



به نام خدا

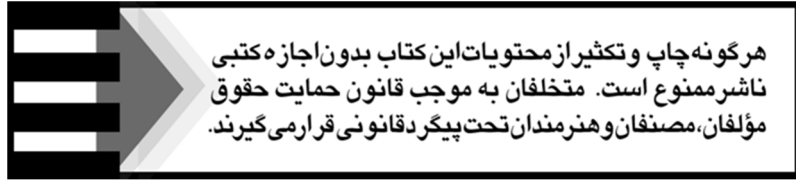


مبانی امنیت اطلاعات و شبکه

SECURITY +

مؤلف

احسان امجدی بیگوند



◀ عنوان کتاب: مبانی امنیت اطلاعات و شبکه SECURITY+

◀ مولف: احسان امجدی بیگوند

◀ ناشر: موسسه فرهنگی هنری دیباگران تهران

◀ صفحه آرایی: فرنوش عبدالهی

◀ طراح جلد: داریوش فرسایی

◀ نوبت چاپ: اول

◀ تاریخ نشر: ۱۳۹۸

◀ چاپ و صحافی: درج عقیق

◀ تیراژ: ۱۰۰ جلد

◀ قیمت: ۸۵۰۰۰۰ ریال

◀ شابک: ۹۷۸-۶۲۲-۲۱۸-۲۴۷-۲

نشانی واحد فروش: تهران، میدان انقلاب،

خ کارگر جنوبی، روبروی پاساژ مهستان،

پلاک ۱۲۵۱

تلفن: ۲۲۰۸۵۱۱۱-۶۶۴۱۰۰۴۶

فروشگاههای اینترنتی دیباگران تهران :

WWW.MFTBOOK.IR

www.dibbook.ir

www.dibagarantehran.com

نشانی تلگرام: @mftbook نشانی اینستاگرام دیبا [dibagaran_publishing](https://www.instagram.com/dibagaran_publishing)

هر کتاب دیباگران، یک فرصت جدید شغلی.

هر گوشی همراه، یک فروشگاه کتاب دیباگران تهران.

از طریق سایتها و اپ دیباگران، در هر جای ایران به کتابهای ما دسترسی دارید.

فهرست مطالب

١٦.....	INTRODUCTION TO SECURITY: فصل اول
١٨.....	FOUNDATION TOPICS
١٨.....	THE CIA OF COMPUTER SECURITY
٢١.....	THE BASICS OF INFORMATION SECURITY
٢٤.....	THINK LIKE A HACKER!
٢٦.....	THREAT ACTOR TYPES AND ATTRIBUTES
٢٨.....	COMPUTER SYSTEMS SECURITY PART I: فصل دوم
٣٠.....	MALICIOUS SOFTWARE TYPES
٣٠.....	VIRUSES
٣٢.....	WORMS
٣٢.....	TROJAN HORSES
٣٣.....	RANSOMWARE
٣٤.....	SPYWARE
٣٤.....	ROOTKITS
٣٥.....	FILELESS MALWARE
٣٥.....	SPAM
٣٧.....	DELIVERY OF MALWARE
٣٧.....	VIA SOFTWARE, MESSAGING, AND MEDIA
٣٩.....	BOTNETS AND ZOMBIES
٤٠.....	ACTIVE INTERCEPTION
٤٠.....	PRIVILEGE ESCALATION

