# تجارت الکترونیک

**مدرس، محسن هوشمند**

mohsenhoshmand@gmail.com

- امنیت و سامانه‌های پرداخت

# جنگ سایبری: اح‌د ۲,۰

- تکامل جنگ‌افزارها در طول زمان
  - از چوب و سنگ به تیر و نیزه به توپخانه و بمب و به سلاح‌های هسته‌ای
  - تشخیص‌پذیری سریع جنگ‌افزارهای فیزیکی
- امروزه نوع دیگری از جنگ‌افزار
  - همه‌گیری و معمول‌شدن سریع
  - ارتش مخفی هک‌کنندگان
    - مجهز به سلاح الگوریتم‌ها و کدهای رایانه‌ای
- فضای سایبری به مثابهٔ میدان نبرد
  - کشورها علیه دیگر کشورها
  - کشورها علیه شرکت‌ها

# جنگ سایبری: اح‌د ۲,۰

- دو نوع هدف جنگ‌سایبری
  - اهداف زیرساختی سخت
    - ساز و برگ‌های دفاعی
    - تجهیزات هسته‌ای
    - شبکه‌های مخابراتی و برق
    - نیروگاه‌ها و کارخانه‌های تولید
    - دیگر زیرساخت‌های عمومی
  - اهداف نرم
    - بانک‌ها و نظام‌های مالی
    - شرکت‌های خصوصی
    - نظام‌های اطلاعات عمومی
    - نظام نگهداری اطلاعات بیمه و مدیریت سلامت

# جنگ سایبری: اح‌د ۲,۰

- هدف جنگ سایبری علیه اهداف سخت
  - زمین‌گیری زیرساخت‌های فیزیکی و اصلی صنعتی خاص یا کل جامعه
- هدف جنگ سایبری علیه اهداف نرم
  - برهم‌زدن و ضعیف‌سازی جمعیت‌ها و سازمان‌ها و نهادها
  - تنبیه شرکت‌ها
  - گرداوری اطلاعات افراد و شرکت‌ها جهت مقاصد بعدی
- تفاوت جنگ سایبری از جاسوسی سایبری
  - نداشتن قصدی در جهت از کار انداختن خدمات اجتماعی اصلی
  - تمرکز بر جمع‌آوری اطلاعات شامل مالکیت فکری
  - احسن جاسوسی‌ها – مخفی و  بی‌سروصدا و در سکوت

# جنگ سایبری: اح‌د ۲,۰

- انتخابات ریاست‌جمهوری اما مورخ ۱۸ آبان ۱۳۹۵
  - نسل جدیدی از جنگ سایبری علیه اهداف نرم
    - برهم‌زدن و تاثیرگذاری بر فرایند سیاسی کل ملت مذکور
  - مبتنی بر گزارش دی ۱۳۹۶
    - همکاری سایبری دولت روسیه و نیروهای ثالث برای طراحی داستان‌ها و تبلیغات غلط و افزایش تنش جهت پشتیبانی از دواطلب خاص «ترامپ»
      - روسیه‌دوست (روسوفیل)
      - تضعیف داوطلب مخالف

# جنگ سایبری: اح‌د ۲,۰

- اجرای طیفی وسیعی از فعالیت‌های سایبری جهت دست‌یابی به اهداف مذکور
  - هک‌کردن ایمیل کمیته ملی دمکرات
    - افشای اطلاعات در ویکی‌لیکس و دس‌لیکس
  - استفاده از صدها ترول اینترنتی جهت ایجاد حساب‌های جعلی در فیس‌بوک و تویتر
    - جهت تولید و انتشار داستان‌های دروغ
  - استفاده از بستر باز تبلیغاتی فیس‌بوک و تویتر جهت دستیابی به گروه‌های جمعیتی با قصد افزایش تنش اجتماعی

# جنگ سایبری: اح‌د ۲,۰

- فیس‌بوک و توییتر رد کردن ادعای استفاده از بسترها
- آذر ۱۳۹۶ در کنگره فیس‌بوک قبول ادعای وجود ۶۰۰ تبلیغات و ۴۷۰ حساب با منشا روسی که خود را امریکایی معرفی کرده بودند
  - پرداخت ۱۰۰۰۰۰ دلار جهت تبلیغاتی که میلیون‌ها عضو امریکایی را هدف گرفته بود
  - جهت پراکندن پیام‌های تفرقه‌افکنانه
- هم‌چنین تویتر مجبور به پذیرش هزاران حساب جعلی مرتبط با روسیه و صدها بات مرتبط استفاده شده جهت نشر اخبار جعلی در زمان رای‌گیری
- هر دو درگیر با مسئله حساب جعلی
  - تویتر ۸۴ میلیون حساب جعلی
  - فیس‌بوک ۱۲۰ میلیون حساب جعلی
  - بسیاری از آنها بات
    - ارسال پیام خودکار در هر چند ثانیه، چند برابر کردن تاثیر پیام‌های جعلی و در چند مورد در فهرست روندهای هر دو شرکت

# جنگ سایبری: اح‌د ۲,۰

- تلاش روسیه جهت تاثیر بر انتخابات امریکا و تلاش امریکا جهت تاثیر بر فرایند سیاسی روسیه
  - چیز جدیدی نیست
  - از پیش از جنگ سرد
    - استفاده از انواع روش‌های و ابزارها و سیاست‌ها
      - چون نهادهای امنیتی و دیپلمات‌ها و داستان‌های خبری و تبلیغات تلویزیونی و رادئویی و پرداخت به سیاست‌مداران و مشاوران
        - جهت مراتب تاثیر بر فرایند سیاسی و دستیابی به «منافع ملی» خود
  - پس چه جدید است؟

# جنگ سایبری: اح‌د ۲,۰

- تلاش روسیه جهت تاثیر بر انتخابات امریکا و تلاش امریکا جهت تاثیر بر فرایند سیاسی روسیه
  - چیز جدیدی نیست
  - از پیش از جنگ سرد
    - استفاده از انواع روش‌های و ابزارها و سیاست‌ها
      - چون نهادهای امنیتی و دیپلمات‌ها و داستان‌های خبری و تبلیغات تلویزیونی و رادئویی و پرداخت به سیاست‌مداران و مشاوران
        - جهت مراتب تاثیر بر فرایند سیاسی و دستیابی به «منافع ملی» خود
  - پس چه جدید است؟
    - استفاده از توانائی‌های هک‌کردن و شبکه‌های اجتماعی جهت تاثیر مستقیم بر عقیده‌ها و اعتقادات کل جمعیت

# جنگ سایبری: اح‌د ۲,۰

- جنگ سایبری علیه فرایندهای دمکراتیک تصمیم‌گیری تهدیدی بزرگ
  - امکان پیگیری و یافتن آن در سپهر سیاسی و محتملا توقف ان با نهادهای امنیتی و شبکه‌های اجتماعی
  - جانی گرفته نمی‌شود
- اما در جنگ سایبری سخت
  - در توان جهت آسیب‌های اجتماعی و فیزیکی به جمعیتی بزرگ
    - محتمل جهت ضررهای جانی

# جنگ سایبری: احد ۲,۰

- از مسائل جنگ‌افزارها
  - دشمن شما همان را دارد که که شما دارائید
  - نابودی حتمی طرفین
    - MAD (اضمحلال حتمی طرفین (اضمحلال حتمی دوطرف «احد»
      - سبقت در تک، شکست و نابودی در پاتک
  - به طریق اولی در جنگ سایبری

# جنگ سایبری: اح‌د ۲,۰

- امریکا و چین و روسیه اماده شدن جهت جنگ سایبری هدف نرم و سخت
  - با امید اتفاق نیفتادن آن با توسعهٔ سلاح‌های جدید و امتحان فنون دفاعی
  - فروردین ۱۳۹۶ ناتو
    - هشتمین بازی‌های سپر مقاوم جنگ سایبری
  - خرداد ۱۳۹۶ وزارت دفاع امریکا
    - ششمین بازی‌های محافظان جنگ سایبری
    - صد سازمان و هشتصد فرد از نیروهای نظامی و شرکت‌های خصوصی

# جنگ سایبری: اح‌د ۲,۰

- نادر بودن حملات علیه اهداف سخت چون زیرساخت‌های فیزیکی
  - نیاز به اطلاع دقیق از زیرساخت
  - معمولا نیاز به اطلاع داخلی از کنترل‌کننده‌های صنعتی
    - رایانه‌های کنترل دریچه‌ها و شیرآلات و دستگاه‌ها
  - شناخته‌شده‌ترین و مستندشده‌ترین حملهٔ زیرساختی

# جنگ سایبری: اح‌د ۲,۰

- نادر بودن حملات علیه اهداف سخت چون زیرساخت‌های فیزیکی
  - نیاز به اطلاع دقیق از زیرساخت
  - معمولا نیاز به اطلاع داخلی از کنترل‌کننده‌های صنعتی
    - رایانه‌های کنترل دریچه‌ها و شیرآلات و دستگاه‌ها
  - شناخته‌شده‌ترین و مستندشده‌ترین حملهٔ زیرساختی
    - استاکس‌نت
    - بدافزاری در سال ۱۳۸۹ محتملا حاصل همکاری امنیتی‌های اسرائیلی و امریکایی
      - جهت از کارانداختن سانتریفیوژهای هسته‌ای ایران
    - برنامه ویروسی بدافزار
      - کارگزاری شده در ماژول‌های کنترل‌کنندهٔ صنعتی سانتریفیوژهای سوخت هسته‌ای ایران
  - اولین حمله سایبری مقیاس‌بزرگ به زیرساخت
  - در پاسخ اتهام‌زنی امریکا به ایران بر تدارک و پشتیبانی ایران از حملهٔ به شرکت ارامکو سعودی با ویروس شمعون پاک کنندهٔ ۳۰۰۰۰ رایانه در شرکت

# جنگ سایبری: اح‌د ۲,۰

- به دنبال معاهداتی شبیه معاهدات تسلیحات هسته‌ای
- نمایشگر افزایش تهدیدپذیری حملات حجم بالا و متعاقبا ضررهای بزرگ
- انجام حملات گروه‌های سازمان‌یافته
  - کشورها علیه منابع اینترنتی دیگر کشورها
- سختی پیش‌بینی و پاسخ به حملات
  - هم برای دولت‌ها و هم برای فیاوری‌ها
- اما
  - مراحلی جهت محافظت تارمانه، ابزار همراه،اطلاعات شخصی از حملات معمول اینترنتی
    - از اهداف این بخش جدید
    - همچنین مجالی برای تامل دربارۀ  چگونگی حفظ تجارت الکترونیکی در قبال به خطر افتادن اینترنت

# محیط امنیتی تجارت الکترونیک

- برای مقید به قوانین
  - اینترنت مأمن فضای بزرگ و راحت و دسترسی به اجناس و افراد و خدمات و کسب‌وکارها در پهنهٔ گیتی
- برای مجرمان
  - منبع عظیم سواستفاده از بسیاری مصرف‌کنندهٔ اینترنت
    - محصولات و خدمات و پول نقد و اطلاعات
- کم خطری دزدی برخط
  - امکان دزدی از دور به جای دستبرد به بانک و و ناشناس ماندن
  - یا پیاده‌کردن راحت موسیقی
- عدم برنامه اینترنت جهت تجارت
  - دارای مشکلات اینترنتی مانند شبکه‌ها قدیمی‌تر
  - شبکهٔ باز تهدیدپذیر

