



مؤسسه فرهنگی هنری
دیباجران تهران

به نام خدا

امنیت سایبری امروز

حملات سایبری، امنیت شبکه و پیشگیری از تهدیدات

مؤلف:

Debrupa Palit

مترجم:

شهرزاد ستوده



هرگونه چاپ و تکثیر از محتویات این کتاب بدون اجازه کتبی ناشر ممنوع است. متخلفان به موجب قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می گیرند.

◀ عنوان کتاب: امنیت سایبری امروز

حملات سایبری، امنیت شبکه و پیشگیری از تهدیدات

◀ مترجم: شهرز ستوده

◀ ناشر: مؤسسه فرهنگی هنری دیباگران تهران

◀ ویراستار: مهدیه مخبری

◀ صفحه آرای: نازنین نصیری

◀ طراح جلد: داریوش فرسای

◀ نوبت چاپ: اول

◀ تاریخ نشر: ۱۴۰۴

◀ چاپ و صحافی: صدف

◀ تیراژ: ۱۰۰ جلد

◀ قیمت: ۵۰۰۰۰۰ ریال

◀ شابک: ۹۷۸-۶۲۲-۲۱۸-۹۴۴-۰

نشانی واحد فروش: تهران، خیابان انقلاب،

خیابان شهدای ژاندارمری-بین ۱۲ فروردین و فخر رازی-

پلاک ۸۸ طبقه دوم-واحد ۶ تلفن: ۶۶۹۵۶۸۹۴-۶۶۹۶۵۷۴۹

فروشگاههای اینترنتی دیباگران تهران :

WWW.MFTBOOK.IR

www.dibagarantehran.com

سرشناسه: پالیت، دبروپا Palit, Debrupa

عنوان و نام پدیدآور: امنیت سایبری امروز: حملات سایبری، امنیت

شبکه و پیشگیری از تهدیدات/ (دبروپا پالیت)؛ مترجم: شهرز ستوده؛

ویراستار: مهدیه مخبری.

مشخصات نشر: تهران: دیباگران تهران: ۱۴۰۴

مشخصات ظاهری: ۳۳۴ ص: مصور،

شابک: ۹۷۸-۶۲۲-۲۱۸-۹۴۴-۰

وضعیت فهرست نویسی: فیبا

یادداشت: عنوان اصلی: Cybersecurity: cyber attacks, network security, and threat prevention

عنوان دیگر: حملات سایبری، امنیت شبکه و پیشگیری از تهدیدات.

موضوع: شبکه های کامپیوتری-تدابیر ایمنی

موضوع: computer networks-security measures

موضوع: کامپیوترها-ایمنی اطلاعات-تدابیر ایمنی

موضوع: computer security-security measures

موضوع: هک کردن-پیشگیری

موضوع: hacking-prevention

شناسه افزوده: ستوده، شهرز، ۱۳۵۳-مترجم

رده بندی کنگره: ۵۹/۵۱۰۵ TK

رده بندی دیویی: ۸۰۰۵

شماره کتابشناسی ملی: ۱۰۱۴۸۴۰۷

نشانی اینستاگرام دیبا dibagaran_publishing نشانی تلگرام: @mftbook

هر کتاب دیباگران، یک فرصت جدید علمی و شغلی.

هر گوشی همراه، یک فروشگاه کتاب دیباگران تهران.

از طریق سایتهای دیباگران، در هر جای ایران به کتابهای ما دسترسی دارید.

فهرست مطالب

مقدمه ناشر	۱۱
پیشگفتار	۱۲
سخن مترجم	۱۶

فصل ۱

مبانی ارتباطات داده و شبکه‌سازی	۱۷
مقدمه	۱۷
ساختار فصل	۱۸
اهداف	۱۸
مدل‌های مرجع شبکه	۱۸
مدل اتصال متقابل سامانه‌های باز (OSI)	۱۹
مدل OSI و مدل TCP/IP	۲۶
انواع فلگ‌های TCP	۲۷
هندشیک سه‌مرحله‌ای	۲۸
ترجمه آدرس شبکه (NAT)	۲۹
رسانه انتقال شبکه	۳۰
دستگاه‌های شبکه	۳۲
پروتکل‌ها: HTTP، HTTPS و DNS	۳۴
پروتکل انتقال ابرمتن (HTTP)	۳۴
پروتکل امن انتقال ابرمتن (HTTPS)	۳۶
سامانه نام دامنه (DNS)	۳۷
مقدمه‌ای بر پراکسی و زنجیره پراکسی	۳۹
زنجیره پراکسی	۳۹
اهداف امنیت اطلاعات	۴۰
محرمانگی، یکپارچگی و دسترس‌پذیری	۴۱
اهداف کلیدی در تأمین امنیت شبکه	۴۲
مفاهیم پایه‌ای رمزنگاری و نهان‌نگاری	۴۳
نهان‌نگاری	۴۴
نتیجه‌گیری	۴۵
نکات مهم این فصل	۴۵