٤١BACKDOORS
٤١LOGIC BOMBS
٤٢PREVENTING AND TROUBLESHOOTING MALWARE
٤٣PREVENTING AND TROUBLESHOOTING VIRUSES
٤٧PREVENTING AND TROUBLESHOOTING WORMS AND TROJANS
٤٨PREVENTING AND TROUBLESHOOTING SPYWARE
٥٠BADWARE
٥٠PREVENTING AND TROUBLESHOOTING ROOTKITS
٥١PREVENTING AND TROUBLESHOOTING SPAM
٥٣YOU CANT'T SAVE EVERY COMPUTER FROM MALWARE!
٥٤SUMMARY OF MALWARE PREVENTION TECHNIQUES
٥٥COMPUTER SYSTEMS SECURITY PART II: فصل سوم
٥٦IMPLEMENTING SECURITY APPLICATIONS
٥٧PERSONAL SOFTWARE FIREWALLS
٥٩HOST-BASED INTRUSION DETECTION SYSTEMS
٦١POP-UP BLOCKERS
٦٢DATA LOSS PREVENTION SYSTEMS
٦٣SECURING COMPUTER HARDWARE AND PERIPHERALS
٦٤SECURING THE BIOS
٦٦SECURING STORAGE DEVICES
٦٧NETWORK ATTACHED STORAGE
٦٧WHOLE DISK ENCRYPTION
٦٩HARDWARE SECURITY MODULES
٦٩SECURING WIRELESS PERIPHERALS
٧٠SECURING MOBILE DEVICE
٧١MALWARE
٧١BOTNET ACTIVITY
٧٢SIM CLONING AND CARRIER UNLOCKING
٧٣WIRELESS ATTACKS
٧٤THEFT

۷۴APPLICATION SECURITY
۷۷BYOD CONCERNS
۸۱OS HARDENING AND VIRTUALIZATION: فصل چهارم:
۸۳HARDENING OPERATING SYSTEMS
۸۳REMOVING UNNECESSARY APPLICATIONS AND SERVICES
۹۲WINDOWS UPDATE, PATCHES, AND HOTFIXES
۹۴PATCHES AND HOTFIXES
۹۸GROUP POLICIES, SECURITY TEMPLATES, AND CONFIGURATION BASELINES
۱۰۰HARDENING FILE SYSTEMS AND HARD DRIVES
۱۰۳KEEPING A WELL-MAINTAINED COMPUTER
۱۰۴VIRTUALIZATION TECHNOLOGY
۱۰۴TYPE OF VIRTUALIZATION AND THEIR PURPOSES
۱۰۵HYPERVISOR
۱۰۵SECURING VIRTUAL MACHINES
۱۰۸APPLICATION SECURITY: فصل پنجم:
۱۰۹SECURING THE BROWSER
۱۱۱GENERAL BROWSER SECURITY PROCEDURES
۱۱۱IMPLEMENT POLICIES
۱۱۳TRAIN YOUR USERS
۱۱۳USE A PROXY AND CONTENT FILTER
۱۱۵WEB BROWSER CONCERNS AND SECURITY METHODS
۱۱۵BASIC BROWSER SECURITY
۱۱۵COOKIES
۱۱۷LSOS
۱۱۷ADD-ONS
۱۱۸ADVANCED BROWSER SECURITY
۱۱۹SECURING OTHER APPLICATIONS
۱۲۲SECURE PROGRAMMING
۱۲۳SOFTWARE DEVELOPMENT LIFE CYCLE
۱۲۴CORE SDLC PRINCIPLES

۱۲۶	PROGRAMMING TESTING METHODS
۱۲۷	INPUT VALIDATION
۱۲۸	STATIC AND DYNAMIC CODE ANALYSIS
۱۲۸	FUZZ TESTING
۱۲۹	PROGRAMMING VULNERABILITIES AND ATTACKS
۱۲۹	BACKDOORS
۱۲۹	MEMORY/BUFFER VULNERABILITIES
۱۳۱	ARBITRARY CODE EXECUTION/ REMOVE CODE EXECUTION
۱۳۱	XSS AND XSRF
۱۳۲	MORE CODE INJECTION EXAMPLES
۱۳۴	DIRECTORY TRAVERSAL
۱۳۵	ZERO DAY ATTACK
۱۳۶	فصل ششم: NETWORK DESIGN ELEMENTS
۱۳۷	OSI MODEL
۱۳۹	NETWORK DEVICES
۱۳۹	SWITCH
۱۴۱	BRIDGE
۱۴۱	ROUTER
۱۴۲	NETWORK ADDRESS TRASLATION, AND PRIVATE VERSUS PUBLIC IP
۱۴۳	NETWORK ZONES AND INTERCONNECTIONS
۱۴۴	LAN VERSUS WAN
۱۴۴	INTERNET
۱۴۴	DEMILITARIZED ZONE (DMZ)
۱۴۶	INTRANET AND EXTRANET
۱۴۷	NETWORK ACCESS CONTROL (NAC)
۱۴۷	SUBNETTING
۱۴۸	VIRTUAL LOCAL AREA NETWORK (VLAN)
۱۵۱	CLOUD COMPUTING
۱۵۲	CLOUD SECURITY
۱۵۴	OTHER "CLOUD"-BASED CONCERNS

