بررسی امنیت سیستم های دارای بلوتوث

Contents

۱– معرفی فناوری بلوتوث

۱–۱– مقدمه

یک استاندارد برای پیوند کوتاه برد، بهره بری انرژی کم، کم هزینه و بی‌سیم می‌باشد، که از تکنولوژی رادیویی بهره می‌برد، تکنولوژی کنونی استاندارد IEEE بنامWPAN های ۸۰۲،۱۵ می‌باشد. بلوتوث یا دندان آبی، نام بازرگانی بی‌سیمی با دوری کم برای فرستادن پیام، عکس یا هر اطلاعات دیگر است که از نام یک پادشاه منطقه اسکاندیناوی الهام گرفته شده است. فناوری بلوتوث شامل چندین نکته کلیدی، که قبول آن را به طور گسترده آسان می کند، می‌باشد. توانایی بی‌سیم و کوتاه برد آن به دستگاه‌های جانبی این اجازه را می‌دهد که توسط یک واسط هوایی ارتباط برقرار کنند، جایگزین شدن کابل‌ها که از اتصال دهنده‌ها با اشکال و سایزهای مختلف و چندین گیره، استفاده می کردند. – بلوتوث هردو نوع داده و صوت را پشتیبانی می کند که آن را به یک تکنولوژی ایده‌آل تبدیل نموده‌است که بسیاری از وسایل را قادر به ارتباط کرده‌است. – بلوتوث از فرکانس غیر منظم استفاده می کند و در هرجای دنیا قابل دسترس است.

بلوتوث یک رشته خصوصیت بی‌سیم است که ارتباطات کوتاه‌برد بین وسایل مجهز به تراشه‌های کوچک و اختصاصی بلوتوث را تعریف می کند. بلوتوث یک استاندارد رادیویی و پروتکل ارتباطی برای مصارف با توان پایین و برد کوتاه می‌باشد که با نصب یک میکروچیپ ارزان قیمت در دستگاه‌ها فعال می‌شود. بلوتوث در حقیقت نام تجاری برای شبکه‌های بی‌سیم شخصی است که با استاندارد IEEE۸۰۲،۱۵ هم شناخته می‌شود. این بلوتوث برای فاصله‌های نزدیک و ارسال پیغام، عکس و یا هر اطلاعات دیگر استفاده می‌شود. اختراع تکنولوژی بلوتوث در سال ۱۹۹۴ تحول عظیمی در عرصه ی ارتباطات به‌ویژه موبایل‌ها به‌وجود آورد. تنها یکی از ویژگی‌های مفیدش حذف سیم‌های بسیار از سازمان‌ها، ادارات و منازل بود. مانند حذف سیم بین موس و کامپیوتر، حذف سیم بین صفحه کلید و کامپیوتر، حذف سیم بین موبایل و کامپیوتر و...

مخترع بلوتوث، یاپ هارتسن اهل هلند است. بلوتوث یا به عبارتی دندان آبی از نام پادشاه دانمارک بنام هارالد بلوتوث الهام گرفته شده‌است. این تکنولوژی یک استاندارد رادیویی و پروتکل ارتباطی برای ارتباط یا اتصال با فاصله کوتاه است.

زمانی که دو دستگاه الکترونیکی نیاز به ارتباط با یکدیگر دارند، باید دارای سیستم‌های ارتباطی مشترک به روش بلوتوث باشند؛ یعنی هر دو دستگاه باید مجهز به تراشه یا میکروچیپ بلوتوث باشند

۲-۱- تاریخچه

هارالد دندان‌آبی (بلوتاند) اول[۱] نام پادشاه دانمارک در سال‌های ۹۴۰ تا ۹۸۵ میلادی بود. وی در سال ۹۱۰ میلادی به‌دنیا آمد. مانند بسیاری دیگر از وایکینگ‌ها، دندان‌آبی نیز جنگ برای دستیابی به گنج در سرزمین‌های دیگر را باارزش می‌دانست. زمانی که خواهر بلوتاند، همسرش اریک ــ پادشاه نروژ ــ را در جنگ سختی که نروژیان درگیر آن بودند از دست داد، به دانمارک آمد و از هارالد خواست تا زمام امور در نروژ را به‌دست گیرد و آرامش و امنیت را در نروژ برقرار کند. هارالد نیز از این فرصت استفاده کرده و قلمرو حکومت خود را گسترش داد. تا قبل از این زمان، نروژ و دانمارک همیشه درحال جنگ با یکدیگر بودند و افراد زیادی در این جنگ‌ها کشته می‌شدند. در سال ۹۶۰ میلادی، هارالد که در اوج قدرت خود بود، اعلام صلح میان دو کشور نمود و با گسترش قلمرو پادشاهی خود، همزمان بر دو کشور دانمارک و نروژ فرمانروایی کرد. وی یکپارچگی بین کشورها را، که پدرش آغاز کرده‌بود، کامل نمود. هارالد بلوتاند، دانمارک و نروژ را به هم پیوند داد، همان‌گونه که امروزه «بلوتوث» دنیای کامپیوترها و ارتباطات را به هم پیوند داده‌است. به افتخار هارالد دندان‌آبی، که مردم دو کشور را با هم پیوند داده و با ایجاد ارتباط بین دو کشور، آنها را از جنگ و مصیبتی که دامن‌گیرشان بود نجات داد، نام فناوریی را که امروزه دنیای کامپیوتر و ارتباطات را به هم پیوند داده بلوتوث نهاده‌اند.

فکر اولیه بلوتوث در شرکت تلفن همراه اریکسون در سال ۱۹۹۴ شکل گرفت. اریکسون که یک شرکت سوئدیِ ارتباطات راه دور است، در آن زمان درحال ساخت یک ارتباط رادیویی کم‌مصرف، کم‌هزینه بین تلفن‌های همراه و یک گوشی بی‌سیم بود. کار مهندسی در سال ۱۹۹۵ شروع شد و فکر اولیه به فراتر از تلفن‌های همراه و گوشی‌های آن‌ها توسعه یافت تا شامل همه انواع وسایل همراه شود. در سال ۱۹۹۸ اریکسون با چند شرکت دیگر موافقت‌نامه‌ای را امضا کرد که بر اساس آن گروه SIG به وجود آمد.

این نام از نام یک پادشاه دانمارکی به نام هارالد بلوتاند (به دانمارکی: Harald Blåtand) گرفته شده‌است. کلمه بلوتاند، بعد از انتقال به زبان انگلیسی، به‌شکل «بلوتوث» تلفظ شد، که معنای «دندان‌آبی» دارد. این حکمران به‌طور صلح‌آمیز، دانمارک، سوئد جنوبی و نروژ شمالی را متحد کرد. این کار به او شهرت یک پادشاه ماهر در ارتباط و مذاکره را در تاریخ داد. شرکت اریکسون اسم بلوتوث را به این فناوری داد، چون امیدوار بود بتواند به‌طور صلح‌آمیز وسایل مختلف را متحد کند.

[۱] Harald I Blåtand

۳-۱- نحوه برقراری ارتباط

ارتباط با فرکانس‌های رادیویی انجام می‌شود، هر وسیله بلوتوث حاوی یک تراشه فرستنده/گیرنده مربعی‌شکل به ضلع ۴ سانتیمتر است، که در باند فرکانسی ۲،۴GHz تا ۲،۴۸GHz کار می‌کند. این فرکانس از این لحاظ انتخاب شده، که در سراسر جهان به طور رایگان در دسترس است و محدودیت‌های داشتن مجوز را ندارد. این باند فرکانس طبق یک توافق نامه بین‌المللی برای استفاده توسط لوازم علمی، پزشکی و صنعتی کنار گذاشته شده و اصطلاحاً به آن ISM می‌گویند؛ باند ISM به ۷۹ کانال تقسیم می‌شود که هرکدام پهنای باند ۱MHzای دارند. بلوتوث ازلحاظ نظری پهنای باند یک مگابایت در ثانیه را دارد، که سرعتی نزدیک به ۷۲۳ کیلوبیت در ثانیه است. این سرعت خیلی بالا نیست، اما برای انتقال داده‌ها بین وسایل دستی و دسترسی به اینترنت کاملاً کافی است.

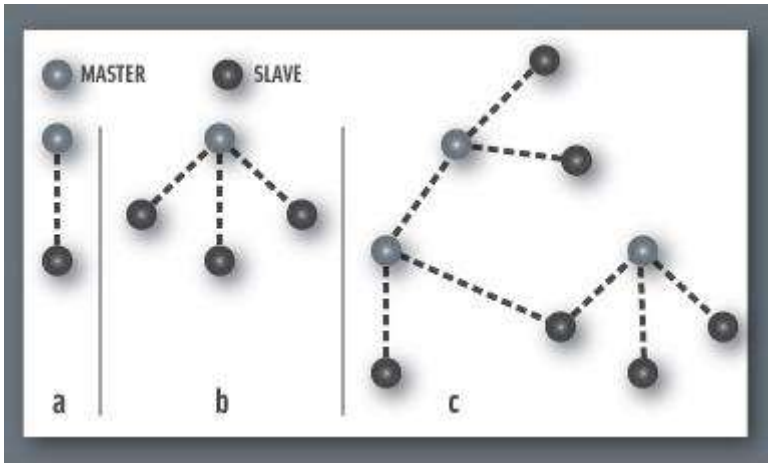
۴-۱- ایجاد شبکه با بلوتوث[۲]

تکنولوژی بلوتوث به گونه ای طراحی شده است که در محیط های چند کاربره به راحتی می تواند کار کند. پس یکی از بزرگترین مزایای این تکنولوژی، آن است که به کمک آن می توان تجهیزات دارای بلوتوث را در یک شبکه قرار داد. ارتباطی که بلوتوث برقرار می کند یا از نوع Point to Point است و یا از نوع ارتباط Point to Multipoint می باشد.شبکه هایی که به این صورت ایجاد می شوند، در دو گروه قرار می گیرند:

۱. Piconet این شبکه حداکثر حاوی هشت دستگاه می باشد که حداقل باید یکی از آنها Master و حداکثر هفت تای دیگر Slave باشند.
۲. Scatternet حداکثر شامل ده شبکه از نوع Piconet می باشد.

دستگاه های یک شبکه Piconet باید تحت پوشش یک فرکانس رادیویی و با یک کانال ارتباطی مشترک، ارتباط برقرار نمایند. آدرس هر دستگاه بصورت یک آدرس ۴۸ بیتی منحصر به فرد می باشد «BD-Address»که بر مبنای پروتکل IEEE 802.11 یا WLAN ایجاد شده است.

[۲] Bluetooth in The Network



- در شکل فوق قسمت a ، ساده ترین نوع شبکه Piconet که ترکیبی از یک دستگاه Master و یک دستگاه Slave می باشد، نمایش داده شده است.
- در شکل فوق قسمت b ، شبکه ای با چهار دستگاه که یکی از آنها Master و سه تای دیگر Slave بوده، نمایش داده شده است.
- در شکل فوق قسمت c ، مثالی از یک شبکه Scatternet که ترکیبی از سه شبکه Piconet می باشد، نمایش داده شده است.

