INSO
19516-1
1st. Edition
2012

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۱-۱۹۵۱۶
چاپ اول
۱۳۹۱

فن‌آوری اطلاعات- امنیت شبکه خانگی
قسمت ۱: الزامات امنیتی

Information technology – Home network Security
Part 1: Security requirements

ICS:35.110;35.200;35.240.99

به‌نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود . پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب ، به عنوان استاندارد ملی ایران چاپ و منتشر می شود . بدین ترتیب ، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5]در کشور فعالیت می کند . در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت‌های علمی ، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون ، برای حمایت از مصرف کنندگان ، حفظ سلامت و ایمنی فردی و عمومی ، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی ، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/ یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور ، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید . همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره ، آموزش ، بازرسی ، ممیزی و صدور گواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی ، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش ، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم ، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند . ترویج دستگاه بین المللی یکاها ، کالیبراسیون (واسنجی) وسایل سنجش ، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2 - International Electrotechnical Commission
3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد
فن‌آوری اطلاعات – امنیت شبکه خانگی- قسمت ۱: الزامات امنیتی "

رئیس:	**سمت و/یا نمایندگی**
نعمتی، فرهاد (فوق‌لیسانس مهندسی کامپیوتر)	دانشگاه آزاد اسلامی تبریز

دبیران:

خاکپور، علی (لیسانس مهندسی کامپیوتر)	شرکت ایران دیتا
خوشقدم، سهیلا (لیسانس مهندسی کامپیوتر)	شرکت ریزفناوران آرکا پژوه

اعضاء: (اسامی به ترتیب حروف الفبا)

اصل‌زاد، محمدعلی (لیسانس مهندسی کامپیوتر)	شرکت ریزفناوران آرکاپژوه
الهی، بهمن (لیسانس مکانیک)	شهرداری تبریز
بدلی افشرد، بابک (فوق لیسانس مهندسی کامپیوتر)	اداره کل استاندارد آذربایجان شرقی
بدلی افشرد، محمدرضا (فوق لیسانس برق الکترونیک)	نیروگاه برق تبریز
جباری خامنه، حسین (دکترای آمار)	دانشگاه تبریز
سرسرای، فرناز (لیسانس مکانیک)	شرکت ریزفناوران آرکاپژوه

عظیمی حسینی، سارا
(لیسانس مهندسی کامپیوتر)
شرکت ریزفناوران آرکاپژوه

فرشی حق‌رو، ساسان
(فوق لیسانس مهندسی عمران)
اداره کل استاندارد آذربایجان شرقی

مسدد، شیدا
(لیسانس مهندسی کامپیوتر)
ایرانسل

فهرست مندرجات

ادامه فهرست مندرجات

پیش‌گفتار

استاندارد " فن‌آوری اطلاعات – امنیت شبکه خانگی – قسمت ۱: الزامات امنیتی" که پیش‌نویس آن در کمیسیون‌های مربوط توسط شرکت ریزفناوران آرکاپژوه تهیه و تدوین شده و در یکصد و شصت و نهمین اجلاسیه کمیته ملی استاندارد رایانه تاریخ ۹۱/۰۲/۱۴ مورد تصویب قرارگرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات سازمان ملی استاندارد ایران، مصوّب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحوّلات و پیشرفت‌های ملی و جهانی در زمینه صنایع ، علوم و خدمات، استاندارد های ملی ایران در موقع لزوم تجدید نظر خواهد شد و هرگونه پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرارخواهدگرفت. بنابراین، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد.

منبع و مأخذی که برای تهیه این استاندارد مورد استفاده قرارگرفته به شرح زیر است:

ISO/IEC 24767-1 :2008, Information technology – Home network security – Part 1: Security requirements.

فن‌آوری اطلاعات – امنیت شبکه خانگی- قسمت ۱: الزامات امنیتی

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین الزامات امنیت شبکه خانگی[1] است که در داخل یا خارج خانه اتفاق می‌افتد. این خدمات به‌عنوان شالوده‌ای برای توسعه خدمت‌های امنیتی در برابر تهدیداتی است که در محیط خانه وجود دارد.

مباحث مربوط به الزامات امنیتی در این استاندارد به روش نسبتا غیر رسمی ارائه شده‌اند. اگرچه بیشتر اقلام مورد بحث در اینجا در راهنمای طراحی ساز و کارهای امنیتی مورد استفاده در شبکه‌های خانگی داخلی یا در طول اینترنت پیش‌بینی شده‌اند اما الزامات رسمی مطرح شده نیستند.

افزاره‌های مختلف به شبکه خانگی متصل می‌شوند، به جدول ۱ مراجعه کنید. افزاره‌های شبکه زنده، افزاره‌هایی برای سرگرمی صوتی و تصویری و افزاره‌هایی برای کار، افزاره‌های اطلاعاتی ویژگی‌ها و کارایی‌های مختلفی را فراهم می‌کنند. این استاندارد تحلیل خطرها برای افزاره‌های شبکه‌بندی شده و تعیین الزامات امنیتی ویژه را فراهم می‌کند.

۲ اصطلاحات و تعاریف و اختصارات

در این استاندارد اصطلاحات و تعاریف زیر به‌کار می‌رود:

۲-۱ اصطلاحات و تعاریف

۲-۱-۱

کالاهای قهوه‌ای

وسایل صوتی یا تصویری که به‌طور معمول برای سرگرمی استفاده می‌شوند. برای مثال: تلویزیون یا افزاره ضبط DVD

۲-۱-۲

قابلیت اعتماد

ویژگی این اطلاعات برای اشخاص غیرمجاز، هستارها یا فرآیندها، اعلام شده یا قابل دسترس نیستند.

۲-۱-۳

احراز هویت[2] داده‌ها

این خدمت‌ها به‌منظور اطمینان از منبع داده درخواست شده توسط یک بخش برای ارتباط، که به درستی تصدیق شده‌اند، استفاده می‌شوند.

1-Home Network Security (HNS)

2- Authentication

۴-۱-۲

یکپارچگی داده‌ها

ویژگی این داده در روش غیرمجاز تغییر نکرده و یا از بین نرفته است.

۵-۱-۲

احراز هویت کاربر

این خدمت‌ها برای اطمینان از ویژگی‌های ادعا شده توسط یک بخش برای ارتباط، که به درستی تصدیق شده است، استفاده می‌شوند این در حالی است که یک خدمت مجوز این اطمینان را می‌دهد که بخش احراز هویت شده و شناسایی شده حق دسترسی به افزاره و یا برنامه کاربردی ویژه را بر روی شبکه خانگی دارد.

۶-۱-۲

کالاهای سفید

دستگاه‌هایی که در زندگی روزمره استفاده می‌شوند برای مثال افزاره تهویه، یخچال و مانند آن.

۲-۲ اختصارات

در این استاندارد اختصارات زیر به کار برده می‌شوند :

A/V	Audio / Visual	صوتی یا تصویری
DDoS	Distributed Denial of Service	عدم پذیرش از خدمت توزیع شده
DoS	Denial of Service	عدم پذیرش از خدمت
DRM	Digital Rights Management	مدیریت حقوق دیجیتال
DTV	Digital TeleVision	تلویزیون دیجیتال
DVD	Digital Versatile Disc	دیسک‌های چندمنظوره دیجیتال
ESM	Externally Supported Multiple homes HES	پشتیبانی خارجی چندگانه خانه HES
ESS	Externally Supported Single home HES	پشتیبانی خارجی مجرد خانه HES
HES	Externally Supported Single home HES	سامانه الکترونیکی خانگی
ICT	Information and Communication Technology	فن‌آوری اطلاعات و ارتباطات
IP	Internet Protocol	پروتکل اینترنت
IPSec	IP Security protocol	پروتکل امنیتی IP
IPv4	Internet Protocol version 4	پروتکل اینترنت نسخه ۴
IPv6	Internet Protocol version 6	پروتکل اینترنت نسخه ۶
IT	Information Technology	فن‌آوری اطلاعات
MPEG	Moving Picture Expert Group	گروه تخصصی تصویر متحرک
OSS	Owner supported single home HES	مالکیت‌پشتیبانی مجرد سامانه الکترونیکی خانه
PDA	Personal Digital Assistant	دستیار دیجیتال شخصی

SSL	Secure Sockets Layer	لایه سوکت‌های ایمن
TCP	Transmission Control Protocol	پروتکل کنترل انتقال
TLS	Transport Layer Security	امنیت لایه انتقال
URL	Uniform Resource Locator	واحد بودن منابع مسیر یاب
VCR	Video Cassette Recorder	ضبط کننده کاست ویدئویی
VoIP	Voice over Internet Protocol	صدا از طریق پروتکل اینترنت

۳ تطابق داشتن

این استاندارد دستورالعمل‌ها را فراهم می‌نماید و حاوی الزامات مطابقت نمی‌باشد.

۴ الزامات امنیتی برای سامانه‌های الکترونیکی و شبکه‌های خانگی

۴-۱ کلیات

با توسعه سریع اینترنت و فن‌آوری شبکه‌بندی مربوطه، رایانه‌ها در دفاتر همانند خانه‌ها برای به‌دست آوردن منابع، توانایی ارتباط با یکدیگر یا با دنیای خارج را کسب کرده‌اند. امروزه با فن‌آوری‌های یکسان پس از این موفقیت‌ها توانسته‌اند به درون خانه‌های ما تعمیم داده شوند و با دستگاه‌های شخصی معمولی ارتباط برقرار نمایند. در انجام این کار، آن‌ها به کاربران اجازه نخواهند داد تا دستگاه‌های خانگی را از داخل و خارج خانه پایش و کنترل کنند بلکه خدمت‌ها و فرصت‌های توسعه جدیدی را مانند کنترل از راه دور و نگهداری تجهیزات خانگی ایجاد می‌کنند. این بدان معنی است که یک محیط محاسباتی خانگی ساده به یک شبکه خانگی با تجهیزات چندگانه برای امنیتی که درخواست خواهد شد، رشد خواهد کرد.

یک سامانه الکترونیکی خانگی نیازمند اعتماد ساکنان خانه و کاربران سامانه است. هدف از امنیت یک سامانه الکترونیکی خانگی فراهم کردن اعتماد در سامانه است. از آنجا که بسیاری از اجزا یک سامانه الکترونیکی خانگی به طور مداوم ۲۴ ساعته و خودکار با دنیای خارج تبادل اطلاعات می‌نماید امنیت فن‌آوری اطلاعات برای حفظ قابلیت اعتماد، یکپارچگی و در دسترس بودن داده و سامانه مورد نیاز است. یک پیاده سازی خوب راه‌حل‌های امنیتی را به‌کار می‌گیرد به‌عنوان مثال فقط کاربران و فرآیندهای مجاز به سامانه و داده ذخیره شده بر روی آن یا متصل به آن یا از سامانه دسترسی دارند و فقط کاربران مجاز می‌توانند از سامانه استفاده نموده و آن را تغییر دهند.

