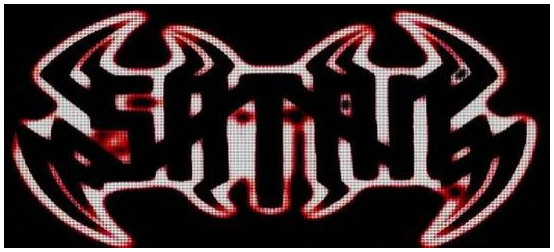
Blue Tooth

Author : Sir.Hitler

The First And The Best Persian Journal About BlueTooth

Satanic Hell & Shabgard



جهنم شیطانی و شبگرد

Bluetooth

مباحثی پیرامون بلوتوس (قسمت دوم)

نویسنده: **Sir.Hitler**

تاریخ: **June 17/2006** **1385/3/27**

ایمیل:

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

با تشکر فراوان از :

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

فهرست

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 گیرند.

تمامی حقوق مادی و معنوی این مقاله در اختیار نویسنده و 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

خجسه باد نام خداوند که نیکوترین آفریدگاران است

و نام تو که نیکوترین آفریدگانی (آریا)

در قسمت اول از این مبحث ما به چگونگی تولد این فناوری ، مشکلات امنیتی و چند دستور برای نفوذ اشاره کردیم . حالا در قسمت دوم میخوایم به شما خوانندگان عزیز مطالب بیشتری رو در رابطه با ویروس هایی که با استفاده از این فناوری خودشون رو گسترش میدن ، تعداد دیگه ای از حفره های امنیتی کشف شده و در نهایت مطالبی در رابطه با چگونگی پیدا کردن "Blue Tag" و موقعیت یابی اشاره کنیم .

Bluetooth Fauna

زمانی که کرم گوشی کبیر (Cabir) شروع به پخش و گسترش خودش میکنه ، بسیاری از مردم متحیر خواهند شد ! این کرم در ابتدا به صورت ویروس توسط گروه A29 نوشته و برای یکی از شرکت های ضد ویروس فرستاده شد ، سپس در دنیای مجازی شروع به گشترش کرد . این کرم در مرحله اول دستگاه هایی که دارای بلوتوس هستند و شرایط خوبی رو برای پیدا کردن قربانی بعدیشون دارند رو شناسایی و آلوده میکند و بدین طریق خود را گسترش میدهد. این کرم خوش رو از طریق حفره هایی که در گوشیهای NOKIA و Sony Ericsson وجود داره گسترش میده . این ویروس اونمقدار هم خطر نداره ! تنها کاری که میکنه باطری گوشیتون رو خراب میکنه . به هر حال این ویروس نشون میده که میتونه خودش رو از طریق بلوتوس پخش کنه و در آینده هم میتونه تعداد این نوع ویروس ها افزایش پیدا کنه ، حتی این ویروسها ممکن است از ویروسی که الان بهش اشاره کردیم خطرناکتر باشه و حتما خسارتهای جبران ناپذیری رو به همراه خواهد داشت . یه مثال خوبی که میتونیم در این رابطه بزنیم اینکه در سال 2001 در کشور ژاپن ، ویروسی ظاهر شد که خودش رو از طریق بلوتوس پخش میکرد و هنگامی که در دستگاهی میشست ، مانع ارتباط صاحب اون دستگاه با شماره های ضروری مثل اورژانس ،پلیس و ... ! حالا حصاب کنید که گاهی اوقات این ویروسها چقدر مشکل ساز خواهند شد . جدیدا توسط Adam Gowdiak که جز مسئولین

یکی از تیم امنیتی هست ، حفره ای در جاوا پیدا شده که ویروس ها میتونن از طریق این حفره سیستم امنیتی گوشی هارو از کار بیندارن و تغیراتی رو در حافظه دستگاه بدن که نتیجش اینکه هرچیزی که در گوشی ذخیره کردید تغیر خواهد کرد !

*بنابراین افزایش اینگونه کرمها و ویروسها مشکلاتی رو برای GSM (اپراتورشون) ایجاد خواهد کرد . سد کردن شماره ها و ناتوانی در برقرار کردن ارتباط مشکلاتی رو در جامعه خواهد داشت که این به سود اپراتور نیست . همینطور مشکلاتی رو برای کاربران ، از جمله اینکه احتمال داره که یک بکدور هم روی هندست نصب شده باشه و بدین ترتیب امنیت کاربر هم خدشه داره میشه و یک هکر با استفاده از این میتونه از طریق بلوتوس یا GPRS بر گوشی مسلط بشه و بتونه از اطلاعاتی که درگوشی هست استفاده کنه.

