یازدهمین کنگره ملی سراسری
فناوریهای نوین در حوزه توسعه پایدار ایران
11th National Congress of
the New Technologies in Sustainable Development of Iran
senaconf.ir

امنیت در سیستم های تعبیه شده

طاهره زارعی[1]

[1] همدان، Tara.zarei94@gmail.com

چکیده

امنیت سیستم تعبیه شده ، زمینه درحال بروزی در تحقیقات امروزی است که به خاطر کاربرد آنها در دستگاه ها، امروزه درجهت دید همگان قرار گرفته اند،این سیستم ها در حال فراگیر شدن در محیط های خانگی و تجاری هستند. با این حال، تلفن های هوشمند، تبلت ها، کنسولهای بازی ویدئویی که همگی با علمکرد اصلی شان شناخته می شوند، دارای قابلیت های بیشتری بوده و قادر به تعاملات بیشتری هستند. علاوه بر این، با اتصال به اینترنت، در معرض همه نوع حمله ای هستند که ممکن است نتایج بدی به همراه داشته باشند. از نظر سنتی، امنیت، حریم خصوصی و قابلیت سازگاری (SPD) در فرآیند طراحی کنار گذاشته شده اند و به عنوان ویژگی های اضافی در نظر گرفته می شوند، محققان با بررسی پروژه های تحقیقاتی نسبتا جدید EU ، ۲۰ پروژه را که تمرکز آنها بر جنبه های امنیتی سیستم های تعبیه شده بود تشخیص دادند. تقسیم بندی ها از گره ها، شبکه ، میان افزار و لایه های زیرین و نیز معماری ها، چارچوب های امنیت سیستم های تعبیه تشکیل شده است. با توجه به این مسئله، الگوهای خاصی با توجه به این موضوعات پیشنهاد شده و محققان برای بررسی مسائل پیشنهادی روی آن تمرکز کرده اند. در نهایت مسائل تحقیقاتی موجود ارائه شده و جهات تحقیقات آتی داده شده است.

این مقاله یک متد همراه با روش چند معیاری برای ارزیابی سطح SPD سیستم در طی فرآیندهای طراحی و اجرا ارائه میکند. سیستم های ساده و پیچیده به صورت برابر ارزیابی می شوند که به نوع خود یک مزیت است. قابلیت کاربرد متد ارائه شده با ارزیابی یک مورد کاربردی از خودرو هوشمند ارائه شده است، همچنین مروری بر تلاشهای تحقیقاتی اخیر EU در سیستم های تعبیه شده را ارائه می کند که مسائل مهم امنیتی و روشهای مربوطه را پیشنهاد کرده اند .

کلمات کلیدی: سیستم های تعبیه شده، ابزارهای تعبیه شده، جیلبریک، ، امنیت، حریم خصوصی

مقدمه

جامعه ما از شبکه ای از سیستم های تعبیه شده (ES) ساخته شده است. سیستم های تعبیه شده یکی از عناصر کلیدی اینترنت اشیا را تشکیل می دهند ، پیشرفت تکنولوژی تاثیرات زیادی نظیر افزایش قدرت و عملکرد سیستم های تعبیه شده را به همراه داشته است. با این حال ماهیت محدودیت منابع آنها و توسعه آنها در شبکه های ناهمگن و پویایی که معمولا تحت حملات مختلف فیزیکی هستند، موجب تشدید مسائل امنیت، حریم خصوصی و قابلیت اتکا در آنها می شود. محدودیت منابع چنین دستگاه هایی ، رسیدگی به مسائل امنیتی را کاری چالش برانگیز می کند چراکه در بسیاری از موارد، به کارگیری متدهای معمولی که به خوبی بکاررفته باشد امکان پذیر نیست، همراه با ارزیابی کارآیی، مصرف انرژی و سایز، سیستم های تعبیه شده از محیط های ایزوله به حوزه های به هم پیوسته وارد شده اند. امنیت ، حریم خصوصی و قابلیت اتکا (SPD) به جای اینکه ویژگی های ذاتی سیستم باشند به عنوان فاکتورهای اضافه ای به کار رفته اند. نتیجه حملات مخرب و موفق ، می تواند خطرات اقتصادی و فیزیکی داشته باشد و امن نگه داشتن آنها و آگاه بودن از حریم خصوصی و قابلیت اتکا مورد نیاز در این شرایط اهمیت دارد ، ،جزییات پروژه های مبتنی بر EU به امنیت سیستم های تعبیه شده ای برمیگردد که برای این مقاله انتخاب شده است ، هدف این مقاله ارائه دیدی از پروژه های حاضر برای تشخیص تمایلات ، تکنولوژی های برتر کنونی توسعه داده شده، فرصت های ترکیب یا توسعه کارهای موجود و در کل مسائل بازی است که باید در آینده بررسی شوند.