١٥٤	SERVER DEFENCE
١٥٤	FILE SERVERS
١٥٤	NETWORK CONTROLLERS
١٥٥	EMAIL SERVERS
١٥٥	WEB SERVERS
١٥٦	FTP SERVER

١٥٨ NETWORKING PROTOCOLS AND THREATS: فصل هفتم:

١٥٩	PORT RANGES, INBOUND VERSUS OUTBOUND, AND COMMON PORTS
١٦٧	PORT ZERO SECURITY
١٦٨	MALICIOUS ATTACKS
١٧٠	DDOS
١٧١	SINKHOLES AND BLACKHOLES
١٧٢	SPOOFING
١٧٣	SESSION HIJACKING
١٧٥	REPLAY
١٧٥	NULL SESSIONS
١٧٦	TRANSITIVE ACCESS AND CLIENT-SIDE ATTACKS
١٧٦	DNS POISONING AND OTHER DNS ATTACKS
١٧٨	ARP POISONING

١٧٩ NETWORK PERIMETER SECURITY: فصل هشتم:

١٨٠	FIREWALLS AND NETWORK SECURITY
١٨١	FIREWALLS
١٨٥	PROXY SERVERS
١٨٨	HONEYPOTS AND HONEYNETS
١٨٩	DATA LOSS PREVENTION (DLP)
١٩٠	NIDS VERSUS NIPS
١٩٠	NIDS
١٩١	NIPS
١٩٣	UNIFIED THREAT MANAGEMENT

١٩٤ **SECURING NETWORK DEVICES** :فصل نهم:

١٩٥	NETWORK DEVICE VULNERABILITIES
١٩٥	DEFAULT ACCOUNTS
١٩٦	WEAK PASSWORDS
١٩٧	PRIVILEGE ESCALATION
١٩٨	BACK DOORS
١٩٨	NETWORK ATTACKS
١٩٨	OTHER NETWORK DEVICE CONSIDERATIONS
١٩٩	CABLE MEDIA VULNERABILITIES
١٩٩	INTERFERENCE
٢٠٠	CROSSTALK
٢٠٠	TAPPING INTO DATA AND CONVERSATION
٢٠١	SECURING WIRELESS NETWORKS
٢٠١	WIRELESS ACCESS POINT VULNERABILITIES
٢٠٢	THE ADMINISTRATION INTERFACE
٢٠٢	SSID BROADCAST
٢٠٢	ROGUE ACCESS POINTS
٢٠٢	EVIL TWIN
٢٠٣	WEAK ENCRYPTION
٢٠٥	WI-FI PROTECTED SETUP
٢٠٥	AD HOC NETWORKS
٢٠٥	VPN OVER OPEN WIRELESS
٢٠٦	WIRELESS ACCESS POINT SECURITY STRATEGIES
٢٠٧	WIRELESS TRANSMISSION VULNERABILITIES
٢٠٩	FINAL NETWORK DOCUMENTATION

٢١٠ **AUTHENTICATION MODELS** :فصل دهم:

