

دروس اصلی و اختیاری

کارشناسی ارشد

مهندسی فناوری اطلاعات

گرایش

امنیت اطلاعات



بسمه تعالی

برنامه آموزشی پیشنهادی دروس دوره کارشناسی ارشد گرایش امنیت اطلاعات

تعداد واحدهای درسی این دوره علاوه بر دروس جبرانی برابر ۳۲ واحد است. این واحدها شامل موارد زیر است:

دروس اصلی	۱۸	واحد
دروس اختیاری	۶	واحد
سمینار	۲	واحد
پایان نامه	۶	واحد

دروس جبرانی:

1- Discrete Structures	۱- ساختمان های گسسته
2- Data Structures	۲- ساختمان داده ها
3- Algorithm Design	۳- طراحی الگوریتم ها
4- Software Development Process	۴- مهندسی نرم افزار
5- Database Systems: Concepts and Design	۵- پایگاه داده ها
6- Operating Systems	۶- سیستم های عامل
7- Artificial Intelligence	۷- هوش مصنوعی

دروس اصلی:

1- Information Security Fundamentals	۱- مبانی امنیت اطلاعات
2- Applied Cryptology	۲- معماشناسی کاربردی
3- Network Security	۳- امنیت شبکه
4- Secure Computer Systems	۴- سیستمهای کامپیوتری امن
5- Database Security	۵- امنیت پایگاه داده ها
6- Security Protocols	۶- پروتکل های امنیتی



دروس اختیاری- گروه یک:

- | | |
|---|-----------------------------------|
| 1- Security Architecture: Design & Analysis | ۱- معماری امنیتی |
| 2- Formal Models and Information Security | ۲- مدل‌های فورمال و امنیت اطلاعات |
| 3- E-Commerce Security | ۳- امنیت تجارت الکترونیک |
| 4- Information Hiding | ۴- اختفاء اطلاعات |
| 5- Secure Communication Systems | ۵- سیستم‌های ارتباطی امن |
| 6- Secure Systems Management | ۶- مدیریت سیستم‌های امن |
| 7- Information Warfare | ۷- نبرد اطلاعاتی |
| 8- Advanced Topics in Information Security | ۸- مباحث پیشرفته در امنیت اطلاعات |

دروس اختیاری- گروه دو:

(یک درس از دروس زیر در رابطه با نیاز پایان نامه بنا به نظر استاد راهنما اخذ می گردد.)

- | | |
|--|---------------------------------------|
| 1- Introduction to Number Theory | ۱- تئوری اعداد مقدماتی |
| 2- Mathematical Game Theory | ۲- تئوری ریاضی بازی‌ها |
| 3- Information Theory & Coding | ۳- تئوری اطلاعات و کدینگ |
| 4- Bio-Computing | ۴- محاسبات زیستی |
| 5- Software Specification, Test and Maintenance | ۵- مشخصات، آزمایش و نگهداری نرم افزار |
| 6- Advanced Operating Systems | ۶- سیستم عامل پیشرفته |
| ۷- یک درس از دروس کارشناسی ارشد سایر گرایش‌های مهندسی کامپیوتر یا فناوری اطلاعات | |



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

تعریف، اهداف، طول و شکل نظام دوره کارشناسی ارشد فناوری اطلاعات گرایش امنیت اطلاعات

مقدمه:

در اجرای اصول قانون اساسی جمهوری اسلامی ایران، از جمله بند "ب" اصول ۲ و ۱۲ اصل سوم، و ایجاد شرایط تحقق بند ۴ همین اصول و نیز اجرای اصل ۳۰ و بند ۷ اصل ۴۳ و ایجاد شرایط تحقق بندهای ۸ و ۱ این اصل و اصول دیگر و نظر به رشد استفاده صنعتی، تجاری، خدماتی و دولتی از کامپیوتر و لزوم محافظت از اطلاعات ذخیره شده و مبادله شده در سیستم های کامپیوتری و جلوگیری از نفوذ ایدانی به این سیستم ها، پس از بررسی و مطالعه مباحث نظری و عملی معاشناسی و امنیت اطلاعات و فنون امنیت سیستم های کامپیوتری و شبکه های ارتباطی کامپیوتری دوره کارشناسی ارشد فناوری اطلاعات با گرایش «امنیت اطلاعات» تدوین می گردد.

۱. تعریف و اهداف:

دوره کارشناسی ارشد مهندسی فناوری اطلاعات "گرایش امنیت اطلاعات یکی از مجموعه های آموزش عالی در زمینه فنی مهندسی است و در آن ابعاد کلی تأمین امنیت برای سیستم های پردازش اطلاعات مطالعه و بررسی می گردد و هدف از آن تربیت افرادی است که به منظور تأمین امنیت انواع سیستم های اطلاعاتی بتوانند راه حل های کاربردی ارائه دهند و با داشتن تبحر عملی و درک تئوری لازم بتوانند طراحی، پیاده سازی و ارزیابی مفاهیم، تکنیک ها، روش ها و رویه های لازم برای امنیت اطلاعات را عملی سازند. و نیز بتوانند پژوهش های اولیه در این زمینه دانش را انجام داده و سبب ارتقاء دانش و تکنولوژی مربوطه در کشور گردند.

۲. مهارت های دانش آموختگان:

دانش آموختگان این رشته قادر خواهند بود بعنوان کارشناس ارشد راه حل هایی کاربردی بمنظور تأمین امنیت انواع سیستم های اطلاعاتی ارائه دهند. آنها قادرند با توجه به آموخته های خود با رعایت تمامی جوانب علمی، فنی و با توجه به نیازهای جوامع راه حل های بهینه را انتخاب کرده، آنها را به نتیجه برسانند.

۳. طول دوره و شکل نظام:

برنامه درسی دوره برای ۴ نیمسال طرح ریزی شده است و طول آن حداکثر ۳ سال می باشد (طبق مقررات وزارت علوم، تحقیقات و فناوری) و طول هر ترم ۱۶ هفته آموزشی کامل، مدت هر واحد درس نظری ۱۶ ساعت، عملی و آزمایشگاهی و کارگاهی ۴۸ ساعت می باشد.

۴. واحدهای درسی:

تعداد واحدهای درسی این دوره علاوه بر دروس جبرانی برابر ۳۲ واحد بصورت زیر است.

۱- دروس اجباری	۱۸ واحد
۲- دروس اختیاری	۶ واحد
۳- سمینار	۲ واحد
۴- پروژه	۶ واحد
جمع کل واحدها	۳۲ واحد



۵. شرایط پذیرش:

پذیرش در این دوره منوط به موفقیت در آزمون متمرکز ورودی کارشناسی ارشد رشته فناوری اطلاعات و همچنین قبولی در مصاحبه آزمون شفاهی است. فارغ التحصیلان دوره‌های کارشناسی مهندسی فناوری اطلاعات، مهندسی کامپیوتر، مهندسی برق، ریاضی و علوم کامپیوتر می‌توانند در این دوره شرکت کنند. دروس امتحانی جهت ارزیابی در آزمون متمرکز شامل ساختمان‌های گسسته، ساختمان داده‌ها، طراحی الگوریتم، معماری کامپیوتر، اصول طراحی پایگاه داده‌ها، مهندسی نرم افزار، زبان تخصصی، سیستم‌های عامل، شبکه‌های کامپیوتری، هوش مصنوعی، و مبانی فناوری اطلاعات می‌باشد.

۶. برنامه و دروس دوره:

برنامه دوره کارشناسی ارشد فناوری اطلاعات گرایش امنیت اطلاعات شامل ۲۴ واحد درسی از دروس اصلی و اختیاری، ۲ واحد سمینار و ۶ واحد پروژه است. دانشجویان موظفند از بین دروس اختیاری ۶ واحد انتخاب کنند. همچنین لازم است دانشجویان دروس جبرانی تعیین شده را گذرانده باشند.