مروری بر تلاش های تحقیقاتی پروژه های اخیر EU در ارتباط با امنیت سیستم تعبیه شده بدنبال یک روش لایه ایی

انطباق سیستم های تعبیه شده در سناریوهای کاربردی مختلف ، رویارویی با مسائل امنیتی را صرف نظر از لایه هایی که احتمالا وجود دارد ، اجتناب ناپذیر کرده ، پروژه های تحقیقاتی Nshield (۲) یک پروژه تحقیقاتی مبتنی بر EU است که روی امنیت سیستم های تعبیه شده تمرکز دارد.

باید متذکر شد که کاربردها بر مبنای چگونگی تشخیص از حوزه های کاربردی تکنولوژی ها ارائه شده که در پروژه ها و مقالات تحقیقی وجود دارد بسیاری از تکنولوژی ها ، بدون تغییر، به حوزه های دیگری نیز مربوط اند، از نظر لایه هایی که برای طبقه بندی پروژه های گذشته انجام شده است سطح پایین ترین آنها گره است که تکنولوژی های میان افزاری و سخت افزاری را دربر میگیرد. لایه شبکه دربردارنده پروتکل های مختلف، طرح های احرازهویت و دیگر مکانیزم های مربوط به امنیت است. در نهایت طبقه بندی رسمی و معماری چارچوب های مختلف و روشهای جامع دیگر در امنیت سیستم های تعبیه شده باید راه حل هایی که اعتبار رسمی دارند را در نظر بگیرند. [1]

۱.کنیک های مربوط به گره های سیستم تعبیه شده

ماهیت ناهمگن این حوزه روشن است. از نظر سخت افزارهای به کاررفته، پلتفرم های مختلفی وجود دارد که توانایی های مختلفی دارند مثل پلتفرمهای TelosB کم توان، IRIS و MICAz از تکنولوژی Crossbow ، Verdex Pro XL6P COM قدرتمند تر از Gumstix و برد FOX LX از سیستم های Acme. در برخی موارد، دستگاه های قوی تری نظیر Freescale i.MX51 و Xilinx Spartan-6از خانواده آرایه گیت قابل برنامه نویسی استفاده شده است. دومی همراه با پلتفرمهای مبتنی بر x86 کم توان ، در توسعه کاربرد آن در آینده استفاده می شود. راه حل های امنیتی به کار رفته اختلافات مشابهی دارند و محیط های عملیاتی مختلف، پروتکل های مختلف و روشهای رمزنگاری متفاوتی دارند، ، گاهی در محیط های خطرناک ، نمی توان از امنیت فیزیکی چشم پوشی کرد. دسترسی فیزیکی به ابزارها موجب احتمال حملات مختلفی نظیر تحلیل توان متغیر یا ساده و حملات خطای دیفرانسیلی شده می تواند موجب افشای اطلاعات امنیتی شود (الگوریتم رمزنگاری به کاررفته ، طول کلید وغیره).

1_1ماژولهای امنیتی مربوط به سخت افزار

1.1.1.ماژول های مقاوم دربرابر مداخله

حوزه مهمی از تحقیقات امنیتی مربوط به شبکه های حسگر بیسیم (WSN) است که هدف آن استفاده از سخت افزار ماژول پلتفرم مورد اعتماد (TPM) و انطباق آن با نیازهای خاص کاربردهایی با منابع محدود است. این مربوط به پیاده سازی طرح گواهی ناشناسی مستقیم (DAA) توسط گروه محاسبات مورد اعتماد می باشد. در یک گزارش جزیی از پیاده سازی عملکرد ذکرشده است و پیشنهاداتی برای پیاده سازی ارائه شده است. نتایج آزمایشات نشان می دهد که بخش تشخیص خودسری پروتکل DDA می تواند بسیار زمان بر باشد و سربار آن در مواردی که محدودیت منابع است زیاد می باشد و با افزایش لیست سیاه TMP های خودسر به صورت خطی زیاد می شود. اولی مبتنی بر پیاده سازی سخت افزاری اجرای MTM روی پردازنده فیزیکی مشابهی به عنوان برنامه کاربردی است و دومی مبتنی بر کارت جاواست که موجب میشود MTM که موجب فعالیت MTM در محیط اجرای جاوا می شود که هر کدام مکانیزمهای ایزولاسیون خاص خود را بین MTM و کاربران آن دارد.

2.1.1.شتاب سخت افزاری

روش دیگر برای ایجاد امنیت گره شبکه حسگر بیسیم ، بر مبنای استفاده از دستگاه های منطقی قابل برنامه نویسی و پیچیده (CPLD) کم انرژی و کم هزینه است که دستگاه های منطقی قابل برنامه نویسی هستند که پیچیدگی آنها چیزی بین آرایه منطقی قابل برنامه نویسی و آرایه گیت قابل برنامه نویسی فیلد است که ویژگی های مربوط به معماری را با هر دو به اشتراک میگذارد. همانطور که ازمایشات دنیای واقعی نشان می دهد این پلتفرم مجهز به CPLD می تواند کارآیی گره استاندارد شبکه حسگر بیسیم را در حین اجرای الگوریتم های خاصی از ۱۲۲۰ به ۳۰۰۰ برساند و مصرف انرژی را به میزان بیش از ۹۸٪ کم کند. این مفهوم در توسعه داده شده که پروتکل های امنیتی و شبکه بندی مختلفی روی پلتفرم بیان شده با طرح های موجود مقایسه شده اند.