# محیط امنیتی تجارت الکترونیک

- هزینه ضرر ناشی و همچنین هزینه‌های مشروط به
  - امنیت شبکه و
  - جبران پس از حملهٔ هک،
  - آسیب‌های ناشی از بدنامی ناشی از حمله اینترنتی و
  - کاهش اعتماد مراجعان و مشتریان
  - ازدست دادن اطلاعات مهم و حساس
- مطالعه ۲۰۱۷
  - میانگین هزینهٔ نقض داده در شرکت‌های ایالات متحده ۷٫۳۵میلیون دلار

# حوزهٔ مسئله

- ناواضح بودن اندازه کل و حجم ضررهای جرائم سایبری
  - مشکلات گزارش
- ارزانی لوازم حملهٔ وب
- کلاهبرداری کارت برخط
- بازار اقتصاد زیرزمین
  - فروش به جای استفاده

**TABLE 5.2 THE CYBER BLACK MARKET FOR STOLEN DATA**

| DATA | PRICE* |
|---|---|
| Individual U.S. card number with expiration date and CVV2 (the three-digit number printed on back of card) (referred to as a CVV) | $5–$8 |
| Individual U.S. card number with full information, including full name, billing address, expiration date, CVV2, date of birth, mother's maiden name, etc. (referred to as a Fullz or Fullzinfo) | $20–$60 |
| Dump data for U.S. card (the term "dump" refers to raw data such as name, account number, expiration data, and CVV encoded on the magnetic strip on the back of the card) | $60–$100 |
| Online payment service accounts | $20–$300 |
| Bank account login credentials | $80–$700 |
| Online account login credentials (Facebook, Twitter, eBay) | $10–$15 |
| Medical information/health credentials | $10–$20 |
| 1,000 e-mail addresses | $1–$10 |
| Scan of a passport | $1–$3 |

# امنیت مناسب تا

- چیستی این گزاره؟
  - هر بار مراجعه به فضای بازاری برابر با خطر از دست رفتن حریم خصوصی
    - اطلاعات آنچه که خریدید
  - ابتدائی‌ترین خطر خریدار
    - عدم دریافت آنچه برایش پرداخت کردید
  - ابتدائی‌ترین خطر فروشنده
    - عدم دریافت مبلغ آنچه فروختید
  - دزدان در دست گرفتن تراکنش و خروج بدون پرداخت یا پرداخت از کیسهٔ دیگری

# امنیت مناسب ت ا

- مواجهه با خطرات مشابه تجارت سنتی
  - دزد دزد است فارغ از بستر
  - کلاه‌برداری، شکستن و ورود
  - اختلاس
  - تعدی و تجاوز (ورود به ملک غیر)
  - خرابکاری
- اما مواجهه پیچیده‌تر و شامل فناوری‌های نو و سیاست‌های سازمانی و قوانین

# محیط امنیت تجارت الکترونیکی

# امنیت مناسب ت ا

- مواد موردنیاز دستیابی به بالاترین سطح امنیت
  - تکنولوژی‌های نو
  - رویه‌ها و سیاست‌های سازمانی
  - استانده‌های صنعتی و قوانین حکومتی
- امکان شکستن امنیت در صورت داشتن منابع کافی
  - پس مطلق نبودن امنیت
- عوامل دیگر
  - ارزش زمانی پول
  - هزینه امنیت در مقابل ضرر محتمل
  - شکستن امنیت معمولا در ضعیف‌ترین پیوندها

# ابعاد امنیت تجارت الکترونیک

- شش بعد کلیدی
  - یکپارچگی، عدم‌انکار، اعتبار، محرمانگی، حریم خصوصی، دسترسی
- یکپارچگی
  - اطمینان از اطلاع نمایشی در تارمانه، یا ارسالی یا دریافتی را شخص غیرمعتبر تغییری نداده باشد
  - تغییر مسیر مبلغ واریزی
- عدم انکار
  - اطمینان از عدم قادر بودن شرکت‌کنندگان به انکار عملی که انجام داده‌اند
  - افزودن نظرات با ایمیل رایگان یا با نام دیگری
  - یا حتی با نام خود و سپس انکار در مرحلهٔ بعد
- اعتبار
  - امکان تصدیق هویت شخص که با آن در ارتباط هستید
  - چگونه مشتری مطمین است که تارمانه همان است که مدعی است
  - چگونه فروشنده از ادعای خریدار مطمئن است
  - جعل- کسی خود را جای دیگری قلمداد کند

# ابعاد امنیت تجارت الکترونیک

- محرمانگی
  - اطمینان از اینکه پیام صرفا در اختیار افراد ذیصلاح باشد
- حریم خصوصی
  - امکان کنترل بر استفاده از اطلاع مشتری که خود شخص در اختیار فروشنده گذاشته است
  - مسئله‌های فروشندگان در رابطه با حریم خصوصی
    - ایجاد سیاسات داخلی جهت مدیریت استفادهٔ خود از اطلاعات مشتری
    - حفاظت از اطلاعات از دسترسی‌های غیرمجاز
    - دریافت اطلاعات کارت یا اطلاعات دیگر
      - هم از دست رفتن محرمانگی و هم از دست رفتن حریم خصوصی
- موجود
  - اطمینان از کار و عملیاتی تارمانه همان‌گونه که موردانتظار است

# ابعاد متفاوت امنیت تا از منظر مشتری و تجارت

| جنبه | از منظر مشتری | از منظر تجاری |
|---|---|---|
| یکپارچگی | ایا اطلاعی که ارسال یا دریافت کردم تغییر کرده است؟ | ایا دادهٔ موجود در مانه بدون داشتن مجوز تغییر یافته؟<br>ایا داده دریافتی از مشتری معتبر است؟ |
| عدم‌انکار | ایا بخشی که با من کار کرده امکان انکار تعامل را دارد؟ | ایا مشتری امکان انکار سفارش را دارد؟ |
| اعتبار | با چه کسی معامله می‌کنم؟<br>چگونه از اینکه طرف با که خود را معرفی می‌کند یکی است؟ | هویت واقعی مشتری چیست؟ |
| محرمانگی | ایا شخص دیگر امکان دیدن پیام‌های مرا دارد | آیا هر کسی بدون مجوز به پیام‌ها و داده محرمانه دسترسی دارد؟ |
| حریم خصوصی | امکان کنترل بر استفاده اطلاعات شخصی من منتقل شده به تاجر | چه استفاده‌هایی از داده‌های شخصی جمع شده می‌توان داشت؟<br>ایا اطلاعات گرداوری شده از مشتری‌ها بدون مجوز است؟ |
| دسترسی | امکان دسترسی به مانه را دارم؟ | ایا مانه عملیاتی است؟ |

# تنش بین امنیت و دیگر ارزش‌ها

- همانند مورد سنتی
- راحتی استفاده
  - افزودن امنیت بیشتر، سخت‌تر شدن استفاده از مانه و کندتر شدن آن
  - کسب امنیت بیشتر به قیمت کاهش سرعت پردازنده‌ها و افزودن میزان زیادی درخواست‌های حافظه بر ابزارهای ذخیره‌سازی
  - افزونه‌ای مختل فیاوری
  - امنیت بیش ازحد مخل جهت سوددهی
  - امنیت کمتر از حد محتملا بدر کردن از فضای فیاوری
- برعهدهٔ کاربر گذاشتن
  - از گزینه اتصال خودکار (کمترین امنیت) تا رمزهای یکبار مصرف (بیشترین امنیت)

# تنش بین امنیت و دیگر ارزش‌ها

- امنیت عمومی  و استفاده‌های مجرمانه از اینترنت
  - تنش بی‌پایان بین فعالیت ناشناس و نیازهای اجتماع جهت ایجاد امنیت عمومی
  - استفاده مجرمان از تکنولوژی جهت طرح جرم یا تهدیدات ملی
- شنود تلگراف در دوران جنگ داخلی امریکا ۱۶۰ سال پیش
  - جهت به دام انداختن خائنان و ترورگرها
- شنود تلفن در سال ۱۸۹۰
- عدم اجازۀ هیچ دولت ملتی به وجود فناوری که مجرمان بتوانند در آن جرم کنند یا تهدید کنند مگر با ترس نظارت و جستجو
  - کارتل‌های مواد مخدر
  - تعقیب قضایی تالارهای فروش کارت در امریکا
    - مانند shadowcrew و carderplanet

