عنوان دوره آموزشی:
شبکه و امنیت اطلاعات در سازمان‌ها

تهیه و تدوین: سید مجتبی مصطفوی


بسم الله الرحمن الرحیم

فهرست مطالب

فصل اول:
آشنایی با فضای سایبری

آشنایی با مفاهیم اولیه سایبری

- ✓ **سایبر:**

بر اساس تعریفی از cyber age، سایبر لغتی است که به هر موجودیتی در ارتباط با کامپیوتر، فناوری اطلاعات و واقعیت مجازی اطلاق می‌شود.

- ✓ **امنیت سایبری:**

مجموعه‌ای از فعالیت‌ها، روال‌ها و سیاست‌های سازمانی در راستای حفاظت از افراد، دارایی‌های فیزیکی و دارایی‌های اطلاعاتی می‌باشد.

- ✓ **حمله سایبری:**

یک تلاش خرابکارانه با استفاده از فناوری‌های دیجیتالی است که در صورت موفق آمیز بودن باعث خرابی، از بین رفتن داده‌های اطلاعاتی یا سرقت اطلاعات محرمانه یک شخص یا سازمان می‌شود.

انواع تهدیدات سایبری

به طور کلی می‌توان انواع تهدیدات سایبری را به گروه‌های کلی زیر تقسیم کرد:

- ✓ بدافزارها و نرم‌افزارهای مخرب
- ✓ دسترسی غیر مجاز به اطلاعات سازمان یا اشخاص
- ✓ استفاده غیرمجاز از اطلاعات سازمان یا اشخاص
- ✓ حملات مهندسی اجتماعی
- ✓ حملات نقض خدمات الکترونیکی
- ✓ خرابکاری‌های تصادفی توسط کاربران قانونی

برخی از مهمترین منابع تهدیدات سایبری

- ✓ رقبای تجاری
- ✓ گروه‌های خرابکار
- ✓ دولت‌های خارجی
- ✓ پرسنل داخلی سازمان
- ✓ سازمان‌ها یا گروه‌های تروریستی

فصل دوم:

انواع تهدیدات سایبری

بدافزارها و نرم‌افزارهای مخرب

یک بد افزار مجموعه‌ای از دستورات است که بر روی کامپیوتر قربانی اجرا شده و باعث می‌شود تا سیستم آلوده، فعالیت های مورد علاقه مهاجم را اجرا نماید. بدافزارها بسیار متنوع می‌باشند اما معمولا در یکی از دسته های زیر قرار می‌گیرند:

- ✓ویروس‌ها (Viruses)
- ✓کرم‌ها (Worms)
- ✓اسب‌های تروا (Trojan Horses)
- ✓بمب‌های منطقی (Logic Bomb)
- ✓روت‌کیت (Rootkits)
- ✓جاسوس افزارها (Spywares)
- ✓تبلیغ افزارها (Adwares)

بدافزارها و نرم‌افزارهای مخرب

هدف از تولید بدافزار چیست؟

- ✓ سرقت اطلاعات شخصی و محرمانه
- ✓ پاک کردن داده‌ها
- ✓ کلیک‌های تقلبی (مثلاً در تبلیغات‌های کلیکی)
- ✓ سرقت شماره سریال نرم افزارها
- ✓ استفاده از منابع کامپیوتر شما
- ❖ انواع بدافزارها در فصل ۴ شرح داده خواهد شد.

حملات مهندسی اجتماعی

- ✓ مهندسی اجتماعی به روشی اطلاق می گردد که طی آن یک فرد غیر مجاز یا یک مهاجم، اعتماد یکی از افراد داخل سازمان را به دست آورده و از طریق آن شخص به اهداف خود می‌رسد.
- ✓ ضعیف ترین و آسیب پذیر ترین لایه امنیتی در هر سازمانی، پرسنل آن سازمان می باشند.
- ✓ به طور طبیعی انسان ها در اکثر موارد به هم اعتماد می کنند.
- ✓ انسان ها بر اساس ذات خود علاقه دارند تا به انسان دیگری کمک نمایند.
- ✓ مثال: یک نفر از تلفن داخلی با شما تماس گرفته و خود را پرسنل IT معرفی نماید و جهت ارائه یک پشتیبانی به شما رمز عبورتان را می پرسد.

حملات مهندسی اجتماعی

حملات مهندسی اجتماعی به دو دسته کلی تقسیم می‌شود:

- ✓ **مبتنی بر انسان:** از تکنیک روابط بین انسان ها یا فعالیت های آن ها برای به دست آوردن اطلاعات استفاده می کند.
- ✓ **مبتنی بر کامپیوتر:** از کامپیوتر و سایر دستگاه های پردازشی برای به دست آوردن اطلاعات استفاده می کند.

حملات مهندسی اجتماعی

مهندسی اجتماعی مبتنی بر انسان:

- ✓ **جستجو در زباله دانی:** معمولاً اطلاعات بسیار زیادی در زباله های یک سازمان یافت می‌شود. با جستجوی آن ها می توان به رمز عبور، نامه های محرمانه و غیره دست پیدا کرد.

- ✓ **جعل هویت:** مهاجم خود را به عنوان یک فرد قانونی، یکی از کارمندان سازمان یا یک شخصیت با اهمیت بالا معرفی نموده و به سازمان نفوذ می‌کند.

- ✓ **پشتیبانی فنی:** شبیه به جعل هویت می باشد اما در این جا پرسنل فنی سازمان خودشان به مهاجم کمک می نمایند. فرض کنید شخصی با واحد فناوری اطلاعات تماس گرفته و خود را به جای یکی از پرسنل معرفی کرده و ادعا کند رمز عبور سیستم را فراموش نموده است.

حملات مهندسی اجتماعی

- ✓ **پشت شانه ها:** هنگام ورود رمز عبور شخصی از پشت سر یا از کنار شما رمز عبور را ببیند.

- ✓ **همراهی:** فرد مهاجم در کنار یک فرد که اجازه ورود دارد قرار گرفته و وارد سازمان گردد و به گونه ای به نظر می آید که همراه فرد مربوطه است. همچنین می تواند از Badge تقلبی استفاده کند.

- ✓ **مهندسی اجتماعی معکوس:** مهاجم شرایطی را تدارک می بیند که شما با او تماس گرفته و اطلاعات را در اختیار آن قرار دهید. به عنوان مثال ابتدا شماره خود را به عنوان پشتیبانی فنی به اطلاع شما رسانده و سپس یک خرابی عمدی در یکی از سرویس هایی که شما استفاده می نمایید به وجود بیاورد تا شما جهت رفع مشکل با آن شخص تماس بگیرید.

حملات مهندسی اجتماعی

مهندسی اجتماعی مبتنی بر کامپیوتر:

- ✓ پنجره های Pop-up
- ✓ ترغیب کاربر به کلیک بر روی یک لینک در یک وب سایت تقلبی
- ✓ ارسال SMS برای قربانی
- ✓ قرار دادن Access Point های بیسیم در یک منطقه خاص و انتظار برای متصل شدن قربانیان به آن
- ✓ حمله ماهیگیری یا Phishing: معمولاً یک ایمیل تقلبی برای شما ارسال می شود که منبع خود را یک سازمان یا شرکت معتبر معرفی می‌کند و از شما می خواهد تا بر روی یک لینک که در ایمیل است کلیک نمایید. احتمالاً یک صفحه مشابه وب سایت اصلی باز می شود و از شما می خواهد که Login نمایید. اگر شما نام کاربری و رمزعبور خود را پر نموده و بر روی دکمه ورود کلیک نمایید، در واقع آن اطلاعات را برای مهاجم ارسال کرده اید.

شبکه‌های اجتماعی اینترنتی و تهدیدات آن

- ✓ شبکه‌های اجتماعی در واقع کانال‌های ارتباطی مبتنی بر فناوری‌های اینترنت و موبایل هستند که کاربران با استفاده از آن محتوای مورد علاقه خود را با یکدیگر به اشتراک می‌گذارند.
- ✓ این امکانات یک فرصت استثنایی برای کاربران خود فراهم می‌کند تا دوستان خود را به صورت آنلاین ملاقات کرده و یا اطلاعات و ایده‌های خود را با دیگران مطرح نمایند.
- ✓ بعضی از شبکه‌های اجتماعی در بخش‌هایی از دنیا محبوبیت بیشتری دارند مانند Orkut در برزیل، Vkontakte در روسیه و Viber در ایران، و برخی دیگر مانند Facebook، Twitter و Linkedin در سرار دنیا.

شبکه‌های اجتماعی اینترنتی و تهدیدات آن

شبکه های اجتماعی در کنار مزایای بزرگ خود باعث به وجود آمدن تهدیدهای متنوعی برای کاربران اینترنتی شده است که برخی از مهم ترین آن ها عبارتند از:

- ✓ توزیع بدافزارها به گونه ای که ممکن است سیستم کاربر با کلیک برروی یک لینک آلوده در صفحه دوستان خود آلوده به ویروس یا سایر بدافزارها شود

- ✓ لو رفتن اطلاعات شخصی افراد در اینترنت

شبکه‌های اجتماعی اینترنتی و تهدیدات آن

- ✓ جمع آوری اطلاعات شخصی کاربران توسط شرکت اداره کننده شبکه اجتماعی و فروش آن به سازمان های دولتی یا تبلیغاتی و یا انجام سو استفاده های دیگر از این اطلاعات
- ✓ قرار دادن لینک های آلوده در صفحات اجتماعی
- ✓ لو رفتن ارتباطات اجتماعی و استفاده از این اطلاعات در حملات مهندسی اجتماعی بر علیه قربانیان

شبکه‌های اجتماعی اینترنتی و تهدیدات آن

- ✓ برخی از شبکه های اجتماعی مانندfacebook به کاربران خود اجازه می دهند تا از ابزارهای متنوعی در حساب کاربری خود استفاده کنند. برخی از این ابزارها ظاهر جذابی دارند اما اهداف خرابکارانه ای را دنبال می کنند.
- ✓ به عنوان مثال در سال ۲۰۱۰ ، ۳۰۰ هزار نفر قربانی یک ابزار مشکوک در facebookشدند. داستان از این قرار بود که ناگهان پروفایل شخصی بسیاری از کاربران پیام زیر را نمایش داد :

“I am shocked!!! I’m NEVER texting AGAIN since I found this out. Video here: http://bit.ly/[REMOVED] - Worldwide scandal!”