۶-۱- دروس اصلی

دروس اصلی به گونه‌ای انتخاب شده‌اند که مبانی و اصول لازم برای گرایش امنیت اطلاعات را پوشش دهند و اخذ آنها نسبت به دروس اختیاری دارای اولویت است. این دروس همه ۳ واحدی بوده و در جدول ضمیمه معرفی شده‌اند.

۶-۲- دروس اختیاری

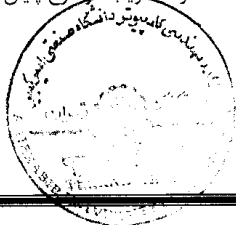
دروس اختیاری، امکاناتی را برای فعالیت تخصصی و تمرکز بیشتر دانشجو در یک زمینه خاص فراهم می‌آورند. این دروس نیز همگی ۳ واحدی می‌باشند و در جدول ضمیمه معرفی شده‌اند. اخذ ۲ درس از این دروس برای دانشجویان الزامی است. دروس اختیاری در دو گروه مطرح شده‌اند. تعداد واحدهای اختیاری ۶ واحد می‌باشد که دانشجو می‌تواند ۲ درس را از گروه یک- اختیاری، یا ۱ درس از گروه یک- اختیاری و ۱ درس از گروه دو- اختیاری (در رابطه با نیاز پایان نامه بنا به نظر استاد راهنما) اخذ نماید.

۶-۳- سمینار

گذراندن درس سمینار برای دانشجویان دوره اجباری است. در این درس دانشجو با انتخاب یک موضوع و یک استاد مشاور پیرامون موضوع خاصی مطالعه و تحقیق بعمل می‌آورد. نتیجه تحقیق دانشجو در این درس بایستی بصورت یک ارائه شفاهی و یک گزارش کتبی ارائه شود.

۶-۴- پروژه تحقیق (پایان نامه)

در این دوره هر دانشجو با انجام یک پایان نامه ۶ واحدی در مورد مسأله خاصی به تحقیق می‌پردازد. موضوع پایان‌نامه الزاماً بایستی در یکی از زمینه‌های مرتبط باشد و زمینه عملی لازم برای انجام آن با دروس اخذ شده توسط دانشجو در این دوره فراهم شده باشد. نحوه تصویب موضوع پایان‌نامه و ارزیابی و دفاع آن مطابق آئین‌نامه‌های تحصیلات تکمیلی می‌باشد.



۷. شرایط اجرایی:

۱-۷- شرایط اجرای این رشته در دانشگاهها

در صورت توانمند بودن در ارائه رشته مهندسی کامپیوتر و دارا بودن قابلیت ها و هیئت علمی متخصص در زمینه های مربوط به امنیت اطلاعات در حد ارائه دوره تحصیلات تکمیلی

۲-۷- امکانات و تجهیزات مورد نیاز

آزمایشگاه های کامپیوتری پیشرفته

۳-۷- تعداد و نوع تخصص اعضای هیأت علمی مورد نیاز

زمینه های گوناگون مهندسی فناوری اطلاعات و امنیت اطلاعات

۴-۷- زمینه تخصصی ورود به گرایش (معلومات ورودیها)

فارغ التحصیلان دوره های کارشناسی مهندسی فناوری اطلاعات، مهندسی کامپیوتر، مهندسی برق، مهندسی صنایع و ریاضی و علوم کامپیوتر

۵-۷- امکانات و شرایط برنامه ریزی و اجرای رشته در این دانشگاه

این دانشگاه با تجهیز امکانات و به راه اندازی مرکز تحقیقات انفورماتیک و بکارگیری هیأت علمی متخصص امکان اجرای این رشته را دارد.



دروس جبرانی

پیشنیاز	ساعت			تعداد واحد	عنوان درس
	عملی	نظری	جمع		
—	—	۴۸	۴۸	۳	۰۱ ساختمان های گسسته
—	—	۴۸	۴۸	۳	۰۲ ساختمان داده ها
—	—	۴۸	۴۸	۳	۰۳ طراحی الگوریتم ها
—	—	۴۸	۴۸	۳	۰۴ مهندسی نرم افزار
—	—	۴۸	۴۸	۳	۰۵ پایگاه داده ها
—	—	۴۸	۴۸	۳	۰۶ سیستم های عامل
—	—	۴۸	۴۸	۳	۰۷ هوش مصنوعی

دروس اصلی (۱۸ واحد)

پیشنیاز	ساعت			تعداد واحد	عنوان درس
	عملی	نظری	جمع		
—	—	۴۸	۴۸	۳	۱ مبانی امنیت اطلاعات
—	—	۴۸	۴۸	۳	۲ معاشناسی کاربردی
شبکه کامپیوتری	—	۴۸	۴۸	۳	۳ امنیت شبکه
سیستم های عامل	—	۴۸	۴۸	۳	۴ سیستمهای کامپیوتری امن
سیستمهای کامپیوتری امن - پایگاه داده ها	—	۴۸	۴۸	۳	۵ امنیت پایگاه داده ها
معاشناسی کاربردی	—	۴۸	۴۸	۳	۶ پروتکل های امنیتی

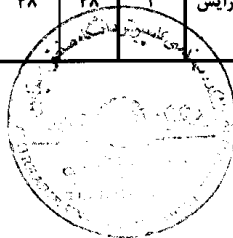


دروس اختیاری - گروه یک

پیشنیاز	ساعت			تعداد واحد	عنوان درس
	عملی	نظری	جمع		
سیستمهای کامپیوتری امن	—	۴۸	۴۸	۳	معماری امنیتی
پروتکل های امنیتی	—	۴۸	۴۸	۳	مدلهای فورمال و امنیت اطلاعات
امنیت شبکه - پروتکل های امنیتی	—	۴۸	۴۸	۳	امنیت تجارت الکترونیک
پردازش سیگنالهای دیجیتال	—	۴۸	۴۸	۳	اختفاء اطلاعات
معماشناسی کاربردی - امنیت شبکه	—	۴۸	۴۸	۳	سیستمهای ارتباطی امن
امنیت شبکه	—	۴۸	۴۸	۳	مدیریت سیستمهای امن
امنیت شبکه	۴۸	۳۲	۸۰	۳	نبرد اطلاعاتی
—	—	۴۸	۴۸	۳	مباحث پیشرفته در امنیت اطلاعات

دروس اختیاری - گروه دو

پیشنیاز	ساعت			تعداد واحد	عنوان درس
	عملی	نظری	جمع		
—	—	۴۸	۴۸	۳	تئوری اعداد مقدماتی
—	—	۴۸	۴۸	۳	تئوری ریاضی بازیها
—	—	۴۸	۴۸	۳	تئوری اطلاعات و کدینگ
—	—	۴۸	۴۸	۳	محاسبات زیستی
—	—	۴۸	۴۸	۳	مشخصات، آزمایش و نگهداری نرم افزار
—	—	۴۸	۴۸	۳	سیستم عامل پیشرفته
—	—	۴۸	۴۸	۳	یک درس از دروس کارشناسی ارشد سایر گرایش های مهندسی کامپیوتر یا فناوری اطلاعات



مبانی امنیت اطلاعات

Information Security Fundamentals

تعداد واحد: ۳ نوع واحد: تعداد ساعت: ۴۸ پیشنیاز: —

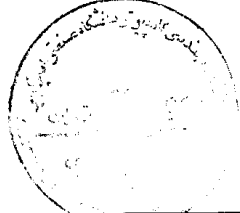
اهداف درس: هدف از این درس تفهیم موضوعاتی است که در تکنولوژی امنیت اطلاعات مطرح می‌شود، بدینصورت که خلاصه نسبتاً جامعی (فراگیری) در مورد موضوعات این زمینه و نیز ارتباط بین زمینه‌ها را به دانشجویان انتقال دهد. بدین منظور در این درس مفاهیم حمله به سیستمهای اطلاعاتی و چگونگی دفاع در مقابل آن مطرح می‌شود.

