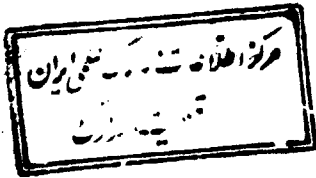


بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

٢٧٤٩٩



دانشگاه علم و صنعت ایران

دانشکده مهندسی کامپیوتر

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

فرامرز گیوکی

۱۴۹۹۱

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

استاد راهنما:

دکتر حمید تمدن

۲۷۴۹۹

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 لایه کاربرد مدل مرجع می باشد. در این پروژه می توان به طراحی و پیاده سازی گونه امنی برای سرویس های پست الکترونیکی در محیط اینترنت و سیستم عامل لینوکس، و همچنین 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.ای.ام. بر اساس استاندارد پی.ای.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 ای طراحی شده است.

در این پروژه مباحث مبنایی و راههای نفوذ امنیت سیستم ها، امنیت پایگاه داده ها و ساختارهای امنیت شبکه ایزو، مکانیسم ها و سرویس های امنیتی، استانداردهای معروف بحث، مقایسه و نهایتاً معیارهای اولیه ای نیز برای ارزیابی سرویس های امنیتی ارائه شده است.

کلید واژه ها: شبکه های کامپیوتری، سرویس های امنیتی، پست الکترونیکی، انتقال پرونده 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 مدیرانه و دلسوز خود نظارت این پروژه را
به عهده داشته اند ، صمیمانه تشکر و قدردانی می نمایم .

فهرست عنوانها

صفحه	عنوان
۱	فصل اول : فصل نخست
۱	۱-۱: درباره پایان نامه
۲	فصل دوم : مفاهیم مبنایی امنیت
۲	۱-۲: مقدمه
۲	۲-۲: راههای نفوذ
۲	۳-۲: دسته های امنیت سیستمهای کامپیوتری
۳	۱-۳-۲: سیستم عامل
۳	۲-۳-۲: پایگاه داده ها
۴	۱-۲-۳-۲: تهدید حملات به مدیریت پایگاه داده ها
۵	۳-۳-۲: شبکه
۵	۱-۳-۳-۲: مولفه های اصلی امنیت شبکه
۷	۴-۲: امنیت شبکه
۷	۱-۴-۲: تعریف
۸	۲-۴-۲: Network Security Overview
۸	۳-۴-۲: اتصال دو کامپیوتر
۸	۴-۴-۲: مله های امنیتی رایج
۹	۵-۴-۲: اجزاء اولیه امنیت شبکه
۱۱	۶-۴-۲: حملات به سیستم شبکه
۱۱	۷-۴-۲: استراتژی های رمزکردن
۱۳	۸-۴-۲: تکنیک های محافظت داده ها حین انتقال
۱۳	۱-۸-۴-۲: داده ها بین فرستنده و گیرنده
۱۳	۲-۸-۴-۲: داده ها بین اجزای بین راهی در یک انتقال
۱۴	۹-۴-۲: پروتکل ارتباطات سیستم باز OSI
۱۵	۱-۹-۴-۲: نیاگرام ۷ لایه سیستم OSI
۱۶	۲-۹-۴-۲: تکنیک داده ها بین اجزای بین راهی در یک انتقال
۱۸	۳-۹-۴-۲: تکنیک داده ها بین فرستنده و گیرنده
۱۹	۱۰-۴-۲: سیاستهای امنیتی حین ارتباط سیستم ها
۱۹	۱-۱۰-۴-۲: Network Security Policy Issue
۲۰	۱-۱-۱۰-۴-۲: مثال MLS/TCP
۲۲	۲-۱-۱۰-۴-۲: مثال SDNS
۲۴	۵-۲: امنیت پایگاه داده ها
۲۴	۱-۵-۲: انواع حملات
۲۵	۲-۵-۲: مشکلات بانک های اطلاعاتی
۲۸	۳-۵-۲: مشکل اجتماع داده ها
۲۹	۴-۵-۲: رویکرد امنیتی برای مقابله با حملات و مشکلات
۳۰	۵-۵-۲: حفاظت سیستم های فایلی
۳۵	فصل سوم: امنیت شبکه
۳۵	۱-۳: مقدمه
۳۵	۲-۳: مباحث نظری امنیت سیستمهای کامپیوتری