حملاتی که از سوی ویروس Mabir انجام میشه رو نمیشه به وضوح دید ، یعنی اینکه شما متوجه آلودگی در گوشی نمیشید و تنها متوجه یکسری اعمال غیر عادی در دستگاه میشید . Cabir هم که یه طورهایی جانشین این ویروس Mabir هست ، جدیدا برای شیوع و گسترش خودش هم از بلوتوس استفاده میکنه و هم از MMS و این هم بسته به شرایط گوشی قربانی هستش ، هر کدوم از روشها کارسازتر باشه با همون روش خودش رو پخش میکنه . زمانی که SMS برای دستگاهی میاد که حامل این ویروس هست ، اون ویروس یک MMSی رو برای دستگاه ارسال کننده SMS میفرسته و بدین ترتیب خودش رو پخش میکنه . و این تکنیکی هوشمندانه وجالبه که نویسنده این ویروس اون رو ابداع کرده ، الحمد الله در ایران بازار SMS بازی گرم و اینقدر مردم علاقه پیدا کردن که امکان داره SMS جکی رو که فرستادی برای یکی از دوستات همون SMS رو چند ساعت بعد از چندتا دیگه از دوستات دریافت کنی ،حالا فکر کنید که یکی از این گوشیها حاوی این ویروس بوده ، یه بازار خوبی رو برای هکرها و سرویس دهندگان گوشی فراهم کرده ، هکرها از اطلاعات در دستگاه سود *میکنن ، سرویس دهنده ها هم از فروش باتری ! مقایسه ها نشون داده که اکسر ویروسهایی که خیلی خطرناک هستن یا از طریق کامپیوتر های حاوی حفره وارد گوشیها شدن

و یا از طریق دانلودهایی که از سایتها انجام میشه ! بدین ترتیب خودشون رو پخش کردن ، بنابراین یکم مواظب سایتهایی که از توش برای گوشیتون بازی ، آهنگ و ... پیدا میکنید باشید . در رابطه با راه اول هم ما یکسری حفره ها رو برای آشنایی بیشتر شما دوستان معرفی میکنیم .*

معرفی آسیب پذیریها و استفاده از آنها

انسان جایز الخطاس و در تمام کارهاش اشتباهاتی رو مرتکب میشه . بنابراین تمامی ساخته های بشر دارای نقایصی هست . در این مبحث ما میخوایم به تعدادی از این اشتباهات که منجر به، به وجود آمدن حفره هایی در فناوری بلوتوس شدن اشاره کنیم . در این قسمت به یکی از حفره های کشف شده در گوشی Sony Ericsson مدل P900 در قسمت Beamer application اشاره خواهیم کرد .

این حفره که میخوایم به شما معرفی کنیم ، بسیار جزئی هست ، ولی اگر استفاده کننده بتونه به نحو صحیح ازش استفاده کنه برای فردی که این حفره در دستگاهش هست ،بسیار خطرناک خواهد بود.

زمانی که شما فایلی رو برای دستگاهی که دارای این آسیب پذیری هست ارسال میکنید ، دستگاه از obexftp و Obex File Transfer یا OBEX Object Push استفاده میکنه ، درصورتی که ریموت نیم فایل از 197 کاراکتر بیشتر باشه ، Beamer application اون رو تکه تکه میکنه و به جای اون USER Panic 11 رو قرار میده ، مثل عکس بالا .

نتیجه ای که برای شما به دنبال داره اینکه شما میتونید با استفاده از خط 743 obexftp client.c (obexftp 0.10.6 version) میتونید فایلتون رو با بیش از 197 کاراکتر برای قربانی بفرستید .

```
---- snip ---
object = build_object_from_file (cli->obexhandle,localname, \
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
\
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
A \
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
A");
---- snip ---
```

بعد از تلفیق کد بالا با فایلتون میتونید به سادگی از اون در obexftp استفاده کنید .

```
# ./obexftp -b 00:0A:D9:E7:0B:1D --channel 2 -p /etc/passwd -v
```

بعد از اینکه اون رو در obexftp اجرا کردید ، در گوشی قربانی Beamer فایل رو به صورت USER Panic 11 در میاره . دلیلشم اینکه زمانی که اطلاعات در 16 بیت متغیر descriptor کپی میشن ، این مقدار اطلاعات از حداکثر فضا برای دریافت این اطلاعات بیشتر هست و برای اینکه در عمل رد و بدل مشکلی پیش نیاد خود دستگاه اون رو به صورت USER Panic 11 درمیاره .

سرریز descriptor یکی از موارد آسیب پذیری در بیشتر گوشیها هستش .

Nokia 9500 vCard Bug

یکی از مواردی که شبیه Descriptor هستش رو میتونید در گوشیهای Nokia 9500 مشاهده کنید . زمانی که فردی در حال خوندن یک vCard هستش . (به خاطر اینکه اطلاعات زیادی در رابطه با این باگ در دستم نیست ، توضیحی رو در این رابطه میدم ،امیدوارم اکتفا بکنه)

حالا بریم سراغ vCard ببینیم چی هست ؟ توضیح خیلی مختصرش این میشه که این کارت ، کارت الکترونیکی بیزنیس (تجارت) هست . این کارت حاوی اطلاعاتی از قبیل ، اسم شخص ، آدرس ، شماره تلفن و ... چیزهایی تو این مایه ها . استفاده vCard ها در گوشیهایی است که دارای بلوتوس هستند . کارشون اینکه اطلاعات رو بین دو دستگاه و با استفاده از