3.1.1.توابعی که از نظر فیزیکی قابل کپی کردن نیستند

استفاده از توابعی که از نظر فیزیکی قابل کپی کردن نیستند (PUF) متدی برای حفاظت از سیستم ها در مقابل حملات به کلیدشان است این توابع، رمزها را از ویژگی های کلیدی مدارهای یکپارچه (IC) استخراج میکنند که می توان در بین سایرین از آنها برای ذخیره امن کلید استفاده کرد. در لایه های امنیتی اضافی ، PUF هایی که از نظر منطقی قابل پیکربندی مجدد اند ، توانایی تغییر رفتار پاسخ خود یا چالش ها را به صورتی تصادفی دارند. بنابراین مهاجم با رفتارهای متغیری مواجه می شود.

4.1.1.رمزنگاری کم هزینه

مروری بر مقالاتی که به دو دسته اصول رمزنگاری مختلف با توجه به سربار انرژی و زمانی در شبکه های حسگر بیسیم پرداخته اند ارائه شده است. تعدادی الگوریتم کلید عمومی و متقارن، توابع هش و اصول رمزنگاری ، و نیز همتایان آنها ارائه شده است. یک طرح امنیتی جالب برای شبکه حسگر بیسیم طرحی است که امنیت شفافی را فراهم میکند وپیشنهاد شده است. این طرح یک رمزنگار مد CBC-X کم هزینه است که قادر به رمزنگاری یا رمزگشایی و احرازهویت است که یک عملیات یک مرحله ایست. در نتیجه در مقایسه با TinySec ، ۵۰-۶۰ ٪ صرفه انرژی دارد.

۲.تکنولوژی های شبکه

ماهیت توزیع شده و ناهمگن سیستم های تعبیه شده و محدودیت منابع ، موجب محدودیت هایی در لایه شبکه نیز شده است. کاربردهای خاصی از سیستم های تعبیه شده نیاز به یکپارچه شدن خدمات ارائه شده دارد. اگر از سرویس های وب استفاده شود، باید از معتبر بودن هر گره شرکت کننده اطمینان حاصل شود بنابراین اطمینان از اینکه سیستم در معرض خطر نیست و داده های ارسالی (مثلا اندازه گیری ها) درست هستند امری مهم است.

۲.۲.تصدیق و احرازهویت گره

قابلیت همکاری با زیرساخت های موجود و اینترنت چالش مهمی است که باید در راستای رسیدن به آنچه اینترنت اشیا نامیده می شود، آنرا در نظر داشته باشیم. یک ابزار ارزشمند در این حوزه ترکیب IEEE802.15.4 با 6LoWPAN (IPv6 روی شبکه کوتاه برد

شخصی بیسیم کم توان است که چالش ها و فرصت های امنیتی جدیدی را معرفی میکند.. نویسندگان در یک مکانیزم مقایسه ای جدید برای هدرهای امنیتی 6LoWPAN همراه با مکانیزمهای رمزنگاری که معمولا با معماری امنیتی IP استفاده می شوند به کار گرفتند که اجازه به کارگیری کانالهای انتها به انتهای امن را بین میزبان های اینترنت و گره های حسگر می دهد. امنیت و محدودیت های ناشی از منابع محدود گره های حسگر در پروژه های EU به میزان وسیعی بررسی شده اند.

1.2.2. ناشناس بودن و حریم خصوصی

در کل طرح های احرازهویت ناشناس و ناشناس بودن ، حوزه های کلیدی دیگری در تحقیقات کنونی اند .زیرا حریم خصوصی در بسیاری از کاربردها (مثل اجتماعی و پزشکی) و دسترسی مخفی به منابع و خدمات ، تکنیک رایجی برای حفاظت از حریم خصوصی کاربر است. یک جنبه جالب دیگر از این کار تفاوتهای بین سازندگان مختلف TPM (مثلا Infineon، Atmel، Winbond، Intel، ST Micro) و شبیه ساز TPM و مشخصات اصلی است. ارتباط بی سیم در شبکه های ادهاک بین خودرویی (VANET) به طور معمول با گواهینامه های دیجیتال پشتیبانی می شود، از این رو گواهینامه‌های مستعار کوتاه مدت اعمال می شوند و به منظور محافظت از حریم خصوصی رانندگان به طور منظم تغییر می کنند. نویسندگان یک معماری PKI توزیع شده برای شبکه های بین خودرویی معرفی و اجرا کرده اند، که از گواهی نامه‌های مستعار برای حفظ حریم خصوصی در کاربردهای بین خودرویی مطابق با استانداردهای مربوطه استفاده می کند. [2]

3.2.مسیریابی امن

پروتکل های مسیریابی امن، بخش دیگری از پژوهش‌های فن آوری های شبکه‌ای را تشکیل می دهند ، یک مرور کلی از مسائل امنیتی و روند فعلی در مسیریابی قابل اعتماد برای شبکه های ad hoc (ادهاک) ارائه شده است، که کاربرد آنها در شبکه های حسگر بیسیم را ارزیابی می کند. پروتکل های مسیریابی پیشرفته معتبر و همچنین چارچوب‌های مسیریابی مورد اعتماد مختلفی ، با تمرکز بر کاربرد آنها در محیط های با منابع محدود، مورد بررسی قرار گرفته اند. یک پروتکل امن مسیریابی مناسب برای این چنین محیط‌ها، به نام سنسور اعتماد محیط مسیریابی (ATSR)، ارائه شده است و عملکرد و اثربخشی آن ارزیابی شده است.