سرفصل مطالب:

- ۱- تعریف امنیت اطلاعات و فرآیند بودن امنیت
- ۲- تهدیدات به سیستم های کامپیوتری، درخت های تهدید، طبقه بندی حملات، برنامه های مخرب کامپیوتری و ویروس و اسب تروا، روش های متداول حمله
- ۳- سرویس های امنیتی
- ۴- برچسب امنیتی، لاتیس برچسب های امنیتی، رویه امنیتی، مدل افشای اطلاعات BLP و بحث و تحلیل آن
- ۵- امنیت عدم استنتاج و عدم تداخل، مدل صحت Biba، مدل صحت کلارک-ویلسون، ممانعت از سرویس
- ۶- اقدامات مقابله کننده محافظ ایمنی، بازرسی، تشخیص نفوذی، تصدیق اصالت و تشخیص هویت، کلمات عبور، رمزنگاری و مدیریت کلید، کنترل دستیابی، کانال های نهانی، نقش ها و امتیازات، هسته عامل امنیتی
- ۷- امنیت شبکه
- ۸- امنیت پایگاه داده ها
- ۹- ارزیابی امنیتی سیستم ها

مراجع:

- 1- Edward Amoroso, *Fundamentals of Computer Security Technology*, Prentice-Hall, 1994.
- 2- Eric Mainwald, *Network Security: A Beginner's Guide*, Osborne/McGraw-Hill, 2002.
- 3- Charles Pfleeger, *Security in Computing*, Prentice-Hall, 1997.
- 4- Marshall Abrams, et. al. (eds.) *Information Security: An Integrated Collection of Essays*, IEEE Computer Society Press, 1995.
- 5- Peter Denning, *Computers Under Attack*, Addison-Wesley, 1990.



معماشناسی کاربردی

Applied Cryptology

تعداد واحد: ۳ نوع واحد: نظری تعداد ساعت: ۴۸ پیشنهاد: —

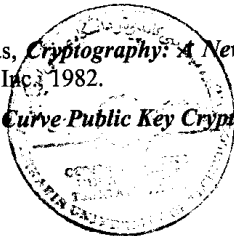
اهداف درس: هدف از این درس ارائه مقدماتی در مورد سرویس های اساسی تأمین امنیت برای محرمانگی، تصدیق اصالت و صحت پیام است. در این درس مکانیزم های حصول آنها و تا حدی نیز پایه ریاضی مربوطه مورد بررسی قرار می گیرد.

سرفصل مطالب:

- ۱- مقدمه (نیاز به سرویس های امنیتی در سیستم های کامپیوتری و ارتباطی و مفاهیم پایه معماشناسی)
- ۲- پیش زمینه های لازم (تئوری اعداد- تئوری اطلاعات- تئوری پیچیدگی)
- ۳- معماشناسی کلاسیک (سیستم های رمز تک الفبائی جانشینی و جایگشتی و تحلیل آنها- سیستم های رمز چندالفبائی و تحلیل آنها)
- ۴- سیستم های رمزنگار مدرن (سیستم های رمزنگاری دنباله ای و قطعه ای، سیستم های رمزنگار متقارن و نامتقارن، معرفی DES و ویژگی های آن، معرفی AES)
- ۵- مقدمه ای بر تحلیل خطی و تحلیل تفاضلی، تحلیل خطی و تحلیل تفاضلی DES
- ۶- رمزنگاری با کلید عمومی (توصیف الگوریتمهای با کلید عمومی KNAPSACK، دیفی هلمن، RSA، رمز ویلیامز، RC5، رمزنگاری منحنی بیضوی و تحلیل آنها)
- ۷- تصدیق اصالت و صحت داده ها (مفاهیم پایه طرح تصدیق اصالت فیات- شامیر، الجمال، ... - مسئله زندانبان و کانال نهران- طرحهای کانال نهران- توابع MAC و HASH و تحلیل آنها و پارادوکس روز تولد)
- ۸- امضای رقمی (انواع پروتکل های امن- مفاهیم پایه امضاء رقمی- طرحهای امضای رقمی ساده- طرح رابین- طرح ماتیاس- امضای RSA و انواع آن و نقاط ضعف- طرح امضای DSS)
- ۹- تبادل کلید و مدیریت کلید (پروتکل های توزیع کلید مبتنی بر سیستم رمز متقارن و نامتقارن- تولید کلید و اعداد random- مدیریت کلید و مدول های امن و کلیدگذاری چندلایه- طرحهای key escrow- دفترچه راهنمای کلید عمومی- گواهی و قبولی گواهی- مدیریت گواهی ها- PKI)

مراجع:

- 1- B. Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C*, John-Wiley & Sons Inc., 1996.
- 2- J. Seberry and J. Pieprzyk, *Cryptography: An Introduction to Computer Security*, Prentice-Hall, 1992.
- 3- C. Meyer, S. Metyas, *Cryptography: A New Dimension in Computer Data Security*, John-Wiley & Sons Inc., 1982.
- 4- A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers.





امنیت شبکه

Network Security

تعداد واحد: ۳ نوع واحد: نظری تعداد ساعت: ۴۸ پیشیناز: شبکه کامپیوتری

اهداف درس: هدف از این درس ارائه مباحث مختلف امنیتی برای سیستم‌های کامپیوتری شبکه شده است. در این درس اهداف محرمانگی، صحت و دسترس‌پذیری برای شبکه‌های کامپیوتری مورد بررسی قرار گرفته و سرویس‌هایی که می‌توانند این اهداف را برآورده کنند ارائه می‌شود. همچنین معماریهای امنیتی شبکه، شامل PKI، و بکارگیری سرویس‌های دایرکتوری و کنترل دستیابی در شبکه‌ها مورد مطالعه قرار می‌گیرد.

سرفصل مطالب:

- ۱- مقدمه ای بر شبکه سازی و امنیت کامپیوتر
- ۲- تهدیدات امنیتی، حملات مسیردهی، ردگیری
- ۳- محرمانگی ترافیک
- ۴- مروری بر رمزنگاری، معماریهای امنیتی PKI، سرویس دایرکتوری X.509 و KERBEROS
- ۵- امنیت لایه دسترسی به شبکه، سرویس های امنیتی ATM، پروتکل های EAP, CHAP, PAP, PPP, L2TP و پروتکل ECP
- ۶- امنیت لایه اینترنت، فیلترهای بسته، NAT, IPsec, VPN، فایروال و اصول طراحی آن، سیستمهای مطمئن
- ۷- امنیت لایه حمل، Socks V5, SASL, ISAKMP
- ۸- امنیت لایه کاربرد، فیلترهای محتوی، مجوز دادن و کنترل دستیابی، شبکه ارتباطی و تهدیدات امنیتی و برنامه مخرب (ویروس، کرم و اسب تروا)، امنیت نامه الکترونیک e-mail, PGP, S/MIME، امنیت Web, SET, SSL، امنیت Java، امنیت مدیریت شبکه و SNMP
- ۹- نفوذگراها، نفوذ، حملات ممانعت از سرویس، سیستم های تشخیص نفوذ
- ۱۰- مونیترینگ و RMON

مراجع:

- 1- William Stallings, *Network Security Essentials: Application and Standards*, Prentice-Hall, 2000.
- 2- S. Ghosh, *Principles of Secure Network Systems Design*, Springer-Verlag, 2002.
- 3- Eric Mainwald, *Network Security: A Beginner's Guide*, Osborne/McGraw-Hill, 2002.
- 4- William Stallings, *Cryptography and Network Security: Principles and Practice*, Prentice- Hall, 1998.
- 5- E. Fisch, G. White, *Secure Computers and Networks*, CRC Press, 2000.
- 6- N. Doraswamy, D. Harkins, *IP Sec: The New Security Standard for the internet, intranets, and Virtual Private Network*, Prentice- Hall, 1999.
- 7- W. Cheswick, Steven M. Bellovin, *Firewalls and Internet Security*, Addison-Wesley, 1994.

