

بسم الله الرحمن الرحيم

تحلیل پروتکل های امنیتی ساده

قادر استفاده دانشجویان دوره کارشناسی ارشد مهندسی فن آوری اطلاعات - امنیت اطلاعات و مهندسی

کامپیوتر - رایانش امن



مؤلفین:

رؤیا مرشدی و علی پاینده

سرشناسه : مرشدی، رویا، ۱۳۶۷
 عنوان و نام پدیدآور : تحلیل پروتکل‌های امنیتی ساده [کتاب] : قابل استفاده دانشجویان دوره کارشناسی ارشد
 مهندسی فناوری اطلاعات /... مؤلفین رویا مرشدی و علی پاینده.
 مشخصات نشر : تهران : رویا مرشدی : علی پاینده، ۱۳۹۶.
 مشخصات ظاهری : ۱۵۶ ص.
 شابک : ۹۷۸-۶۰۰-۰۴-۷۸۴۵-۲
 وضعیت فهرست نویسی : فیبا
 یادداشت : کتابنامه.
 موضوع : شبکه‌های کامپیوتری -- تدابیر ایمنی
 موضوع : Computer network – security measures
 موضوع : رمزنگاری
 موضوع : Cryptography
 موضوع : پروتکل‌های شبکه کامپیوتری
 موضوع : Computer network protocol
 شناسه افزوده : پاینده، علی
 رده بندی کنگره : ۳۱۳۹۶ ق ۳۱۳۹۶/م ۵۹/م ۵۹/TK۵
 رده بندی ویدیویی : ۰۰۵/۸
 شماره کتابشناسی ملی : ۴۷۴۶۰۲

نام کتاب: تحلیل پروتکل‌های امنیتی ساده

مؤلفین: رویا مرشدی و علی پاینده

ناشر- مؤلف: رویا مرشدی

طراح جلد: رویا مرشدی

جایگاه: چاپار

سال انتشار و نوبت چاپ: چاپ اول ۱۳۹۸

تیراژ: ۱۰۰۰

قیمت: ۳۰۰۰ تومان

شابک: ۹۷۸-۶۰۰-۰۴-۷۸۴۵-۲

نشانی پست الکترونیک: Royamorshedi@gmail.com

حق چاپ و نشر این کتاب متعلق به مؤلفین بوده و هرگونه کپی یا نقل مطالب بدون اجازه مؤلفین پیگرد قانونی دارد.

مقدمه مؤلفین

در جهانی که با رشد انفجاری و سریع ذخیره داده‌ها و ارتباطات الکترونیکی روبه‌رو هستیم، حفاظت از اطلاعات تبدیل شده بسیار حیاتی است. این کتاب به ارائه یک مجموعه از کارهای تحقیقاتی در زمینه رمزنگاری می‌پردازد. در این کتاب بحث بر سر بعضی چالش‌های محاسباتی و به مکسیم‌هایی برای دفاع در برابر آن‌ها ادامه می‌یابد. هدف و تمرکز این کتاب بررسی نحوه تأمین ارتباطات امن و یا چند طرف می‌خواهند بر روی یک کانال یا شبکه ناامن ارتباط امن داشته باشند. همچنین بررسی نحوه تأمین سرویس‌های امنیتی (تبادل کلیدهای محرمانه، تصدیق هویت، برقراری یک ارتباط امن و...) و بررسی انواع پروتکل‌های امنیتی، و بررسی مقدماتی روش‌های تحلیل پروتکل‌های امنیتی را فرض به کارگیری رمزنگاری کامل و صحیح بودن پیاده‌سازی و سیستم‌عامل می‌باشد.

این کتاب یک منبع با ارزش دانش پر تنگی است. محققان، مهندسان، دانشجویان کارشناسی ارشد و دکترها مشغول به کار در زمینه پروتکل‌های امنیتی است. همچنین برای اعضای هیات علمی دانشگاه‌ها مفید می‌باشد.