سؤالات چندگزینه‌ای..... ۴۶

پاسخ‌ها..... ۴۸

سؤالات..... ۴۸

فصل ۲

رمزگشایی از هک..... ۴۹

مقدمه..... ۴۹

ساختار فصل..... ۴۹

اهداف..... ۵۰

مقدمه‌ای بر هک..... ۵۰

مفهوم هک اخلاقی..... ۵۱

تفاوت بین هک و هک اخلاقی..... ۵۲

مراحل هک اخلاقی..... ۵۳

هکتیویسم..... ۵۵

اهداف هکتیویسم..... ۵۶

شکل‌های مختلف حملات هکتیویستی..... ۵۷

تخریب وبسایت..... ۵۸

نرم‌افزار RECAP..... ۵۸

تکثیر وبسایت..... ۵۹

انواع هکینگ..... ۵۹

انواع رایج هکینگ..... ۵۹

انواع هکرها..... ۶۱

تعریف و انواع جرائم سایبری..... ۶۳

حملات و طبقه‌بندی آن‌ها..... ۶۶

حملات فعال..... ۶۶

حملات غیرفعال..... ۶۸

اصطلاحات ضروری..... ۶۹

هدف ارزیابی..... ۶۹

اکسپلویت..... ۷۰

آسیب‌پذیری..... ۷۱

تهدید سایبری..... ۷۳

نتیجه‌گیری..... ۷۷

نکات مهم این فصل..... ۷۷

سؤالات چندگزینه‌ای..... ۷۷

پاسخ‌ها..... ۸۱

۸۱	پرسش‌ها
----	---------

فصل ۳

۸۳..... حقوق سایبری

۸۳	مقدمه
۸۳	ساختار فصل
۸۴	اهداف
۸۴	تروریسم سایبری
۸۹	اقدامات حفاظتی در برابر تروریسم سایبری
۸۹	حقوق سایبری
۹۲	جرائم مشمول قوانین سایبری
۹۲	کلاهبرداری
۹۲	کپی‌رایت
۹۲	اسرار تجاری
۹۳	قانون کار و قرارداد
۹۳	افترا
۹۳	آزادی بیان
۹۳	آزار و تعقیب
۹۴	جعل ایمیل
۹۸	جرائم سایبری علیه زنان
۹۹	تعقیب سایبری
۹۹	تماشاگری جنسی
۱۰۰	داکسینگ
۱۰۱	اغفال سایبری
۱۰۲	قوانین هند در زمینه جرائم سایبری علیه زنان
۱۰۳	ادله در فضای سایبری، نظارت و پایش
۱۰۵	نتیجه‌گیری
۱۰۶	نکات مهم این فصل
۱۰۶	سؤالات چندگزینه‌ای
۱۰۹	پاسخ‌ها
۱۱۰	سؤالات