-
- 8- D. Marchette, *Computer Intrusion Detection and Network Monitoring*, Springer-Verlag, 2001.
 - 9- Vesna Hessler, *Communication Security*, Part2 of Security Fundamentals for E-Commerce, Artech House Publishers.





سیستم های کامپیوتری امن

Secure Computer Systems

تعداد واحد: ۳ نوع واحد: نظری تعداد ساعت: ۴۸ پیشنیاز: سیستم های عامل

اهداف درس: از آنجا که برنامه های کاربردی توسط سیستم های نرم افزاری مانند سیستم های عامل عمل می کنند، اجرای امن چنین برنامه های کاربردی وابسته به آنست که چه اطمینان هایی در مورد سیستم های عامل یا سیستم های نرم افزاری زیرین مفروض است. در این درس پیاده سازی حفاظت برای سیستم های نرم افزاری کامپیوتری یکپارچه و توزیع شده مورد بررسی قرار می گیرد، و اهمیت معماری سیستم در مورد متدولوژی های بررسی اطمینان ها برای هسته های امنیتی مورد توجه قرار می گیرد.

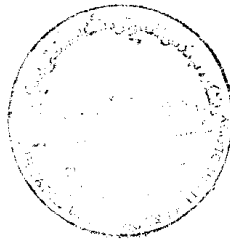
سرفصل مطالب:

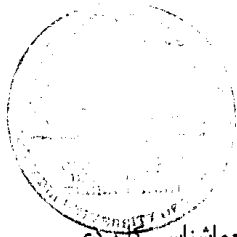
- ۱- اطمینان در فضای اطلاعات، مفروضات امنیت در سیستم های کامپیوتری مدرن و ناچاری از خطا
- ۲- اصول طراحی سیستم های امن (حفاظت از اطلاعات در سیستم های کامپیوتری، سخت افزار Segmentation برای محافظت فضای آدرس درونی)
- ۳- تصدیق اصالت (کلمات عبور، کارت های محافظت شده با PIN، کلمات عبور یکبارگی، بیومتریک، امنیت کلمه عبور، امنیت کلمه عبور یونیکس، تحکیم کلمه عبور با حرکات ضربه به کلید)
- ۴- کنترل دستیابی و مجوز (کنترل دستیابی تفویضی - لیست های کنترل دستیابی و قابلیت ها، پیاده سازی کنترل دستیابی (Java, Unix, Multics) قابلیت ها در Hydra، لغو، بهبود درشت دانگی کنترل دستیابی در Windows NT - کنترل دستیابی دستوری، مدل های کنترل دستیابی دستوری و پیاده سازی هایشان، مدل Bell-Lapadula، کنترل خط مشی روی عملیات اشیاء، کنترل دستیابی مبتنی بر نقش - کنترل جریان اطلاعات، یک مدل توزیع شده برای جریان اطلاعات، خط مشی امنیتی دیوار چین و مدل کلارک- ویلسون)
- ۵- کانال نمان (مسئله زندان - تحلیل کانال نمان، اسب تروا)
- ۶- هسته های امنیتی (طراحی و پیاده سازی هسته امنیتی)
- ۷- امنیت سیستم های توزیع شده (تصدیق اصالت و کنترل دستیابی در سیستم های توزیع شده، کنترل دستیابی در محیط توزیع شده باز، جداسازی مدیریت کلید از امنیت سیستم فایل)

مراجع:

- 1- Morrie Gasser, *Building a Secure Computer System*, Van Nostrand Reinhold Company, New York, ISBN: 0-442-23022-2, 1988.
- 2- Jerome H. Saltzer, Michael D. Schroeder, *The Protection of Computer Systems*, IEEE Tutorial Paper, /www.ecl.cs.sunysb.edu/
- 3- M. Gasser, A. Goldstein, C. Kaufmann, B. Lampson, *The Digital Distributed System Security Architecture*, in 12th National Computer Security conference (NIST/NCSC), Battimore, 1989.
- 4- M. Zeleznik, *Security Design in Distributed Computing Applications*, /citesecr.nj.nec.com/zeleznik93security.html

-
- 5- E. Fisch, G. White, *Secure computers and Networks*, CRC Press, 2000.
 - 6- P. Gutmann, *The Design and Verification of a Cryptographic Security Architecture*, Springer-Verlag, 2002.
 - 7- S. Ames, M. Gasser, R. Shell, *Security Kernel Design and Implementation: An Introduction*, IEEE Computer, Vol. 16, No. 1, 1983.
 - 8- M. Harrison, W. Ruzzo, J. Ullman, *Protection in Operating Systems*, Communications of the ACM, Vol. 19, No. 8, 1976.
 - 9- P. Denning, *Fault Tolerant Operating Systems*, Computer Surveys, V. 8, n. 4, 1976.





پروتکل‌های امنیتی

Security Protocols

تعداد واحد: ۳ نوع واحد: نظری تعداد ساعت: ۴۸ پیشنهاد: معماشناسی کاربردی

اهداف درس: در این درس پروتکل‌های امنیتی مختلف توصیف شده، همچنین حملات و دفاع‌های مختلف در مقابل آنها مطرح می‌گردد. پروتکل‌های مختلف مانند پروتکل‌های تصدیق اصالت و امضاء، مدیریت حقوق دیجیتال، پروتکل‌های امنیتی در شبکه‌های توزیع شده، بدون سیم و با سیم، رأی‌گیری الکترونیک، پروتکل‌های پرداخت الکترونیک، تکنیک‌های رمزنگاری بصری در این درس مورد توجه هستند.

سرفصل مطالب:

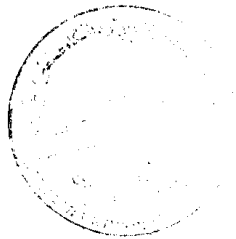
- ۱- مقدمه (پروتکل، پروتکل‌های امن و انواع آن، کلاس‌های حملات به پروتکل‌های امن و مدل‌های امنیتی، امضا و تصدیق اصالت و هویت، پروتکل‌ها و مکانیزم‌ها، مدیریت و برقراری کلید و گواهی)
- ۲- بلوک‌های سازنده پروتکل (تعریف پروتکل، ارتباط با استفاده از رمزنگاری متقارن، توابع یکطرفه، ارتباط با استفاده از رمزنگار نامتقارن، امضاهای رقمی، چهارچوبی برای مکانیزم‌های امضای رقمی، RSA و طرح‌های امضای مربوطه، طرح امضای فیات-شامیر، DSA و طرح‌های امضای مربوطه، طرح‌های امضای رقمی یکبارمصرف، طرح‌های امضای رقمی حکم دار، طرح‌های امضای رقمی کور، طرح‌های امضای رقمی غیرقابل انکار، طرح‌های امضای رد-توقف)
- ۳- پروتکل‌های ساده (پروتکل‌های مبادله کلید، پروتکل‌های تصدیق اصالت، پروتکل‌های تصدیق اصالت و مبادله کلید، تحلیل فورمال پروتکل‌های مبادله کلید و تصدیق اصالت، رمزنگاری با کلید عمومی چندگانه، تقسیم راز، اشتراک راز، محافظت رمزنگارانه از پایگاه داده‌ها)
- ۴- پروتکل‌های متوسط (سرویس‌های مهر زمانی، کانال نمان، امضای رقمی غیرقابل انکار، امضای با تأیید کننده مشخص، امضای نیابتی، امضاهای گروهی، محاسبه با اطلاعات رمز شده، طرح‌های Bit Commitment، طرح‌های سکه اندازی عادلانه، پوکر ذهنی، جمع‌کننده‌های یک طرفه، افشای همه یا هیچ رازها، KEY (ESKROW)
- ۵- پروتکل‌های پیشرفته (اثبات‌های صفر-دانش، اثبات صفر-دانش هویت، امضاهای کور، رمزنگاری کلید عمومی مبتنی بر هویت، انتقال بی‌خبر، امضاهای بی‌خبر، امضای قرارداد توامان، نامه دیجیتال سفارشی، مبادله همزمان رازها)
- ۶- پروتکل‌های خاص (انتخابات امن، محاسبات چندطرفه امن، پخش بدون-نام پیام، اسکنااس دیجیتال)
- ۷- مدیریت کلید (تولید کلید، فضای غیرخطی کلید، انتقال کلید، تأیید کلید، استفاده از کلید، ذخیره کلید، تازه کردن کلید، عمر کلید، از بین بردن کلید، مدیریت کلیدهای عمومی)
- ۸- الگوریتم‌های امضای رقمی با کلید عمومی
- ۹- طرح‌های تشخیص هویت
- ۱۰- الگوریتم‌های مبادله کلید (طرح دیفی-هلمن، پروتکل‌های ایستگاه به ایستگاه، پروتکل سه دوره شامیر،

