دفاع از تلفن‌های موبایل در مقابل حملات

به موازات استفاده از فناوری‌های پیشرفته در تلفن‌های موبایل و سایر دستگاه‌های الکترونیکی نظیر PDA، مهاجمان از روش‌های جدیدتری برای به دام انداختن قربانیان خود استفاده می‌نمایند.

مهاجمان با ارسال پیام کوتاه (SMS) و یا نامه‌های الکترونیکی (Email)، می‌توانند کاربران را ترغیب به استفاده از یک وب سایت مخرب نموده و یا آنان را متقاعد نمایند که کدهای مخربی را بر روی دستگاه قابل حمل خود نصب نمایند.

تهدیدات امنیتی

اکثر تلفن‌های موبایل دارای قابلیت ارسال و یا دریافت پیام کوتاه می‌باشند.

برخی از تلفن‌های موبایل و یا دستگاه‌های PDA دارای قابلیت اتصال به اینترنت نیز می‌باشند.

برخلاف مفید بودن امکانات فوق برای استفاده‌کنندگان، مهاجمان نیز ممکن است از اینگونه پتانسیل‌ها در جهت اهداف مخرب خود سوءاستفاده نموده و عملیات زیر را انجام دهند:

سوءاستفاده از سرویس:

اکثر تلفن‌های موبایل دارای محدودیت‌های مختص به خود در خصوص تعداد پیام ارسالی و یا دریافتی می‌باشند.

در صورتی که یک مهاجم بتواند تعداد زیادی پیام ناخواسته را برای شما ارسال نماید (Spam)، ممکن است هزینه‌های فیزیکی و منطقی بیشتری را به شما تحمیل نماید.

یک مهاجم همچنین می‌تواند تلفن موبایل و یا دستگاه PDA شما را آلوده به کدهای مخربی نماید که به آنان اجازه استفاده غیرقانونی از آن را خواهد داد. با توجه به این که از لحاظ قانونی تلفن به نام شما است، این موضوع می‌تواند مشکلات قانونی متعددی را برای مالک آن به دنبال داشته باشد.

ترغیب کاربران به استفاده از یک وب سایت مخرب:

با این که دستگاه‌های PDA و تلفن‌های موبایلی که به شما امکان دستیابی به نامه‌های الکترونیکی را می‌دهند، گزینه‌ای مناسب برای حملات استاندارد Phishing می‌باشند، مهاجمان با استفاده از پتانسیل‌های جدید موجود در اینگونه دستگاه‌ها قادر به ارسال پیام کوتاه نیز می‌باشند.

این نوع پیام‌ها در ظاهری موجه و ارسالی توسط یک شرکت معتبر خود را قلمداد نموده و کاربران را ترغیب به استفاده از یک وب سایت مخرب می‌نمایند.

اینگونه وب سایت‌ها از مکانیزم‌های مختلفی برای تشویق کاربران برای درج اطلاعات شخصی و یا دریافت یک فایل مخرب استفاده می‌نمایند. استفاده از تلفن موبایل و یا دستگاه PDA کاربران برای تدارک سایر حملات: مهاجمانی که قادر به دستیابی و کنترل سرویس‌های ارائه شده در تلفن‌های موبایل و یا دستگاه‌های PDA کاربران گردند، ممکن است از آنها برای تهاجم علیه سایر کاربران استفاده نمایند. بدین ترتیب، از یک طرف هویت مهاجمان پوشیده خواهد ماند و از طرف دیگر تعداد قربانیان افزایش خواهد یافت.

دستیابی به اطلاعات حساس و مهم:

در برخی موارد، تلفن‌های موبایل قادر به انجام برخی تراکنش‌های خاص می‌باشند (نظیر مشاهده صورتحساب بانکی و یا واریز پول به حساب بانکی و...). مهاجمی که بتواند به تلفن موبایلی که از آن به منظور تشخیص اطلاعات، سوءاستفاده و یا فروش آنها به سایر افراد غیرمجاز گردد.

حفاظت در مقابل تهدیدات

به منظور حفاظت در مقابل تهدیدات، رعایت موارد زیر توصیه می‌گردد:

رعایت توصیه‌های امنیتی در خصوص حفاظت از دستگاه‌های قابل حمل.

رعایت اقدامات احتیاطی و پیشگیرانه به منظور ایمن نمودن تلفن‌های موبایل و دستگاه‌های PDA همانند روش هایی که از آنها به منظور ایمن سازی کامپیوتر استفاده می‌گردد، امری الزامی است.