فصل ۴

۱۱۱..... بدافزارها

۱۱۱	مقدمه
-----	-------

۱۱۲	 ساختار فصل
۱۱۲	 اهداف
۱۱۲	 مقدمه‌ای بر بدافزار
۱۱۳	 نشانه‌های آلودگی سیستم به بدافزار
۱۱۴	 کرم رایانه‌ای
۱۱۵	 اسب تروآ
۱۱۷	 جاسوس افزار
۱۱۸	 تبلیغ افزار
۱۱۹	 باج‌افزار
۱۲۲	 ویروس رایانه‌ای
۱۲۲	 انواع ویروس‌های رایانه‌ای
۱۲۴	 نشانه‌های حملات بدافزار
۱۲۶	 آنتی‌ویروس‌های محبوب و روش‌های تشخیص آنها
۱۲۶	 روش شناسایی مبتنی بر امضا
۱۲۸	 روش مبتنی بر اکتشاف
۱۳۰	 روش مبتنی بر فضای ابری
۱۳۱	 حملات انکار سرویس و انکار سرویس توزیع شده
۱۳۴	 سیستم شناسایی نفوذ و سیستم جلوگیری از نفوذ
۱۳۸	 مفاهیم Eavesdropping و snooping
۱۴۲	 بات‌ها / زامبی‌های بات‌نت‌ها
۱۴۳	 بات‌ها
۱۴۳	 بات‌نت‌ها
۱۴۵	 تهدیدات مبتنی بر برنامه‌های وب
۱۴۵	 اسکریپت‌نویسی میان‌سایتی
۱۴۶	 تزریق به پایگاه داده
۱۴۸	 تزریق فرمان
۱۴۹	 سرریز بافر
۱۵۱	 حمله پیمایش دایرکتوری
۱۵۲	 داندلدهای خودکار
۱۵۴	 اقدامات پیشگیرانه
۱۵۴	 کی لاگرها
۱۵۵	 فایروال‌ها
۱۵۷	 نتیجه‌گیری
۱۵۷	 نکات مهم این فصل
۱۵۸	 سوالات چندگزینه‌ای

۱۶۱	پاسخ‌ها
۱۶۲	پرسش‌ها

فصل ۵

۱۶۳.....دنیای رمزنگاری

۱۶۳	مقدمه
۱۶۳	ساختار فصل
۱۶۴	اهداف
۱۶۴	اصول بنیادی رمزنگاری
۱۶۷	رمزگذاری با کلید متقارن
۱۶۹	استاندارد رمزنگاری پیشرفته (AES)
۱۷۰	استاندارد رمزنگاری داده‌ها (DES)
۱۷۲	الگوریتم بین‌المللی رمزنگاری داده‌ها
۱۷۲	بلوفیش
۱۷۳	رمز ری‌وست ۴
۱۷۳	رمز ری‌وست ۵
۱۷۴	رمز ری‌وست ۶
۱۷۵	رمزنگاری کلید نامتقارن
۱۷۷	الگوریتم ریویست-شامیر-ادلما
۱۷۷	الگوریتم امضای دیجیتال
۱۷۸	تبادل کلید دیفی-هلمن
۱۸۰	نقش توابع درهم‌ساز
۱۸۲	پروتکل‌های رمزنگاری
۱۸۵	اهمیت امضاهای دیجیتال
۱۸۶	فرآیند ایجاد امضای دیجیتال در رمزنگاری
۱۸۸	تکنیک‌های تحلیل رمز
۱۹۱	نتیجه‌گیری
۱۹۱	نکات مهم این فصل
۱۹۱	سؤالات چندگزینه‌ای
۱۹۴	پاسخ‌ها
۱۹۵	پرسش‌های تشریحی

فصل ۶

۱۹۶.....شبکه‌های بی‌سیم و چالش‌های امنیتی آن‌ها

۱۹۶	مقدمه
-----	-------

۱۹۶	 ساختار فصل
۱۹۷	 اهداف فصل
۱۹۷	 مقدمه‌ای بر امنیت شبکه‌های بی‌سیم
۲۰۰	 پروتکل‌های رمزگذاری Wi-Fi
۲۰۱	 WEP
۲۰۱	 WPA
۲۰۱	 WPA2
۲۰۲	 WPA3
۲۰۳	 آسیب‌پذیری‌های رایج در شبکه‌های بی‌سیم
۲۰۷	 مکانیسم‌های احراز هویت و کنترل دسترسی
۲۰۹	 سامانه تشخیص و پیشگیری از نفوذ در شبکه‌های بی‌سیم (IDPS)
۲۱۷	 نظارت و مدیریت امنیت شبکه‌های بی‌سیم
۲۲۳	 نتیجه‌گیری
۲۲۴	 نکات مهم این فصل
۲۲۴	 سوالات چندگزینه‌ای
۲۲۷	 پاسخ‌ها
۲۲۸	 سوالات

فصل ۷

۲۲۹..... امنیت ابری

۲۲۹	 مقدمه
۲۲۹	 ساختار فصل
۲۳۰	 اهداف
۲۳۰	 مدل‌های استقرار ابر
۲۳۱	 ابر عمومی
۲۳۲	 ابر خصوصی
۲۳۴	 ابر جامعه‌ای
۲۳۶	 ابر ترکیبی
۲۴۰	 مدل‌های خدمات ابری
۲۴۰	 زیرساخت به عنوان خدمت (IaaS)
۲۴۲	 پلتفرم به عنوان خدمت (PaaS)
۲۴۴	 نرم‌افزار به عنوان خدمت (SaaS)
۲۴۷	 امنیت و تهدیدات در محیط‌های ابری
۲۵۱	 مراحل پیشگیری از ریسک‌های امنیتی رایانش ابری
۲۵۲	 امنیت داده و حفظ حریم خصوصی در فضای ابری

