۵ /۱۱/ ۱۳۷۸

دانشگاه علم وصنعت ایران

دانشکده مهندسی کامپیوتر

طراحی و پیاده سازی پست الکترونیکی، انتقال پرونده و ورود از دورامن

فرامرز گیوکی

پایان نامه برای دریافت درجه کارشناسی ارشد
در رشته مهندسی کامپیوتر(نرم افزار)

استاد راهنما:
دکتر حمید تمدن

چکیده

امنیت در شبکه های کامپیوتری برای بسیاری از استفاده کننده گان اهمیت اساسی دارد. یکی از مباحث در شبکه ها فراهم سازی امنیت در لایهء کاربرد مدل مرجع می باشد. در این پروژه می توان به طراحی وپیاده سازی گونهءامنی برای سرویس های پست الکترونیکی درمحیط اینترنت وسیستم عامل لینوکس، وهمچنین طراحی برای سرویس های انتقال پرونده و ورود از دور نیز اشاره کرد . برای پست الکترونیکی ، نرم افزار اس.ای.ام. طراحی و پیاده سازی شده است. اس.ایی.ام. بر اساس استاندارد پی.ایی.ام ، که با پشتیبانی زبان فارسی همراه بوده است . پروتکلی برای انتقال پرونده طراحی شده که بر مبنای مشتری _ سرویس دهنده است . برای ورود از دور نیز روش تصدیق اعتبار ویژه أی طراحی شده است .

در این پروژه مباحث مبنایی وراههای نفوذ امنیت سیستم ها، امنیت پایگاه داده ها و ساختارهای امنیت شبکهء ایزو ، مکانیسم ها و سرویس های امنیتی ، استانداردهای معروف بحث ، مقایسه ونهایتا" معیارهای اولیه أی نیز برای ارزیابی سرویس های امنیتی ارائه شده است.

کلید واژه ها: شبکه های کامپیوتری،سرویس های امنیتی،پست الکترونیکی،انتقال پروندهء امن،ورود از دور امن، رمزنگاری ، ارزیابی امنیت .

تقدیم و تشکر :

تقدیم به همسرم که بهترین مشوق من برای رسیدن به این مقطع بوده است .

تقدیم و تشکر :

تقدیم به خانواده ام که سهم بزرگی را برای رسیدن به این مقطع را داشته اند .

تقدیر و تشکر :

ضمن سپاس بیکران خداوند ، بر خود لازم می دانم از استاد محترم آقای دکتر حمید تمدن که با ارائه راهنمایی های مدبرانه و دلسوز خود نظارت این پروژه را به عهده داشته اند ، صمیمانه تشکر و قدردانی می نمایم .

فهرست عنوانها

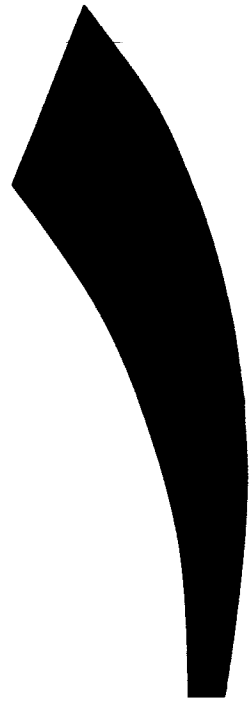
فهرست شکل ها

عنوان | صفحه

فهرست جدول ها

عنوان | صفحه

فصل اول



ساختار پایان نامه

فصل اول:

۱-۱: ساختار پایان نامه

- **فصل دوم:** در این فصل مباحث مبنایی امنیت سیستم های کامپوتری مورد بحث قرار گرفته است. راههای نفوذدسته های امنیت سیستمهای کامپیوتری معرفی شده و به امنیت شبکه وهمچنین امنیت پایگاه داده ها پرداخته شده است.

- **فصل سوم:** مباحث نظری امنیت سیستم های کامپیوتری، دلایل ضرورت توجه به امنیت شبکه های کامپیوتری وهمچنین نگرشهای مبنایی امنیت شبکه ، ساختارهای امنیت شبکهء ایزو، مکانیسم ها و سرویس های امنیتی،استاندارد پی.ایی.ام. و پی.جی.پی. که دو راه حل معروف برای امنیت هستند،بحث شده وسپس با هم مقایسه و معماری امنیت شبکه و پیاده سازی سرویس های امنیت شبکه مورد بررسی قرار گرفته اند.

- **فصل چهارم:**دراین فصل به مسائل سرویس های امنیت پست الکترونیکی ، معماری ونرم افزار اس.ایی.ام،وظایف و ویژگیها ، نمودار عملیاتی وسپس پیاده سازی پست الکترونیکی امن و امکانات اصلی اس.ایی.ام.، مدیریت پیغام ، مدیریت امنیت ، ویرایش نشانیها و واسط کاربردی امن ،وهمچنین شرح کلی برنامه ها تشریح شده اند.

