

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

امنیت و فضای سایبری

مؤلفین:

مهندس روح‌اله آب‌نیکی

متخصص ارشد شبکه و امنیت

مهندس سعید بنائیان‌فر

دانشجوی دکتری مخابرات امن و رمزنگاری

سرشناسه	: آبنیکی، روح‌اله، ۱۳۶۱ -
عنوان و نام پدیدآور	: امنیت و فضای سایبری/مؤلفین روح‌اله آبنیکی، سعید بنائیان‌فر.
مشخصات نشر	: تهران: دیار، ۱۳۹۹.
مشخصات ظاهری	: ۱۶۱ ص:، مصور، جدول، نمودار.
شابک	: ۲۵۰۰۰۰ رایان: 7-671201-600-978
وضعیت فهرست نویسی	: فیبا
یادداشت	: کتابنامه: ص: ۱۶۰.
موضوع	: فضای مجازی -- تدابیر امنیتی
موضوع	: Cyberspace -- Security measures
موضوع	: رمزگذاری داده‌ها
موضوع	: Data encryption (Computer science)
موضوع	: شبکه‌های کامپیوتری -- تدابیر امنیتی
موضوع	: Computer networks -- Security measures
شماره افزوده	: بنائیان‌فر، سعید، ۱۳۶۸ -
رده بنیاد کنگره	: HMA51
ردیف دیویی	: ۳۰۳/۴۸۲۲
شماره کتابشناختی ملی	: ۶۱۱۹۲۶۸

نام کتاب: امنیت و فضای سایبری

مؤلفین: روح‌اله آبنیکی - سعید بنائیان‌فر

ناشر: نشر دیار

نوبت چاپ: اول

سال چاپ: ۱۳۹۹

تعداد صفحات: ۱۶۱

تیراژ: ۱۰۰ نسخه

قیمت: ۳۵۰۰۰ تومان

شابک: ۷-۰۱-۶۷۱۲-۶۰۰-۹۷۸

ISBN: 978-600-6712-01-7

نشر دیار

تلفن سفارش: ۰۹۳۸۸۶۸۲۳۰۸

تلفن انتشارات: ۰۲۱-۶۶۹۲۵۰۲۵

فهرست مطالب

عنوان	صفحه
پیش گفتار	۱۳
فصل اول (معرفی واژگان امنیت و سایبر)	۱۵
سایبر	۱۵
جهان سایبری (Cyber World)	۱۵
فضای سایبری (Cyber Space)	۱۸
لایه های جهان سایبری	۱۸
لایه فیزیکی	۱۸
لایه نحوی (ترکیبی)	۱۹
لایه معنایی	۱۹
لایه خدمات	۱۹
لایه شناختی	۱۹
تعریف سازمان های ISO و ITU از سایبر	۲۰
راهبران تغییر جهان سایبری	۲۰
تاریخچه امنیت و امنیت سایبری	۲۳
معماری امنیت سامانه ارتباطی باز (OSI)	۲۴
مدل امنیت شبکه	۲۵
استانداردها	۲۶
فصل دوم (رمزنگاری)	۲۷
رمزنگاری	۲۷
کدگذاری	۲۷
هدف از کدگذاری	۲۷
رمزنگاری	۲۸
هدف از رمزنگاری	۲۸
انواع رمزنگاری	۲۹
رمزنگاری متقارن	۲۹
اصول رمزنگاری متقارن	۳۰
رمزنگاری نامتقارن	۳۰