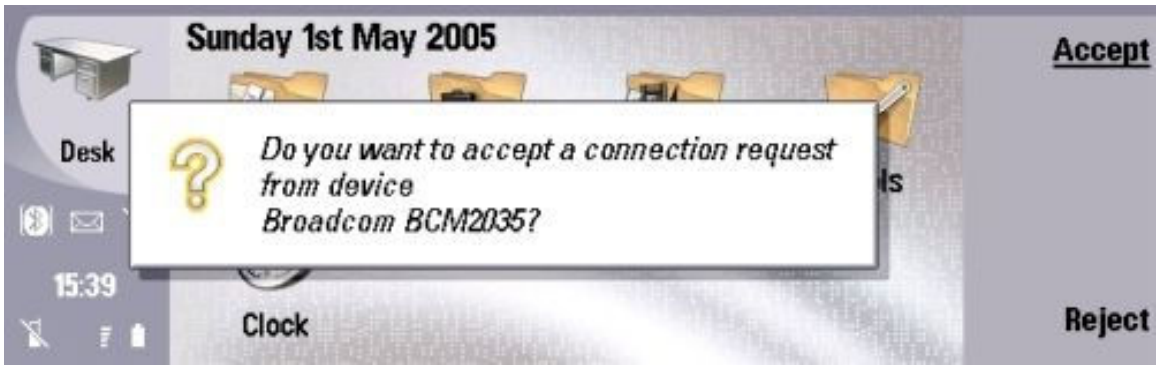
PIM Item Transfer (OBEX Object Push رد و بدل میکنند ، که این فناوری توسط گوشیهای Nokia9500 ساپورت میشه . به هرحال این کارت جالب دارای حفره هایی هستش که کوچک هستند ، ولی با یکم فکر میشه استفاده های بزرگی ازشون کرد.

زمانی که شما یک vCard رو باز میکنید که اسم اون از 245 کاراکتر بیشتر هست(N:Field) بیشتر هستش ، Nokia9500 اون رو تکه تکه میکنه و نتیجش میشه user panic11 . مثل همون خطایی که در گوشی P900 بهش پرداختیم .
حالا یکی از این vCard هارو در پایین میبینید(محتویاتش) :

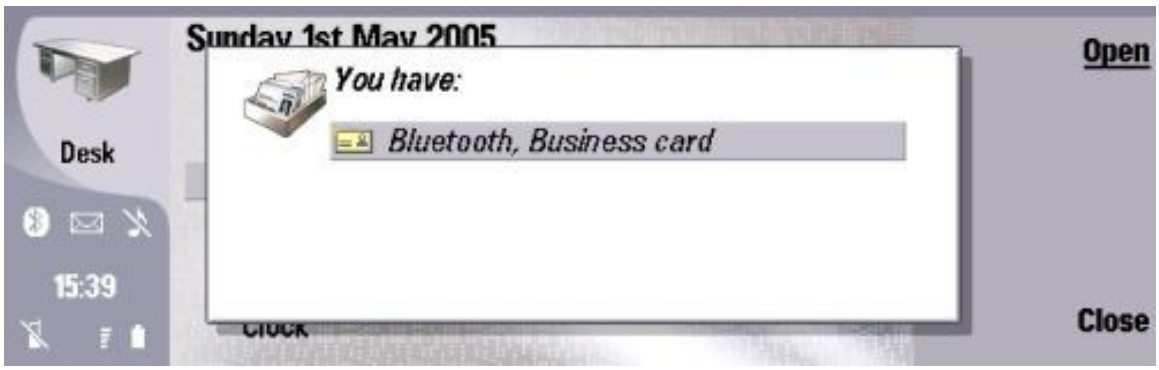
```
--- Nokia9500.vcf ---
BEGIN:VCARD
VERSION:2.1
N:AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA \
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA \
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA \
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA \
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA;BIALOGLO
WY
FN:Marek Bialoglowy
ORG:INDEPENDENT
TITLE:COO
TEL;WORK;VOICE:+6221
TEL;WORK;FAX;
ADR;WORK;ENCODING=QUOTED-PRINTABLE:;;Indonesia
LABEL;WORK;ENCODING=QUOTED-PRINTABLE:Indonesia
URL;WORK;
EMAIL;PREF;INTERNET:bialoglowy@gmail.com
REV:20050430T1958490
END:VCARD
--- Nokia9500.vcf ---
```

برای اینکه بتونیم نتیجه هایی رو از این نفوذپذیری بدست بیاریم ، اول یک vCard که اطلاعاتی مثل اطلاعات در بالا رو داره ،رو از طریق بلوتوس برای دستگاه مورد نظر ارسال میکنیم . در طول مدتی که من داشتم این کار رو انجام میدادم ،برای تست ، یک vCard رو وارد Microsoft Outlook کردم و از این طریق اون رو با بلوتوس ارسال کردم .

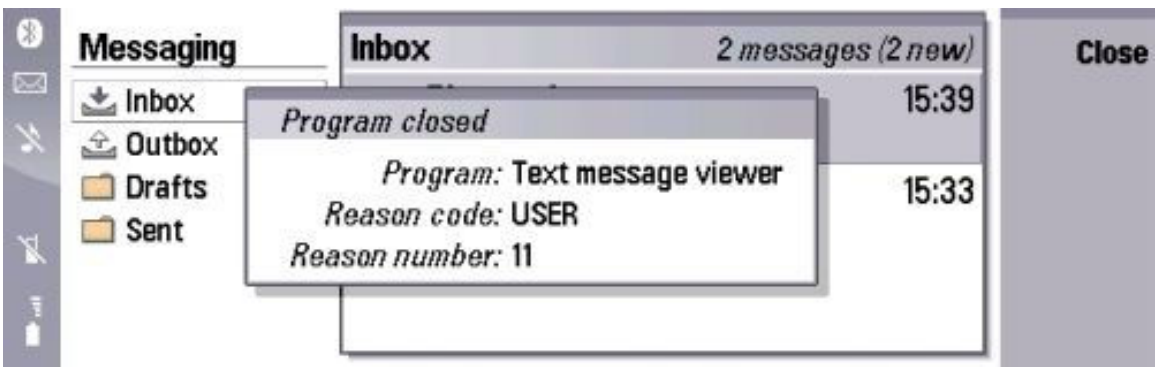
در این مرحله ، نیاز دستگاه کاربر رو برای دریافت اطلاعات vCard میبینید که از شما اجازی این کار رو میخواهد . همموطوری که در شکل پایین مشاهده میکنید.