الزامات امنیتی برای سامانه الکترونیکی خانگی می‌تواند به چندین روش شرح داده شود. این استاندارد به امنیت فن‌آوری اطلاعات از سامانه الکترونیکی خانگی محدود شده است اگرچه امنیت فن‌آوری اطلاعات نیازمند نگرشی فراتر از خود سامانه است. از این رو خانه باید توانایی انجام اعمال هرچند محدود را در شرایط شکست سامانه فن‌آوری اطلاعات داشته باشد. از ویژگی‌های خانه هوشمند این است که معمولا توسط سامانه الکترونیکی خانگی پشتیبانی می‌شود و باید امکان اجرا در زمان شکست سامانه را داشته باشد. در چنین شرایطی یکی از واقعیت‌هایی که در الزامات امنیت وجود دارد این است که نمی‌تواند از خود سامانه جدا شود اما سامانه نباید از پیاده‌سازی راه‌حل‌های مجدد جلوگیری نماید.

چندین شرط در امنیت وجود دارد اینکه فقط ساکنان و صاحبان سامانه الکترونیکی خانگی به آن اعتماد داشته باشند کافی نیست بلکه فراهم کنندگان خدمات و محتوا باید به محتوا و خدمات پیشنهادی که تنها به عنوان مجوز استفاده می‌شوند، اعتماد کنند. بنابراین یکی از مبناهای امنیت یک سامانه این است که باید بر عهده یک مدیر امنیت واحد باشد و پرواضح است که باید مدیریت برعهده ساکنان و یا صاحبان سامانه باشد. با این حال فراهم‌کنندگان خدمت و محتوا باید به سامانه الکترونیکی خانگی اعتماد کنند و کاربران، آن خدمت درست را که به یک عمل قراردادی کاهش داده شده به‌کار می‌برند. برای مثال امکان دارد این قرارداد مفاهیم یا فرآیندهایی که باید توسط سامانه الکترونیکی خانگی پشتیبانی شوند را شامل شود. انتظار نمی‌رود یک ساختار واحد در سامانه الکترونیکی، انواع خانه‌ها را پشتیبانی کند. هر مدل ممکن است مجموعه متفاوتی از الزامات امنیت را داشته باشد. سه مدل متفاوت از طراحی یک سامانه الکترونیکی هر یک با مجموعه متفاوتی از الزامات امنیت تشریح خواهد شد.

واضح است که برخی از الزامات امنیت مهم‌تر از دیگری به‌نظر می‌رسد. بنابراین دیده می‌شود که پشتیبانی از برخی اقدامات متقابل اختیاری خواهد بود. علاوه‌براین، اقدامات متقابل می‌توانند ارزش وکیفیت متفاوتی داشته باشند. همچنین مدیریت و نگهداری از این اقدامات نیازمند مهارت‌های متفاوتی است. این استاندارد سعی دارد که دلایل الزامات امنیت ذکر شده را توضیح دهد بدین معنی که به طرح سامانه الکترونیکی خانگی اجازه می‌دهد که مشخص نماید کدام ویژگی‌های یک سامانه الکترونیکی خانگی خاص باید پشتیبانی شود. با توجه به الزامات کیفیت و مدیریت و اقدامات نگهداری، باید دقت کرد که کدام مکانیزم باید برای آن ویژگی انتخاب شود.

این الزامات امنیت در شبکه خانگی به چگونگی امنیت و خود خانه بستگی دارد و همچنین به اینکه چه چیزی در شبکه درون خانه دیده می‌شود، وابسته است. اگر در این شبکه فقط یک رایانه شخصی به یک چاپگر یا کابل مودم متصل است در آن صورت اقدامات امنیتی در آن کابل و تجهیزات متصل به آن، در انتهای هر دوی آنها که می‌توانند امنیت کل شبکه مورد نیاز خانه را تامین کنند، به‌کار برده می‌شود.

با این حال زمانی که یک خانه شامل ده‌ها نه صدها وسایل شبکه با بعضی از متعلقات آن برای کل شبکه و برخی دیگر برای شخصی بودن آن درون خانه باشد اقدامات امنیتی پیچیده بیشتری باید در نظرگرفته شود.

۴-۲ امنیت سامانه الکترونیکی خانگی

۴-۲-۱ تعاریفی از سامانه الکترونیکی خانگی و امنیت سامانه

یک سامانه الکترونیکی خانگی و شبکه‌بندی می‌تواند به‌عنوان مجموعه‌ای از اجزایی که پردازش، مدیریت، انتقال و ذخیره اطلاعات هستند، تعریف شوند و توانایی ارتباط و یکی کردن محاسبات چندگانه، کنترل، پایش و وسایل مکاتبه در خانه را دارند.

سامانه‌های الکترونیکی خانگی و شبکه‌ها قابلیت سرگرمی، اطلاعات، مکاتبه و وسایل امنیتی را خواهند داشت به‌اضافه دستگاه‌های خانه به یکدیگر مرتبط می‌شوند و این وسایل و دستگاه‌ها، اطلاعات را به اشتراک می‌گذارند و می‌توانند از درون خانه یا از راه دور آن را کنترل و بر آن پایش کنند و بر این اساس، همه شبکه‌های خانگی نیازمند برخی از مکانیزم‌های امنیتی برای حفظ اعمال روزانه خود خواهند بود.

شبکه و اطلاعات امنیتی را می‌توان به‌عنوان یک شبکه توانا با یک سامانه اطلاعاتی برای پایداری در سطحی از اطمینان، اتفاقات تصادفی یا اعمال مخرب دانست. چنین رویدادها و اعمالی می‌توانند با دسترس‌پذیری، اعتبار، یکپارچگی، قابل اطمینان بودن داده‌های ذخیره شده یا انتقال یافته و همچنین خدمت‌های مربوطه پیشنهادی با شبکه‌ها و سامانه‌های آن سازگار باشد.

رویدادهای امنیتی ممکن است به شکل زیر گروه‌بندی شده باشد:

الف- ارتباطات الکترونیکی می‌تواند حائلی شود و داده، کپی یا تغییر نماید. این امر موجب آسیب و هجوم سراسری به حریم خصوصی اشخاص و استفاده سراسری از داده‌های جدا شده می‌شود؛

ب- دسترسی غیرمجاز به رایانه و شبکه رایانه‌ای خانگی با قصد و نیت مخرب برای کپی، تغییر یا خراب کردن داده انجام می‌شود و به سامانه‌ها و تجهیزات خودکار موجود در خانه بسط داده می‌شود؛

پ- حمله‌های مختل‌کننده در اینترنت کاملا معمول شده و امکان دارد در آینده شبکه تلفن بیشتر آسیب‌پذیر باشد؛

ت- نرم‌افزارهای مخرب مانند ویروس‌ها می‌توانند رایانه‌ها را غیرفعال کرده داده‌ها را تغییر داده و یا پاک کنند و یا تجهیزات خانگی را دوباره برنامه‌ریزی نماید. برخی از حمله‌های ویروس‌ها بسیار مخرب و پرهزینه هستند؛

ث- ارائه اطلاعات نادرست توسط انسان‌ها و هستارها می‌تواند باعث خسارت قابل توجهی شود برای مثال مشتری‌ها ممکن است نرم افزار مخربی را از یک سایت به‌ظاهر خوب با منبع معتمد دانلود کنند، ممکن است قراردادها فسخ شده و اطلاعات محرمانه به فرد دیگری ارسال شود؛

ج- بیشتر رویدادهای امنیتی به این علت است که پیش‌بینی نشده و اتفاقات غیرعمدی مانند بلایای طبیعی (سیل‌ها، طوفان‌ها، زلزله‌ها)، غیرفعال‌شدن سخت‌افزار یا نرم‌افزار و اشتباه انسانی می‌باشد.

علاوه بر این رویدادها، امنیت‌های دیگری که به موضوع مرتبط بوده و برای خانه مهم هستند نیز وجود دارند مانند قابلیت اطمینان سامانه. ایمنی و امنیت فیزیکی خارج از دامنه و کاربرد امنیت اطلاعات است. ایمنی به پیشگیری از آسیب‌های انسانی و ساختمانی مربوط می‌شود. امنیت فیزیکی شامل حفاظت از خانه، سخت‌افزار سامانه الکترونیکی خانگی به‌وسیله درهای مناسب و قفل‌های پنجره است. این موضوع‌ها هر چند مربوط به خانه است ولی در این استاندارد انجام نشده است.

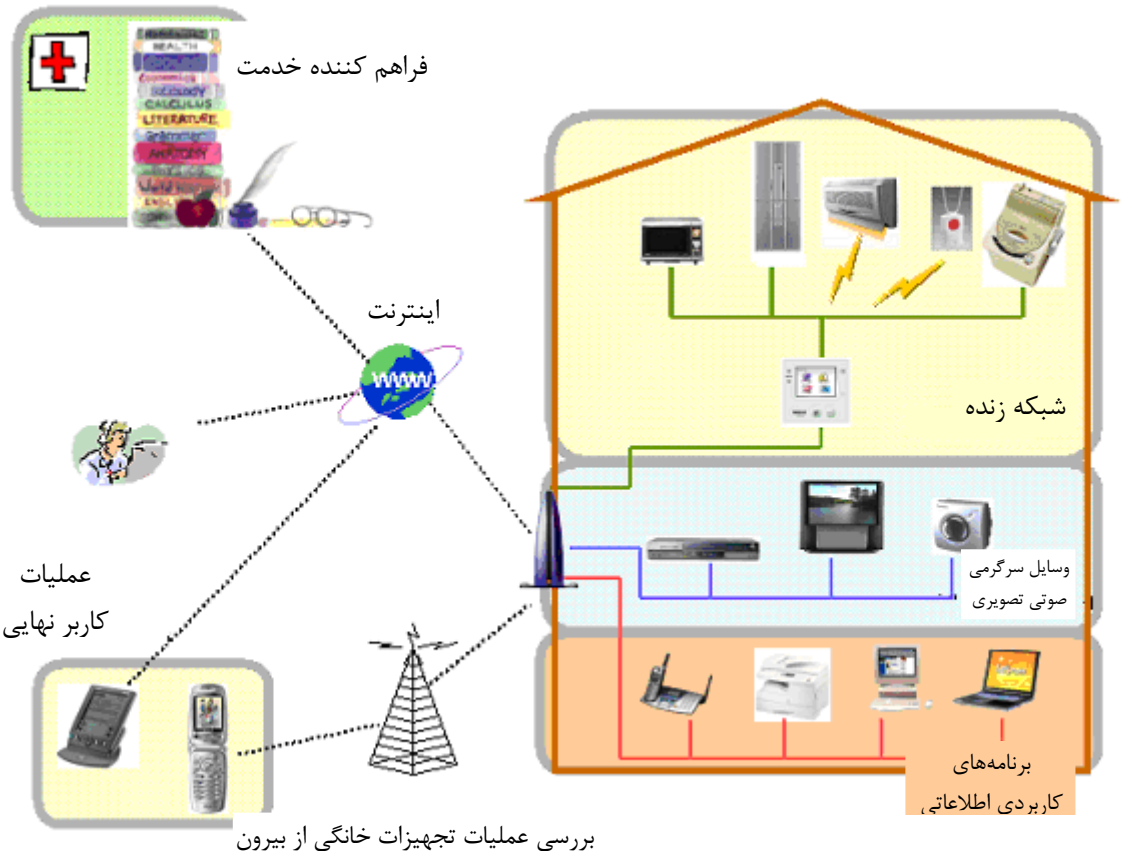
از این رو یک سامانه الکترونیکی خانگی نمی‌تواند کاملا قابل اطمینان باشد یا امنیت آن حفاظت شده باشد. باید فرض شود که ناتوانی در همه یا قسمتی از سامانه می‌تواند اتفاق بیفتد. این فقدان دسترس‌پذیری باید در نظر گرفته شود. بنابراین نیاز به بازیابی فرآیندهای آماده به‌منظور راه‌اندازی مجدد این قسمت از داده و سامانه وجود دارد و امکان پشتیبانی مجدد از فن‌آوری‌ها و شیوه‌ها را فراهم می‌کند. راه‌حل مجدد خارج از دامنه و کاربرد سامانه الکترونیکی خانگی است اما نباید از وجود چنین راه‌حل‌هایی جلوگیری کنیم.