۳۱	 اصول رمزنگاری نامتقارن
۳۲	 زیرساخت کلید عمومی (PKI)
۳۳	 پروتکل های توزیع کلید
۳۳	 اشتراک کلید متقارن با استفاده از رمزنگاری نامتقارن و توافق کلید
۳۳	 توابع چکیده ساز (hash)
۳۴	 کدهای احراز اصالت پیام (MAC)
۳۵	 احراز هویت
۳۵	 استاندارد X.509
۳۷	 امضای دیجیتال (Digital Signature)
۳۸	 امضای وکالت
۳۸	 امضای کرر
۳۹	 امضای گروهی
۳۹	 امضای حلقه
۴۰	 امضای رمز
۴۰	 پروتکل کربروس (Kerberos)
۴۱	 فناوری جدید مدیریت شبکه محلی (NTLM)
۴۱	 NTLM
۴۱	 NTLM v2
۴۱	 NTLM2
۴۲	 پروتکل مسیر دسترسی شبکه (LDAP, LDAPS)
۴۲	 استفاده از کلیه خدمات با یکبار ورود (SSO)
۴۳	 فصل سوم (پروتکل های امنیتی)
۴۳	 امنیت در سطح انتقال
۴۵	 HTTP و HTTPS
۴۶	 SSH و SSL, TLS
۴۷	 امنیت شبکه محلی WLAN بی سیم
۴۷	 مرور استاندارد IEEE 802.11 (مختص شبکه های بیسیم محلی)
۴۸	 استاندارد IEEE 802.11i (مختص امنیت شبکه های بیسیم محلی)
۴۹	 احراز هویت
۴۹	 کنترل دسترسی
۴۹	 حریم خصوصی یکپارچگی پیام

۵۲	 پروتکل های رمزنگاری در شبکه بی سیم محلی WLAN
۵۲	 پروتکل WEP
۵۲	 پروتکل WPA
۵۲	 پروتکل WPA۲ (۸۰۲.۱۱ i)
۵۲	 پروتکل WPA۳
۵۳	 امنیت ابتدا به انتها نقطه اتصال بیسیم
۵۳	 مختل کننده های بی سیم (Jamming Device)
۵۴	 نماد های جالشی در ارتباط بی سیم
۵۵	 امنیت در پست الکترونیکی email
۵۵	 POP3
۵۵	 IMAP
۵۶	 SMTP
۵۷	 استفاده از PGP برای افزایش امنیت پست الکترونیکی
۵۸	 S/MIME
۵۸	 امنیت IPsec (امنیت پروتکل اینترنت)
۶۰	 مدهای کاری در IPsec
۶۰	 حالت Transport
۶۰	 حالت Tunneling
۶۱	 کپسوله کردن اطلاعات امنیتی (ESP)
۶۱	 تبادل کلید اینترنت
۶۲	 شناسه و خدمات دسترسی
۶۲	 پروتکل PAP
۶۳	 پروتکل CHAP
۶۳	 پروتکل های MS-CHAP و MS-CHAPv2
۶۳	 پروتکل های EAP (Extensible Authentication Protocol)
۶۵	 پروتکل های AAA
۶۵	 پروتکل RADIUS
۶۶	 پروتکل TACACS+
۶۷	 پروتکل Diameter
۶۹	 فصل چهارم (دستگاه ها و سخت افزارهای امنیتی)
۶۹	 دیوار آتش
۷۰	 انواع دیوار آتش