حفاظت از شماره تلفن موبایل و یا آدرس پست الکترونیکی: مهاجمان، اغلب از نرم‌افزارهایی خاص به منظور یافتن وب سایت‌ها و یا آدرس‌های پست الکترونیکی استفاده می‌نمایند.

از آدرس‌های جمع آوری شده در ادامه برای تدارک حملات و ارسال پیام‌های ناخواسته استفاده می‌گردد.

شماره تلفن‌های موبایل نیز می‌تواند بطور اتوماتیک جمع آوری گردد.

با اعمال محدودیت در ارائه اطلاعات شخصی (شماره تلفن موبایل و آدرس پست الکترونیکی)، احتمال هدف قرار گرفتن شما کاهش پیدا می‌نماید.

عدم استفاده از لینک‌های توصیه شده در نامه‌های الکترونیکی و یا پیام‌های کوتاه. همواره با دیده شک به آدرس‌های ارسالی در نامه‌های الکترونیکی و پیام‌های کوتاه ناخواسته نگاه کنید.

با این که در برخی موارد ممکن است این نوع لینک‌ها ظاهری موجه را داشته باشند، ولی این احتمال وجود خواهد داشت که آنها شما را به یک وب سایت مخرب هدایت نمایند. دریافت نرم‌افزار از منابع کاملاً مطمئن: امروزه وب سایت‌های متعددی را می‌توان یافت که بازی و یا نرم‌افزارهای رایگان را به منظور نصب روی دستگاه‌های PDA و یا تلفن‌های موبایل در اختیار کاربران قرار می‌دهند.

این نوع نرم‌افزارها ممکن است حاوی کدهای مخربی باشند که آلودگی موبایل و یا PDA را به دنبال داشته باشد.

توصیه می‌گردد که هرگز از سایت هایی که هویت آنها به اثبات نرسیده و نسبت به صحت و صداقت عملکرد آنها اطمینان حاصل نشده است، نرم‌افزاری دریافت نگردد.

در صورت دریافت یک فایل از یک وب سایت معتبر نیز می‌باید در ابتدا با استفاده از نرم‌افزارهای آنتی ویروس آن را بررسی نمود. بررسی تنظیمات امنیتی: از امکانات امنیتی ارائه شده همراه دستگاه خود استفاده نمائید.

مهاجمان از مزایای اتصالات Bluetooth به منظور دستیابی و یا دریافت اطلاعات موجود روی دستگاه کاربران استفاده می‌نمایند.

در زمانی که از پتانسیل Bluetooth استفاده نمی‌گردد آن را غیرفعال نمائید تا امکان استفاده از آن توسط کاربران غیرمجاز سلب گردد.

www.srco.ir

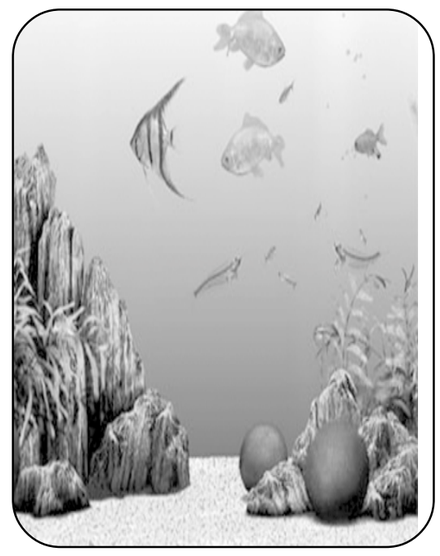
معرفی نرم افزار

Aquazone Desktop Garden RETAIL

امروزه بسیاری از افراد در اتاق شخصی و یا محل کار خود دارای یک آکواریوم کوچک و یا بزرگ می باشند.

نگهداری از ماهی‌ها و مراقبت از آن‌ها امروزه به یکی از سرگرمی‌های افراد مختلف تبدیل شده است.

همچنین آرامشی که با نگاه کردن به ماهی‌ها و حرکات آن‌ها در آب موجب آرامش افراد می‌شود موجب شده تا بسیاری از افراد مختلف اقدام به تهیه یک آکواریوم و نگهداری از آن‌ها نمایند.



بسیاری از افراد به این موضوع علاقه مند می‌باشند اما به علت صرف هزینه و قیمت بالای ماهی‌های آکواریومی و همچنین کمبود وقت اقدام به تهیه یک آکواریوم نمی کنند در حالی که به این موضوع بسیار علاقه مند می‌باشند.