۳۶	۳-۳: دلایل ضرورت توجه به امنیت شبکه های کامپیوتری
۳۷	۴-۳: نگرشهای مبنایی امنیت شبکه
۳۷	۳-۴-۱: رمزگذاری پیوند گرا
۳۷	۳-۴-۲: رمزگذاری انتها به انتها
۳۸	۳-۵: ساختارهای امنیتی ایزو
۳۸	۳-۵-۱: سرویسهای امنیتی
۳۸	۳-۵-۱-۱: گروه بندی منطقی سرویس های امنیتی
۳۹	۳-۵-۱-۱-۱: سرویس های امنیت موجودیتی
۳۹	۳-۵-۱-۱-۲: سرویس های امنیت ارتباطی
۳۹	۳-۵-۱-۱-۳: سرویس های امنیت پایگاه داده ها
۳۹	۳-۵-۱-۱-۴: سرویس های امنیت کنترل پردازش
۳۹	۳-۵-۲: مکانیسم های امنیتی
۳۹	۳-۵-۳: مسائل طراحی و پیاده سازی
۴۰	۳-۶: سرویسهای امنیت شبکه
۴۰	۳-۶-۱: استاندارد پی.ای.بی.ام
۴۱	۳-۶-۱-۱: نگاهی به پی.ای.بی.ام.
۴۲	۳-۶-۱-۲: قابلیت‌های پی.ای.بی.ام.
۴۲	۳-۶-۱-۳: سرویسها، الگوریتم های رمزنگاری و کلیدها
۴۳	۳-۶-۱-۴: محرمانگی پیغام
۴۴	۳-۶-۱-۵: مدیریت کلید
۴۴	۳-۶-۱-۶: محیط پیغام گذاری
۴۵	۳-۶-۱-۷: نمودار عملیاتی
۴۷	۳-۷-۱: برنامه پی.جی.بی.
۴۸	۳-۷-۱-۱: سرویسهای پی.جی.بی.
۴۸	۳-۷-۱-۲: کلیدهای رمزگذاری
۴۹	۳-۷-۱-۳: نمودار عملیاتی
۵۰	۳-۸-۱: مقایسه پی.ای.بی.ام. با پی.جی.بی.
۵۱	۳-۷: معماری امنیت شبکه
۵۱	۳-۷-۱: نگرش ایجاد امنیت شبکه
۵۱	۳-۷-۲: اجزای معماری امنیت شبکه
۵۱	۳-۷-۲-۱: قلمروهای امنیت شبکه
۵۲	۳-۷-۲-۲: سرویس دهنده امنیت
۵۳	۳-۷-۲-۳: سرویس های امنیتی
۵۳	۳-۷-۲-۴: مکانیسم های امنیتی
۵۴	۳-۷-۲-۵: پایگاه داده های مدیریت امنیت
۵۴	۳-۷-۳: امنیت داده های ذخیره شده
۵۵	۳-۷-۴: سرویس تصدیق اعتبار با روش کربرس
۵۵	۳-۷-۴-۱: عملیات کربرس
۵۷	۳-۷-۴-۲: معماری سرویس تصدیق اعتبار نمونه
۵۸	۳-۸: پیاده سازی سرویسهای امنیت شبکه
۵۸	۳-۸-۱: مشخصات محیط پیاده سازی
۵۸	۳-۸-۲: ابزارهای برنامه سازی استفاده شده