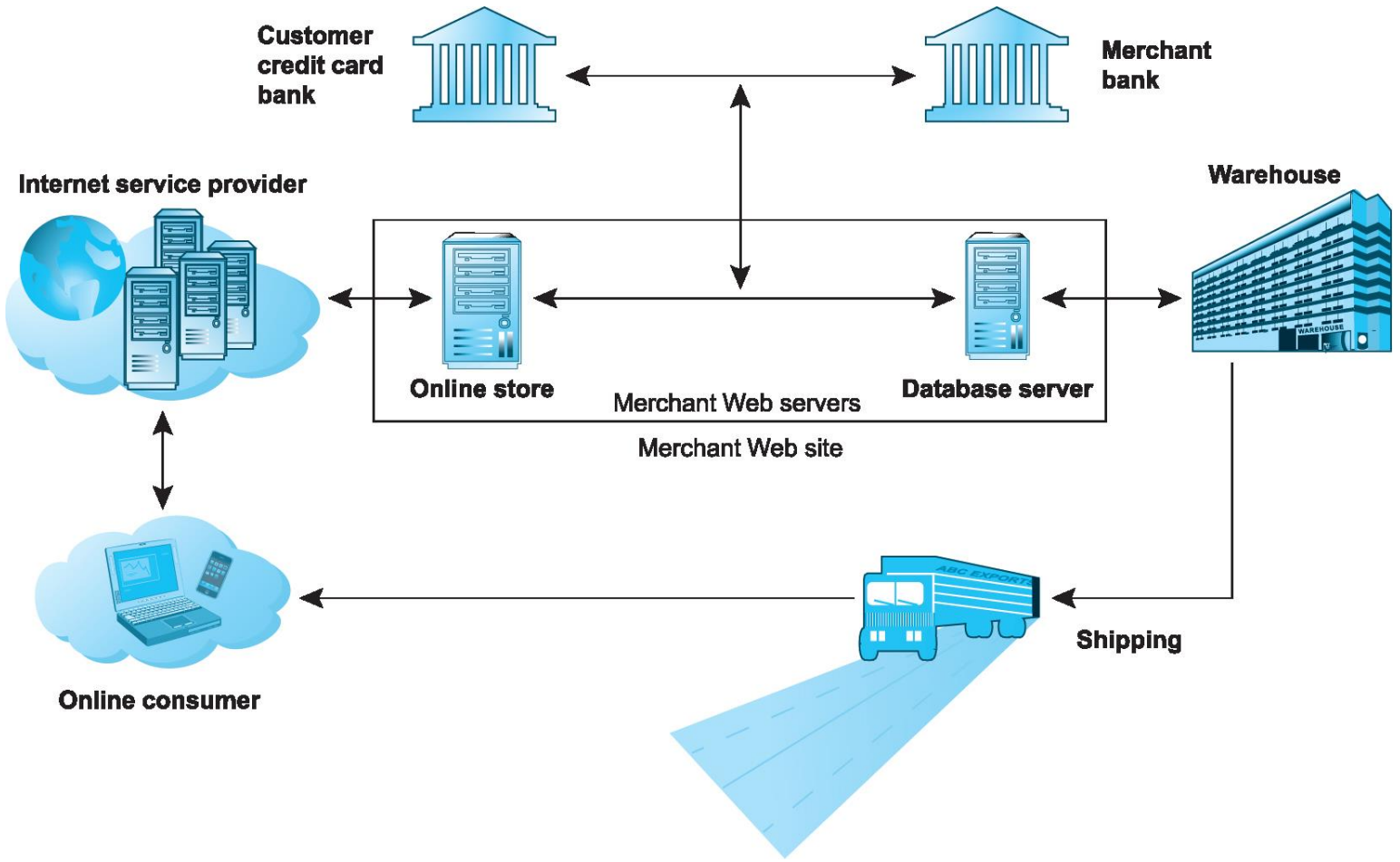
# تنش بین امنیت و دیگر ارزش‌ها

- اعمال تروریستی
  - برنامه‌ریزی- رمزی یوسف
  - استخدام و بکارگیری- عمر فاروق عبدالمطلب
  - اسنودن- گزارش دسترسی به سرورهای شرکت‌هائی  چون فیس‌بوک و گوگل و اپل و مایکروسافت
    - جستجوی اطلاعات شهروندان امریکا بدون مرجع قضائی

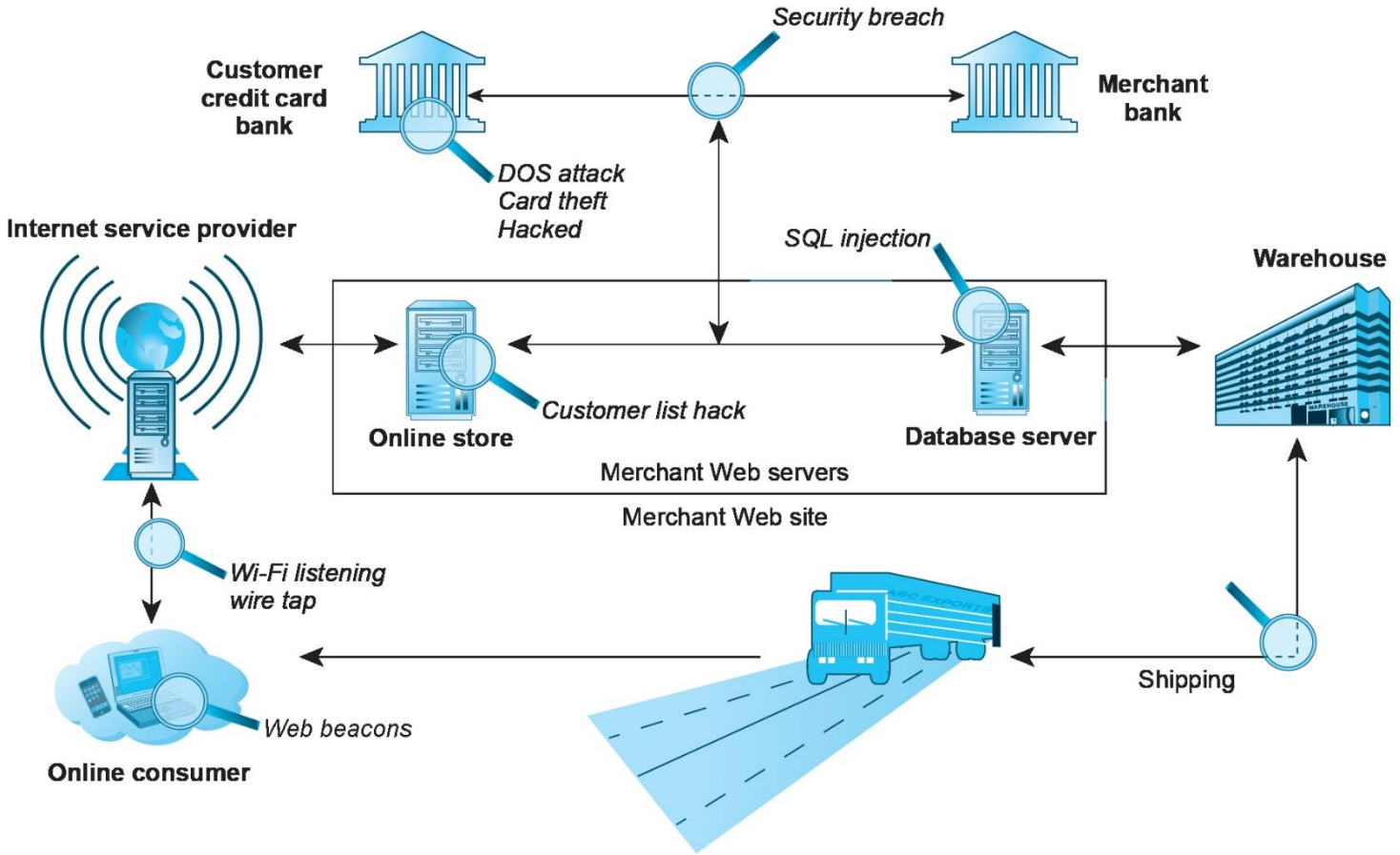
# تهدیدات امنیتی در محیط تجارت الکترونیک

- سه نقطه اصلی آسیب‌پذیری محیط تجارت الکترونیک از منظر فناوری
  - مشتری
  - سرور
  - خطوط ارتباطی
    - کانال‌های ارتباطی اینترنت

# نمونه معمول تراکنش تجارت الکترونیک



# نقاط آسیب‌پذیر در تراکنش تجارت الکترونیک



# مهمترین نمونه‌های معمول تهدیدات امنیتی

- کد مخرب
- برنامه‌های ناخواسته
- طله‌گذاری
- هک‌کردن و خرابکاری سایبری
- دزدی /کلاهبرداری کارت
- جعل

# کد مخرب

- یا بدافزار
- Malicious code یا malware
- گستره‌ای از تهدیدات شامل
  - ویروس‌ها
  - کرم‌ها
  - باج‌افزار
  - اسب‌های تروا
  - در رو ( در پشتی)
  - بات‌ها، بات‌نت‌ها (شب‌بات)
- بهره‌جویی و ابزارهای بهرجوئی exploit
  - استفاده از آسیب‌پذیری نرم‌افزارها
  - کیت‌های بهره‌جوئی
  - مجموعه بهره‌جوی انگلر angler
- ۲۰۱۶
  - تولید ۳۵۷میلیون بدافزار
    - میانگین نیم‌میلیون در روز!

# کد مخرب

- قبلا صرفا تک نفره و جهت تضعیف کامپیوتر
- امروزه گروه‌های کوچک هک یا شرکت‌های مورد حمایت دولتی
  - جهت دزدی ایمیل‌ها و اعتبارات مربوط به اتصال و داده شخصی و اطلاع مالی
  - تفاوت بین جرم خرده‌پا (آفتابه‌دزد) و جرم سازمان‌یافته
- تحویل بدافزار
  - معمولا با پیوستی به ایمیل یا پیوندی در ایمیل
  - یا در صفحات ورد و اکسل
  - اخیرا اتصال آن به زنجیره تبلیغات برخط
    - بدیغات! Malvrtising
  - یکی از مهم‌ترین تبلیغات آلوده به بدافزار
    - یاهو ۶,۹ میلیون کاربر بازدیدکنندهٔ روزانه
    - ۲۰۱۶ بنگاه‌های خبری چون نیویرک تایمز و aol و بی‌بی‌سی تبلیغات منتشر در چند شبکه تبلیغی و رسیدن به بنگاههای مذکور
      - به دست گرفتن رایانه  با کلیک شدن، رمز کردن داده کاربر
  - امکان جلوگیری با بلوکه کردن تبلیغات ظاهر شدنی
  - استفاده از فلش ادوب
    - جلوگیری مرورگرهای اصلی از اجرای خودکار ان

# کد مخرب

- پیاده‌کردن از داخل ماشین
  - Drive-by download
  - بدافزار همراه با فایل درخواستی جهت پیاده
  - درخواست آگاهانه یا ناآگاهانه
  - از روش‌های شایع آلوده کردن رایانه
  - تعبیه در پی‌دی‌اف
  - امروزه بیشتر حرفه‌ای و سازمانی تا ناوارد و تازه‌کار
    - سخن‌کوتاه بحث پول

# ویروس

- برنامه رایانه‌ای
  - قادر به ایجاد و تولید از خود
  - پخش به دیگر فایل‌ها
- همچنین اجرای عمل مخربی payload
  - از نمایش پیامی یا تصویری تا تخریب فایل‌ها و فرمت‌کردن حافظه جانبی رایانه از کار انداختن یا بدکار کردن برنامه‌ها

# کرم

- معمولا ویروس‌ها همراه کرم
- به جای پخش از فایل به فایل
  - طراحی‌شده جهت پخش از رایانه به رایانه
- لازم نبودن فعال شدن به دست کاربر
- کرم اسلامر Slammer
  - از بدنامان محل!
  - هدف آن آسیب‌پذیری شناخته شده «پ‌د» در سرور سکیول مایکروسافت
    - آلوده کردن ۹۰ درصد رایانه‌های در سطح دنیا پس از ده دقیقه از انتشار اولیه!
      - از کار انداختن دستگاه‌های خودپرداز بانک امریکا
      - صندوق بقالی‌ها مانند زنجیره پابلیکس در اتلانتا
      - از کار انداختن اتصالات اینترنتی در کره جنوبی و افت بازار سهام
- کرم کانفیکر در سال ۲۰۰۸
  - پیچیده‌ترین پس از اسلامر تاکنون
    - آلوده کردن ۱۱ میلیون کامپیوتر
  - ۲۰۱۷ راه‌اندازی مجدد با باج افزار واناکرای

# باج‌افزار

- نوعی از بدافزارها ( و معمولا از نوع کرم)
  - قفل کردن رایانه یا فایل‌ها و جلوگیری از دسترسی شما بدان‌ها
  - معمولا نمایش پیامی که دادگستری یا نیروی پلیس فعالیت غیرمجازی بر روی رایانه شما پیدا کرده است
    - درخواست پرداخت جریمه جهت بازکردن رایانه و جلوگیری از پیگیرد قانونی
- از انواع
  - رمزقفلcryptolocker
    - رمز کردن فایل‌هابا رمزگذاری نامتقارن و درخواست بازگشایی آن مثلا با بیتن‌کوین
      - انجام نیافتن در زمان مقرر معمولا منجر به رمز شدن آن برای همیشه
  - رمزدفاع Cryptodefense
  - رمزدیوار
- افزایش ۴۰۰درصدی حملات باج‌افزارها
  - مرتبط با رشد ارز مجازی بیت‌کوین
- مهم‌ترین واناکرای wannaCry
  - آلوده کردن ۲۳۰هزار رایانه در پهنه دنیا
  - هدف رایانه‌های استفاده کننده از سیستم‌عامل ویندوز
  - رمزکردن داده و درخواست پرداخت بیت‌کوین