در این مطلب با معرفی نرم‌افزاری این مشکل را برای این عده از افراد که جزو کاربران کامپیوتر نیز می‌باشند حل می‌کنیم.

Aquazone نام نرم‌افزاری می‌باشد که کاربران به کمک آن‌ها قادر به ساخت و تهیه یک آکواریوم مجازی می‌باشند و می‌توانند از ماهی‌های خود در این آکواریوم مجازی نگهداری کنند. در این برنامه همانند یک آکواریوم واقعی کاربران می‌بایست در زمان‌های مشخص به ماهی‌های خود غذا داده، ماهی‌های گوشتخوار را از دسته دیگر ماهی‌ها جدا سازی نمایند، در هنگام تولید مثل یک ماهی آن ماهی را از دیگر ماهی‌ها جدا نماید و.... همچنین کاربران می‌توانند در این نرم‌افزار اقدام به خرید انواع ماهی‌های آکواریومی نمایند و در آکواریوم مجازی خود آن‌ها را نگهداری کنند.

این نرم‌افزار جالب توسط شرکت Smith Micro Software ساخته شده است.

tehroon20.com

Security Administrator

محافظت از کامپیوتر شما و محدود کردن دسترسی به اینترنت با نرم‌افزار Security Administrator امکان پذیر است.

Security Administrator یک نرم‌افزار امنیتی کامل برای محافظت از پسوردها و تعیین انواع دسترسی برای کاربران کامپیوتر تا بتوانید آن‌ها را از تغییر دادن و دست پیدا کردن به اطلاعات محدود کنید.

شما می‌توانید دسترسی را برای هر یک از اشخاص به پنل‌های مدیریتی، محتویات نمایش، شبکه، پسوردها، پرینتر، تنظیمات سیستم و تنظیمات اینترنت محدود کنید.

همچنین می‌توانید تنظیماتی مانند غیر فعال کردن کلیدها، گزینه منوها، پنجره داس، ویرایش رجیستری، اینترنت و دسترسی به شبکه را اعمال کنید.

مخفی کردن آیکون‌های دسکتاپ، شبکه محلی، درایو USB یا هر چیزی که در taskbar شما می‌باشد یکی از مهمترین ابزار این نرم‌افزار است.

از بهترین ابزارهای این نرم‌افزار تعیین پسوورد محافظتی و محدود کردن کاربران برای اجرای نرم‌افزارهای مخصوص، میزان استفاده اینترنت و میزان استفاده از کامپیوتر برای بچه‌ها یا کارمندان می‌باشد.

قابل استفاده در ویندوزهای Windows 9x/ME: Windows NT4 /Windows 2000 /Windows XP/ Windows 2003/ Windows Vista

freedownload.ir

استاندارد باز چیست؟

قسمت اول

تعریف استانداردهای باز

بروس پرنز، یکی از حامیان مطرح نرم‌افزار متن‌باز، این طور عنوان می‌کند که استاندارد باز چیزی بیش از یک ویژگی بوده و اصول استانداردها، فرایند ارائه و اجزای آنها چیزی هستند که استاندارد را باز (Open) می‌کنند. وی می‌گوید که استانداردها باید اصول دسترس‌پذیری را اجرا کرده و انتخاب کاربر را به بالاترین سطح ممکن برسانند.

به علاوه هیچ گونه حق امتیاز، دزدی تبعیضی و غارتی نباید وجود داشته باشد.

به منظور اطمینان از اجرای این اصول، گسترش استانداردهای باز، ارائه آنها به صورت زیرمجموعه و انجام برخی اقدامات، ضروری می‌باشد. سخنان پرنز در انجمنهای FOSS با استقبال گسترده‌ای مواجه شده است.

اصول استانداردهای باز- بروس پرنز

بروس پرنز اصول زیر را برای استانداردهای باز مطرح کرده است. او معتقد است که استاندارد باز چیزی بیشتر از یک ویژگی می‌باشد.

اصول یک استاندارد، فرآیند ارائه و اجرای آن، چیزی است که استاندارد را به استاندارد باز تبدیل می‌کند. اصول ارائه شده توسط پرنز در زیر مطرح شده‌اند.

- اصل در دسترس بودن:

استانداردهای باز برای انجام بررسی و اجرا در دسترس می‌باشد.