در مورد برقراری ارتباط بوسیله بلوتوث با سایر تجهیزات بلوتوث دار، به دو نکته زیر توجه نمایید:

- برد تجهیزات بلوتوث از یک متر آغاز شده و تا حداکثر ۱۰۰ متر ادامه می یابد. توجه به این نکته ضروری می باشد که تکنولوژی بلوتوث جهت ارتباط در فواصل کوتاه طراحی شده است.
- ممکن است امواج تولیدی توسط دستگاه بلوتوث شما با امواج سایر دستگاه ها تداخل کند و سبب مشکل گردد. بطور مثال در هواپیما، کارکردن با تلفن همراه ممنوع می باشد. یکی از دلایل وجود این ممنوعیت آن است که امواج بلوتوث با امواج دستگاه های ناوبری هواپیما تداخل کرده و سبب بروز مشکلاتی در امر ناوبری و کنترل هواپیما خواهد شد. به همین علت تلفن همراه یا هرگونه تجهیزاتی که در آن ریز تراشه بلوتوث قرار داشته باشد، نباید در هواپیما روشن باشند.

۵-۱- تداخل امواج

یکی از راه‌ها برای جلوگیری از تداخل امواج ارسال سیگنال‌های بسیار ضعیفی درحدود ۱ میلی‌وات است. استفاده از امواج کم قدرت، شعاع برد سیگنال‌های بلوتوث را به حدود ۱۰متر محدود می‌کند؛ و هم چنین استفاده از این گونه سیگنال‌های ضعیف ایجاد تداخل بین امواج بلوتوث با امواج تلفن همراه، کامپیوتر یا دستگاه تلویزیون

به‌طورکلی منتفی می‌شود. بلوتوث از یک فناوری دیگر به نام «جهش فرکانس در طیف گسترده» یا(FHSS) بهره می‌گیرد، که احتمال استفاده از فرکانس برابر توسط دو دستگاه به طور همزمان را تقریباً به صفر می‌رساند. بر پایه این تکنولوژی هر وسیله این امکان را دارد که از ۷۹ فرکانس منحصربه‌فرد که به صورت اتفاقی از میان یک سری فرکانس‌های از پیش تعیین شده انتخاب می‌شوند، استفاده کند؛ و به طور منظم تغییر فرکانس می‌دهد. درمورد بلوتوث این عمل تغییر فرکانس در دستگاه فرستنده حدود ۱۶۰۰ بار در ثانیه اتفاق می‌افتد، بر پایه همین تکنولوژی از اختلال بین امواج بلوتوث با دستگاه‌هایی مثل کنترل درب پارکینگ یا تلفن‌های بی‌سیم جلوگیری می‌شود.

۶-۱- معماری

واحد پایه در سیستم بلوتوث یک "پیکونت است که از یک گره اصلی و حداکثر هشت گره پیر و فعال به فاصله حداکثر ده متر، تشکیل شده‌است. در یک فضای بزرگ و واحد می‌توان چندین پیکونت داشت و حتی می‌توان آن‌ها را از طریق یک گره که نقش پل ایفاء می‌کند، به هم متصل کرد. به مجموعه‌ای از پیکونت‌های متصل بهم اصطلاحاً) شبکه متفرق/پراکنده) گفته می‌شود. در یک پیکونت علاوه بر هفت گره فعال پیرو، می‌تواند تا ۲۵۵ گره غیر فعال وجود داشته باشد. این‌ها دستگاه‌هایی هستند که گره اصلی آن‌ها را در حالت استراحت و کم توان وارد کرده تا مصرف باتری آن کاهش یابد. یک دستگاه در حالت غیر فعال هیچ کاری نمی‌تواند انجام دهد به جز آن که به سیگنال فعال سازی خود یا سیگنال Beacon که از گره اصلی می‌رسد، پاسخ بدهد.[۲]

هنگامی که دو دستگاه بلوتوث دار در محدوده ارتباط قرار می‌گیرند آن‌ها جهت برقراری ارتباط با یکدیگر تلاش می‌کنند. اگر در آن زمان هیچ پیکونتی موجود نباشد یک فرایند مبادله فعال می‌شود. یک دستگاه به عنوان گره اصلی در نظر گرفته می‌شود و بقیه به عنوان گره‌های پیرو انتخاب می‌شوند. گره اصلی فرکانس، ترتیب پرش‌های فرکانس، زمان‌بندی و ترتیب گره‌های پیرو را انتخاب می‌کند. گره اصلی هم چنین مسئول تعلیم دادن گره‌های پیرو برای تغییر وضعیت دادن به حالت‌های دیگر برای زمان‌های غیرفعال است.

گره اصلی و پیرو باید اطلاعات ساعت و آدرس را به منظور وارد شدن گره پیرو به پیکونت متعلق به آن گره اصلی، مبادله کنند. هر دستگاه بلوتوث یک مشخصه جهانی(Global ID) منحصربه‌فرد برای ایجاد مدل پرش (hopping pattern) دارد.

امواج رادیویی گره اصلی مشخصه جهانی و اختلاف ساعت خود را با هر گره پیرو موجود در پیکونت خود تقسیم می‌کند.

یک دستگاه بلوتوث می‌تواند دریکی از حالات زیر باشد:

۱. Standby (آماده به خدمت): هنگامی است که دستگاه روشن است ولی به پیکونت وصل نیست.
۲. Inquiry (در حال جستجو): هنگامی است که در خواست‌هایش را برای پیدا کردن دستگاهایی که می‌تواند به آنها وصل شودمی فرستد.
۳. Page (فراخوانی): مربوط به گره اصلی در پیکونت است و به معنی پیغام‌هایی است که دستگاه برای دعوت گره‌های پیرو جهت اتصال به پیکونت ارسال می‌کند.
۴. Connect (اتصال): وقتی که ارتباط موفقیت آمیز بین گره اصلی و دستگاه جدید برقرار شود. دستگاه جدید که نقش پیرو را بازی می-کند به حالت connected درآمده و یک آدرس فعال دریافت می‌کند.
۵. Transmit (ارسال): حالتی است که دستگاه در حال ارسال داده خود می‌باشد. وقتی که ارسال داده تمام شد به حالت connected در می‌آید.
۶. Sniff: حالت کم‌مصرف دستگاه است که مربوط به گره پیرو می‌باشد و به اندازه بازه زمانی از قبل تعیین شده استراحت می‌کند[۳].دستگاه در زمان مشخص شده برای انتقال اطلاعات بیدار می‌شود (فعال می‌شود)، سپس دستگاه دوباره به حالت غیرفعال برمی‌گردد تا زمان sniff مشخص شده بعدی فرا برسد.
۷. Hold (حالت انتظار): حالت کم مصرف دیگری است که گره پیرو به مدت از پیش تعیین شده‌ای غیرفعال است، اگرچه در این حالت انتقال داده‌ای صورت نمی‌گیرد.

وقتی که دستگاه پیرو داده‌ای برای ارسال یا دریافت نداشته باشد ممکن است دستگاه اصلی، آن را به سمت حالت استراحت هدایت کند. وقتی که دستگاه وارد حالت استراحت می‌شود، آدرس فعال خود را در پیکونت رها می‌کند. این آدرس پس از آن به گره پیروایی که، گره اصلی آن را از حالت غیرفعال دوباره فعال می‌کند، اختصاص داده می‌شود.

۷-۱- پروتکل

استاندارد بلوتوث پروتکل‌های متعددی دارد که به طور ناموزون در چند لایه گروه‌بندی شده‌اند. ساختار لایه‌ها از مدل OSI, TCP/IP، مدل ۸۰۲ یا هر مدل شناخته شده دیگر تبعیت نمی‌کند. با این وجود IEEE در

[۳] sleep

حال اصلاح بلوتوث است تا با مدل ۸۰۲ سازگار تر شود. معماری پروتکل بلوتوث که توسط کمیته ۸۰۲ اصلاح شده‌است.[۲]

مشخصه بلوتوث، پروتکلی است که بلوتوث را به سه گروه منطقی تقسیم می کند که عبارتند از:

۱. گروه پروتکل انتقال
۲. گروه پروتکل لایه‌های میانی
۳. گروه کاربردها

پروتکل‌های انتقال به دستگاه‌های مجهز به بلوتوث این امکان را می‌دهند که محل یکدیگر را تعیین کنند و لینک‌های فیزیکی و منطقی را توسط پروتکل‌های لایه بالاتر و درخواست‌ها مدیریت نمایند. به این نکته باید توجه نمود که استفاده از واژه Transport در اسم این پروتکل به این منظور نیست که این پروتکل منطبق با لایه انتقال از مدل ارجاعی اتصال داخلی سیستم باز، نمی‌باشد. بلکه این پروتکل‌ها مطابق با لایه Data link و لایه فیزیکی از مدل OSI می‌باشند. لایه‌های رادیویی، باند پایه، مدیریت لینک، کنترل منطقی اتصال و انطباق و واسط کنترل ند میزبان که به صورت HCI نامیده می‌شود، در گروه پروتکل‌های انتقال قرار دارند. این پروتکل‌ها هردو انتقال هم‌زمان و غیرزمان را پشتیبانی می کنند. تمام پروتکل‌ها در این گروه برای پشتیبانی از ارتباط بین دستگاه‌های مجهز به بلوتوث لازمند.

گروه دوم از پروتکل‌ها به نام پروتکل‌های میانی شامل سه قسمت و پروتکل‌های استاندارد صنعتی می‌باشند. مانند پروتکل‌های ایجاد و توسعه یافته توسط SIG. این پروتکل‌ها به درخواست‌های موجود و جدید امکان می‌دهند که بر روی لینک‌های بلوتوث عمل کنند. پروتکل‌های استاندارد صنعتی شامل پروتکل نقطه به نقطه (PPP)، پروتکل اینترنت (IP)، پروتکل کنترل انتقال (TCP)، پروتکل‌های درخواست بی‌سیم(WAP) و پروتکل‌های تبادل شئ OBEX))می‌باشند که از تجمیع داده توسط اشعه مادون قرمز (IrDA)نتیجه می‌شوند.

پروتکل‌های ایجاد شده توسط گروه SIG که صرفاً مرتبط با بلوتوث هستند، شامل:

۱) مقلد پورت سریال (RFCOMM) که درخواست‌های legacy را قادر می‌سازد، به صورت یکپارچه بر روی پروتکل‌های انتقال بلوتوث فعالیت کنند. پروتکلی جهت شبیه‌سازی استاندارد درگاه سریال (serial port) است که در تمام PCها از آن برای اتصال صفحه کلید، موس، مودم و امثال آن استفاده می‌شود. این پروتکل برای آن طراحی شده تا بتوان از دستگاه‌های قدیمی به سهولت استفاده کرد.

۲) پروتکل TCS که مبتنی بر بسته‌است، برای مدیریت عملیات telephony که telephony پروتکلی بی درنگ است که برای سه پروفایل انتقال صدا به کارمی آید. این پروتکل همچنین تنظیم و قطع ارتباط را برعهده دارد.

۳) پروتکل کشف خدمات (SDP) که به دستگاه‌ها اجازه می‌دهد اطلاعاتی درمورد سرویس‌های موجود یکدیگر به دست آورند. به طورکلی برای کشف و تشخیص انواع خدماتی که درون شبکه عرضه می‌شود، کاربرد

دارد. استفاده مجدد از پروتکل‌های موجود و خط اتصال یک پارچه بین درخواست‌های موجود یک اولویت بالا در توسعه مشخصات بلوتوث بود.