مبادله کلید رمز شده، مذاکره کلید محافظت شده، توزیع کلید کنفرانس و پخش راز)

(۱- الگوریتمهای خاص برای پروتکلها

مراجع:

- 1- B. Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C*, John Wiley and Sons Inc., 1996.
- 2- A. Menezes, et. al., *Handbook of Applied Cryptography*, CRC Press, 1996.
- 3- A. Beutelspacher et. al., *Modern Topics in Cryptography*, in German, Vieweg, 1995.
- 4- P. Ryan, S. Schneider, M. Goldsmith, G. Lowe and B. Roscoe, *Modelling and Analysis of Security Protocols*, Addison-Wesley, 2001.



امنیت پایگاه داده ها

Database Security

تعداد واحد: ۳ نوع واحد: نظری تعداد ساعت: ۴۸ پیشنهاد: سیستم های کامپیوتری امن - پایگاه داده ها

اهداف درس: این درس دربرگیرنده نکات منطقی در رابطه با امنیت پایگاه داده ها است. رویه های صحت و محرمانگی اطلاعات در زمینه سیستم های پایگاه داده ها مرور گشته، و مدل سازی سیستم های پایگاه داده ها همراه با نکات پیاده سازی مانند serialization, atomicity و کنترل مبتنی بر دیدگاه مطرح می شود. همچنین مسائلی مانند نپذیری (releasability) در طراحی پایگاه داده امن، امنیت در پایگاه داده های آماری، رویکردهای امنیت برای پایگاه داده های شی گرا، و جمع آوری و استفاده از پایگاه داده های بازرسی همراه با تشخیص نفوذ مطرح می گردد.

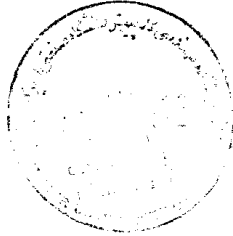
سرفصل مطالب:

- ۱- مقدمه ای بر پایگاه داده ها (مفاهیم یک پایگاه داده، اجزاء یک پایگاه داده، پرسش (query)، مزایای استفاده)
- ۲- خواسته های امنیتی (یکپارچگی پایگاه داده و صحت امان ها، قابلیت بازرسی، کنترل دستیابی، تصدیق اصالت کاربر، دسترسی پذیری، قابلیت اعتماد (reliability))
- ۳- اطلاعات حساس (عوامل حساس سازی، تصمیم های مختلف در مورد دسترسی، دسترس پذیری داده ها، اطمینان از اصالت، انواع افشاء شدن، امنیت و دقت)
- ۴- مسئله استنتاج
- ۵- کنترل دستیابی تفویضی در DBMS ها
- ۶- کنترل دستیابی دستوری
- ۷- کانال های نهان
- ۸- مدل رابطه ای امن چندسطحی
- ۹- معماری DBMS امن چندسطحی
- ۱۰- محصولات تجاری و پروتوتایپ های تحقیقاتی
- ۱۱- ارزیابی و تعبیر پایگاه داده مطمئن
- ۱۲- مکانیزم ها و مدل های صحت
- ۱۳- امنیت در پایگاه داده آماری
- ۱۴- بازرسی در پایگاه داده رابطه ای
- ۱۵- امنیت Oracle9i
- ۱۶- تشخیص نفوذ و Data Mining
- ۱۷- بقاء پایگاه داده ها در نبردهای اطلاعاتی
- ۱۸- خط مشی های اعمال کنترل دستیابی چندگانه



مراجع:

- 1- M. Abrams, S. Jajodia, H. Podell (eds.) *Information Security: An Integrated Collection of Essays*, IEEE Computer Society Press, 1995.
- 2- E. Fernandez, et.al., *Database Security and Integrity*, Addison-Wesley, 1981.
- 3- C. Date, *An Introduction to Data Base Systems*, Vol.1, and Vol. 2, Addison-Wesley.
- 4- D. Denning, *Cryptography and Data Security*, Addison-Wesley, 1982.
- 5- C. Pfleeger, *Security in Computing*, Prentice-Hall, 1997.
- 6- D. Denning, *A Review of Research on Statistical Data Base Security*, Foundations of Secure Computation, Academic Press, 1978.
- 7- D. Denning, *Views for Multi-level Data base Security*, IEEE Trans. Software Eng., 1987.
- 8- P. Ammann, S. Jajodia, C. McCollcom, B. Blaustein, *Surviving information Warfare attacks on Databases*, Proc. IEEE Symposium on Research in Security and Privacy, 1997.
- 9- *Oracle White Paper: Oracle 9i Database Security for e Business*.
- 10- N. Adam and J. Wortmann, *Security- control methods for statistical databases*, ACM Computing Surveys, Vol. 21, No. 4, 1989.
- 11- D. Clark, D. Wilson, *A Comparison of Commercial and Military Computer Security Policies*, Proceedings of the IEEE Symposium on Security and Privacy, 1987.
- 12- M. Theriault and A. Near man, *Oracle Security Handbook*, Osborne/McGraw-Hill, 2001.



نبرد اطلاعاتی

Information Warfare

تعداد واحد: ۳ نوع واحد: نظری - عملی تعداد ساعت: ۳۲ + ۴۸ پیشیاز: امنیت شبکه

اهداف درس: این درس از دو بخش نظری و عملی تشکیل می شود. ابتدا از بعد مدیریتی مفهوم نبرد اطلاعاتی، ابعاد آن و اقدامات مختلفی که در این موضوع مطرح می گردد تعریف و مطالعه می گردد. سپس از بعد فنی تجربیات درباره نصب، پیکره بندی و تست سخت افزارها و نرم افزارهای امنیتی آفندی و پدافندی مطرح می شود.

