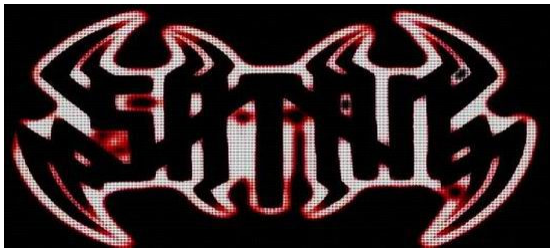
Blue Tooth

Author : Sir.Hitler

The First And The Best Persian Journal About BlueTooth

Satanic Hell & Shabgard



جهنم شیطانی و شبگرد

Bluetooth

مباحثی پیرامون بلوتوس (قسمت اول)

نویسنده: **Sir.Hitler**

تاریخ: **April 20/2006** **1385/1/31**

ایمیل:

Sir.Hitler@Gmail.com
Sir_Adolf.Hitler@Yahoo.com

با تشکر فراوان از :

Satanic Soulful ,Hell Hacker , A.Mehrvarz , Little Hacker, Bl2k S hahro Z , XShabgardX, Hamid Star2005, Farhad1507, BlackIce

ملاحظه:

لازم به تذکر است کلیه مطالب گفته شده تنها جنبه آموزشی داشته و هرگونه استفاده نادرست به عهده خود کاربر می باشد و نویسنده این مقاله و تیم امنیتی جهنم شیطانی و شبگرد هیچ گونه مسئولیتی نسبت به استفاده نا درست از این مقاله را بر عهده نمی گیرد.

تمامی حقوق مادی و معنوی این مقاله در اختیار تیم های ذکر شده میباشد و استفاده از مطالب این مقاله با ذکر نام نویسنده و همچنین گروه های مربوطه بلامانع است.

منابع:

1. Bluetooth SIG - http://www.bluetooth.com/
2. Research of trifinite group - http://trifinite.org/
3. Research of Ollie Whitehouse - http://www.blackops.cn/
4. Research of The Shmoo Group - http://www.shmoo.com/
5. BlueZ Project - http://www.bluez.org/
6. BlueLon (Bluetooth BodyTag producer) - http://www.bluelon.com/
7. FTE (producer of BT Sniffer) ? http://www.fte.com/
8. Bluetooth Device Discovery (presentation) - by Bruce Potter
9. Bluetooth Vulnerabilities Fact and Fiction (WiCon 2004 presentation) by Pentest Lmited
10. Bluetooth ? The universal radio interface for ad hoc, wireless connectivity by Jaap Haartsen
11. Positioning and Location Technologies (presentation) by Peter Ørbæk, WorkSPACE, PalCom projects
12. Positioning using Bluetooth (presentation) - IT University of Copenhagen

خجسته باد نام خداوند که نیکوترین آفریدگاران است و نام تو که نیکوترین آفریدگانی (آریا)

مقدمه:

(BT)Bluetooth تکنولوژی بیسیم که راهی آسان را برای دسترسی به شیوع جدید مکالمه بین افراد و اتصال به اینترنت بدون نیاز به سیم، کابل و متصل کننده میسر میسازه. این فناوری توسط 3000 شرکت کوچک و بزرگ از جمله : Sony Ericsson،Nokia،Motorola، Intel، IBM، Toshiba،Motorola، Apple،Microsoft و حتی شرکت های خودرو سازی مانند BMW و TOYOTA پشتیبانی و استفاده میشود. گستردگی این فناوری را در بازار میتوان مشاهده کرد . برای مثال استفاده زیادی در زمینه های پرینتر ، لپ تاپ، کیبورد ، ماشین و بیشترین استفاده عمومی که در تلفن های همراه است که این میزان 60٪ میباشد. این تکنولوژی محبوبیت زیادی را بدست آورده به طوریکه 3میلیون نفر در هر هفته جذب این فناوری میشوند. مطابق گفته ی IDC تا سال 2008 کاربران این فناوری به 922 میلیون نفر میرسد ! این تکنولوژی به نظر بسیار جالب و سودمند است بنابراین می تواند امنیت کاربرانش را تا حد زیادی تهدید نماید.

