MOBILE HACKING

NOBODY_CODER@YAHOO.COM

موضوع مقاله : هک موبایل (درس 4 سیستم عامل ها 2)

نویسنده مقاله : سینا احمدی

عضو انجمن هک و امنیت آشیانه

نام کاربری در فروم آشیانه : NobodyCoder

ایمیل : Nobody_Coder@yahoo.com

WWW.ASHIYANE.ORG

نفوذ به یک سیستم عامل :

همانطور که گفته شد سیستم عامل یکی از مهمترین عوامل در نفوذ به یک تلفن همراه است ! اگر درس سیستم عامل ها (1) را مطالعه کرده باشید با کمی توجه می فهمید که Symbian بسیار بیشتر از سیستم عامل های دیگر مورد استفاده قرار گرفته است ! بنابراین در ابتدا به آنالیز و بحث در رابطه با این سیستم عامل می پردازیم .

سیمبین :

در ابتدای پیدایش تلفن همراه آنها سیستم خاصی نداشتند و دارای سخت افزاری ساده بودند و به نرم افزار حرفه ای و پیچیده ای نیز نیاز نداشتند ! اما شرکت های مشهور آن زمان گوشی های نسل بعدی خودشان را به بازار ارائه کردند !این گوشی ها سخت افزار بسیار قوی تری داشتند ! بنابراین برای استفاده از سخت افزار قوی به نرم افزار حرفه ای و پیچیده نیز نیاز داشتند ! بنابراین مایکروسافت سیستم عاملی برای گوشی ها طراحی کرد و آن را Windows CE نامگذاری نمود ! شرکت های

به نام آن زمان نیز نمی خواستند که تمام سیستم های نرم افزاریشان متعلق به

مایکروسافت نباشد ! بنابراین با همکاری هم سیستم عامل جدیدی را به وجود آوردند و اسم آن را Symbianگذاشتند ! شرکت هایی که با همکاری هم سیمبین را به وجود آوردند عبارتند از :

Nokia ،Sony-Erricson ،LG ،Samsung ، Motorola ،Arima ،BenQ ،Fujitsu ،Lenovo ، Sanyo ،Sendo ،Mitsubishi Electronics و Siemense.

طراحی و عملکرد سیمبین :

سیمبین تشابه بسیاری به سیستم عامل های PC دارد و در ساختن این OS سعی شده که عملکردی شبیه به سیستم عامل کامپیوتر ها داشته باشد ! همانطور که می دانید سیستم عامل های کامپیوتر امکانات وسیعی برای خدمات دهی بهتر دارند ! همچنین سیمبین هم مانند آنها دارای امکاناتی از جمله : Multi task Multi Thread , Memory Manager می باشد ! هدف اصلی طراحان سیمبین این بود که این سیستم عامل در حداقل امکانات بهترین خدمات را به کاربر بدهد ! به طور مثال با 2 گیگ رم کارایی خوبی را با سرعت بسیار ارائه دهد ! پایه این سیستم عامل بر رویevent ها بنا شده و

به همین دلیل سیستم با استفاده از سی پی یو بار بسیار کمی را روی موبایل می ریزد !

اطلاعات بالا تقریبا فقط تاریخچه ای از این سیستم عامل بود ! اما یکی دیگر از اطلاعاتی که ما برای نفوذ به سیمبین احتیاج داریم برنامه نویسی آن است ! باید بدانیم که برای سیمبین باید از چه زبان های برنامه نویسی استفاده کنیم ! اگر در بخش برنامه نویسی در فروم آشیانه رفته باشید می بینید که من چندین مقاله و تاپیک در رابطه با برنامه نویسی سیمبین نوشته و قرار داده ام ! برای اطلاعات زیاد درباره برنامه نویسی سیمبین به بخش برنامه نویسی موبایل در فروم آشیانه رجوع کنید ! اما توضیح مختصری نیز در مقاله درباره برنامه نویسی تحت این سیستم عامل داده ام !