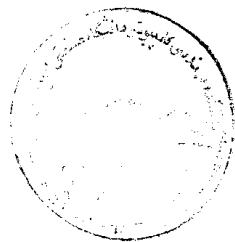
سرفصل مطالب:

الف- بعد مدیریتی:

- ۱- نظریه نبرد اطلاعاتی (منابع اطلاعاتی، نقش ها، نبرد اطلاعاتی آفندی، نبرد اطلاعاتی پدافندی، بازی، جرم، حقوق افراد، امنیت ملی)
- ۲- نبرد اطلاعاتی آفندی (منابع باز و دزدی اطلاعات، مدیریت وجهه، خائنین درونی، استراق سمع سیگنال ها، آنالیز ترافیک، جعل ارتباطی، مونتورینگ شبکه، نظارت محیط، خرابکاری، رخنه گری و ورود به کامپیوترها، ظاهر سازی، برنامه های مخرب)
- ۳- نبرد اطلاعاتی پدافندی (اختفاء و سری کردن، تصدیق اصالت و علامتگذاری Watermark، مونتورینگ و فیلتر کردن، تشخیص نفوذ و سوء استفاده، مونتور کردن نقاط ضربه پذیر، آموزش و آگاهی امنیتی، مدیریت مخاطره، مدیریت وقایع)
- ۴- امنیت زیرساختارهای بحرانی (اصول پذیرفته شده امنیت سیستمها، نظریه سیستمهای پیچیده، سیستم های پیچیده تطبیق پذیر، زیرساخت های بحرانی کشور و ارتباط آنها با یکدیگر، خط مشی رمزنگاری کشوری)

ب- بعد فنی:

- رفتار در رابطه با کامپیوتر
- پروتکل های شبکه
- حملات ترافیک و دفاع
- حملات تصدیق اصالت و دفاع
- حملات e-mail و دفاع
- سرویس های ترمینال، NFS، و X-Windows
- Web
- تشخیص نفوذ
- فایروال
- Screening router
- رمزنگاری اتصال



- گیرانداختن رخنه کار

- نرم افزار Probe

- مدیریت امنیت

مراجع:

- 1- D. E. Denning, *Information Warfare and Security*, Addison-Wesley, 1999.
- 2- *Maximum Security*, Sam Publishing, 1998.
- 3- S. McClure, J. Scambray, and G. Kurtz, *Hacking Exposed: Network Security Secrets & Solutions*, 3ed., McGraw-Hill/Osborne, 2001.





مدل های فورمال و امنیت اطلاعات

Formal Models and Information Security

تعداد واحد: ۳ نوع واحد: نظری تعداد ساعت: ۴۸ پیشنهاد: پروتکل های امنیتی

اهداف درس: در این درس تکنیکهای پایه برای مدل کردن و تحلیل رسمی سیستمهای کامپیوتری مطرح می گردد و توجه کاربرد برای موارد اطمینان اطلاعات (Information Assurance)، رویه امنیتی (Security Policy) و پروتکل های امنیتی (Security Protocols) است. در این درس پس از یادگیری مبانی منطق کلاسیک، استقراء و تکرار، نحو برنامه، بازنویسی، سیستم های راکتیو، منطق زمانی، چک کردن مدل و انتزاع، از این روش ها برای تحقیق درستی نرم افزار و سخت افزار و پروتکل های امنیتی استفاده می کنیم.

همچنین در این درس روش های فورمال ریاضی برای مشخص کردن و مدل کردن و تحقیق صحت سیستم های با کنترل دستیابی مطالعه می گردد. جنبه های ریاضی این مدل ها شناسائی و تحلیل می گردد. مدل های فورمال و غیر فورمال رویه امنیتی بحث می گردد. و چندین مدل کنترل دستیابی و درستی شان بررسی می شود.

سرفصل مطالب:

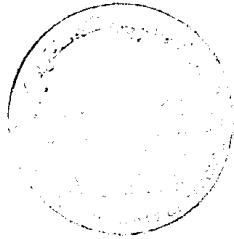
- نظریه مجموعه ها و منطق (رابطه ها و مجموعه های مرتب، استقراء و تکرار، منطق first-order و مدل ها و Completeness و Soundness)
- مکانیزاسیون منطق (محاسبه اثبات، نظریه سیستم های بازنویسی، مراحل تصمیم و منطق گزاره ای)
- ACL2 (منطق ACL2، زبان برنامه نویسی ACL2، مکانیزاسیون ACL2، مدلسازی با زبان برنامه نویسی ACL2، مثال هائی از سخت افزار، نرم افزار و پروتکل های امنیتی)
- سیستم های راکتیو (مقایسه سیستم راکتیو با تبدیلی، Safety & Liveness، منطق زمانی، model checking، انتزاع، ترکیب Theorem Proving و model checking، تقارن، عدم وابستگی داده ها، سیستم های پارامتری شده)
- مدلسازی پروتکل های امنیتی و ابزارهای مربوطه (معرفی CSP، مدل کردن پروتکل های امنیتی در CSP، بیان اهداف پروتکل، معرفی FDR، Casper، نوشتن پروتکل ها و نفوذگرها برای FDR، اثبات قشیه، تبدیل های ساده ساز، رویکردهای دیگر مانند منطق BAN، تحلیلگر NRL، رویکرد B-method، رویکرد استقرائی، رویکرد عدم تداخل)
- رویه امنیتی (رویه محرمانگی، رویه صحت، رویه های دورگه، رویه نویسی، مدل جریان اطلاعات، مدل ماتریس دستیابی، مدل Bell-Lapadula، مدل های مبتنی بر lattice، عدم تداخل و عدم استنتاج، مدل های صحت مانند Biba و کلارک-ویلسون، مدل های n-tree برای مجوزدهی گروهی)

مراجع:

- 1- M. Kaufmann, P. Manolios and J. S. Moore, *Computer Aided Reasoning: An Approach*, Kluwer Academic Publishers, 2000.

2- P. Ryan, S. Schneider, M. Goldsmith, G. Lowe and B. Roscoe, *Modelling and Analysis of Security Protocols*, Addison-Wesley, 2001.

3- M. Bishop, *Computer Security: Art and Science*, Addison-Wesley.





امنیت تجارت الکترونیک

E-commerce Security

تعداد واحد: ۳ نوع واحد: نظری تعداد ساعت: ۴۸ پیشیاز: امنیت شبکه و پروتکل‌های امنیتی

اهداف درس: با توجه به اهمیت چشمگیر امنیت برای تجارت الکترونیک، در این درس درکی عمیق از مسائل امنیتی مربوط به تجارت الکترونیک و راه حل‌های مربوطه فراهم می‌گردد. در این درس مسائل متنوع مطرح، از طراحی Secure Web و کاربردهای Secure Mobile Commerce گرفته تا امنیت درونی شبکه، تا امنیت کارمندان و تصدیق اصالت آنها مطرح می‌شود.

سرفصل مطالب:

- امنیت اطلاعات (مقدمه ای بر تهدیدات امنیتی و مدیریت مخاطره، مکانیزم‌های امنیتی، مدیریت کلید و گواهی‌ها)
- سیستم‌های پرداخت الکترونیک (تجارت الکترونیک، سیستم‌های پرداخت الکترونیک و سرویس‌های مختلف مربوطه، B2B, home-banking, ابزارهای پرداخت، کیف پول الکترونیک، کارت‌های هوشمند، امنیت پرداخت الکترونیک)
- سرویس‌های امنیتی پرداخت (معرفی مفاهیم سرویس‌های امنیتی و امنیت عملیات پرداخت، امنیت پول دیجیتال، امنیت چک الکترونیک، دسترس پذیری و قابلیت اعتماد)
- امنیت عملیات پرداخت (بی‌نامی کاربر و عدم قابلیت ردگیری مکان، بی‌نامی پرداخت کننده، شبه نام‌ها، عدم ردگیری عملیات پرداخت، محرمانگی داده‌های عملیات پرداخت، عدم انکار پیام‌های عملیات پرداخت، تازگی پیام‌های عملیات پرداخت)
- امنیت پول دیجیتال (عدم ردگیری عملیات پرداخت، محافظت در مقابل صرف کردن دوباره، امنیت در مقابل جعل سکه‌ها، امنیت در مقابل سرقت سکه‌ها)
- امنیت چک الکترونیک
- پروتکل IOTP (Internet Open Trading Protocol) و موضوعات امنیتی مربوطه
- امنیت web (پروتکل HTTP، امنیت سرویس گیر web، امنیت سرویس گیر web، امنیت کدهای متحرک، نکات تجارت الکترونیک مبتنی بر web، سیستم‌های Java Commerce, micro payment)
- امنیت عامل‌های متحرک (معرفی عامل‌های متحرک و موضوعات امنیتی مربوطه، محافظت platform از عامل‌های متخاصم، محافظت عامل‌ها از platform متخاصم)
- امنیت تجارت متحرک (مروری بر تکنولوژی، امنیت GSM، پروتکل WAP و WTLS و موضوعات امنیتی WML، محیط اجرای ایستگاه متحرک (MEXE))
- امنیت کارت‌های هوشمند (امنیت سخت افزار، امنیت سیستم عامل کارت، Java Card, SIM Card, بیومتریک)

مراجع:

- 1- Vesna Hessler, *Security Fundamentals for E-Commerce*, Artech House Publishers.
- 2- Jon C. Graff, *Cryptography and E-Commerce*, John-Wiley & Sons Inc.
- 3- C. Sexton, *E-Commerce and Security*, Digital Press.
- 4- A. Ghosh, *E-Commerce Security: Weak Links, Practical Solution*, John-Wiley & Sons Inc.
- 5- A. Sechrouchni and M. H. Sherif, *Protocols for Secure Electronic Commerce*, CRC Press.
- 6- M. Hendry, *Smart Card Security and Application*, Artech House Inc., 2001.