شبکه‌های اجتماعی اینترنتی و تهدیدات آن

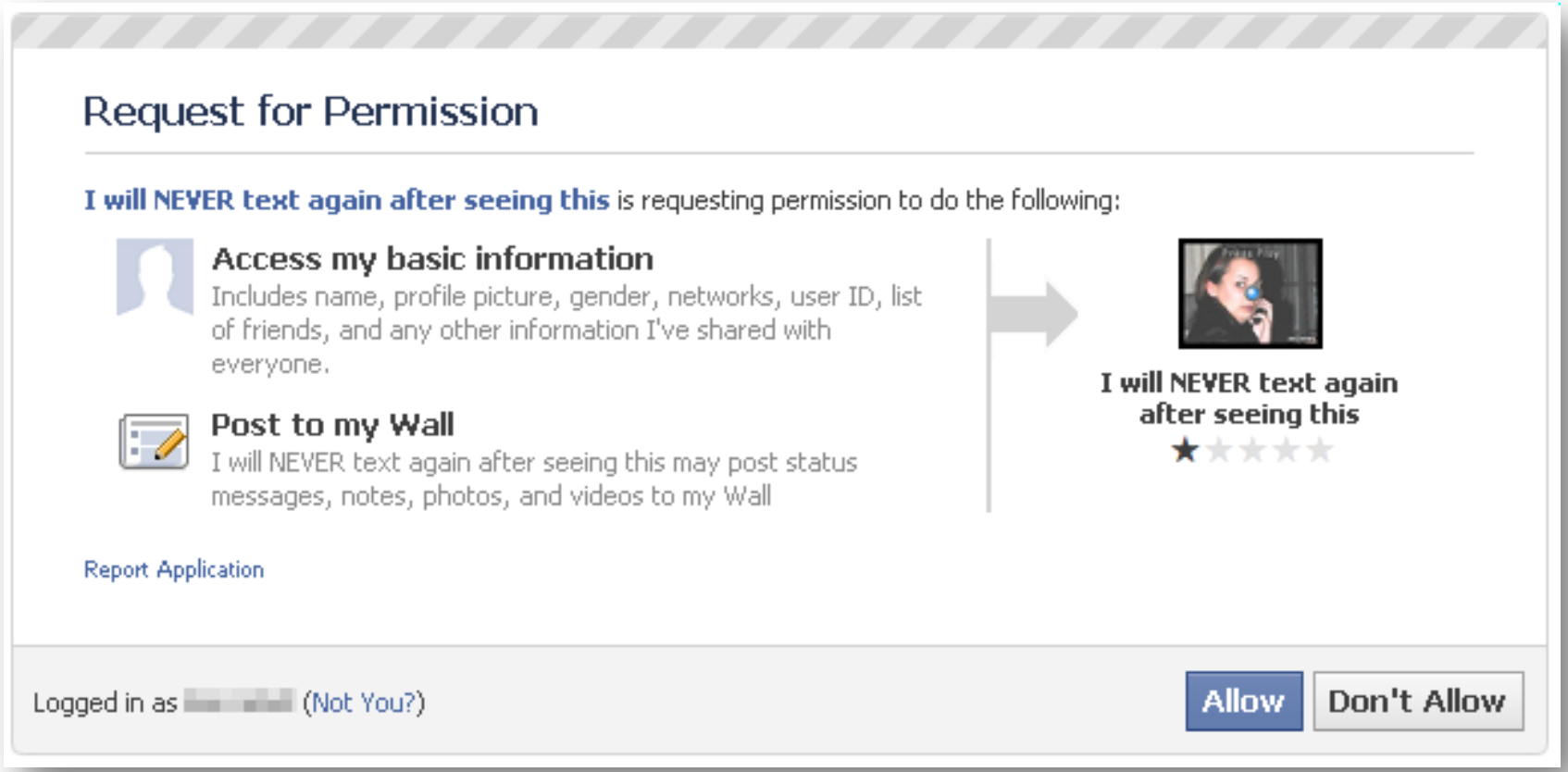
- ✓ طبق تحقیقات انجام شده حدود ۳۰۰ هزار نفر بر روی این لینک ها کلیک کردند و به صفحات مختلفی که ابزارهای خرابکارانه facebook در آن‌ها قرار داده شده بود، منتقل شدند. دو نمونه از این صفحات عبارت بودند از:

http://apps.facebook.com/wonttextagain/

http://apps.facebook.com/nevertxtingagain/

- ✓ یک نمونه درخواست اجازه دسترسی به یک ابزار مخرب در facebook در اسلاید بعد نمایش داده شده است.

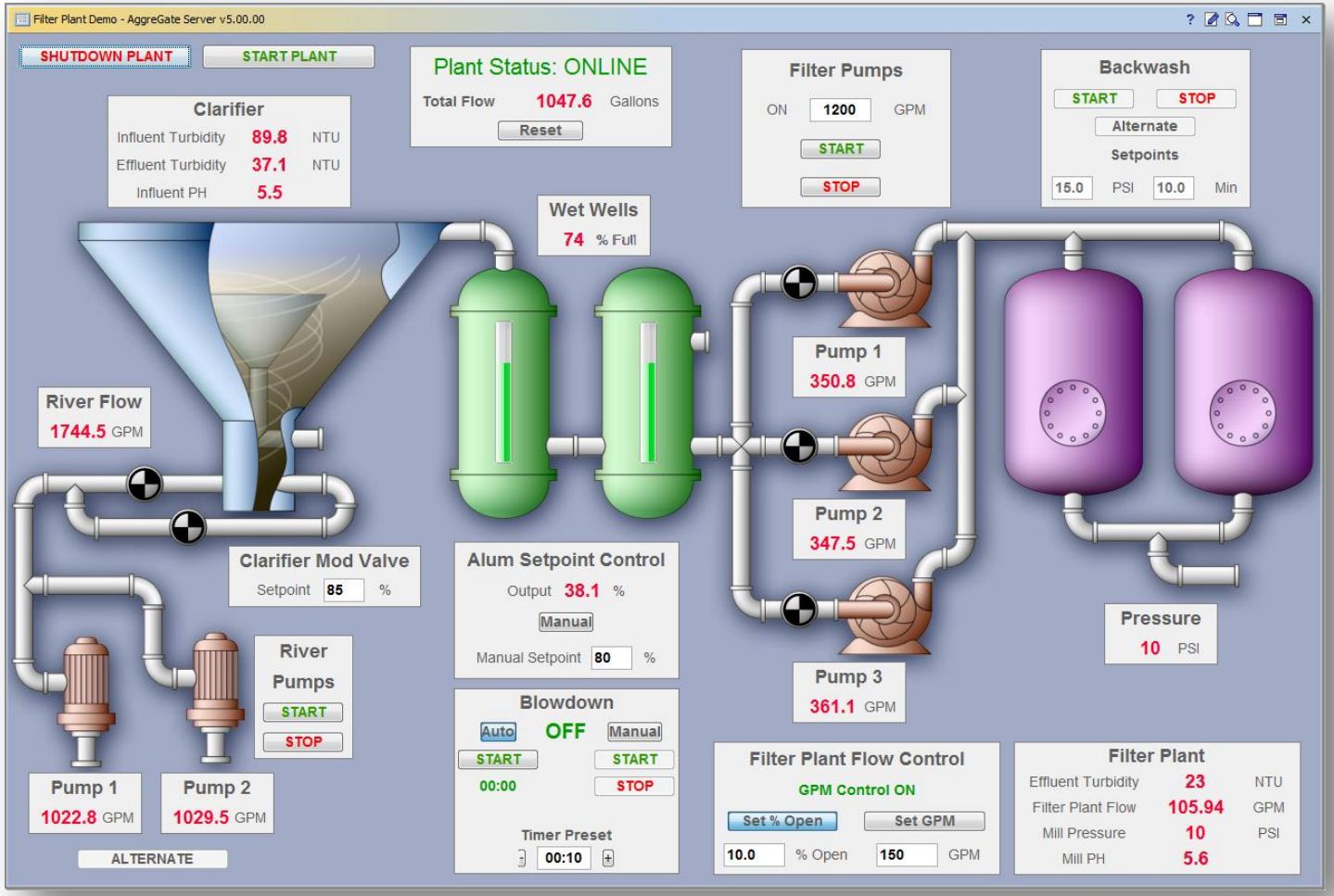
شبکه‌های اجتماعی اینترنتی و تهدیدات آن



سامانه‌های اسکادا و تهدیدات مربوط به آن

- ✓سامانه‌های اسکادا به منظور پایش و کنترل فرآیندهای صنعتی از راه دور طراحی و ساخته شدند.
- ✓سامانه‌های اسکادا همواره جزء مهمی از زیرساخت‌های حیاتی کشورها محسوب می‌شوند.
- ✓برای کنترل فرآیندها و تجهیزات صنعتی در سامانه اسکادا از دستگاهی به نام PLC (Programmable Logic Controllers) استفاده می‌شود که مشابه رایانه است.
- ✓در اسلاید بعد یک نمونه ساده از رابط کاربری اسکادا نمایش داده شده است.