اگر درخواست ،مبنی بر دسترسی به vCard پذیرفته بشه ، اطلاعات vCard برای کاربر ارسال میشه . همونطوری که در شکل پایین مشاهده میکنید.



چند ثانیه بعد از اینکه فرد اطلاعات vCard رو دریافت کرد ، اون رو باز میکنه و چیزی رو که شما در عکس زیر مشاهده میکنید مشاهده میکنه .



از این نفوذ پذیری ، خوشبختانه یا بدبختانه نمیشه بهره برداری درستی به نفع کاربرها کرد. میشه از این به عنوان یک پشته ، در بسیاری از سریزهای بافر که رواج دارن استفاده کرد. افزون بر اینکه با این کار ، میشه کاربر رو از لحاظ امنیت ، به پایینترین سطوح کشوند. بنابراین Symbain OS باید طرحی رو برنامه ریزی بکنه که دستگاه رو در هر حالتی ، حتی در مواقعی که بالا ذکر شد ، بتونه امن نگه داره و از ارتباط با این جور برنامه ها ممانعت بکنه. احتمال خیلی کمی هم داره که فردی پیدا بشه و از این آسیب پذیری به طوری مثبت استفاده بکنه ! در این رابطه صحبت کردن هم خیلی جالبه ، ولی به خاطر اینکه هدف ما از نوشتن این مقاله ، چیز دیگه ای هست ،دیگه وارد جزئیات این قسمت نمیشیم .

اتصال بدون اجازه

برای اینکه در رابطه با این آسیب پذیری بیشتر توضیح بدیم ، دوباره سری به ES P900 میزنیم . افزون بر اینکه آسیب پذیری Beamer ، برای اینکه ما بفهمیم فایل مورد نظر بدون اجازه از کاربر در این گوشی ارسال یا دریافت شده خیلی مهم هستش .
در هنگام تست روی این گوشی ، بعد از اینکه فایل رو فرستادم ، دستگاه از من درخواست کرد که Pin رو وارد کنم ،بعد از چند بار کنسل کردن ، و تقاضای ارتباط دوباره ، دستگاه بدون اینکه از من PIN رو بخواد ، فایل رو قبول میکرد ، بدون اینکه کاربرش بدونه ! قابل ذکر که این تنها راه برای ارتباط بدونه اجازه نیست ، اکثر اوقات ، فایلهایی که فرستاده میشن ، بدون اینکه کاربر بدونه قبول میشن ، دلیلشم اینکه دستگاه از OBEX Objet Push (channel2) برای ارسال و دریافت فایل ها و اطلاعات استفاده میکنه . دلیل این نفوذ پذیری به نظر میاد این باشه که ،OBEXFTP خیلی سریعتر از Symbain OS هستش و این میزان سرعت هم مشکلاتی رو ایجاد کرده . به هر حال این واضح که خیلی از دوستان (هکر های عزیز) با استفاده از این نفوذ پذیری ها میتونن با دستگاه مورد نظرشون ارتباط برقرار بکنن و هرکاری که خواستن برروی اون انجام بدن ،البته مشروط براینکه بلوتوس روشن

باشه و در حالت Disvoverable و البته این دستگاه آپدیت نشده باشه و این آسیب پذیری ها فیکس نشده باشه .

بلوتوس دارای 3 مد مختلف :

1- دستگاه میتونه با تمام دستگاه ها بدون نیاز به خبر کردن و حتی دریافت اجازه از کاربرش ، ارتباط برقرار بکنه و فایلها رو ارسال و دریافت کنه. (میشه یکی واسه کسایی که دستگاه رو رو این حالت قرار میدن ،امنیت رو به طور کل تعریف کنه ؟)

2- در این حالت دستگاه برای ارتباط ، از کاربرش اجازه میخواد و تا وقتی که فرد اجازه نده هیچ فایلی رو ارسال و یا دریافت نمیکنه . (امنیت معمولی !)

3- تو این قسمت هم که دیگه کاربر میتونه همه جور مانع سر راه بذاره تا فقط افرادی که میخواد ،بتونن با دستگاه ارتباط برقرار بکنن .

از اونجا که ایرانیها مردمانی راحت طلبن ، مطمئین باشید که از هر 10 نفر ، فقط یکیشون حالت دوم رو انتخاب کرده ،ما بقی حالت اول رو انتخاب کردن همون OBEX . همونطوری هم که گفتم ، به خاطر راحت طلبی هیچ کدوم حالت سوم رو انتخاب نمیکنن ، مگر چی بشه و یه استثناهایی پیش بیاد .