٢١٢	AUTHENTICATION MODELS AND COMPONENTS
٢١٢	AUTHENTICATION MODELS
٢١٤	LOCALIZED AUTHENTICATION TECHNOLOGIES
٢١٤	802.1X AND EAP

٢١٧LDAP
٢١٧KERBEROS AND MUTUAL AUTHENTICATION
٢١٩REMOTE DESKTOP SERVICES
٢٢٠REMOTE AUTHENTICATION TECHNOLOGIES
٢٢٠REMOTE ACCESS SERVICE
٢٢١VIRTUAL PRIVATE NETWORKS
٢٢٣RADIUS VERSUS TACACS

٢٢٥.....ACCESS CONTROL METHODS AND MODELS: فصل يازدهم:

٢٢٦ACCESS CONTROL MODELS DEFINED
٢٢٦DISCRETIONARY ACCESS CONTROL
٢٢٨MANDATORY ACCESS CONTROL
٢٢٨ROLE-BASED ACCESS CONTROL (RBAC)
٢٢٩ATTRIBUTE-BASED ACCESS CONTROL (ABAC)
٢٣٢RIGHTS, PERMISSIONS AND POLICIES
٢٣٢USERS, GROUPS, AND PERMISSIONS
٢٣٦PERMISSION INHERITANCE AND PROPAGATION
٢٣٧MOVING AND COPYING FOLDERS AND FILES
٢٣٨USERNAMES AND PASSWORDS
٢٤٠POLICIES
٢٤١COMPLEXITY AND LENGTH OF A PASSWORD
٢٤٣USER ACCOUNT CONTROL (UAC)

٢٤٤.....VULNERABILITY AND RISK ASSESSMENT: فصل دوازدهم:

٢٤٥CONDUCTING RISK ASSESSMENTS
٢٤٧QUALITATIVE RISK ASSESSMENT
٢٤٨QUANTITATIVE RISK ASSESSMENT
٢٥٠SECURITY ANALYSIS METHODOLOGIES
٢٥١SECURITY CONTROLS
٢٥٢VULNERABILITY MANAGEMENT
٢٥٣PENETRATION TESTING
٢٥٥OVAL

۲۵۶	ASSESSING VULNERABILITY WITH SECURITY TOOLS
۲۵۶	NETWORK MAPPING
۲۵۷	VULNERABILITY SCANNING
۲۵۹	NETWORK SNIFFING
۲۶۰	PASSWORD ANALYSIS

۲۶۳ **MONITORING AND AUDITING** : فصل سیزدهم:

۲۶۴	MONITORING METHODOLOGIES
۲۶۴	SIGNATURE-BASED MONITORING
۲۶۵	ANOMALY-BASED MONITORING
۲۶۵	BEHAVIOR-BASED MONITORING
۲۶۵	USING TOOLS TO MONITOR SYSTEMS AND NETWORKS
۲۶۵	PERFORMANCE BASELINING
۲۶۷	PROTOCOL ANALYZER
۲۶۸	WIRESHARK
۲۶۹	SNMP
۲۷۰	ANALYTICAL TOOLS
۲۷۲	CONDUCTING AUDITS
۲۷۳	AUDITING FILES
۲۷۵	LOGGING
۲۷۸	LOG FILE MAINTENANCE AND SECURITY
۲۸۰	AUDITING SYSTEM SECURITY SETTINGS
۲۸۳	SIEM

۲۸۴ **ENCRYPTION AND HASHING CONCEPTS** : فصل چهاردهم:

۲۸۵	CRYPTOGRAPHY CONCEPTS
۲۸۷	SYMMETRIC VERSUS ASYMMETRIC KEY ALGORITHMS
۲۸۷	SYMMETRIC KEY ALGORITHMS
۲۸۸	ASYMMETRIC KEY ALGORITHMS
۲۸۹	PUBLIC KEY CRYPTOGRAPHY
۲۹۰	KEY MANAGEMENT
۲۹۰	STEGANOGRAPHY