۲۵۴	مدیریت هویت و دسترسی در محیط‌های ابری
۲۵۶	بهترین شیوه‌ها و استانداردهای امنیت ابری
۲۶۱	تطبیق‌پذیری و حاکمیت در رایانش ابری
۲۶۴	ابزارها و فناوری‌های امنیت ابری
۲۶۷	نتیجه‌گیری
۲۶۷	نکات مهم این فصل
۲۶۷	سؤالات چندگزینه‌ای
۲۷۰	پاسخ‌ها
۲۷۱	سؤالات تشریحی

فصل ۸

امنیت در دنیای دیجیتال

۲۷۲	مقدمه
۲۷۲	ساختار فصل
۲۷۳	اهداف
۲۷۳	امنیت مبتنی بر رمز عبور
۲۷۴	مزایای احراز هویت مبتنی بر رمز عبور
۲۷۴	معایب احراز هویت مبتنی بر رمز عبور
۲۷۴	کاربرد رمز عبور
۲۷۵	انواع مختلف رمز عبور
۲۷۶	انواع حملات به رمز عبور و اقدامات پیشگیرانه
۲۸۰	امنیت اینترنت اشیاء
۲۸۵	امنیت شبکه‌های اجتماعی
۲۹۰	امنیت و رمز ارزها
۲۹۳	نرم‌افزارهای مجموعه امنیتی
۲۹۵	فایروال
۲۹۶	انواع فایروال‌ها
۳۰۲	نتیجه‌گیری
۳۰۲	نکات مهم این فصل
۳۰۳	سؤالات چندگزینه‌ای
۳۰۶	پاسخ‌ها
۳۰۶	سؤالات تشریحی

فصل ۹

روندهای نوظهور و مباحث پیشرفته در امنیت سایبری..... ۳۰۸

۳۰۸	مقدمه
۳۰۸	ساختار فصل
۳۰۹	اهداف
۳۰۹	امنیت ابری و مجازی‌سازی
۳۱۶	هوش مصنوعی (AI) و یادگیری ماشین (ML) در امنیت سایبری
۳۱۹	جرم‌شناسی دیجیتال
۳۲۴	پیامدهای فناوری بلاک‌چین بر امنیت سایبری
۳۲۶	پیامدهای محاسبات کوانتومی بر امنیت سایبری
۳۲۷	چالش‌های امنیتی در اینترنت اشیاء
۳۲۹	نتیجه‌گیری
۳۲۹	نکات مهم این فصل
۳۳۰	سؤالات چندگزینه‌ای
۳۳۳	کلید پاسخ‌ها
۳۳۴	سؤالات

خط‌مشی انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب‌هایی با کیفیت عالی است که بتواند
خواسته‌های به روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد.
هر کتاب دیباگران تهران، یک فرصت جدید شغلی و علمی

حمد و سپاس ایزد منان را که با الطاف بی‌کران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگی این مرز و بوم در زمینه چاپ و نشر کتب علمی و آموزشی گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گسترده‌گی علوم و سرعت توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه، نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش برجسته نموده است.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران و محققان در زمینه‌های گوناگون و مورد نیاز جامعه تلاش نموده برای رفع کمبودها و نیازهای موجود، منابعی پُر بار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهد.

کتابی که در دست دارید تألیف "جناب آقای شهروز ستوده" است که با تلاش همکاران ما در نشر دیباگران تهران منتشر گشته و شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

با نظرات خود مشوق و راهنمای ما باشید

با ارائه نظرات و پیشنهادات و خواسته‌های خود، به ما کمک کنید تا بهتر و دقیق‌تر در جهت رفع نیازهای علمی و آموزشی کشورمان قدم برداریم. برای رساندن پیام‌هایتان به ما از رسانه‌های دیباگران تهران شامل سایتهای فروشگاهی و صفحه اینستاگرام و شماره‌های تماس که در صفحه شناسنامه کتاب آمده استفاده نمایید.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران
dibagaran@mftplus.com