- ۷۰ دیوار آتش نرم افزاری
- ۷۱ دیوار آتش سخت افزاری
- ۷۲ فایروالهای Stateless و Stateful
- ۷۲ فایروالهای Stateless
- ۷۲ فایروالهای Stateful
- ۷۳ مفهوم Demilitarized Zone (DMZ)
- ۷۴ سامانه های تشخیص /پیشگیری نفوذ (IDS/IPS)
- ۷۵ سامانه های تشخیص نفوذ مبتنی بر هاست (HIDS)
- ۷۵ سامانه های تشخیص نفوذ مبتنی بر شبکه (NIDS)
- ۷۶ جانمایی حساس و جمع آوری کننده ها
- ۷۶ روش های اشکارسازی
- ۷۷ آشکارسازی مبتنی بر امضا (Signature-Based)
- ۷۷ آشکارسازی مبتنی بر تحلیل رفتار (Heuristic/Behavioral)
- ۷۷ منابع اطلاعات و ترندها
- ۷۸ گزارش دهی مبتنی بر قوانین
- ۷۸ مفاهیم False Negatives و False Positives
- ۷۹ سامانه های تشخیص نفوذ در مقابل سامانه های پیشگیری از نفوذ فعال در مقابل غیر فعال
- ۸۰ شتاب دهنده های SSL/TLS
- ۸۰ رمزگشاهای SSL
- ۸۱ هانی پات Honeypot (محل های جذاب برای مهاجم)
- ۸۲ هانی نت (شبکه های جذاب برای مهاجم)
- ۸۳ هانی توکن (رمزها و عبارات جذاب برای مهاجم)
- ۸۳ پروتکل امنیتی IEEE 802.1x
- ۸۴ بایومتریک (ویژگی های منحصر به فرد فیزیکی افراد)
- ۸۴ سامانه های بایومتریکی برای احراز هویت کاربران
- ۸۶ بایومتریک و جرم یابی
- ۸۷ امنیت سخت افزار
- ۸۹ جرم یابی دیجیتال آزمایشی در سیم کارت های تلفن همراه
- ۹۰ تکنولوژی طراحی توابع فیزیکی غیر قابل کنترل (PUFs) مزایا و تبادلات
- ۹۰ APUF
- ۹۰ BPUF
- ۹۰ ROPUF

۹۱	 پروتکل NAT و PAT
۹۲	 ایزوله کردن ترافیک با استفاده از شبکه های محلی مجازی (VLAN)
۹۲	 شبکه محلی مجازی
۹۴	 سرورهای پراکسی
۹۵	 سرورهای پراکسی شفاف در مقابل سرورهای پراکسی غیر شفاف
۹۶	 پراکسی معکوس
۹۷	 کاربردهای پراکسی
۹۷	 دروازه های مستی
۹۸	 پیاده سازی شبکه امن
۱۰۰	 مناطق رمزنگاری ها
۱۰۰	 اینترنت
۱۰۰	 اکسترانت
۱۰۱	 DMZ
۱۰۲	 دفاع لایه ای
۱۰۳	 فصل پنجم (بدافزارها و حملات سایبری)
۱۰۳	 انواع بدافزارها
۱۰۳	 ویروس ها
۱۰۴	 کرم ها
۱۰۴	 بمب های منطقی
۱۰۵	 تروجان ها
۱۰۵	 RAT
۱۰۵	 باج افزارها (Ransomware)
۱۰۶	 Keylogger ها
۱۰۶	 جاسوس افزار (Spyware)
۱۰۶	 تبلیغاتهای مزاحم (adware)
۱۰۶	 درهای پشتی (Backdoor)
۱۰۶	 روت کیت ها (RootKit)
۱۰۶	 بات نت (Botnet)
۱۰۷	 انواع حملات
۱۰۷	 حملات غیر فعال
۱۰۷	 حملات فعال
۱۰۸	 حملات مشترک

۱۰۸		منع خدمات دهی (DoS) و منع خدمات دهی به صورت گسترده (DDoS)
۱۱۰		ارتقای سطح دسترسی
۱۱۰		دستکاری و جعل (IP&MAC Spoofing)
۱۱۱		حمله ارسال سیل آسای پیام همزمانی
۱۱۱		حمله مردی در میانه (MitM)
۱۱۲		حمله ARP Poisoning
۱۱۳		حملات به DNS
۱۱۴		حمله DNS Poisoning
۱۱۵		حمله Pharming
۱۱۵		حمله DDoS به DNS
۱۱۵		حمله Amplification
۱۱۶		حمله گذرواژه
۱۱۶		حمله جست و جو کامل (Brute Force)
۱۱۷		حمله واژه نامه (Dictionary)
۱۱۷		گذرواژه های چکیده شده
۱۱۸		عبور چکیده ها
۱۱۸		حمله روز تولد
۱۱۹		حمله جدول رنگین کمان (Rainbow Table)
۱۱۹		حمله تکرار
۱۲۰		حمله متن آشکار معلوم
۱۲۱		سرقت و حملات مرتبط
۱۲۱		سرقت کلیک
۱۲۱		سرقت نشست
۱۲۲		سرقت دامنه
۱۲۲		حمله مردی در مرورگر
۱۲۳		دستکاری راه اندازها
۱۲۳		حمله روز صفرم
۱۲۳		ضعف های بافر حافظه
۱۲۴		نشست حافظه
۱۲۴		سر ریز اعداد صحیح
۱۲۵		سر ریز بافر و حملات سرریز بافر
۱۲۵		حملات زمان بندی (زمان سنجی) کانال جانبی
۱۲۶		Pointer Dereference