الزامات امنیتی در شبکه‌های خانگی فقط برای استفاده در خانه معرفی نشده‌اند بلکه آن‌ها توسط برنامه‌های کاربردی در خارج از خانه نیز در خواست شده‌اند، هر کدام از آن‌ها ممکن است تاثیر مهمی بر خدمات اعم از عملیات کاربران محلی، قابلیت نگهداری از راه دور توسط فروشنده، برای فراهم کردن برنامه‌های کاربردی

چندین شکل داشته باشند. یکبار دیگر مرزهای شبکه‌های خانگی به دنیای بیرون نزدیک می‌شوند، در نظر گرفتن امنیت در شبکه‌های خانگی توسط اطلاعات و حوزه فن‌آوری ارتباطات تجاری و بیشتر این‌ها به‌طور گسترده مورد بحث قرار گرفته‌اند (برای مثال به مجموعه استاندارد ISO/IEC 18028 و پیوست الف مراجعه کنید).

با این حال هنوز برخی از ویژگی‌های متفاوت میان برنامه کاربردی داخلی و برنامه کاربردی شرکت‌های بزرگ مانند زیرساخت‌های شبکه‌های خانگی و سازمانی، نیازهای کاربران محلی و تجاری وجود دارد. بنابراین لازم است ابتدا به معرفی برخی از مدل‌های شبکه خانگی موجود و تشریح برخی از دامنه‌های برنامه کاربردی و سپس رسیدگی به این مدل‌ها برای شناسایی تهدیدهای ممکن برای شبکه‌های خانگی و در نهایت جزئیات الزامات امنیتی بپردازیم.

شکل ۱ یک مدل شبکه خانگی مفهومی را نشان می‌دهد. دروازه‌ای میان خانه و دنیای خارج که اینترنت است قرار می‌گیرد، درون خانه انواع وسایل مختلف وجود دارد ممکن است همان‌طور که در شکل ۱ مشخص شده است، در برخی از گروه‌ها قرارگیرند.



شکل ۱- مدل مفهومی از شبکه‌های خانگی

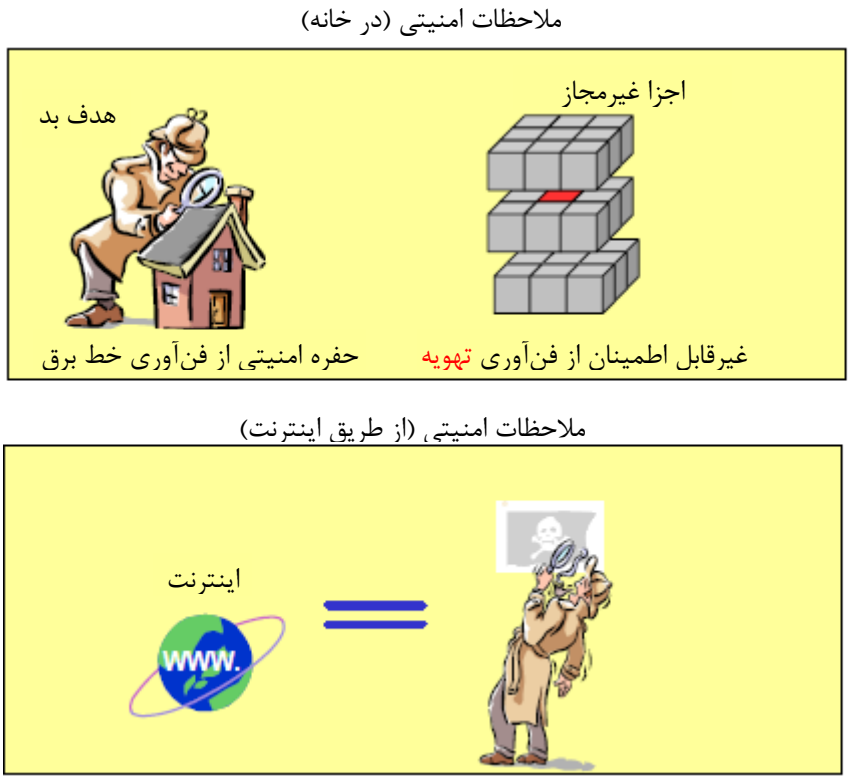
شبکه زنده[1]: ممکن است این شبکه شامل یک ماشین ظرفشویی، افزاره تهویه مطبوع و پلوپز برقی باشد و می‌تواند عملیات کنترل فعال‌سازی یا غیرفعال‌سازی را از داخل و خارج فراهم نماید.

شبکه صوتی یا تصویری: ممکن است شامل تلویزیون‌ها، افزاره‌های پخش DVD و دیگر تجهیزات صوتی و تصویری باشد و می‌تواند از طریق تلویزیون به اینترنت متصل شود (خدمات تبعیض گونه‌ای مطابق با پیشنهادها به‌وسیله رایانه‌های شخصی را فراهم می‌کند.)

سامانه‌های سینما خانگی مختلف قادرند منابع صوتی و تصویری را میان تجهیزات صوتی و تصویری و رایانه‌های شخصی به اشتراک گذارند.

شبکه افزاره اطلاعاتی: ممکن است شامل سرویس‌دهای خانگی، چاپگرها، و رایانه‌های شخصی و لپ‌تاب‌ها، PDAها، تلفن‌های تصویری، سرویس‌دهها و گوشی‌های VOIP باشند و چاپ صفحه نمایش DTV به برخی از چاپگر در ارتباط با رایانه شخصی، جستجو برنامه کاربردی داده‌های ذخیره شده در رایانه شخصی، PDAها و یا تلفن‌های تصویر VOIPهای مبتنی بر ارتباطات صوتی و تصویری باشد.

در نهایت در بررسی دقیق از امکانات شبکه‌های خانگی روشن می‌شود که الزامات امنیتی را می‌توان به دو قسمت تقسیم کرد: دفاع در برابر تهدیدهای خارجی و دفاع در برابر تهدیدهای داخلی. شکل ۲ ملاحظات مختلفی در محیط‌های خانگی متفاوت را نشان می‌دهد.



شکل ۲ – ملاحظات مختلف در محیط‌های خانگی مختلف

1-Living

برای مسائل داخل خانه مشکلات امنیتی ممکن است از فن‌آوری‌های شبکه‌بندی نا امن به‌وجود آید، مانند خطوط انتقال برق یا بی‌سیم و کنترل دسترسی برای کاربران یا کاربردهای مختلف. برای مسائل خارج از خانه تقریباً ممکن است در حفره‌های امنیتی اینترنت باشند.

۴-۳ موضوعات مربوط به امنیت سامانه الکترونیکی خانگی (خارج از دامنه و کاربرد این استاندارد)

۴-۳-۱ مدیریت حقوق دیجیتال (DRM)

مدیریت حقوق دیجیتال در مورد مشکل کپی‌برداری غیرقانونی و توزیع کالای دیجیتالی با حق چاپ مربوط است. نمونه‌های معمولی آن نرم‌افزارهای رایانه، موسیقی و فیلم‌هایی هستند که ممکن است در شبکه یا وسایلی مانند CD تحویل داده شوند.

این به نفع فراهم کننده محتوا است که هیچ کپی غیرقانونی از مطالب و محتوا توسط ساکن یا مالک خانه ساخته نشود. از این رو تهدیدی برای ساکن یا مالک خانه نیست اما نسبت به فراهم کننده محتوا و مطالب آن خارج از دامنه و کاربرد این استاندارد می‌باشد.

۴-۳-۲ کنترل والدین

در بسیاری از خانه‌ها که کودکان حضور دارند برای جلوگیری از دسترسی فرزندان به داده‌هایی که امکان دارد آسیبی به کودکان برسد به حفاظت پدر و مادر نیاز است. مانند فیلم‌هایی با خشونت شدید و غیراخلاقی. فن‌آوری این موضوع را توسط کنترل دسترسی کسب کرده و می‌تواند در شکل‌های مختلفی باشد یکی ممنوع کردن دسترسی به فراهم‌کننده‌های ناخواسته و دیگری فقط اجازه دسترسی با انتخاب از فراهم‌کنندگان مجاز است. علاوه‌براین داده‌ها می‌توانند برای کودکان نامناسب باشند و از این رو برای مکانیزم کنترل دسترسی مبتنی بر این اطلاعات اجازه می‌دهند. آخرین روش تنها در صورتی کار می‌کند که داده به‌طور مناسب مشخص شده باشد و این علامت‌گذاری را می توان با روش کنترل دسترسی درک کرد. با این حال هیچ یک از این روش‌ها تضمین شده نیستند.

۴-۳-۳ خدمات و محصولات کاهش جرم

خدمت‌ها و محصولات Criminogenic دوره‌ای است که برای محصولات و خدمات با میل به تبدیل شدن به اهداف یا ابزار جرم استفاده می‌شوند. در حال حاضر استانداردی در این زمینه وجود ندارد اما باید توجه داشت که در آینده ممکن است الزامات فنی روی سامانه الکترونیکی خانگی به منظور کاهش جرم روی محصولات نصب شده در خانه و همچنین در مورد خدمات آن وجود داشته باشد.

۴-۳-۴ موضوع مصرف کنندگان

دستورالعمل‌های متعددی در مورد چگونگی استفاده از یک سامانه وجود دارد. همه کاربران سامانه الکترونیکی خانگی ممکن است مشکلات خود را به خوبی توسط دستورالعمل‌ها در مورد چگونگی استفاده از سامانه (برای مثال خرید الکترونیکی) و چگونگی نگهداری و به‌روز رسانی به‌منظور جلوگیری از آسیب‌پذیری، مانند جلوگیری از ویروس‌ها، کرم‌ها و غیره را رفع کرده باشند.