۵۹	فصل چهارم : پست الکترونیکی امن
۵۹	۱-۴: سرویس امنیت شبکه
۵۹	۱-۱-۴: تهدیدهای امنیتی پست الکترونیکی
۶۰	۲-۱-۴: مکانیسمهای امنیتی
۶۱	۳-۱-۴: سرویسهای امنیتی پست الکترونیکی
۶۲	۲-۴: معماری پست الکترونیکی امن
۶۲	۱-۲-۴: نرم افزار اس.ای.ام.
۶۲	۲-۲-۴: وظایف اس.ای.ام.
۶۳	۳-۲-۴: ویژگیهای اس.ای.ام.
۶۴	۴-۲-۴: مکانیسمهای امنیتی
۶۴	۵-۲-۴: نمودار عملیاتی اس.ای.ام.
۶۶	۶-۲-۴: واسط برنامه کاربردی امن
۶۷	۳-۴: پیاده سازی پست الکترونیکی امن
۶۷	۱-۳-۴: نرم افزار اس.ای.ام.
۶۸	۱-۱-۳-۴: امکانات اصلی اس.ای.ام.
۶۹	۱-۱-۲-۴: مدیریت پیغام
۶۹	۲-۱-۲-۴: مدیریت امنیت
۶۹	۳-۱-۲-۴: ویرایش نشانیها
۷۰	۴-۱-۲-۴: واسط برنامه کاربردی امن
۷۰	۲-۱-۳-۴: شرح کلی برنامه ها
۷۲	فصل پنجم: انتقال پرونده امن
۷۲	۱-۵: سرویس امنیت شبکه
۷۲	۱-۱-۵: تهدیدهای امنیتی انتقال پرونده
۷۲	۲-۱-۵: انتقال پرونده در شبکه اینترنت
۷۳	۳-۱-۵: نیازمندیهای امنیتی انتقال پرونده
۷۳	۲-۵: معماری انتقال پرونده
۷۳	۱-۲-۵: پروتکل انتقال پرونده امن
۷۵	۲-۲-۵: معماری مشتری-سرویس دهنده
۷۵	۳-۲-۵: پردازش سرویس دهنده
۷۵	۴-۲-۵: پردازش مشتری
۷۶	۵-۲-۵: نمودار عملیاتی
۷۷	۶-۲-۵: ضرورت و ویژگیهای طرح
۷۷	۳-۵: پیاده سازی انتقال پرونده
۷۷	۱-۲-۵: برنامهء سرویس دهنده
۷۸	۲-۲-۵: برنامهء مشتری
۷۹	۳-۲-۵: برنامهء مدیریت امنیت
۸۰	فصل ششم: ورود از دور
۸۰	۱-۶: سرویس امنیت شبکه
۸۰	۱-۱-۶: تهدیدهای امنیتی ورود از دور
۸۱	۲-۱-۶: تصدیق اعتبار در برنامه ورود از دوریونیکس
۸۱	۲-۶: معماری ورود از دور
۸۲	۱-۲-۶: تصدیق اعتبار

۸۲	۲-۲-۶: ایجاد نشست امن
۸۳	۳-۶: پیاده سازی ورود از دور
۸۳	۱-۳-۶: تصدیق اعتبار
۸۳	۲-۳-۶: ایجاد نشست امن
	فصل هفتم : رمزنگاری
۸۴	۱-۷: مفاهیم مبنایی رمزنگاری
۸۴	۱-۱-۷: تعریف سیستمهای رمز
۸۴	۲-۱-۷: سیستمهای رمز کلاسیک
۸۵	۳-۱-۷: سیستمهای رمزنگاری متقارن
۸۶	۱-۳-۱-۷: استاندارد رمزگذاری داده ها
۸۶	۲-۳-۱-۷: الگوریتم رمزگذاری داده های بین المللی
۸۷	۳-۳-۱-۷: الگوریتم رمزگذاری سریع
۸۸	۴-۱-۷: سیستمهای رمزنگاری جریانی
۸۸	۵-۱-۷: سیستمهای رمزنگاری نامتقارن
۸۹	۱-۵-۱-۷: سیستم رمزگذاری کلید عمومی آر.اس.ا.
۹۰	۳-۷: پیاده سازی روالهای رمزگذاری
۹۰	۱-۳-۷: استاندارد رمزگذاری داده ها (DES)
۹۰	۲-۳-۷: الگوریتم کلید عمومی (RSA)
۹۰	۳-۳-۷: الگوریتم رمزگذاری داده های بین المللی (IDEA)
۹۱	۴-۳-۷: الگوریتم درهم سازی MD4
۹۱	۵-۳-۷: الگوریتم درهم سازی MD5
۹۱	۶-۳-۷: تبدیل مبنای ۶۴
۹۱	۳-۷: سرویس نمونه تصدیق اعتبار با روش کربرس
۹۲	۱-۳-۷: برنامه های سرویس دهنده اصلی
۹۲	۲-۳-۷: برنامه های سرویس دهنده ب
۹۲	۳-۳-۷: برنامه های مشتری الف
۹۲	۴-۳-۷: روش های تبدیل گذر واژه به کلید
۹۳	۵-۳-۷: برنامه مدیریت پایگاه داده کربرس
	فصل هشتم : ارزیابی امنیت شبکه
۹۴	۱-۸: مقدمه
۹۴	۲-۸: ارزیابی امنیت
۹۴	۳-۸: معیارهای ارزیابی امنیت
۹۵	۱-۳-۸: کتاب نارنجی: معیارهای ارزیابی سیستمهای کامپیوتری معتمد
۹۵	۱-۱-۳-۸: رده بندی ارزیابی امنیت
۹۶	۲-۳-۸: معیارهای ارزیابی امنیت تکنولوژی اطلاعات
۹۷	۱-۲-۳-۸: رده بندی ارزیابی امنیت
۹۸	۳-۳-۸: مقایسه معیارهای ارزیابی امنیت
۹۸	۴-۸: معیارهای ارزیابی سرویس های امنیتی
۱۰۰	۵-۸: ارزیابی امنیت سرویس های ایجاد شده
۱۰۱	پیوست ها پیوست الف: بازگشت نامه
۱۰۲	پیوست ب: واژه نامه فارسی به انگلیسی
۱۰۸	پیوست ج: واژه نامه انگلیسی به فارسی