مشکل عمده ای که OBEX (حالت اول) داره اینکه بدون اجازه ارتباطها رو برقرار میکنه ، و بسیاری از گوشیها و PDA ها روی این حالت هستن .

برای مثال ، XDA O2 که دارای سیستم عامل قدیمی WinCE هست ، در حالت پیشفرض ، تمامی ارتباطهارو بدون اجازه از کاربر برقرار میکنه . با اینکه در نسخه جدید بلوتوس در این گوشی ، حالت دوم درونش قرار داده شده ، بسیاری از کابرها اون رو در حالت اول قرار میدن . یه چیز دیگه ای هم که وجود داره اینکه ،خیلی از کاربرها بدون اینکه فایل و فرستنده رو بشناسن ، اون رو باز میکنن ،مخصوصا اگر اسم فایل Naked_on_the_bed یا Sex و یا اسم هایی تو این مایع ها باشه ! من نمیدونم این افراد به چه امیدی دستگاه رو در این حالت قرار میدن ، بابا لا اقل در حالت دوم قرار بدید بعد هر چی که تقاضا برای ارسال و

دریافت اومد ، قبول کنید ! امیدوارم دوستانی که درحال خوندن این مقاله هستن دستگاهشون رو در حالت اول قرار نداده باشن و یا اینکه تا یه فایل با اینجور اسم ها میبینن اونهارو دریافت و یا باز نکنن !

موقعیت یابی بلوتوس

شاید جالب باشه بدونید که پارک جانورشناسی (باغ وحش) آلبرگ در دانمارک ، از فناوری به نام BlueTags استفاده میکنه، حالا میخواین بدونید این BlueTags چیه و چیش تو این جا جالبه ؟ BlueTags یه فناوری هستش که از سریق اون موقعیت یابی میکنن . حالا تو این باغ وحش ، در جلو در ورودی ، یک BlueTags به لباس بازدید کننده ها ، مخصوصا بچه ها وصل میکنن ، که اول از همه بر مکانهایی که این ها میرن تسلط داشته باشن، در مرحله دوم هم در صورتی که بچه ای تو این پارک بزرگ گم شد ، بتونن بدون ناراحتی و در کمترین زمان اون رو به والدینش تحویل بدن. در واقع ساختار و متد این فناوری از بلوتوس گرفته شده . دستگاه های گیرنده ای رو در مناطق معلومی نصب میکنن ،سپس این دستگاه ها امواج BlueTags رو ارسال میکنه که گیرنده پس از دریافت اونها ،موقعیت رو پیدا میکنه. برای مثال ، یه گیرنده در کنار قفس شیرها میذارن ، این گیرنده ، امواجی که از BlueTags های نزدیک خودش هست رو دریافت میکنه و موقعیت اونهارو مشخص میکنه،به محض اینکه مکان عوض بشه ، و فرد سمت قفس ببر ها بره ، در این موقع میزان امواج در سمت قفس ببر قوی میشه ، بدین ترتیب دیگه گیرنده اولی به دستگاه کاری نداره و تمام اطلاعات توسط گیرنده دومی آنالیز میشن . قابل ذکر که BlurTags ها مختلف رو با استفاده از MAC ADDRESS شون تشخیص میدن و اینطوری میشه که سیستم مرکزی میتونه مکان هر بلوتگ رو شناسایی کنه و در صورت لزوم از خطرات احتمالی جلوگیری بکنه . همینطور در درازمدت میشه از این سیستم برای تهیه نقشه هایی پیرامون میزان بازدید از هر قسمت ، قسمتهایی که بیشتر نیاز به نگهبان دارن و... استفاده کرد و با تهیه این نقشه ها مسئولین این باغ وحش میتونن برای قسمتهای پر بازدید ، امکانات خوبتر و

بهتری رو نسبت به بقیه قسمتها تدارک ببینن تا بازدیدکننده احساس رضایت بکنه . مشاهده میکنید که این فناوری خیلی به درد این باغ وحش میخوره و میزان کاربردهایی که میشه ازش بهره برد ، زیاد هست . بنابراین تکنولوژی بلوتوس فراتر از تصور من و شما کاربرد داره و در آینده هم حتما این کاربردها جذابتر و بیشتر میشه .

بلوتگ و اختفا

همونطوری که در قسمت اول توضیح دادیم ، هر بلوتوس که در حالت فعال باشه ، دارای آدرس مشخص و مخصوص به خودش هست که یه طورایی به وسیله اون آدرس شناخته میشه . همینطور ما در این قسمت اشاره کردیم که چطوری میشه به این دستگاه ها که بلوتوسشون در حالت فعال قرار داره و تعدادشون هم بسیار زیاد هست بدون اجازه کاربر اون دستگاه متصل شد و اطلاعات بدست اورد. مگر اینکه ما بخواهیم با استفاده از سرویس ویژه ای به اون دستگاه درسترسی پیدا کنیم (OBEX, Dial-up etc) . نداشتن اجازه برای برقرار کردن ارتباطهای LMP (Link Manager Protocol) و L2CAP (Logical Link Control and Adaptation Protocol) و همینطور وجود داشتن فقط و فقط یک آدرس برای هر دستگاه ، میتونه دلیلی بر وجود داشتن مشکل مهمی در این فناوری باشه ، و اون مشکل هم اینکه با استفاده از این مطالب میشه از هر بلوتوس در حالت فعال ، یک بلوتوگ درست کرد و اگر یه خورده دقت میکنید میفهمید که اینطوری میشه موقعیت یابی کرد .