# اسب تروا

- جلوهٔ بی‌خطری و سپس انجام عملی غافلگیرکننده
- ویروس نیست
  - عدم توانایی تولید از خود
  - اما جاده‌صاف کن ورود ویروس‌ها یا دیگر کدهای مخرب مانند بات‌ها و روتکیت‌ها
- دارای برنامهٔ پنهان جهت سرقت گذرواژه‌ها و ارسال آن
- دراپرها و پیاده‌سازها و دیگر انواع
  - ۱۳۹۰ سونی تجربه بزرگترین نقض داده در زمان خود
    - دستیابی به اطلاعات ۷۷ میلیون کاربرثبت‌شده شامل کارت بانک
  - معمولا استفاده در بدافزارهای مالی  پخش شده با شب‌بات‌ها
    - زئوس
      - سرقت اطلاعات با بررسی کلیک‌های روی صفحه کلید
      - ۱۰ میلیون رایانه از سال ۲۰۰۷
    - تینبا
      - اولین بار دیده شده در ۱۳۹۱ با فروش اطلاعات اعتباری از طریق حمله هنگامی که کاربر در حال دستیابی به تارمانه بانکی خود است
    - رمنیت
      - جهت سرقت رمزهای بانکی، کلوچک‌های جلسات، داده شخصی

# درپشتی

- ویژگی ویروس‌ها و کرم‌ها و اسب‌های تروا
  - موجب‌ساز دسترسی دور به رایانه آلوده شده
- داون‌اپ
  - کرم با درپشتی
- ویروت
  - ویروس که که فایل تایپ‌ها را تغییر می‌دهد
  - همچنین دارای درپشتی جهت پیاده و نصب تهدیدات بیشتر

# بات‌ها

- نصب مخفیانه بر رایانه متصل به اینترنت
- پس از نصب پاسخ به شخص ثالث خارجی
  - شبان‌بات
- شب‌بات
  - مجموعه رایانه‌های مسّخر
    - جهت انجام فعالیت‌های مخبر مثل ارسال اسپم، حمله دداس، دزدی اطلاعات از دیگر رایانه‌ها و ذخیره ترافیک شبکه برای مقاصد بعدی
- مشخص نبودن تعداد دقیق اما محتملا هزاران که کنترل‌گر میلیون‌ها کامپیوتر
- تهدیدی بزرگ برای اینترنت و تا
  - به دلیل امکان انجام حملات بسیار بزرگ با استفاده روش‌های متنوع و گسترده

# بات‌ها

- روستوک
  - بزرگترین منبع اسپم‌سازی با تحت انقیاد گرفتن پانصدهزار رایانه
  - کنترل سرورهای واقع در شش محل خدمات رسانی در امریکا
    - اطلاعی از اینکه روستوک چه می‌کند نداشتند
  - ۱۳۹۰ اتحاد شبه پلیس فتای امریکا و واحد جرائم دیجیتال مایکروسافت جهت از کار انداختن آن
- ۱۳۹۲
  - مایکروسافت و پلیس فدرال به دنبال از کار انداختن ۱۴۰۰ شبات زئوس محور
  - خالی کردن حساب‌های بانکی نزدیک ۵۰۰ میلیون دلار

**TABLE 5.4 NOTABLE EXAMPLES OF MALICIOUS CODE**

| NAME | TYPE | DESCRIPTION |
|---|---|---|
| WannaCry | Ransomware/ worm | First appeared in May 2017. Exploits vulnerabilities in older versions of Windows operating systems, encrypts data, and demands a ransom payment to decrypt them. |
| Cryptolocker | Ransomware/ Trojan | Hijacks users' photos, videos, and text documents, encrypts them with virtually unbreakable asymmetric encryption, and demands ransom payment for them. |
| Citadel | Trojan/botnet | Variant of Zeus Trojan, focuses on the theft of authentication credentials and financial fraud. Botnets spreading Citadel were targets of Microsoft/FBI action in 2012. |
| Zeus | Trojan/botnet | Sometimes referred to as king of financial malware. May install via drive-by download and evades detection by taking control of web browser and stealing data that is exchanged with bank servers. |
| Reveton | Ransomware worm/Trojan | Based on Citadel/Zeus Trojans. Locks computer and displays warning from local police alleging illegal activity on computer; demands payment of fine to unlock. |
| Ramnit | Trojan/botnet | One of the most prevalent malicious code families still active. In operation since 2010, but largely disappeared in 2015 after the botnet that spread it was taken down. Reemerged in 2016 to become one of the most common financial trojans. |
| Conficker | Worm | First appeared 2008. Targets Microsoft operating systems. Uses advanced malware techniques. Largest worm infection since Slammer in 2003. Used in 2017 in conjunction with various ransomware attacks. |
| Netsky.P | Worm/Trojan | First appeared in early 2003. It spread by gathering target e-mail addresses from the computers, then infected and sent e-mail to all recipients from the infected computer. It was commonly used by bot networks to launch spam and DoS attacks. |
| Storm (Peacomm, NuWar) | Worm/Trojan | First appeared in 2007. It spread in a manner similar to the Netsky.P worm. Could also download and run other Trojan programs and worms. |
| Nymex | Worm | First discovered in 2006. Spread by mass mailing; activated on the 3rd of every month, and attempted to destroy files of certain types. |
| Zotob | Worm | First appeared in 2005. Well-known worm that infected a number of U.S. media companies. |
| Mydoom | Worm | First appeared in 2004. One of the fastest spreading mass-mailer worms. |
| Slammer | Worm | Launched in 2003. Caused widespread problems. |
| Melissa | Macro virus/ worm | First spotted in 1999. At the time, the fastest spreading infectious program ever discovered. It attacked Microsoft Word's Normal.dot global template, ensuring infection of all newly created documents. It also mailed an infected Word file to the first 50 entries in each user's Microsoft Outlook Address Book. |

# بات‌ها

- روستوک
  - بزرگترین منبع اسپم‌سازی با تحت انقیاد گرف
  - کنترل سررورهای دواقع در شش محل خدما
    - اطلاعی از اینکه روستوک چه می‌کند نداشت
  - ۱۳۹۰ اتحاد شبه پلیس فتای امریکا و واحد
- ۱۳۹۲
  - مایکروسافت و پلیس فدرال به دنبال از کار ان
  - خالی کردن حساب‌های بانکی نزدیک ۵۰۰ م

# کد مخرب

- تهدیدی برای کاربر و سرور
  - در سطح سرور
    - اما سرورهای معمولا دارای ضدویروس
    - امکان از کار انداختن تارمانه
    - نادر
  - در سطح مشتری
    - شایع‌تر
    - امکان انتشار به میلیون‌ها رایانه دیگر

# برنامه‌های محتملا ناخواسته

- POTENTIALLY UNWANTED PROGRAMS (PUPS)
- نصب برنامه‌های ناخواسته و محتملا بدون رضایت مشتری
  - انگل‌های مرورگر
    - نظارت و تغییر مرورگر کاربر
  - آگهی‌افزار
    - استفاده از تبلیغات ظاهر شدنی
  - جاسوس‌افزار
    - رهگیری نوشتن کاربر، ایمیل‌ها، پیام‌ها
- معمولا در شبکه‌های اجتماعی و مانه‌های محتوای تولیدی کاربران
  - سختی حذف پس از نصب
    - Pcprotect
      - جلوه چون ضدبدافزار قانونی در حالی که خود بدافزار

# برنامه‌های محتملا ناخواسته

- آگهی‌افزار
  - استفاده جهت نمایش  تبلیغات ظاهر شدنی حین بازدید مانه
  - ابزاری مورداستفادهٔ مجرمان سایبری
  - گزارش سیسکو
    - ۷۵ درصد سازمان‌های جستجو شده در سال ۲۰۱۶ آلوده به آگهی‌افزار مخرب
- انگل‌های مرورگر
  - یا رباینده تنظمیات مرورگر
    - نظارت و تغییر مرورگر کاربر یا ارسال اطلاع مراجعه و بازدید مانه‌ها به رایانه دور
    - معمولا جزوی از آگهی افزار
    - ۱۳۹۴
      - لنوو ارسال لبتاب‌های ویندوزی با آگهی‌افزار نصب‌شدهٔ سوپرفیش
      - موجب خطر  ربایش هنگام وصل شدن به شبکه بی‌سیم و جمع‌آوری هر چیزی که در مرورگر تایپ می‌شود
      - غیرقانونی اعلام کردن آگهی افزارها از سوی مایکروسافت
- جاسوس‌افزار
  - رهگیری نوشتن کاربر، ایمیل‌ها، پیام‌ها

# طله‌گزاری

- مهندسی اجتماعی social engineering
  - تکیه بر کنجکاوی و طمع و زودباوری بشر به منظور فریب آنها به انجام عملی که منجر به پیاده‌کردن بدافزار
  - کوین میتنیک
    - بدست آوردن اطلاعات بدون فناوری‌های پیچیده
- طله‌گذاری PHISHING
  - هرگونه تلاش برخط، فریبندهٔ شخصی ثالث
  - جهت دست یافتن به اطلاعات محرمانه یا سود مالی
  - معمولا بدون کد مخرب بلکه مبنی بر فنون و روش‌های مهندسی اجتماعی
    - نامهٔ نیجریه‌ای

# طله‌گزاری

- طله‌گذاری کلاهبرداری ایمیلی فیاوری
  - نوعی از نامه نیجریه‌ای
  - معرفی خود به عنوان کارمند رتبه بالاتر در شرکت و در خواست از کارمند سطح پایین جهت انتقال مبلغ به حساب کلاهبرداری
  - طبق گزارش پلیس فدرال سرقت سه میلیون دلار در طول سه سال تا ۱۳۹۶
- طله‌گزاری نیزه
  - وانمود کردن به جای پی‌پل و ای‌بی و امثالهم و جهت اعتبار حساب
  - کنترل بر پیوند هدایت به مانه‌ای تحت کنترل کلاهبردار و مجبور به افشای اطلاعات شخصی و محرمانه
- تکیهٔ طله‌گذار بر فنون شیادی
  - اما استفاده از ایمیل
  - معمولا ایجاد تارمانه‌ای که شبیه نهاد مالی معتبر و کلک زدن جهت وارد کردن اطلاعات مالی
    - یا بارگذاری بدافزاری بر رایانه قربانی
    - استفاده جهت کلاهبرداری هویتی و دزدی
    - دزدی هویت