گروه درخواست شامل درخواست‌های فعلی، که از لینک‌های بلوتوث استفاده می‌کنند، می‌باشد. آن‌ها می‌توانند شامل درخواست‌های legacy مانند درخواست‌های مطلع از بلوتوث باشند. این لایه محل قرارگرفتن انواع برنامه‌های کاربردی و پروفایل‌ها است. این لایه برای انجام کار از خدمات پروتکل‌های موجود در لایه‌های زیرین بهره می‌گیرد. هر برنامه کاربردی، زیرمجموعه‌ای از پروتکل‌های مختص به خود را به خدمت می‌گیرد. ابزارهای ویژه‌ای مثل گوشی بی‌سیم(Headset) بسته به نوع برنامه کاربردی آنها، فقط به برخی از پروتکل‌ها نیازمندند.

۸-۱- مزایا

۱. محدودیت در انتقال داده(Data) از طریق سیم

- دستگاه‌هایی که با سیم کار می‌کنند از طریق رابط‌های سریال یا موازی(parallel) و یا USB به کامپیوتر متصل می‌شوند. اگر از ارتباط سریال استفاده شود در هر سیکل زمانی یک بیت ارسال می‌شود و ارتباط موازی در هر سیکل ۸ تا ۱۶ بیت را ارسال می‌نماید. این مقادیر در دنیای ارتباطات پرسرعت امروزی بسیار کم است؛ که این مشکل با امواج بلوتوث حل شده‌است.

۲. قیمت ارزان فناوری بلوتوث

- یکی دیگر از دلایل استفاده از تراشه‌های بلوتوث قیمت بسیار مناسب آن است. قیمت این تراشه‌ها است. این تکنولوژی از محدوده فرکانس ۲،۴۰ تا ۲،۴۸ گیگا هرتز که محدوده‌ای رایگان است استفاده می‌کند که ۷۹ کانال ارتباطی را شامل می‌شود.

۳. سرعت انتقال اطلاعات در بلوتوث

- از ارتباط همزمان استفاده شود نرخ انتقال اطلاعات ۴۲۳ کیلوبایت در ثانیه خواهد بود. در این نوع ارتباط دستگاه فرستنده و گیرنده به طور هم‌زمان قادر به دریافت و ارسال اطلاعات هستند. در نوع دیگر ارتباط که ارتباط غیرهمزمان نام دارد نرخ انتقال اطلاعات ۷۲۰ کیلوبایت در ثانیه خواهد بود. البته با وجود سرعت بیشتر این ارتباط نسبت به ارتباط هم‌زمان، قابلیت ارسال و دریافت در یک زمان را ندارد.

۴. برتری بلوتوث در مقابل تکنولوژی مادون قرمز

- فرستنده مادون قرمز و گیرنده آن می‌بایست در مقابل هم قرار بگیرند تا ارسال اطلاعات صورت گیرد، در غیر این صورت و وجود داشتن مانعی در بین راه، انتقال اطلاعات به درستی صورت نمی‌گیرد. یکی دیگر از مشکلات مادون قرمز اصطلاح «یک به یک» است. به این معنی که فقط می‌توان اطلاعات را از یک دستگاه تنها به یک دستگاه دیگر ارسال نمود و در یک لحظه قادر به ارسال اطلاعات از یک دستگاه به چند دستگاه نخواهیم بود اما هر دو مشکل IrDA از طریق بلوتوث قابل رفع است

۵. عدم تداخل امواج بلوتوث با دیگر امواج

- برای جلوگیری از تداخل اطلاعات بلوتوث از تکنیکی به نام FHSS استفاده می‌کند و این تکنیک به دستگاه‌ها اجازه می‌دهد که در یک محدوده فرکانسی مشخص شده به صورت خودکار تغییر فرکانس داشته باشند. در واقع در این تکنولوژی یابنده کانال آزاد بیش از ۱۶۰۰ بار در ثانیه کانال‌های ارتباطی را چک می‌کند تا از کانال‌های اشغال شده با خبر باشد و در صورت ایجاد یک ارتباط جدید یک کانال آزاد را به آن ارتباط اختصاص دهد.

۶. اتوماتیک بودن

- دستگاه‌های مجهز به تراشه‌های بلوتوث به طور خودکار یکدیگر را تشخیص داده و ارتباط برقرار می‌کنند و داده‌ها بدون دستور ما یا با دستور ما انتقال پیدا می‌کنند.

۷. کم مصرف بودن

- احتیاج به انرژی بسیار کم برای برقراری ارتباط با وسایل دیگر موجب صرفه جویی زیاد در مصرف باتری می‌شود. هر سیگنال بلوتوثی که که گوشی تلفن همراه ارسال یا دریافت می‌کند فقط ۱میلی وات از باتری آن را مصرف می‌کند یعنی در واقع می‌توانیم بگوییم که این فعالیت تأثیری روی باتری ندارد.

۹-۱- کاربرد

- ایجاد شبکه بی‌سیم بین کامپیوترها در محیط‌های کوچک که پهنای باند کمی مورد نیاز است.
- ایجاد ارتباط بی‌سیم با دستگاه‌های ورودی و خروجی کامپیوترهای شخصی، مانند صفحه کلید، چاپگر، موس و میکروفن.
- بلوتوث فروش زیادی در تلفن‌های سلولی داشته‌است که آنها را قادر ساخته که به کامپیوترها وPDAs و hands free ها و بسیاری دیگر از دستگاه‌ها متصل شوند و به این ترتیب یک شبکه بی‌سیم LAN را ایجاد می‌کنند. به طوریکه کنترل بی‌سیم ارتباط میان یک تلفن همراه و hands free مشهورترین

کاربرد آن می‌باشد.

- ارسال تصاویر جهت چاپ :بعضی از دستگاه های پرینتر به تکنولوژی بلوتوث مجهز می باشند. به همین خاطر شما قادر خواهید بود تا از طریق PDA یا گوشی تلفن همراه خود، تصاویر مورد علاقه خود را از طریق بلوتوث برای چاپ ارسال نمایید.
- انتقال فایل (مثل عکس و voice و غیره) بین گوشی‌های موبایل و PDAs و کامپیوترها از طریق OBEX.
- handsfree بلوتوث برای گوشی موبایل و smart phoneها
- جایگزین کردن ارتباطات سریال سیمی در (دستگاه‌های اندازه‌گیری و آزمایش ، ابزارهای پزشکی ، گیرندهای GPS ، وسایل کمک شنوایی)
- در دستگاه‌های کنترل راه دور که سابقاً از تکنولوژی INFRARED در آنها استفاده می‌شد.
- اتومبیل و استفاده از تکنولوژی بلوتوث به‌عنوان hands free تلفن در آن
- کنترل از راه دور تلویزیون بجای اینفرارد
- کنترل بی‌سیم کنسول‌های بازی، مانند WII شرکت NINTENDO و PLAYSTATION 3 سونی که هر دو قرار است در دسته‌های بازی بی‌سیم خود از این تکنولوژی استفاده کنند.
- اسپیکر بلوتوث و همچنین هدفون بلوتوث و دیگر محصولات صوتی پرتابل
- تعویض کننده اسلاید : به کمک گوشی تلفن همراه و تکنولوژی بلوتوث و یا تجهیزات خاص منظوره می توانید در زمان ارائه مطالب در جلسات یا کنفرانس ها، اسلاید های خود را از راه دور تعویض کنید.

مثال هایی از کاربرد

- یک موس مجهز به تکنولوژی بلوتوث می‌تواند در فاصله دورتر از حد معمول نسبت به مانیتور استفاده شود.
- یک صفحه کلید مجهز به بلوتوث می‌تواند در فاصله دورتری نسبت به مانیتور مورد استفاده قرار گیرد. این امکان فشار بر روی چشم را برای افرادی که دوربین(long-sighted) می‌باشند، کاهش می‌دهد. افزایش فاصله هم چنین اثر تشعشع الکترومغناطیسی که از مانیتور ساطع می‌شود را کاهش می‌دهد. این گونه صفحه کلیدها این توانایی را دارند که بیش از یک کامپیوتر را پشتیبانی کنند. (به روش سوئیچینگ دینامیک)
- استفاده از ایمیل هنگامی که کامپیوتر قابل حمل ما (لپ‌تاپ) هم چنان در چمدان قرار دارد. هنگامی که لپ‌تاپ ما یک ایمیل دریافت می‌کند، یک هشدار از طریق تلفن موبایل خود می‌گیریم مبتنی براین که ایمیل جدید رسیده‌است. هم چنین می‌توانیم تمام ایمیل‌ها رسیده را در صفحه نمایش تلفن همراه باز نموده و آنهایی را که انتخاب کرده‌ایم، بخوانیم.
- فردی که جهت کسب وکار همواره در حال سفر است، می‌تواند از لپ‌تاپ خود درخواست کند که یک چاپگر مناسب را به محضی که به سالن هتل وارد می‌شود، مکان یابی نموده و یک نتیجه چاپی را هنگامی که چاپگر یافت شده‌است و به درخواست لپ‌تاپ پاسخ مثبت داده‌است، به آن بفرستد.
- اتصال بدون کابل به چاپگرها و دستگاه‌های فاکس.
- اتصال بدون کابل به دوربین‌های دیجیتالی و ویدئو پروژکتورها.

- اتصال بدون سیم از تلفن سلولی به hands free.

۱۰-۱- نسخه های بلوتوث

نسخه‌های مختلف بلوتوث از نظر سرعت، مصرف انرژی و از همه مهم‌تر امنیت متفاوت هستند. قابلیت EDRو HS و همین‌طور افزایش حجم بسته‌ها در بلوتوث ۴,۲ سرعت را بیشتر می‌کند و امنیت ارتباط با رمزگذاری داده و همین‌طور روش آدرس‌دهی ابزار مجهز به بلوتوث در شبکه، متفاوت است.

ویژگی اساسی استاندارد بلوتوث این است که نسخه‌های جدید، با نسخه‌های قبلی سازگاری دارند. به عنوان مثل ابزاری مجهز به بلوتوث ۴,۰، با محصولاتی که بلوتوث ۲ و ۳ دارند، سازگار است.

بلوتوث ۱/۰ و ۱/۰ Bو ۱/۱

اولین نسخه‌ی استاندارد بلوتوث، همراه با مشکلات فراوان معرفی شده و ارتباط وسایل مختلف، با سازگاری مطلوبی دنبال نمی‌شد.

دستگاه‌هایی که از این نسخه‌ها استفاده می‌کردند مجبور بودند آدرس سخت‌افزاری دستگاه را در فرایند Hand shakingدو دستگاه فاش کنندکه در این صورت اصل پنهان نگه داشتن هویت دستگاه نقض می‌شد.

نسخه‌ی ۱,۱ بسیاری از مشکلات موجود را حل کرد و ارتباط بی‌سیم با کانال‌های رمزگذاری نشده را ممکن کرد. علاوه بر این نمایش قدرت سیگنال دریافتی یا به اختصار RSSI نیز به بلوتوث اضافه شد.

بلوتوث ۱,۲

تغییرات مهم این نسخه شامل افزایش سرعت اکتشاف و برقراری ارتباط بین وسایل مجهز به بلوتوث، استفاده از باندهای فرکانسی مختلف برای مقابله با تداخل سیگنال، افزایش عملیاتی سرعت ارتباط تا ۷۲۱ کیلوبیت بر ثانیه نسبت به نسخه‌ی ۱,۱ و در نهایت بهبود استریم صدا با ارسال مجدد بسته‌های داده‌ای که درست منتقل نشده‌اند، است.