میشه با ساختن یه رسیور بلوتوسی کوتاه برد که بتونه بلوتوس های اطراف رو هر 1دقیقه یکبار شناسایی کنه و اطلاعات مکانی اونها رو به سیستم برای شناسایی مکانی بده ساخت . در اینصورت با قرار دادن چندین رسیور در فواصل معین میشه تغیرات مکانی اونهارو بطور کامل ضبط کرد و در صورت نیاز به فرد مورد نظر مراجعه کرد . همینطور میشه دستگاه هایی رو هم که در حالت فعال نیستن رو شناسایی کرد ،یعنی هر 1دقیقه سعی به فرستادن

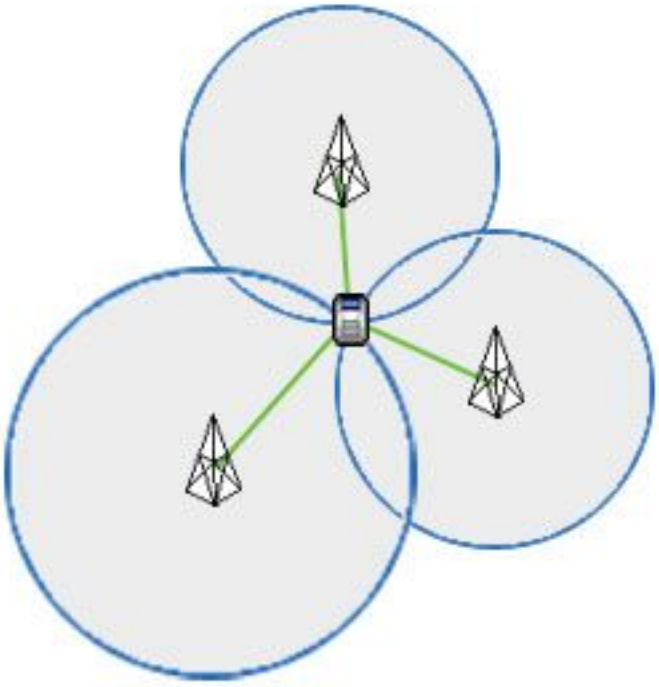
اطلاعات میکنیم و در صورتی که حتی دستگاه برای یک ثانیه هم فعال بشه ، ما میتونیم موقعیت اون رو بدست بیاریم(البته در صورتی که از قبل Mac Address رو داشته باشیم) ! لازم به ذکر که تمام این کارها با استفاده از مشکلات بالا و بدون اطلاع کاربر دستگاه انجام میشه .

حالا یه مثال میزنیم تا متوجه بشید که این قسمت در چه جاهایی به کار میاد . برای مثال شما یه سوپر مارکت دارید و میخواین علاوه بر دوربین های امنیتی که بر مشتریان نظارت دارن ، شما هم به شخصه نظارت داشته باشید ، بدین منظور تعدادی از این رسیور ها رو در سوپر مارکتتون نصب میکنید . از اونجایی که تو این دوره اکثر گوشیها دارای بلوتوس هستن و اکثر کاربرها هم از هندست برای راحتی استفاده میکنن ، شما میتونید تغیرات مکانی اونها رو ببینید . حالا فکر میکنید این به چه درد میخوره ؟ الان میگم ، شما هر چقدر هم دوربین بذارید باز یکسری نقاط کور وجود خواهد داشت که شما بر اونها هیچ تسلطی ندارید ،ولی با استفاده از این رسیور ها میتونید در تمامی سوپر مارکتتون نظارت رو داشته باشید . و نقاط کور رو شناسایی کنید و سعی در بهبود اونها بکنید (البته سوپر مارکت به معنای واقعی ،نه این بقالی ها که اسم خودشون رو گذاشتن سوپر مارکت !)

باید این رو بگم که فقط شما نمیتونید از این کار در محیط های بسته و مشخص استفاده کنید ،بلکه در مکانهای بزرگ هم میشه استفاده کرد . برای مثال دولت میتونه برای اینکه از موقعیت افرادی که از کشورهای دیگه وارد کشورش شدن ، با استفاده از این کار مطلع بشه و در واقع یک بانک کاطلاعاتی بدست بیاره ! برای مثال شما میتونید با استفاده از رسیورهای با برد زیاد ، یک منطقه از شهر رو که به نظر مهم هست رو مورد پردازش قرار بدید. البته باید گفت که در صورتی که شما بخواهین از رسیورهای کوتاه برد استفاده کنید ، برای یک محیط 10 در 10 کیلومتر که شما باید در هر 10 متر یک رسیور بذارید ، نیاز به 250000 تعداد رسیور دارید !پس بسته به نیازتون باید رسیور رو مشخص کنید .

Trilateration برای پیگیری

و موقعیت یابی



باید بگم که متاسفانه یا خوشبختانه ،موقعیت یابی بلوتوس خیلی آسونه ولی ابزاری که این کار نیازمند خیلی گران هست . برای مناطق یزرگ و وسیع هم ما نیاز به چند تکنیک و ابزار خاص داریم که به اون **Trilateration** میگیم . در واقع این تکنیک، تکنیکی هست شبیه تکنیکی که پلیس برای شناسایی گوشی ها و فرستنده ها در مناطق مخصوص و مهم استفاده میکنه (GPS) . شما میتونید نوع قرار گرفتن ابزارها رو در عکس بالا مشاهده کنید.