# طله‌گزاری

- تغییر رمز گوگل
  - دستیابی به حساب معاون هیلاری کلینتون و دیگر اعضای کمیته ملی دمکرات
- طبق گزارش ورایزن
  - باز شدن ۳۰ درصد ایمیل‌ها
  - کلیک شدن پیوست دوازده درصد آنها
- مبارزه با طله
  - DMARC
    - موفقیت آن در سال‌های گذشته

# هک‌کردن، خرابکاری سایبر و هک‌گرائی

- هک کردن
- هک‌گر
  - فردی به قصد دستیابی به دسترسی غیرمجاز به رایانه
    - در مقابل کرک‌گر – هک‌گر با قصد جرم
  - دسترسی با یافتن ضعف در رویه‌های امنیتی تارمانه و رایانه
  - قبلا متخصصین عاشق چالش ورود به تارمانه‌های دولتی و شرکتی
  - امروزه به دنبال
    - خرابکاری سایبری
      - برهم زدن، آسیب رساندن، تخریب وب سایت
    - نقض داده
      - سرقت اطلاعات شرکتی و شخصی جهت منافع مالی

# هک‌کردن، خرابکاری سایبر و هک‌گرائی

- هک‌گرائی
  - مناصب سیاسی
  - معمولا حمله به دولت‌ها و سازمان‌ها و حتی افراد جهت اهداف سیاسی
  - ویکی‌لیکس و LilzSec و Anonymous
  - گروه‌های ببری
    - تحت استخدام سازمان امنیت شرکت جهت اندازه‌گیری وضعیت امنیتی
    - یافتن مصالح محافظتی
      - کلاه‌سفیدها
        - در خدمت سازمان و یافتن و رفع اشکلات امنیتی
        - انجام کار با انعقاد قرارداد
        - سیب و مایکروسافت
      - کلاه سیاه‌ها
        - همانند سفیدها ولی بدون پرداخت و با هدف ضرر زدن
        - افشای اطلاعات بدست‌آمده
        - اعتقاد به آزاد بودن اطلاعات و افشای اطلاعات محرمانه
- در میانه- کلاه خاکستری‌ها
  - به دنبال خیر بزرگ‌تر با یافتن و آشکار کردن اشکالات امنیتی
  - انتشار اشکالات بدون برهم زدن یا ضرررسانی
  - نام و پرستیژ
  - مظنون

# نقض داده

- نقض داده data breach
  - هنگام از دست دادن کنترل سازمان‌ها بر اطلاعاتشان به خوارج
  - ۱۳۹۵ نقض داده و برملایی اطلاعات حدود ۱,۱ میلیارد نفر در ۱۵ نقض بزرگ
  - ۱۰۹۳ نقض داده در سال ۱۳۹۵
  - بیشترین انها در بخش فیاوری ۴۵ درصد، سپس بخش سلامت ۳۵ درصد
- عوامل اساسی
  - هک‌کردن ۵۵ درصد
  - ایمیل تصادفی/ اینترنت ۹ درصد
  - خطای انسانی/ قصور ۸,۷ درصد
  - دزدی داخلی
- در امریکا بیشترین نقض داده شماره امنیت اجتماعی
- یاهو (سه میلیارد نفر) و اکویفکس (۱۴۳ میلیون نفر) دو مورد از بدنام‌ها

# مورد اکویفکس

- اکویفکس
  - شرکت معتبر در گزارش اعتبار و امتیاز
- اعلام در اواخر تابستان ۱۳۹۶
  - هک شدن  و دسترسی و پیاده‌شدن اطلاعات ۱۴۳ میلیون شهروند امریکائی
  - شامل اطلاعات شخصی
  - اطلاع در اواسط بهار ولی تاخیر تا زمان مذکور
  - انجام ماه‌ها قبل از کشف آن
- نامشخص بودن و عدم انتشار اطلاع از نحوهٔ حمله
  - سود بردن از ایراد در اپاچی استرات Apache Struts
    - نرم‌افزار متن‌باز جهت ایجاد تعامل در تارمانه‌ها
    - اطلاع دادن بخش امنیت سیسکو به اکویفکس دو روز قبل از انجام نقض داده دربارهٔ ایراد مذکور
    - ادعا بر تولید ولی گزارش‌ها مبنی بر پیاده‌سازی ناکامل

# مورد اکویفکس

- اعتبار
  - شریان اقتصادهای در حال‌توسعه و توسعه‌یافته
  - استعفای مدیر عامل
- بزرگتر از اکویفکس
  - یاهو سه میلیارد
  - ای‌بی ۱۴۵ میلیون
    - اما پیچیده‌ترین به دلیل نوع اطلاعات سرقتی
    - ۸۲ درصد تمامی افراد دارای اعتبار
- قبل از استعفا قول مبنی بر برگرداندن امنیت به اطلاعات
  - اما نیاز به صدور جدید کارت‌ها ،تعویض شماره‌های ملی، گواهی‌نامه‌ها
  - امنیت بیشتر پد بزرگ در تناقض با کسب و کار

# دزدی/کلاهبرداری کارت

- وقوع دزدی کارت نگران‌کننده‌ترین مورد در اینترنت
  - موجب عدم خرید اینترنتی
  - اما در عمل بی‌مبنا
    - ۰,۹ درصد وبی
    - ۰,۸ درصد تراکنش موبایلی
- سعی بر مبارزهٔ فیاوران با پدیده مذکور
  - روش خودکار تشخیص کلاهبرداری
  - مطالعهٔ انسانیِ سفارشات
  - رد کردن درخواست‌های مظنون
  - نیاز به سطوح بیشتر امنیت مانند نشانی ایمیل و موارد مشابه

# دزدی/کلاهبرداری کارت

- تصویب قوانین مصوب و مقصر دزدی
  - کمتر از مقداری، مسئول خود شخص
  - از مقداری بیشتر، مسئول نهاد اعتباری
  - در عوض بانک‌ها گرفتن عوارض بیشتر
  - تجار با گرانتر فروختن محصولات
- تغییر تکنولوژی از مغناطیسی به چیپ‌های کامپیوتری جهت مشکل‌تر شدن نقض داده

# دزدی/کلاهبرداری کارت

- دلیل اصلی هک‌کردن و تاراج سرورهای شرکت
  - دستیابی به اطلاعات ذخیره شده میلیون‌ها کارت
  - البرت گونزالز ۱۳۸۹
    - سازمان‌دهی بزرگترین دزدی تعداد کارت اعتباری در امریکا
    - همراه چند همکار روسی
    - ورود به سیستم رایانه مرکزی بارنز و نوبل، بی‌جی و چند شرکت دیگر
    - دزدیدن ۱۶۰میلیون کارت اعتباری
    - موجب ضرر ۲۰۰ میلیون دلاری
    - محکوم به ۲۰ سال زندان

# دزدی/کلاهبرداری کارت

- سفارشات بین‌المللی دارای خطر بالاتر کلاهبرداری

- مشکلات امنیت مرکزی
  - پیچیدگی تعیین هویت کاربر
  - عدم وجود فناوری با درجهٔ مطلق جهت تعیین هویت شخص
    - تا یافتن چنین فناوری فروش اینترنتی متضررتر از فروش سنتی
      - امضای الکترویکی
      - اجازه چند عاملی

  - تشخیص اثر انگشت
    - امکان هک شدن پد اثر انگشت

# سرقت/کلاهبرداری هویت

- سرقت هویت IDENTITY FRAUD
- دسترسی و استفاده غیرمجاز به اطلاعات شخصی غیر جهت سود مالی غیرقانونی
  - شماره کد امنیت
  - گواهینامه
  - شماره کارت
  - کاربری و گذرواژه
- وام! خرید، دریافت خدمات دیگر
- تمامی روش‌های اشاره شده خاصه نقض داده
- در سال ۲۰۱۶ حدود پانزده میلیون امریکایی تجربهٔ سرقت هویت
  - ضرر ناشی حدود ۱۶ میلیارد دلار

# تارمانه‌های جعل، سدمه، اسپم

- جعل Spoofing
  - تلاش برای مخفی سازی هویت واقعی با استفاده از ایمیل غیر یا نشانی آی‌پی دیگر
  - تغییر بسته‌های تی‌سی‌پی‌آی‌پی
  - مسیریاب‌ها مجهز به موانعی برای این گونه موارد
  - مرتبط با سدمه pharming
    - تغییر مسیر خودکار پیوند وبی به نشانی دیگر، به مذاق هک‌کننده
    - مستقیما خطری ندارند ولی تهدیدی برای یکپارچگی مانه
    - انحراف به جایی جعلی منجر به جمع‌آوری اطلاعات و دزدی فیاوری
    - یا در صورت قصد برهم‌زدن تغییر سفارش‌ها
    - عدم رضایت مشتری یا عدم موجودی
  - تهدید اعتبار
    - چی راست است و چه دروغ

# تارمانه‌های جعل، سدمه، اسپم

- تارمانه‌های اسپم (هرز) و آت و آشغال spam(junk) websites
  - پیشنهاد مجموعه‌ای از تبلیغات برای دیگر مانه‌ها
  - احتمال داشتن کد مخرب
    - امریکا اب و هوا
    - ایران آهنگ

# حمله‌های نشسته در میان و شنود (بویشگری)

- شنود(بوینده) sniffing
  - برنامهٔ استراق سمع
  - امکان یافتن مشکلات شبکه
    - استفاده قانونی موجب تشخیص گلوگاه‌ها
  - امکان استفاده جهت جرائم و اطلاعات تملیکی
    - بسیار ضررافرین و سخت جهت تشخیص
  - ۱۳۹۲ محکومیت پنج هک‌گر در پی سرقت اطلاعات فروشگاه‌های زنجیره‌ای خرده‌فروشی ۷-یازده و شرکتی فرانسوی

# حمله‌های نشسته در میان و شنود

- فال‌گوشی! ایمیل email wiretap
  - نوعی از خطر شنود
  - نگهداری و ضبط اطلاعات ایمیل‌ها در سطح سرور ایمیلی
  - امکان نصب روی کامپیوتر و سرور
  - کارمندان یا دستگاه‌های دولتی
  - قانون پاترویت امریکا
    - اجازه به پلیس فدرال
- حملهٔ نشسته در میان man-in-the-middle (MitM) attack
  - نوعی استراق سمع اما فعالتر!
  - تبدیل از انفعالی به فعال
  - مهاجم در میان راه است و ارتباطات بین دو بخش را تغییر می‌دهد
    - در حالی که دو بخش خیال می‌کنند مستقیم با هم در ارتباطند
    - امکان تغییر محتوا

# حمله بندآوری خدمت

- حملهٔ بندآوری خدمت DoS
  - بمباران تارمانه با پینگ و درخواست صفحه
  - بندآوردن و امکان از کار افتادن سرور
  - شب‌بات‌ها
    - حملهٔ توزیع‌شده
    - تشکیل شده از هزاران رایانهٔ مشتری
  - امکان از کار افتادن تارمانه یا غیرممکنی دسترسی کاربر به آن
    - پرهزینه برای مانه‌های تجارت الکترونیکی
    - عدم امکان خرید مشتریان با از کار افتادن مانه
    - آسیب بیشتر به شهرت مانه با هر چه طولانی‌تر بودن از کار افتادن مانه
  - عدم آسیب به اطلاعات یا نواحی دسترسی محدود سرور
    - امکان نابودی فیاوری برخط شرکت
  - معمولا همراه با تهدید و باج‌خواهی