۴-۳-۵ موضوع فراهم کننده خدمت‌ها

الزامات امنیتی برای فراهم‌کنندگان خدمات به‌منظور فعال کردن کاربران و صاحبان سامانه الکترونیکی خانگی از داده‌های فراهم‌کنندگان خدمات و اعتماد به داده‌های آن‌ها وجود دارد. این برای همه انواع فراهم‌کنندگان خدمات ثابت است همانند فراهم کردن داده‌ها به کاربران (برای مثال در شکل خدمات صوتی یا تصویری) و فراهم نمودن این خدمات برای خانه (برای مثال پایش بر زنگ خطر سارق) و ارائه این خدمات به سامانه الکترونیکی خانگی (برای مثال ارائه نرم‌افزار و به‌روز رسانی نرم‌افزار دائمی) همه این فراهم‌کنندگان خدمات، باید به کاربران سامانه الکترونیکی خانگی و صاحبان آن‌ها تضمین داده باشند که داده ورودی می‌تواند مورد قبول باشد. از یک منبع قابل اعتماد به‌دست می‌آید و در طول هر دو ارتباط به دلیل حفظ حریم خصوصی و در برابر تغییرات مخرب محافظت می‌شود.

۴-۳-۶ موضوع مجدد

در هر مجموعه الکترونیکی و سامانه نرم‌افزار امکان دارد اشتباهاتی باشد برای مثال خرابی تجهیزات، اشکالات نرم‌افزاری، اشتباهات انسانی، رعد و برق، سیل یا خسارات مخرب. بنابراین فن‌آوری‌های مجدد و شیوه‌های ایمنی اجزای حیاتی که در خانه مهم است باید در نظر گرفته شود. برای مثال قفل درب‌ها به مکانیزم مجدد سامانه الکترونیکی خانگی بستگی دارد با این وجود ساکنان خانه هنوز توانایی باز کردن و قفل کردن درها را دارند.

۴

۴-۳-۷ موضوع برون‌سپاری

مشکلی که وجود دارد در مورد چگونگی حفظ امنیت سامانه الکترونیکی خانگی است. زمانی که مسئولیت پشتیبانی از پردازش اطلاعات به سازمان دیگری برون‌سپاری شود.

۵ چالش‌ها

۵-۱ کلیات

چالش‌های شبکه خانگی به‌طور عمده از طبقه‌بندی پیچیده وسایل و انواع مختلفی از رسانه‌های فیزیکی و پروتکل‌های ارتباطی مختلف حاصل می‌شود. برخی از چالش‌های امنیتی در زمان استقرار برخی از زیرساخت‌های شبکه‌های خانگی که به خوبی شناخته شده هستند که در زیر مطرح شده‌اند:

۵-۲ چالش همیشه فعال

اتصال همیشه فعال با پهنای باند وسیع، دسترسی به اینترنت را سریع و آسان می‌کند. اما متاسفانه همین امر خانه، دفتر یا تجارت وسیع شما مستعد خطرات اینترنتی قرار می‌دهد. مانند هکرها و ویروس‌ها.
وسایل خانگی با ارتباط همیشگی به‌ویژه در حملات آسیب‌پذیر هستند. از آنجایی که آن‌ها معمولا به مدت ۲۴ ساعت در شبانه‌روز بر خط نگه داشته می‌شوند و همیشه با همان آدرس IP به اینترنت متصل هستند.

۵-۳ چالش خطوط برق

مسائل مربوط به تضمین امنیت داده‌ها برای خانه‌ها با استفاده از همان خطوط برق حاصل می‌شود، مخصوصا آن‌هایی که در مناطق قدیمی‌تری هستند. بیشتر خانه‌ها، زیر شبکه خط برق را با همسایگان خود با ترانسفورماتور توزیع یکسان، به اشتراک می‌گذارند. دستورات خط برق می‌تواند به‌راحتی از یک خانه به وسایل موجود در خانه‌های نزدیک برسد و بنابراین با کنترل مورد نظر از این وسایل تداخل پیدا می‌کند.

۵-۴ چالش بی‌سیم

شبکه‌های بی‌سیم بسیاری از چالش‌های امنیتی جدیدی را در مقابل شبکه‌های سیمی سنتی مطرح می‌کنند. ماهیت شبکه‌های بی‌سیم آن‌ها را به اشکال مختلف حملات، آسیب‌پذیر می‌سازد مانند استراق سمع غیر فعال، مداخله فعال، نشت اطلاعات محرمانه، دستکاری داده‌ها، جعل هویت و محرومیت از خدمات. کاربران مخرب، دیگر نیازی برای به‌دست آوردن دسترسی فیزیکی به رسانه شبکه ندارند. آن‌ها به‌سادگی می‌توانند در محدوده انتقال یک گره در حال ارسال، از انتقالات کاربران جلوگیری نماید.

۵-۵ چالش افزارآلات طبقه‌بندی شده

شبکه‌های بالقوه وسایل خانگی: کالاهای سفید، کالاهای قهوه‌ای، تجهیزات مخابراتی، تجهیزات رایانه‌ای، سامانه‌های روشنایی، سامانه نگهداری خانه، زنگ و سامانه‌های پایش و زنگ خطر، سامانه‌های سلامتی و غیره است. برخی از آن‌ها مانند کالاهای سفید یا سامانه روشنایی، توسط منابع محدود، اجباری شده و نمی‌توانند محاسبات پیچیده را ارائه دهند. اما برخی از تجهیزات اطلاعاتی یا وسایل صوتی یا تصویری برنامه‌های کاربردی مختلفی را پشتیبانی می‌کنند و امنیت بالایی را برای حفاظت از اطلاعات نیاز دارند. خدمات امنیتی برای این وسایل مختلف، نیازمند ملاحظات متفاوتی هستند.

۵-۶ نیازهای متنوع و متعدد کاربران

هنگام صحبت از نیازهای کاربر، هر کاربر به یک فرد با نیازهای خاص مبتنی بر او، سبک زندگی، وضعیت اقتصادی، آموزش و غیره به رسمیت شناخته می‌شود. مدل‌های خانه‌های متفاوت موجب الزامات امنیتی متفاوتی می‌شود برای مثال، نگرانی‌های امنیتی به‌وجود آمده از خانواده‌ای بدون فرزند ممکن است متفاوت از خانواده ای با فرزندان باشد.

اغلب نوجوانان برای کسب برخی از درجات استقلال در تلاش هستند. ممکن است این تلاش شامل مالکیت شبکه شخصی و احتمالا شامل دعوت از دوستان به خانه شود. چرا نوجوانان نمی‌خواهند محتویات DVD خود را با والدین به اشتراک گذارند؟ چرا دوستان آن‌ها می‌خواهند درون شبکه‌های خانگی به قسمت شبکه-بندی خود متصل شوند؟

از سوی دیگر ممکن است والدین برخی از محدودیت‌ها را به فرزندان خود تحمیل کنند. برای مثال ممکن است والدین بخواهند مطمئن شوند که فرزندان آن‌ها قادر به دسترسی به برنامه‌های تلویزیونی در روزهای مدرسه پس از ساعت ۷ بعد از ظهر نخواهند بود یا کودکان زیر ۱۲ سال مجاز به مشاهده فیلم دارای امتیاز R در پخش کننده DVD نیستند.

برای خانه‌های مجرد، تمام افزاره‌های داخل خانه متعلق به آن شخص است و ممکن است هیچ الزامات کنترل دسترسی در داخل خانه موجود نباشد. بنابراین صاحب خانه ممکن است بخواهد نماینده برخی مزایای فراهم‌کنندگان خدمات، برای حفظ اهدافی که وظیفه تامین امنیت شبکه از دسترسی خارجی را بر عهده دارد، باشد.

۵-۷ برنامه‌های کاربردی متعدد و متنوع

برنامه‌های کاربردی در شبکه‌های خانگی می‌تواند تقریبا به‌صورت زیر طبقه‌بندی شود:

الف- اتوماسیون خانه: کنترل خانه، امنیت و پایش خانه؛

ب- تفریح و سرگرمی؛

پ- اطلاعات و ارتباطات.

برای برنامه‌های کاربردی مختلف، ممکن است الزامات امنیتی یکسان باشد.

برای اتوماسیون خانه، سازندگان کالاهای سفید شامل یک رابط شبکه در محصولات خود خواهند بود طوریکه فراهم‌کنندگان خدمات با اجازه صاحبان خانه می‌توانند بر وضعیت تجهیزات و کالاهای مصرفی از راه دور پایش کنند. علاوه‌براین مراحل باید انجام شوند تا اطمینان حاصل شود که دستورات کنترل، می‌توانند به‌تنهایی آدرس منبع امن را تایید کنند.

برای تفریح و سرگرمی، کاربران همیشه می‌خواهند افزارآلات سرگرمی خانه را با یکدیگر مرتبط کنند تا قادر به توزیع و اشتراک‌گذاری ویدیو و صدای دیجیتال در سراسر خانه باشند. اما مشکلات کنترل دسترسی ناشی از آسانی ارتباط است. همچنین، امکان دارد صاحبان افزاره بخواهند مطمئن شوند که کاربران مجاز، تنها از مطالب خاصی استفاده می‌کنند.

برای اطلاعات و ارتباطات، حفاظت از حریم خصوصی مهم‌تر از مسائل دیگر است برای اینکه ارتباط ممکن است شامل برخی از صورت‌های مالی، حساب بانکی و اطلاعات مربوط به کارت اعتباری و همچنین اطلاعات شخصی باشد.

۶ مدل‌های امنیتی

۶-۱ مقدمه

ایجاد یک سامانه الکترونیکی خانگی پیچیده که قابل اعتماد باشد، و مدیریت آن به‌منظور حفظ قابلیت اعتماد آن، کار بی اهمیتی نیست. این کار به روش‌های اجرایی خط‌مشی‌های امنیت که به نوبه خود به کاربرد فنون امنیتی مانند کنترل دسترسی، حفظ یکپارچگی و غیره متکی هستند، بستگی دارد. سه سناریو یا مدل کاملا متفاوت می‌تواند برای امنیت سامانه الکترونیکی خانگی شناسایی شده باشد. تعجب‌آور نیست که مشاهده کنید همه این شباهت‌ها در شکل‌های متفاوتی از سازمان‌ها هستند. تهدیدها والزامات امنیتی که در یک خانه هستند اغلب وزن‌های متفاوتی از آن‌ها در یک سازمان هستند. این استاندارد سه مدل را مشخص می‌کند:

۱- (OSS[1])، امنیت مالک خانه پشتیبانی شده
۲- (ESS[2])، امنیت خانه پشتیبانی شده خارج از خانه
۳- (ESM[3])، امنیت چند خانه پشتیبانی شده خارج از خانه

۶-۲ OSS مالک خانه پشتیبانی شده

اولین و ساده‌ترین مدل متشکل از واحد مجزا با خود سامانه الکترونیکی خانگی است (متشکل از یک یا چند واحد سامانه) که به‌طور کامل توسط صاحب یا ساکنان خانه مدیریت می‌شوند. این رابطه امروزه با استفاده خصوصی از سامانه‌های رایانه‌ای با قابلیت اتصال به اینترنت دیده می‌شود. بسیاری از تهدیدها و نقاط ضعف سامانه‌های رایانه‌ای در این معماری یافت می‌شود.
با این حال، بسیاری از صاحبان خانه یا ساکنان عموما با امنیت رایانه و منفعت رساندن از طریق در دسترس بودن فهرست‌های بررسی امنیتی بی‌خبر هستند. یک رویکرد بهتر استفاده از پشتیبانی حرفه‌ای برای امنیت سامانه الکترونیکی خانگی است که ما را به سوی معماری بعدی راهنمایی می‌کند.