4.2. تشخیص نفوذ و گره مخرب

IDS همچنین ابزاری کلیدی در حفظ شبکه‌ی ES توزیع شده است. یک طرح IDS پویا و توزیع شده، ارائه شده و پیشتر بحث شده، که در آن گره‌ها به عنوان ناظران محلی همسایگان خود عمل می کنند، و با ترکیب اطلاعات دریافت شده از دیگر ناظران، قادر به تشخیص سازمان های مخرب هستند.. تکنیک های دفاعی برای شبکه های حسگر مبتنی بر مکان گره ها بررسی شده، با فرض اینکه هر گره قادر به تشخیص محل خود باشد. به منظور تسهیل در تجزیه و تحلیل و درک درستی از داده های IDS، روش های مختلف پیشرفته‌ای در اتحادیه اروپا، از جمله روش های مبتنی بر شبکه های عصبی برای تجسم داده ها بررسی شده است، آگاهی از وسایل نقلیه نزدیک و موقعیت خود، پایه اساسی برنامه‌های کاربردی ایمنی الکترونیکی در VANET است. محققان تلاش می کنند به این چالش ها با ارائه یک راه حل همیارانه کاملا توزیعی رسیدگی کنند، یعنی یک پروتکل سبک وزن که تنها به تبادل اطلاعات در میان نهادهای همسایه است، و امکان شناسایی موثر گره‌ها مخرب را فراهم می کند.

۳. فناوری میان‌افزار و جایگذاشت

در جابجایی به لایه های بالاتر، یعنی میان‌افزار و جایگذاشت ، محققان با چالش های دیگر با افزایش پیچیدگی سیستم، درگیر می شوند. از سوی دیگر، عامل‌هایی از یک سطح بالاتر، استفاده از ویژگی های پیشرفته تر مانند مدیریت امن و کارآمد منابع (با جمع آوری اطلاعات از لایه های پایین تر) و مکانیزم تسهیل در ایجاد قابلیت همکاری و مدیریت شبکه ES ناهمگن، را میسر می کند.

۳.۱. میان‌افزار مورد اعتماد

نرم افزار مورد اعتماد یکی دیگر از موضوعات مهم پژوهشی لایه‌ی میان‌افزارها است و ریتر و همکارانیک نرم افزار پشته مورد اعتماد (که به عنوان یک رابط بین برنامه های کاربردی و TPM عمل می کند) پیشنهاد داده‌اند تا با چارچوب امنیتی موجود یکپارچه شود، و انطباق با فن آوری محاسباتی قابل اعتماد را آسان کند. نمونه اولیه توسعه یافته است و با استفاده از محیط برنامه نویسی دات نت (.NET) ارائه شده است، که از قابلیت تشخیص خطا محیطی (به عنوان مثال در مورد سرریز بافر) بهره می برد

۳.۲. میان‌افزار سرویس‌گرا

ویژگی های اصلی یک میان‌افزار سرویس‌گرای امن برای سیستم های تعبیه شده‌ی هم‌رتبه، به منظور رویارویی با چالش های امنیتی مختلف از IoT، ارائه شده است. در اینجا مفهوم کلی گروهها استفاده شده است، یعنی همتایان خدماتی در داخل گروه ها ارائه می دهند و کشف این خدمات نیز در گروه انجام می شود. خدمات می توانند بدون شرایط و یا با شرایط کامل باشند، و ممکن است بدون نشست و یا با نشست کامل باشند. مدل سرویس ارائه شده میان‌افزار مبتنی بر مولفه، اصول لازم مانند امنیت، عدم تجانس، قابلیت همکاری و مقیاس پذیری را فراهم می کند. مدل با دو کاربرد بسیار مختلف، از جمله کاربرد WSN برای نظارت بر تشعشعات در نیروگاه های هسته‌ای و برای مراقبت های بهداشتی در یک محیط تلفن همراه، تایید شده است.استقرار و ساماندهی خدمات وب در سیستم های تعبیه‌شده ناهمگن دیگر حوزه پژوهشی و کاری در حال ظهور است که معمولا به لایه میان‌افزار اختصاص داده می شود، و از استانداردسازی مشخصات دستگاه برای خدمات وب سایت (DPWS)، چارچوب باز و تحقیقات انجام شده در پروژه SIRENA، و SOCRADES، استفاده می کند.