مدیریت سیستم های امن

Secure Systems Management

نوع واحد: نظری تعداد ساعت: ۴۸ پیشنیاز: امنیت شبکه

اهداف درس: هدف از این درس اینست که درکی در مورد ملاحظات امنیتی در رابطه با مدیریت سیستم های اطلاعاتی مبتنی بر کامپیوتر برای دانشجویان فراهم آورد. از اینرو اعمال امنیتی که لازم است تا یک سیستم امن را از لحاظ عملیاتی امن نگهدارند مطالعه می گردد. این زمینه شامل موضوعاتی از قبیل مدیریت مخاطرات، اعتباردهی و گواهی است. همچنین ملاحظات عملیاتی مانند گزارش دهی اعلام های خطر، بازرسی و مدیریت کلیدهای رمزنگاری را شامل می گردد.

سرفصل مطالب:

- مدیریت پیکره بندی و امنیت سیستم، اعتباردهی و گواهی دهی
- مدیریت مخاطرات امنیتی
- مدیریت امنیت (شناسایی اجزاء تحت مدیریت، خط مشی امنیتی سازمان، خط مشی امنیتی و نرم افزارهای مورد اطمینان، اطلاعات و سیستم های پردازش اطلاعات، زیرساخت امنیتی سازمان، سرویس ها و مکانیزمهای امنیتی، طبقه بندی داده ها و کنترل دسترسی، امنیت پرسنل، امنیت فیزیکی و محیطی، مدیریت ارتباطات و عملیات، نگهداری و ایجاد سیستم ها، مدیریت تداوم کار، بازیابی از فجایع طبیعی، استانداردها)
- جنبه های قانونی امنیت
- مدیریت کلید و توافقات امنیتی
- بازرسی امنیتی
- گزارش دهی اعلام خطرهای امنیتی
- مدیریت امنیت در سیستم های main frame و شبکه

مراجع:

- 1- NIST, *Guideline for computer Security Certification and Accreditation*, FIPS PUB 102, 1983.
- 2- NIST, *Guideline for the Analysis of Local Area Network Security*, FIPS PUB 191, 1994.
- 3- NIST, *Guidelines for Automatic Data Processing Physical Security and Risk Management*, FIPS PUB 31, 1974.
- 4- ISO/IEC, *Management Plan for Security*, JTC1/SC21 SD-1.
- 5- ISO, *OSI Basic Reference Model, Part2: Security Architecture*, 7498-2, 1989.
- 6- ISO/IEC, *OSI Systems Management, Part7: Security Alarm Reporting Function*, 10164-7, 1992.

-
- 7- ISO/IEC, *OSI Systems Management, Part8: Security Audit Trail Function*, 10164-8, 1993.
 - 8- ISO/IEC, *OSI Systems Management, Part 9: Objects and Attribute for Access Control*, 10164-9, 1995.
 - 9- ISO/IEC, *OSI Security Frameworks for Open Systems, Part8: Key Management*, 10181-8.
 - 10- IETF, *Internet Security Association and Key Management Protocol (ISAKMP)*, 1997.
 - 11- A. Blyth, and G. L. Kovacich, *Information Assurance*, Springer-Verlag, 2001.





معماری امنیتی

Security Architecture: Design & Analysis

تعداد واحد: ۳ نوع واحد: نظری تعداد ساعت: ۴۸ پیشنهاد: سیستم‌های کامپیوتری امن

اهداف درس: رشد فزاینده وابستگی به سیستم‌های بزرگ، توزیع شده و شبکه، عواقب نفوذ و رخنه در سیستم را با اهمیت می‌کند. از اینرو در معماری سیستم‌ها بایستی توانائی‌های امنیتی که با این تهدیدات مقابله کند لحاظ گردد. در این درس مطالب لازم برای طراحی و تحلیل سیستم‌های امن و بقاءپذیر فراهم می‌گردد.

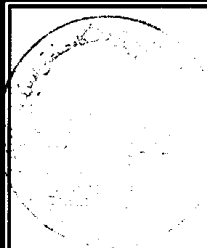
سرفصل مطالب:

- ۱- خط مشی‌های امنیتی (انواع مختلف رویه‌ها، ایجاد رویه‌ها، طبقه بندی اطلاعات و طرح مراقبت دستیابی)
- ۲- استخراج نیازها از رویه (تهدیدات، نیازهای امنیتی- مدیریتی، نیازهای امنیتی- عملیاتی، نیازهای امنیتی- فنی)
- ۳- اصول طراحی زیرساخت امنیتی (اجزاء زیرساخت، اهداف زیرساخت امنیتی، چهارچوب راهنمای طرح مانند موارد تصدیق اصالت و مجوز دادن و حسابرسی، مراقبت دستیابی‌های فیزیکی و منطقی، معماری امنیتی ISO)
- ۴- افراز کردن شبکه (مبناهای (platform) فایروالی، تشریح اجزاء فایروال، استراتژی فایروالی، متدها و مدل افراز کردن، مدل‌های امنیت سرورها، متدها و مدل‌های افراز کردن داخلی، VPN ها شامل انواع VPN، ویژگیهای VPN، تکنولوژی VPN)
- ۵- امنیت Wireless (تفاوت امنیت در Blue tooth، wireless، امنیت آن، WAP و امنیت آن، WLAN ها و امنیت آن)
- ۶- استحکام مبنای (platform) سیستم (نیازهای منابع، هزینه و مورد کار، تشریح اجزاء مبنای، رویکرد برای استحکام مبنای، رهنمودهای عملی برای استحکام، ابزارهای استحکام سازی، سیستمهای تشخیص نفوذ)
- ۷- امنیت کاربرد (جایگاه امنیت کاربرد، مدل‌های مجوز دادن، منابع محافظت شده، امنیت نامرئی کاربرد (مورد web)، مخزن امنیتی WAC، جریان امنیتی WAC)
- ۸- PKI (گواهی‌های دیجیتال، اجزای PKI، معماری‌های PKI و خط مشی برای گواهی)
- ۹- مدیریت رویدادهای امنیتی و مدیریت امنیت (پروتکل‌های رویدادها، جمع‌آوری و طبقه بندی رویدادها، مدیریت امنیت، بهترین اعمال برای مدیریت زیرساخت امنیت)
- ۱۰- تعیین اعتبار (تهدیدات- متدولوژی ارزیابی امنیت)
- ۱۱- امنیت و بقاءپذیری سیستم (اصول معماری سیستم، روشهای بقاءپذیری و امنیت، ایجاد سیستم‌های بقاءپذیر و امن، تحلیل معماری و موازنه مزایا- نواقص، تحلیل بقاءپذیری سیستم برای عملکردهای بحرانی مأموریت، روش تحلیل شبکه بقاءپذیر، پیاده سازی معماری امنیتی)

مراجع:

- 1- Christopher King, Curtis Dalton and Ertem Osmanoglu, *Security Architecture: Design, Deployments and Operations*, Osborne-McGraw-Hill, 2001.