این طرح در سال 1994 مطرح شد ، زمانی که تیم تحقیقات اریکسون به مدیریت Dr.Jaap Haartsen و Dr.Sven Mattisson به دنبال ساخت دستگاهی کم مصرف بودند که بتواند دستگاههایی که در فاصله کم از یکدیگر قرار دارند را بدون نیاز به سیم به یکدیگر متصل نماید و آن را جایگزینی مناسبی برای اتصال کابلی تلفن همراه به رایانه ، هدست و دیگر وسائل بکنند. این تکنولوژی به طوری توسعه داده شد که ما آن را با نام کنونی Bluetooth می شناسیم. SIG Bluetooth (Special Interest Group) در می سال 1998انتشار یافت و در سپتامبر همان سال به صورت رسمی در شرکتها مورد استفاده قرار گرفت. اولین شرکتهایی که از این فناوری در محصولاتشان استفاده کردند IBM،Ericsson ، Intel ، Nokia و Toshibaبودند . و بعد از آن در دسامبر سال 1999 سه شرکت بزرگ به نامهای :

Microsoft، Lucent Technologies و Motorola وارد جمع استفاده کنندگان از این فناوری شدند.

بعد از سالها پیشرفت در این رابطه آخرین تکنولوژی Bluetooth را به طور رایگان و سراسری پیش از پخش آن در سال 2005 برای مصرفی کم و دو دستگاه Bluetooth در اندازه 10-100 متر برای اشتراک گذاشتن اطلاعات همراه توان عملیاتی بالا 723.2 Kbps تا حد 2.1Mbps با تشخیص برای بالا بردن سرعت اطلاعات در ISM های 2.4 GHz رادیو استفاده کردند . هر دستگاه میتوانست همزمان با 7 دستگاه دیگر ارتباط داشته باشد.

همچنین تکنولوژی Bluetooth نامزده تامین کردن کنترل و امنیت از QOSشد . هرچند این امکان وجود دارد که در آینده مشکلات امنیتی را از خود بروز دهد و به راحتی در مقابل حملات خرابکارانه تسلیم شود.

از جمله مواردی که در این روزها از تکنولوژیBT استفاده میشود به شرح زیر میباشد:

1. اتصال بدون سیم هدست به تلفن همراه .
2. بروز رسانی تقویم ، دفترچه تلفن و دیگر اطلاعات بین PDA و PC.
3. انتقال تصاویر ،موزیک و بازی بین تلفن های همراه .

این تکنولوژی با پیشرفت های بیشتر و به روز رسانیهایی که در آینده خواهد داشت پایدار خواهد ماند که اکسر این به روز رسانیها در زمنیه افزایش سرعت ، امنیت و قیمت میباشد.

امنیت در BT

بیشترین چیزی که عموم مرد از پایه و مکانیزم امنیت این سیستم مطلع اند آنست که کاربر قادر به انتخاب حالت"Discoverable" و "non-discoverable" میباشد. و گمان میکنند که بدین صورت هیچ خطری آنها را تهدید نمی کند اما در ادامه این مقاله به راه هایی برای نفوذ اشاره خواهم کرد.

زمانی که BT در حالت Discoverable میباشد ، هر دستگاهی به راحتی میتواند به متصل شود و اطلاعات را رد و بدل کند . همین قسمت باعث میشه که میزان زیادی از افراد که هیچ اطلاعاتی در رابطه با امنیت ندارند ، مورد حمله قرار بگیرن. همونطوری که در شکل معلومه میتونید با گذاشتن یک تیک مانع از ظاهر شدن حالت دستگاهتون برای دیگر دستگاه ها بشید.

تنظیم BT در حالت non-discoverable مانع از اشتراک گذاری اطلاعات میشود .

اسکن کردن آدرسهای بلوتوسی

دستگاه تعیین هویت BT که از 48 بیت تشکیل شده بینظیر میباشد . IEEE جایی است که 3 بایت اول توسط دستگاه مخصوصی تعین میشود و 3بایت آخر هم به طور رایگان معین میشود. برای مثال ، نمایش شش گوشه یی آدرسهای بلوتوسی در گوشی Sony Ericsson P900 شبیه 00:0A:D9:EB:66:C7 میباشد.جایی که 3بایت اول آدرس (00:0A:D9) در IEEEو توسط Sony Ericsson ثبت میشود. این به این معنی میباشد که تمام گوشی های P900 3بایت آدرس بلوتوسی مشابه شروع میشن و 3 بایت آخر هم توسط خود Sony Ericsson در دستگاه معین میشه که این 3 بایت آخر در دستگاه های مختلف P900 فرق میکنه – اما ... .