٢٩١	ENCRYPTION ALGORITHMS
٢٩٢	DES AND 3DES
٢٩٢	AES
٢٩٣	RC
٢٩٤	BLOWFISH AND TWOFISH
٢٩٤	RSA
٢٩٤	DIFFIE-HELLMAN
٢٩٤	ELLIPTIC CURVE
٢٩٧	HASHING BASICS
٢٩٨	CRYPTOGRAPHIC HASH FUNCTIONS
٢٩٨	MD5
٢٩٨	SHA
٢٩٩	LANMAN, NTLM, AND NTLMv2
٢٩٩	LANMAN
٣٠٠	NTLM AND NTLMv2
٣٠١	HASHING ATTACKS
٣٠١	PATH THE HASH
٣٠٢	HAPPY BIRTHDAY
٣٠٣	ADDITIONAL PASSWORD HASHING CONCEPTS
٣٠٥	PKI AND ENCRYPTION PROTOCOLS : فصل پانزدهم
٣٠٤	PUBLIC KEY INFRASTRUCTURE
٣٠٤	CERTIFICATE
٣٠٧	SSL CERTIFICATE TYPES
٣٠٨	SINGLE-SIDED AND DUAL-SIDED CERTIFICATES
٣٠٨	CERTIFICATE CHAIN OF TRUST
٣٠٩	CERTIFICATE FORMATS
٣١٠	CERTIFICATE AUTHORITIES
٣١٤	WEB OF TRUST
٣١٤	SECURITY PROTOCOLS
٣١٥	S/MIME

۳۱۶SSL/TLS
۳۱۸SSH
۳۱۹PPTP, L2TP, AND IPSEC
۳۱۹PPTP
۳۱۹L2TP
۳۲۰IPSEC

فصل شانزدهم: SOCIAL ENGINEERING, USER EDUCATION, AND

۳۲۲ FACILITIES SECURITY

۳۲۳SOCIAL ENGINEERING
۳۲۴PRETEXTING
۳۲۴MALICIOUS INSIDER
۳۲۵DIVERSION THEFT
۳۲۵PHISHING
۳۲۷HOAXES
۳۲۷SHOULDER SURFING
۳۲۸EAVESDROPPING
۳۲۸DUMPSTER DIVING
۳۲۸BAITING
۳۲۸PIGGYBACKING/ TAILGATING
۳۲۹WATERING HOLE ATTACK
۳۲۹USER EDUCATION

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

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 دانشگاهی، علوم پایه و به ویژه علوم کامپیوتر و انفورماتیک گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گسترده‌گی علوم و 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 روشن می‌نماید.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری جمعی از اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران، محققان و نیز پرسنل ورزیده و ماهر در زمینه امور نشر درصدد هستند تا با تلاش‌های مستمر خود برای رفع کمبودها و نیازهای موجود، منابعی پُر بار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت "جناب آقای احسان امجدی بیگونند" و تلاش جمعی از همکاران انتشارات میسر گشته که شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

کارشناسی و نظارت بر محتوا: زهره قزلباش

در خاتمه ضمن سپاسگزاری از شما دانش‌پژوه گرامی درخواست می‌نماید با مراجعه به آدرس dibagaran.mft.info (ارتباط با مشتری) فرم نظرسنجی را برای کتابی که در دست دارید تکمیل و ارسال نموده، انتشارات دیباگران تهران را که جلب رضایت و وفاداری مشتریان را هدف خود می‌داند، یاری فرمایید.

امیدواریم همواره بهتر از گذشته خدمات و محصولات خود را تقدیم حضورتان نماییم.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران
bookmarket@mft.info

با سپاس از پدر و مادر عزیزم بخاطر زحمات و مهر بی دریغشان...
این کتاب را به همسر عزیزم و دخترم، نیکی، که در زمان نگارش این
متن، بی صبرانه برای ورودش به کانون گرم خانواده لحظه شماری
میکنیم، تقدیم می کنم.