زبان اصلی برای برنامه نویسی تحت سیمبین C++ است

زبان های دیگری که مورد استفاده قرار می گیرند عبارت اند از :

Visual Basic (mobileVB) , Personal java , Perl , Python , OPL , Delphi , Visual C .net & etc

اما اکثر زبان های فوق برای اجرا شدن در سیمبین احتیاج به یک مکمل یا Plugin دارند ! اما با C++ میتوانید بدون نیاز به پلاگین برنامه نویسی کنید ! در فروم آشیانه چند زبان را به صورت کامل در چند تاپیک توضیح داده ام !

نسخه های اصلی سیمبین :

سیمبین دو نسخه اصلی دارد ! یکی از آنها را که نوکیا طراحی کرده و ورژن های مختلف دارد و معروف ترینشان که همان نسخه اصلی است Symbian Series 60بوده و دیگری UIQ می باشد ! سیمبین سری 60 را خود نوکیا از آن استفاده می کند ! اما UIQ را شرکت سونی اریکسون برای گوشی های سری P خود از آن استفاده می کند ! به دلیل اینکه از UIQ که رابط بسیار زیبا ، گرافیکی و پر سرعتی دارد نسخه های زیر از آن ارائه شد :

UIQ2 & UIQ3

UIQ3 به نظر من هوشمند ترین سیستم عامل موبایل بوده و بر روی گوشی های زیر نصب شده است :

P990 , P990a , P990c , P990i , P1 & etc

اما از لحاظ امنیت :

از لحاظ امنیت سیستم عامل Symbian شباهت زیادی به ویندوز دارد ! همانطور که خاصیت های زیادی برای بالا بردن سرعت و گرافیک کاربر در آن استفاده شده می توان از تمامی آنها برای نفوذ به سیستم سوء استفاده کرد !

Symbian60 نا امن ترین نسخه از سیمبین است ! اما متاسفانه این سیستم عامل بسیار مشهور شد و روی بسیاری از گوشی های نوکیا نصب گردید !

در نسخه UIQ3 کمی روی امنیت سیستم کار شده و طبق تست هایی که من انجام دادم به نتایج زیر رسیدم:

پس از نفوذ به S60 توانستم به تمامی فایل ها و مموری خارجی گوشی دست پیدا کنم و آنها را به گوشی دیگری منتقل نمایم !

پس از نفوذ به UIQ3 توانستم در گوشی اختلال ایجاد کنم و به طور مثال : گوشی بی دلیل روی ویبره رفت ، ریست شد و ... اما نتوانستم به فایل ها و مموری خارجی دست یابم ! اما Log File ها در دسترس بود !

توجه داشته باشید که در S60 اختلالات زیادی نیز به وجود آوردم

گوشی هایی که در آزمایشات بالا از آن استفاده کردم:

S60 = 7610

UIQ3 = P990i

گوشی که با آن نفوذ انجام شد : HTC Verizon touch pro

درس سیستم عامل ها (2) به پایان رسید ! این درس یکی از مهمترین درس های نفوذ به تلفن همراه بود ! توجه داشته باشید که این سری مقالات تماما به دلیل افزایش آگاهی و بالابردن امنیت نوشته شده اند و نویسنده مقاله هیچگونه مسئولیتی در قبال سوء استفاده از مقالات نمی پذیرد !

نویسنده مقاله : سینا احمدی [NobodyCoder]

سایت : Ashiyane.org

تاریخ انتشار مقاله : 30 مرداد 88

تشکر فراوان از :

Behrooz_ice , Q7X , Shadow , Azazel , Virangar , INJECTOR , Magic Coder , Ali_Eagle , Jok3r , 0261 , A_O , ERoR , r00t_b0x , Removal_load , tHe.mostafa , PLUS & All Ashiyane moderator , defacers & members . . . ;)

NobodyCoder
nobody_coder@yahoo.com