در تئوری فعال کردن حالت non-discoverable در بلوتوس کاربر رو از ارتباطهای غیر مجاز حمایت میکند . ولی در عمل این حالت کلیه ارتباطهارو اعم از مجاز و غیر مجاز خاموش میکند . در اینجا نرم افزاری هست که دستگاه هایی رو که در حالت non-discoverable میباشد رو کشف میکند. یه مثال برای استفاده از Redfang توسط Ollie Whitehouse. یه کاربرد کوچیکش اینه که به سادگی میتونه یکی یکی به آدرس های بلوتوسی که شما به اون دادید متصل بشه تا که تعداد دستگاه ها در محدوده شما تموم بشه و در آخر هم دستگاه هایی که بلوتوس آن ها روشن هست رو نشون میده . این شیوه در بسیاری از عقاید در مقایسه با بسیاری از مهمترین ابزارها، که این روش را در خود جای داده اند از بین رفته، در ادامه دلیل این رو میفهمید . اصلیترین مانعی که بر سر راه این ترفند وجود دارد زمانی میباشد که برای پیدا کردن دستگاه های روشن میباشه. در بررسیهای انجام شده این عملکرد با دقت بالا و سطح عملیاتی خوب در مینیموم زمان، 6ثانیه میباشد (که در حالتهای دیگه به طور میانگین بین 2.5 تا 10 ثانیه متغیر است). این که در کمتر از 3 ثانیه بتونیم یک دستگاه روشن رو پیدا کنیم امکانپذیر است در عین حال ما تعدادی دستگاه رو به خاطر دقت کم اسکن و پیچیدگی در آن از دست خواهیم داد . بیاین این میزان زمان رو در اعداد بزرگتر حساب کنیم تا بهتر به این پی ببرید که زمان زیادی رو ما باید صرف اسکن این دستگاه ها کنیم. برای مثال تعداد آدرسهایی که در شرکت Sony Ericsson به ثبت رسیده 16777216 میباشد . اگر ما متوسط زمان که 6 ثانیه برای اسکن هر دسگاه میباشد رو فرض کنیم مدت زمانی که برای اسکن این میزان دستگاه نیاز داریم 1165 روز میباشد !!! و این به این معنی هست که ما بیشتر از 6 سال برای این عملیات و پیدا کردن دستگاه های مورد نظر وقت نیاز داریم . این مسلم که این میزان زمان برای یک هکر بسیار بسیار زیاد میباشه . حالا میگید چیکار کنیم؟ جواب اینکه یک ترفند وجود دارد که به ما کمک میکنه تا عملیات اسکنمون رو بسیار راحت تر از آنچه که گفته شد انجام بدیم.

تا به حال شده رو یه گوشی یه LED ببینید که داره چشمک میزنه ؟ تا به حال به خودتون گفتید که این چرا داره چشمک میزنه؟! درسته راه عملی که به کمک یه هکر میاد تا تشخیص بده بلوتوس در کدام دستگاه روشن و در کدام دستگاه روشن نیست همین راه که به اون LED قشنگه نگاه کنه .

ساده کردن آدرسها

در ابتدا باید این رو بگم که اگر شرکت سازنده دستگاه معلوم باشه بیدرنگ تعداد آدرسهای بلوتوسی محدود میشه . علاوه بر این بسیاری از شرکتهای سازنده هم آدرسهای قابل پیشبینی رو که به طریق رنج میباشد برای هر مدل از دستگاه هاشون انتخاب کردن که این کار مارو بازم آسونتر میکنه . برای مثال آدرس اکثریت گوشیهایه Sony Ericsson مدل P900 با این هفت رقم جادویی شروع میشه : 00:0A:D9:E ، و این به این معنی که فقط 5 عدد برای ما نامعلوم است. که این باعث میشه تعداد دستگاه هایی که ما می خواستیم اسکن کنیم از 16 میلیون به 1048576 برسه. علاوه بر این 4 بایت از اون آدرسهای P900 عملا در یک رنج مختصر و مفید بین E7-EE میباشد . به این دلیل تعداد آدرسهایی که ما میخواهیم اسکن کنیم باز هم کاهش پیدا کنه و به 524288 عدد برسه . اگر ما میانگین اسکنمون رو 6ثانیه فرض کنیم و بخوایم این تعداد دستگاه رو اسکن کنیم به 36 روز زمان نیاز داریم. همینطور که مشاهده میکنید این میزان زمان بسیار کمتر از زمان اولیه است که 1165 روز بود و جای کاستن بیشتر از این میزان آدرسها وجود ندارد و همونطور که مسلم است این زمان باز هم برای یک هکر زمانی زیادمیباشد. اینجا یه راه دیگه هم هست که با مثال واستون توضیح میدم. به نظر میاد که شرکت NOKIA برای گوشیهایش رندوم خوبی را توضیح کرده است ولی بسیار شگفت آور میباشد . میتونیم تعدادی گوشی P900 را پیدا کنیم که دارای آدرس یکسانی باشند که این آدرس 11:11:11:50:11:11 .