پیشگفتار

کتاب حاضر به صورت جامع به مباحث اساسی و پیشرفته امنیت سایبری می‌پردازد؛ از مفاهیم پایه‌ای تا مباحث پیشرفته هک، قوانین سایبری، شناسایی بدافزارها، شبکه‌های بی‌سیم و راهکارهای امنیتی برای حضور امن در دنیای دیجیتال. با پرداختن به این حوزه‌ها، کتاب درکی فراگیر از فناوری‌ها و تهدیداتی که محیط آنلاین ما را شکل می‌دهند، ارائه می‌دهد. این اثر با تشریح دقیق پیچیدگی‌های امنیت سایبری، افراد مبتدی را توانمند می‌سازد تا با اطمینان در فضای دیجیتال حرکت کرده و از خود و دارایی‌های دیجیتالی‌شان در برابر تهدیدات نوظهور محافظت کنند؛ و بدین ترتیب در ایجاد محیطی آنلاین امن‌تر برای همگان نقش‌آفرینی نمایند.

این کتاب، شالوده‌ای از اصول امنیت سایبری، شناختی عملی از روش‌ها و تاکتیک‌های هکرها، درکی روشن از چارچوب‌های قانونی، و مهارت‌های ضروری برای شناسایی و مقابله مؤثر با تهدیدات سایبری در اختیار خواننده قرار می‌دهد؛ دانشی که او را برای حضور آگاهانه و مطمئن در فضای دیجیتال توانمند می‌سازد.

کتاب شامل نه فصل است که به ترتیب به مفاهیم ارتباطات داده و شبکه، هک، قوانین سایبری، جزئیات مربوط به بدافزارها، مبانی رمزنگاری، شبکه‌های بی‌سیم و چالش‌های امنیتی آن‌ها، امنیت ابری، امنیت در جهان دیجیتال و روندهای نوظهور در امنیت سایبری می‌پردازد. بنابراین، فراگیران با تمام جنبه‌های کلیدی امنیت سایبری آشنا خواهند شد. توضیحات فصل‌ها به شرح زیر است:

◀ فصل ۱: مبانی ارتباطات داده و شبکه

این فصل به طور جامع اصول پایه‌ای لازم برای درک سیستم‌های ارتباطی مدرن را بررسی می‌کند. با ارائه یک دید کلی اولیه آغاز می‌شود و سپس به بررسی دقیق مفاهیم ارتباطات داده و شبکه می‌پردازد. مدل‌های مرجع شبکه، از جمله مدل‌های OSI و TCP/IP مورد مقایسه و تحلیل قرار می‌گیرند و نقش آن‌ها در برقراری ارتباطات بدون اختلال تشریح می‌شود.

این فصل همچنین به بررسی پروتکل‌های بنیادینی نظیر هندشیک سه مرحله‌ای و فلگ‌های TCP پرداخته و اهمیت آن‌ها در تضمین انتقال مطمئن داده‌ها را برجسته می‌سازد. مفاهیم ترجمه آدرس شبکه (NAT) نیز مورد بررسی قرار می‌گیرند تا درکی از نقش آن در مدیریت شبکه‌ها ارائه شود. سپس به تدریج به حوزه مهم امنیت اطلاعات وارد شده، اهداف اصلی آن نظیر محرمانگی، یکپارچگی و دسترس‌پذیری را تبیین می‌کند. افزون بر این، مفاهیم پایه رمزنگاری و نهان‌نگاری نیز معرفی می‌شوند تا پایه‌ای برای درک نقش این علوم در حفظ امنیت اطلاعات در محیط‌های شبکه‌ای فراهم گردد.

◀ فصل ۲: رمزگشایی هک

این فصل به بررسی انواع مختلف هک و هکرها می‌پردازد و چشم‌اندازی دقیق از فضای پیچیده جرائم سایبری و انواع آن، همچنین تفاوت‌های اساسی میان حملات غیرفعال و فعال امنیتی ارائه می‌دهد. مفاهیم کلیدی نظیر تهدید، آسیب‌پذیری، هدف ارزیابی، حمله و بهره‌برداری به تفصیل شرح داده می‌شوند و پایه‌ای قوی برای درک خوانندگان از فضای امنیت سایبری ایجاد می‌گردد.

تأکید فصل بر جنبه‌های اخلاقی هک نیز، درک متعدهانه‌ای از این حوزه پویا و در حال تحول فراهم می‌آورد و آن را به منبعی ارزشمند برای کسانی که به دنبال نگاهی دقیق و متوازن به مسئله هک هستند، تبدیل می‌سازد.

