به نام خداوند بخشنده مهربان

مبانی امنیت شبکه

Fundamentals of Network Security



یاشار ابری

دانشکده مهندسی، دانشگاه تهران

Yasharabri.ut.ac.ir@gmail.com

yasharabri@ut.ac.ir

معرفی درس

- مبانی امنیت شبکه‌های کامپیوتری
- Fundamentals of Computer Network Security
- ۳ واحد نظری
- درس اختصاصی

راه‌های ارتباطی

سایت اطلاع رسانی

https://utwp.ir/utabri/

+ سامانه های دانشگاه تهران

کانال‌های اطلاع‌رسانی



@utabri

ارزیابی

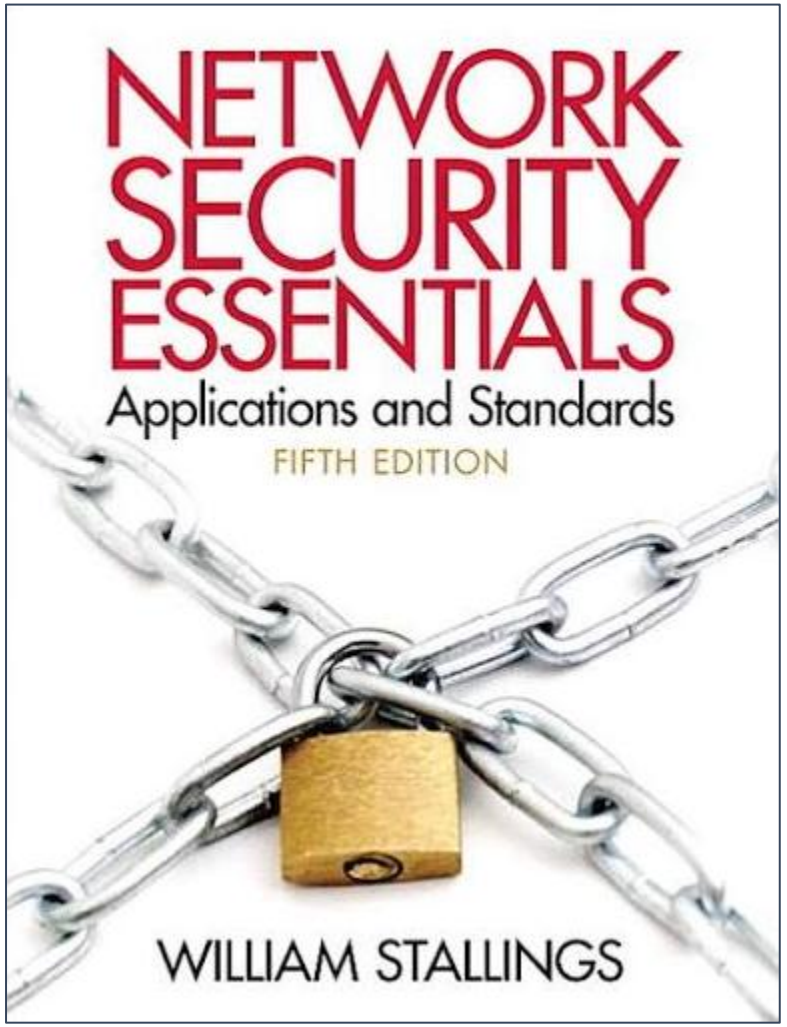
- اصلی: (بارم‌بندی انعطاف‌پذیر است)