- به حداکثر رساندن انتخاب کاربر:

استانداردهای باز، بازار رقابتی عادلانه‌ای را برای پیاده‌سازی استاندارد به وجود می‌آورند و موجب وابستگی کاربر به یک گروه یا تولیدکننده نمی‌شوند.

- عدم وجود حق امتیاز:

پیاده‌سازی استانداردهای باز، فاقد حق امتیاز یا هرگونه هزینه‌ای می‌باشد. ارائه گواهی تأیید توسط سازمان استاندارد شاید هزینه‌ای داشته باشد.

- عدم وجود تبعیض:

استانداردهای باز و سازمانهای ارائه‌دهنده آنها میان محصولات مختلف تبعیض قائل نمی‌شوند مگر از لحاظ انطباق آنها با استاندارد فنی. سازمانهای صادرکننده مجوز باید روش کم هزینه یا رایگانی را برای تأیید محصولات، ارائه کرده و خدمات تأیید خود را نیز ارتقا بخشند.

- گسترش یا زیرمجموعه:

استانداردهای باز را می‌توان گسترش داده و یا به صورت زیرمجموعه‌هایی ارائه نمود. با این وجود ممکن است که سازمانهای اعطاکننده مجوز از تأیید زیرمجموعه‌ها خودداری کرده و شرایطی را برای موارد توسعه یافته تعیین کنند.

- عملکردهای مربوط به غارت:

استانداردهای باز از مجوزهایی استفاده می‌کنند که با استفاده از روشهای استفاده و گسترش، مانع از تخریب استاندارد می‌شوند. مجوزهای ضمیمه شده به یک استاندارد ممکن است مطرح کردن اطلاعات مرجع را برای موارد توسعه یافته و وجود مجوزی را برای ایجاد، توزیع و فروش نرم‌افزار منطبق با موارد توسعه یافته الزامی کند. در غیر این صورت استاندارد باز از فرایند توسعه و گسترش ممانعتی به عمل نخواهد آورد.

بروس پرنز به عملکردهای پیشنهادی مطرح شده برای ارائه و اجرای هر یک از اصول نیز پرداخته است. سیاست استانداردهای باز ایالات ماساچوست آمریکا آن را به عنوان خصوصیاتی تعریف کرده که برای سامانه‌هایی در دسترس عموم قرار داشته و توسط انجمن باز توسعه پیدا کرده و یک نهاد استاندارد نیز آن را تأیید می‌کند. چارچوب همکاری بینابین اروپایی (EIF) اتحادیه اروپا به نیازمندیهای موجود، این مورد را نیز اضافه کرده است که استانداردهای باز باید به رایگان یا با هزینه اندکی در دسترس قرار گرفته، نسخه برداری و توزیع باید بدون وجود حق امتیاز انجام شده و در استفاده مجدد از آن هیچ گونه محدودیتی نباید وجود داشته باشد.

بنابراین تعریف پرنز با تعریف اتحادیه اروپا و ایالت ماساچوست مطابقت داشته است و این روش توسط بسیاری از سیاستمداران به عنوان مبنای سیاستگذاری مربوط به استاندارد باز استفاده شده است.

سازمانهای دیگری مانند مؤسسه استاندارد ملی آمریکا (ANSI)، بخش استانداردسازی ارتباطات اتحادیه بین المللی مخابرات (ITU-T) و اتحادیه نرم‌افزارهای تجاری (BSA) نیز تعاریف و سیاستهای مربوط به استانداردهای باز را ارائه کرده‌اند.

همه این سازمانها معتقدند که استاندارد باز باید برای پیاده سازی و توسعه در دسترس عموم قرار داشته باشد.

به علاوه وجود حقوق مالکیت معنوی (IPR) برای در دسترس قرار گرفتن این استانداردها در شرایط یکسان با پرداخت هزینه منطقی یا به رایگان نیز ضروری می‌باشد.

www.ictna.ir

تازه های دنیای رایانه

جایگاه NAT

بخش اول

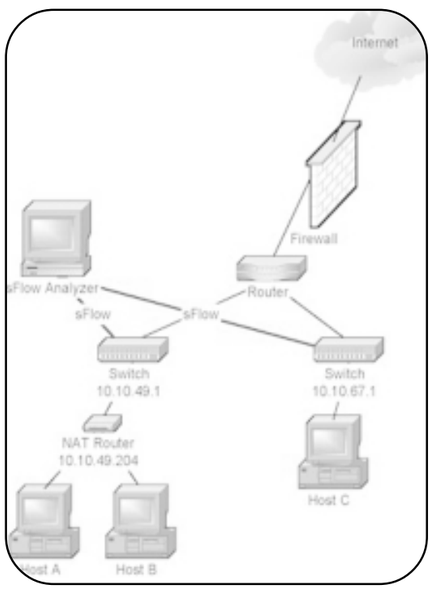
اینترنت با سرعتی باورنکردنی همچنان در حال گسترش است.