- **فصل پنجم** : در این فصل به مسائل سرویس های امنیت انتقال پرونده امن ، معماری آن ،پروتکل و معماری مشتری_سرویس دهنده ، و نمودار عملیاتی و سپس پیاده سازی انتقال پرونده و برنامه های آنها ارائه شده اند.

- **فصل ششم** : دراین فصل نیزبه مسائل سرویسهای امنیت ورود ازدور، معماری ،تصدیق اعتبار و ایجاد نشست امن ، نمودار عملیاتی و سپس پیاده سازی ورودار دور مورد بحث واقع شده اند.

- **فصل هفتم** : مفاهیم مبنایی رمزنگاری یعنی تعریف سیستم های رمز ، سیستم های رمز کلاسیک ،رمزنگاری متقارن، رمزنگاری جریانی، رمزنگاری نامتقارن وهمچنین پیاده سازی روالها و الگوریتم رمزگذاریها ،سرویس نمونه تصدیق اعتباربا روش کربرس و برنامه های سرویس دهنده و مشتری ارائه شده است.

- **فصل هشتم** : در این فصل به مبحث ارزیابی امنیت پرداخته شده است. این بحث شامل مدلهای امنیتی و معیارهای ارزیابی امنیت سیستم های کامپیوتری و شبکه ها، ونیز ارزیابی امنیت سرویس های طراحی و پیاده سازی شده با استفاده از این معیارها می باشد.

- **پیوستها** : در این قسمت ، واژه نامه فارسی به انگلیسی وهمچنین واژه نامه انگلیسی به فارسی و بازگشت نامه ارائه شده است.

فصل دوم

۲

مفاهیم مبنایی امنیت

فصل دوم: مفاهیم مبنایی امنیت

۲-۱: مقدمه

در واژه نامه ها ، تعریف ***امنیت*** عبارت است از : *مجموعه ای از ابزارها برای جلوگیری از سرقت ، حمله ، جنایت ، جاسوسی و خرابکاری* . امنیت ، به کیفیت یا حالت امن بودن اشاره دارد . به این معنی که چه میزان قابلیت اطمینان نسبت به وقوع خطر وجود دارد .

رشد استفاده از قابلیت اطمینان در کامپیوترها ، به مفهوم امنیت نیز کشیده شده است . استفاده از کامپیوتر به ادارات ، سازمان های دولتی و نظامی و حتی به خانه ها سرایت کرده است و مقادیر بزرگی از داده های حیاتی و حساس ، از قبیل پرونده های پزشکی ، مالی ، اعتباری ، تجاری و اطلاعات محرمانهء شخصی ، دولتی و نظامی ، در کامپیوترها ذخیره می شوند . دستیابی های غیر مجاز ، نفوذیابی و خرابکاری داده ها ، می تواند به خصوصی و سری بودن اطلاعات ، خدشه وارد نموده و احتمال وقوع این مشکلات، نگرانی هایی را برای اشخاص ، سازمانها و شرکتهای استفاده کننده از سیستمهای کامپیوتری ایجاد نموده است . بر این اساس باید مکانیسم هایی در سیستمهای کامپیوتری در نظر گرفته شود تا از ضررهای احتمالی جلوگیری شده و امنیت سیستم ، تامین گردد . **امنیت سیستم های کامپیوتری** ، مطالعهء سیاستها ، مکانیسمها و ابزارهای اعمال و مدیریت امنیت در سیستمهای کامپیوتری است .

تهدیدهای عمدهء امنیت سیستم های کامپیوتری ، از جانب کاربران و ایجاد کنندگان سیستم های مبتنی بر کامپیوتر بوده و شامل : افشاء یا تغییر غیر مجاز از سرویسهای سیستم یا انکار سرویس از جانب کاربران مجاز ، می باشد . اهداف امنیت سیستم های کامپیوتری ، ایجاد محافظت در مقابل این تهدیدها و حذف آنها است . برای این منظور در سیستم های کامپیوتری باید مکانیسم هایی برای جلوگیری از دستیابی های غیر مجاز ، به مخاطره افتادن داده ها و انکار خدمات ، فراهم شده و راه حلی برای تامین تمامیت دادههای سیستم پیش بینی گردد. منظور از تمامیت داده ها ، محافظت در مقابل تغییرات نامشخص یا غیر مجاز داده ها می باشد .

۲-۲: راههای نفوذ به سیستمهای کامپیوتری

راه های متعددی برای نفوذ به سیستمهای کامپیوتری وجود دارد ، که معروفترین آنها در زیر میآیند:

- **استفاده از پایانه های متصل** : ساده ترین راه نفوذ به یک سیستم کامپیوتری ، آن است که شخصی براساس اعتبار خود واز راه یک پایانه ، به آن متصل شده ، اما اتصال خود را قطع نکرده باشد . شخص غیرمجازی ، به این ترتیب می تواند