سامانه‌های اسکادا و تهدیدات مربوط به آن



سامانه‌های اسکادا و تهدیدات مربوط به آن

- ✓برخی از مهمترین موارد استفاده اسکادا عبارتند از:
  - لوله‌های گاز و نفت
  - سامانه‌های آب و فاضلاب
  - سامانه‌های ترابری
  - تجهیزات الکترونیکی
  - عملیات تولید در کارخانه‌ها

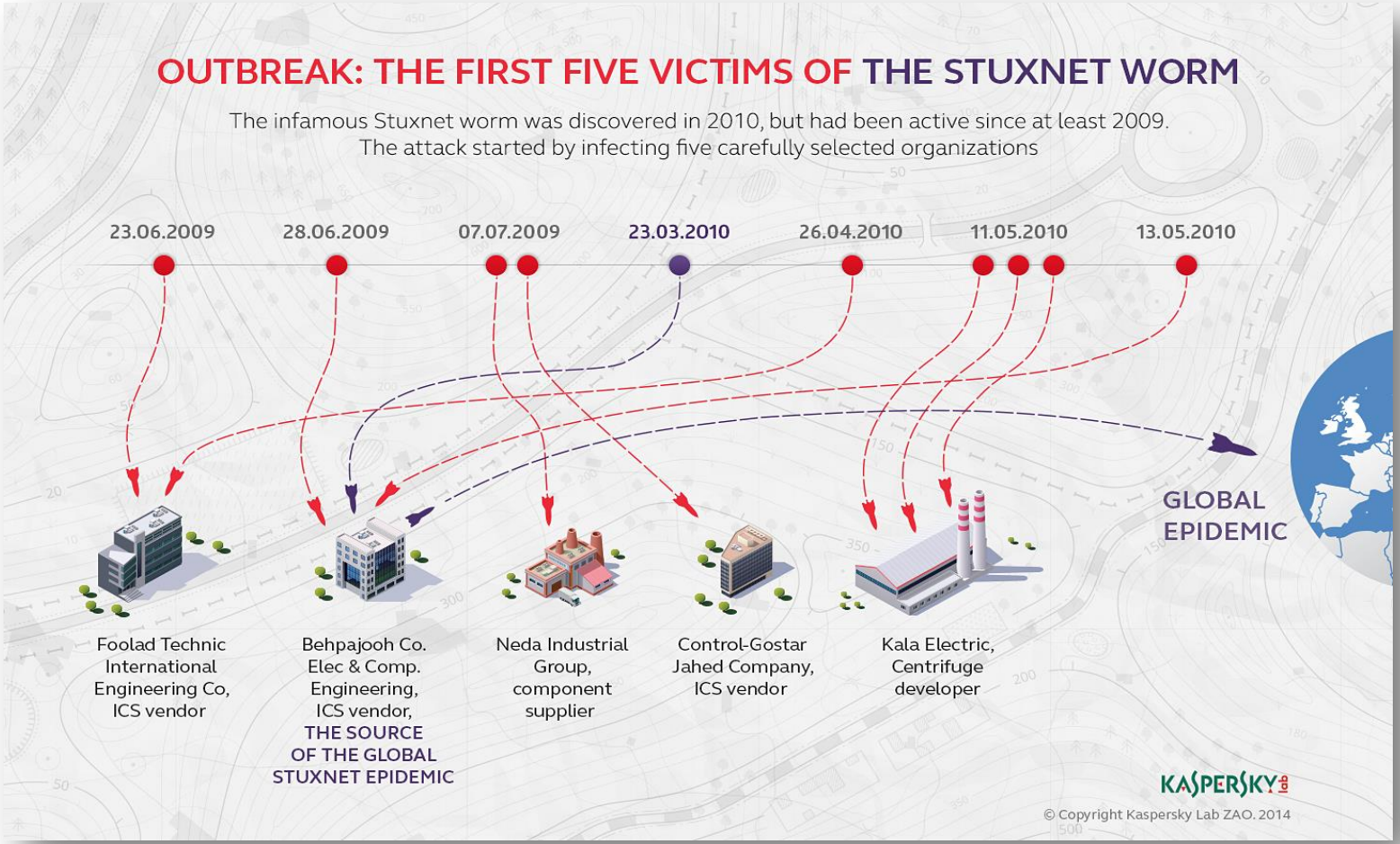
سامانه‌های اسکادا و تهدیدات مربوط به آن

- ✓ تهدیدات سایبری در سامانه‌های اسکادا بسیار مشابه تهدیدات در شبکه‌های رایانه‌ای است.
- ✓ به عنوان مثال می‌توان به توزیع بدافزارها، گسترش دسترسی، خرابکاری در سامانه‌ها و غیره اشاره نمود.
- ✓ حملات سایبری به این سامانه‌ها می‌تواند منجر به از کار افتادن واحدهای صنعتی یا حتی رخ دادن انفجار شود.
- ✓ همانطور که در شکل اسلاید بعد مشاهده می‌شود یک مهاجم از طریق اینترنت به سامانه نفوذ کرده و قسمت‌های مختلف آن را تحت کنترل خود گرفته است. فرآیند گسترش دسترسی با مسیر قرمز نمایش داده شده است.

آشنایی با بد افزار استاکسنت (Stuxnet)

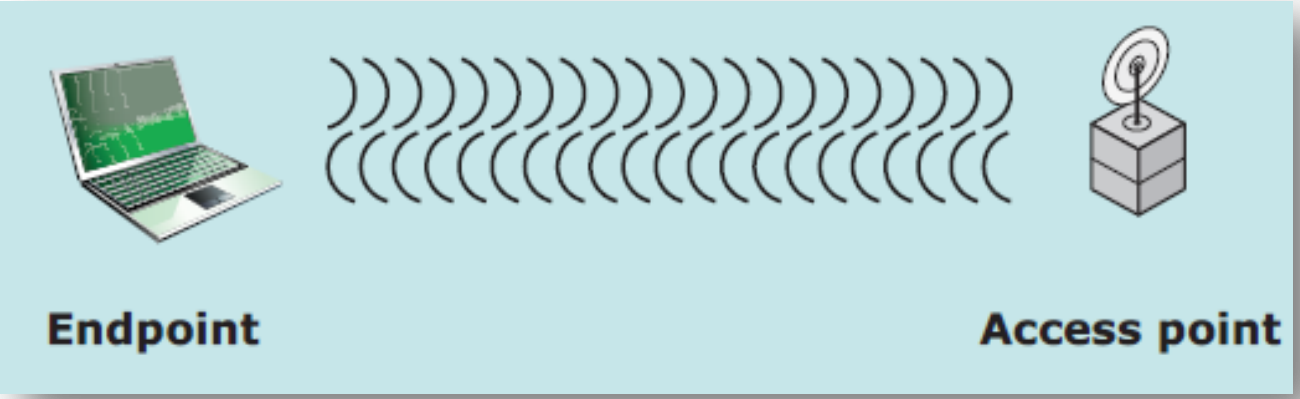
- ✓ استاکسنت تنها یک ویروس یا کرم اینترنتی ساده نیست بلکه با شناسایی آن دنیای بدافزارها وارد عصر جدیدی شد.
- ✓ اولین بدافزار شناخته شده معروفی می‌باشد که هدف آن سامانه‌های کنترل صنعتی یا همان اسکادا بوده است.
- ✓ از چندین Zero Day Exploit بهره می‌برد که هم شبکه‌های کامپیوتری و هم سامانه‌های صنعتی در برابر آن آسیب‌پذیر بوده‌اند.
- ✓ هدف اصلی آن از کار انداختن یکی از نیروگاه‌های هسته‌ای ایران بود که البته در مجموع با شکست مواجه شد.
- ✓ در اسلاید بعد اولین قربانیان این بد افزار و شیوه گسترش آن نمایش داده شده است.

آشنایی با بد افزار استاکسنت (Stuxnet)



تهدیدات شبکه‌های رایانه‌ای بی‌سیم

- ✓ استفاده از شبکه های بی سیم مزایای بسیاری دارد که مهم‌ترین آن ها راحتی کاربرد و اتصال آسان کامپیوترها به یکدیگر می باشد. در شکل زیر ارتباط بین یک کامپیوتر و یک نقطه تماس بی سیم نمایش داده شده است:



تهدیدات شبکه‌های رایانه‌ای بی‌سیم

مانند هر راهکار دیگری این راحتی کاربرد باعث به وجود آمدن تهدیدات بالقوه ای نیز شده است که عبارتند از:

- ✓ **دسترسی غیر قانونی تصادفی:** در صورتیکه بر روی نقطه تماس خود رمز عبور تنظیم نشده باشد ممکن است افراد غیر مجاز به طور تصادفی به شبکه بی سیم شما متصل شوند.
- ✓ **دسترسی خرابکارانه:** در صورت عدم استفاده از رمز عبور پیچیده یا استفاده از پروتکل های رمز نگاری ضعیف ممکن است یک مهاجم با استفاده از ابزارها و روش های خرابکارانه به شبکه بی سیم متصل شود.

تهدیدات شبکه‌های رایانه‌ای بی‌سیم

- ✓ **حمله مرد میانی:** مهاجم می تواند با استفاده از یک کامپیوتر که دارای دو کارت شبکه بی سیم است از یک طرف نقطه تماس اصلی متصل شده و از سوی دیگر نقطه تماس را برای شما شبیه سازی کند تا کامپیوتر شمابه آن متصل شود و به این ترتیب کل اطلاعات تبادل شده بین کامپیوتر و نقطه تماس را شنود کند.

- ✓ **جعل هویت:** اگر نقطه تماس از آدرسMAC کامپیوترها برای شناسایی و کنترل دسترسی آن ها استفاده کنند آنگاه یک مهاجم ممکن است با شنود داده های شبکه آدرس MAC قربانی را شناسایی و آن را جعل نماید.