ما فقط نمیتونیم با انتخاب هدفمون میزان زمان اسکن رو کاهش بدیم ، بلکه میتونیم با افزایش سرعت اسکن زمان کمتری رو صرف اسکن کنیم . مثلا میتونیم با استفاده از RedFang (V2.5)که دارای مولتی اسکن میباشد و به کاربر خودش اجازه میده تا با استفاده از چند دانگل بلوتوسی اسکنش رو انجام بده و ما با استفاده از این راه میتونیم میزان زمان برای اسکن کاملمون رو کاهش بدیم . اگر ما فقط از 8 عدد USB دانگل بلوتوسی استفاده کنیم بعلاوه روشهایی که گفته شد در بالا میتونیم تمام دستگاه های مورد نظرمون با رنج کردن فقط در 4 روز و نیم پیدا کنیم . درسته بازم این زمان زیادی ولی با استفاده از اولین روشی که گفتم (LED) میتونیم دستگاه هایی که در حالت non-discoverable هستند رو از رنجمون جدا کنیم و میزان زمانمون رو بسیار کمتر از 4 روز و نیم بکنیم . البته بعید نیست که در آینده نزدیک راه ها و ابزارهای بهتر و سریعتری برای اینکار ابداع بشه .

پیدا کردن آدرس در هنگام مکالمه

آدرسهای بلوتوسی رو در هنگام ارتباط بلوتوسی نیز میشه پیدا کرد . این آدرسها به خودی خود مخفی نیست حتی اگر کاربر اون رو در زمان ارتباط مخفی کنه . این یکی از بزرگترین ایرادهای این سیستم سودمند هست. بسامد فرکانسها که 1600 در ثانیه میباشد مانع از ایجاد زمینه برای مخفی شدن آدرس دستگاه در هنگام ارتباط میشود . به هر حال در سیستم بلوتوس از بسامدهای متوالی فرکانس استفاده شده است و این به این معنا میباشد که یک هکر که دارای تجهیزات کامل هست میتونه همزمان و با استفاده و سرمشق گرفتن از فرکانسهای از پیش تعیین شده وارد ارتباط بین دو دستگاه شود. افزون بر این بسامد ها در پیکونت در میان تمام دستگاه ها تقسیم شده که شاید این عمل برای یک هکر بیشتر مفید باشه. و قابل ذکر هست که در سالهای قبل دستگاه هایی در مراکز تجاری وجود داشت که میتونست ارتباطات بلوتوسی رو از هوا بگیره و اونهارو آنالیز کنه، امروزه قیمت این دستگاه ها بسیار زیاد میباشد (تقریبا 9500$) که این میزان برای هکرهای معمولی بسیار بالا هست . اما دستگاه های خوبی که به درد یه سری افراد و ارگان ها میخوره (مثل سازمان جاسوسی CIA که برای بدست آوردن یه سری اطلاعات این پول واسشون هیچه !

