 10-5 – الوظائف الأمنية لنظام إدارة الطاقة المنزلية في الشبكة المنزلية**

| المتطلبات الأمنية | الوظائف الأمنية | الوصف |
|---|---|---|
| التيسر | تدبير مكافحة هجوم رفض الخدمة | ينبغي النظر في القدرة على كشف هجوم رفض الخدمة والتخفيف من حدته. وينبغي على وجه التحديد، حماية الخدمة التي يستعملها العملاء للتحكم في الحمولات والمصادر الكهربائية الموزعة ضد جهوم رفض الخدمة. |
| | الأمن المادي | ينبغي النظر في القدرة على منع النفاذ المادي غير المصرح به من أجل منع المستعملين غير المخوّلين من استعمال النظام HEMS. |
| السلامة | استيقان الرسالة | ينبغي النظر في القدرة على توليد بيانات سلامة التجفير والتحقق منها من أجل ضمان سلامة معلومات الحالة الواردة من الأجهزة الأخرى (الحمولات والمصادر الكهربائية الموزعة وأجهزة شحن المركبة الكهربائية) ورسالة التحكم الموجهة إلى الأجهزة الأخرى (الحمولات والمصادر الكهربائية الموزعة وأجهزة شحن المركبة الكهربائية). ويمكن توليد بيانات سلامة التجفير بواسطة شفرة استيقان الرسالة القائمة على الاختزال (HMAC) أو آلية التوقيع الرقمي. |
| | استيقان الكيان | • ينبغي النظر في القدرة على استيقان المطاريف البعيدة. ويمكن اعتبار التحقق من الشهادة كأسلوب استيقان. وبالنسبة إلى الحمولات ذات القدرة الحاسوبية المنخفضة، يمكن تحقيق الاستيقان عن طريق التحقق من الإثباتات التي يتم توليدها استناداً إلى سر متقاسم مسبقاً.<br>• ينبغي النظر في القدرة على استيقان المستعملين الذين يحاولون استعمال النظام HEMS. والتحقق من كلمة السر وسيلة نموذجية لاستيقان المستعمل. ويمكن للقياسات البيومترية وشفرة الاستجابة السريعة أن تكون أحد الحلول البديلة. |
| | مراقبة النفاذ | ينبغي النظر في القدرة على السماح للمستعملين المخوّلين فقط بتغيير تشكيلة النظام HEMS أو استعمال وظائفه. وينبغي الفصل بين حسابات المسؤولين وعامة المستعملين. وينبغي إنشاء حسابات منفصلة واستعمالها لأغراض مختلفة بحيث يتاح للمهاجمين نفاذ محدود إلى المعلومات والوظائف الحساسة والحسابات الأخرى في حال اختراق حساب واحد. |

**الجدول 10-5 – الوظائف الأمنية لنظام إدارة الطاقة المنزلية في الشبكة المنزلية**

| المتطلبات الأمنية | الوظائف الأمنية | الوصف |
|---|---|---|
| | سلامة التطبيق | ينبغي النظر في القدرة على ضمان سلامة التطبيق من أجل الكشف عن التطبيقات التي تتعرض للإصابة بالبرمجيات الضارة أو للتعديل من جانب المهاجمين. وقد يقوم المهاجمون عمداً بتغيير أو حذف الملفات القابلة للتنفيذ أو المكتبات، مما يؤدي إلى عدم استقرار التطبيق. ومن خلال هذه المقدرة، تستطيع أجهزة الشبكة المنزلية تحديد ما إذا كان التطبيق قد تغير أم لا. ويمكن أن يكون التحقق من شفرة سلامة التجفير الخاصة بالتطبيق التي تُولد عند تثبيت التطبيق أو تحديثه مثالاً لمنهج هذه المقدرة. |
| السرية | التجفير أو فك التجفير | • ينبغي النظر في القدرة على تجفير أو فك تجفير الرسائل الموجهة من وإلى كيان آخر في الشبكة المنزلية من أجل حماية رسائل التحكم والرسائل التي تتضمن المعلومات المحددة لهوية الشخص.<br>• ينبغي النظر في القدرة على تجفير أو فك تجفير البيانات المخزنة في النظام HEMS من أجل حماية المعلومات المحددة لهوية الشخص في هذا النظام إذا لزم الأمر. |
| عدم النكران | توقيع رقمي | ينبغي النظر في القدرة على التحقق من التوقيع الرقمي الذي تتضمنه رسالة التحكم. |
| | تدقيق | ينبغي النظر في القدرة على إنشاء سجلات تدقيق والاحتفاظ بها بغية ضمان المساءلة. |

## 6.10 الوظائف الأمنية للسطح البيني لخدمات الطاقة

يعرض الجدول 10-6 الوظائف الأمنية للسطح البيني لخدمات الطاقة (ESI) في الشبكة المنزلية. ويبين التقابل بين المتطلبات الأمنية والوظائف الأمنية، ويعرض كذلك تفاصيل القدرات اللازمة لتنفيذ الوظائف الأمنية.