-
- 2- Knight, Sullivan, Elder, Wang, *Survivability Architectures: Issues and Approaches*, 2000.
 - 3- C. Salter, O. Saydjari, B. Schneier, and J. Walner, *Toward a Secure System Engineering Methodology*, Proceedings of New Security Paradigms Workshop 1998.
 - 4- J. Sherwood, A. Clarke, and D. Lignas, *Security Architecture: How to Build and Run a Secure Enterprise Network*, Addison-Wesley Professional.



سیستم های ارتباطی امن

Secure Communications Systems

تعداد واحد: ۳ نوع واحد: نظری تعداد ساعت: ۴۸ پیشنهاد: معماشناسی کاربردی- امنیت شبکه

اهداف درس: در این درس امنیت سیستم های ارتباطی و چگونگی بکارگیری رمزنگاری برای تأمین امنیت در این سیستم ها مورد بحث قرار می گیرد. بدین منظور جنبه های فنی امنیت و نیز کاربردها و مسائل خاص شان مطالعه می گردند.

سرفصل مطالب:

- ۱- تهدیدات و راه حل ها (تهدیدات فنی به امنیت ارتباطات، تداخل، jamming، تشخیص توسط دشمن، استخراج اطلاعات از روی شکل موج، تصدیق اصالت، صحت، دسترس پذیری، مقابله با تهدیدات تشعشعی)
- ۲- امنیت صوت در کاربردهای نظامی (رمزنگاری آنالوگ برای ارتباطات رادیویی HF برد بلند دریائی، واحد رمزنگاری دیجیتال در عملیات زمینی، مدول رمزنگاری رادیویی)
- ۳- امنیت تلفن (تهدیدات خاص برای تلفن، تکنولوژی های شبکه، راه حل های امنیت تلفن، مدیریت دستیابی و کلید، پیاده سازی شبکه، توزیع کلید)
- ۴- سیستم های GSM امن (معماری پایه GSM، ویژگی های امنیتی GSM استاندارد، جنبه های امنیت خاص برای کاربران GSM، مدیریت کلید و ابزارها، عملیات و امنیت GPRS)
- ۵- امنیت در شبکه های رادیویی VHF/UHF خصوصی (کاربری و ویژگیها، تهدیدات، اقدامات مقابله، معماری و طراحی شبکه ارتباطی، اجزاء سخت افزاری، مدیریت کلید، بعضی ویژگیهای امنیتی خاص مانند حذف کلید از دوردست، انسداد از راه دور، و ردگیری ساکت)
- ۶- اقدامات حفاظت الکترونیک- خیزش فرکانسی frequency Hopping (EPM, EA, ESM), کاربردهای نظامی، معماری شبکه، مراحل مأموریت، مشخصه های فرکانسی شبکه های خیزش COMSEC و TRANSEC، ابزارها و مدیریت داده ها و کلید، اجزاء سخت افزاری)
- ۷- رمزنگاری Link (تکنولوژی پایه رمزنگاری Link، پروسه رمزنگاری، پارامترهای رمزنگاری، مدیریت شبکه، امنیت Link نظامی)
- ۸- سیستم های امن (شبکه های فکسیمیلی امن، امنیت PC، امنیت E-mail، شبکه اختصاصی مجازی امن، انتقال داده های نظامی)

مراجع:

- 1- R. V. Sutton, *Secure Communications: Applications and Management*, John-Wiley & Sons Inc., 2002.
- 2- D. J. Torrieri, *Principles of Secure Communication Systems*, Artech House, 1992.

اختفاء اطلاعات

Information Hiding

تعداد واحد: ۳ نوع واحد: نظری تعداد ساعت: ۴۸ پیشنهاد: پردازش سیگنالهای دیجیتال

اهداف درس: در این درس پس از معرفی مبحث اختفاء اطلاعات، عمدتاً دو تکنیک مستترنگاری و علامتگذاری حق انتشار که رشد فزاینده ای برای کاربردهای multi media دارند مورد مطالعه قرار می گیرد.

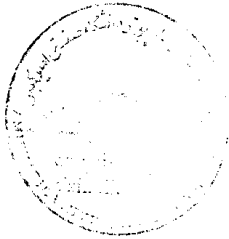
سرفصل مطالب:

- ۱- مقدمه (تعریف اختفاء اطلاعات، تاریخچه، کاربردها در سیستم های ارتباطی مدرن، کانال نمان، مستترنگاری، بی نامی و علامتگذاری حق انتشار)
- ۲- اصول مستترنگاری (معرفی مدل ارتباطات مستتر، مستترنگاری لغوی، مستترنگاری فنی، پروتکل های مختلف مستترنگاری، مستترنگاری ساده و مستترنگاری با کلید خصوصی و مستترنگاری با کلید عمومی)
- ۳- تکنیک های مستترنگاری (روش های مختلف اختفاء اطلاعات برای ارتباطات مستتر، مانند سیستم های جانیشینی، روش های اختفاء در تصاویر دورنگ، مستترنگاری آماری، تکنیک های تولید پوشش و انحراف، مستترنگاری در تصاویر)
- ۴- تحلیل مستتر (مفاهیم تحلیل مستتر، ترمینولوژی، اصول تحلیل مستتر، ابزارهای تحلیل مستترنگاری متداول)
- ۵- علامتگذاری حق انتشار (علامتگذاری حق انتشار و Watermarking، کاربردهای watermark، ارزیابی سیستم های watermark)
- ۶- تکنیک های علامتگذاری (اصول طراحی سیستم های علامتگذاری watermark، علامتگذاری مرئی و نامرئی، انتخاب مکان های میزبان، جنبه های روانی- بصری، انتخاب فضای کار (wavelet, DCT, DFT)، فورمت بیت های علائم watermark، اپراتور وارد کردن watermark و بهینه سازی گیرنده watermark، مقابله با حملات به watermark های دیجیتال)
- ۷- قوام سیستم های علامتگذاری حق انتشار (copyright marking) (قوام علائم حق انتشار در مقابل حملات عمومی، دسته بندی حملات مختلف مانند حملات پروتکلی، حملات oracle، محدودیت های WWWspider و معماری سیستم)
- ۸- انگشت نگاری (fingerprinting) (اصول و کاربرد انگشت نگاری در ردگیری خائن، انگشت نگاری آماری، انگشت نگاری نامتقارن، انگشت نگاری بدون نام)
- ۹- ابعاد حقوقی (کاربرد علائم Watermark برای حق انتشار روی اینترنت)

مراجع:

- 1- S. Katzenbeisser, F. Petitcolas (eds.), *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House, 1999.

- 2- N. F. Johnson, Z. Duric and S. Jajodia, *Information Hiding: Steganography and Watermarking-Attacks and Countermeasures*, Kluwer Academic Publishers, 2000.
- 3- P. Wayner, *Disappearing Cryptography-Information Hiding: Steganography and water marking*, 2nd ed. Morgan Kaufman Publishers, 2002.
- 4- I. Cox, M. Miller, and J. Bloom, *Digital Watermarking*, Morgan Kaufmann Publishers, 2001.
- 5- M. Wu, and B. Liu, *Multi media Data Hiding*, Springer-Verlag, 2002.



مباحث پیشرفته در امنیت اطلاعات

Advanced Topics in Information Security

تعداد واحد: ۳ نوع واحد: نظری تعداد ساعت: ۴۸ پیشنهاد:

این درس به منظور ارائه مطالب جدید مطرح در رشته فناوری اطلاعات که هنوز به صورت درس استاندارد مطرح نشده‌اند ارائه می‌گردد.