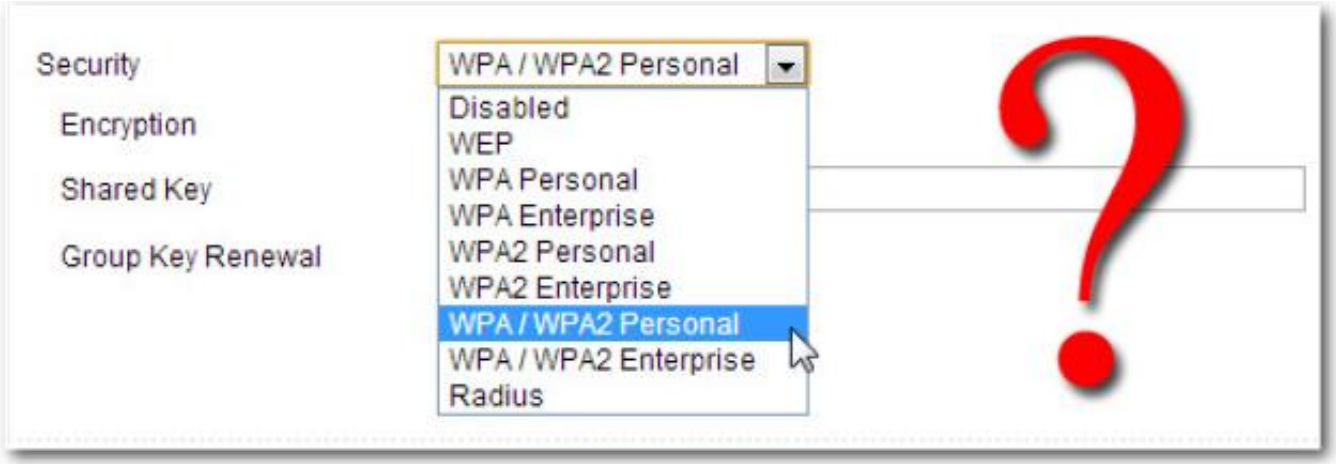
تهدیدات شبکه‌های رایانه‌ای بی‌سیم

مهم ترین الگوریتم های رمزنگاری شبکه های بی سیم به شرح زیر می باشند:

- ✓ **WEP**: اولین الگوریتم رمزنگاری مورد استفاده در شبکه های بی سیم است. در حال حاضر این الگوریتم بسیار آسیب پذیر بوده و تمام رایانه هایی که از این الگوریتم استفاده می کنند باید به روز رسانی شوند.
- ✓ **WPA**: به عنوان جایگزین الگوریتم WEPبه کار گرفته شد اما امروزه این الگوریتم غیرقابل اطمینان بوده و در برابر نفوذ مهاجمین آسیب پذیر است.
- ✓ **WPA2**: در حال حاضر به عنوان مطمئن ترین الگوریتم رمزنگاری پرکاربرد می باشد که در اکثر تجهیزات بی سیم پشتیبانی می شود. قویاً توصیه می شود در تمام شبکه های بی سیم از این الگوریتم برای رمزنگاری داده ها بهره برداری شود.

تهدیدات شبکه‌های رایانه‌ای بی‌سیم

در شکل زیر یک نمونه از فهرست الگوریتم های قابل انتخاب در یک دستگاه نقطه تماس نمایش داده شده است.



فصل سوم:

پلیس فتا (فضای تولید و تبادل اطلاعات)

یا پلیس سایبری و وظایف آن

جرایم رایانه‌ای

- ✓ همزمان با توسعه سامانه‌های رایانه‌ای، جرایم رایانه‌ای نیز به وجود آمدند.
- ✓ نسل اول جرایم رایانه‌ای تنها شامل وقوع جرم بر روی خود رایانه‌ها می‌شد.
- ✓ در نسل دوم جرایم رایانه‌ای که به عنوان جرایم علیه داده نیز از آن‌ها تعبیر می‌شود، علاوه بر داده‌های موجود در رایانه‌ها شامل داده‌های موجود در ابزارهای انتقال داده نیز می‌شد.
- ✓ نسل سوم جرایم رایانه‌ای شامل خرابکاری‌های اینترنتی نیز می‌گردد و با نام جرایم سایبری شناخته می‌شود.

ضرورت تشکیل پلیس فتا

- ✓ گسترش جرایم رایانه‌ای در دنیا باعث شد تا حکومت‌ها به فکر ایجاد سازوکار قانونی و حقوقی جهت رسیدگی و مبارزه با این‌گونه جرایم بیافتند.
- ✓ توسعه روزافزون زیرساخت‌های فناوری اطلاعات و ارتباطات در کشور از یک سو و رشد قارچ‌گونه جرایم در این حوزه از سوی دیگر لزوم ایجاد سازوکاری برای برقراری امنیت در فضای تولید و تبادل اطلاعات جمهوری اسلامی ایران را توجیه می‌کند.
- ✓ پلیس فتا در بهمن ماه سال ۱۳۸۹ رسماً آغاز به فعالیت نمود.

اهداف تشکیل پلیس فتا

- ✓ تامین امنیت فضای تولید و تبادل اطلاعات کشور
- ✓ صیانت از هویت دینی، ملی و ارزش‌های انسانی جامعه در فتا
- ✓ حفظ حریم خصوصی و آزادی‌های مشروع
- ✓ صیانت از منافع، اسرار و اقتدار ملی در فتا
- ✓ حفظ زیرساخت‌های حیاتی کشور در مقابل حملات الکترونیک
- ✓ حفاظت از اعتماد و آسودگی خاطر آحاد شهروندان جامعه برای انجام تمامی امور قانونی

چشم‌انداز پلیس فتا

فصل چهارم:

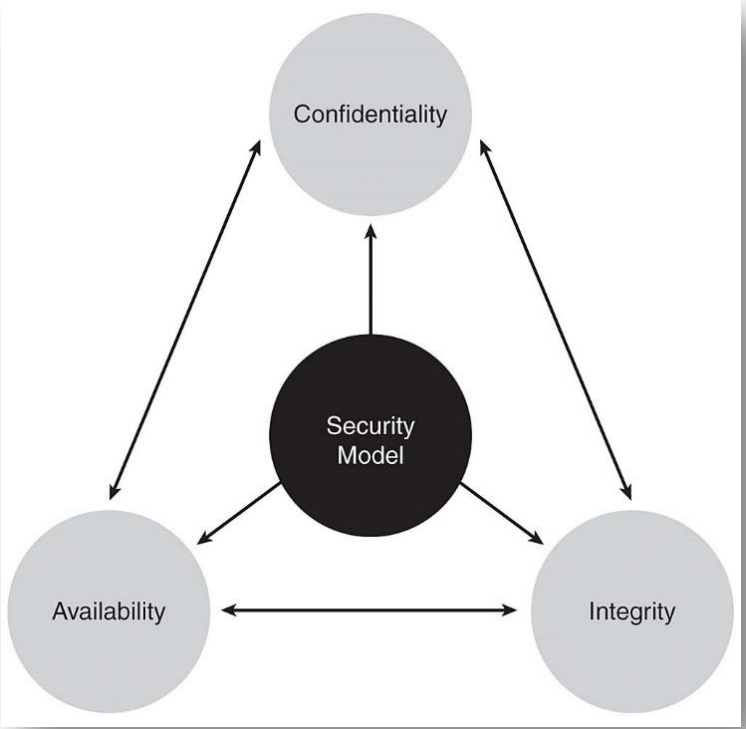
امنیت، حفاظت و نگهداری اطلاعات

مروری بر برخی مفاهیم امنیتی

- ✓ **حریم شخصی (Privacy)**: جلوگیری از دسترسی غیر مجاز به اطلاعاتی که خصوصی و شخصی تلقی می گردند.
- ✓ **شناسایی (Identification)**: پروسه ای که طی آن کاربر هویت خود را مشخص می نماید.
- ✓ **احراز هویت:** تایید و یا عدم تایید اعتبار هویت ادعا شده توسط کاربر.
- ✓ **مجوزدهی (Authorization)**: پس از تایید هویت کاربر، حقوق دسترسی های آن باید تعیین گردد.
- ✓ **بازرسی (Auditing)**: بررسی فعالیت های انجام شده توسط کاربران و همچنین نحوه عملکرد سیستم های اطلاعاتی.
- ✓ **عدم انکار (Non Repudiation)**: حصول اطمینان از این که کاربران نتوانند رویدادهای رخ داده توسط خود را انکار نمایند.

اصول امنیت اطلاعات

اهداف سه‌گانه امنیت:

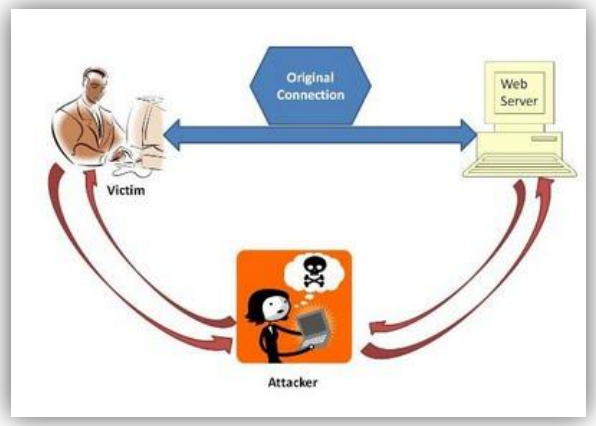


محرمانگی (Confidentiality)

- ✓ محافظت از اطلاعات در برابر افشاء غیر مجاز
- ✓ جلوگیری از دسترسی افراد به اطلاعات به صورت غیر قانونی
- ✓ اطمینان از این که سطح مناسبی از محرمانگی به داده های مختلف اعمال گردیده است
- ✓ معمولاً جهت تامین محرمانگی از رمزنگاری و کنترل دسترسی استفاده می شود

یکپارچگی (Integrity)

- ✓ اطمینان از عدم ایجاد، تغییر و یا حذف غیر مجاز اطلاعات
- ✓ باید از دقت و قابلیت اعتماد در اطلاعات و سیستم های اطلاعاتی اطمینان حاصل نمود
- ✓ باید از تغییر غیر قانونی اطلاعات ذخیره شده و یا اطلاعات در جریان، پیش گیری نمود
- ✓ مثال: استفاده از توابع Hash و امضای دیجیتال روش هایی جهت حفظ یکپارچگی اطلاعات می‌باشند



دسترسی پذیری (Availability)

- ✓ اطمینان از در دسترس بودن سرویس ها و اطلاعات برای کاربران مجاز
- ✓ حمله به آن راحت، اما حفاظت از آن بسیار دشوار می باشد
- ✓ حملات غالباً از نوع انکار سرویس (DoS) می باشند
- ✓ مثال: از دسترس خارج نمودن وب سایت خدمات الکترونیک یک بانک
- ✓ مثال: خاموش نمودن سرور اتوماسیون اداری