تعداد کامپیوترهای ارائه دهنده اطلاعات (خدمات) و کاربران اینترنت روزانه تغییر و رشد می‌یابد.

با اینکه نمی توان دقیقاً اندازه اینترنت را مشخص کرد ولی تقریباً یکصد میلیون کامپیوتر میزبان (Host) و ۳۵۰ میلیون کاربر از اینترنت استفاده می‌نمایند.

رشد اینترنت چه نوع ارتباطی با Network Address Translation) NAT) دارد؟ هر کامپیوتر به منظور ارتباط با سایر کامپیوترها و سرویس دهندگان وب روی اینترنت، می‌باید دارای یک آدرس IP باشد.

IP یک عدد منحصر بفرد ۳۲ بیتی بوده که کامپیوتر



موجود در یک شبکه را مشخص می‌کند. اولین مرتبه‌ای که مسأله آدرس دهی توسط IP مطرح گردید، کمتر کسی به این فکر می‌افتاد که ممکن است خواسته‌ای مطرح شود که نتوان به آن یک آدرس را نسبت داد. با استفاده از سیستم آدرس دهی IP می‌توان ۴/۲۹۴/۹۷۶/۲۹۶ (۲۳۲) آدرس را تولید کرد. (به صورت تئوری). تعداد واقعی آدرس‌های قابل استفاده کمتر از مقدار (بین ۳/۲ میلیارد و ۳/۳ میلیارد) فوق است.

علت این امر، تفکیک آدرس‌ها به کلاس‌ها و رزو بودن برخی آدرس‌ها برای multicasting، تست و موارد خاص دیگر است. همزمان با انفجار اینترنت (عمومیت یافتن) و افزایش شبکه‌های کامپیوتری، تعداد IP موجود، پاسخگوی نیازها نبود.

منطقی ترین روش، طراحی مجدد سیستم آدرس دهی IP است تا امکان استفاده از آدرس‌های IP بیشتری فراهم گردد. موضوع فوق در حال پیاده سازی بوده و نسخه شماره شش IP، راهکاری در این زمینه است.

چندین سال طول خواهد کشید تا سیستم فوق پیاده سازی گردد، چراکه می‌بایست همه زیرساخت‌های اینترنت تغییر واصلاح گردند. NAT با هدف کمک به مشکل فوق طراحی شده است.

NAT به یک دستگاه اجازه می‌دهد که به صورت یک روتر عمل نماید.

در این حالت NAT به عنوان یک آژانس بین اینترنت (شبکه عمومی) و یک شبکه محلی (شبکه خصوصی) رفتار نماید.

این بدان معنی است که صرفاً یک IP منحصر بفرد به منظور نمایش مجموعه‌ای از کامپیوترها(یک گروه) مورد نیاز خواهد بود.

کم بودن تعداد IP صرفاً یکی از دلایل استفاده از NAT است.

در ادامه به بررسی علل استفاده از NAT خواهیم پرداخت. قابلیت‌های NAT عملکرد NAT مشابه یک تلفتچی در یک اداره بزرگ است.

فرض کنید شما به تلفنچی اداره خود اعلام نموده اید که تماس‌های تلفنی مربوط به شما را تا به وی اعلام ننموده اید، وصل نکند.

در ادامه با یکی ازمشتریان تماس گرفته و برای وی پیامی گذاشته اید که سریعاً با شما تماس بگیرد.

شما به تلفنچی اداره می گویید که منتظر تماس تلفن از طرف یکی از مشتریان هستم، در صورت تماس وی، آن را به دفتر من وصل نمایید. در ادامه مشتری مورد نظر با اداره شما تماس گرفته و به تلفنچی اعلام می‌نماید که قصد گفت وگو با شما را دارد (چراکه شما منتظر تماس وی هستید). تلفنچی جدول مورد نظر خود را بررسی تا نام شما را در آن پیدا نماید.

تلفنچی متوجه می‌شود که شما تلفن فوق را درخواست نموده اید، بنابراین تماس مورد نظر به دفتر شما وصل خواهد شد.

www.majidlearn.com