۳.۳. میان‌افزار آگاه از متن

مرور وسیعتری از میان‌افزار آگاه ازمتن ارائه شده، که خواص و استفاده از آنها را طبقه بندی می کند. یک رویکرد مبتنی بر هستی شناسی دنبال شده است، که از زبان هستی شناسی وب و زبان قانون وب به منظور توسعه قوانین نظارت و تشخیص استفاده می کند. در این روش، هر اختلال در عملکرد می تواند شناسایی شود و روش خوددرمان در یک راه موثر، توسعه‌پذیر و مقیاس پذیر احضار شود، که نتایج تجربی آن را به اثبات رسانده است.

۳.۴. میان‌افزار منعطف و مقاوم در برابر خطا

جنبه قابلیت شکل پذیری مجدد (انعطاف) و پیامدهای آن بر امنیت از دیدگاه سطح بالاتردر نظر گرفته شده است. یک معماری امنیتی ارائه شده است که بر اساس یک لایه میان‌افزار است، و پیکر بندی دوباره و ارتباطات امن را با اجرای سیاست خاص نرم افزاری تنفیذ، گرفتن احراز هویت از یک منبع راه دور (به عنوان مثال چارچوب ALoader) و همچنین خدمات کلید زنی دوباره برای توزیع و ابطال کلیدی (یعنی چارچوب کلیدزنی دوباره)، ارائه می دهد . طرح ارائه شده در یک میان‌افزار قابلیت تنظیم و سازگار است که با هدف کاهش پیچیدگی تحقق یک سطح امنیتی مناسب برای یک برنامه WSN داده شده است.

۴. معماری‌ها و فرمالیسم

سیستم های جاسازی شده معمولا بلوک های ساختمانی از یک سیستم بزرگتر و پیچیده تر هستند، که برای یک هدف مشخص ایجاد شده اند. یک طراحی دقیق از این معماری‌ها، و همچنین خدمات ارائه شده آنها، قطعا اثر مثبتی بر هر گونه مسائل مربوط به امنیت، با به حداقل رساندن نقص‌های پیش بینی نشده و کمبودها، خواهد داشت. فرمال‌سازی فرآیند طراحی و معماری سیستم های جاسازی شده، در اکثر موارد، منجر به یکپارچه سازی آسان تر سیستم نهایی می شود، در حالی که سطح بالایی از امنیت و قابلیت اعتماد را حفظ می کند. برخی از روش ها در پژوهش حاضر بر ارائه چارچوب کاملا برجسته و یا فرمال‌سازی فرآیند طراحی و توسعه سیستم های امنیتی و قابل اعتماد تمرکز دارد، بخصوص در کاربردهایی که در آن ایمنی بسیار مهم است. طرح پیشنهادی برمبنای یک شرط تقاضای خدمات در

موقعیت های بحرانی استوار است، که در آن بازیگران مختلف می تواند نقش داشته باشند، همچنین حاوی دستگاه های مشتری ناهمگن است. این مدل شامل دو بخش است: رابط کاربری سیستم امنیتی که مدل طراحی سیستم را برای برقراری ارتباطات امن و در دسترس بودن منابع خلاصه می کند؛ و بلوک ساختمانی که اجرای یک مکانیزم امنیتی را خلاصه می کند.[3]

۵. معیارهای امنیتی

تحقیقات قبلی درباره معیارهای امنیتی عمدتا روی امنیت نرم افزار تمرکز دارند. معیارهای امنیت سطح سیستم به سازمانها و وبسایت هایی برمیگردد که آسیب پذیری های سیستم های مخلتف کشف شده را منتشر میکند. برخی از این سازمانها و وبسایت ها US-CERT ، NIST ، MITRE و تمرکز امنیتی هستند. یک مدل ریاضیاتی برای اندازه گیری فرکانسی که در آن آسیب پذیری هایی وجود در US-CERT وجود دارد ارائه شده است بعلاوه شاخص آسیب پذیری سیستم را با استفاده از ویژگی های سیستم، فاکتورهای بالقوه ای که از آنها چشم پوشی شده ، برای استفاده از آن بعنوان معیار آسیب پذیری سیستم کامپیوتری محاسبه شده است.

6. مورد خودروی هوشمند

دراین بخش مورد خودروی هوشمند به کاررفته در مقاله را شرح داده میشود تا قابلیت اتکای متد ارائه شده را نشان دهد.. هدف اصلی، تحلیل بهترین پیکربندی برای SPD_{Goal} پیشنهادی هر سناریو و ارزیابی سطح SPD است که در آن سطح ، سیستم اجرا خواهد شد.

1.6.توضیح سیستم

در این مورد به جنبه حریم خصوصی راندن موتورسیکلت (MB) پرداخته می شود. یک راننده جوان مجاز به استفاده از MC را در صورت نداشتن سرعت زیاد دارد (سرعت زیر ۸۰ کیلومتر در ساعت). والدینش به او میگویند که حریم خصوصی او در محدوده سرعت مجاز رعایت می شود (سناریو ۱)، اما به او نمی گویند که اگر از این سرعت تجاوز کند چه می شود (سناریو۲) ،والدین یک پیام کوتاه درباره سرعت و مکان موتور دریافت میکنند. والدین یک پیام کوتاه درباره سرعت و مکان موتور دریافت میکنند. ما یک سناریوی اورژانسی نیز در صورت تصادف در نظر میگیریم (سناریو ۳) که هشدار پیام کوتاه هم به والدین هم به اورژانس ارسال میشود و اطلاعات مربوط به موتورسیکلت در یک سیستم درونی حفظ می شود. خودروی هوشمند که توضیحاتی در موردش داده شد از سه زیرسیستم مختلف تشکیل شده تا نیازهای مورد کاربردی را فراهم کنند.