همونطوری که گفته شد ، از متدی شبیه به متد بالا در بلوتوس استفاده میشه . اما تنها فرقش اینکه به جای استفاده از GSM ، از رسیورهای بلوتوس استفاده میشه . محاصبه میزان سیگنال و بقیه آنالیزها ، بستگی به محاصبات در نوع قرار دادن رسیورها داره.

اگر شما خیلی مایل هستید تا از این متد استفاده کنید ، برای راهنماییتون میتونم این دو منبع رو معرفی کنم که با یه سرچ کوچیک در گوگل میتویند از محتویاتش برخوردار بشید:

1- An indoor Bluetooth-based positioning system: concept, Implementation and experimental evaluation, by Silke Feldmann, Kyandoghere Kyamakya, Ana Zapater and Zighuo Lue from Institute of Communications Engineering in Hanover.

2- Bluetooth Positioning, Josef Hallberg, Marcus Nilsson, Kåre Synnes from Luleå University of Technology / Centre for Distance-spanning Technology.

درکل برای اینکه شما اطلاعات بیشتری در این رابطه داشته باشید باید بگم که شما در صورتی که از سه رسیور بلوتوس در مناطق مشخصی استفاده کنید (مثل عکس صفحه قبل) میتونید از تکنیک trilateration استفاده کنید و حرکات هر دستگاه رو با دقت مطلوب داشته باشید . اگر هم از 4 بلوتوس رسیور استفاده کنید که عالی میشه و دقت بالاتر میره.

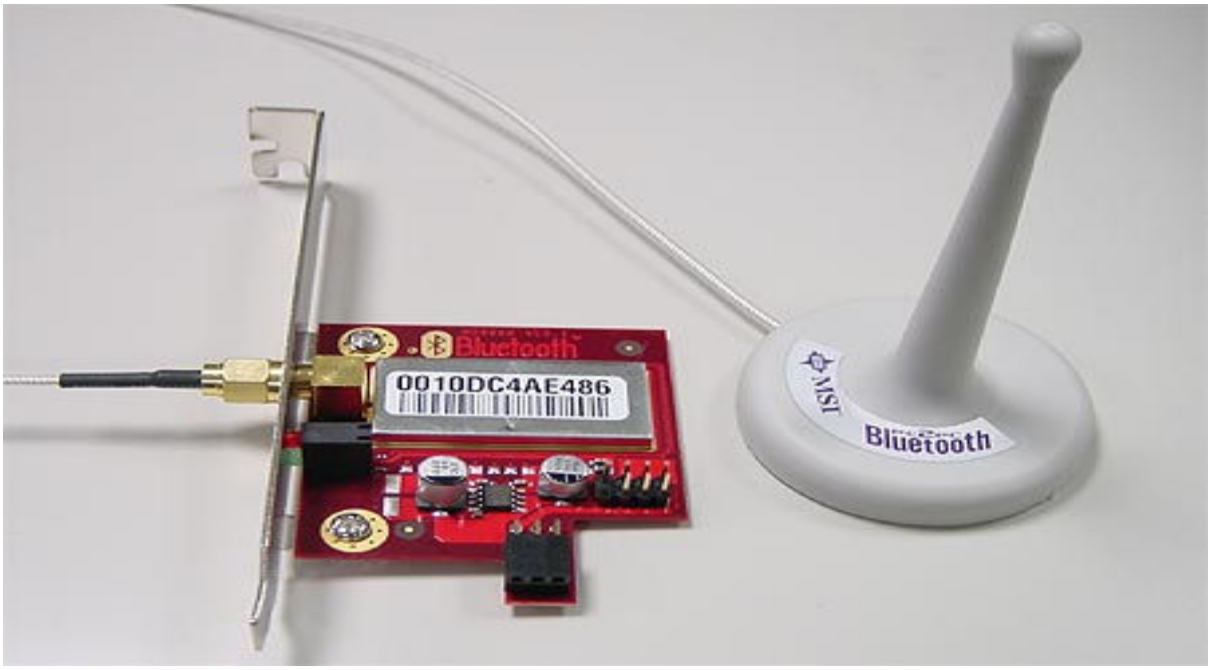
شما با استفاده از این تکنیک میتونید 100 متر رو بطور کامل پشتیبانی کنید (با بلوتوس های دانگل کلاس1) و حرکات رو زیر نظر داشته باشید ، در صورتی هم که شما فضای بزرگتری دارید ، باید هر 100 متر این کار رو انجام بدید و رسیور قرار بدید . بنابراین این تکنیک برای افراد عادی که اونطورها هم مایه دار نیستن ، در 100 توصیه میشه . چون هرچقدر محیط بیشتر بشه ، تعداد بلوتوس رسیور ها هم افزایش پیدا میکنه .

انواع مختلف بلوتوس

نوع استاندارد بلوتوس ، نوع دانگل کلاس 1 هستش که در عکس انواع اون رو مشاهده میکنید . این نوع بلوتوس دارای یه آنتن کوچیک هستش که با استفاده از اون میتونه حد اکثر 100 متر رو پوشش بده .

این تصاویری از توع استاندارد بلوتوس هست.