◀ فصل ۳: حقوق سایبری

این فصل به بررسی ابعاد قانونی فعالیت‌های سایبری می‌پردازد. مباحثی کلیدی همچون قوانین سایبری، جرایمی نظیر هک، سرقت داده، جعل هویت، فریب از جعل ایمیل، ارسال پیام‌های توهین‌آمیز، تماشاگری جنسی و تروریسم سایبری پوشش داده می‌شوند. بحث کاملی در خصوص مجازات‌های قانونی این جرائم در هند ارائه شده و درکی عمیق از عواقب قانونی آن‌ها به خوانندگان منتقل می‌شود.

خوانندگان با ماهیت در حال تحول تهدیدات سایبری، ساختارهای قانون‌گذاری جهت مقابله با آن‌ها و اهمیت بازدارندگی قانونی در عصر دیجیتال آشنا می‌شوند. این فصل منبعی حیاتی برای افرادی است که قصد دارند به‌درستی در فضای پیچیده حقوق سایبری حرکت کرده و پیامدهای قانونی هر نوع فعالیت سایبری را درک کنند.

◀ فصل ۴: بدافزار

این فصل دیدگاهی جامع در خصوص نرم‌افزارهای مخرب و تهدیدات مرتبط با آن‌ها ارائه می‌دهد و دانش لازم برای محافظت در برابر حملات سایبری را در اختیار خوانندگان قرار می‌دهد. انواع مختلف بدافزار از جمله ویروس‌ها، کرم‌ها، تروجان‌ها، جاسوس‌افزارها، تبلیغ‌افزارها و باج‌افزارها معرفی شده و ویژگی‌ها و شیوه عملکرد هریک به تفصیل بیان می‌گردد.

همچنین دسته‌بندی ویروس‌های رایانه‌ای شامل ویروس‌های فایل، ویروس‌های بوت‌سکتور و ویروس‌های ماکرو شرح داده شده‌اند. علائم حملات بدافزاری و نرم‌افزارهای آنتی‌ویروس معروف و روش‌های شناسایی آن‌ها (امضامحور، مبتنی بر تحلیل رفتار یا مبتنی بر فضای ابری) نیز مورد بررسی قرار می‌گیرند.

افزون بر این، ابزارهایی نظیر VirusTotal جهت تحلیل بدافزار، حملات DOS و DDOS، سیستم‌های تشخیص نفوذ (IDS) و پیشگیری از نفوذ (IPS)، کی‌لاگرها، فایروال‌ها و تهدیدات مرتبط با BOT و BOTNET توضیح داده می‌شوند. تهدیدات مبتنی بر وب نظیر تزریق اسکریپت از طریق سایت (XSS)، تزریق SQL و حملات فیشینگ نیز پوشش داده شده‌اند تا مخاطبان را برای دفاع مؤثر در برابر تهدیدات در حال تحول دیجیتال توانمند سازند.

◀ فصل ۵: دنیای رمزنگاری

در این فصل، خوانندگان با دنیای جذاب رمزنگاری و روش‌های محافظت از ارتباطات دیجیتال آشنا می‌شوند. فصل با معرفی اصول پایه رمزنگاری آغاز شده و سپس به بررسی دقیق رمزنگاری متقارن (با کلید مشترک) و نامتقارن (با جفت کلید عمومی/خصوصی) می‌پردازد. نقش توابع هش در حفظ یکپارچگی داده و امضای دیجیتال برای تأیید صحت و اصالت پیام‌ها نیز به‌طور جامع تحلیل می‌شوند.

پروتکل‌های رمزنگاری و روش‌های تحلیل رمز نیز مورد بررسی قرار گرفته‌اند. با ارائه توضیحات شفاف و مثال‌های عملی، فصل خوانندگان را به درک جامعی از مکانیزم‌های پیچیده سیستم‌های رمزنگاری مدرن می‌رساند و توانایی لازم برای استفاده از این ابزارها جهت حفظ امنیت اطلاعات حساس در دنیای به‌هم‌پیوسته امروزی را در اختیارشان قرار می‌دهد.

◀ فصل ۶: شبکه‌های بی‌سیم و چالش‌های امنیتی آن‌ها

این فصل نگاهی جامع به پیچیدگی‌های شبکه‌های بی‌سیم در عصر دیجیتال دارد. مفاهیم پایه مانند پروتکل‌های رمزگذاری Wi-Fi و آسیب‌پذیری‌های رایج در سیستم‌های بی‌سیم معرفی می‌شوند. با تحلیل‌های دقیق، فصل به بررسی بهترین راهکارها برای ایمن‌سازی مؤثر اتصالات بی‌سیم می‌پردازد تا خوانندگان را در مقابله با تهدیدات احتمالی و محافظت از شبکه در برابر نفوذ و سرقت داده توانمند سازد.

