



۳-۲-۱۷ مبانی امنیت اطلاعات (CE362)

مبانی امنیت اطلاعات

تعداد واحد	پیش نیاز	هم نیاز
۳	شبکه‌های کامپیوتری	-

اهداف درس:

با توجه به گسترش روز افزون فناوری اطلاعات، فراهم نمودن امنیت آن اهمیت ویژه‌ای پیدا کرده است. هدف از این درس آشنایی دانشجویان با امنیت در فناوری اطلاعات در سطوح مختلفی مانند سطح سازمانی، سطح سرویس و سطح سیستم و بطور خاص امنیت شبکه‌های ارتباطی می‌باشد. در این درس دانشجویان پس از یادگیری مفاهیم پایه‌ای امنیت اطلاعات با معماری امنیت سازمانی آشنا می‌شوند. همچنین راهکارهای پایه‌ای امنیت در سیستم‌های کامپیوتری مانند رمزنگاری، تصدیق هویت، کنترل دسترسی و تشخیص نفوذ بحث و بررسی می‌شوند. در ادامه به امنیت زیرساخت‌های ارتباطی و امنیت سیستم و بطور خاص امنیت وب و بررسی انواع بدافزارها پرداخته می‌شود.

سرفصل مطالب:

- مقدمه (مفاهیم اولیه، نیازمندی‌های امنیت، انواع و ماهیت تهدیدها، دسته‌بندی‌های حملات، لایه‌های حفاظتی و دسته بندی مکانیزم‌های دفاعی)
- معماری امنیتی (معرفی استاندارد X.800، معرفی معماری امنیتی سازمانی، خط مشی‌های امنیتی، مدیریت ریسک، مدیریت حوادث و تداوم کسب و کار)
- رمزنگاری (رمزنگاری مرسوم (متقارن) و محرمانگی پیام، رمزنگاری با کلید عمومی و تصدیق هویت پیام، امضای رقمی)
- مدل‌ها و روش‌های کنترل دسترسی (سرویس‌های AAAA، مدل‌های کنترل دسترسی MAC/DAC/RBAC، انواع مدل‌ها و روش‌های تصدیق هویت، تصدیق هویت مبتنی بر گذرواژه و حملات مرتبط، تصدیق هویت مبتنی بر زیست سنجی)
- امنیت سیستم و نرم‌افزار (امنیت فایل سیستم، بدافزارها، ویروس‌ها و کرم‌ها، حفاظاها (فایروال‌ها) و سیستم‌های تشخیص نفوذ مبتنی بر میزبان، ماشین‌های مجازی)
- امنیت وب (حملات سمت سرور، حملات سمت کلاینت، نشست‌های وب و کوکی‌ها، SSL و HTTPS)
- امنیت شبکه و لایه انتقال (ناحیه بندی امنیتی شبکه، امنیت لایه و کنترل دسترسی میان ناحیه‌ای، امنیت بی سیم، VLAN و VPN)



[1] W. Stallings, *Network Security Essentials. Application and Standard*, 6th Edition, Prentice-Hall, 2012.
 [2] T. R. Peltier, *Information Security Fundamentals*, 2nd Ed., CRC Press, 2014.
 [3] M. Goodrich, R. Tamassia, *Introduction to Computer Security*, Pearson Education, 2014.