برخی علل بروز نقض های امنیتی

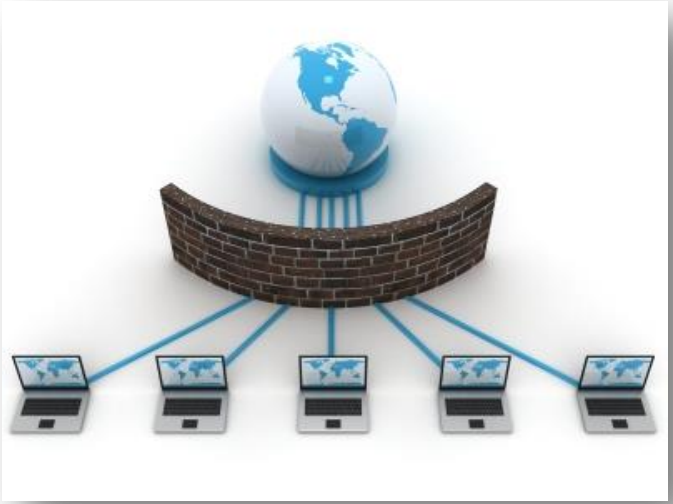
- ✓ **ضعف های موجود در فناوری:**
  - ضعف در پروتکل ها
  - ضعف سیستم عامل (ویندوز، لینوکس، مکینتاش، سولاریس و ...)
  - ضعف تجهیزات شبکه (سوییچ، روتر، سرور و ...)
- ✓ **پیکربندی و تنظیمات نادرست:**
  - عدم مدیریت صحیح Account کاربران
  - استفاده از رمز عبور ساده و قابل پیش بینی و رمز عبور پیش فرض
  - پیکر بندی اشتباه تجهیزات شبکه
- ✓ **عدم بروز رسانی سیستم عامل ها و نرم افزار های کاربردی**

برخی علل بروز نقض های امنیتی

- ✓ **ضعف سیاست های امنیتی:**
  - عدم وجود یک سیاست امنیتی مکتوب و مصوب
  - سیاست های سازمانی اشتباه
  - اهمیت ندادن به مدیریت امنیت سیستم های اطلاعاتی و شبکه
  - نصب نرم افزارها و تجهیزات مغایر با سیاست های امنیتی
  - عدم وجود برنامه ای مدون جهت مقابله با حوادث غیر مترقبه

کنترل های دسترسی به اطلاعات مهم

- ✓ کنترل های دسترسی ویژگی های امنیتی هستند که شیوه ارتباط افراد مختلف را با سیستم ها، منابع و اطلاعات مشخص می کنند
- ✓ کنترل های دسترسی باید از اهداف سه گانه امنیت (CIA) پیروی نمایند



اجزای کنترل های دسترسی به اطلاعات مهم

اجزای کنترل دسترسی که ما باید درباره آن ها تصمیم گیری کنیم عبارتند از:

- ✓ **شناسایی:** شما چه کسی هستید؟
- ✓ **احراز هویت:** ثابت نمایید همان شخصی هستید که ادعا می نمایید.
- ✓ **مجوزها:** اجازه دسترسی به چه منابعی را دارید؟
- ✓ **بازرسی یا ممیزی:** دسترسی و فعالیت های شما ثبت شده و بعداً مورد بررسی قرار می گیرد.

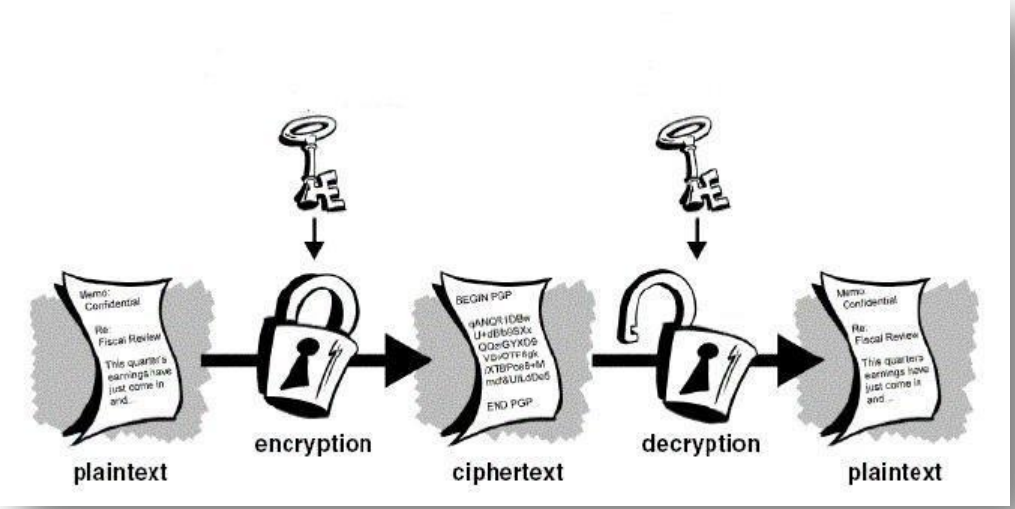
روش‌های رمزنگاری

- ✓ رمزنگاری یک روش مهم و موثر در تامین محرمانگی اطلاعات به شمار می‌آید
- ✓ اغلب اوقات حجم قابل توجهی از اطلاعات محرمانه سازمان بر روی رایانه‌های رومیزی یافت می‌شود
- ✓ با رمزنگاری اطلاعات حساس در رایانه‌ها می‌توان تا حدی مطمئن شد که این اطلاعات تنها توسط کاربران مجاز قابل دسترس هستند
- ✓ در خصوص رایانه‌های سیار توصیه می‌شود کل حافظه و یا حداقل کل پارتیشن حاوی اطلاعات رمز شود
- ✓ ایده اصلی در رمزنگاری، ذخیره و ارسال داده به شکلی که تنها افراد قانونی و مجاز بتوانند آن را تفسیر و درک کنند
- ✓ روش‌های رمزنگاری به دو دسته کلی رمزنگاری متقارن و رمزنگاری نامتقارن تقسیم می‌شود

روش‌های رمزنگاری

۱) رمزنگاری متقارن (Symmetric):

- ✓ از یک کلید مشابه برای رمزنگاری و رمزگشایی استفاده می‌شود



روش‌های رمزنگاری

- **مزایای رمزنگاری متقارن:**
  - ✓ سرعت بالا
  - ✓ امنیت بالا در صورت استفاده از کلیدهای طولانی
  - ✓ محرمانگی و یکپارچگی داده‌ها را تامین می‌کند.
- **معایب رمزنگاری متقارن:**
  - ✓ بزرگترین مشکل آن توزیع و مدیریت کلیدهای رمزنگاری است.
  - ✓ عدم انکار و احراز هویت فرستنده داده‌ها را تامین نمی‌کند.

روش‌های رمزنگاری

✓ **پرکاربردترین الگوریتم‌های رمزنگاری متقارن:**

- الگوریتم DES (Data Encryption Standard)
- الگوریتم 3DES
- الگوریتم AES (Advanced Encryption Standard)
- الگوریتم IDEA (International Data Encryption Algorithm)
- الگوریتم Blowfish
- الگوریتم‌های RC4، RC5 و RC6

روش‌های رمزنگاری

روش رمزنگاری OTP (One Time Pad):

- ✓ در واقع با اعمال تغییراتی در سیستم رمزنگاری متقارن طراحی شده است
- ✓ یک روش رمزنگاری بسیار امن است
- ✓ در صورتی که به درستی پیاده‌سازی شود غیرقابل شکستن است
- ✓ هرگاه که یک پیام ارسال گردد، از یک کلید منحصر به فرد در آن زمان استفاده می‌شود و بنابراین هر بار کلید رمزنگاری فرق خواهد کرد
- ✓ از هر کلید تنها یک بار باید استفاده می‌شود

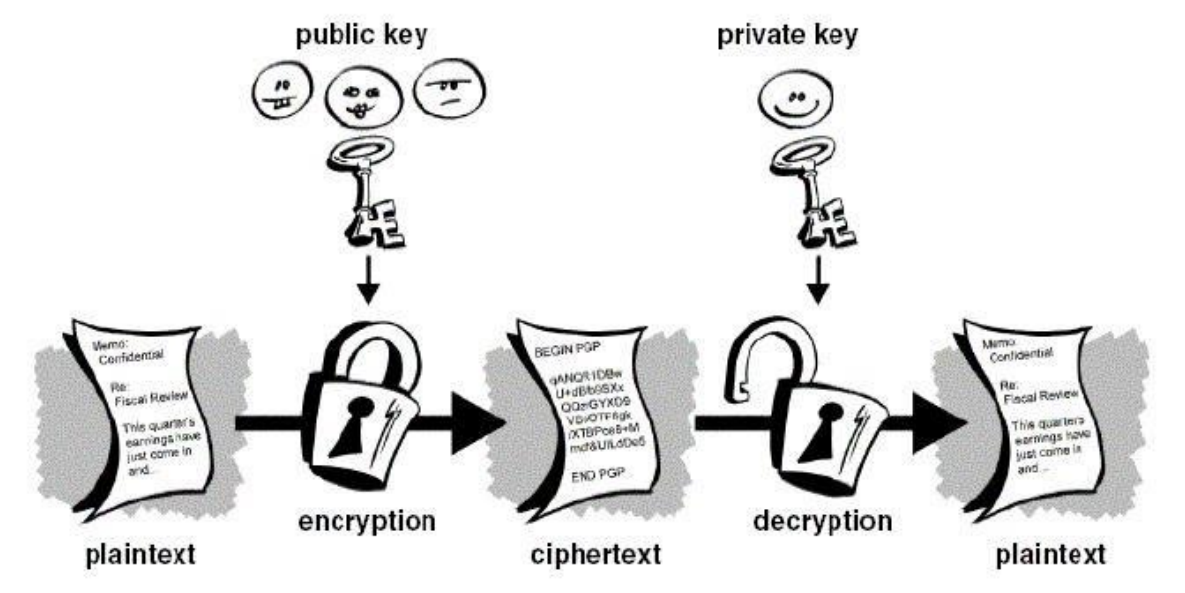
روش‌های رمزنگاری

۲) رمزنگاری نامتقارن (Asymmetric):