۱۲۷	تزریق کتابخانه پیوند پویا
۱۲۷	حملات مهندسی اجتماعی
۱۲۹	فصل ششم (کنترل و حفاظت فیزیکی)
۱۲۹	استفاده از نشان
۱۳۰	مقایسه انواع قفل های درب
۱۳۰	امنیت درب با استفاده از رمز
۱۳۱	امنیت درب با استفاده از کارت هوشمند
۱۳۲	امنیت درب با استفاده از بیومتریک
۱۳۳	به دنباس شدن داخل (Tailgating)
۱۳۳	جلوگیری از Tailgating با استفاده از تله انسانی
۱۳۴	افزایش امنیت فیزیکی با استفاده از گارد
۱۳۴	نظارت منطقه با استفاده از دوربین
۱۳۵	فنس کشی، روشنایی و علائم هشدار دهنده
۱۳۶	امنیت دسترسی با استفاده از راه ها
۱۳۷	استفاده از قفل های سخت افزاری
۱۳۷	امنیت کامپیوترها با استفاده از قفل کابل
۱۳۷	امنیت سرورها با استفاده از محفظه های قفل دار
۱۳۸	نگه داری امن دستگاه های هوشمند
۱۳۸	مدیریت دارایی
۱۳۹	سامانه های گرمایشی و تهویه هوا (HVAC)
۱۳۹	راهرو های سرد و گرم
۱۴۰	سامانه های HVAC و آتش
۱۴۰	سرکوب آتش
۱۴۱	نظارت محیطی
۱۴۱	محافظت
۱۴۱	کابل کشی محافظت شده
۱۴۲	کابل کشی گسترده محافظت شده
۱۴۲	قفس فارادی
۱۴۵	فصل هفتم (مفاهیم بنیادی خطر)
۱۴۵	خطر و مقابله با آن
۱۴۶	آسیب پذیری (vulnerability)

۱۴۶	 شناسایی آسیب پذیرها
۱۴۶	 مدیریت خطر (Risk Management)
۱۴۷	 ارزیابی خطر (Risk Assessment)
۱۴۷	 ارزیابی کمی خطر
۱۴۸	 ارزیابی کیفی خطر
۱۴۸	 مستند کردن ارزیابی ها
۱۴۹	 فصل هشتم (سایبر و سایبرنتیک)
۱۴۹	 تهدیدات سایبری
۱۴۹	 عوامل تهدیدات سایبری
۱۴۹	 انواع تهدیدات سایبری
۱۵۰	 فعالیت های سایبری
۱۵۰	 جرایم سایبری
۱۵۱	 جاسوسی سایبری
۱۵۱	 تروریسم سایبری
۱۵۳	 جنگ سایبری
۱۵۴	 آسیب پذیری های جهان سایبری
۱۵۴	 عملیات سایبری
۱۵۵	 تهدیدات سایبری، قانونی بودن و استراتژی
۱۵۵	 زیرساخت اطلاعات بحرانی (CII)
۱۵۶	 حملات فیزیکی سایبری (Cyber-Physical Attacks)
۱۵۷	 سامانه های نظارت بر کنترل و جمع آوری داده ها (SCADA)
۱۵۸	 امنیت اسکادا
۱۵۸	 اختصاصی سازی هانی پات ها برای سامانه های اسکادا
۱۵۹	 استراتژی امنیت سایبری و اجرای طرح (CSIP)
۱۶۰	 امنیت سایبری و محافظت از سامانه های کنترل صنعتی (ICS)
۱۶۱	 منابع

