درس تخصصی گرایش رایانش امن: امنیت شبکه

نام درس	امنیت شبکه		
نام درس به انگلیسی	Network Security		
نوع واحد	تخصصی	مهندسی کامپیوتر	۳ واحد
مقطع	کارشناسی		
هم‌نیازها			
پیش‌نیازها	شبکه‌های کامپیوتری		
مطالب پیش‌نیاز			
کتاب(های) مرجع	[1] William Stallings, *Network Security Essentials: Applications and Standards*. Prentice Hall, 4th Edition, 2010. [2] William Stallings, *Cryptography and Network Security Principles and Practices*. 5th Edition, Prentice Hall, 2010. [3] Charlie Kaufman, Radia Perlman, and Mike Speciner, *Network Security: Private Communication in a Public World*. 2nd Edition, Prentice Hall, 2002.		
اهداف درس	گسترش رو به رشد شبکه‌های کامپیوتری در سازمان‌ها و همچنین اتصال بسیاری از شبکه‌های محلی و کوچک به شبکه جهانی اینترنت، شبکه‌ها را به بستری پرمخاطره در تبادل داده‌ها تبدیل نموده است. هدف از ارائه این درس، آشنایی دانشجویان با مخاطرات، تهدیدات، و حملات ممکن در شبکه‌های کامپیوتری و همچنین آشنایی با روش‌های حفاظت داده‌ها و منابع در شبکه‌ها است. مکانیزم‌های امنیتی و پروتکل‌های متعددی که در لایه‌های مختلف شبکه (لایه شبکه، لایه انتقال، لایه کاربرد) مطرح شده‌اند در این درس مرور می‌شوند. علاوه بر این امنیت در شبکه‌های بی‌سیم و شبکه‌های نسل آتی (NGN) نیز مورد بررسی اجمالی قرار می‌گیرند.		
نتایج درس	دانشجویانی که این درس را با موفقیت پشت سر بگذارند بینش مناسبی در موارد زیر خواهند داشت: ۱- شناخت روش‌های متعدد رمزنگاری متقارن و نامتقارن و کاربرد هر کدام ۲- آشنایی با ابزارهای تامین امنیت شبکه‌های محلی و سیستم تشخیص مهاجم ۳- آشنایی با مکانیسم‌های موجود امنیتی در لایه‌های مختلف شبکه ۴- توان استفاده از کتابخانه‌های موجود رمزنگاری در برنامه‌های کاربردی		
فهرست مباحث	- مقدمه‌ای بر امنیت شبکه o تهدیدات و حملات شبکه‌ای o آسیب‌پذیری‌های شبکه o مکانیزم‌های امنیتی در شبکه - کاربرد رمزنگاری در امنیت شبکه o رمزنگاری در سطح اتصال (Link Layer) در مقابل رمزنگاری انتها-به-انتها (End-to-End) o حفظ محرمانگی و کنترل صحت در شبکه بر مبنای رمزنگاری - احراز اصالت در شبکه o طراحی پروتکل‌های احراز اصالت o پروتکل احراز اصالت Kerberos - کنترل دسترسی به شبکه o دیواره آتش و انواع آن o انواع آرایش دیواره آتش - امنیت داده در حال انتقال		

	o امنیت IP و پروتکل IPSec o شبکه‌های خصوصی مجازی (VPN) o مباحث امنیتی در IPv6 - امنیت شبکه‌های بی‌سیم o امنیت شبکه‌های بی‌سیم محلی o امنیت شبکه‌های WiMAX - امنیت لایه انتقال o مباحث امنیتی در وِب o پروتکل SSL & TLS o پروتکل HTTPS o پروتکل SSH - امنیت پست الکترونیکی o پروتکل PGP o پروتکل S/MIME o پروتکل DKIM - مباحث امنیتی در شبکه‌های NGN - سیستم‌های تشخیص و تحلیل شبکه o سیستم‌های تشخیص و پیشگیری از نفوذ (IDS/IPS) o سیستم‌ها و شبکه‌های تله عسل (Honeypots & Honeynets) - معماری امنیتی شبکه
نرم‌افزارهای مورد نیاز	ابزار openssl برای انجام تکالیف عملی مرتبط با رمزنگاری ابزار iptables و snort برای امنیت شبکه
پیشنهادی تکالیف	تکالیف تئوری و عملی (۵ سری)
پروژه‌های پیشنهادی	انجام یک پروژه عملی برای ارزیابی یکی از مکانیسم‌های مطرح شده در درس با استفاده از ابزار شبیه‌ساز شبکه
نمره‌دهی پیشنهادی	تکالیف کامپیوتری و گزارش‌ها ٪۳۰ آزمون‌های کتبی ٪۷۰
سایر مراجع	[1] Eric Cole, *Network Security Bible*. 2nd Edition, Wiley, 2009.