- ✓بجای استفاده از یک کلید یکسان، از یک زوج کلید که با روابط ریاضی به هم مرتبط هستند برای رمزنگاری و رمزگشایی استفاده می‌شود.
- ✓این زوج کلید عبارتند از کلید عمومی و کلید خصوصی
- ✓کلید عمومی می‌تواند برای هر کسی ارسال شود
- ✓کلید خصوصی محرمانه بوده و تنها در اختیار مالک آن قرار خواهد گرفت

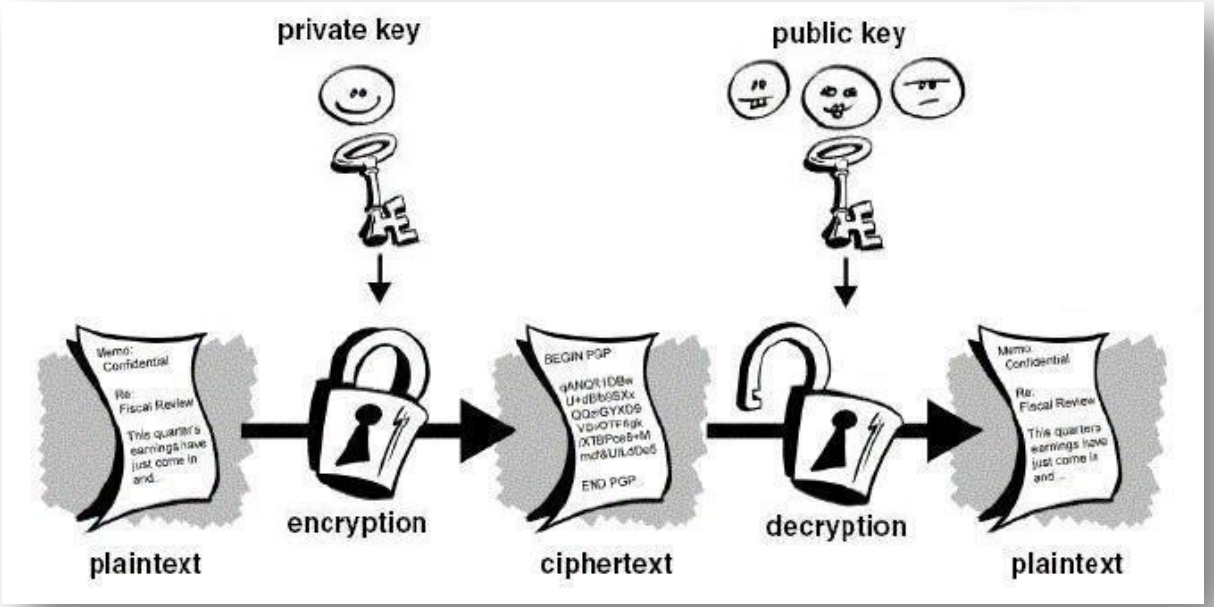
روش‌های رمزنگاری

در شکل زیر فرآیند رمزنگاری پیام توسط کلید عمومی و رمزگشایی آن توسط کلید خصوصی نمایش داده شده است:



روش‌های رمزنگاری

فرآیند رمزنگاری و رمزگشایی پیام می‌تواند به صورت برعکس نیز انجام شود که در شکل زیر نمایش داده شده است:



روش‌های رمزنگاری

مزایای رمزنگاری نامتقارن:

- ✓ توزیع کلید به سادگی صورت می‌گیرد
- ✓ به راحتی قابل توسعه است
- ✓ می‌تواند علاوه بر محرمانگی، خدمات احراز هویت و عدم انکار را نیز ارائه دهد

معایب رمزنگاری نامتقارن:

- ✓ از نظر ریاضیاتی بسیار پیچیده است
- ✓ بسیار کند است
- ✓ امنیت آن معمولاً به مراتب پایین‌تر از الگوریتم‌های رمزنگاری متقارن است

روش‌های رمزنگاری

پرکاربردترین الگوریتم‌های رمزنگاری نامتقارن:

- ✓ الگوریتم Diffe-Hellmian
- ✓ الگوریتم RSA
- ✓ الگوریتم El-Gamal
- ✓ الگوریتم Elliptic Curve

پیشگیری از سرقت اطلاعات

ابزارهای مختلفی برای پیشگیری از سرقت اطلاعات وجود دارد که اکثر آن‌ها بر روی موارد زیر تمرکز دارند:

- ✓ دسته‌بندی داده‌ها و جداسازی اطلاعات محرمانه از اطلاعات غیر محرمانه
- ✓ اعمال کنترل دسترسی بر روی داده‌های محرمانه
- ✓ رمزنگاری داده‌های محرمانه
- ✓ محافظت از داده‌ها در برابر بدافزارها
- ✓ کنترل ابزارها و نرم‌افزارهای مورد استفاده
- ✓ کنترل پست الکترونیک و داده‌های ذخیره شده در محیط رایانش ابری

تهیه نسخه پشتیبان (Backup)

- ✓ فایل پشتیبان در واقع یک نسخه کپی از اطلاعات مهم ما است که می‌تواند در هنگام نیاز، این اطلاعات را بازیابی کند.
- ✓ هدف از تهیه فایل پشتیبان، پیش‌گیری از نابودی اطلاعات مهم و یا رخ دادن تغییرات ناخواسته در آن‌ها می‌باشد.
- ✓ فایل پشتیبان از اطلاعات می‌تواند به دو روش کلی تهیه شود:
  - تهیه یک یا چند کپی ساده از داده‌ها و ذخیره آن در محل‌های متفاوت از داده اصلی
  - پشتیبان‌گیری منظم از داده‌ها با استفاده از نرم‌افزارهای مخصوص این کار

تهیه نسخه پشتیبان (Backup)

- ✓ **روال‌های بازیابی:** فایل‌های پشتیبان تهیه شده باید هر چند وقت یکبار طی روال‌های مشخص به طور آزمایشی بازیابی شوند تا اطمینان حاصل شود که در صورت ازبین رفتن داده‌های اصلی، امکان بازیابی کامل داده‌ها وجود دارد.
- ✓ پشتیبان‌گیری از داده‌ها را می‌توان به دو دسته کلی تقسیم کرد:

۱) پشتیبان‌گیری کامل: در هر بار اجرا از کل داده‌ها فایل پشتیبان تهیه می‌شود.

۲) پشتیبان‌گیری از تغییرات: در اولین مرحله از کل داده‌ها یک فایل پشتیبان تهیه و پس از آن در هر بار اجرا تنها از تغییرات به وجود آمده در داده‌ها پشتیبان گرفته می‌شود. به این ترتیب فایل‌های پشتیبان حجم دیسک کمتری را اشغال می‌کنند. اما این روش پشتیبان‌گیری نیاز به دقت بیشتری دارد.

تهیه نسخه پشتیبان (Backup)

- نرم‌افزارهای متعددی برای پشتیبان‌گیری از اطلاعات موجود بر روی رایانه‌های رومیزی یا لپ‌تاپ وجود دارد و با یک جستجوی ساده در این اینترنت قابل دسترس هستند. برخی از معروفترین این ابزارها عبارتند از Acronis True Image، Norton ghost و ... .
- این ابزارها قابلیت پشتیبان‌گیری از فایل و پوشه، یک درایو و یا کل دیسک سخت را دارند.

گواهینامه‌های دیجیتالی

- گواهینامه دیجیتالی (digital certificate) در واقع یک فایل دیجیتالی است که هویت یک شخص، موسسه و یا حتی یک دستگاه را مشخص می‌کند. این فایل توسط یک مرکز صدور گواهی (Certification Authority یا CA) معتبر صادر می‌شود و در عمل مشابه یک گواهینامه رانندگی یا یک پاسپورت است.
- مرکز صدور گواهی معادل دیجیتالی دفاتر صدور پاسپورت در دنیای واقعی می‌باشد. آن‌ها گواهینامه‌های دیجیتالی را صادر کرده و هویت مالک آن را تایید می‌کنند.

گواهینامه‌های دیجیتالی

چهار نوع اصلی گواهینامه‌ها عبارتند از:

- ✓ **گواهینامه سرور:** به عنوان مثال هنگام اتصال به یک سرور بانک شما می‌توانید گواهینامه آن سرور را مطالعه نمایید تا از صحت خدمات آن سرور مطمئن شوید.
- ✓ **گواهینامه شخصی:** هویت یک شخص را تایید می‌کند.
- ✓ **گواهینامه سازمانی:** هویت یک سازمان خصوصی یا دولتی را تایید می‌کند.
- ✓ **گواهینامه توسعه دهنده:** هویت توسعه دهنده یک نرم افزار خاص را تایید می‌کند.