_ یک سیستم درونی (BE) که واسط موتور سیکلت را برای کاربر نهایی می سازد .
_ یک سیستم تعبیه شده ، که روی خودرو برای نظارت بر شرایط موتورسیکلت نصب می شود.
_ ارتباط سیستم تعبیه شده با سیستم درونی که یک لینک متحرک بین آنهاست.

1.1.6.زیرسیستم ارتباطی سیستم تعبیه شده با سیستم درونی

این زیرسیستم به وسیله سیستم درونی به سیستم تعبیه شده متصل می شود. ارتباطات هم از طریق GPRS هم SMS برای مطلع کردن والدین و اورژانس برقرار می شود،ممکن است کل سیستم در ۹ پیکربندی اجرا شود (A تا I) که میزان حفاظت از حریم خصوصی را بررسی میکند .

- Conf. A : سیستم تعبیه شده هیچ پیامکی نمی فرستد، داده های GPRS با کلید ۱۲۸ بیتی رمز می شود. سیستم تعبیه شده پیکربندی دور را از سیستم درونی قبول میکند.
- Conf. B: مثال بالا، به جز سیستم های تعبیه شده ای که هر ۱۲۰ ثانیه یک پیام برای روشن ماندن می فرستد .
- Conf. C: مثل بالا، به جز BE که پیامی را به ES مفرستند و آخرین مورد هر ۶۰ ثانیه جواب می دهد.

- Conf. D: سیستم تعبیه شده یک پیامک به والدین می فرستد ، داده های GPRS برای BE با کلید ۶۴ بیتی رمز می شوند. سیستم تعبیه شده پیکربندی دور را از BE قبول میکند.
- Conf. E: مثل بالا ، به جز اینکه سیستم تعبیه شده اطلاعات مکان و سرعت را هر ۱۰ ثانیه به BE می فرستد
- Conf. F: همانند فوق به جزاینکه BE پیامی را به سیستم تعبیه شده می فرستد و آخری هر ۵ ثانیه با اطلاعات مکان و سرعت پاسخ می دهد.
- Conf. G: سیستم تعبیه شده پیامکی به والدین و یک پیام دیگر به خدمات اورژانس می فرستد. داده های رمزنشده درباره وضعیت موتور سیکلت از سیستم تعبیه شده به BE ارسال می شود. سیستم تعبیه شده پیکربندی دور را از BE قبول میکند.
- Conf. H: همانند بالا اما سیستم تعبیه شده اطلاعات مکان و سرعت را هر ۲ ثانیه به BE می فرستد.
- Conf. I: همانند فوق اما BE پیامی را به سیستم تعبیه شده می فرستد و آخری هر ۰,۵ ثانیه با اطلاعات مکان و سرعت پاسخ می دهد.

2.1.6.تعریف معیار و انتخاب

سطح SPD عناصر که یک سیستم تعبیه شده را تشکیل می دهند می توانند با چندین معیار اندازه گیری شوند. تعریف و انتخاب معیارهای لازم نیاز به متخصصانی در این فیلد دارد و باید با مهندسی سیستم انجام شود. یکی از ایده های ورای این کار ایجاد و حفاظت از پایگاه داده های معیارهای رایج است. مزیت اصلی آن استفاده مجدد از معیارهای به کار رفته برای اندازه گیری سطح SPD عناصر مرتبط یا مشابه یا استفاده از مقادیر SPD موجود برای زیرسیستم ها یا اجازیی با پیکربندی داده شده است.

3.1.6. تعریف معیار

متد تعریف معیار پیشنهادی از چهار فاز تشکیل شده است: تشخیص پارامتر، وزندهی پارامتر، یکپارچه کردن معیار با اجزا و اجرای معیار. سیستم خودروی هوشمند با پنج پارامتر در چهار فاز ارزیابی می شود. فاز تشخیص پارامتر شامل تحلیل اجزاییست که توسط خود معیار بررسی خواهند شد، در گام بعدی وزن دهی پارامتر، عکس العمل مقادیر ممکن هر پارامتر از اجزای سطح SPD را ارزیابی میکند ،در فاز بعدی، یکپارچگی معیار با اجزا شامل تشخیص مقادیر ممکنی است که پارامتر باید بر مبنای همه پیکربندی هایی که در آن سیستم اجرا می شوند داشته باشد، بعد از همه پارامترها، وزن مقادیر آن عنصر و ارزش پیکربندی احتمالی تشخیص داده می شود و گام نهایی، اجرای معیار است.