بسیاری از هکرها میتونن به راحتی احساس کنن که فلان گوشی در حالت Discoverable هست یا نه. الان بهتون میگم چجوری ، قبل از استفاده کردن از ارتباط بلوتوسی ما باید گوشیمون رو در حالت Discoverable قرار بدیم و زیاد اتفاق میافته که فرد پس از پایان ارتباط فراموش میکنه که باید دستگاهش رو از حالت Discoverable در بیاره و این یه فرصت خوب برای یه هکر خوبه . بدین صورت یه هکر خوب راحت میتونه به گوشی مورد نظرش متصل بشه و آدرس اون رو بدست بیاره. هیچ گوشی در مراکز بزرگ تجاری برای ارتباط بلوتوسی به صورت دستی در دسترس نیست این به این معنی که یه دستگاه همیشه ارتباطها رو جذب میکنه و مانع از رسیدن اون به مقصد اصلیش میشه . از طرفه دیگه آدرس بلوتوسی یک دستگاه ثابت هست و نمیتونه خودش را با کاربرش تطبیق بده و آدرس خودش رو عوض کنه و در اینجاس که فقط به یه مهاجم نیاز داریم که اون آدرس رو برای دفعه اول پیدا کنه که میتونه برای همیشه به اون دستگاه حمله کنه . و در این جاس که شما میتونید ببینید که فقط یه لحظه کوتاه برای یک هکر نیاز هست تا به دستگاهی که در حالت Discoverable هست نفوذ کنه و تا وقتی که طرف مقابل دستگاه رو خاموش نکنه میتونه به اون دستگاه متصل بشه و هرچی که میخواد بدست بیاره و دستگاه مقابل هم نمیتونه کانکشنی که بهش وصل شده را بلوک کنه . به خاطر اینه که عوض کردن سیم کارت فایده ای نداره و گوشیها هم به راحتی ارتباطهایی که از طرف کاربر که به صورت L2CAP است رو بدون هیچ تقاضای از پیشی قبول میکنند. متاسفانه شایانه ذکر هست که گوشیهای موجود که اکثر مردم از انها

استفاده میکنن قابلیت محدود کردن ارتباطهای سطح پایین L2CAP ندارند و نمیتونند این ارتباطهارو سد(بلوک) کنن. برای همین است که بهتره فایروال گوشی رو در حالت Default قرار ندیم.

امنیت و متد در بلوتوس

توبه این قسمت یک کم به امنیت میپردازیم و میگیم که برای افزایش امنیت چه کارهایی میشه کرد . البته به قول دوستان امنیت حد و مرز نداره ولی ما میتونیم با انجام دادن چند کار، امنیت رو تا حدی بالا ببریم که حد اقل از دست گروهی از هکرها (جوجه هکرها)راحت بشیم !

هیچ وقت تنظیمات اولیه نمیتونه به طور کامل موثر باشه و ما با کمی دستکاری میتونیم اون رو در بهترین وضعیت قرار بدیم . در تنظیمات اولیه ، هر دستگاهی میتونه به راحتی با دستگاه شما ارتباط برقرار کنه و این کمی نا خوشاینده . شما میتونید دستگاهتون رو طوری تنظیم کنید که هر فردی که خواست با دستگاه شما ارتباط برقرار کنه و فایل یا شماره تلفن و یا هرچیز دیگه ای رو از دستگاه شما بگیره یا به دستگاه شما بفرسته، دستگاه برای این ارتباط نیاز به رمز عبور داشته باشه . درواقع هر کسی که میخواد با دستگاه شما ارتباط برقرار کنه بایدرمز عبوری که از قبل توسط دستگاه مشخص شده رو بده و بعد از دادن این رمز میتونه به دستگاه شما متصل بشه و بیتونه فایل مورد نظر رو رد و بدل کنه . و فرد مقابل هر بار که بخواد با دستگاه شما ارتباط برقرار کنه باید اون رمز عبور رو که شما واسه اون فرد تایین کردید رو بده و این راه تا حد زیادی میتونه امنیت شما رو بالا ببره و مانع از ارتباط هر کاربر با دستگاه شما بشه.

نسخه Vendor

متاسفانه فرایند تصدیق و سرویس اجازه به دسترسی به طور صحیح توسط سازنده ها تکمیل نشده. بعضی از این ضعف ها در محصولات شرکت های تولید گوشی همچون Sony Ericsson و Nokia دیده شده که این ضعف ها باعث میشه تا یک هکر به راحتی بتونه با استفاده از سرویس بلوتوس به دفترچه تلفن ، عکس ها ، اطلاعات سالنامه دسترسی پیدا کنه و حتی با افرادی که میخواد مکالمه کنه و یا به آنها SMS بفرسته . برای اینکه بفهمیم میزان این حفره چقدر خطرناک میتونیم فرض کنیم که یک هکر تونسه به گوشی ما متصل بشه و با استفاده از دفترچه تلفنمون شماره دوستانمون رو پیدا کرده و با استفاده از خط