۶-۳ ESS امنیت خانه پشتیبانی شده خارج از خانه

سناریوی دوم نیز شامل خانه مجرد است. اما به جای اجازه از مالک یا ساکن، مسئولیت سامانه الکترونیکی خانگی به‌ویژه برای امنیت و قابلیت اعتماد به آن، به یک فراهم‌کننده خدمات حرفه‌ای فن‌آوری اطلاعات برون سپاری داده شده است. این بسیار شبیه به اکثر شرکت‌های کوچک است که بخش فن‌آوری اطلاعات خیلی کوچکی راه‌اندازی کرده‌اند. فراهم کننده خدمات می‌تواند اطمینان حاصل نماید که راه‌حل‌های امنیتی مناسبی انتخاب و به‌درستی نصب و نگهداری می‌شوند. به این ترتیب مزیت آن امنیت و اعتماد است که می‌تواند در نصب وقت‌گیر و دشوار باشد، حفظ و به‌روز رسانی آن تحت مسئولیت کارشناسان حرفه‌ای است.
با این حال، در واقع می‌توان یک قدم بیشتر برداشت و اجازه داد سامانه الکترونیکی خانگی توسط فراهم کننده خدمات حرفه‌ای نگهداشته شده، اجرا و به‌کار گرفته شوند. این ما را به مدل سوم راهنمایی می‌کند.

۶-۴ ESM امنیت چند خانه پشتیبانی شده از خارج از خانه

مدل سوم جایی است که فراهم‌کننده خدمات در خدمت تعدادی از خانه‌ها است. مدل سوم می‌تواند به‌جز خانه‌های محلی در یک منطقه بزرگ پخش شود اما همچنین می‌تواند یک آپارتمان و یا گروهی از خانه‌های شهری باشد، جایی‌که همه آپارتمان‌ها در یک خانه یا خانه‌های شهری در منطقه‌ای باشد که توسط بخش خدمات محلی خدمت می‌گیرند. یکی از تفاوت‌های عمده میان دو مدل اول و این مدل، این است که ارتباطات پیشین به خانه و از خانه مستقیم هستند در حالی که در دومی ارتباطات از طریق ESM می‌باشد.
در این سناریو، صاحب یا ساکنان خانه نقشی مشابه کارفرما یا بخشی در یک سازمان بزرگ با یک گروه حرفه‌ای فن‌آوری اطلاعات را بر عهده دارند. این سناریو قطعا راحت و امن‌ترین راه‌حل برای بسیاری از صاحبان و ساکنان خانه است. اگر این معماری یکی از رایج‌ترین معماری‌ها باشد موفقیت آن قطعا به هزینه

1-Owner Supported Single (OSS)
2-Externally Supported Single (ESS)
3--Externally Supported Multiple (ESM)

ماهانه شارژ این خدمات بستگی دارد. این شارژها امکان دارد متعادل باشند در صورتی‌که شرکت‌های بیمه، حق بیمه را برای آن دسته از مشتریان که این خدمات را اتخاذ کرده‌اند، کاهش دهند.

۷ تحلیل تهدید

۷-۱ کلیات

در تحلیل تهدید، به نظر می‌رسد خسارت‌های قابل احتمال برای صاحب یا ساکن خانه ناشی از اقداماتی در سامانه الکترونیکی خانگی، شبکه خانگی و یا هر قطعه از اطلاعات در سامانه باشد.

تهدیدات سامانه‌ها و شبکه‌های خانگی مشابه تهدیدات سامانه و شبکه‌های سازمانی هستند. با این حال تهدیدات مختلف با مفهوم محلی نسبت به تجاری و پیکربندی شبکه و برنامه کاربردی متفاوت است. برای مثال هنگامی‌که انکار(انکار اینکه معامله صورت گرفته) به طور واضح یک مشکل جدی برای بانک یا شرکت کارگزار است. جایی‌که معامله کاملا خصوصی و غیرتجاری است نگرانی کمتری برای خانه است. در مقابل، شرکت‌های تجاری کوچک با پنهان‌کردن ساعات روز، شبکه‌های خود را مشغول می‌کنند در حالی‌که کاربران مسکونی ممکن است مایل باشند ترافیکی را که نشان می‌دهد آیا آن‌ها در خانه هستند یا نه به خوبی مخفی کنند.

کاربران خانگی ممکن است احساس آسیب‌پذیری کمتری داشته باشند، زیرا افزارآلات شبکه مأموریتی حساس ندارند، سامانه‌های شرکت‌های بزرگ اطلاعات حیاتی شرکت را نگه می‌دارند و به احتمال بسیار زیاد تبدیل به هدف حملات نشده‌اند، اما چنین دیدگاهی منسوخ شده است. افزارآلات شبکه خانگی ممکن است هدف نهایی برای هک نباشند، اما نقطه شروع برای حمله به دیگر افزارآلات، هدف مزاحمان است.

از آنجا که معمولا امکان تعیین انگیزه هنگامی که شما مورد حمله قرار گرفته‌اید وجود ندارد، کاربران خانه باید به اندازه کافی از تهدیدات آگاه بوده و بدانند چه راه‌حل‌هایی در دسترس هستند.

تهدیدات زیر برای سامانه و شبکه خانگی شناسایی شده‌اند:

۷-۲ دسترسی غیرمجاز

واضح است کاربران خانگی مراقب هستند در مورد اینکه چه چیزهایی برای انجام چه اعمالی مجاز هستند یا چه داده‌هایی بر روی هر افزاره در دسترس هستند. برای مثال در مورد یک پخش‌کننده VCR و کنترل‌کننده آن، تنها کنترل‌کننده VCR متعلق به پخش‌کننده VCR می‌تواند به آن دسترسی داشته باشد. به‌عبارت دیگر کنترل‌کننده VCR توسط اعضایی که جز خانواده نیستند انجام یا مالک شده است، همانند مهمانی که از خانه دیدن می‌کند. یک همسایه یا یک دسترسی کاربر از طریق اینترنت ممکن نیست مجاز به دسترسی پخش‌کننده VCR متعلق به یک خانواده خاص باشد. بنابراین به حفاظت از سامانه الکترونیکی خانگی از کاربران غیرمجاز و از اتفاقات راه‌اندازی شده توسط سامانه‌های غیرمجاز درون خانه و یا بیرون از خانه نیازمندیم.

یک مزاحم غیرمجاز ممکن است برای مثال یک سامانه خودکار برنامه‌ریزی شده برای جستجوی پیام‌های آسیب‌پذیر باشد یا فردی باشد که استراق سمع می‌کند و یا در غیراینصورت نقض کننده یکپارچگی کانال‌های ارتباطی است.

دسترسی ممکن است فعال یا غیرفعال باشد. یک مقدار رهگیری شده غیرفعال برای استراق سمع در واقع خواندن ترافیک شخص دیگر است. رهگیری فعال ممکن است شامل تغییرات محتوای پیام‌ها، حذف یا چینش بخشی از ارتباطات یا تغییر پروتکل کنترل اطلاعات به‌ویژه سرآیند (شامل آدرس منبع یا مقصد) باشد.

بیشتر تهدیدها، مزاحم فعال است (محلی یا راه دور) که قادر به دستکاری سامانه الکترونیکی خانگی، نصب یک اسب تروا یا انجام خدمات به نیابت از ساکن یا صاحب خانه است. یک اسب تروا می‌تواند به کاربران غیرمجاز و فرآیندها اجازه دسترسی به داده‌ها و سامانه را دهد. بدین ترتیب قابلیت اعتماد، یکپارچگی و همچنین دسترس‌پذیری از داده و سامانه نقض می‌شود.

شکلی از دسترسی مجاز زمانی است که نفوذگر وانمود به کاربر قانونی نماید مانند صاحب خانه. این، جعل هویت[1] نامیده می‌شود. این نفوذگر می‌تواند وانمود نماید که فراهم کننده خدمت است و با صاحب خانه قرارداد دارد.

نفوذگر در روشی دیگر امکان دارد به سامانه خانگی فریب بزند که فکر کند یک کاربر مجاز است چرا که نفوذگر یک پیام قانونی را می‌رباید و دوباره در زمانی دیگر ارسال می‌کند. این یک حمله پخش نامیده می‌شود. برای مثال اگر نفوذگر بتواند یک پیام را از سامانه هشدار سارق خانه، رهگیری نماید به آن بگوید که خاموش شود، پخش همین پیام در زمان بعد ممکن است نتیجه نامطلوبی را حاصل نماید.

یک مزاحم غیرفعال تنها قادر به خواندن داده‌ها است و همچنین می‌تواند به‌عنوان یک تهدید باشد. داده‌ها می‌توانند حساس باشند هم از نقطه نظر حفظ حریم خصوصی و هم می‌توانند درصورت خالی بودن خانه، آن را نمایان سازند. تهدید قبلی می‌توانست داده‌های شخصی را آشکار کند و مثالی از دومی که خواندن از تنظیمات گرمایشی است می‌تواند برای یک سارق بالقوه بسیار آموزنده باشد. این تهدیدها برای هر سه مدل وجود دارند. بنابراین مهم این است که اطمینان حاصل شود که تنها کاربران مجاز، دسترسی به سامانه الکترونیکی خانگی و داده‌های آن را دارند و سامانه‌های بیگانه به آسانی نمی‌توانند به این نوع از داده‌های سامانه الکترونیکی خانگی دسترسی داشته باشند.

حتی اگر تمام ارتباطات خدمات یکپارچه بودن و قابلیت اعتماد بکار برده شوند، هنوز هم استراق سمع‌کننده می‌تواند اطلاعات زیادی در مورد شبکه خانگی با استفاده از منبع پایش و اطلاعات مقصد و زمان هر پیام، یاد بگیرد. این، تجزیه و تحلیل ترافیک نامیده می‌شود.

تهدیدهای نقض حریم خصوصی در دو معماری اخیر بیشتر است (ESS و ESM)، چون در این مدل‌ها، نه‌تنها ساکنان بلکه سازمان‌های خارجی حمایت از سامانه الکترونیکی خانگی ممکن است مجاز به دسترسی به سامانه باشند. توصیه می‌شود که این سازمان‌ها، به‌هرحال، تنها قادر به حفظ سامانه الکترونیکی خانگی و

1- Masquerade

دسترسی به اطلاعات حیاتی حفظ حریم خصوصی باشند. این یک مسئله غیرفنی است و متکی به رابطه اعتماد میان فراهم کنندگان خدمات و مشتریان خود است.

۳-۷ نرم‌افزار مخرب و پیکربندی

پیکربندی و نرم‌افزار مخرب می‌تواند، به‌عنوان مثال از طریق لینک ارتباطی و یا بارگذاری یک بسته نرم‌افزاری آلوده وارد سامانه الکترونیکی خانگی در خانه شود. بارزترین نمونه نرم‌افزارهای مخرب، ویروسی است که وارد سامانه الکترونیکی خانگی می‌شود. یک ویروس ممکن است داده‌ها و برنامه‌های نرم‌افزاری را نابود کرده و سامانه را غیرقابل استفاده نماید. این تهدیدی برای یکپارچگی نرم‌افزار و پیکربندی اطلاعات بر روی افزاره‌های دسترسی و شبکه خانگی است.