بلوتوث ۲,۰ وEDR

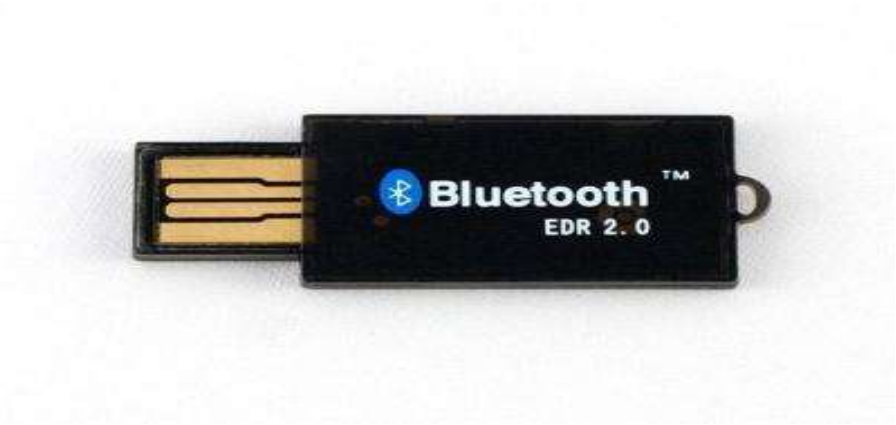
بلوتوث ۲ در سال ۲۰۰۴ معرفی شد. ویژگی مهم این نسخه معرفی EDR یا Enhanced Data Rate به معنی سرعت انتقال داده‌ی بهینه شده است EDR .جزء مشخصه‌های اصلی بلوتوث ۲,۰ نیست بلکه به عنوان یک قابلیت اضافی در نظر گرفته شده و لذا ممکن است تجهیزات مجهز به بلوتوث ۲,۰، از EDR پشتیبانی نکنند.

- EDR قابلیت اضافی بلوتوث ۲ یا ۲,۱ است و سرعت بالایی دارد.

- سرعت نامی EDR معادل ۳ مگابیت بر ثانیه است اما در آزمایش واقعی، سرعت آن چیزی در حد ۲,۱ مگابیت بر ثانیه است
- EDR از ترکیب دو روش مدولاسیون SFSK و PSK بهره می‌گیرد.
- EDR توان مصرفی را نیز به کمک کاهش سیکل کاری کاهش می‌دهد.

بلوتوث ۲,۰ تغییرات زیادی نسبت به نسخه‌ی ۱,۲ ندارد و حتی برخی سازندگان، محصولات مجهز به نسخه‌ی قبلی را با ذکر پشتیبانی از بلوتوث ۲,۰ معرفی می‌کنند، البته بدون سرعت بیشتر.

بلوتوث ۲,۱ وEDR



پشتیبانی از بلوتوث ۲,۰ به همراهEDR

در این نسخه که سال ۲۰۰۷ مشخصه‌های آن اعلام شده، امنیت ارتباط بیشتر شده است. جفت شدن محصولات دارای بلوتوث با امنیت بیشتری صورت می‌گیرد. Extended inquiry response یا به صورت مخفف EIR قبل از برقراری ارتباط با بررسی موارد امنیتی بیشتر و فیلتر کردن کامل‌تر، امنیت ارتباط را بهبود می‌بخشد.

بلوتوث ۳,۰ وHS

این نسخه در سال ۲۰۰۹ معرفی شد. سرعت تئوری بلوتوث ۳,۰ به همراه HS به ۲۴ مگابیت بر ثانیه می‌رسد ولیکن انتقال داده توسط بلوتوث صورت نمی‌گیرد بلکه از لینک ارتباطی ۸۰۲,۱۱ استفاده می‌شود HS .هم مثل EDRیک قابلیت اضافی است و اگر لوگوی HS روی محصولی درج نشده باشد، سرعت لینک بلوتوث به مراتب کمتر خواهد بود. زمانی که ارسال داده با سرعت کمی صورت می‌گیرد، صرفاً بلوتوث فعال است و زمانی

که بسته‌های بزرگ داده ارسال می‌شود، ۸۰۲٫۱۱ که معمولاً در وای فای استفاده می‌شود، وارد عمل شده و انتقال داده با سرعت بسیار بالاتری صورت می گیرد.

پشتیبانی از بلوتوث ۳٫۰ به همراه EDR و HS

بهینه‌سازی توان مصرفی با اضافه کردن سیستم کنترلی حلقه بسته برای بررسی و کنترل توان مصرفی، اضافه شدن دو حالت ERTM و SM برای برقراری ارتباطی با قابلیت اطمینان بالا و یا بدون قابلیت اطمینان بالا (بدون ارسال مجدد داده و کنترل جریان داده) از ویژگی‌ها مهم این نسخه است.

بلوتوث ٤٫۰ و بلوتوث کم‌مصرف یاBLE

در سال ۲۰۱۰ مشخصه‌های بلوتوث ۴٫۰ که با نام بلوتوث اسمارت (هوشمند) شناخته می‌شود، اعلام شد . در این نسخه ، سه حالت بلوتوث کلاسیک (قدیمی)، بلوتوث بسیار سریع (High Speed) و بلوتوث کم‌مصرف (Blutooth Low Energy) به عنوان سه پروتکل ارتباطی تعریف شد.

بلوتوث بسیار سریع مبتنی بر وای–فای است و بلوتوث کلاسیک مثل نسخه‌های قدیمی‌تر بلوتوث است و حالت کم‌مصرف مشابه Wibree سابق است.

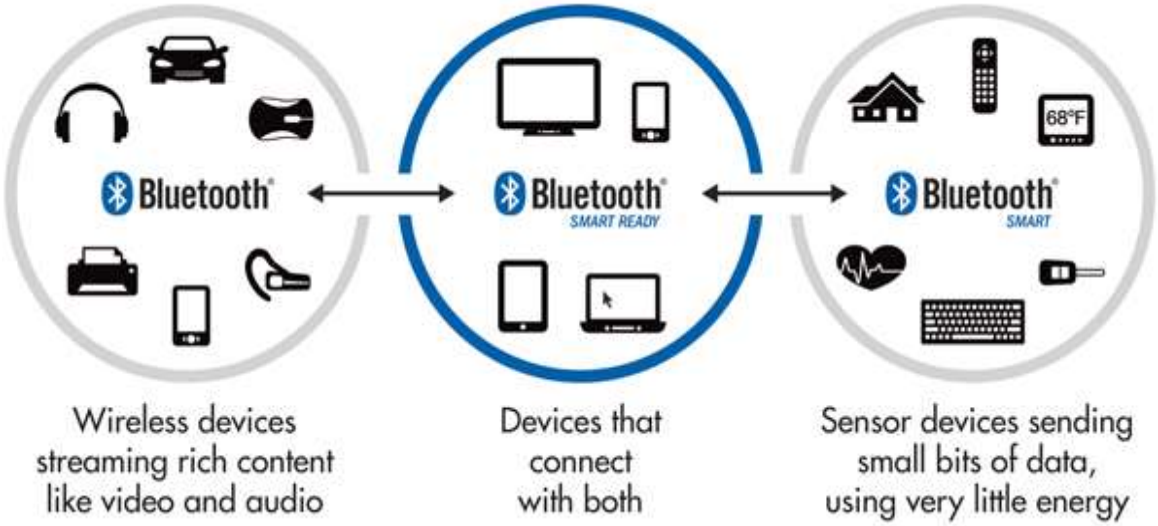
بلوتوث ۴٫۰ شامل تغییراتی مثل کاربرد ساده‌تر، BLE ،افزایش امنیت و رمزگذاری AES است.بلوتوث کم‌مصرف با نام بلوتوث اسمارت هم به کار می‌رود.

BLEیا مخفف بلوتوث کم‌مصرف از زیرمجموعه‌های بسیار مهم بلوتوث ۴٫۰ است، پروتکلی برای برقراری سریع لینک ارتباطی ساده و البته کم‌مصرف. بلوتوث کم‌مصرف از نظر توان مصرفی، بهینه‌تر از بلوتوث ۱٫۰ تا بلوتوث ۳٫۰ است و در محصولاتی مثل اینترنت اشیاء (وسایل منزل و وسایل پوشیدنی) کاربرد دارد BLE .در سال ۲۰۱۱ با تغییر نام به راه خود ادامه داد. در واقع به جای ذکر پشتیبانی ازBLE ،

لوگوی Bluetooth Smart Ready برای محصولات و لوگوی Bluetooth Smart برای حسگرها مورد استفاده قرار گرفت. البته هنوز هم پشتیبانی از BLE در جدول مشخصات محصولات مختلف دیده می‌شود.

بلوتوث اسمارت یا بلوتوث کم‌مصرف و لوگوی آن

د ر تصویر زیر محصولاتی با بلوتوث کم‌مصرف در سمت راست دیده می‌شود، دسته‌ی دیگر محصولاتی با بلوتوث معمولی در سمت چپ است. وسایل مجهز به بلوتوث ممکن است از بلوتوث کم‌مصرف پشتیبانی کنند و در این صورت به هر دو نوع متصل می‌شوند و اصطلاحاً می‌گوییم که بلوتوث کم‌مصرف دوگانه دارند.



محصولاتی با بلوتوث کم‌مصرف در سمت راست و بلوتوث معمولی در سمت چپ

بلوتوث کم‌مصرف به دو شکل پیاده‌سازی شده، یک حالته که در حقیقت شامل همین پروتکل بدون پروتکل‌های دیگر است و حالت دوگانه که بلوتوث کم‌مصرف را در کنار بلوتوث کلاسیک در قالب یک کنترلر بلوتوث پشتیبانی می‌کند. حالت دوگانه از نظر هزینه‌ی تراشه چندان تفاوتی با حالت یگانه ندارد و به همین علت

کمپانی‌های بزرگی مثل کوآلکام، تگزاس اینسترومنت و برودکام از آن استقبال کرده‌اند.

اندروید ٤,٣ (نسخه‌ی ۱۸ واسط برنامه‌نویسی اندروید) و پشتیبانی از بلوتوث کم‌مصرف و کلاسیک

بلوتوث دوگانه در اندروید استودیوی ۱۸ به بعد پشتیبانی شده و در حقیقت اندروید ۴,۳ و نسخه‌های بعدی، از این کنترلر دوگانه پشتیبانی می‌کنند.

بلوتوث ٤,١

این نسخه در سال ۲۰۱۳ معرفی شد که در حقیقت یک بروزرسانی نرم‌افزاری برای سخت‌افزار بلوتوث ۴,۰ است و نیازی به سخت‌افزار جدید وجود ندارد. ویژگی‌های این نسخه اضافه شدن چند قابلیت جدید و بهبود کاربری است. پشتیبانی هم‌زمان از LTE و ۸۰۲,۱۱ n PALو بهبود معماری صوتی برای پشتیبانی از مکالمه با پوشش باند عریض از جمله قابلیت‌های بلوتوث ۴,۱ است.