❖ مقدمه مولف

از سال ۱۹۷۰ به بعد که به تدریج هکرها در معنای امروزی، متولد شدند، تا به الان، دنیای دیجیتال، فناوری‌های مختلفی را به خود تجربه کرده است که هرکدام از آن‌ها در طول این دوران یا جایگزین تکنولوژی‌های بهینه‌تر شدند و یا در مسیر تکامل خود گام برداشته‌اند. اما در این مسیر همواره رشد و خدمت به بشر مد نظر نبوده است و به موازات آن اهداف و اقداماتی در جهت سوءاستفاده از این تکنولوژی‌ها برای مقاصد شخصی، سیاسی، اقتصادی، فرهنگی و... نیز متولد شده و رشد کرده‌اند. در چنین شرایطی باید نه فقط صرفاً به فکر توسعه تکنولوژی‌ها و محصولات جدیدتر بود بلکه محافظت از آن‌ها نیز به مراتب در جایگاهی بالاتر از آن‌ها می‌تواند قرار داشته باشد؛ چراکه در صورت دسترسی‌ها غیرمجاز و سوءاستفاده‌های احتمالی از پیشرفت‌های حاصله در دنیای شبکه و تکنولوژی نه تنها زندگی بهتر را رقم نخواهد زد بلکه تاثیرات ناشی از سوءاستفاده‌های انجام شده، شرایط فعلی را نیز در مخاطره قرار خواهد داد. مطالعه این کتاب برای علاقه‌مندان به امنیت اطلاعات و همچنین کارشناسانی که تصمیم به فعالیت در حوزه امنیت شبکه و اطلاعات را دارند، توصیه می‌شود.

در این کتاب سعی شده است تا به هر دو وجه شبکه و امنیت پرداخته شود؛ به این معنا که ضمن آشنایی با مولفه‌هایی که نقش اساسی در شبکه را دارند، به نحوه ایمن کردن آن‌ها نیز به‌عنوان اصل موضوع، اشاره شده است. این مولفه‌ها شامل بخش‌های مختلفی مانند فایروال‌ها، آنتی‌ویروس‌ها، فایل‌های حساس، منابع عملیاتی، تهدیدها، حملات، رمزنگاری، مهندسی اجتماعی و... که می‌توانند در یک شبکه سازمانی وجود داشته باشند و یا اثرات خود را نشان دهند، است. علاوه بر این بیان مفاهیم پایه‌ای و اصلی در دنیای امنیت اطلاعات و تبیین آن‌ها نیز یکی از اهداف این کتاب بوده است که در متن کتاب به‌خوبی به آن پرداخته شده است.

پایه اصلی مطالب این کتاب مفاهیم ارائه شده در نسخه اصلی کتاب security+ از موسسه EC-Council بوده که به زبان فارسی بیان شده است. هدف از ترجمه آن، انتقال مفاهیم موجود به زبان گویاتر برای فارسی‌زبانان بوده است. ضمن آن که هدف از ارائه این کتاب، ترجمه آن بوده است اما سعی شده است تا اثرات هر دو وجه زبانی تحت تاثیر یکدیگر قرار نگیرند.

با توجه به آن که بسیاری از مفاهیم و عبارات به‌صورت تخصصی و در فرمت اصلی‌شان در دنیای شبکه بیان می‌شوند، سعی شده در مواجهه با آن‌ها ترجمه لغوی و یا قرابتی تا حد امکان صورت نگیرد و یا در صورت ترجمه، معادل استاندارد آن‌ها در باورقی بیان شود. علاوه بر این، از آنجایی که ترجمه برخی تیتراها ممکن بود مفهوم اصلی را نرساند و یا از زیبایی بیان آن بکاهد، تصمیم بر آن شد تا عبارات تیتراها در این کتاب با همان فرمت زبان اصلی باشد و معنا و توضیح آن‌ها در ادامه متن بیاید.