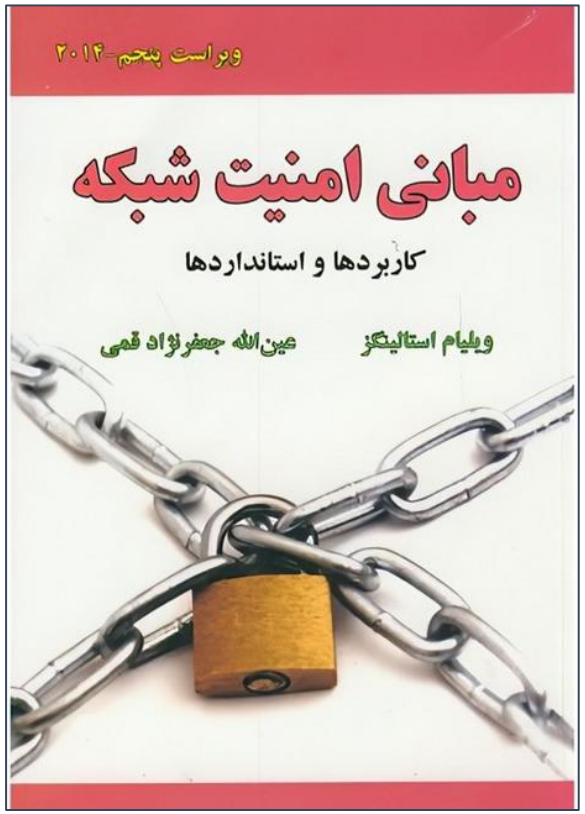
حضور در کلاس	۷۰٪
همکاری با تی‌ای‌ها	
تکلیف / پروژه	
آزمون پایان ترم	۳۰٪

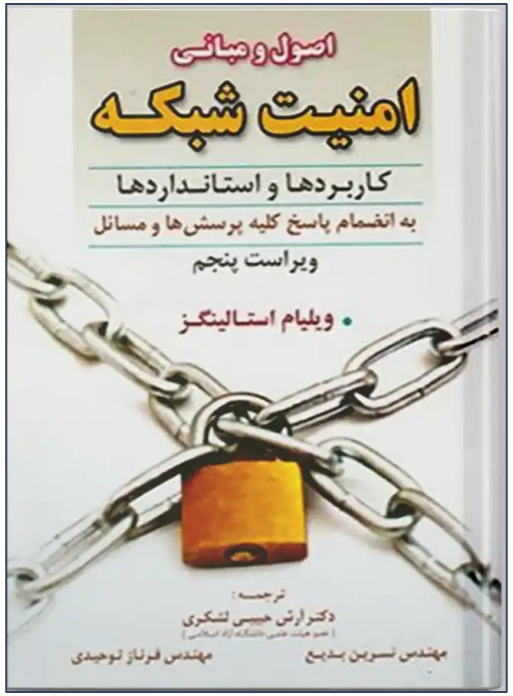
- امتیازی:
  - کار مطالعاتی
  - مقاله علمی مجله یا نشریه

منابع پیشنهادی

- برای مطالعه بیشتر







۱ نگاهی کلی بر امنیت رایانه و شبکه

- سرفصل‌های این بخش:
  - مفاهیم پایه امنیت رایانه (محرمانگی، جامعیت، دسترس‌پذیری)
  - معماری امنیتی OSI (X.۸۰۰) و انواع حملات
  - سرویس‌های امنیتی و مکانیزم‌های امنیتی
  - مدل کلی برای امنیت شبکه

مفاهیم پایه امنیت رایانه

- **محرمانگی (Confidentiality):** اطمینان از این‌که اطلاعات فقط در دسترس افرادی باشد که مجاز به دیدن آن هستند؛ شامل حفظ حریم خصوصی داده‌های شخصی نیز می‌شود.
- **جامعیت (Integrity):** تضمین این‌که داده و نرم‌افزار فقط توسط افراد مجاز و به شیوه مشخص تغییر کند؛ یعنی داده در مسیر انتقال یا ذخیره‌سازی دستکاری نشده باشد.
- **دسترس‌پذیری (Availability):** اطمینان از این‌که سیستم‌ها و داده‌ها هر زمان که کاربر مجاز نیاز داشت، در دسترس و قابل استفاده باشند؛ حملات DoS دقیقاً همین ویژگی را هدف می‌گیرند.
- **اصالت و پاسخگویی:** NIST دو مفهوم اصالت (Authenticity، یعنی اثبات این‌که پیام واقعاً از منبع ادعاشده آمده) و پاسخگویی (Accountability، یعنی قابل ردیابی بودن اقدامات هر کاربر) را به سه‌گانه CIA افزوده تا تصویر کامل‌تری از امنیت ارائه شود.

حضرت امام حسن عسکری علیه السلام: هیچ کسی را به گونه‌ای احترام مکن که او را به رنج و مشقت بیفکنی.