اسب تروا برنامه غیرمجازی است که پنهانی در یک پیام قانونی وارد منزل یا افزاره دسترسی می‌شود. یکبار دیگر در خانه، اسب تروا می‌تواند در پردازنده هر افزاره شبکه مسقر شود. برای مثال یک اسب تروا می‌تواند درون MPEG جدا شده از جریان انتقال داده‌های خصوصی، مندرج و محل اقامت خود را در پردازنده تلویزیون دیجیتال در دست گیرد. سپس می‌تواند از منابع پردازنده تلویزیون و شبکه خانگی دیجیتال جهت مصالحه امنیت شبکه داخلی استفاده نماید.

کرم‌ها و ویروس‌ها در هر دوی مطبوعات مشهور و تکنیکی، شهرت قابل توجهی کسب کرده‌اند. یک کرم، برنامه‌ای است که می‌تواند خود را تکثیر نموده و کپی‌ها را از رایانه‌ای به رایانه دیگر در سراسر اتصالات شبکه ارسال کند. به محض ورود، کرم ممکن است دوباره به تکثیر و انتشار فعال شود. علاوه‌براین، این کرم معمولا برخی از توابع ناخواسته را انجام می‌دهد. یک کرم با حمله به شبکه خانگی می‌تواند در سراسر شبکه به افزاره‌های متعدد گسترش یابد. اگر کرم فعالیت‌های مضر مانند پاک کردن حافظه غیر فرار از افزاره را انجام دهد صاحب خانه می‌تواند وسایل متعددی را پیدا کند از تلویزیون دیجیتالی گرفته تا به توسترها، که به درستی کار نمی‌کنند.

ویروس کدی است که درون برنامه جاسازی شده و باعث می‌شود یک کپی از خود را در یک یا چند برنامه قرار دهد. همچنین برخی از عملکردهای غیرمجاز بر روی افزاره میزبان انجام می‌شود. برخلاف یک کرم یک ویروس به طور فعال سعی در گسترش خود در پردازنده‌های دیگر در شبکه خانگی نخواهد کرد. بنابراین صدمه آن به یک افزاره واحد محدود خواهد شد. با این حال یک وسیله خانگی ضروری به بهره‌برداری از شبکه خانگی ممکن است به روش نامطلوب و غیر قابل پیش بینی عمل کند.

برخی از حملات ممکن است در سازش با پیکربندی شبکه خانگی توسط تغییر اطلاعات امنیتی باشند. سه نمونه از این نوع امنیت اطلاعات از سرویس‌دهنده‌های خارجی، کلیدهای عمومی مورد اعتماد و یا کلمه عبور مورد استفاده در فرآیند تصدیق و قوانینی برای فیلتر کردن ترافیک ناخواسته در رابط دسترسی نشان داده شده است.

۴-۷ محرومیت از خدمت‌ها

محرومیت از خدمت‌ها باعث می‌شود سامانه غیرقابل استفاده شود. برخی از تاسیسات غیرقابل استفاده، سبب زحمت و تنها نیازمند تجدید نظر در زمان دیگر می‌باشند. در شرایط دیگر می‌توانند تهدید جدی در خانه باشند برای مثال از کار انداختن زنگ خطر سامانه.

یک حمله محرومیت از خدمات، تحت تاثیر سیل دسترسی به شبکه با ترافیک بی‌فایده و جلوگیری از رسیدن پیام‌های درست به شبکه خانگی واقع می‌شود. پیام‌های ورودی می‌تواند شبکه خانگی را برای پاسخگویی و اتصال به منابع افزاره دسترسی و بنابراین آسیب رساندن به ترافیک خروجی مجبور نماید. شبکه خانگی ممکن است قربانی یک حمله عدم پذیرش خدمت یا شریک بی‌خبر[1] باشد. اگر رایانه‌ای در شبکه خانگی به خطر بیفتد حمله کننده ممکن است بتواند از آن برای کمک بسته سیل‌آسا[2]، بدون اطلاع صاحب خانه استفاده کند. این امر، حمله محرومیت از خدمات توزیع شده نامیده می‌شود.

۵-۷ اصلاحات ناخواسته از داده‌ها در هنگام برقرای ارتباط

امکان دارد بخشی از اطلاعات به‌طور تصادفی تغییر یافته یا چنانچه پیام به اشتباه تفسیر شود دوباره در حال انجام ارتباط باشند. تغییرات جزئی از یک بیت در طول انتقال ممکن است توسط کد تصحیح خطای استاندارد تصحیح شده باشد اما حفاظت از یکپارچگی واقعی در طول ارتباط نیازمند فن‌آوری رمز گذاری است.

۶-۷ خطاهای کاربر

خطری که وجود دارد این است که کاربر مجاز باعث خطاها و استناد به خدمت‌های اشتباه یا پارامترهای معیوب در دستورات می‌شود. چنین اشتباهاتی زمانی‌که ساکن خانه در خانه حضور دارد نسبت به زمانی‌که دور از خانه هستند، احتمالا اهمیت کمتری دارند. یک روش برای به حداقل رساندن چنین اشتباهات این است که کاربر یک افزاره با واسط کاربر ساده‌ای را فراهم می‌کند که استفاده و انجام صحه گذاری ورودی را آسان می‌کند. اقدام متقابل دیگر، محدود کردن مجموعه دستوراتی است که می‌تواند زمانی‌که دور از خانه هستند درخواست شود.

۷-۷ اشکالات سامانه

اشکالات در یک سامانه الکترونیکی خانگی قطعا در برخی از مواقع رخ خواهد داد. این هم می‌تواند به دلیل نقض امنیت یا به‌دلیل ناپایداری سامانه، قطع شدن برق، رعد و برق و یا بسیاری از دلایل دیگر باشد. نتیجه این است که بخش یا همه داده‌ها و سامانه، بیش از این در دسترس نیستند. در نتیجه نیازمند یک فرآیند بازیابی و احتمالا فن‌آوری و روش‌های مجدد می‌باشند.

1-Unwitting Participant
2-Packet Flood

۸-۷ امنیت فراهم‌کنندگان خدمت‌ها

در نهایت، برای امنیت فراهم‌کنندگان خدمت‌ها به‌عنوان نقطه متمرکز مرکزی در معماری سوم ESM بیان شده است. یک مجموعه کامل از اقدامات امنیتی پیچیده باید نصب شود. این‌ها بسیار شبیه به سازمان‌های دستکاری داده‌های حساس هستند و باید در ۲۴ ساعت یک شبانه روز از هفت روز در یک هفته قابل درمان باشند. این الزامات اگرچه در این استاندارد تشریح نشده است اما انجام خواهند شد.

۸ الزامات امنیتی

۸-۱ کلیات

یک ساکن یا صاحب خانه، می‌تواند رابطه قابل اعتمادی با کمک تعدادی از افزاره‌ها و روش‌های مختلف برقرار نماید. اعتماد به سامانه الکترونیکی خانگی به‌طور کلی شامل ترکیبی از اقدامات شمارشگر فنی (مانند دیوار آتش[1]، نرم‌افزار ضد ویروس، و غیره)، اقدامات رویه‌ای (مانند برنامه کاربردی ارتقا نرم‌افزار، اقدامات پشتیبان‌گیری و بازیابی، آموزش امنیت و آگاهی) و اقدامات متفرقه مانند بیمه می‌باشد. این امر شامل دستورالعمل و روش‌های زیر است، به‌عنوان مثال: چگونگی نصب، پیکربندی، نگهداری، به‌روز رسانی و یا استفاده از سامانه.

لازم به ذکر است که بسیاری از مکانیزم‌ها و خدمت‌های امنیتی که برای مقابله با تهدیدهای بالقوه در محیط‌های کسب و کار توسعه یافته‌اند ممکن است برای شبکه‌های خانگی با توجه به محدودیت امکانات فن‌آوری اطلاعات از قبیل سنسورها و لوازم خانگی مناسب نباشند.

در شرح زیر مجموعه‌ای از تهدیدات امنیتی که برخی بسیار جدی و برخی دیگر جدیت کمتری دارند، برای راه‌حل‌های امنیتی سامانه الکترونیکی خانگی به‌منظور بهبود اعتماد به آن در دسترس هستند. جدول ۱ به‌اختصار، برخی از مکانیسم دفاعی در برابر تهدیدات فهرست‌شده در بند ۷ را بیان می‌کند:

جدول ۱ - تهدیدات امنیتی و دفاعی مربوطه

تهدید	دفاع
رهگیری فعال اضافه کردن پیام‌ها تغییر داده	 تصدیق داده یکپارچگی داده
محرومیت از خدمت	دیوار آتش، کنترل دسترسی، نفوذ فیلتر
استراق سمع	خدمت‌های قابل اعتماد
جعل هویت	احراز هویت کاربر یا افزاره (بخشی از کنترل دسترسی)
دسترسی از راه دور	کنترل دسترسی
پخش[2]	خدمت‌های ضد پخش، احراز هویت پخش محافظت شده
انکار	رمزنویسی کلیدهای عمومی
شکست سامانه	بازیابی، fallback و ...

1- Firewall
2-Replay

تحلیل ترافیک	توسعه پیام
دسترسی غیرمجاز به داده‌ها در ارتباط	خدمت‌های محرمانه
دسترسی غیرمجاز به داده‌ها در سامانه	کنترل دسترسی
تغییر غیرمجاز در داده	کنترل دسترسی
اصلاح ناخواسته از داده	کد تصحیح خطا ،خدمت یکپارچگی داده
خطای کاربر	رابط کاربر، کنترل دسترسی از راه دور
ویروس، کرم، اسب تروا:	
فایل‌های باز و ضمیمه‌ها	مدیریت، نرم‌افزار
نصب نرم‌افزار جدید	مدیریت، نرم‌افزار
به‌روز رسانی نرم‌افزار بر خط	مجوز
به‌روزرسانی محلی نرم‌افزار	مدیریت، نرم‌افزار

۸-۲ کنترل دسترسی

دسترسی غیرمجاز به سامانه الکترونیکی خانگی و خدمت‌های آن همان‌طور که در بند ۷ شناسایی‌شده، شدیدترین تهدید است و حفاظت در برابر این تهدید مکانیزم کنترل دسترسی خوبی است. کاربرد خوبی است که برای سطوح مختلف از حقوق دسترسی به افراد مختلف داده شود. برای اولین‌بار مدل (OSS)[1] مهم است که کاربر را تشخیص دهد، به‌عنوان یک مدیر سامانه اقدام نماید، همان شخص به‌عنوان یک کاربر معمولی اقدام کند. چندین سطح از حقوق دسترسی قابل قبول است. برخی از توابع وجود دارند که می‌توانند به هر کسی اجازه دهند، در حالی‌که به توابع دیگر فقط دسترسی محدود داده خواهد شد، به‌عنوان مثال به کودکان. دلایل خوبی برای ارائه بیشتر محدودیت حقوق دسترسی در زمانی که دور از خانه هستند نسبت به زمانی که از درون خانه اقدام می‌نمایند، وجود دارد. (به دسترسی و کنترل از راه دور زیر مراجعه کنید.)