**الجدول 10-6 – الوظائف الأمنية للسطح البيني لخدمات الطاقة في الشبكة المنزلية**

| المتطلبات الأمنية | الوظائف الأمنية | الوصف |
|---|---|---|
| التيسر | الأمن المادي | ينبغي النظر في القدرة على منع النفاذ المادي غير المصرح به من أجل منع المستعملين غير المخوّلين من استعمال السطح البيني لخدمات الطاقة (ESI). |
| السلامة | مراقبة النفاذ | • ينبغي النظر في القدرة على السماح للأجهزة المحلية المخوّلة فقط بالنفاذ إلى الشبكة المنزلية. وبالنسبة لنقطة النفاذ إلى الواي فاي، ينبغي تطبيق النفاذ واي فاي المحمي II (WPA) وينبغي أن تكون كلمة السر الخاصة بها معقدة من أجل عرقلة الهجمات القائمة على تخمين كلمة السر. وبالإضافة إلى ذلك، ينبغي وقف تشغيل وظيفة إذاعة معرِّف الهوية (ID) للخدمة المنشأة. وبالنسبة إلى نقطة النفاذ ZigBee أو بلوتوث، ينبغي تطبيق السمات الأمنية على نحو تام للوفاء بالمتطلبات الأمنية.<br>• ينبغي النظر في وقف الحركة غير المخوّلة على أساس معرّفات هوية متفرّدة. ويمكن استعمال عنوان التحكم في النفاذ إلى الوسائط (MAC) أو عنوان بروتوكول الإنترنت (IP) للجهاز كمعرّف هوية متفرّد. |
| | سلامة التطبيق | ينبغي النظر في القدرة على ضمان سلامة التطبيق من أجل الكشف عن التطبيقات التي تتعرض للإصابة بالبرمجيات الضارة أو للتعديل من جانب المهاجمين. وقد يقوم المهاجمون عمداً بتغيير أو حذف الملفات القابلة للتنفيذ أو المكتبات، مما يؤدي إلى عدم استقرار التطبيق. ومن خلال هذه المقدرة، تستطيع أجهزة الشبكة المنزلية تحديد ما إذا كان التطبيق قد تغير أم لا. ويمكن أن يكون التحقق من شفرة سلامة التجفير الخاصة بالتطبيق التي تُولد عند تثبيت التطبيق أو تحديثه مثالاً لمنهج هذه المقدرة. |

## 7.10 الوظائف الأمنية للاتصال

يعرض الجدول 10-7 الوظائف الأمنية للاتصال في الشبكة المنزلية. ويبين التقابل بين المتطلبات الأمنية والوظائف الأمنية، ويعرض كذلك تفاصيل القدرات اللازمة لتنفيذ الوظائف الأمنية.

**الجدول 10-7 – الوظائف الأمنية للاتصال في الشبكة المنزلية**

| المتطلبات الأمنية | الوظائف الأمنية | الوصف |
|---|---|---|
| التيسر | تدبير مكافحة هجوم رفض الخدمة | ينبغي النظر في القدرة على كشف هجوم رفض الخدمة والتخفيف من حدته. |
| السلامة | استيقان الرسالة/الكيان | ينبغي النظر في قدرة الاستيقان المتبادل لكيانات الاتصال والرسائل من أجل ضمان سلامة بيانات الاتصال. ويمكن أن يكون أمن طبقة النقل (TLS) أو أمن طبقة نقل وحدات البيانات (DTLS) باستعمال الشهادات خياراً مناسباً للوفاء بهذا الغرض. وينبغي انتقاء خوارزمية للتجفير الآمن من أجل أمن طبقة النقل أو أمن طبقة نقل وحدات البيانات. |
| | مراقبة النفاذ | • ينبغي النظر في القدرة على السماح للأجهزة المحلية المخوّلة فقط بالنفاذ إلى الشبكة المنزلية.<br>• ينبغي النظر في وقف الحركة غير المخوّلة على أساس معرّفات هوية متفرّدة. ويمكن استعمال عنوان التحكم في النفاذ إلى الوسائط (MAC) أو عنوان بروتوكول الإنترنت (IP) للجهاز كمعرّف هوية متفرّد. |
| السرية | التجفير أو فك التجفير | ينبغي النظر في القدرة على تجفير أو فك تجفير البيانات المخزنة في النظام HEMS من أجل حماية المعلومات المحددة لهوية الشخص في هذا النظام إذا لزم الأمر. |

# بيبليوغرافيا


[b-ITU-T G.9959] Recommendation ITU-T G.9959 (2015), Short range narrow-band digital radiocommunication transceivers – PHY, MAC, AR and LLC layer specifications.

[b-ITU-T L.1430] Recommendation ITU-T L.1430 (2013), *Methodology for assessment of the environmental impact of information and communication technology greenhouse gas and energy projects*.

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

[b-ITU-T Y.4409] Recommendation ITU-T Y.4409/Y.2070 (2015), *Requirements and architecture of the home energy management system and home network services*.

[b-ITU-T Smart-O-33] ITU-T FG-Smart Grid: Smart-O-33Rev.6 (2011), *Smart grid architecture*; http://www.itu.int/en/ITU-T/focusgroups/smart/Documents/smart-o-0033r6_architecture_deliverable.doc

## 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، 2019