عنوان

فهرست شکل ها

صفحه

۸	شکل ۱ اتصال دو کامپیوتر
۹	شکل مدل ساده شبکه
۱۱	شکل استراتژی های رمزکردن
۱۲	شکل رمزگذاری و رمزگشایی
۱۵	شکل ۷ لایه سیستم OSI
۱۶	شکل تکنیک داده ها بین اجزای بین راهی در یک انتقال
۱۷	شکل Routing with Link Encryption
۱۸	شکل تکنیک داده ها بین فرستنده و گیرنده
۱۹	شکل Routing with End-to-End Encryption
۲۰	شکل امنیتی حین ارتباط سیستمها
۲۱	شکل MLS/TCP Domains of Interpretation
۲۳	شکل Placement of SNDS Protocols
۲۵	شکل Database Architectural Attacks
۲۸	شکل مشکل اجتماع داده ها
۳۰	شکل Database port to secure Base
۳۱	شکل File security for Database
۳۲	شکل Integrity Lock Architecture
۳۳	شکل رمزگذاری پیوند گرا
۳۷	شکل رمزگذاری انتها به انتها
۳۸	شکل محیط پیغام گذاری پی.ای.ام.
۴۵	شکل ارسال و دریافت پیغامهای پی.ای.ام.
۴۶	شکل ارسال و دریافت پیغامها در پی.جی.پی.
۴۹	شکل قلمروهای امنیت شبکه
۵۲	شکل سطح اول نمودار عملیاتی اس.ای.ام.
۶۴	شکل سطح دوم نمودار عملیاتی اس.ای.ام.
۶۴	شکل سطح سوم نمودار عملیاتی اس.ای.ام.
۶۵	شکل پروتکل انتقال پرونده امن
۷۴	شکل نمودار عملیاتی پردازنده مشتری
۷۶	شکل ورود به سرویس دهنده از راه دور
۸۲	شکل سیستم رمزنگاری عمومی
۸۵	شکل خلاصه الگوریتم آر.اس.ا.
۸۹	شکل فراروند ارزیابی امنیت