مرحله اول، ثبت و ثبت‌نام از کاربران مجاز. مدیریت دقیق کاربران مجاز و ثبت‌نام شده اهمیت دارد. به‌عنوان مثال، کاربرد خوبی است که فورا حقوق دسترسی کاربرانی را که طرح‌های خود را تغییر می‌دهند لغو کند، به‌عنوان مثال حقوق یک بازدید کننده برای ورود به خانه باید لغو شده باشد در صورتی‌که بازدید کننده زودتر از طرح‌ریزی اولیه خانه را ترک کند.

در مرحله دوم، احراز هویت مناسب از کاربر، که تأیید هویت کاربر است، شرط ضروری برای یک سامانه کنترل دسترسی است. بعد از شناسایی کاربران مجاز تایید شده توسط سامانه الکترونیکی خانگی می‌توان حقوق دسترسی درستی برای منابع درخواست‌شده برای آن کاربران، فراهم نمود. با این‌حال قدم اول این است که الزامات برای کاربران مجاز ثبت شوند. این برای مدل اول توضیح داده شده در بالا، چندان دشوار نیست، اما برای دو روش دیگر به‌خصوص برای سومین معماری مهم است که فراهم کننده خدمات، مالک یا ساکنان خانه و کاربران را به درستی ثبت کند.

جعل هویت را می‌توان با استفاده از کنترل دسترسی با احراز هویت مناسب همراه با خدمات یکپارچه داده‌ها خنثی کرد.

1- Open Source Software (OSS)

با این حال، احراز هویت برای مقابله موثر کوتاه با حملات پخش با شکست مواجه می‌شود. با این وجود، حملات پخش می‌توانند با استفاده از ارائه منحصر به فرد و مناسب پارامترهای گوناگون زمان، دفاع کنند. یک روش ساده این است که پیام‌های تکرارشده را امتحان کنند که این قابل انجام است، برای مثال با امتحان برچسب زمان یا دنباله تعدادی از فیلدها در برابر پیام‌های ذخیره شده قبلی.
علاوه‌بر این کنترل دسترسی فیزیکی و منطقی در ساختمان، نسبت به افزاره‌های سامانه الکترونیکی خانگی که نیازمند محافظت هستند حساس است. برای مثال، در صورتی‌که نگهداری توسط یک بیگانه در منزل انجام شود کاربرد خوبی است قبل از دادن دسترسی به ساختمان و تجهیزات آن احراز هویت درخواست شود. همچنین هر به‌روز رسانی و نگهداری از راه دور نیازمند احراز هویت است.

۸-۳ احراز هویت پیام‌ها و داده

یکی دیگر از نگرانی احراز هویت مناسب از پیام درخواست کننده خدمت‌ها، این است که در آن پیام در هر دو جهت (از سوی کاربر به خانه و یا از خانه به کاربر) نیازمند احراز هویت است. الزامات احراز هویت پیام از کاربر به منزل واضح است، از این رو این‌ها پیام‌هایی هستند که اقدامات کاملا موثری درون خانه خواهند داشت. با این حال، کاربرد خوبی است برای اینکه اجازه دهد پاسخ پیام‌ها از خانه به کاربر داده شود و همچنین تایید شود که مبادا دشمن یک اذعان جعلی درج کند و یا پیام را زمانی‌که در واقع پیام اصلی هرگز نرسیده بود تایید نماید. همچنین، تصدیق اطلاعیه‌ها و پاسخ از خانه در نهایت ممکن است شامل اطلاعات مربوط به وضعیت، مانند درجه حرارت از خانه و یا اینکه آیا سامانه زنگ خطر روشن است، باشد.

۸-۴ کنترل دسترسی از راه دور

اغلب ساکنان می‌خواهند به سامانه الکترونیکی خانگی زمانی‌که دور از خانه هستند دسترسی داشته باشند. بنابراین لازم است به سامانه اجازه دسترسی از خارج داده شود. این نیازمند مکانیزم احراز هویت خوبی است همان‌طور که در بالا توضیح داه شده است. در مقایسه با محیط‌های کسب و کار، که یک کاربر معمولی به‌طور معمول فقط دسترسی به محیط فن‌آوری اطلاعات و در نتیجه به‌طور معمول دریافت حقوق دسترسی دارد همان حقوق دسترسی‌ها به‌طور معمول در یک محیط خانه و به‌علاوه پشتیبانی کنترل از راه دور بر روی افزاره‌های بسیاری از خانه‌ها وجود دارد. ممکن است این امر نیازمند یک کنترل دسترسی مختلف با کمترین حقوق دسترسی باشد که به‌هنگام عمل از راه دور به‌منظور محدود کردن تعداد عملیات و پارامترها که می‌توانند مورد استفاده قرار گیرند، انجام می‌شود. از آنجا که عملیات، ناخواسته به‌هنگام دور بودن از خانه دشوارتر رعایت می‌شود، توجه به کاربر رابط بر روی افزاره‌های مورد استفاده برای دسترسی از راه دور و نیز توجه ویژه برای جلوگیری از اشتباهات نیاز است.

۸-۵ حفاظت از ارتباطات

به‌طور کلی یک کاربر نمی‌خواهد هیچ استراق سمع‌کننده‌ای متن یک پیام را بفهمد. این امر نه تنها بدنه پیام (که حاوی دستورات اجرا شده است)، بلکه به زمینه‌های سرآیند آن که ممکن است به اطلاعات مربوط به صاحب افزاره مربوط شود را نیز آشکار کند. به‌عنوان مثال، [به :] زمینه سرآیند حاوی یک URL از هستار

نشان داده شده است، که ممکن است نوع افزاره و محل آن را نشان دهد. ممکن نیست کاربر بخواهد هر کسی بداند که آیا یک مجموعه تلویزیونی در خانه وجود دارد و یا قطعا در کدام اتاق آن قرار گرفته است.
چهار نوع از ارتباطات در محیط خانه وجود دارد. توسط کابل در خانه، بی‌سیم در خانه و توسط کابل یا بی‌سیم به و از خانه. همه این‌ها، شاید با استثنای ارسال داده توسط کابل، در داخل خانه نیازمند قابلیت اعتماد و حفاظت از یکپارچگی به‌منظور حصول اطمینان از اینکه فقط کاربران مجاز به داده‌ها دسترسی دارند و این‌که تغییرات غیرمجاز را می‌توان شناسایی کرد، می‌باشند. الزامات امنیتی برای ارتباطات با استفاده از کابل در یک خانه واحد به این‌که چه شکلی از کابل استفاده شده باشد، بستگی دارد. به‌طور کلی، می‌توان اظهار داشت که احتمالی وجود دارد که ارتباطات را بتوان در خارج از خانه شناسایی کرد، و سپس نیاز برای حفاظت از قابلیت اعتماد وجود دارد. علاوه‌بر این، اگر یک بیگانه بتواند تغییر دهنده یا وارد کننده داده‌ها به سامانه باشد، حفاظت از یکپارچگی همچنین ممکن است لازم باشد.
محافظت در برابر تجزیه و تحلیل ترافیک را می‌توان با ایجاد ترافیک ساختگی برای پنهان کردن پیام‌های مفید ایجاد کرد.
حفاظت از داده‌ها در طول ارتباطات توسط قابلیت اعتماد و خدمات حفاظت از حریم خصوصی و یکپارچگی و توسط خدمات تایید هویت از هدف در نظرگرفته شده است. مهم است که چنین راه‌حل‌هایی در استانداردهای پذیرفته شده بین‌المللی به‌منظور اطمینان از قابلیت همکاری با جهان خارج پایه‌گذاری شود.

۸-۶ دیوارهای آتش

اگر کاربران خانگی نسبت به حفاظت از افزاره‌های خانگی و داده‌های موجود در خانه از مزاحمان خارجی نگران باشند آن‌ها نیازمند دیوار آتش هستند. معمولا یک دیوار آتش بین شبکه محلی و اینترنت قرار دارد. علاوه بر این دیوارهای آتش ممکن است برای قسمت‌بندی شبکه‌های محلی به چندین دامنه امنیتی جهت حفاظت از افزاره‌های شخصی استفاده شوند. که می‌تواند برای کنترل ترافیک ورودی وخروجی شبکه مورد استفاده قرارگیرد.
هدف اصلی یک دیوار آتش جلوگیری از حملات هک شبکه از بیرون است. پاسخ‌های سامانه برای سرپیچی خدمات باید برای جلوگیری ازیک هکر بالقوه در یافتن اطلاعات مفید سامانه به‌عنوان آدرس فیزیکی IP طراحی شده‌باشد.
لازم به ذکر است که یک دیوار آتش که در مقابل ارتباطات مبتنی بر پروتکل IPv4 موثر است، امکان دارد برای ارتباطات مبتنی بر پروتکل در حال ظهور IPv6 موثر نباشد.

۸-۷ حفاظت از ویروس

داشتن یک ویروس، کرم یا اسب تروا در سامانه الکترونیکی خانگی برای همه نگران کننده است. حفاظت در مقابل این مسئله کاملا فنی نیست. بیشتر به‌دلیل رفتار کاربران سامانه الکترونیکی خانگی است. بنابراین باید یک سیاست سختگیرانه داشت، برای مثال، می‌گوید: در هنگام باز کردن پیوست‌های ایمیل از منابع نامعلوم مراقب باشید. یکی دیگر از مقابله‌ها در برابر حملات ویروس ممکن است از طریق مکانیزم کنترل دسترسی توسط مسدود کردن دسترسی به هر قسمت که قادر به تایید درست خودش نیست، به‌دست آید.

مطابق اصول فنی، روش‌های مختلفی برای تشخیص نرم‌افزارهای مخرب وجود دارد. بنابراین هیچ استانداردی که بتواند در برابر ویروس‌ها حفاظت کند وجود ندارد. هر روز ویروس‌های جدیدی وارد شبکه بین‌المللی می‌شوند و چندین شرکت، سخت در تلاش برای پیدا کردن حفاظتی در برابر آن‌ها هستند. که می‌تواند هم از طریق ارتباطات خارجی مانند فایل ضمیمه در ایمیل وارد سامانه شود، همچنین می‌تواند از طریق بارگذاری نرم‌افزار آلوده در داخل سامانه الکترونیکی خانگی وارد شود. روش پیشنهادشده به‌دست آوردن بسته نرم‌افزاری حفاظت از ویروس از یکی از تولیدکنندگان ابزارهای حفاظت از ویروس است و مطمئن شوید که مرتبا به‌روز رسانی می‌شوند.

۸-۸ حفاظت در برابر حملات محرومیت از خدمت‌ها

دو نوع از محرومیت از خدمت‌ها وجود دارد. یکی، هنگامی رخ می‌دهد که یک کاربر واقعی از سامانه الکترونیکی خانگی برای دسترسی به یک خدمت از راه دور تلاش کند و از این دسترسی محروم شده است. در این مورد این خدمت ممکن است با قابلیت سرریز در دسترس قرار گیرد یا با یک حمله محرومیت از خدمات برخورد کند. گزینه‌ها برای کاربر واقعی بسیار محدود است. در این مورد، این امکان وجود دارد تا سرویس دیگری را امتحان کند یا صبر کند تا بار ترافیک کاهش یابد و یا خدمات مجددا تنظیم شوند.