# حمله بندآوری خدمت و حملهٔ بندآوری خدمت توزیعی

- حملهٔ بندآوری خدمت توزیع شدهDDoS
  - استفاده از هزاران یا صدها رایانه جهت حمله به شبکه هدف
- تهدیدی برای عملیات سیستم به دلیل  خاموش کردن نامحدود آن
- بیشتر تارمانه‌ها تجربهٔ چنین حمله‌ای
  - اطلاع از آسیب و خطرات آن و به دنبال آن تعریف ابزارهای جدید جهت جلوگیری از حملات بعدی
  - بهار ۱۳۹۶گزارش آکامی
    - افزایش سی درصدی نسبت به زمستان ۱۳۹۵
    - افزایش استفاده از روش حمله به مسیریاب‌های غیرایمن و ابزارهای نصب و پخش جهت بزرگترکردن حمله

# حمله بندآوری خدمت و حملهٔ بندآوری خدمت توزیعی

- امکان استفاده از ابزارهای اینترنت اشیاء، ابزارهای موبایلی
  - پائیز ۱۳۹۵
    - شب‌بات میرای استفاده از حملات بندآوری توزیعی خدمت برای حمله به داین و امازون و ایربنب، نتفیلکس، توئیتر، نیویورک‌تایمز
    - هک‌کنندگان قادر به حدس رمزهای ابزارهای معمول (مانند تنظیمات کارخانه مانند ادمین یا ۱۲۳۴۵)
    - سپس ترتیب حمله به سرور داین
    - حمله بندآوری معمولا به شبکه مجزا اما در مورد داین حمله به پایگاه اتصال اینترنت در امریکا
  - گسترش حجم اطلاعات با روش‌های بزرگ‌سازی/انعکاس
  - سیاه‌کن!
    - استفاده از بخت جهت انحراف ذهن و سپس وارد کردن بدافزار و ویروس یا دزدی داده
  - استفاده از گوشی‌های همراه
    - حملهٔ با مبدا چینی استفاده از تبلیغات مخرب بار شده در کاربردهای همراه و مرورگرهای همراه به مثابهٔ سازوکار حمله

# حمله بندآوری خدمت و حملهٔ بندآوری خدمت توزیعی

- حمله دیگر با مبدا چین
  - علیه بستر توسعهٔ نرم‌افزار گیت‌هاب
  - مشخصا به دو پروژهٔ ضدسانسور چینی قرارگرفته در بستر
  - از نوع توپ بزرگ

# حملات داخلی

- گمان بر حملهٔ عامل خارجی
- بیشترین خطرات به نهادهای فیاوری درون‌سازمانی
  - کارمندان بانک دزدی پول بیشتر نسبت به رباینده‌گان بانک

- دسترسی کارمند به اطلاعات محرمانه
- رویه‌های امنیتی ضعیف
  - امکان بررسی اطلاعات بدون گذاشتن ردی از خود
- خودی‌ها محتملا منبع حملهٔ سایبری نسبت به خارجی‌ها
  - لزوما نه برای جرم خودشان بلکه عامل پخش ناآگاهانهٔ اطلاعات

# نرم‌افزارهای با ضعف طراحی

- گاهی ضعف در سیستم عامل و گاهی در نرم‌افزارهای کاربردی مانند مرورگرها
- عوامل شکاف‌های نرم‌افزاری و آسیب‌پذیری‌ها
  - افزاش پیچیدگی و اندازهٔ برنامه نرم‌افزاری
  - درخواست‌های تحویل زمان‌بر به بازارها
- حملات تزریق سکیول
  - بهره‌بردن از آسیب‌پذیری‌های ناشی از کاربردهای وبی با طراحی کد ضعیف
    - ضعف در تائیداعتبار درست یا فیلتر داده‌های ورودی کاربر در صفحه
    - موجب ورود کد برنامه مخرب به سیستم و شبکهٔ شرکت
    - استفادهٔ حمله‌کننده از این ضعف‌ها جهت ارسال پرسش سکیولی به پد
      - جهت دستیابی به آن، کارگذاشتن کد مخرب یا دسترسی به سیستم‌های دیگر در شبکه
    - کاربردهای وبی بزرگ دارای صدها محل ورودی داده کاربر
      - هرکدام عامل ایجاد فرصت حملهٔ تزریق سکیول
    - وجود ابزارهای بررسی کاربر وبی برای این نوع آسیب‌پذیری‌ها

# نرم‌افزارهای با ضعف طراحی

- یافتن هزاران نقاط آسیب‌پذیر در مرورگرهای اینترنتی،رایانه‌ها، نرم‌افزار لینوکس،کاربردها و سیستم‌عامل همراه
- ۱۳۹۵
  - دههزار گزارش نقطه آسیب‌پذیر
  - بیش از ۲۰ درصد اسیب‌پذیری وبی
    - اسکریپت‌نویسی بین مانه و خطرات سکیول
  - آسیب‌پذیری روز–صفر
    - قبلا گزارش نشده و فعلا نبود وصله
  - گزارش ۴۰۰۰ آسیب‌پذیری در سال مذکور
    - با تعداد کمتری حملهٔ مرتبط با آنها
- طراحی رایانه با درگاه‌های باز جهت ارسال و دریافت با رایانه‌های دیگر
  - معمولا درگاه‌های ۴۴۵ تی‌سی‌پی، ۸۰، ۴۴۳
- شرکت سوفوس
  - گزارش یافتن آسیب‌پذیری روز صفر در افیس مایکروسافت
    - پروتکل تبادل دادهٔ پویای مایکروسافت
    - استفاده برای اشتراک داده بین کاربردها
    - امکان استفاده برای تحویل تروا‌های دسترسی از راه دور

# نرم‌افزارهای با ضعف طراحی

- ۱۳۹۳ ایراد در سیستم رمزگذاری اپن‌اس‌اس‌ال
  - مورداستفادهٔ میلیون‌ها تارمانه
  - باگ خونریزی قلبی
  - اجازه به رمزگشایی جلسه اس‌اس‌ال و یافتن نام کاربر، رمزها، اطلاعات دیگر
  - با استفاده از اپن‌س‌س‌ل
    - در همکاری با ضربه قلب برای تسهیل در تماس ماندن کاربر دور پس از اتصال به سرور وب
    - امکان درز یافتن بخشی از محتوای حافظهٔ سرور محتملا داری رمز و کلید رمزگذاری
  - همچنین shellshock بر لینوکس و یونیکس و س‌ع مک
    - امکان استفاده از CGIجهت افزودن کدمخرب

# مسائل امنیتی شبکه اجتماعی

- شبکه‌های اجتماعی مکانی برای
  - ویروس‌ها
  - دزدی هویت
  - بدافزارها
  - طله‌گذاری
  - اسپم
- کلاهبرداری اشتراک
  - اشتراک بی‌اطلاع و دستی ویدئوها و داستان‌ها و تصاویر دارای نشانی به مانه‌های مخرب
- پیشنهادات جعلی، دگمه‌های پسند جعلی،کاربردهای جعلی

# مسائل امنیتی شبکه اجتماعی

- دارای نظارت و دقت کمتر
  - موتورهای جستجو دارای فهرستی از نشانی‌های مخرب و بررسی آنها در مانه‌ها
- باز
  - هر کس دارای امکان ایجاد صفحهٔ شخصی حتی مجرمان
- بیشترین حملات
  - حملات مهندسی اجتماعی
  - ترغیب بازدیدکننده به کلیک نشانی‌های به نظر علیه سلام

# مسائل امنیتی بستر موبایلی

- گوشی همراه منبع اطلاعات شخصی و مالی افراد
  - استفاده جهت انجام تراکنش‌ها از خرید خرده تا بانک همراه
- دارای خطرات مشابه ابزار اینترنتی
  - امکان هک کردن بی‌سیم‌های عمومی
  - یافتن خطا در پروتکل امنیت بی‌سیم WPA2
    - ایجاد امکان دزیدن رمزها و ایمیل و ترافیک شبکه‌های بی‌سیم
    - بیش از ۴۰ درصد اندرویدی‌ها
- با این وصف
  - اطلاع کم عموم مردم از خطرات دستگاه همراه

# مسائل امنیتی بستر موبایلی

- بدافزار تلفن سلولی همراه
  - کاربردهای همراه مخرب
  - کرم بلوتوث در سرع سیمبین
  - عامل جستجوی بدون وقفه دیگر موبایل
    - خالی شدن سریع باتری
  - آیفون
    - تاثیر بر قفل‌شکسته‌ها و تبدیل آن به ابزارهای‌شب‌بات
    - با استفاده از کرم iKee.B

# مسائل امنیتی بستر موبایلی

- ۱۳۹۵
  - یافتن هژده میلیون آلودگی بدافزاری همراه‌ها
  - به سمت تحت تاثیر قرار دادن پرداخت همراه و کاربردهای بانک همراه
  - گزارش سیمانتک بر یافتن بدافزاری اندرویدی
    - یافتن پیام‌های متنی با کدهای تایید بانکی و رد کردن آن‌ها به حمله‌کننده
      - بویش پیامک

- ایفن
  - سه خطر روز-صفر
- کاربردهای همراه استارباکس (کاربرد پرداخت با بیشترین امار پرداخت در امریکا)
  - ذخیرهٔ نام کاربری و گذرواژه و ایمیل در متن معمولی
  - امکان دسترسی هر کس به آن با وصل کردن گوشی به رایانه
  - اشتباه گرفتن تاکید بر راحتی و استفادهٔ آسان در طراحی کاربرد با مسائل امنیتی

# مسائل امنیتی بستر موبایلی

- طله صوتی vishing
  - پیام‌های صوتی جهت به کمک به کودکان قطحی‌زده هائیتی
- طله متنی Smishing
- هلیغات madware

# گمان بر امن بودن گوشی هوشمند

- دلخوشی به حفاظت گوگل یا اپل
- اما امکان استفاده از گوشی هوشمند همچون هر ابزار اینترنتی دیگر
- درخواست فایل بدون اطلاع کاربر
- حذف فایل
- انتقال فایل
- نصب برنامه و اجرا در زمینه جهت پایش و جمع‌اوری اطلاعات کاربر
- تبدیل به بات
- کاربردها محتمل‌ترین مکان نقض امنیت
- شبکه‌های ناامن
- استفاده از ضعف‌های سیم‌کارت

# مسائل امنیتی ابر

- حرکت به خدمات ابری موجب خطرات امنیتی
- حمله بندآوری توقف در دسترسی خدمات ابر
  - ۱۳۹۵ داین dyn موجب بر هم خوردن خدمات ابری در امریکا
  - بیشتر حملات حمله‌های کاربرد وب
  - خطر بیشتر برای شرکت‌های با شبکهٔ هیبرید
  - دراپباکس و امکان دسترسی به فایل‌ها در آن بدون اجازه
  - انتشار عکس‌های خصوصی چهره‌ها
    - حمله‌های تک-پایین در راستای رمز و دسترسی
    - لاورنس و آی‌کلاود
  - اتصال بیشتر دستگاه‌ها و کاربردها با خدمات ابری
    - استفاده از فضای ابری جهت اتصال به حساب‌های وصل شده
    - مثال هونان
- عدم امتحان و بررسی زیرساخت
- نداشتن رمزگذاری و رویه‌های قوی امنیتی در ابرها

