

امنیت فناوری اطلاعات در مقابله با حملات سایبری

گردآوری و تالیف:

مهندس علیرضا انصاری

(عضو هیات علمی دانشگاه هوایی شهید ستاری)

دکتر حمید محمدحسین

(عضو هیات علمی دانشگاه فرماندهی و ستاد آجا)



انتشارات دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

زمستان ۱۳۹۴

سر شناسه: انصاری، علیرضا

عنوان و نام پدید آور: امنیت فناوری اطلاعات در مقابله با حملات سایبری/مؤلف: علیرضا انصاری، حمید محمدحسین

مشخصات نشر: تهران- ارتش جمهوری اسلامی ایران- دانشگاه جنگ- دانشگاه فرماندهی و ستاد- ۱۳۹۴

مشخصات ظاهری: ۳۰۸ صفحه، مصور، جدول، نمودار

شابک: ۹۷۸-۹۶۴-۲۵۲۳-۹۱-۷

وضعیت فهرست‌نویسی: فیپا

موضوع: امنیت فناوری اطلاعات

موضوع: حملات سایبری

شماره: ۱، ایشناسی ملی: ۳۸۲۱۴۱۵

عنوان: امنیت فناوری اطلاعات در مقابله با حملات سایبری

مؤلفین: علیرضا انصاری، حمید محمدحسین

ویراستار: حسین ومنی فرد

صفحه آرای: توحید نووزنی اصفهانی

طرح روی جلد: علیرضا قانع

ناظر چاپ: سامان آزاد

ناشر: انتشارات دافوس آجا

شمارگان: ۱۰۰۰ نسخه

تعداد صفحه: ۳۰۸ص

تاریخ نشر: زمستان ۱۳۹۴

چاپ اول

لیتوگرافی، چاپ و صحافی: چاپخانه دانشگاه فرماندهی و ستاد

قیمت: ۱۸۰۰۰۰ ریال

نشانی: تهران، میدان پاستور، خیابان دانشگاه جنگ، دانشگاه فرماندهی و ستاد، انتشارات

دافوس

تلفن: ۰۲۱-۶۶۴۱۴۱۹۱

www.dafosaja.ac.ir

مسئولیت صحت مطالب بر عهده‌ی مؤلفین می‌باشد.

کلیه حقوق برای دافوس آجا محفوظ است. (نقل مطالب با ذکر مأخذ بلامانع است).

فهرست مطالب

فصل ۱: امنیت و مفهوم آن در فضای سایبر	۱۱
۱-۱- مقدمه	۱۲
۱-۲- استانداردهای امنیت اطلاعات	۱۳
۱-۳- پیدایش اینترنت	۱۵
۱-۴- فضای سایبر و جنگ سایبری	۱۹
۱-۵- ساختار دفاع سایبری برخی از کشورهای جهان	۲۲
۱-۶- جنگ سایبری چیست و چه هدفی را دنبال می‌کند	۳۸
۱-۷- انواع تهدیدها، مخدعاتی از جنگ سایبر	۳۹
۱-۸- انگیزه‌های جنگ سایبر	۴۰
۱-۹- مفهوم امنیت در فضای سایبر	۴۲
فصل ۲: موضوعات مطرح در حوزه امنیت	۴۷
۲-۱- مقدمه	۴۸
۲-۲- مفاهیم کلی امنیت شبکه	۴۸
۲-۳- مولفه‌های امنیت رایانه	۵۲
۲-۴- مراحل ایمن‌سازی	۵۵
۲-۵- امنیت شبکه لایه‌بندی شده با دیدگاه عملیاتی	۵۹
فصل ۳: امنیت سیستم‌های رایانه‌ای	۸۵
۳-۱- مقدمه	۸۶
۳-۲- تهدیدات امنیتی سیستم‌های رایانه‌ای	۸۶
۳-۲-۱- نرم‌افزارهای مخرب	۸۶
۳-۲-۲- راه‌های انتقال بدافزارها	۹۳
۳-۲-۳- روش‌های مقابله با بدافزارها	۹۶
۳-۳- دسته‌بندی انواع حملات بر علیه شبکه	۹۷
۳-۳-۱- حملات تکه‌تکه سازی	۹۹
۳-۳-۲- حملات عدم پذیرش سرویس	۱۰۱
۳-۳-۳- حملات توزیع شده عدم پذیرش سرویس	۱۱۴
۳-۳-۴- حملات درب‌های پشتی	۱۲۴
۳-۳-۵- حملات جعل هویت	۱۲۷