شما برای اونها مزاحمت ایجاد کرده و یا حتی ارگانهای دولتی را با استفاده از SMS بمباران میکنه . با دریافت صورت حساب گوشی حتما متوجه میشید که تمامی اون مزاحمت ها و تمام اون SMS ها از گوشی شما بوده و شما هم نمیتونید فرستنده ی اصلی اون SMS ها رو شناسایی کنید چون دستگاه شما نمیتونه شماره دستگاه هایی رو که از طریق سرویس بلوتوس به دستگاه شما متصل شدن رو ذخیره کنه و اوضاع زمانی بدتر میشه که دستگاه شما میزان زیادی SMS رو برای دوستانتون فرستاده و اون SMS ها هم حاوی کلمات ..... هست .

میزان آسیب پذیری گوشیهای Sony Ericsson و Nokia رو در بالا دیدید ، همچنین این آسیب پذیری رو میشه بدونه هیچ تخصص خاصی در گوشی مورد نظر پیدا کرد . در واقع هر کاربری که به میزان لازم از راه های نفوذ و بلوتوس و طریقه کار با اون اطلاعات داشته باشه میتونه با استفاده از Linux آسیب پذیری هایی رو پیدا کنه. در این جا هم دو دستور برای سرقت دفترچه تلفن در گوشی T610 معرفی میکنم :

```
# hcitool scan
Scanning .

00:0A:D9:15:0B:1C T610-phone
```

```
# obexftp -b 00:0A:D9:15:0B:1C --channel 10 -g telecom/pb.vcf -v
Browsing 00:0A:D9:15:0B:1C ...
Channel: 7
No custom transport
Connecting...bt: 1
done
Receiving telecom/pb.vcf...\done
Disconnecting...done
```

این دستوری هست که شما با استفاده از اون میتونید اطلاعات دفترچه تلفن یک گوشی فاقد امنیت T610 رو سرقت کنید. شما با استفاده از هر دو دستور hcitool و obexftp (دستورات استاندارد در بلوتوس هستند)،استفاده از سیستم عامل Linux و استفاده از بسته استاندارد بلوتوس میتونید این سرقت رو انجام بدید.

قابل ذکر هست که این آسیب پذیری توسط آدام لاری (Adam Laurie) کشف شده و در گوشیهای نوکیا مدل : 6310، 6310i ، 8910 و 8910i و در گوشیهای Sony Ericsson مدل : T68،T68i، R520M ،T610 و Z600 کاربرد داره و به احتمال زیاد در آینده مدل های دیگه ای هم به این لیست اضافه میشه . این آسیب پذیری توسط تیم trifinite.group به طور وسیع آزمایش شده و به اطلاعات دیگه ای هم

رسیده اند که اگر تمایل دارید تا از اونها اطلاعی داشته باشید میتونید به آدرس اینترنتی این تیم : http://trifinite.org/trifinite_group.html مراجعه کنید.

با یک اسکن درست و حصابی میتونید آسیب پذیری هایی رو در یک سری از گوشیها مشاهده کنید . زیاد واستون عجیب نیست وقتی که در حیاط خونتون گوشیهای قدیمی که فاقد پیشرفت روز هستند و فقط میتونند شماره بگیرن و ارتباط برقرار کنن یا SMS بفرستن ، نتونن خوب جواب بدن و به تناسب خودش دارای ایرادهایی هست و هیچ انتظاری هم از آپدیت این نوع گوشیها نه از لحاظ نرم افزاری و نه از لحاظ سخت افزاری نیست ولی وقتی متعجب میشید که یه گوشی رو میبینید که از هر لحاظ آپدیت هستش و بعد از اینکه اون رو یه اسکن می کنید متوجه میشید که این دستگاه دارای ایراد های هستش . حالا فکر میکنید این ایرادها از کجان ؟ از اون جایی که شرکت های سازنده پس از ساخت دستگاه هاشون اونهارو فقط یک تست اولیه ساده میکنن (مثل همین ماشینهای ایران خودرو که خیلی قشنگ تست میشن و هیچ مشکل فنی ندارن !)و اون محصول رو روانه بازار میکنن . و باید گفت که به احتمال قوی در این دستگاه ها در آینده آسیب پذیری های امنیتی توسط متخصصان امنیتی در این زمینه کشف خواهد شد که حتما میزان آسیب پذیری ها بسیار بالا خواهد بود .