# مسائل امنیتی اینترنت اشیاء

- محیطی پرچالش جهت حفاظت
- ۱۳۹۴
  - جیپ چروکی
    - کنترل از دور و موجب از کار انداختن ترمز، خاموشی موتور، و فرمان چرخ
  - فیات کرایسلر
- وسایل پزشکی
- داین
  - پانصدهزار دستگاه ااش
- شب‌بات

| CHALLENGE | POSSIBLE IMPLICATIONS |
| --- | --- |
| Many IoT devices, such as sensors, are intended to be deployed on a much greater scale than traditional Internet-connected devices, creating a vast quantity of interconnected links that can be exploited. | Existing tools, methods, and strategies need to be developed to deal with this unprecedented scale. |
| Many instances of IoT consist of collections of identical devices that all have the same characteristics. | Magnifies the potential impact of a security vulnerability. |
| Many IoT devices are anticipated to have a much longer service life than typical equipment. | Devices may "outlive" the manufacturer, leaving them without long-term support that creates persistent vulnerabilities. |
| Many IoT devices are intentionally designed without the ability to be upgraded, or the upgrade process is difficult. | Raises the possibility that vulnerable devices cannot or will not be fixed, leaving them perpetually vulnerable. |
| Many IoT devices do not provide the user with visibility into the workings of the device or the data being produced, nor alert the user when a security problem arises. | Users may believe an IoT device is functioning as intended when, in fact, it may be performing in a malicious manner. |
| Some IoT devices, such as sensors, are unobtrusively embedded in the environment such that a user may not even be aware of the device. | Security breach might persist for a long time before being noticed. |

# مسائل امنیتی اینترنت اشیاء

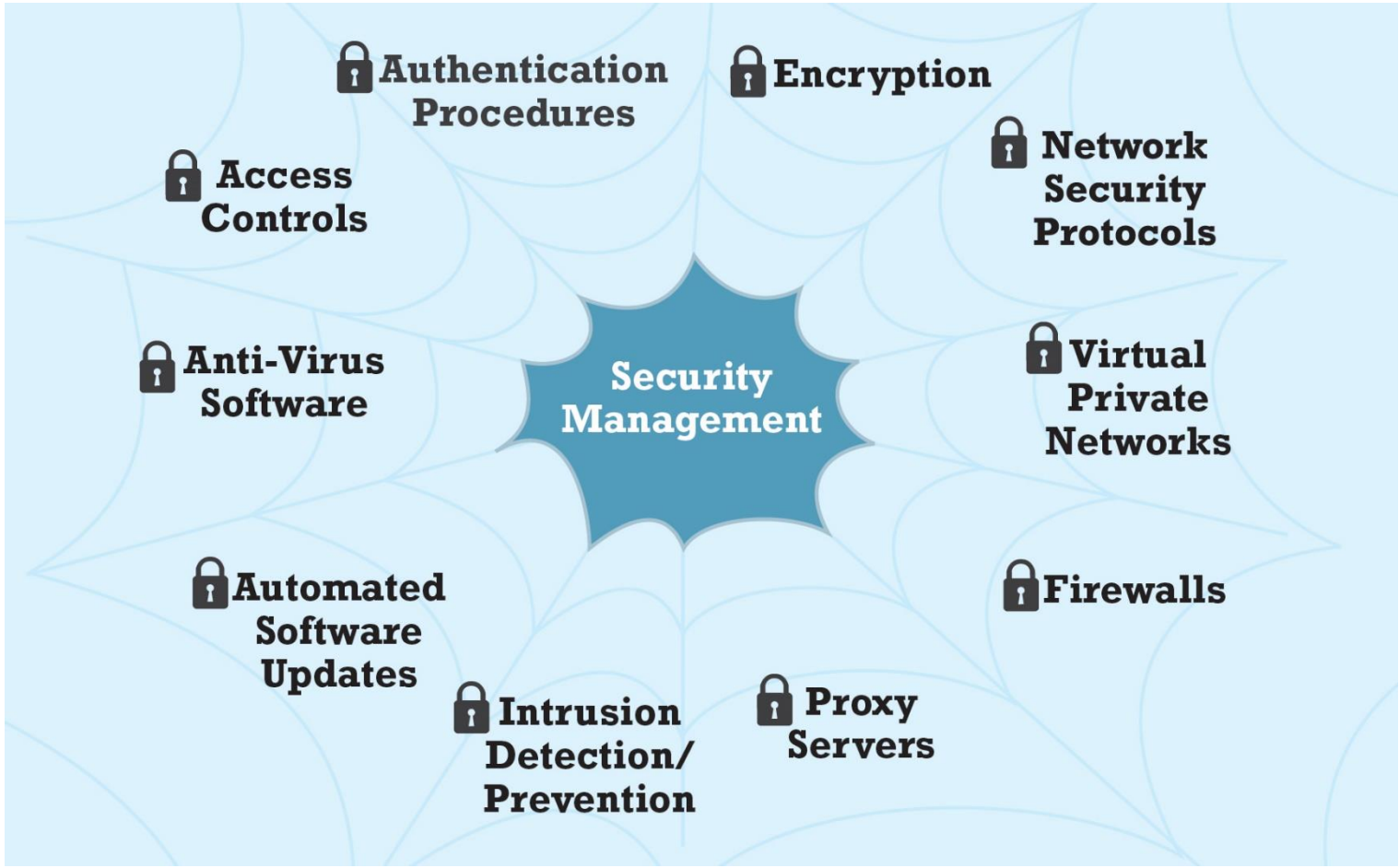
- محیطی پرچالش جهت حفاظت
- حجم عظیم نشانی‌های متصل به هم
- دستگاه‌های تقریبا مشابه با عمر طولانی خدمت‌رسانی
- بدون ویژگی‌های بروزکردن
- دید کم نسبت به نحوهٔ کار و داده و امنیت

# راه‌حل؟

- فناوارنه
- سیاست‌گذاری

# راه‌حل‌های فناوری

- استفاده از مجموعه ابزارهایی که حمله یا تخریب خارجی به مانه را مشکل می‌کند



# راه‌حل‌های فناوری

- حفاظت از ارتباطات اینترنتی
  - محتمل‌ترین محل تهدید اینترنتی
  - متفاوت از شبکهٔ خصوصی
  - مهم‌ترین راه- رمزگذاری
- امن‌سازی کانال‌های ارتباطی
- شبکه‌های محافظ
  - دیوارآتش
  - سرور پراکسی
- حفاطت از سرورها و مشتری‌ها
  - امنیت سیستم عامل
  - نرم‌افزار ضدویروس

# رمزگذاری

- تبدیل داده به متن رمزی صرفا قابل خواندن فرستنده و گیرنده
  - کلید key یا cipher هر روش تبدیل
- امن کردن ذخیره اطلاعات  و ارسال اطلاعات
- عرضهٔ ۴ بعد کلیدی از شش بعد امنیت تجارت الکترونیک
  - یکپارچگی پیام
    - عدم تغییر پیام
  - عدم‌انکار
    - عدم انکار ارسال پیام
  - احراز هویت
    - تشخیص هویت فرد یا رایانه
  - محرمانگی
    - اطمینان از نخواندن غیر
- دارای سابقه
  - جانشینی substituition
  - جابجایی transposition
  - ایران چه؟

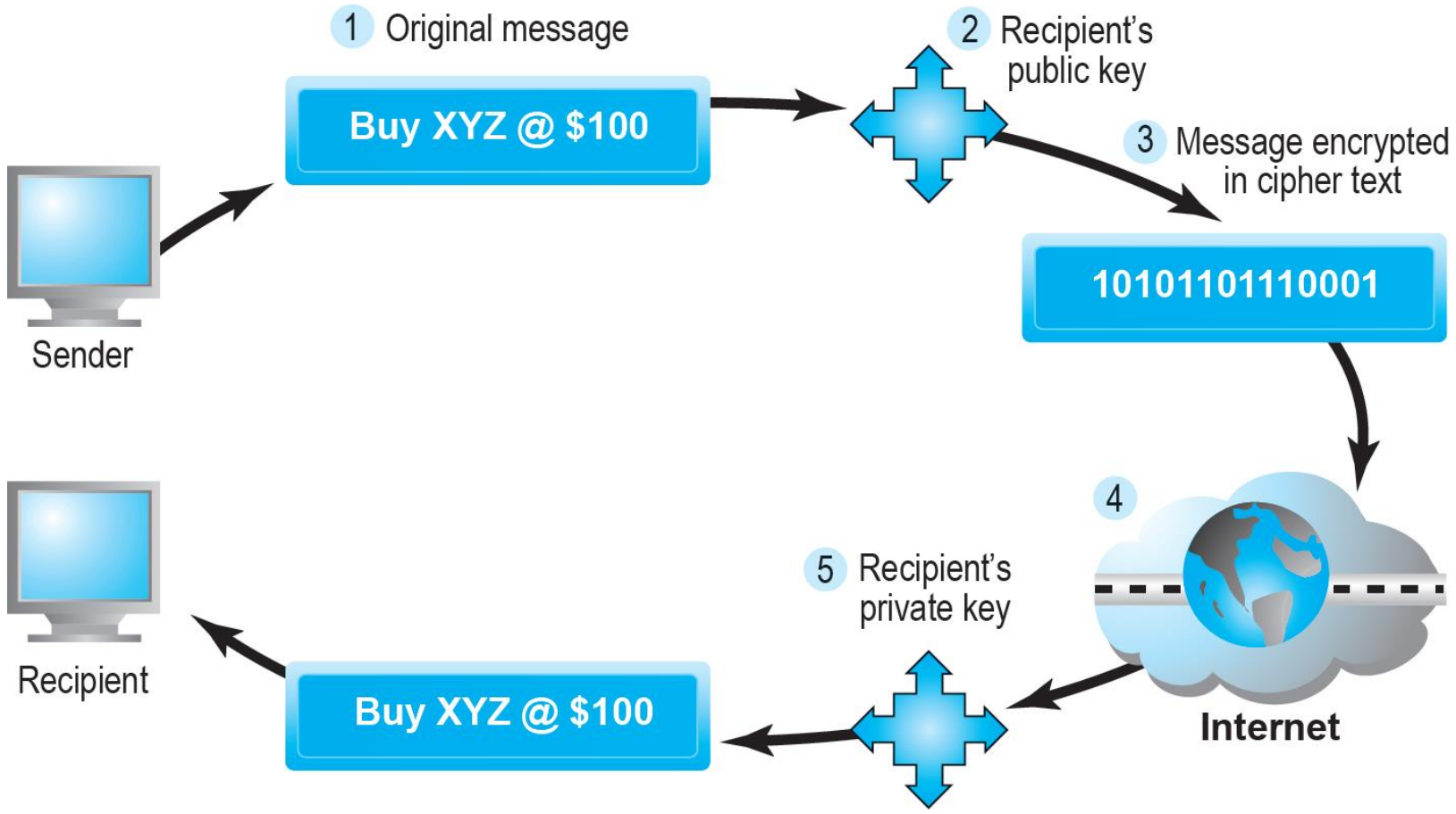
# رمزنگاری کلید متقارن

- استفاده گیرنده و فرستنده از کلید دیجیتال یکسان برای رمزگذاری و رمزگشایی پیام
- نیاز به مجموعه کلیدهای متفاوت برای هر تراکنش
- قدرت رمزگذاری- طول کلید دودوئی
- استانداۀ رمزگذاری داده DES
  - طول کلید ۵۶ بیتی
  - رمز کردن سه باره هر بار کلیدی جداگانه
- استانداۀ رمزگذاری پیشرفته AES
  - اندازه کلید ۱۲۸ و ۱۹۲ و ۲۵۶ بیتی
- استفادۀ دیگر استانداه از کلیدهایی تا ۲۰۴۸ بیت