فهرست مطالب

۵	فهرست مطالب.....
۱	فصل ۱ - فصل اول.....
۲	۱-۱ تعاریف.....
۲	۲-۱ دوره در سیستم امن.....
۳	۳-۱ تمهیدات امنیتی در لایه های مختلف شبکه.....
۳	۴-۱ تعاریف.....
۴	۵-۱ جایگاه پروتکل های امنیتی در سلسله مراتب ایجاد امنیت شبکه.....
۵	۶-۱ مشخصات پروتکل های امنیتی.....
۶	۷-۱ تعاریف سرویس های امنیتی.....
۹	۸-۱ انواع پروتکل های امنیتی.....
۱۰	۹-۱ دسته بندی پروتکل های امنیتی از نظر نحوه اجرا.....
۱۱	۱۰-۱ حملات علیه پروتکل های امنیتی.....
۱۲	۱۱-۱ دسته بندی حملات تحلیل پروتکل های امنیتی.....
۱۲	۱۲-۱ انواع حملات غیرفعال تحلیل پروتکل های امنیتی.....
۱۳	۱۳-۱ انواع حملات فعال تحلیل پروتکل های امنیتی.....
۲۰	۱۴-۱ تفاوت سه حمله (حمله فردی در میان، حمله تکرار، حمله بازتاب).....
۲۰	۱۵-۱ اصول طراحی پروتکل های امنیتی.....
۲۱	۱۶-۱ عوامل مهم در نگارش پروتکل های امنیتی.....
۲۳	فصل ۲ - فصل دوم.....
۲۴	۱-۲ مبانی ریاضی.....
۲۷	۲-۲ مکانیزم های ایجاد امنیت در پروتکل های امنیتی.....

۲۷	۲-۳- اصول اساسی در رمزنگاری
۲۷	۲-۴- پروتکل های مخفی نگاری
۲۷	۲-۵- تفاوت رمزنگاری و مخفی نگاری
۲۷	۲-۶- الگوریتم های رمزنگاری متقارن
۲۹	۲-۷- الگوریتم های رمزنگاری نامتقارن
۳۱	۲-۸- حملات به الگوریتم های رمزنگاری
۳۱	۲-۹- توابع یک طرفه
۳۳	۲-۱۰- مولدهای دنباله تصادفی و شبه تصادفی
۳۴	۱۱- مهرهای زمانی
۳۵	۱۱-۲- مکانیزم امضای دیجیتال
۳۶	فصل ۳- فصل سوم
۳۷	۳-۱- پروتکل های امضای ساده
۳۷	۳-۲- امضای دیجیتال به نیمه
۳۷	۳-۳- امضای دیجیتال با زیاده پیام
۳۷	۳-۴- تفاوت های امضای دیجیتال به ضمیمه و امضای دیجیتال با بازیابی پیام
۳۸	۳-۵- تعاریف شکست یک طرح امضای دیجیتال
۳۸	۳-۶- تفاوت بین امضای وجودی و امضای انتزاعی
۳۸	۳-۷- سناریوهای حمله علیه طرح های امضای دیجیتال
۶۹	۳-۸- پروتکل های تصدیق اصالت ساده
۶۹	۳-۹- خواص و معیارهایی که در پروتکل های تصدیق اصالت به رد توجه قرار می گیرند
۸۳	۳-۱۰- پروتکل های تصدیق اصالت دوطرفه
۹۵	۳-۱۱- پروتکل های استغفار کلید ساده
۹۶	۳-۱۲- پروتکل های مبادله کلید
۱۰۹	۳-۱۳- پروتکل های مبادله کلید تصدیق اصالت شده
۱۳۵	۳-۱۴- پروتکل های توافق کلید
۱۴۹	فصل ۴- فصل چهارم
۱۵۰	۴-۱- پروتکل های اشتراک راز ساده و دسته بندی آنها
۱۵۱	۴-۲- سناریوهای مختلف تقلب در طرح های اشتراک راز (آستانه ای)
۱۵۵	۴-۳- منابع