نوع دوم بلوتوس ، این مدل هست که نسبت به نوع اول از هر لحاظ اصلاح شده و و اون رو با نام بلوتوس آداپتر میشناسن . و میزان برد اون یه چیزی در حدود 200 متر هستش . البته این بستگی به نوع آنتن و نوع کابل مرتبطش داره . البته با استفاده از تعدادی متد و تکنیک شما میتونید با استفاده از 5 آداپتر بلوتوس ، میتونید حتی تا یک مایل رو هم پوشش بدید ! (بنابر دلایلی نمیتونم این تکنیک رو تو این مقاله ذکر کنم :D)



همونطوری که مشاهده میکنید ، هرچقدر این آنتن بزرگتر باشه ، فضای بیشتری رو پوشش میده ، من با استفاده از این مدل D-Link ANT24-1400 14dbi تونستم از فاصله 500 متری با گوشیSoney Ericsson P900 ارتباط برقرار کنم . البته اگر شما از آملی فایر استفاده کنید میتونید تا فاصله یک کیلومتر هم پوشش بدید !

موقعیت یابی در محیط های بزرگ

موضوع قبل رو یادتونه؟ موضوع قبلیش چی؟ اگر قشنگ این دو موضوع رو خونده باشید ، متوجه یه نکته شدید . میتونید بگید چیه؟

(این قسمت فکر کنم فقط به درد دولت بخوره تا بتونه از کارهای خرابکارانه جلوگیری کنه .)

با استفاده از یه بلوتوس آداپتر شما میتونید تقریبا یه فاصله 1کیلومتری رو پوشش بدید ، اگر شما از 36 آداپتر استفاده کنید (هر 1.5 کیلومتر یکی) میتونید یک محیط به اندازه 100 کیلومتر مربع رو تحت پوشش قرار بدید . شما میتونید با ترکیب trilateration و این نکته ای که تو این بخش اشاره کردم ، هر گونه فعالیت بلوتوسی ای رو که در محیطی به وسعت 100 کیلومتر مربع انجام میشه رو تحت نظر بگیرید ! بدون هیچ گونه مانعی ، بدون هیچ گونه قطعی و خلاصه روشی جالب برای کنترل مناطق حساس هستش . البته همونطور که گفتم ، این طرح فقط به درد دولت و ارگانهای نظامی میخوره ، چون هزینه ای که باید صرف این طرح بشه چیزی در حدود 10،000 $ هستش که این میزان برای من و شما خیلی زیاد ، ولی برای دولت و دیگر ارگانها که میخوان از مناطقشون حفاظت کنن ، هیچ پولی نیست . البته یکی از کاربردهای این طرح ، در راهنمایی و رانندگی ، چون میتونن محیط وسیعی رو پوشش بدن ، و از اون در مناطق پر رفت و آمد استفاده کنند تا بتونن سرعت و ترافیک رو در جاده ها کنترل کنن !

جمع بندی

در کل هر سیستمی و تکنولوژی یکسری مشکلات داره و بلوتوس هم از این قضیه مستثنا نیست . البته بلوتوس با تلاش SIG هر روز پیشرفته تر ،سریع تر و امنتر میشه. ما در این دو مقاله به نکات قوت و ضعف این تکنولوژی پرداختیم. راه های نفوذ و ... رو بهتون گفتیم. مواردی رو که میشه ازش استفاده کرد رو گفتیم. البته این موارد خارج از اون مواردی بود که فکر میکردیم . قابل ذکر که بگم این تکنولوژی امنیت خوبی رو داره و مشکلات امنیتی که

در اون پیدا کردن زیاد بزرگ نیست و این مشکلات در اولین فرصت توسط گروه SIG برطرف میشه تا کاربران با خیال راحت تر از این فناوری زیبا استفاده کنند.

نکات امنیتی در یک جمله

1- بلوتوس رو زمانی فعال کنید که لازمش دارید .
2- دستگاه خودتون رو در حالت مخفی قرار بدید.
3- از رمز عبورهای طولانی و غیر معمول استفاده کنید و هرگز رمز عبورتون رو 1234 و اینجور رمز عبورها نذارید.
4- تمامی درخاست هایی که نمیشناسید و تمایل به اتصال به گوشی شما دارن رو رد کنید.
5- هر چند دقیقه یکبار (زمانی که بلوتوس روشن) لیست افرادی که به گوشی شما متصل اند رو چک کنید.
6- گوشی خودتون رو همیشه آپدیت کنید .

این مقاله هم تمام شد و ما همین جا مبحث بلوتوس رو میبندیم . منتظر مقالات ما در موضوعات مختلف باشید.

©CopyRight®


Author: Sir.Hitler
Sir.Hitler@Gmail.com
Sir_Adolf.Hitler@Yahoo.com
Developed in SATANIC Digital Network Security Team
With Speacial Thnx 2: Satanic Soulful , Hell Hacker , Little Hacker ,
Bl2k, XShabgardX, Hamid Star2005, BlackIce
Amin Mehrvarz , Farhad1507
Research By : Sir.Hitler
Copy Right For Satanic & Shabgard Team 2003-2007
For More Information Go To http://Satanichell.com


www.Satanichell.Com


All Right Reserved For Shabgard Security ™©®
Mr.XShabgardX
2005-2006 For More Information
Visit:Http://Shabgard.Org
Shabgard