بحار، جلد۷۸، صفحه۳۷۴

نمودار سه‌گانه CIA به‌صورت مثلث با سه رأس محرمانگی، جامعیت و دسترس‌پذیری



- **تغییرات رخ داده را تشخیص می‌دهد:**
  - در حال ذخیره‌سازی
  - در حال انتقال
  - در حال پردازش

- **محافظت در برابر:**
  - دسترسی غیرمجاز
  - استفاده غیرمجاز
  - افشا

- **محافظت از داده‌ها:**
  - موجود در سیستم‌ها
  - در حال انتقال
  - در حال پردازش

- **کنترل و اطمینان:**
  - دسترسی مجاز
  - سطح قابل قبول عملکرد
  - تحمل خطا
  - افزونگی
  - پشتیبان گیری قابل اعتماد
  - جلوگیری از دست رفتن یا تخریب داده‌ها

حضرت امام مهدی عجل الله تعای فرجه الشریف: برای تعجیل فرج زیاد دعا کنید، چون همین دعا موجب فرج شماست.
منتخب‌الاثر، ص۲۶۸

خطر، آسیب‌پذیری و تهدید

- از این پس ممکن به جای **«امنیت شبکه‌های کامپیوتری»** عبارت **«امنیت دیجیتال»** را نیز به همین معنی به کار ببریم.
- در ادامه بهتر است با ۳ اصطلاح مهم در امنیت دیجیتال آشنا شویم چرا که تقریبا محور امنیت روی آنها می‌چرخد:
  - خطر، احتمال وقوع یک اتفاق ناگوار است.
  - تهدید، اتفاق ناگواری است که ممکن است رخ دهد.
  - آسیب پذیری، ضعفی است که تهدید از آن بهره می‌برد.
- بنابراین، برای اینکه یک جمله ای بنویسیم: **خطر پتانسیل آسیب است که اگر تهدید از آسیب پذیری استفاده کند و تحقق یابد، رخ می‌دهد.**

حضرت امام موسی کاظم علیه‌السلام: تجربه‌ها برای ادب کردن و گذشت روزها برای موعظه و پند کافی است.

حیاة امام کاظم علیه‌السلام، ج۱، ص۲۵۶

دژکوب و قلعه مثالی برای درک سه‌گانه امنیت

- برای درک بهتر فرض کنیم که دیوارهای یک قلعه در برابر دژکوب مقاوم نیستند. پس در این صورت:
  - مقاوم نبودن دیوارهای قلعه آسیب‌پذیری آن است.
  - دژکوب‌ها به دلیل قدرت انهدام دیوار تهدید هستند.
  - پس در این صورت قلعه در خطر انهدام توسط دژکوب‌ها قرار دارد.

حضرت امیرالمومنین علی بن ابی طالب صلوات‌الله‌علیه‌و آله: به خدا سوگند فاطمه مرا هیچ‌گاه خشمگین نکرد و در هیچ کاری از من سرپیچی ننمود.