۱۳۱	۳-۳-۶- حملات ربودن نشست
۱۳۴	۳-۳-۷- حملات نوع Replay
۱۳۵	۳-۳-۸- حمله نشست تهی
۱۳۶	۳-۳-۹- حملات دسترسی تراگذری و سمت سرویس گیرنده
۱۳۷	۳-۳-۱۰- حملات مبتنی بر DNS
۱۴۳	۳-۳-۱۱- مسموم سازی ARP
۱۴۵	۳-۳-۱۲- حملات مبتنی بر استراق سمع
۱۵۰	۳-۳-۱۳- حملات مبتنی بر سرریز بافر
۱۵۱	۳-۳-۱۴- حملات مبتنی بر تزریق
۱۵۳	۳-۳-۱۵- حملات رهم شکستن کلمات عبور
۱۵۵	۳-۳-۱۶- حملات مبتنی بر مهندسی اجتماعی
۱۵۷	فصل ۴: امنیت زیرساخت ها و ارتباطات
۱۵۸	۴-۱- مقدمه
۱۵۸	۴-۲- مفهوم زیرساخت های امنیتی
۱۵۹	۴-۲-۱- امنیت فیزیکی
۱۶۸	۴-۲-۲- امنیت منطقی
۱۷۰	۴-۳- ایمن سازی تجهیزات زیربنایی شبکه های مختلف
۱۷۰	۴-۳-۱- امنیت فیزیکی ارتباطات
۱۷۱	۴-۳-۲- امنیت فیزیکی ایستگاه های کاری
۱۷۱	۴-۳-۳- امنیت فیزیکی تجهیزات شبکه
۱۹۱	فصل ۵: پیاده سازی و نگهداری شبکه های امن
۱۹۲	۵-۱- مقدمه
۱۹۲	۵-۲- ارتقاء امنیت در سطح شبکه
۱۹۴	۵-۳- پیاده سازی مدل های امنیت پایهای
۱۹۷	۵-۴- طبقه بندی و ایمن سازی اطلاعات
۱۹۸	۵-۵- ایمن سازی سیستم های سخت افزاری و نرم افزاری
۱۹۸	۵-۵-۱- ایمن سازی سیستم ها
۱۹۸	۵-۵-۲- ایمن سازی مولفه های شبکه بندی
۱۹۹	۵-۵-۳- ایمن سازی نرم افزار
۲۱۱	۵-۶- عوامل اساسی و تاثیرگذار در ایجاد مشکلات امنیتی

۲۱۲	۵-۷- تهدیدات مبتنی بر منابع انسانی
۲۱۵	فصل ۶: رمزنگاری و امنیت
۲۱۶	۶-۱- مقدمه
۲۱۶	۶-۲- تاریخچه رمزنگاری و امنیت
۲۱۸	۶-۳- رمزنگاری متقارن در مقابل رمزنگاری نامتقارن
۲۲۰	۶-۴- قدرت رمزنگاری
۲۲۷	۶-۵- الگوریتم‌های رمزنگاری
۲۳۲	۶-۶- رمزنگاری در مقابل درهم‌سازی
۲۳۳	۶-۶-۱- درهم‌سازی کلمه عبور
۲۳۴	۶-۶-۲- امضای دیجیتال، یک Email
۲۳۴	۶-۶-۳- الگوریتم‌های درهم‌سازی
۲۳۵	۶-۷- پنهان‌نگاری
۲۳۷	۶-۷-۱- پنهان‌سازی اطلاعات در یک فایل WAV
۲۴۰	۶-۷-۲- پنهان‌سازی اطلاعات در یک فایل JPG
۲۴۵	فصل ۷: سخت‌افزارهای امنیتی
۲۴۶	۷-۱- مقدمه
۲۴۶	۷-۲- آسیب‌پذیری‌های رسانه
۲۴۸	۷-۳- سوئیچ‌های مدیریت‌شده
۲۵۳	۷-۴- دیوارهای آتش
۲۵۵	۷-۵- سخت‌افزار IDS
۲۵۶	۷-۶- احراز هویت
۲۵۶	۷-۷- دستگاه‌های بیومتریک
۲۵۷	۷-۷-۱- اثر انگشت خوان
۲۵۹	۷-۷-۲- احراز هویت صوتی
۲۵۹	۷-۷-۳- دستگاه Hand geometry reader
۲۶۰	۷-۷-۴- احراز هویت دست‌خط
۲۶۰	۷-۷-۵- شناسایی چهره
۲۶۰	۷-۷-۶- اسکنرهای عنبیه و شبکیه
۲۶۱	۷-۸- تحمل خطا
۲۶۱	۷-۸-۱- افزودن تحمل خطا به یک سیستم کامپیوتری