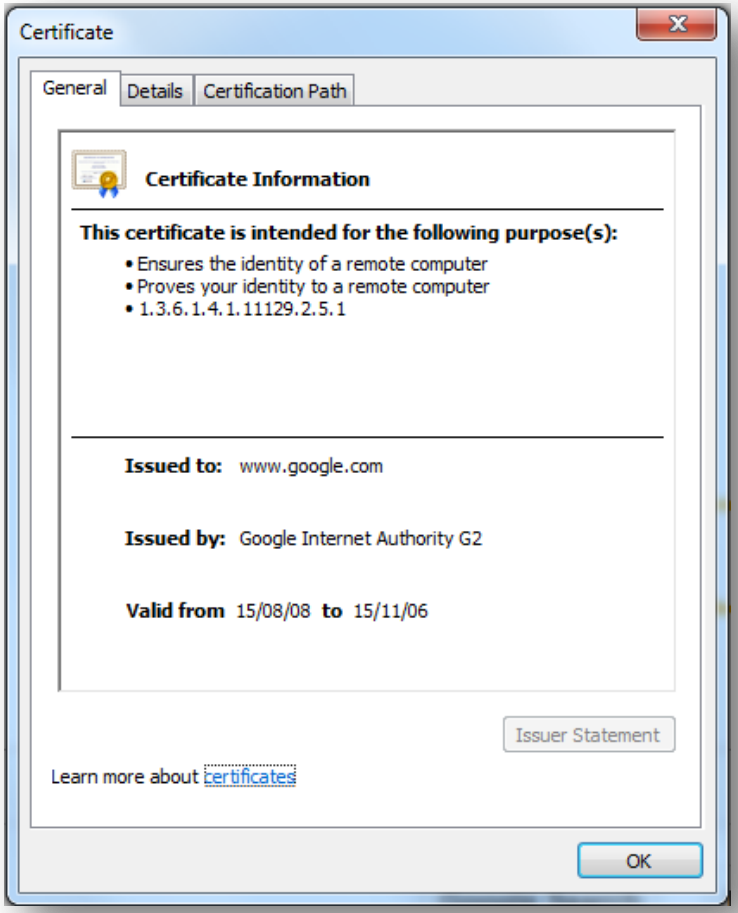
گواهینامه‌های دیجیتالی

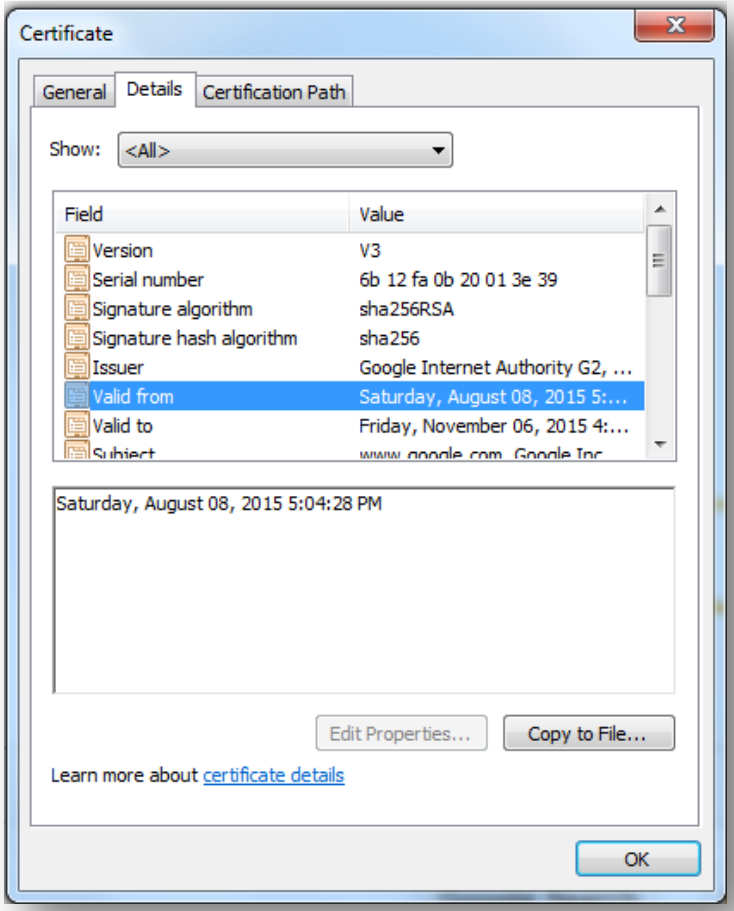
یک گواهینامه دیجیتال استاندارد شامل اطلاعات زیر می‌شود:

- ✓ نام صادرکننده گواهینامه
- ✓ نام مالک گواهینامه
- ✓ موضوع
- ✓ تاریخ صدور
- ✓ تاریخ انقضاء
- ✓ امضای دیجیتال صادرکننده گواهینامه و ...

در اسلاید بعد یک نمونه گواهینامه دیجیتالی سایت google.com نمایش داده شده است.

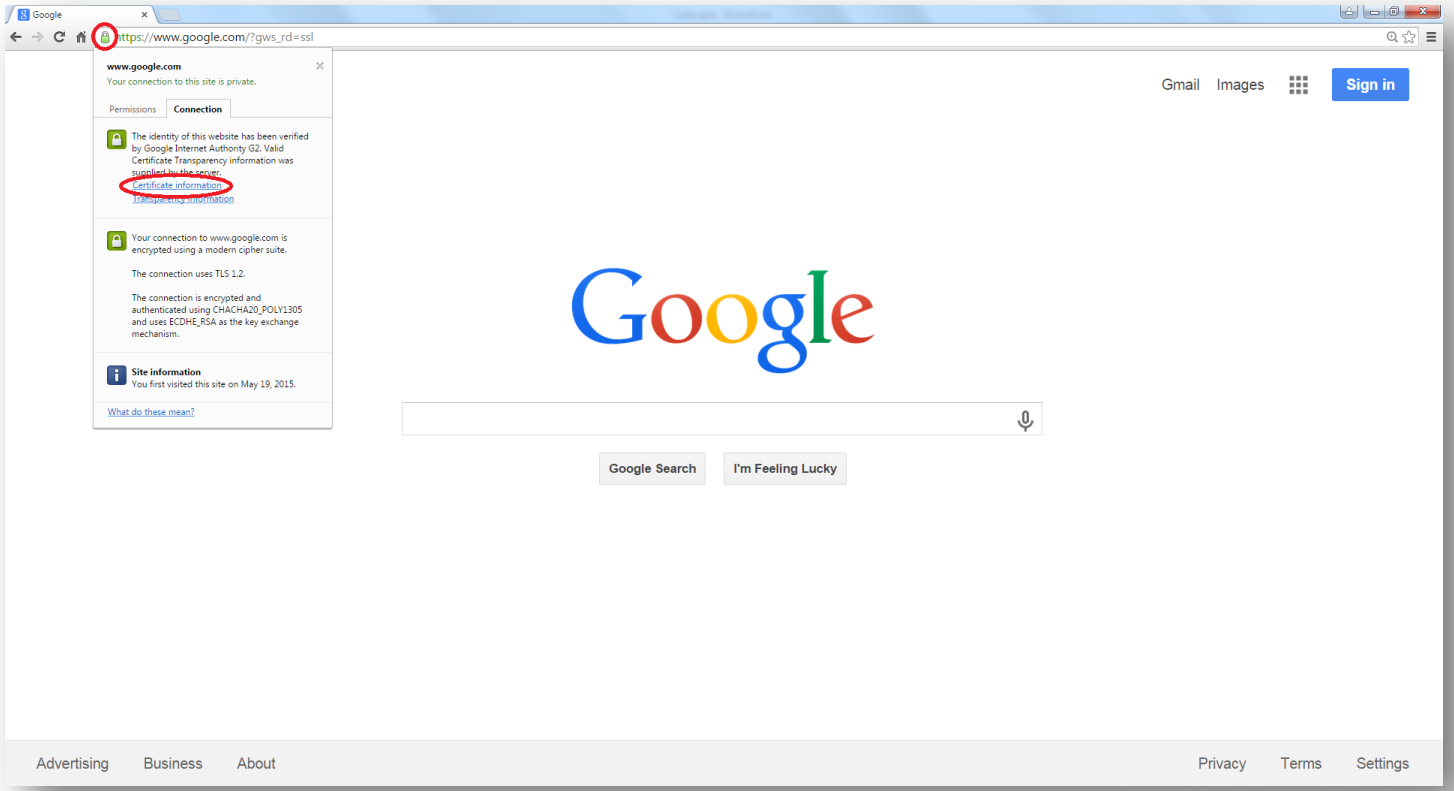
گواهینامه‌های دیجیتالی





گواهینامه‌های دیجیتالی

برای جزییات گواهینامه دیجیتال یک وب سایت می‌توانید با کلیک بر روی آیکون «قفل» در گوشه سمت چپ بالای مرورگر وب خود این اطلاعات را مشاهده کنید.



انواع بدافزارها و نرم‌افزارهای مخرب

ویروس:

یک برنامه یا قسمتی از یک کد می‌باشد که بر روی کامپیوتر شما و بدون اطلاعتان نصب می‌شود. ویروس‌ها می توانند خود را تکرار (Replicate) نمایند. به عبارت دیگر یک ویروس ساده می‌تواند خود را بارها کپی نموده و در جاهای مختلف توزیع نماید.

انواع بدافزارها و نرم‌افزارهای مخرب

کرم‌ها:

یک برنامه یا الگوریتم می‌باشد که خود را در سراسر شبکه کامپیوتری توزیع می‌کند و معمولا به منظور فعالیت‌های خرابکارانه استفاده می‌شود. تفاوت آن‌ها با ویروس‌ها این است که کاملاً خودکفا بوده و برای اجرا یا توزیع نیاز به هیچ نرم افزار میزبانی ندارند.

انواع بدافزارها و نرم‌افزارهای مخرب

بمب منطقی:

یک کد برنامه نویسی شده است که در یک نرم افزار یا سیستم عامل قرار داده می‌شود. این برنامه، بی صدا و بدون هیچ فعالیتی در سیستم باقی می‌ماند تا یک عامل محرک از قبل پیش بینی شده رخ دهد. این عامل محرک می‌تواند زمان، مجموعه‌ای از اتفاقات، باز شدن یک وب سایت یا هر چیز دیگری باشد.

انواع بدافزارها و نرم‌افزارهای مخرب

اسب تروا:

برنامه‌ای مخرب با ظاهری فریبنده می‌باشد که معمولا به صورت یک نرم افزار مفید یا یک بازی جذاب به نظر می‌آید. برخلاف ویروس‌ها، خود را گسترش نمی‌دهد اما فعالیت‌های مخرب انجام خواهد داد. یکی از انواع متداول آن برنامه‌هایی هستند که ادعا می‌کنند کامپیوتر شما را از ویروس‌ها پاک خواهند کرد اما در واقع ویروس جدیدی بر روی سیستم تولید می‌نمایند.

انواع بدافزارها و نرم‌افزارهای مخرب

روت کیت:

یک کامپوننت می‌باشد که به منظور ایجاد یک دسترسی پنهان و دائمی (گاهی اوقات غیر قابل پاک کردن) به یک سیستم استفاده می‌شود. معمولا بر روی هسته سیستم‌عامل نصب می‌گردد.