بحار، ج۴۳، ص۱۳۴

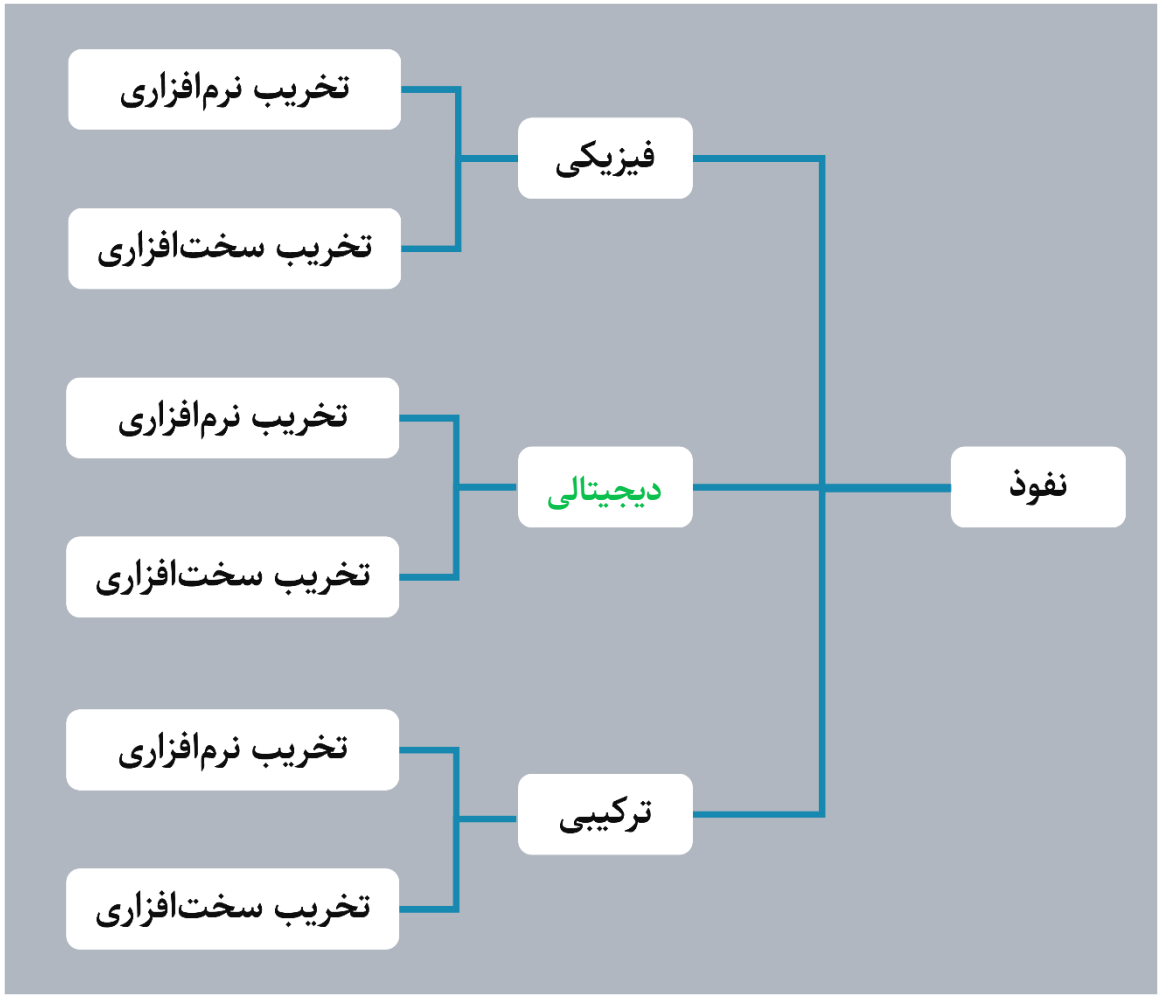
تصویر دژکوب و قلعه مثالی برای درک سه‌گانه امنیت



حضرت صدیقه کبری فاطمه الزهرا سلام‌الله‌علیها: خدایا! گفتار و کردار توبه‌کاران و رستگاری و پاداش مجاهدان را از تو می‌طلبم.

فلاح سائل، ص ۳۱۲

نمودار انواع نفوذ و انواع تخریب‌های احتمالی آنها



امیرالمومنین علی بن ابی‌طالب صلوات‌الله‌علیه و آله:
من هر گاه فاطمه (سلام‌الله‌علیها) را می‌دیدم، تمام غم و غصه‌هایم برطرف می‌شد.
بحار، ج۴۳، ص۱۳۴

تفاوت حملات فعال و غیرفعال

ویژگی	حمله غیرفعال (Passive)	حمله فعال (Active)
هدف اصلی	سرقت اطلاعات (جاسوسی)	تغییر اطلاعات یا تخریب سیستم
تغییر در داده‌ها	خیر (فقط خواندن)	بله (تغییر، حذف یا اضافه کردن)
قابلیت تشخیص	بسیار سخت (چون اثری ندارد)	نسبتاً آسان (اثر مخرب دارد)
تأثیر بر سیستم	کمترین میزان اختلال	ایجاد اختلال و آسیب جدی
ابزار دفاعی اصلی	رمزنگاری (Encryption)	دیواره آتش، احراز هویت و IDS

حضرت صدیقه کبری فاطمه زهرا سلام‌الله‌علیها: هر کس خدا را خالصانه عبادت کند، خداوند برترین مصلحت خود را نثارش می‌کند.