# رمزنگاری کلید عمومی(نامتقارن)

- دیفی و هلمن
- حل مسئلهٔ تبادل کلید
- استفاده از دو کلید دیجیتالی مرتبط با هم
  - کلید عمومی (انتشار عمومی)
  - کلید خصوصی (صرفا نزد صاحب)
- استفاده از هر دو کلید جهت رمز کردن و واکردن ویام
- عدم امکان رمزگشایی پیامی با همان استفاده از همان کلید استفاده شده در رمزگذاری
- فرستنده استفاده از کلید عمومی جهت رمز کردن پیام
  - گیرنده استفاده از کلید خصوصی جهت باز کردن آن

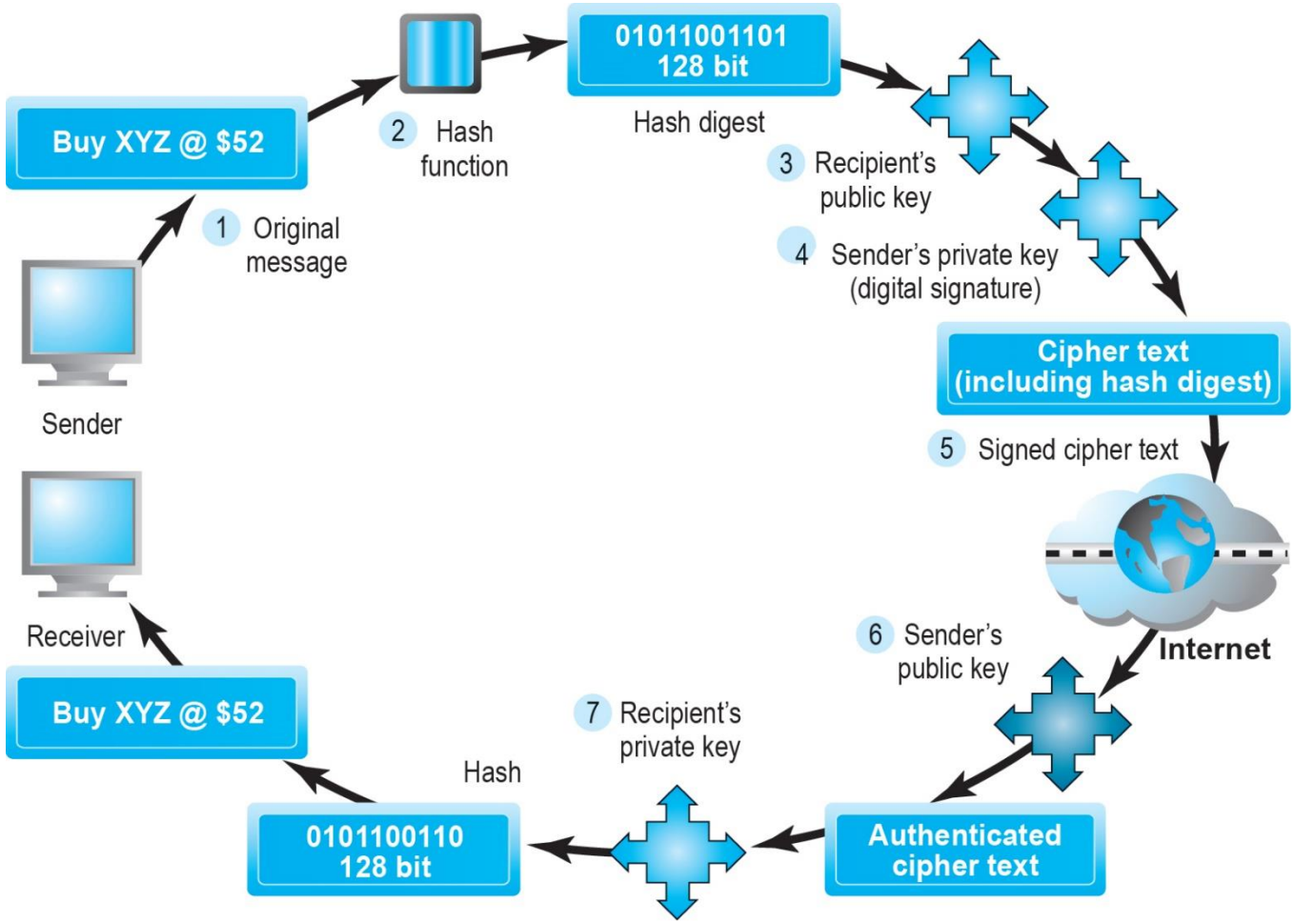
# رمزنگاری کلید عمومی



# رمزنگاری کلید عمومی با استفاده از امضای دیجیتال و خلاصه‌های درهم

- تاکنون اطمینان از اینکه پیام خوانده نشود
  - ولی از کجا مطمئن باشیم فرستنده کیست
  - موجب عدم احراز هویت، انکار، عدم یکپارچگی
- تابع درهم
  - الگوریتم تولید عصاره پیام با طول ثابت
- فرستنده
  - اعمال الگوریتم ریاضی (تابع درهم) به پیام و سپس رمزکردن پیام و نتیجهٔ درهم با کلید عمومی گیرنده
  - رمزکردن پیام و نتیجه هش با کلید خصوصی فرستنده
    - ایجاد امضای دیجیتال جهت عدم‌انکار و احراز هویت
- گیرنده
  - استفاده از کلید عمومی فرستنده جهت احراز هویت و سپس کلید خصوصی خود جهت رمزگشایی نتیجه هش و پیام

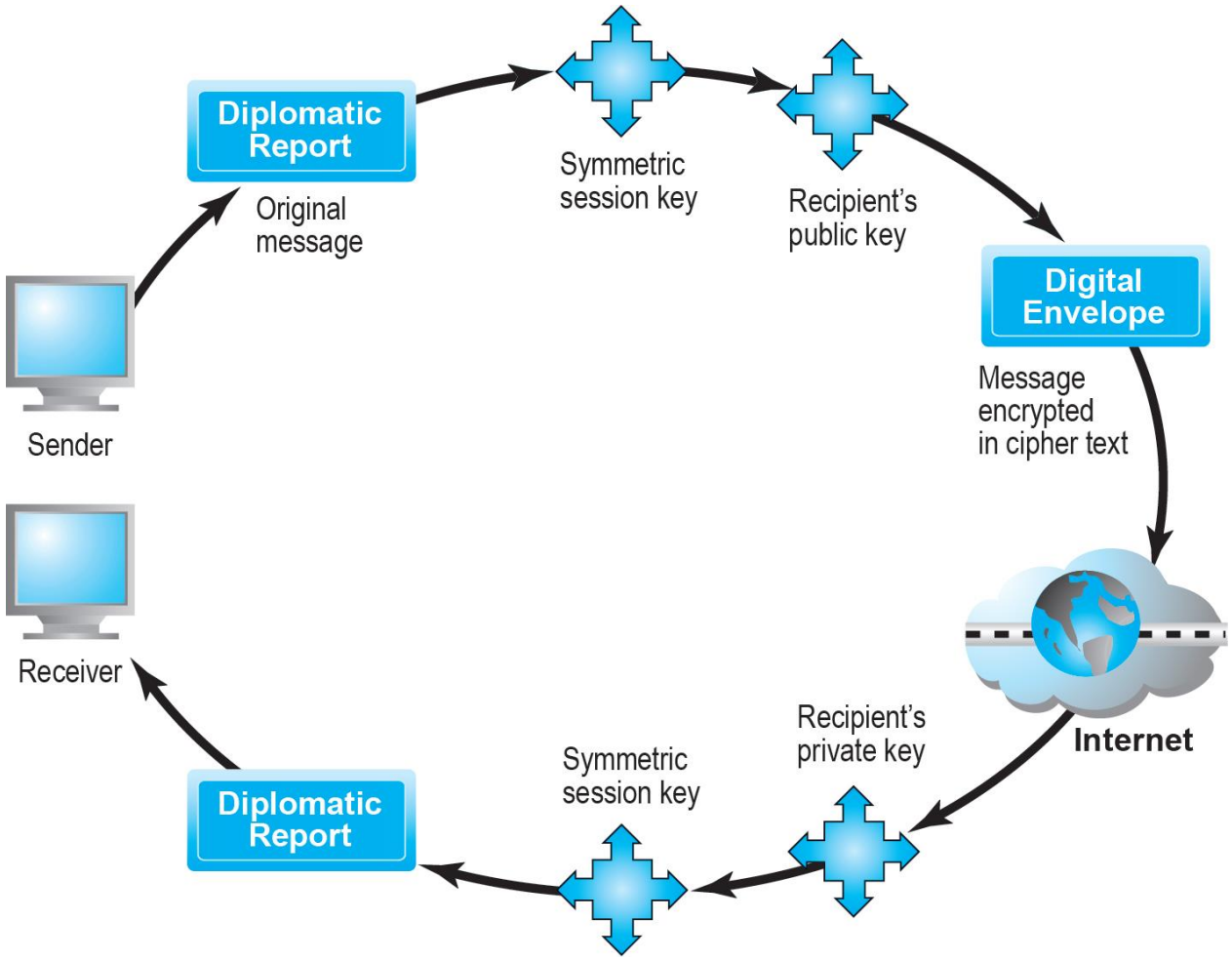
# رمزنگاری کلید عمومی با استفاده از امضای دیجیتال و خلاصه‌های هش



# پاکت دیجیتال

- ضعف‌های نشانیِ
  - رمزگذاری کلید عمومی
    - محاسبات کند
    - کاهش سرعت انتقال
    - افزایش زمان پردازش
  - رمزگذاری متقارن
    - خطوط انتقال ناامن
- استفاده رمزگذاری کلید متقارن جهت رمزکردن داده
- استفاده از رمزگذاری کلید عمومی جهت رمزگذاری و ارسال کلید متقارن

# پاکت دیجیتال



# منابع تهیه این درس

- Laudon
- Stalings