درک عمیق از امنیت Wi-Fi، استفاده از مکانیزم‌های رمزنگاری قوی و تأکید بر اقدامات پیشگیرانه و رویکردهای راهبردی از دیگر مباحث این فصل است که موجب می‌شود خوانندگان بتوانند در محیطی امن‌تر و مقاوم‌تر در برابر تهدیدات سایبری، به فعالیت خود ادامه دهند.

◀ فصل ۷: امنیت رایانش ابری

در این فصل، امنیت در فضای رایانش ابری به‌طور کامل بررسی می‌شود. فصل با معرفی مفاهیم پایه‌ای رایانش ابری، مدل‌های پیاده‌سازی (ابر عمومی، خصوصی، ترکیبی) و مدل‌های خدماتی IaaS، PaaS، SaaS آغاز می‌شود. سپس به بررسی تهدیدات و ریسک‌های رایج در محیط‌های ابری مانند نفوذ به داده‌ها و دسترسی‌های غیرمجاز پرداخته می‌شود.

راهکارهای حفظ امنیت و حریم خصوصی داده‌ها، مدیریت هویت و دسترسی (IAM)، و الزامات رعایت استانداردها، الزامات قانونی و چارچوب‌های حاکمیتی نیز در این فصل بررسی شده‌اند. در پایان، ابزارها و فناوری‌های متنوعی را معرفی می‌کند که می‌توانند در کاهش ریسک‌های امنیتی در محیط‌های ابری به‌کار روند.

◀ فصل ۸: امنیت در دنیای دیجیتال

این فصل به عنوان راهنمایی جامع برای محافظت فردی در فضای دیجیتال عمل می کند. اهمیت رمزهای عبور در محافظت از حساب های آنلاین تبیین شده و انواع رمزها از جمله رمزهای زیستی، تصویری مبتنی بر الگو و روش های ساخت رمز قوی تحلیل می شوند. همچنین به انواع حملات مبتنی بر رمز عبور و روش های مقابله با آنها پرداخته شده است.

استراتژی هایی نظیر رمزگذاری داده های حساس، استفاده از بسته های نرم افزاری امنیتی، پیکربندی فایروال ها و به روزرسانی منظم سیستم عامل برای برطرف سازی آسیب پذیری ها نیز از دیگر نکات کاربردی این فصل است. با اجرای این اقدامات، خوانندگان می توانند با اطمینان بیشتری در فضای دیجیتال فعالیت نمایند.

◀ فصل ۹: روندهای نوظهور و موضوعات پیشرفته در امنیت سایبری

در این فصل، موضوعات حیاتی همچون امنیت ابری و مجازی سازی در عصر رایانش ابری بررسی می شود. چالش های امنیتی اینترنت اشیا (IoT) به دلیل رشد فزاینده دستگاه های متصل، از دیگر موضوعات محوری این فصل است. نقش یادگیری ماشین و هوش مصنوعی در ارتقاء توانایی شناسایی تهدیدات و پاسخ گویی به آنها نیز مورد تحلیل قرار گرفته است.

فصل همچنین به بررسی فناوری بلاک چین در امنیت سایبری می پردازد و ماهیت غیرمتمرکز و تغییرناپذیر آن را به عنوان راهکاری نوآورانه در حفظ امنیت تراکنش ها و هویت های دیجیتال معرفی می کند. با ارائه پوشش جامع این موضوعات، خوانندگان درک عمیقی از چشم انداز در حال تحول امنیت سایبری و راهبردهای پیشرفته لازم برای مقابله با تهدیدات نوظهور به دست می آورند.