4.1.6. معیارهای مورد کاربردی

در این مقاله از یک روش چندمعیاره در سیستم های تعبیه شده و زیرسیستم ارتباطات سیستم درونی استفاده شده است.پنج معیار زیر برای اندازه گیری سطح اهمیت هر چهار جز تشکیل دهنده زیرسیستم تعریف شده :

_ معیارهای مربوط به پورت
_ معیار کانال ارتباطی
_ معیار نرخ پیام GPRS

1.4.1.6.معیار پورت ها

معیار پورت، تاثیر عنصر پورت را در زیرسیستم ارتباطی ES-BE می سنجد، همه مقادیر ارائه شده فقط به ارزیابی حریم خصوصی مربوط هستند.

1_تشخیص پارامتر : تحلیل اجزای پورت و زیرسیستم ارتباطی ES-BE با تشخیص چهار پروتکل یا کلاس پورت شامل SSH، SNMP، دام SNMP و SMS پایان می یابد

2_وزن دهی پارامتر: فرمولبندی وزن توسط متخصص این فیلد ،را ارائه میکند

3_یکپارچه کردن معیارعنصر: تشخیص همه مقادیر ممکن پورت برای پیکربندی داده شده سیستم ، گزینه های متعددی فراهم میکند.

4_اجرای معیار.

2.4.1.6. معیار کانال ارتباطی

معیار کانال ارتباطی، سطح SPD ارائه شده توسط دوکانال ممکن را که توسط زیرسیستم ارتباطی ES-BS ارائه شده است را اندازه میگیرد: ارسال داده GPRS و پیام کوتاه.

3.4.1.6.معیار نرخ پیام GPRS

معیار نرخ پیام GPRS ، مدت زمانی را که در آن داده ها از طریق کانال GPRS منتقل می شوند ارزیابی میکند. این معیار میزان اطلاعاتی را که در شرایطی که کانال در معرض خطر قرار گرفته ، با مشکل مواجه می شوند را ارزیابی میکند.

۷. پیدایش اصطلاح جیلبریک کردن

واژه جدید جیلبریک ، واژه ایست که معمولا برای توضیح فرآیند دور زدن امنیت با هدف حذف یا عبور از محدودیت امنیتی یک وسیله به کار می رود. این واژه در دستگاه های اپل بعد از اولین انتشار آیفون به وجود آمد. مفهوم روت کردن هم مشابه جیلبرینگ کردن است ، با این حال ارتباط بیشتری به دستگاه های اندرویدی دارد . رایج تر است استفاده جدید واژه جیلبریک کردن به انتشار اولین آیفون در سال ۲۰۰۷ بر میگردد. تیم توسعه آیفون ، اولین جیلبریک را توسعه داده اند (تیم آیفون ۲۰۰۷)، این واژه مفهومی شبیه خارج شدن از ویژگی های سیستم عامل یونیکس دارد که با عنوان chroot jail شناخته می شود (BSD آزاد) که دسترسی آن به دایرکتوری ریشه و فرزندان محدود است.

1.7.تغییرات سخت افزاری

روش دیگر برای دسترسی به سیستم های تعبیه شده استفاده از تراشه های مد است. در یک وسیله سخت افزاری فیزیکی، از تراشه های مد در زمان نصب تراشه یک وسیله که معمولا کنسول بازی است به منظور دورزدن امنیتی استفاده می کند. معمولا مدچیپ به برد اصلی لحیم می شود و محدودیت های امنیتی خاصی را فراهم میکند.

2.7چرا مدچیپ

رایج ترین کاربرد مدچیپ در دور زدن DRM است تا اجازه دهد که بازی های وارد شده یا کپی شده روی سیستم اجرا شوند، با این حال مواردی هست که تراشه های مد نیاز به عملکرد بیشتری دارند که معمولا وقتی اتفاق می افتد که مجوز ها ، قانونی بودن نرم افزار را برای استفاده در یک سیستم تعبیه شده قبول نمی کنند. مثلا XBMC Foundation با نام XBMC منتشر شد که در اصل برای ایکس باکس مایکروسافت بود (XBMC، ۲۰۱۳) . مرکز اطلاعات ایکس باکس در سال ۲۰۰۳ برای کنسول بازی ایکس باکس مایکروسافت ایجاد شد و تا امروز در تعدادی از ابزارهای تحت پشتیبانی باقی مانده است و به کاربران امکان تجربه تعاملی و قوی را می دهد که در آن زمان در دستگاه ها وجود نداشت.