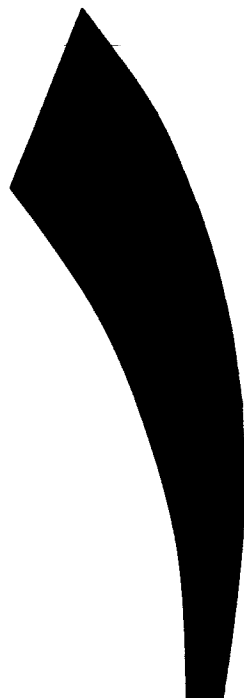
عنوان

فهرست جدول ها

صفحه

۳۲	جدول Integrity Lock Architecture
۴۳	جدول خلاصه الگوریتم های پی.ای.ام.
۴۴	جدول به کارگیری کلیدها در پی.ای.ام.
۴۸	جدول خلاصه سرویسهای پی.جی.پی.
۴۸	جدول کلیدهای رمزگذاری مورد استفاده در پی.جی.پی.
۵۰	جدول مقایسه پی.ای.ام. و پی.جی.پی.
۶۱	جدول سرویسهای پایه ای پست الکترونیکی
۸۷	جدول حالتهای عمل استاندارد رمزگذاری داده ها
۹۸	جدول مقایسه معیارهای ارزیابی امنیت

فصل اول



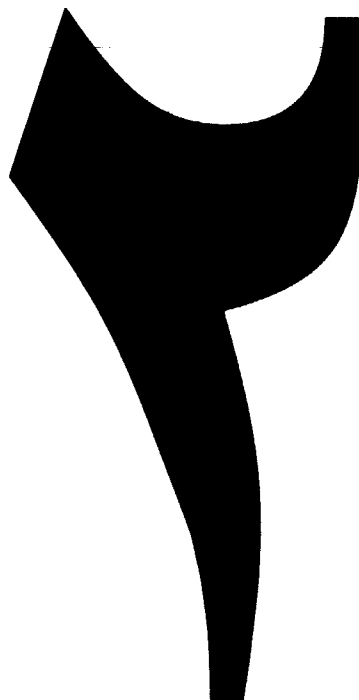
ساختار پایان نامه

فصل اول:

۱-۱: ساختار پایان نامه

- **فصل دوم:** در این فصل مباحث مبنایی امنیت سیستم های کامپیوتری مورد بحث قرار گرفته است. راههای نفوذناسته های امنیت سیستمهای کامپیوتری معرفی شده و به امنیت شبکه و همچنین امنیت پایگاه داده ها پرداخته شده است.
- **فصل سوم:** مباحث نظری امنیت سیستم های کامپیوتری، دلایل ضرورت توجه به امنیت شبکه های کامپیوتری و همچنین نگرشهای مبنایی امنیت شبکه ، ساختارهای امنیت شبکهء ایزو، مکانیسم ها و سرویس های امنیتی، استاندارد پی.ای.ام. و پی.جی.پی. که نوراه حل معروف برای امنیت هستند، بحث شده و سپس با هم مقایسه و معماری امنیت شبکه و پیاده سازی سرویس های امنیت شبکه مورد بررسی قرار گرفته اند.
- **فصل چهارم:** در این فصل به مسائل سرویس های امنیت پست الکترونیکی ، معماری ونرم افزار اس.ای.ام، وظایف و ویژگیها ، نمودار عملیاتی و سپس پیاده سازی پست الکترونیکی امن و امکانات اصلی اس.ای.ام.، مدیریت پیغام ، مدیریت امنیت ، ویرایش نشانیها و واسط کاربردی امن ، و همچنین 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 :** در این فصل نیز به مسائل سرویسهای امنیت ورود از دور، معماری ، تصدیق اعتبار و ایجاد نشست امن ، نمودار عملیاتی و سپس پیاده سازی ورود از 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 و همچنین پیاده سازی روالها و الگوریتم رمزگذاریها ، سرویس نمونه تصدیق اعتبار با 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، و نیز 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 و همچنین واژه نامه انگلیسی به فارسی و بازگشت نامه ارائه شده است.

فصل دوم



مفاهیم مبنایی امنیت

فصل دوم: مفاهیم مبنایی امنیت

۱-۲: 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 محرمانه 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 ، مطالعه سیاستها ، مکانیسمها و ابزارهای اعمال و مدیریت امنیت در سیستمهای کامپیوتری است .

تهدیدهای عمده 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 بر اساس اعتبار خود و از راه یک پایانه ، به آن متصل شده ، اما اتصال خود را قطع نکرده باشد . شخص غیرمجازی ، به این ترتیب می تواند