سخن مترجم

در عصری که مرزهای زندگی دیجیتال و فیزیکی به گونه‌ای بی‌سابقه درهم‌تنیده شده، امنیت سایبری از حاشیه به متن حیات فردی و جمعی ما کوچ کرده و به ضرورتی اجتناب‌ناپذیر بدل گشته است. ترجمه کتاب ارزشمند «امنیت سایبری امروز» اثر دیپروپا پالیت را فرصتی مغتنم می‌دانم تا گامی هرچند کوچک در مسیر ارتقای دانش و حساسیت جامعه فارسی‌زبان نسبت به این عرصه حیاتی بردارم. انتخاب این کتاب نه تصادفی که پاسخی آگاهانه به خلاء منابع آموزشی جامع، به‌روز و قابل‌هضم به زبان فارسی بود؛ منابعی که بتوانند از مفاهیم بنیادین شبکه و داده‌ها آغاز کنند و خواننده را تا پیچیده‌ترین مباحث هک اخلاقی، حقوق سایبری، رمزنگاری، امنیت ابری و روندهای نوظهور مانند اینترنت اشیا و هوش مصنوعی همراهی نمایند.

ساختار منسجم و گام‌به‌گام کتاب، نقطه قوت ممتاز آن است. کتاب با تشریح اصول ارتباطات داده و شبکه‌ها (فصل ۱) پایه‌ای مستحکم می‌سازد، سپس وارد عرصه پریهاو اما ضروری هک و انواع آن (فصل ۲) و پیامدهای قانونی فعالیت‌های سایبری (فصل ۳) می‌شود. فصل‌های میانی با تمرکز بر شناخت عمیق بدافزارها و تهدیدات مرتبط (فصل ۴) و کالبدشکافی دنیای پیچیده رمزنگاری (فصل ۵)، خواننده را برای درک چالش‌های امنیت در شبکه‌های بی‌سیم (فصل ۶) و محیط‌های رایانش ابری (فصل ۷) آماده می‌کند. کتاب با ارائه راهکارهای ملموس برای امنیت فردی در دنیای دیجیتال (فصل ۸) و نگاهی آینده‌نگرانه به روندهای نوظهور و پیشرفته (فصل ۹) به پایان می‌رسد. این سیر منطقی نه تنها درک جامعی از اکوسیستم امنیت سایبری ارائه می‌دهد، بلکه کاربردی بودن را سرلوحه قرار داده است: از تحلیل مکانیزم‌های حملات رایج مانند XSS، تزریق SQL، فیشینگ و DDoS و راه‌های مقابله با آنها، تا معرفی ابزارهای عملیاتی مانند VirusTotal و سیستم‌های IDS/IPS، و ارائه دستورالعمل‌های شفاف برای ایمن‌سازی شبکه‌های وای‌فای، محیط‌های ابری و دستگاه‌های شخصی.

فرآیند ترجمه این اثر فنی، خود سفری چالش‌برانگیز بود. یافتن معادل‌های دقیق و پذیرفته‌شده برای انبوهی از اصطلاحات تخصصی نیازمند مشورت با منابع معتبر و متخصصان حوزه بود. حفظ تعادل ظریف میان روانی بیان برای مخاطب غیرمتخصص و دقت فنی مورد انتظار خواننده حرفه‌ای، همواره مدنظر قرار داشت. همچنین، بومی‌سازی برخی مثال‌ها، به‌ویژه در فصل حقوق سایبری که به قوانین خاص هند اشاره داشت، برای ارتباط بیشتر با مخاطب ایرانی ضروری بود. امیدوارم حاصل این تلاش، متنی باشد که هم دقت علمی را رعایت کرده و هم برای طیف گسترده‌ای از خوانندگان فارسی‌زبان – از دانشجویان و متخصصان فناوری اطلاعات و امنیت که به دنبال مرور اصول یا آشنایی با حوزه‌های جدید هستند، تا مدیران سازمان‌ها که نیازمند درک ریسک‌های سایبری و الزامات حفاظتی‌اند، و حتی کاربران عادی که خواهان مهارت‌های محافظت از حریم خصوصی و داده‌های خود در فضای آنلاین می‌باشند – قابل‌استفاده و الهام‌بخش باشد.

در نهایت، عمیقاً امیدوارم این ترجمه سهمی هرچند اندک در توانمندسازی دیجیتال جامعه، افزایش تاب‌آوری در برابر تهدیدات، و نهایتاً کمک به شکل‌گیری فضای سایبری امن‌تر و قابل‌اعتمادتر برای تمامی فارسی‌زبانان داشته باشد. در این مسیر پریچ‌وخم، دانش نورافکنی است که راه را روشن می‌کند، و کتاب حاضر تلاشی است برای فراهم آوردن این نور. سپاس فراوان از ناشر گرامی که امکان عرضه این گنجینه دانش به جامعه فارسی‌زبان را فراهم ساخت.

با احترام،

شهرزاد ستوده