خطر AP تقلبی

یکی از خطرهایی که میتونه وجود داشته باشه ، اینه که در لیست دستگاه هایی که از طریق بلوتوس به شما متصل هستند فقط نام اونها ذکر میشه نه آدرس بلوتوسیشون که شما میتونید این رو به صورت واضح در عکس مقابل مشاهده کنید.

همینطوری که در مقابل مشاهده میکنید ، نام دستگاهی که از طریق بلوتوس به دستگاه ما متصل هست ، ULTOR نام داره . شما میتونید با استفاده از این اسم با هر دستگاه دیگه ای به ما متصل بشید و اطلاعات مورد نیازتون رو دریافت کنید و ما هم فکر میکنیم شما همون ULTOR اصلی هستید . اگر دستگاه ما در لیست خودش میتونست آدرس دستگاه مقابل رو بده خیلی بهتر بود و ما با استفاده از این روش میتونستیم مانع از اتصال دستگاه های دیگه با نامی که برای ما آشناس بشیم . همین اشکال کوچیک در سیستم بلوتوس میتونه در راه های مختلفی استفاده بشه و ضرر هایی رو از لحاظ مادی و معنوی بزنه به خصوص در سرویس های عمومی که از بلوتوس استفاده میکنن. به عنوان

مثال سرویس بلوتوس اینترنت اکسس میتونه توسط همین مشکل و استفاده از AP تقلبی مورد حمله قرار بگیره . این دستگاه میتونه از یه اسم که برای اکسس پوینت به کار رفته استفاده کنه و خودش رو جای اون به سیستم معرفی کنه و با کمی کار کردن بر روی رمز عبور اون دستگاه می تونیم رمز عبور رو بدست بیاریم که برای دوستانی که تو کار بدست آوردن رمز عبور هستن ، کار مشکلی نیست. به هر حال در طول ارتباط دستگاه با سرویس بلوتوس اینتریت اکسس میتونیم اطلاعات رو کپچر کنیم و بعد از آنالایز اونها میتونیم از اونها استفاده کنیم که توی این اطلاعات بدست اومده همه چیز میتونه باشه.

این نوع حمله رو میشه از راه های مختلفی انجام داد ، برای مثال در بعضی کشورها کیوسک هایی برای کاربران تلفن همراه وجود داره که افراد میتونن در اون مکان ها زنگ گوشی ، بازی و ... رو از طریق بلوتوس دریافت کنن. ما میتونیم زنگ یا بازی خودمون رو در خواست و از همین طریق بلوتوس دریافت کنیم و توی دلمون میگیم خدا پدر و مادر کسی که این دکه رو راه انداخت بیامرزه. حالا شما ببینید چند نفر آدم همزمان توی اون دکه هستند و می خوان فلان بازی یا زنگ که جدید هست رو دریافت کنن . وقتی که در لیست شما اسم "Mobile-Kiosk" میاد شما فکر میکنید که تا چند لحظه دیگه شما هم صاحب اون بازی جدید میشید . حالا بپردازیم به مشکل این کار، شما از کجا مطمئنید که اون اسمی که در لیست شما وجود داره تقلبی نیست و دستگاه دیگه ای به دستگاه شما با اسم "Mobile-Kiosk" متصل نشده؟ همونطوری که قبلا گفته شد شما هیچ اطلاعاتی رو در مورد اینکه این همون دستگاهی هست که شما میخواستید یا نه ندارید چون آدرس بلوتوسیش رو نمیتونید ببینید. شاید یه هکر با استفاده از اون اسم و با استفاده از کامپیوترش در همون دور و ورا عوض اینکه اون بازی جالب رو واستون بفرسته داره یه ویروس یا چیز دیگه ای که به هر حال واستون ضرر داره رو میفرسته . گاهی اوقات هم بعضی از این حمله ها توسط بعضی از عوامل و ابزارها که به طور خصوصی در اختیار تک و توک این کیوسک ها هست خنثی میشه ولی بیشتر این نوع کیوسک ها دارای ساده ترین ابزارها هستند و رمز عبورشون هم همیشه ساکن و بدون تغیر هستش.