بحار، ج۷۰، ص۲۴۹

حمله‌های امنیتی (Security Attacks)

مثال رایج	توضیح	نوع حمله
استراق سمع، تحلیل ترافیک	مهاجم فقط اطلاعات را می‌بیند یا الگوی ارتباط را بررسی می‌کند، بدون تغییر داده‌ها؛ چون چیزی تغییر نمی‌کند تشخیص آن بسیار سخت است.	غیرفعال (Passive)
جعل هویت (Masquerade)	مهاجم خود را به‌جای یک موجودیت مجاز جا می‌زند تا امتیازات آن را به دست آورد.	فعال (Active)
بازپخش (Replay)	مهاجم یک پیام معتبر قدیمی را دوباره ارسال می‌کند تا اثری غیرمجاز ایجاد کند، مثلاً تراکنش تکراری.	فعال (Active)
تغییر پیام (Modification)	بخشی از یک پیام قانونی تغییر داده می‌شود یا ترتیب پیام‌ها به‌هم می‌ریزد.	فعال (Active)
ممانعت از سرویس (DoS)	جلوگیری از استفاده عادی یا مدیریت تسهیلات ارتباطی، مثلاً با سیل کردن ترافیک به سمت یک سرور.	فعال (Active)

حضرت امام حسن بن علی مجتبی علیه‌السلام: هلاکت و نابودی دین و دنیای هر شخص در ۳ چیز هست: تکبر، حرص، حسد.

اعیان الشیعة، ج۱، ص۵۵۷

سرویس‌های امنیتی

- **احراز اصالت (Authentication):** اطمینان از این‌که طرف ارتباط همان کسی است که ادعا می‌کند؛ شامل احراز اصالت موجودیت همتا و منشأ داده.
- **کنترل دسترسی (Access Control):** توانایی محدود کردن و کنترل دسترسی به سیستم‌ها و برنامه‌ها بر اساس هویت و مجوزهای هر کاربر.
- **محرمانگی داده:** حفاظت از داده در برابر افشای غیرمجاز، چه در حالت انتقال و چه در حالت ذخیره‌شده.
- **جامعیت داده:** تضمین این‌که داده دریافتی دقیقاً همانی است که فرستاده شده و در مسیر تغییر نکرده است.
- **عدم انکار (Non-repudiation):** جلوگیری از این‌که فرستنده یا گیرنده بتواند ارسال یا دریافت پیام را انکار کند؛ پایه امضای دیجیتال.

حضرت خاتم الانبیا محمد مصطفی صلی الله علیه و آله و سلم: هر کس برادر خود را برای گناهی که از آن توبه کرده سرزنش کند نمی‌میرد تا خود آن گناه را مرتکب شود.