3.7.جیلبریک کردن یا تغییر در تحلیل قانونی ابزارهای تعبیه شده

کامل ترین تحلیل را می توان بعد از مالکیت یک دستگاه خام بدست آورد، یک ارزیابی مبتنی بر هدف شامل موارد زیر است:

1)تشابه نشانه های دیجیتالی مربوطه ای که به یک شخص مربوط است ارائه شده

2)عمومیت متدها و تکنیک ها

3)در دسترس بودن کمک بخش صنعت
4)احتمال توسعه متدها و تکنیک ها بدون دانش تخصصی یا تجهیزات

4.7.چالش های جیلبریک کردن و تغییر ابزارها

با توجه به نوع تغییرات مورد نیاز ، سه مسئله مهم مطرح است:

_ چالشهای تکنیکی: دنبال کردن متدهای پیچیده برای نصب تغییرات سخت افزاری یا نرم افزاری
_ مسائل حقوقی و قانونی در روت کردن یا جیلبریک کردن: چالشهای تغییرات نرم افزاری و
_ مسائل قانونی تراشه های مد : چالشهای تغییر سخت افزار

۸.نتایج وارزیابی

در این مقاله در ابتدا به بررسی و مطالعه روی طرح های پژوهشی اتحادیه اروپا که مربوط به امنیت سیستم های تعبیه شده میباشد پرداخته شده است که یک موضوع بسیار فعال با بسیاری از پروژه های تکمیل شده و در حال انجام است که بودجه قابل توجهی را دریافت کرده است. از این بررسی الگوهای خاصی در مورد مسائل مورد بررسی به منظور رسیدگی به مسائل ذکر شده بما میدهد وبا تکامل به حوزه کاربردی سیستم های امنیتی تعبیه شده، مدیریت اطلاعات خصوصی حساس و الزامات آنها بر این اساس تغییر می کند. موضوعات مختلف در مورد باز بودن امنیت در تمام حوزه‌های کاربردی مذکور وجود دارد. مسائلی که تحقیقات آینده باید با آن مقابله کند، همانطور که میدانیم سیستم های تعبیه شده که ابزارهای جدا از هم تا ابزارهایی که شدیدا به هم وابسته اند را دربرمیگیرد و عنصر کلیدی اینترنت اشیاست در بخش بعدی بررسی امنیت ، حریم خصوصی و قابلیت اتکا (SPD) در نظر گرفته شده که فاز طراحی آن مورد توجه کافی نبوده است اما بعنوان یک افزونه به کار رفته اند، بعلاوه با هر جنبه از SPD به تنهایی و بدون جستجوی یک راه حل متعادل برخورد شده است، برای بررسی این مشکل، متد چندمعیاری که همه جنبه های SPD را در برمیگیرد در هر دو فاز طراحی و اجرا ارائه شده است. مزیت اصلی آن سادگی اش است ، چندمعیاری فرآیند کلیدی است که همراه با سایر گام ها به کار رفته و مقیاس پذیری آن با شروع ارزیابی زیرسیستم ها شروع شده و با ارزیابی کلی سیستم خاتمه می یابد. نتیجه بدست آمده یک سطح کلی از SPDSystem است که به ما کمک میکند که بفهمیم کدام پیکر بندی مطابق با SPDGoal پیش بینی شده کار میکند. مورد کاربردی نشان دهنده سادگی این روش است چراکه یک فرآیند چند معیاری ساده در طی ارزیابی کلی سیستم استفاده می شود. مقیاس پذیری نشان داده شده چراکه سیستمهای ساده و پیچیده به صورت برابر ارزیابی می شوند و هر جز ، هر زیرسیستم و سیستم بدست آمده را می توان با سه تایی (s,p,d) طبقه بندی کرد.

و در بخش آخر مقاله در مورد ابزارهای تعبیه شده که ارتباط نزدیکی با سخت افزار و نرم افزار دارد و همچنین پتانسیل ایجاد چالش قانونی را دارد مورد بررسی قرار گرفت ، به نظر می رسد که قوانین کامپیوتری که مدتها جدا از امنیت کامپیوتر بررسی می شدند امروزه وارد دنیای هکرها شده اند و نیاز به دورزدن مکانیزمهای امنیتی هست نه کپی کردن ، بلکه بدست آوردن اسناد موجود در رسانه ذخیره سازی سیستم تعبیه شده می باشد. این بیشتر کارهکرهای کلاه سیاه است تا کلاه سفید. این فعالیت باید برای توسعه جستجوی اطلاعات موجود و صحت شواهد بدست آمده از آن وسیله توسعه داده شود. شاید باید یک شخص ثالث هم باشد که شخص علاقه مند به بازیابی شواهد بعنوان یک هکر کلاه طلایی یا درجه کارآگاهی یاپلیسی وجودداشته باشد.

منابع

[1]Embedded Systems Security: A Survey of EU Research EffortsCharalampos Manifavas1, Konstantinos Fysarakis2, Alexandros Papanikolaou2* and Ioannis Papaefstathiou2SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks (2014) Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1151. Received 14 May 2014; Revised 15 September 2014; Accepted 26 September 2014

[2] Multi-Metrics Approach for Security, Privacy and Dependability in Embedded systems, In˜aki Garitano2

• Seraj Fayyad1,2

• Josef Noll1,2

Published online: 13 March 2015 _ Springer Science+Business Media New York 2015

[3] Locking Out the Investigator: The Need to Circumvent Security in Embedded Systems, Huw Reada, Iai Sutherlandbc, Konstantinos Xynosa & Frode Roarsonab a University of South Wales, Pontypridd, United Kingdom b Noroff University College, Kristiansand, Norway c Edith Cowan University, Perth, Australia Published online: 25 Mar 2015.