۲۶۶	۷-۸-۲- افزودن تحمل خطا به یک شبکه کامپیوتری
۲۶۹	فصل ۸: نرم افزارهای امنیتی
۲۷۰	۸-۱- مقدمه
۲۷۰	۸-۲- ردیابی بسته
۲۷۳	۸-۳- پوشش پورت
۲۸۰	۸-۴- شکستن کلمات عبور
۲۸۱	۸-۴-۱- حدس کلمه عبور
۲۸۱	۸-۴-۲- شکستن کلمه عبور با روش Brute Force
۲۸۲	۸-۴-۳- حملات دیکشنری
۲۸۳	۸-۴-۴- مقابله با شکستن کلمات عبور
۲۸۴	۸-۴-۵- سیاست های در مورد کلمات عبور
۲۸۶	۸-۵- تشخیص نفوذ
۲۸۷	۸-۵-۱- تشخیص نفوذ مبتنی بر میزبان
۲۸۹	۸-۵-۲- تشخیص نفوذ مبتنی بر شبکه
۲۹۳	۸-۶- دسترسی راه دور امن
۲۹۴	۸-۷- سیاست ها و رویه های امنیتی
۲۹۴	۸-۷-۱- رسانه ذخیره سازی
۲۹۵	۸-۷-۲- سیاست مورد استفاده قابل قبول
۲۹۶	۸-۷-۳- رویه های امنیتی
۲۹۹	فصل ۹: سرویس ها و مکانیزم های امنیتی
۳۰۰	۹-۱- مقدمه
۳۰۰	۹-۲- سرویس های امنیتی
۳۰۰	۹-۲-۱- احراز هویت
۳۰۱	۹-۲-۲- کنترل دسترسی
۳۰۱	۹-۲-۳- محرمانگی داده
۳۰۲	۹-۲-۴- سلامت یا جامعیت داده
۳۰۳	۹-۲-۵- عدم انکار
۳۰۳	۹-۲-۶- سرویس دسترسی پذیری
۳۰۳	۹-۳- مکانیزم های امنیتی
۳۰۳	۹-۳-۱- مکانیزم های امنیتی فراگیر

۳۰۷ مکانیزم‌های امنیتی خاص ۹-۳-۲

۳۰۸ مدل‌های کنترل دسترسی ۹-۳-۳

www.ketab.ir

مقدمه مولفین:

خداوند را شکرگزاریم که توفیق گردآوری و تالیف کتاب امنیت فناوری اطلاعات در مقابله با حملات سایبری را به ما اعطا فرمود. کتاب حاضر، یکی از کتاب‌های آموزشی مفید برای ایجاد امنیت فناوری اطلاعات به منظور مقابله با حملات سایبری می‌باشد. این کتاب شامل ۹ فصل می‌باشد. در فصل اول کتاب ابتدا به تایخچه امنیت پرداخته و سپس ضمن معرفی فضای سایبر و جنگ سایبری، ساختار دفاع سایبری برخی از کشورها و همچنین انواع تهدیدهای مختلف ناشی از جنگ سایبری و انگیزه‌های جنگ سایبری مورد بحث قرار گرفته است. در فصل دوم کتاب به موضوعات طرح در حوزه امنیت اطلاعات پرداخته و در این خصوص ضمن معرفی مولفه‌های امنیت رایانه، مراحل ایمن‌سازی و امنیت شبکه لایه‌بندی شده توضیح داده شده است. فصل سوم کتاب که بحث عنوان امنیت سیستم‌های رایانه‌ای است، تهدیدات امنیتی سیستم‌های رایانه‌ای مورد بحث قرار گرفته و ضمن تبیین تهدیدات انواع حملات سایبری بر علیه شبکه، به توضیح نوع حملات و نحوه مقابله با آنها پرداخته شده است. فصل چهارم، امنیت زیرساخت‌ها و ارتباطات را توضیح داده و به ایمن‌سازی تجهیزات ریزپردازش شبکه‌های رایانه‌ای مختلف پرداخته است. در فصل پنجم که بحث عنوان پیاده‌سازی و نگهداری شبکه‌های امن می‌باشد، نحوه ارتقاء امنیت در سطح شبکه را توضیح داده و نحوه پیاده‌سازی مدل‌های امنیت پایدار مورد بحث قرار گرفته است. ایمن‌سازی سیستم‌های سخت‌افزاری و نرم‌افزاری نیز در این فصل توضیح داده شده است و در نهایت عوامل اساسی و تاثیرگذار در ایجاد مشکلات امنیتی و تهدیدات مبتنی بر منابع انسانی مورد بحث قرار گرفته است. در فصل ششم رمزنگاری و الگوریتم‌های مربوط به آن توضیح داده شده است و سپس به معرفی پنهان‌نگاری پرداخته شده است. در فصل‌های هفتم و هشتم نیز به ترتیب سخت‌افزارهای امنیتی و نرم‌افزارهای امنیتی معرفی و مورد بحث قرار گرفته‌اند. در آخرین فصل نیز سرویس‌ها و مکانیزم‌های امنیتی مورد بحث قرار گرفته است. به طور کلی در این کتاب به عمل سعی شده است، اطلاعاتی کامل و دقیق در ارتباط با فضای سایبری، شبکه‌های کامپیوتری، امنیت سخت‌افزار و امنیت نرم‌افزار برای علاقه‌مندان فراهم گردد.

هر چند دقت زیادی به عمل آمده است که کتاب حاضر عاری از لغزش باشد، اما بی‌گمان این چنین نیست و تذکر خوانندگان و صاحب‌نظران ارجمند در مورد لغزش‌های احتمالی، موجب امتنان خواهد بود. به امید آن که این کتاب بتواند بخشی از خلاء موجود در موضوع مورد بحث خود را پر کرده و برای خوانندگان مفید فایده باشد. انشاء...

از دریافت نظرات و پیشنهادهای سازنده شما به نشانی پست الکترونیکی زیر سپاسگزار خواهیم بود.

علیرضا انصاری

AlirezaAnsari@gmail.com