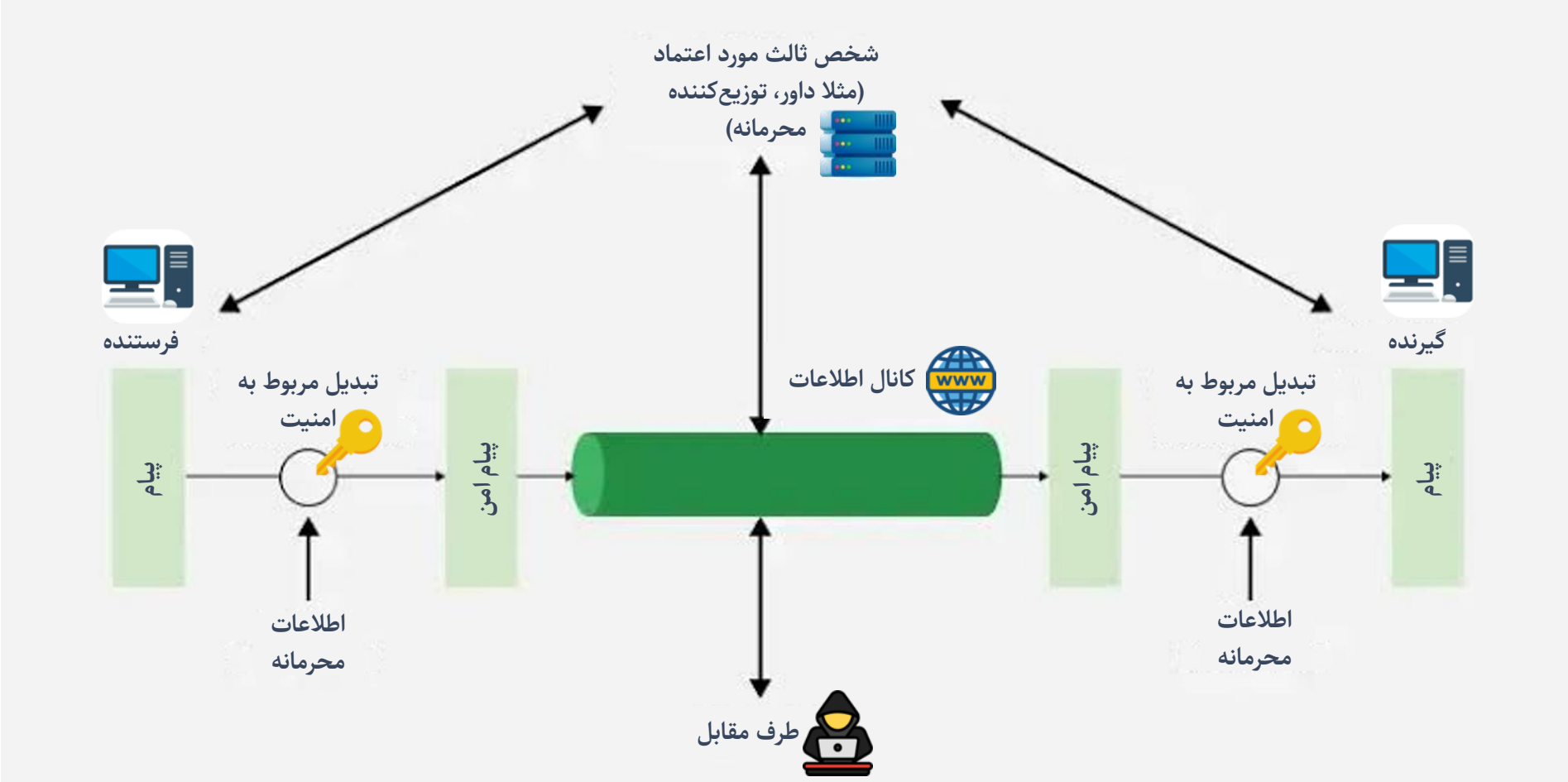
تنبیه الخواطر جلد ۱ صفحه ۱۱۳

مکانیزم‌های امنیتی و مدل شبکه

- **مکانیزم‌های فراگیر (Pervasive):** مکانیزم‌هایی مانند کنترل دسترسی و ثبت رویداد (Logging) که به یک سرویس خاص محدود نیستند و در سرتاسر سیستم عمل می‌کنند.
- **مکانیزم‌های خاص:** رمزنگاری، امضای دیجیتال و کنترل مسیریابی، هرکدام برای پیاده‌سازی یک یا چند سرویس امنیتی مشخص طراحی شده‌اند.
- **مدل امنیت شبکه:** برای انتقال امن پیام از فرستنده به گیرنده در حضور یک مهاجم، به یک تبدیل امنیتی (مانند رمزنگاری)، یک اطلاعات محرمانه مشترک (کلید) و معمولاً یک طرف سوم مورد اعتماد نیاز است.

حضرت امیرالمومنین علی بن ابیطالب صلوات الله علیه و آله:
برای دوست خود خیرخواهی و یک رنگی‌ات را، برای آشنایان خود یاری‌ات را و برای عموم مردم خوشرویی‌ات را صرف کن.
غرر، حدیث ۲۴۶۶

نمودار مدل امنیت شبکه با فرستنده، گیرنده، کانال ناامن، مهاجم و طرف سوم مورد اعتماد در وسط



حضرت صدیقه کبری
فاطمه زهرا سلام الله
علیها:
خداوند کامل کردن
پیمانه‌ها و ترازوها را برای
زشت نشان دادن کم
فروشی قرار داد.
من لایحضر، ج۳، ص۵۶۸