مهندسی عمومی بلوتوس

فناوری بلوتوس توسط انسان ها استفاده میشه و انسان هم جایز الخطاس و با داشتن کمی اطلاعات در این زمینه میشه حملاتی رو به سادگی انجام داد. از جمله این اطلاعات که میتونه به یه هکر کمک کنه میشه به آشنایی با امنیت پایه در بلوتوس ، آشنایی با عموم کاربران و سلایق انها و داشتن اطلاعاتی در رابطه با بلوتوس که بتونه در مراحل مختلف مارو کمک کنه میشه اشاره کرد. با یه آزمایش کوچیک در این زمینه ها شما میتونید اطلاعات مورد نیاز رو در زمینه مهندسی عمومی در بلوتوس بدست بیارین و حملات

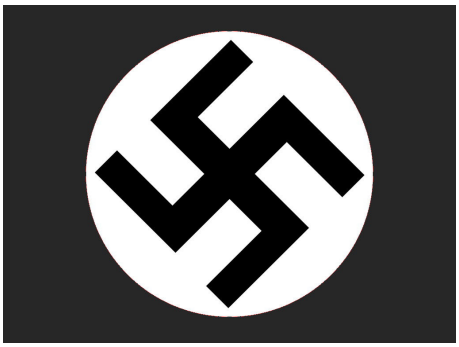
خودتون رو بهتر انجام بدید.که من یه آزمایش کوچیک رو در پایین انجام دادم که میتونید اطلاعات مختصری رو بهتون بده.

توی این آزمایش اسم کامپیوتر من "Mobile-Kiosk" بود و ما میخوایم به دستگاه هایی که در یکی از اون دکه هایی که در بالا راجبش صحبت شد و در اونجا تمامی گوشیها به اجبار در حالت Discoverable هستند حمله کنیم . توی این مدتی که من در کمین بودم تونستم 11 دستگاه رو که فاقد امنتی بودن رون رو شناسایی کنم و به همشون تونستم متصل بشم .به غیر از یکیشون ما بقی کلمه عبور نداشت و همون یکی هم رمزش 1234 بود ، این در حالی بود که من به هدست اونها وصل شده بودم و به مکالمات تعدادی از اونها داشتم گوش میدادم ! تو مدتی که من به این دستگاه ها متصل بودم تونستم دفترچه تلفنشون رو یه مرور کنم ، صندوق SMS رو نگاه بکنم و SMS هاشون رو بخونم یا برای دوستانم از طریق گوشی اونها SMS بفرستم و ... .

این نوع حملات به افرادی که هیچ اطلاعاتی رو در زمینه امنیت ندارن و کاراشون هم .... میتونه خیلی خطرناک باشه . این افراد بدون اینکه هیچ اطلاعات خاصی رو در رابطه با امنیت داشته باشن هر ارتباط رو قبول میکردن و به راحتی دستگاهشون رو در اختیار من میذاشتن . از این افراد کم نیستن و با کمترین مشکل میشه به دستگاه اونها متصل شدو از این خرابکاریها کرد.

خلاصه مطالب در قسمت اول

در قسمت اول به معرفی سیستم بلوتوس ، توضیحی در رابطه با افزایش امنیت در این سیستم ، شرح تعدادی از دستورهایی که میتونه در رابطه با هک این سیستم کاربرد داشته باشه و مهندسی اجتماعی در بلوتوس پرداختیم. در قسمت دوم به توضیحی در رابطه با آسیب پذیری های دیگه ای در بلوتوس ، انواع مختلف بلوتوس (آنتن) ، چگونگی وارد شدن به دستگاه دیگران و در آخر هم اطلاعاتی رو راجب کرم هایی که به تازگی وارد این دنیا شدن و خودشون رو از طریق این سیستم پخش میکنند خواهیم پرداخت.



نکته : این نشانه که صلیب (چلیپا)شکسته نامیده شده است ، در حقیقت صلیب شکسته نیست ، نام آریایی آن گردونه مهر میباشد و نماد دین میترا که به 1400 سال پیش از میلاد مسیح در ایران میرسد، بر میگردد . به احتمال زیاد این نشان از ایران بر اثر ارتباط سیاسی و نظامی دوران باستان به یونان رفت و سپس نازی ها در دوران نیرومندی خود که تعصب و فلسفه نژادی را میستودند ، تبلیغات و آموزش های خود را متوجه این کار کردند و به این نشان ارزش سمبولیک آریایی بودن خود دادند .