انواع بدافزارها و نرم‌افزارهای مخرب

جاسوس افزار و تبلیغ افزار:

جاسوس افزار: با هدف سرقت اطلاعات شخصی قربانی یا اطلاعات محرمانه سازمان‌ها به کار می‌رود.

تبلیغ افزار: با هدف تبلیغات و کسب درآمد برای مهاجمین استفاده می‌شود. یک نمونه متداول، بدافزارهایی هستند که به صورت خودکار صفحات تبلیغاتی وب را بر روی سیستم قربانی باز می‌کنند.

انواع بدافزارها و نرم‌افزارهای مخرب

درب پشتی:

یک مکانیزم پنهان می‌باشد که به منظور نقض کردن کنترل‌های دسترسی در سیستم‌ها به کار می‌رود. به عبارت ساده‌تر یک راه ورودی پنهان برای مهاجمین در سیستم قربانی ایجاد می‌نماید.

انواع بدافزارها و نرم‌افزارهای مخرب

بدافزارهای چند وجهی:

یک نوع بدافزار مانند ویروس، کرم و غیره به طور مستمر شکل و ظاهر خود را تغییر می‌دهد و به این ترتیب شناسایی آن توسط آنتی ویروس‌ها می‌تواند بسیار دشوار شود.

فصل پنجم:

روش‌های احراز هویت

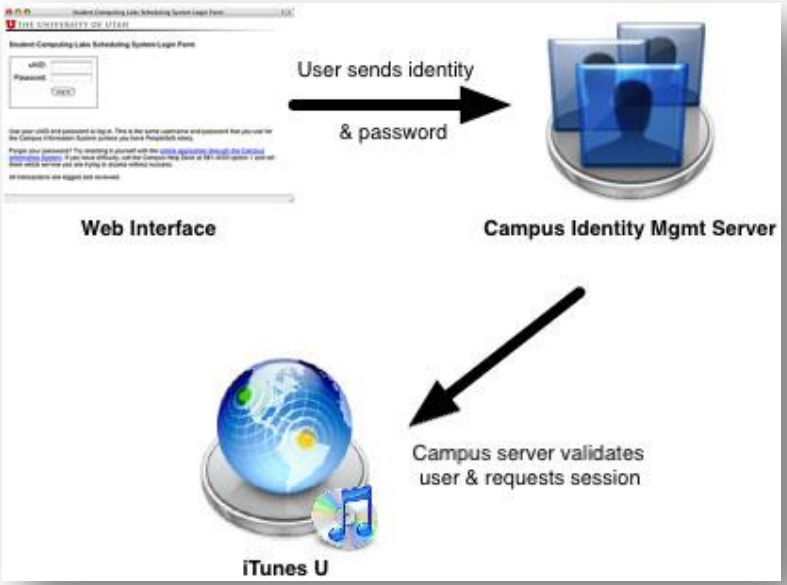
انواع احراز هویت

- عوامل احراز هویت در سه گروه زیر دسته بندی می شود:

✓آن چه شما می دانید

✓آن چه شما در اختیار دارید

✓آن چه شما هستید



آن چه شما می دانید!

- معمولاً عبارتی می باشد که آن را به خاطر می سپارید:

✓Password

✓Passphrase

✓PIN (Personal Identity Number)

✓Combination Lock

❖نکته: ضعیف ترین عامل احراز هویت می باشد

ویژگی های یک رمز عبور مناسب

- ✓ هیچ گاه از نام خود یا نزدیکان خود، نام کاربری، آدرس ایمیل، کد پرسنلی یا کد ملی، شماره تلفن در رمز عبور استفاده ننمایید
- ✓ سعی کنید لغات عامیانه یا لغاتی که در فرهنگ لغات موجود است را به کار نبرید
- ✓ از ترکیب حروف کوچک و بزرگ استفاده نمایید
- ✓ از ترکیب حروف، اعداد و سایر کارکترها استفاده نمایید

آن چه شما در اختیار دارید!

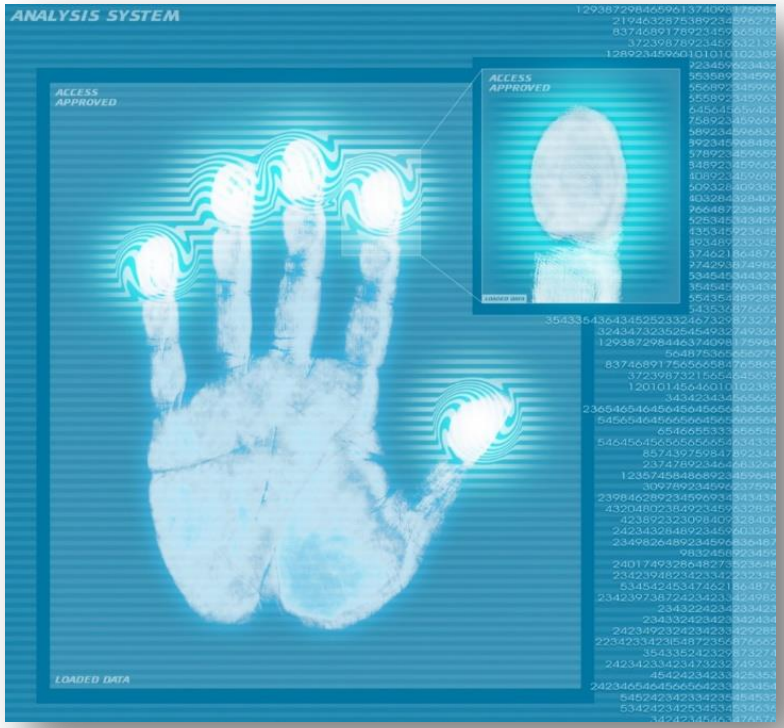
✓ یک وسیله فیزیکی می باشد که شخص با استفاده از آن احراز هویت می گردد:

- Smart Card
- USB Token
- Memory Card

❖ Memory Card توانایی پردازش داده ها را ندارد اما Smart Card دارای یک پردازنده کوچک می باشد.

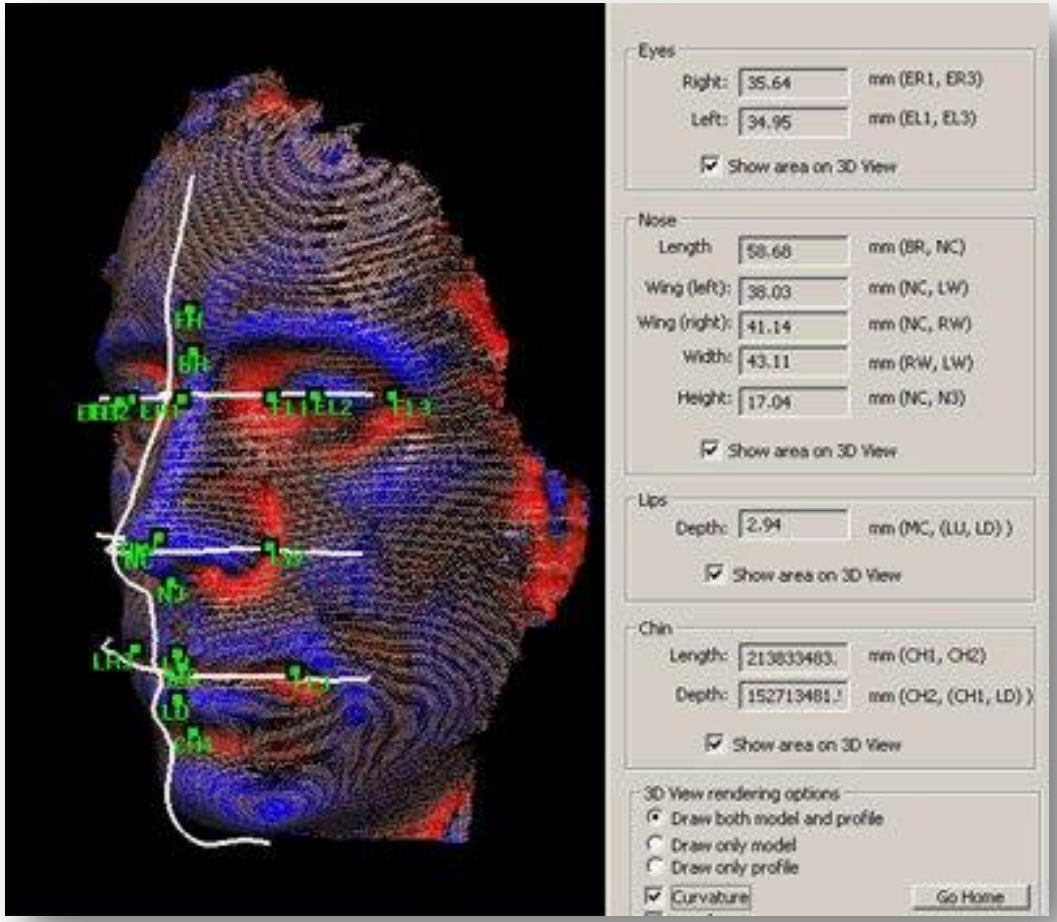
آن چه شما هستید!

ویژگی های فیزیکی شما می باشد که برای احراز هویتتان استفاده می گردد:



- ✓ اثر انگشت (Finger Print)
- ✓ صدا (Voice)
- ✓ عنبیه چشم (Iris)
- ✓ شبکیه چشم (Retina)
- ✓ چهره
- ✓ خطوط کف دست

آن چه شما هستید!



احراز هویت چند عامله

- ✓ معمولاً استفاده از هیچ یک از عوامل ذکر شده به تنهایی قابل اطمینان کامل نیستند
- ✓ برای مقابله با این مشکل از ترکیب دو یا چند عامل استفاده می کنند:
  - Smart Card یا Token به همراه PIN
  - رمز عبور به همراه اثر انگشت
  - اسکن شبکیه چشم به همراه Smart Card