وضعیت دیگر این است که سامانه الکترونیکی خانگی حمله محرومیت از خدمات را دریافت کرده است. حملات محرومیت از خدمات برای دفاع در برابر زمان واقعی تقریبا غیرممکن است. در واقع، مکانیزم‌های امنیتی به‌تنهایی نمی‌توانند در برابر حملات محرومیت از خدمات موثر باشند چون به‌طور ناقابل برای از هم پاشیدن هر نوع دفاع ارسال پیام‌های اضافی جعلی آسان است. طراحی دقیق و پیاده‌سازی پروتکل و افزاره دسترسی می‌تواند خستگی منابع را تسکین دهد که به‌موجب آن سیل بخش‌هایی از شبکه خانگی یا دسترسی به افزاره را می‌بندد. به‌عنوان مثال، اگر افزاره دسترسی، به رسمیت شناخته شود برای باز کردن ۵۰۰۰ ارتباط TCP همزمان درخواست خواهد شد، که آن می‌تواند در شرایط زنگ خطر باشد که در آن درخواست‌های دریافتی اضافی که رمزنگاری به‌درستی تایید شده نیست، نادیده گرفته می‌شوند و آن اولویت بر روی صف‌های خروجی خود برای منشا پیام‌ها در خانه را ارائه می‌دهد.

برای اطمینان از شبکه خانگی نمی‌شود یک شرکت کننده بی‌خبردر حمله محرومیت از خدمات توزیع شده باشد، اقدامات باید برای حصول اطمینان از این‌که نرم‌افزار غیرقانونی نصب شده است انجام شود. افزاره کنترل دسترسی با نفوذ فیلترینگ پیاده‌سازی‌شده به‌عنوان RFC 2267 مشخص شده مانع استفاده از IP آدرس‌های جعل‌شده است. لازم به‌ذکر است، با این‌حال اگر حمله کننده از آدرس شبکه‌های معتبر استفاده نماید هیچ اثری ندارد. نفوذ فیلترینگ، منبع حمله را بسیار آسان‌تر ردیابی می‌کند برای اینکه آدرس منبع بسته، منبع ترافیک می باشد. یک مزیت دیگر این است که واکنش قربانی به سامانه حمله‌کننده برگردانده می‌شود بنابراین از آسیب جلوگیری می‌شود. برای انجام نفوذ فیلترینگ، افزاره‌های دسترسی هر بسته با آدرس‌های منابعی که از درون شبکه خانگی سرچشمه می‌گیرند را بلوکه می‌کنند.

۸-۹ حسابرسی

حسابرسی، یک مکانیزم امنیتی است که در هیچ مکانیزم حفاظتی اجرا نمی‌شود، اما چیزی که معمولا برای کنترل و بررسی مکانیزم‌های امنیتی استفاده می‌شود به‌عنوان عملکرد در نظرگرفته شده است. حسابرسی، عملیات امنیتی حساس مربوطه را ثبت می‌کند. اینکه عملیات امنیتی باید ثبت شوند، تصمیم گرفته شده‌است. اگر تمام عملیات مرتبط با امنیت بر روی سامانه ثبت شوند ممکن است در اینکه هر رخداد ناخواسته در میان مقدار زیادی از داده‌های ثبت‌شده تشخیص داده شوند، مشکلی به‌وجود آید. از سوی دیگر، اگر فقط عملیات حساس بسیار محدود ثبت شوند، رخنه‌های امنیتی ممکن است تشخیص داده‌نشوند.

به‌طورکلی می‌توان حالتی باشد که کمترین عملیات مرتبط با تنظیماتی از پارامترهای امنیتی را دارد. مانند ثبت نام از کاربران و همه تلاش‌های احراز هویت شکست خورده باید به ثبت برسند. حتی احراز هویت‌های موفق اغلب مفید است، زیرا می‌تواند پس از آن مشخص کرد اینکه چه کسی در زمان مشخص از سامانه استفاده کرده است.

۸-۱۰ بازیابی

در صورت شکست سامانه نیاز است که بتواند دوباره قابل راه‌اندازی باشد. این بی‌ربط است اگر سامانه به‌دلیل نقض امنیتی یا به‌شکل دیگری از شکست‌ها، شکست بخورد. مناسب‌ترین روش در تهیه بازیابی این است که مرتبا از سامانه پشتیبانی (رونوشت) بگیرد. هرچند وقت نیاز به ایجاد رونوشت‌ها، وابسته به این است که سامانه الکترونیکی خانگی هرچند وقت تغییر می‌کند.

۹ راه‌حل‌های امنیتی مورد نیاز

۹-۱ کلیات

الزامات در این بند تعیین شکل و توانایی راه‌حل‌های امنیتی نسبت به نوع حفاظت از آن، را فراهم می‌کند.

۹-۲ سطوح مختلف از خدمات امنیتی برای برنامه‌های کاربردی مختلف در یک خانه

برای فعالیت‌های مختلف، سطوح مختلف امنیتی اغلب پذیرفته شده است. به‌عنوان مثال، کنترل‌کردن درجه حرارت تهویه هوا در یک اتاق خواب از اتاق نشیمن، نیازمند همان سطح از امنیت برای کنترل یک افزاره خانگی از بیرون نیست. با توجه به عوامل مختلف در شبکه‌های خانگی تقریبا غیر ممکن است که یک راه حل مهم خدمت‌های امنیتی را فراهم کند و بتواند مدل‌های مختلف شبکه‌بندی‌های خانگی، نیازهای کاربران مختلف، و برنامه‌های کاربردی را در یک زمان پوشش دهد.

بنابراین نیاز است که یک راه‌حل امنیتی باید قادر به حمایت از چندین سطوح کیفیتی امنیت در خانه‌های واحد باشد.

۹-۳ تسهیلات

به‌طور کلی، کاربران مسکونی راه‌حل‌هایی را انتخاب خواهند کرد که هزینه مالی بیش از حد و نیاز به دانش زیاد نداشته باشد. بنابراین راه‌حل انتخاب‌شده باید تا آنجا که ممکن است الزامات زیر را برآورده سازد:

الف- هزینه کم؛

ب- پیچیدگی کم؛

پ- سهولت استفاده (تا حد امکان به‌صورت خودکار).

همچنین، قابلیت اطمینان برای کاربران مسکونی ضروری است. اگر این فرآیند نگهداری رایگان، سهولت استفاده، نصب سریع نباشد، به احتمال زیاد پذیرفته نمی‌شود. کاربران یک سامانه پیچیده را مهندسی یا مدیریت نمی‌کنند. این به‌ویژه برای امنیت مدل OSS مهم است اما همچنین برای ESS و به میزان کمتر مدل ESM که در بالا توضیح داده شد، اهمیت دارد.

پیوست الف

(اطلاعاتی)

مقایسه بین الزامات سامانه‌های دفتری فناوری اطلاعات و سامانه الکترونیکی خانگی

دفتر سامانه فن‌آوری اطلاعات سامانه اطلاعاتی خالصی است که در مقایسه با سامانه الکترونیکی خانگی برای کنترل افزاره‌ها به‌جز افزاره‌های فن‌آوری اطلاعات استفاده نمی‌شود مانند چاپگر و غیره. شبکه داخلی و الزامات امنیتی درنتیجه می‌تواند به‌طور قابل ملاحظه‌ای مختلف باشد. بنابراین امنیت در شبکه‌های بیرونی بسیار شبیه است. از آنجا که دفتر خانه بخشی از سامانه الکترونیکی خانگی است یک سامانه الکترونیکی خانگی شامل تمام الزامات خارجی به‌عنوان یک سامانه اداری است. علاوه‌بر این، چندین تهدید دیگر برای خانه وجود دارد که نیازمند آن است که در نظر گرفته شود.

چندین الزامات دیگر در مورد امنیت اطلاعات خارجی برای مقایسه سامانه الکترونیکی خانگی نسبت به خانه و محیط‌های فن‌آوری دفتری شناسایی‌شده که به شرح زیر است:

- مانند برخی از دفاتر، یک خانه هوشمند ۲۴ ساعت یک شبانه روز و ۷ روز هفته را روی خط اینترنت است.
- الزامات تنها برای کنترل از راه دور سامانه نیست بلکه کنترل از راه دور افزاره‌ها در خانه نیز وجود دارد مانند گرمایشی، با این حال، حقوق دسترسی مشابه زمانی که آن‌ها از راه دور کنترل می‌شوند به همان اندازه زمانی که کنترل آنها ازداخل خانه است به افزاره داده نمی‌شود. بنابراین، باید مشخص شده باشد که کنترل از درون خانه است یا از راه دور. این ممکن است به‌عنوان مثال به‌وسیله اجازه‌ای که دروازه مستقیم ارتباطات برای یک مکانیزم کنترل دسترسی مختلف از آن استفاده می‌شود در زمانی‌که دسترسی سامانه از درون خانه است، حل شده باشد.

الف- این تجهیزات، هر کدام از افزاره‌ها در خانه کنترل شده است، به‌ویژه در مورد کنترل از راه دور، باید در چنین شیوه‌ای که از اشتباهات اجتناب شود طراحی شده باشد. در نتیجه الزامات امنیتی بر روی رابط کاربری از افزاره‌ای که کنترل از راه دور ساخته شده است وجود دارد؛

ب- در صورت خرابی سامانه، باید راه‌حل‌های مجدد وجود داشته باشد که آن نیز بتواند افزاره‌ها را کنترل کند و به‌طور معمول از سامانه الکترونیکی خانگی بدون سامانه آن را اداره کند. به‌عنوان مثال قفلی که بر روی درها است. یک سامانه شکست باید استفاده از این افزاره‌ها را متوقف کند.

سامانه الکترونیکی خانگی باید ایمن از شکست باشد. این بدان معنی است که در صورت از کار افتادن افزاره باید حالتی را که باعث صدمه به ساختمان یا ساکنان آن نمی‌شود را شروع کند. این الزامات بیشتر علاقمند به افزاره‌هایی هستند که توسط سامانه کنترل شده‌اند نه توسط خودش.

پیوست ب

(اطلاعاتی)

کتابنامه

[1] ISO/IEC 10116, Information technology – Security techniques – Modes of operation for an n-bit block cipher

[2] ISO/IEC 18028 (all parts), Information technology – Security techniques – IT network security

[3] ISO/IEC 18033-3, Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers

[4] ISO/IEC 27002, Information technology – Security techniques – Code of practice for information security management

کمسیون اروپایی COM (2001) 298:

امنیت اطلاعات و شبکه : پروپزال یک راهکار سیاستی اروپایی

http://ec.europa.eu/transparency/regdoc/liste.cfm?&type=1&annee=2001&numero=298&ElementsPerPage=20&tri=cote&CL=en

Freier, A.O., P. Carlton and P.C. Kocher, The SSL Protocol Version 3.0.

Dierks, T. and C. Allen, The TLS Protocol Version 1.0, RFC 2246, Internet Engineering Task Force, January 1999.

Kent, S., R. Atkinson, Security Architecture for the Internet Protocol, RFC 2401, Internet Engineering Task Force, November 1998.

NIST, FIPS PUB 197, "Advanced Encryption Standard (AES)," November 2001.

RFC 2267, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing