امنیت تجارت الکترونیک

فصل اول:
مفاهیم امنیتی و مقدمه ای بر امنیت تجارت الکترونیکی

تهیه و تنظیم: دکتر آرش حبیبی لشکری

اولین نسخه: دی 1393
بروزرسانی: شهریور1394

فهرست:

- سرفصلهای این درس
- تعاریف
- اهداف امنیتی
- سایر اهداف و چالشها
- حملات و خطرات
- انواع حملات
- سرویسهای امنیتی
- مکانیزمهای امنیتی
- تهدیدهای تجارت الکترونیک
- نقاط ضعف یک انتقال الکترونیکی
- حملات رایج در تجارت الکترونیک
- روشهای پیشگیری

سرفصلهای این درس

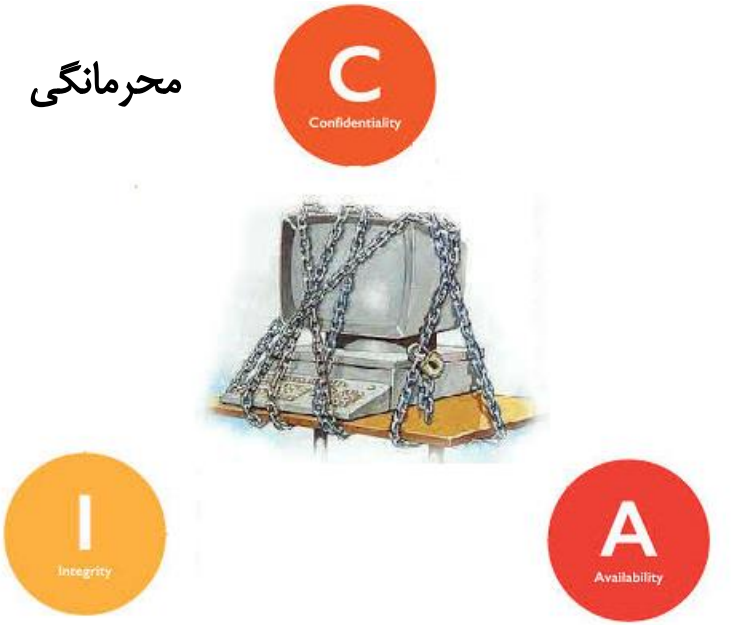
سرفصل ها:

- مقدمه
- مکانیزمهای امنیتی و مدیریت کلید و گواهینامه ها
- بدافزارها و حملات
- سیستمهای پرداخت و امنیتهای مرتبط
- امنیت پول الکترونیکی
- امنیت چک الکترونیکی
- پروتکل IOTP
- شبکه ارتباطی و امنیت لایه دسترسی شبکه
- امنیت لایه های انتقال، اینترنت و کاربردی
- امنیت وب ، سرویس دهنده و کاربر
- امنیت موبایل، عامل موبایل و تجارت موبایل
- امنیت کارتهای هوشمند

تعاریف اصلی

تعریف و اهداف امنیت

حفاظت داده شده به یک سیستم اطلاعاتی مکانیزه بمنظور بدست آوردن اهداف کاربردی شامل حفظ یکپارچگی، دسترس‌پذیری و محرمانگی منابع آن سیستم اطلاعاتی را امنیت گویند.



محرمانگی

یکپارچگی

دسترس پذیری

تعاریف اهداف امنیت

محرمانگی: این عبارت به دو مفهوم بر می‌گردد:

محرمانگی داده: اطمینان از اینکه اطلاعات محرمانه و شخصی برای افراد احراز هویت نشده قابل دسترس نبوده و فاش نمی‌شود.

حریم خصوصی: اطمینان از اینکه افراد بتوانند کنترل کنند که چه اطلاعاتی مربوط به آنها جمع‌آوری شده و ذخیره می‌گردد و همچنین بوسیله چه کسانی و برای چه کسانی این اطلاعات ارسال شده و فاش می‌شود.

یکپارچگی: این عبارت به دو مفهوم برمی‌گردد:

یکپارچگی داده: اطمینان از اینکه اطلاعات تنها در یک وضعیت خاص و تایید شده تغییر می‌یابند.

یکپارچگی سیستم: اطمینان از اینکه یک سیستم توابع انتخابی خود را در وضعیت سالم و بدون عیب و دور از دستکاریهای تایید نشده عمدی یا سهوی اداره می‌نماید.

دسترس پذیری: اطمینان از اینکه سیستمها بدون معطلی کار می‌کنند و سرویسها همواره برای کاربران احراز هویت شده فعال و در دسترس هستند.

مشخصات اهداف امنیت

محرمانگی: حفظ محدودیت مجوزها روی دسترسی و فاش نمودن اطلاعات بهمراه معانی حفاظت از استقلال پیامهای شخصی و اطلاعات اختصاصی. در واقع فقدان محرمانگی باعث فاش شدن غیر مجاز اطلاعات خواهد شد.

یکپارچگی: محافظت در برابر دستکاری و خرابی غیرمجاز اطلاعات شامل اطمینان از عدم انکار فعالیت‌ها و اعتبار اطلاعات. در واقع فقدان یکپارچگی باعث دستکاری بدون مجوز یا خرابی اطلاعات خواهد شد.

دسترس پذیری: اطمینان از دسترسی بموقع و قابل اعتماد به اطلاعات و استفاده از آنها. فقدان دسترس پذیری باعث قطع دسترسی و استفاده بموقع از اطلاعات یا یک سیستم اطلاعاتی خواهد شد.

سایر مفاهیم در امنیت

اعتبار: ویژگی واقعی بودن و توانایی بازبینی شدن و قابل اعتماد بودن، یعنی اطمینان در قابلیت اعتماد به یک انتقال، یک پیغام، یا مولد یک پیغام. این بدین معناست که کاربر همان کسی است که ادعا می‌کند و هر ورودی رسیده به سیستم از منبع قابل اعتمادی ارسال شده است.

پاسخگویی: هدف امنیتی که باعث می‌شود نیاز به ردیابی فعالیتهای یک موجودیت تنها از طریق همان موجودیت انجام گردد را پاسخگویی گویند. این مفهوم عملیاتی چون عدم انکار فعالیت، بازداری از انجام یک عملیات، تشخیص علت و محل ایجاد مشکل، پیشگیری و تشخیص نفوذ، و فعالیتهای بازیابی و منطقی پس از آنها را پشتیبانی می-نماید.

معماری امنیتی

- **حمله امنیتی**: هر فعالیتی که امنیت اطلاعات متعلق به یک سازمان را بخطر بیاندازد.

- **سیاستهای امنیتی**: تعریف آنچه که باید برای یک سازمان یا سیستم امن باشد. برای یک سازمان محدودیت رفتار و یا محدودیت دسترسی به اطلاعات سازمان با اجرای مکانیزمهای امنیتی لازم،و یا برای یک سیستم محدودیتهای مرتبط با عملکرهای یک سیستم یا کنترل میزان دسترسی به اطلاعات و پردازشهای سیستم.

- **سرویس امنیتی**: یک پردازش یا سرویس ارتباطی که امنیت سیستمهای پردازش داده و انتقال اطلاعات یک سازمان را بهبود دهد. سرویسها حملات امنیتی را تشخیص داده و از یک یا چند مکانیزم امنیتی برای مهیا نمودن سرویس استفاده می‌نمایند.

- **مکانیزم امنیتی**: یک پردازش (یا یک تجهیز که چنین پردازشی را داراست) که برای تشخیص، پیشگیری یا بازیابی اطلاعات از یک حمله امنیتی طراحی شده است.

آسیب پذیری، خطر، حمله و ریسکهای امنیتی

- آسیب پذیری یا Vulnerability: یک عیب یا شکاف در سیستم که میتواند برای حمله باز و آماده باشد. درواقع هر نوع ضعف موجود در سیستم که به یک مهاجم اجازه دهد تا با حمله به سیستم ضمانت اطلاعاتی آن را کاهش دهد.
- خطر، تهدید یا Threat: یک پتانسیل برای نقض امنیت که همواره وجود داشته و زمانی که شرایط، توانایی، فعالیت، یا اتفاق خاصی بوجود آید می‌تواند امنیت را نقض کرده و ایجاد آسیب نماید. در واقع Threat، یک خطر احتمالی است که از یک نقطه ضعف استفاده می‌نماید.
- حمله یا Attack: یک تهاجم به سیستم امنیتی که از یک خطر هوشمندانه حاصل شده است. در واقع حمله یا Attack، یک فعالیت هوشمندانه‌ای است که بصورت تلاشی عمدی برای گریز از سرویسهای امنیتی و ایجاد نقص در سیاست امنیتی یک سیستم انجام می‌گیرد.
  - ✓ حملات منفعل : بطور ذاتی درحال استراق سمع یا بازبینی انتقالها هستند. هدف طرف مهاجم بدست آوردن اطلاعاتی است که منتقل می‌شوند. (مانند آنالیز ترافیک)
  - ✓ حملات فعال: در ایجاد تغییراتی در جریان داده یا تولید یک رشته کاذب شرکت نموده و می‌توانند به چهار دسته تقسیم شوند: ناشناس، بازپخش، دستکاری پیامها، و محرومیت – از - خدمات.
- آنالیز ریسک عبارت است از بررسی ارتباط بین سه عامل:

(جدیت یک خطر) و (احتمال وقوع آن خطر) و (هزینه پیاده سازی یک مکانیزم امنیتی مناسب آن خطر)

سرویسهای امنیتی

در استاندارد X.800 :

یک سرویس امنیتی عبارت است از سرویسی است که توسط یک پروتکل لایه‌ای در سیستم‌های باز ارتباطی مهیاگردیده و از امنیت کافی سیستمها و یا انتقال داده‌ها درآن اطمینان حاصل شده باشد.

در سند RFC4949 :

یک پردازش یا سرویس ارتباطی که توسط یک سیستم برای دادن یک نوع خاص حفاظت به منابع سیستم مهیاگردیده است؛ سرویسهای امنیتی در واقع سیاستهای امنیتی را پیاده‌سازی نموده و توسط مکانیزمهای امنیتی پیاده‌سازی می‌شوند.

انواع سرویسهای امنیتی

- احراز هویت
- کنترل دسترسی
- محرمانگی داده
- یکپارچگی داده
- عدم انکار

سرویسهای امنیتی: احراز هویت

سرویس احراز هویت نگران معتبر بودن یک ارتباط است

- در مورد موضوع مربوط به یک پیام منفرد، مانند یک سیگنال آگهی یا زنگ خطر، وظیفه سرویس احراز هویت در واقع حصول اطمینان از دریافت پیام از منبعی است که فرستنده مدعی ارسال آن است.

- در مورد موضوع عمل متقابل درحال پیشرفت، مانند اتصال یک پایانه به یک میزبان، دو جنبه درگیر خواهند بود. اول آنکه، در زمان شروع ارتباط، سرویس اطمینان حاصل می‌نماید که دو موجودیت تایید طلاحیت شده‌اند (یعنی هر موجودیت همانی است که ادعا نموده است). دوم آنکه، سرویس می‌بایست اطمینان حاصل نماید که به هیچ طریقی مداخله‌ای در ارتباط بوجود نیاید که شخص سومی بتواند بطور ناشناس بعنوان یکی از دو طرف اصلی برای مقاصدی چون ارسال و دریافت تایید نشده اقدام نماید.

سرویسهای امنیتی: کنترل دسترسی

کنترل دسترسی عبارت است از محدود کردن و کنترل میزان دسترسی به سیستمها و برنامه‌های کاربردی میزبان ازمیان لینکهای ارتباطی.

برای دستیابی به این نوع کنترل، هر موجودیت که سعی در گرفتن دسترسی دارد ابتدا می‌بایست شناسایی یا تعیین هویت شده و آنگاه دسترسی‌ها و اختیارهای شایسته و صحیح می‌تواند به شخص داده شود.

سرویسهای امنیتی: محرمانگی داده

محرمانگی عبارت است از حفاظت داده ارسال شده در برابر حملات منفعل. بر اساس محتویات ارسال داده می‌توان چندین لایه حفاظتی تعیین نمود.

برای نمونه، وقتی یک اتصال TCP بین دو سیستم برقرار می‌شود، این محافظت گسترده از آزادسازی هر داده انتقالی کاربر بر روی TCP محافظت می‌نماید.

جنبه دیگر محرمانگی در واقع محافظت جریان ترافیک از تجزیه و تحلیل است. برای آنکه مهاجم نتواند منبع و مقصد، پریود، طول، یا سایر مشخصات ترافیک یک ارتباط را زیر نظر داشته باشد، می‌توان از این سرویس استفاده نمود.

محرمانگی روی حملات منفعل کار میکند

سرویسهای امنیتی: یکپارچگی داده

- یک سرویس یکپارچگی با یک رشته پیام کار می‌کند و اطمینان حاصل می‌نماید که پیام ارسالی بدون تکرارشدن، اضافه شدن، تغییر یافتن، مرتب شدن مجدد، و یا بازپخش به مقصد رسیده باشد (اتصال - محور). تخریب داده نیز زیر نظر این سرویس انجام می‌گیرد.
- از طرف دیگر، در یک سرویس غیراتصال - محور با پیامهای مجزا و انفرادی بدون توجه به محتویات بزرگتر کار می‌نماید و بطور عمومی فقط محافظت در برابر تغییر پیام را مهیا می‌نماید.

سرویس یکپارچگی به حملات فعال مرتبط است و لذا تشخیص بیشتر از پیشگیری دارای اهمیت خواهد بود.

سرویسهای امنیتی: عدم انکار

از امکان تکذیب فرستنده و گیرنده یک پیام از ارسال یا دریافت آن جلوگیری می‌نماید.

- وقتی یک پیام ارسال می‌گردد، گیرنده می‌تواند ثابت نماید که فرستنده منتصب به پیام درحقیقت آن پیام را ارسال نموده است.
- بطور مشابه، وقتی یک پیام دریافت می‌شود، فرستنده می‌تواند اثبات نماید که گیرنده منتصب در حقیقت آن پیام را دریافت نموده است.

سرویسهای امنیتی: دسترس پذیری

یک سیستم دسترس پذیر خواهد بود اگر سرویسها بر پایه طراحی سیستم برای زمانی که کاربر آنها را تقاضا می‌نماید آماده و مهیا باشند

- تعدادی از این حملات توسط اقدامات متقابل خودکار مانند احراز هویت و رمزگذاری قابل پیشگیری بوده و تعدادی نیز نیازمند اقدامات فیزیکی برای جلوگیری و بازیابی از به هدر رفتن میزان دسترس‌پذیری منابع در یک سیستم توزیع‌شده هستند.
- یک سرویس دسترس‌پذیری در واقع یک سیستم را از دسترس‌پذیر بودن آن مطمئن می‌نماید. این سرویس نشان می‌دهد که نگرانیهای امنیتی با حمله محرومیت - از - خدمات افزایش خواهند یافت.

مکانیزمهای امنیتی

برای اجرا و پیاده سازی سرویسهای امنیست به مکانیزمهای امنیتی نیاز داریم که به دو صورت مکانیزمهای خاص و عمومی قابل دسته بندی هستند.

مکانیزمهای خاص مانند:

- **به رمز درآوردن:** استفاده از الگوریتمهای ریاضی برای انتقال داده به فرمی که به آسانی قابل فهم نباشد. انتقال و بازیابی توالی داده وابسته به الگوریتم و تعداد کلیدهای رمزگذاری که ممکن است صفر یا بیشتر باشند، خواهد بود.
- **امضاء الکترونیکی:** داده اضافه شده، یا یک انتقال رمزشده، به یک واحد داده که به یک گیرنده واحد داده اجازه می‌دهد تا فرستنده و یکپارچگی داده را تایید نموده و از در برابر جعل از آنها محافظت نماید.
- **کنترل دسترسی** : یک تعداد مکانیزمی که میزان دسترسی به منابع را اجرا می‌نماید.
- **کنترل مسیریابی:** فعال نمودن انتخاب مسیرهای امن فیزیکی خاص برای داده خاص و اجازه تغییر مسیر، بخصوص هنگامی که مشکوک به یک نفوذ امنیتی باشد.

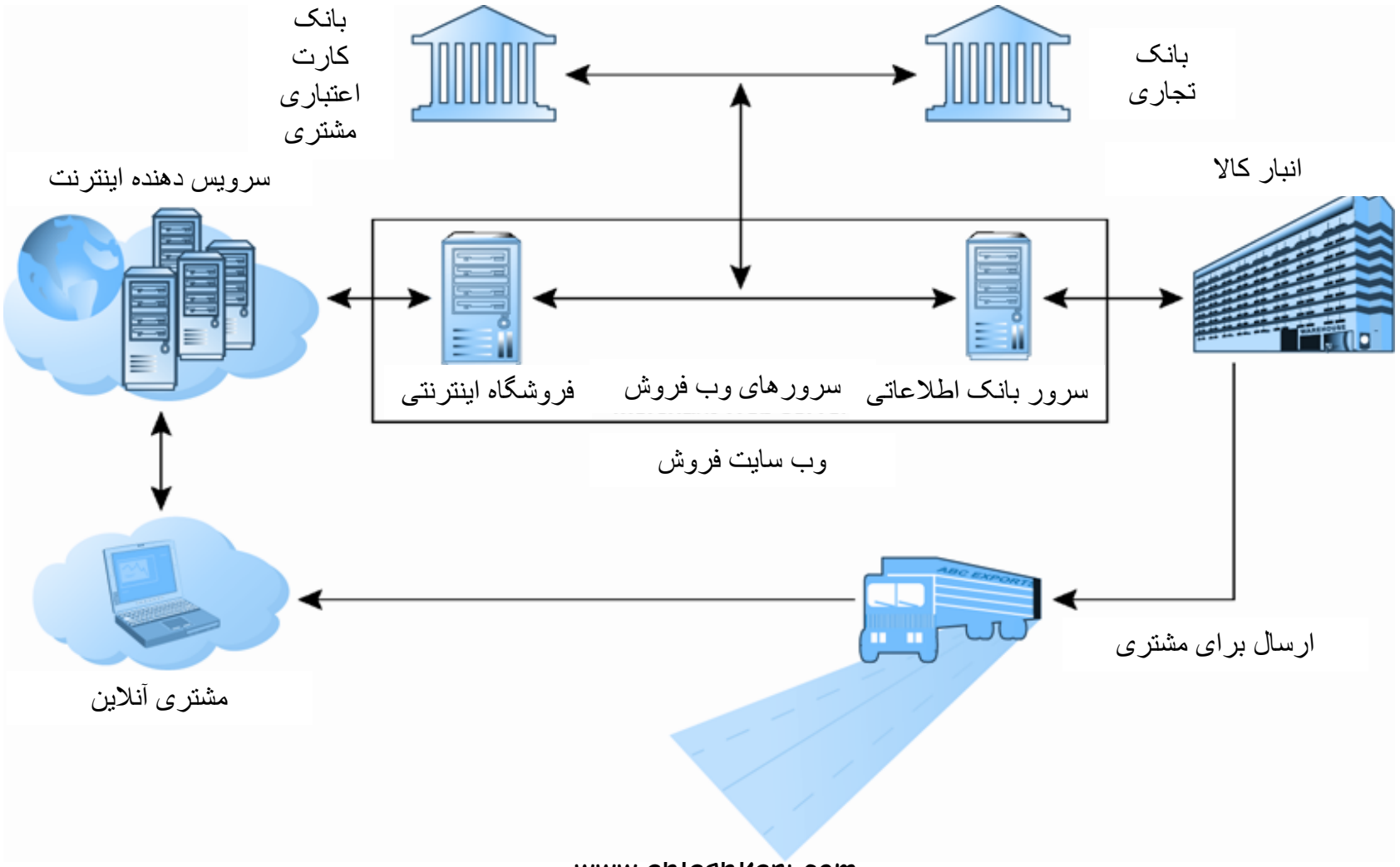
مقدمه ای بر امنیت تجارت الکترونیکی

تهدیدهای امنیتی در تجارت الکترونیک

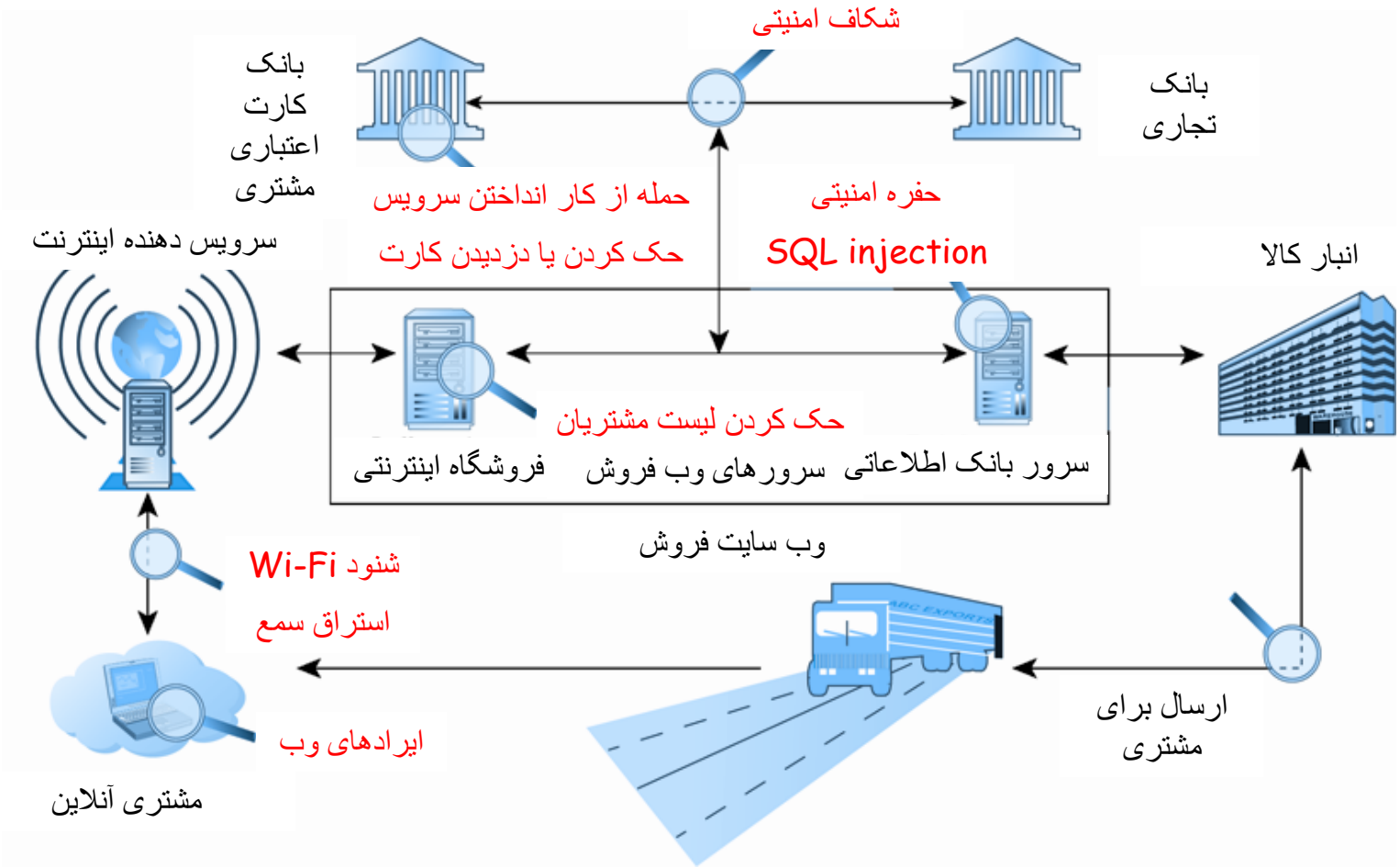
سه نقطه ضعف اصلی محیطهای تجارت الکترونیک

1. سرویس گیرنده
2. سرویس دهنده
3. خطوط ارتباطی (شبکه و اینترنت)

یک انتقال نمونه در تجارت الکترونیک



نقاط ضعف در یک انتقال الکترونیکی



چالشها و تهدیدهای امنیتی در تجارت الکترونیک

- بدافزارها
  - ویروسها
  - کرمها
  - تروجانها
  - دربهای پشتی
  - روت کیتها
  - بات ها، بات های شبکه
- برنامه های ناخواسته
  - آگهی افزارها
  - جاسوس افزارها
- هکرها

چالشها و تهدیدهای امنیتی در تجارت الکترونیک (ادامه)

- حملات
  - مهندسی اجتماعی
  - فیشینگ
  - از کار انداختن سرویس (DOS)
  - تلاش برای بدست آوردن اطلاعات محرمانه
    - اسپم یا هرزنامه
    - جعل وبسایتهای مشروع (Pharming)
    - استفاده از اطلاعات برای تقلب
    - شکاف داده: زمانی که یک سازمان کنترل خود را برای جلوگیری از دسترسی دیگران به داده های خود از دست میدهد.
- دزدیدن یا تقلب کردن در کارتهای اعتباری
  - هکرها سرورهای تجاری را هدف قرار داده و از داده های آنها برای تولید کارت اعتباری با هویت کاذب استفاده می نمایند

چالشها و تهدیدهای امنیتی در تجارت الکترونیک (ادامه)

- استراق سمع
- طراحی ضعیف نرم افزارهای سرویس دهنده و سرویس گیرنده
- امنیت شبکه های اجتماعی
- حملات مرتبط با پلتفرمهای موبایل

برخی از راه حلهای موجود

- محافظت از ارتباطات اینترنتی
  - رمزنگاری
- امنیت کانالهای ارتباطی
  - SSl و VPN
- محافظت از شبکه ها
  - دیوارهای آتش، سیستمهای تشخیص مهاجم
- محافظت از سرویس دهنده ها و کاربران
  - کنترل دسترسی
  - تایید صلاحیت
- طراحی و پیاده سازی پروتکلهای خاص
  - پروتکل IOTP

خلاصه:

اهداف امنیتی، حملات، خطرها، آسیب پذیری ها، ریسکهای امنیتی، سرویسهای امنیتی، مکانیزمهای امنیتی، تهدیدهای تجارت الکترونیک، نقاط ضعف یک انتقال الکترونیکی، حملات رایج در تجارت الکترونیک، روشهای پیشگیری

جلسه بعدی:

مکانیزمهای امنیتی و رمزنگاری

هیچ راهی برای به دست آوردن تجربه به جز از
طریق تجربه وجود ندارد.