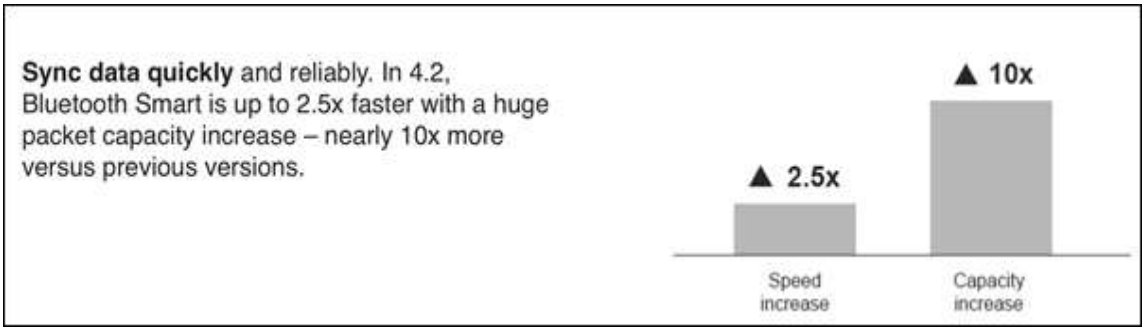
بلوتوث ٤,٢

این نسخه در سال ۲۰۱۴ معرفی شده و در آن برخی ویژگی‌های اساسی برای اینترنت اشیاء اضافه شده است.شاید مهم‌ترین مورد پشتیبانی از IPv6 برای آدرس‌دهی محصولات در شبکه بسیار عظیم اینترنت اشیاء باشد چرا که بنابر تخمین‌های اولیه، در سال ۲۰۲۰ بیش از ۲۸ میلیارد محصول پوشیدنی و وسایل منزل و محیط کار، به اینترنت متصل هستند و به این ترتیب تعدادIP ها بیش از چیزی است که IPv4 توانایی ارایه‌ی آن را دارد.

پشتیبانی از IPv6 در بلوتوث اسمارت

سرعت بلوتوث ۴٫۲ نسبت به نسخه‌ی قبلی حدود ۲٫۵ برابر است. با افزایش حجم بسته‌های داده تا حداکثر ۱۰ برابر، سرعت اشاره شده حاصل می‌شود.

امنیت محصولات بهینه شده و در عین حال توان مصرفی کمتر است. آدرس‌دهی بر عهده‌ی پردازنده‌ی اصلی نیست بلکه کنترلر بلوتوث با مصرف انرژی کمتر این کار را انجام می‌دهد و از طرفی اگر سایر محصولات به عنوان محصول مورد اعتماد تعریف نشده باشند، بلوتوث اسمارت فعال نشده و به آنها متصل نمی‌شود.



سرعت بلوتوث ٤٫۲ با افزایش حجم بسته‌ها تا ۱۰ برابر، حداکثر ۲٫۵ برابر نسخه‌ی قبلی است

قابلیت‌ها و ویژگی‌های مهم بلوتوث ٤٫۲ شامل موارد زیر است:

- افزایش حجم بسته‌های داده در محصولات کم‌مصرف از ۲۷ بایت به ۲۵۱ بایت و افزایش سرعت تبادل داده به بیش از ۸۰۰ کیلوبیت بر ثانیه که در مقال اینترنت اشیاء بسیار مفید است.
- محدوده‌ی ارتباطی با مصرف انرژی پایین، بهینه‌تر است.

- امنیت با جلوگیری از ردیابی محصولاتی با بلوتوث کم‌مصرف، بیشتر شده است.
- توان مصرفی با تغییرات جزئی‌تر تنظیمات توان مصرفی بهبود پیدا کرده است.
- رمزگذاری مبتنی بر FIPS امنیت ارتباط محصولاتی با بلوتوث کم‌مصرف را بیشتر می‌کند. این الگوریتم رمزگذاری، مثل AES در بلوتوث کلاسیک، بسیار امن است و لازمه‌ای برای گسترش اینترنت اشیاء به حساب می‌آید.

۲– بررسی امنیت فناوری بلوتوث

۲–۱– بخش اول : امن سازی

۲–۱–۱– مقدمه

تکنولوژی بلوتوث را می توان در خانه، محل کار، ماشین و ... مورد استفاده قرار داد. تکنولوژی بلوتوث در زمان انتقال اطلاعات بصورت بسیار امن و با محافظت و جلوگیری از هرگونه نفوذ و مداخله،عملیات انتقال اطلاعات را انجام می دهد. البته امنیت بلوتوث بطور کامل و صد در صد نمی باشد و نفوذگران حرفه ای «که تعداد آنها بسیار معدود می باشند» با کمک تجهیزات پیشرفته خود، قادر به ردگیری امواج بلوتوث و سرقت یا دستکاری اطلاعات در حال انتقال می باشند. ذکر این نکته خالی از لطف نمی باشد که با ظهور نسخه های جدیدتر از این تکنولوژی، بحث امنیت و سرعت ارتقاء یافته و روز به روز از تعداد نفوذگران فوق کاسته خواهد شد.

تکنولوژی بلوتوث از همان ابتدا بصورت امن طراحی شده است. به طور کلی سه مدل امنیتی برای برقراری یک ارتباط بی سیم از طریق بلوتوث وجود دارد :

- Security Mode 1: non-Secure
  - بدون امنیت است.
- Security Mode 1: Service Level Enforced Security
  - در مرحله سرویس‌دهی امنیت را برقرار می‌کند، بعد از اینکه کانال ارتباطی پیدا شد.
- Security Mode 1: Link Level Enforced Security
  - در مرحله لینک امنیت را ایجاد می‌کند، قبل از اینکه کانال ارتباطی پیدا شود.

تولیدکنندگان در زمان تولید هر محصول، نوع مدل امنیتی آن را تعیین می کنند. مدل های امنیت در دستگاه ها و سرویس ها متفاوت است. برای دستگاه ها دو سطح trusted device و untrusted device وجود دارد. یک دستگاه trust یا مورد اعتماد، دستگاهی است که قبلا با دستگاه ما ارتباط برقرار کرده است و بطور نا محدود به تمام سرویس های داخل دستگاه دسترسی دارد.

سرویس ها نیز دارای سه سطح امنیتی می باشند:

- Service that require authorization and authentication
- Service that require authentication only
- Service that are open to all devices.

۲-۱-۲- تهدیدات امنیتی مرتبط با فناوری بلوتوث

با رعایت نکات ایمنی و بکارگیری پتانسیل‌های خاصی نظیر «تأیید» و یا «رمزنگاری» می‌توان یک محیط ایمن ارتباطی را ایجاد نمود که دارای شرایط ایمنی مساعدی باشد. تعداد زیادی از دستگاه هائی که از بلوتوث استفاده می‌نمایند از کدهای عددی کوچک (موسوم بهPin code) در مقابل رمزهای عبوری استفاده می‌نمایند و همین موضوع می‌تواند مشکلات امنیتی خاص خود را به دنبال داشته باشد. در صورتی که افراد غیرمجاز قادر به تشخیص و ردیابی یک دستگاه بلوتوث گردند، می‌توانند اقدام به ارسال پیام‌های ناخواسته نموده و یا حتی الامکان استفاده از دستگاه بلوتوث را غیرممکن نمایند. یک مهاجم می‌تواند با استفاده از مکانیزم‌های موجود به اطلاعات موجود بر روی دستگاه مورد نظر دستیابی و حتی به آنان آسیب رساند

۳-۱-۲- حفاظت در مقابل تهدیدات

۱. غیرفعال کردن بلوتوث در زمانی که از آن استفاده نمی‌گردد.
۲. استفاده از بلوتوث در حالت نهان. با پیکربندی دستگاه مورد نظر در حالت نهان، سایر دستگاه‌ها قادر به شناسائی دستگاه مورد نظر نخواهند بود. این موضوع باعث نمی‌گردد که دستگاه‌های بلوتوث قادر به برقراری ارتباط با یکدیگر نباشند. در چنین مواردی می‌توان دستگاه‌ها را «جفت» نمود. بدین ترتیب آنان می‌توانند حتی در حالت نهان نیز با یکدیگر ارتباط برقرار نمایند.
۳. تا جایی که ممکن است از برقراری ارتباط یا انتقال اطلاعات حساس و شخصی با استفاده از دستگاه بلوتوث خودداری کنید.
۴. از کلمات رمزقوی که به طور رندم (تصادفی)، هنگامی که هر دو ابزار بلوتوث به یکدیگر متصل می شوند، ایجاد می شود استفاده کنید. رمز عبور را هنگامی که درخواست های غیرمنتظره به شما می رسد هرگز وارد نکنید.
۵. از دستگاه در تمام زمان ها مراقبت و حفاظت فیزیکی به عمل آورید. ابزارهای مفقود و یا سرقت شده را از لیست دستگاه هایی که با بلوتوث به آن متصل می شوید حذف کنید.
۶. از پذیرش فایل های پیوست یا برنامه هایی که از طریق اتصالات ناخواسته بلوتوث برای شما ارسال می شود خودداری کنید و درخواست اتصال آن ها را رد کنید و تنظیمات سیستم خود را به گونه ای انجام دهید که در قسمت بولوتوث سیستم غیرقابل شناسایی و یا مخفی باشد.

۴-۱-۲- انتقال داده به صورت امن

بلوتوث به اندازه کافی دارای رمز و شناسایی می‌باشد. به علاوه طرح جهش فرکانسی به صورت ۱۶۰۰ بار در ثانیه تأثیر گذار است. در بلوتوث صحت اطلاعات دارای این اجزا می‌باشد:

- تولید عدد به صورت تصادفی
- رمزنگاری
- رمزگذاری کلید مدیریت
- شناسایی و تصدیق

۵-۱-۲- تکنیک ایجاد امنیت در بلوتوث

هر وسیله مبتنی بر بلوتوث یک آدرس ۴۸ بیتی منحصربه‌فرد دارد. رویه تأیید استفاده از کلیدهای متقارن هست و رمزنگاری با کلیدی ۱۲۸ بیتی انجام می‌شود. این کلید ۱۲۸ بیتی که به صورت تصادفی انتخاب می‌شود وظیفه انجام مذاکرات امنیتی بین دستگاه‌ها را بر عهده دارد. وقتی دو سیستم مبتنی بر بلوتوث یک کانال ارتباطی بین همدیگر برقرار می‌کنند. هر دو یک کلید آغازین را ایجاد می‌کنند. برای اینکار یک کلید عبور (Pass Key) یا شماره شناسایی شخصی وارد ارتباط می‌شود و کلید آغازین ساخته می‌شود و کلید پیوندی (Link Key) بر اساس کلید آغازین محاسبه می‌شود. از این به بعد کلید پیوندی برای شناسایی طرف ارتباط استفاده می‌شود.

اولین چالش امنیتی کلید عبور هست که به اختصار PIN نامیده می‌شود. مثل هر کلید دیگری کلیدهای طولانی از کلیدهای کوتاه امن تر هستند. اگر هکری بتواند کلید عبور را کشف کند می‌تواند کلیدهای آغازین ممکن را محاسبه کند و بعد از آن کلید پیوندی را بدست آورد. کلید عبوری طولانی می‌تواند محاسبات را برای یافتن کلیدهای بعدی بسیار سخت بکند.

کلید آغازین جایگزین لینک‌های رمزنگاری نشده می‌شود که این یک نقطه ضعف اساسی به حساب می‌آید. بهتر است که در پردازش هر دو دستگاه بلوتوث این قسمت در محل امن تری قرار بگیرد. چرا که یک هکر می‌تواند داده‌های انتقالی که به یک دستگاه بلوتوث فرستاده می‌شود را ضبط کند و از آن برای خلق PIN استفاده کند. هم چنین استفاده از یک کلید عبوری ثابت و کوتاه در تمام مواقع می‌تواند امنیت یک ارتباط بلوتوث را کاملاً به به خطر بیندازد.

کلید لینک می‌تواند ترکیبی از کلیدها یا کلیدهای واحد باشد. بهترین حالت امنیتی این است که از کلیدهای ترکیبی شامل کلیدهای واحد استفاده شود. وقتی از یک کلید واحد استفاده می‌کنیم. باید برای همه تعاملات امنیتی از همان کلید استفاده نمود و این کلید باید برای تمامی دستگاه‌های مجاز به اشتراک گذاشته شود. این یعنی هر دستگاه مجاز می‌تواند به ترافیک شبکه دسترسی داشته باشد.

۲-۲- بخش دوم:چرا بلوتوث یک خطر امنیتی است؟

۱-۲-۲- مقدمه

در این بخش قصد داریم به این سوال پاسخ دهیم که چرا بلوتوث یک خطر امنیتی است و برای حل این مشکل چه باید کرد؟

در اطراف ما داستان ها و باور های اشتباه بسیاری در مورد بلوتوث وجود دارد[۴]:

۱- فعال سازی بلوتوث عمر باتری را کاهش میدهد.

۲- امواج بلوتوث برای سلامتی مضر است.

۳- بلوتوث فقط در اتاق های کوچک کار میکند (بلوتوث دارای سه کلاس میباشد : کلاس ۳ با بردی کمتر از ۱۰ متر ؛ کلاس ۲ با بردی حدود ۱۰ متر ؛ کلاس ۱ با بردی حدود ۱۰۰ متر)

۴- بلوتوث در حالت مخفی (غیر قابل مشاهده) امن هستند.

۵- امواج بلوتوث و Wi-Fi با هم تداخل دارند.

مشابه این باور های اشتباه از سال ۱۹۸۹ بارها و بارها تکرار شده اند و بسیاری از مشکلات آن زمان ؛امروزه اثبات شده اند.

اما برخی از آن مشکلات پتانسیل ایجاد یک حفره ی امنیتی و آسیب پذیری را دارند.بنابراین باور این موضوع که بلوتوث هم اکنون یک تکنولوژی امن است ؛اشتباه می باشد.

ما به شما پیشنهاد نمیکنیم که بلوتوث را به طور کامل از بین ببرید .چون با تمام بحث های موجود ؛استفاده از این تکنولوژی در بسیاری از راه ها مفید است.

تمامی هدف ما این است که شما را از خطرات استفاده از این فناوری آگاه سازیم.بنابر این در همین راستا ؛نکات زیر را هنگامی که از بلوتوث استفاده میکنید در نظر بگیرید.

۲-۲-۲- ارتباطات امن به حد کافی خوب نیستند.

زمانی که نسخه ی ۲,۱ بلوتوث در سال ۲۰۰۷ منتشر شد ؛ آنها یک ویژگی امنیتی جدید با نام جفت شدن امن آسان [۵] یا SSP را معرفی کردند. هر دستگاهی که از بلوتوث ۲,۰ یا نسخه ی قدیمی تر آن استفاده میکند از SSP حمایت نمیکرد بنابراین آن دستگاه ها کاملا نا امن بودند.البته میتوان گفت حتی برای دستگاه هایی که از SSP استفاده میکنند هم ضمانتی برای تضمین امنیت آنها وجود ندارد.محققان کشف کردند که الگوریتم

---

[۴] www.makeuseof.com

[۵] Secure Simple Pairing

رمزگذاریی که در بلوتوث ۲٫۱ استفاده می شود (که همان الگوریتمی است که در نسخه های قبلی نیز استفاده میشده) خودش ناامن است و باعث شد تا آنها به سمت یک الگوریتم رمزنگاری جدید (AES-CCM) که در بلوتوص ۴٫۰ معرفی شد سوق پیدا کنند.اما حتی این الگوریتم هم ثابت کرد که دارای نقص های قابل بهره برداری است ؛ چراکه SSP را شامل نمی شود.

سپس ما وارد دوران بلوتوث ۴٫۱ شدیم که ویژگی جدیدی به آن اضافه شده بود با نام ارتباط امن[۶] با دستگاه های دارای بلوتوث غیر کم مصرف[۷].و بعد از آن دوران بلوتوث ۴٫۲ که همان ویژگی را برای دستگاه های بلوتوث کم مصرف نیز استفاده کرد.بنابر این به نظر میرسد با شروع به کار دستگاه هایی که از نسخه ۴٫۲ بلوتوث که هم از SSP و هم از رمزنگاری AES-CCM پشتیبانی میکند ؛استفاده می کنند دارای امنیت مناسبی هستند.

مشکل آنجا است که برای فرایند جفت شدن دو دستگاه بلوتوث ۴ متد در SSP وجود دارد:

۱- مقایسه عددی[۸]

۲- فقط کار کردن[۹]

---

۶ Secure Connections

۷ Non-LE

۸ Numeric Comparison

۹ Just Works

۳- خارج از گره[۱۰]

۴- رمز ورود [۱۱]

هر کدام از این متد ها معایب و شمکلات خودشان را دارند.روش مقایسه عددی نیازمند صفحه نمایش است ؛ حال آنکه تمامی دستگاه ها ی دارای بلوتوث صفحه نمایش ندارند.روش فقط کار کردن در مقابل حملات و بهره برداری ها آسیب پذیر است.روش خارج از گره نیازمند یک کانال ارتباطی مجزا است که باز هم تمامی دستگاه ها این ویژگی را ندارند و در آخر روش رمز ورود میتوان مورد استراق سمع قرار گیرد .

راهکار

- از اتصال به دستگاه هایی که از بلوتوث قدیمی تر از نسخه ۴,۲ استفاده میکنند خود داری کنید .همچنین فریمور تمام دستگاه های بلوتوث خود را به آخرین نسخه موجود بروز رسانی کنید.اگر امکان بروزرسانی آنها وجود ندارد ؛یا آن دستگاه ها را دور بیاندازید با با مسولیت خودتان از آنها استفاده کنید.

۳-۲-۲- بسیاری از بردار های حمله همچنان وجود دارند.[۱۲]

آسیب پذیری هایی که در بالا به آنها اشاره شد ؛تنها نمونه از اسیب پذیری های موجود برای دستگاه های بلوتوث نیستند.واقعیت این است که بسیاری از حملات که در نسخه های قدیمی تر وجود داشتند ؛همچنان پابرجا هستند و تنها نحوه اجرای آنها تغییر کرده است.

- استعفا [۱۳]: در این حمله مهاجم میتواند امواج موجود در فضا را جهت یافتن انتقالات بلوتوث شنود کند و با بهره برداری از آسیب پذیری درست میتواند داده را بخواند یا بشنود .بنابراین اگر شما از یک هدفون بلوتوث جهت مکالمه استفاده میکنید ؛آگاه باشید که مهاجمان میتوانند به صحبت های شما گوش دهند.
- سرقت اطلاعات [۱۴] :در این حمله مهاجم میتواند به محض اینکه دستگاه ها با هم جفت شدند

---

[۱۰] Out-of-Band

[۱۱] Passkey Entry

[۱۲] nvd.nist.gov

[۱۳] Eavesdropping

[۱۴] Bluesnarfing

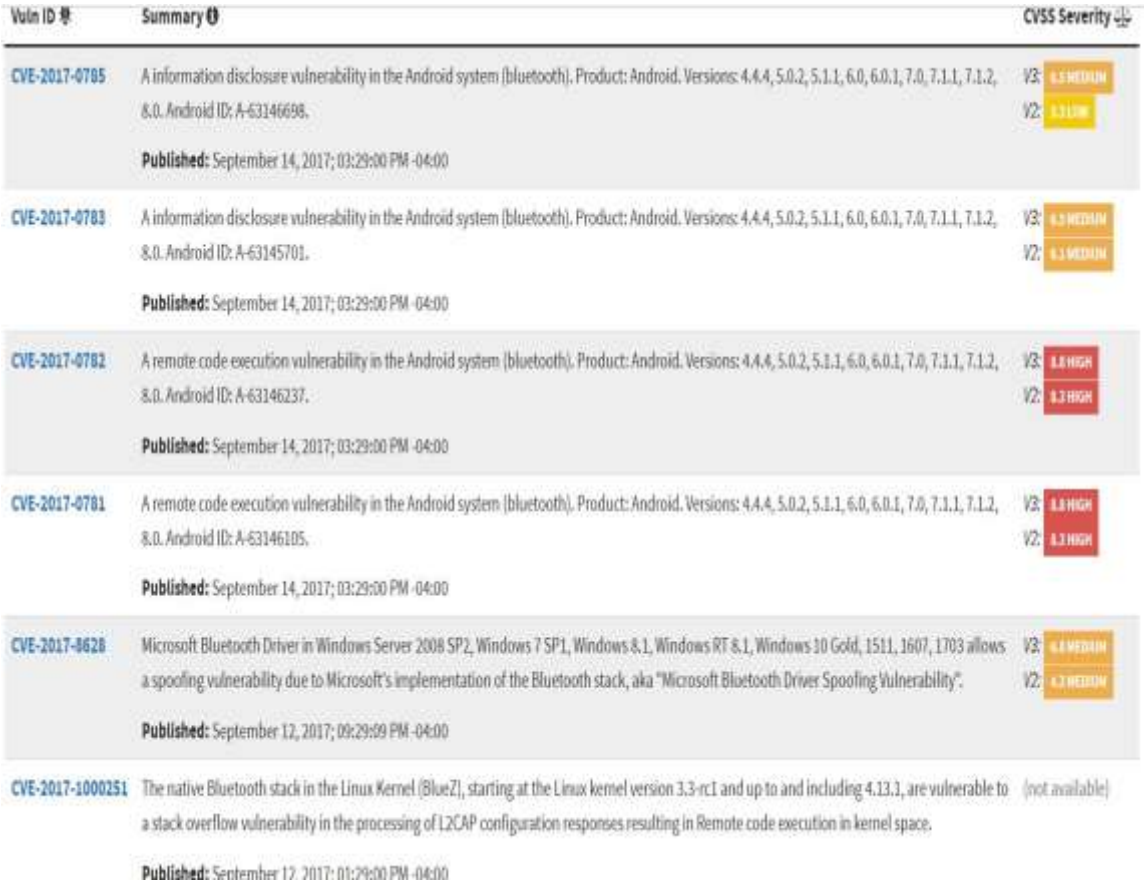
؛به اطلاعات شما دسترسی پیدا کرده و آ»ها را به سرقت ببرند.ارتباط ایجاد شده معمولا بدون اطلاع شما صورت میگیرد ومیتواند باعث سرقت اطلاعات مخاطبین ؛تصاویر؛فیلم ها ؛رویداد های تقویم و غیره شود.

- کنترل دستگاه [۱۵] : در این حمله مهاجم میتواند جنبه های مختلف دستگاه را از راه دور کنترل کند.میتواند تماس برقرار کند ؛ پیام کوتاه ارسال کند ؛تماس ها و پیام های ورودی را فوروارد کند ؛تنظیمات را تغییر دهد :صفحه ی نمایش و کیبورد را ببیند و ....
- منع سرویس : در این حمله مهاجم میتواند سیل اطلاعات بی هوده را به سمت دستگاه شما ارسال کند و باعث مسدود شدن ارتباط ؛ هدر رفت عمر باتری و یا کراش کردن دستگاه شما شود.

راهکار

- اگر امکان تغییر دادن کلمه عبور بلوتوث بروی دستگاه شما وجود دارد (بروی تلفن ها ؛تبلت ها و ساعت های هوشمند امکان پذیر است) پس سریعا این کار را انجام دهید .مطمین شوید که از کدی استفاده کنید که امن باشد.(عدم استفاده از کد های ساده مثل ۱۱۱۱ یا ۱۲۳۴ و ...)این کار میتواند در مقابل بعضی از روش های حمله موثر باشد ؛ولی تنها روشی که امنیت آن تضمین شده است ؛ غیر فعال کردن بلوتوث است.

[۱۵] Bluebugging



Vuln ID	Summary	CVSS Severity
CVE-2017-0785	A information disclosure vulnerability in the Android system (bluetooth). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-63146698. **Published:** September 14, 2017; 03:29:00 PM -04:00	V3: 6.5 MEDIUM V2: 3.3 LOW
CVE-2017-0783	A information disclosure vulnerability in the Android system (bluetooth). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-63145701. **Published:** September 14, 2017; 03:29:00 PM -04:00	V3: 6.5 MEDIUM V2: 6.1 MEDIUM
CVE-2017-0782	A remote code execution vulnerability in the Android system (bluetooth). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-63146237. **Published:** September 14, 2017; 03:29:00 PM -04:00	V3: 8.8 HIGH V2: 9.3 HIGH
CVE-2017-0781	A remote code execution vulnerability in the Android system (bluetooth). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-63146105. **Published:** September 14, 2017; 03:29:00 PM -04:00	V3: 8.8 HIGH V2: 9.3 HIGH
CVE-2017-8628	Microsoft Bluetooth Driver in Windows Server 2008 SP2, Windows 7 SP1, Windows 8.1, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703 allows a spoofing vulnerability due to Microsoft's implementation of the Bluetooth stack, aka "Microsoft Bluetooth Driver Spoofing Vulnerability". **Published:** September 12, 2017; 09:29:00 PM -04:00	V3: 6.8 MEDIUM V2: 4.2 MEDIUM
CVE-2017-1000251	The native Bluetooth stack in the Linux Kernel (BlueZ), starting at the Linux kernel version 3.3-rc1 and up to and including 4.13.1, are vulnerable to a stack overflow vulnerability in the processing of L2CAP configuration responses resulting in Remote code execution in kernel space. **Published:** September 12, 2017; 01:29:00 PM -04:00	(not available)

نمونه هایی از آسیب پذیری های بلوتوث

۴-۲-۲- حتی در حالت مخفی هم پیدا میشوید

ظهور انتقال در حالت کم مصرف (LE) در بلوتوث ۴,۰ به طور گسترده ای مورد استقبال قرار گرفت .علت این استقبال این بود که این ویژگی طول عمر باتری دستگاه را بهبود میبخشید.اما بلوتوث کم مصرف به اندازه ی نسخه های کلاسیک بلوتوث نا امن بود.دلیل این بود که بلوتوث به محض روشن شدن اطلاعات خود را در محیط برادکست میکرد و هر کسی در اون محدوده میتوانست آن را ببیند و در وهله اول این دقیقا همان موضوعی است که باعث میشود استفاده از بلوتوث راحت باشد.

مشکل اما آنجاست که این براد کست اطلاعات شامل جزییاتی منحصر به فرد در مورد دستگاه نیز میباشد.از جمله شناسه ی منحصر به فرد جهانی که با نام UUID[۱۶] شناخته میشود . آمیختن این اطلاعات با قدرت سیگنال دریافتی (RSSI[۱۷]) و با کمک جابه جایی دستگاه شما میتواند باعث ردیابی و مشاهده هدف

[۱۶] universally unique identifier

[۱۷] received signal strength indicator

شود.

اغلب مردم فکر میکنند با تغییر تنظیم بلوتوث و قرار دادن آن بروی "غیر قابل کشف" در واقع میتوانند از ان نوع خطرات در امان باشند ولی این موضوع صحیح نیست.همانطور که شرکت AS Ars چندی پیش ثابت کرد که ابزار های متن – بازی [۱۸]هستند که با کمک آنها میتوان دستگاه هایی را که در حالت غیر قابل کشف هستند را نیز شنود کرد.

راهکار

- متاسفانه هیچ راهکاری برای این مورد جز غیر فعال کردن بلوتوث وجود ندارد.چون شما اطلاعات خود را در محدوده ی مکانی خود برادکست میکنید.

۳-۲- بخش سوم: حملات رایج

۱-۳-۲- شیوه کلی حملات

با وجود مکانسیم های دفاعی تکنولوژی بلوتوث، استفاده از آن می تواند منجر به افشا و از دست رفتن اطلاعات به شیوه های زیر شود.

۱-۱-۳-۲- روش اول :

فرد مهاجم یا هکر پیامی برای شما ارسال می کند و از شما می خواهد که بلوتوث خود را برای دریافت پیام، که اکثرا مقاصد تبلیغاتی دارند روشن کنید. این شیوه همانند روشی است که در ایمیل های اسپم و همچنین حملات

[۱۸] Blue Hydra

فیشینگ علیه کاربران ایمیل استفاده می شود.

هنگامی که یک پیام کلاهبرداری با محتوای مضر از طریق بلوتوث ارسال می شود، ممکن است کاربر را به پاسخ دادن به پیام و همچنین افزودن مهاجم به دفترچه آدرس خود ترغیب و تشویق کند. صاحبان دستگاه های دارای بلوتوث باید آگاه باشند، شاید پیامی را که دریافت می کنند یکی از انواع حملات مهندسی اجتماعی باشد که در آن با تغییرات و دست کاریهایی که توسط مهاجم ایجاد می شود منجر به افشای اطلاعات می شود.

۲-۱-۳-۲ روش دوم :

در این روش اتصال به اجبار با دستگاه دارای قابلیت بلوتوث جهت دسترسی به اطلاعاتی همچون لیست تماس، تقویم، ایمیل، پیام های متنی، تصاویر، فیلم ها، کد IMEI و اطلاعات دیگری که در کارت حافظه ذخیره شده، برقرار می شود. IMEI کد وشناسه منحصر به فردی برای هر دستگاه است که هکر و مهاجم می تواند با تغییر و دسترسی به آن تمامی تماس های ورودی شخص را به دستگاه خود منتقل کند.

این شیوه در مقایسه با شیوه اول بسیا مخرب تر است، زیرا در حالت دوم اتصال بدون اطلاع صاحب دستگاه صورت پذیرفته است. یکی دیگر از مواردی که توسط مجرمان پس از اتصال از طریق بلوتوث انجام می شود تخلیه شارژ باطری گوشی کاربر است که موجب مختل شدن ادامه کار دستگاه شخص می شود.

برخی از شیوه های شناخته شده ی حملات بلوتوث عبارت اند از :

۱- شناسایی هویت[۱۹]
۲- ردیابی موقعیت مکانی[۲۰]
۳- منع سرویس [۲۱]
۴- دسترسی و کنترل ناخواسته به اطلاعات و ارتباطات صوتی[۲۲]
۵- دسترسی و کنترل اطلاعات توسط دستگاه های غیر مجاز (احراز هویت نشده)[۲۳]

۲-۳-۲- انواع حملات بلوتوث

با توجه به این موضوع که هم اکنون میلیارد ها دستگاه در دنیا از فناوری بلوتوث استفاده میکنند ؛نقص های امنیتی مخرب به صورت کلی در حال رخدادن هستند و این انتظار وجود دارد که در آینده ی نزدیک این میزان افزایش چشم گیری داشته باشد.متقابلا افزایش استفاده دستگاه ها از بلوتوث ؛نگرانی های امنیتی را تشدید

[۱۹] Identity detection
[۲۰] Location tracking
[۲۱] Denial of service (DoS)
[۲۲] Unintended control and access of data and voice channels
[۲۳] Unauthorized device control and data access

میکند. زین پس ساختار امنیتی بلوتوث نیازمند یک توسعه پایدار و متداول میباشد تا از تهدیدات ناشناخته ی جدید جلوگیری کند. همانند هر سیستم ارتباطی بیسیم ؛ اتقال بلوتوثی هم میتواند عمدا مسدود شود یا اطلاعات دستکاری شده ؛یا غلط توسط مجرمان سایبری به دستگاه قربانی تحویل داده شود.

تهدیدات امنیتی در بلوتوث را میتوان به سه شاخه زیر دسته بندی کرد:

۱- تهدید افشاء اطلاعات[۲۴] : در این تهدید ؛جریان اطلاعات به سمت سیستمی ارسال میشود که اجازه دسترسی به آن اطلاعات را ندارد.

۲- تهدید یکپارچگی اطلاعات[۲۵] : در اسن تهدید ؛ اطلاعات به صورت عمدی جهت گمراه کردن گیرنده اصلاح میشود.

۳- تهدید منع سرویس : در این نوع تهدید ؛ کاربر از دریافت سرویس مورد نظر خود باز میماند به طوری که آن سرویس یا در دسترس نیست ؛ یا به شدت محدود شده است.

۱-۳-۲- حمله BlueBorne

[۲۴] Disclosure threat

[۲۵] Integrity threat

میلیاردها دستگاه اندروید، iOS، ویندوز و لینوکس که از بلوتوث استفاده می‌کنند در معرض خطر حملات سایبری قرار گرفتند. این حمله می‌تواند از راه دور رخ دهد و هیچ نیازی به تعامل با کاربر ندارد. آزمایشگاه Armis که در حوزه‌ی حفاظت از دستگاه‌های اینترنت اشیاء فعالیت می‌کند، در مجموع ۸ آسیب‌پذیری را در پیاده‌سازی بلوتوث کشف کرده است که دستگاه‌های تلفن همراه، رومیزی و دستگاه‌های اینترنت اشیاء را در معرض حمله‌ای با نام BlueBorne قرار می‌دهد.

محققان امنیتی توضیح دادند تنها چیزی که برای اجرای این حمله ضروری است، این است که بر روی دستگاه قربانی، بلوتوث فعال باشد و نیازی به اتصال دستگاه قربانی به دستگاه مهاجم و یا اینکه بلوتوث قربانی قابل مشاهده باشد، وجود ندارد. مهاجمی که در محدوده‌ی بلوتوث قربانی قرار دارد، می‌تواند از یکی از این آسیب‌پذیری‌های پیاده‌سازی بلوتوث بهره‌برداری کرده و منجر به اجرای کد از راه دور، حمله‌ی مرد میانی و یا افشای اطلاعات شود. تنها چیزی که مهاجم نیاز دارد این است که تشخیص دهد بر روی سامانه‌ی قربانی از چه سیستم عاملی استفاده شده تا بهره‌برداری مخصوص به آن را اجرا کند.

اجرای حمله‌ی BlueBorne هیچ نیازی به این ندارد که کاربر قربانی بر روی پیوندی کلیک کرده و یا پرونده‌ای را باز کند. تمامی عملیات مربوط به حمله نیز در پس‌زمینه انجام شده و قربانی به هیچ چیزی شک نخواهد کرد. محققان می‌گویند به دلیل اینکه این حمله از بلوتوث بهره‌برداری می‌کند و بلوتوث نیز جزو بردارهای حمله‌ی معمول نیست، بسیاری از راه‌کارهای امنیتی، عملیات مخرب را شناسایی نخواهند کرد. مهاجمان می‌توانند از این آسیب‌پذیری‌ها بهره‌برداری کرده و بر روی سامانه‌های قربانیان، باج‌افزار و دیگر بدافزارها را نصب کنند. محققان همچنین معتقدند از این روش می‌توان برای ایجاد کرم استفاده کرد تا از طریق بلوتوث از یک دستگاه به

دستگاه‌های دیگر توزیع شود. محققان نشان دادند که می‌توان از آسیب‌پذیری‌های BlueBorne بهره‌برداری کرده و حمله‌ی مرد میانی را بر روی ماشین ویندوز انجام داد. محققان همچنین توانستند نشست مرورگر قربانی را به سمت یک وب‌گاه فیشینگ هدایت کنند.

محققان در یک ویدئو نیز نشان دادند که می‌توانند کنترل یک ساعت هوشمند سامسونگ را که بر روی آن سامانه عامل Tizen اجرا می‌شود در دست گرفته و از مالک دستگاه جاسوسی کنند. آسیب‌پذیری‌هایی که اجازه‌ی حمله‌ی BlueBorne را می‌دهند در پیاده‌سازی‌های بلوتوث بر روی بسترهای مختلف کشف شده‌اند. محققان آسیب‌پذیری‌های افشای اطلاعات، اجرای کد را در ماشین لینوکس، یک آسیب‌پذیری با شناسه‌ی CVE- ۲۰۱۷-۸۶۲۸ برای اجرای حمله‌ی مرد میانی را در ویندوز کشف کرده‌اند. چهار آسیب‌پذیری اجرای کد، حمله‌ی مرد میانی و افشای اطلاعات در بستر اندروید و یک اشکال اجرای کد نیز در iOS کشف شده است.

بلوبورن شامل آسیب پذیری های زیر میباشد:

آسیب پذیری اجرای کد از راه دور (RCE) در کرنل لینوکس	CVE-2017-1000251
نقص نشت اطلاعات در پشته بلوتوث لینوکس (BlueZ)	CVE-2017-1000250
نقص افشا اطلاعات در ان اندروید	CVE-2017-0785
آسیب پذیری اجرای کد از راه دور (RCE) در اندروید	CVE-2017-0781
نقص اجرای کد از راه دور (RCE) در اندروید	CVE-2017-0782
آسیب پذیری حمله مردی در میانه (MitM) در بلوتوس ورژن Pineapple	CVE-2017-0783
نقص حمله مردی در میانه (MitM) در پیاده سازی بلوتوث در ویندوز	CVE-2017-8628
آسیب پذیری اجرای کد از راه دور (RCE)در پرتکل Low Energy Audio اپل	CVE-2017-14315

شرکت Armis در آنالیز های خود نشان داده اند که چگونه مهاجم با کاوش دستگاه قربانی سیستم عامل آن را بدست می آورد و بهره بردار خود را متناسب با آن محیا میکند. و سپس در هنگام پیاده سازی ارتباط بلوتوث ؛ از آسیبپذیری موجود استفاده کرده و دستگاه قربانی را به دست میگیرد.

شرایط و پیش نیاز های اجرای حمله Blue Born

1 -بلوتوث قربانی باید فعال باشد.

2 -مهاجم باید در رنج سیگنال بلوتوث قربانی قرار گیرد (بسته به کلاس بلوتوث قربانی از کمتر از ۱۰ متر تا حدود ۱۰۰ متر)

3 –حمله وابسته به پلتفورم یا سیتم عامل مورد استفاده دستگاه قربانی است ؛بنابراین باید بهره برداری[۲۶] که قرار است مورد استفاده قرار گیرد از قبل مشخص شود.

راهکار

چندین وصله امنیتی برای این آسیب پذیری ها وجود دارد .بهترین راهکار برای مقابله با این آسیب پذیری ها بروز رسانی امنیتی آنها است.

شرکت گوگل در به‌روزرسانی‌های امنیتی مربوط به ماه سپتامبر این آسیب‌پذیری‌ها را وصله کرده است. شرکت مایکروسافت نیز آسیب‌پذیری موجود در ویندوز را با کد CVE-2017-8628 وصله کرد و همچنین آن را در به‌روزرسانی ماه سپتامبر خود نیز قرار داد. شرکت اپل با انتشار نسخه‌ی ۱۰ از iOS مشکل را برطرف کرده ولی در نسخه‌های پیشین، آسیب‌پذیری‌ها همچنان وجود دارند. به توسعه‌دهندگان لینوکس نیز این آسیب‌پذیری‌ها اطلاع داده شده و در حال کار برای انتشار وصله هستند. این آزمایشگاه امنیتی توضیحات هریک از آسیب‌پذیری‌ها را در منتشر کرده ولی انتشار بهره‌برداری از آن‌ها به زمان بعد موکول کرده است.

[۲۶] Exploit

۳- جمع بندی

۳-۱- آینده ی بلوتوث

ویرایش بعدی بلوتوث LISBON نامیده شده که شامل یک تعداد مشخصه‌است از جمله افزایش امنیت و قابلیت استفاده بیشتر از بلوتوث که ویژگی‌های اصلی آن به ترتیب زیر است:

۱. تغییر رمز به صورت اتوماتیک: به‌طور تناوبی کدهای رمزی تغییر داده می‌شود تا امنیت افزایش یابد.
۲. گسترش پاسخ به درخواست‌ها: در طول پروسه بازبینی و درخواست، اطلاعات بیشتری جمع‌آوری شده و به دستگاه‌ها امکان فیلترینگ بهتری را جهت ارتباط می‌دهد.
۳. کاهش توان مصرفی: سبب کاهش توان مصرفی، وقتی که وسایل در وضعیت sniff low power هستند، می‌شود
۴. افزایش کیفیت سرویس: سبب خواهد شد که وقتی ترافیک مخابراتی در یک خوشه پیکونت بالاست، داده‌های صوتی و تصویری با کیفیت بالا ارسال شوند.
۵. جفت شدن وسایل به طور ساده: به شکل اساسی وظیفه بهبود در جفت شدن وسایل بلوتوث را به عهده دارد. به‌طوری که در یک زمان هم کارایی و هم امنیت افزایش می‌یابد. انتظار می‌رود که این مورد به‌طور قابل توجهی در استفاده از بلوتوث افزایش یابد.

ویرایش بعد از LISBON نسخه SEATTLE نامیده می‌شود که مشخصه و ویژگی‌های بیشتری را دارد که عمده آنها روی UWB متمرکز شده‌است. این خصیصه امکان استفاده از بلوتوث را در عرض باند بسیار بالای رادیویی موجب شده که به دنبال آن ارسال و انتقال اطلاعات داده‌ها را با سرعت بسیار بالا فراهم می‌کند.

نوآوری‌های اخیر در «آنتن» های «بلوتوث» به این وسایل اجازه داده است تا از بردی که در ابتدا برای آن طراحی شده است بسیار فراتر قدم بگذارند. در همایش دوازدهم DEF CON[۲۷]، گروهی از هکرها که با عنوان Flexilis شناخته می‌شوند، توانستند دو وسیله «بلوتوث» را که حدود نیم مایل (۸۰۰ متر) از یکدیگر دور بودند با موفقیت به هم متصل کنند. آنها از آنتنی مجهز به یک «نوسان‌نما»[۲۸] و یک «آنتن یاگی»[۲۹] استفاده کردند که همه آنها به قنداق یک تفنگ متصل شده بود. کابلی آنتن را به کارت «بلوتوث» در رایانه متصل می‌کرد. بعدها

[۲۷] همایش سالانه «هکر» ها که در «لاس‌وگاس» برگزار می‌شود

[۲۸] Scope

[۲۹] Yagi

آنتن را «تیرانداز آبی» نامیدند.

۲-۳- نتیجه‌گیری

تکنولوژی بی‌سیم بلوتوث نکات کلیدی مهمی را در بر می‌گیرد که استفاده گسترده آن را آسان می‌کند.

این تکنولوژی یک تکنولوژی بی‌سیم کوتاه برد است که به دستگاه‌های پیرامون اجازه می‌دهد که از یک واسط هوایی منفرد (به جای استفاده از کابل‌هایی با اتصال گرهای با شکل‌ها، اندازه‌ها و تعداد گیره مختلف) برای اتصال استفاده کنند.

این تکنولوژی یک استاندارد باز است که در دسترس عموم است وبدون حق امتیاز (انحصار) است.

بلوتوث از هر دونوع داده و صوت پشتیبانی می‌کند که باعث تبدیل شدن آن به یک تکنولوژی ایده‌آل برای ارتباط بین وسیله‌ها است.

بلوتوث از یک باند با فرکانس نامنظم که در همه جای دنیا قابل دسترس است استفاده می‌کند.

برای دستیابی به درک کامل از بلوتوث شبکه‌ای کامل از دستگاه‌های متفاوت بلوتوث (چند گانه) مورد نیاز است و این منتهی به رسیدن به شبکه‌های پراکنده بلوتوث می‌شود که باید اشاره به تشکیل، شکل دهی، زمان‌بندی و مسیریابی و شبکه‌ها کند. معماری بلوتوث به صورت شبکه‌های پیکونت است که یک دستگاه وظیفه هماهنگی بقیه ندها در شبکه را بر عهده دارد. استاندارد بلوتوث پروتکل‌های متعددی دارد که از استاندارد IEEE۸۰۲،۱۵ تبعیت می‌کند.

۳-۳- سخن آخر

ممکن است بلوتوث دیگر آینده ای نداشته باشد. امروزه ما به یک تکنولوژی امنتر برای جایگزین شدن بلوتوث مانند Wi-Fi Directنیازمندیم .یک راه ارتباطی متفاوت دستگاه به دستگاه با برد کوتاه .هرچند که این تکنولوژی همانند بلوتوث همه جایی نشده است اما پتانسیل آن را دارد. البته هر تکنولوژیی مشکلات مربوط به خود را نیز دارد.

برای مطالعه بیشتر درباره ی Wi-Fi Direct میتوانید به این وبسایت مراجعه فرمایید

۴-۳- منابع

- http://www.ijsrp.org/research-paper-0416/ijsrp-p5252.pdf
- https://duo.com/blog/an-analysis-of-blueborne-bluetooth-security-risks
- https://www.trendmicro.com/vinfo/au/security/news/internet-of-things/blueborne-bluetooth-vulnerabilities-expose-billions-of-devices-to-hacking
- http://www.makeuseof.com/tag/5-myths-bluetooth-can-safely-ignore-now/
- https://pomcor.com/2015/06/03/has-bluetooth-become-secure/
- https://nvd.nist.gov/view/vuln/search-results?query=bluetooth&search_type=all&cves=on
- https://arstechnica.com/information-technology/2016/09/hands-on-blue-hydra-can-expose-the-all-too-unhidden-world-of-bluetooth/
- http://www.makeuseof.com/tag/the-differences-between-bluetooth-4-0-and-wi-fi-direct-you-need-to-know/
- http://www.makeuseof.com/tag/3-ways-bluetooth-device-security-risk/
- https://www.bluetooth.com/what-is-bluetooth-technology/discover-bluetooth
- https://www.us-cert.gov/ncas/current-activity/2017/09/12/BlueBorne-Bluetooth-Vulnerabilities
- https://www.kb.cert.org/vuls/id/240311
- https://www.webroot.com/us/en/business/resources/articles/corporate-security/a-review-of-bluetooth-attacks-and-how-to-secure-mobile-workforce-devices
- https://cve.mitre.org/
- https://nvd.nist.gov/vuln/categories
- https://www.kaspersky.com/blog/bluetooth-security/1637/