

سیستم های کامپیوتری امن

تالیف:

فاطمه صالح احمدی

فاطمه حاجی علی عسگری

سرشناسه :
عنوان و نام پدیدآور :
مشخصات نشر :
مشخصات ظاهری :
شابک :
وضعیت فهرست نویسی :
فایا :

صالح احمدی، فاطمه، ۱۳۵۳ -
سیستم‌های کامپیوتری امن/ فاطمه صالح احمدی، فاطمه
حاجی‌علی‌عسگری.
تهران: نشر پونه، ۱۳۹۷.
۳۳۰ ص.: مصور، جدول، نمودار.
978-600-6681-62-7
فیبا

یادداشت :
موضوع :
موضوع :
موضوع :
موضوع :
شناسه افزودن :
رده‌بندی کنگره :
رده‌بندی دیویی :
شماره کتابشناختی ملی :

کتابنامه :
کامپیوترها -- ایمنی اطلاعات
Computer security
کامپیوترها -- راهنمای آموزشی
Computers -- Study and teaching
حاجی‌علی‌عسگری، فاطمه، ۱۳۵۳ -
۱۳۹۷ س ۹/ص ۶/۹ QAV۶
۰۰۵/۸
۵۳۸۱۷۶۱

خ طالقانی شرقی - خ جهان - ساختمان پونه - شماره ۶ - طبقه سوم



نشر پونه تلفن ۷۷۶۰۵۷۹۸

نام کتاب :
مؤلف :
ناشر، صفحه‌آرایی :
نوبت چاپ :
لیتوگرافی، چاپ، صحافی :
شمارگان :
قیمت :
شابک :

سیستم‌های کامپیوتری امن
فاطمه صالح احمدی، فاطمه حاجی‌علی‌عسگری
پونه
اول ۱۳۹۷
پیمان نو اندیش
۱۰۰۰ جلد
۲۵۰۰۰۰ ریال
۷ - ۶۲ - ۶۶۸۱ - ۶۰۰ - ۹۷۸

فهرست

فصل اول	۳۲
مقدمه ای بر معماری و امنیت کامپیوتر، مدارات منطقی، زبان اسمبلی و سستم عامل	۳۲
مقدمه	۳۳
تعریف کامپیوتر	۳۳
اجزاء کامپیوتر	۳۳
معماری کامپیوتر	۳۵
معماری کامپیوتر داروین	۳۵
معماریفون نیومن	۳۶
ایرادات معماری نیومن	۳۶
طبقه بندی فلین (Flynn)	۳۸
وسایل ورودی/خروجی و واسط شبکه	۳۹
تعریف سخت افزار	۴۰
اجزای تشکیل دهنده سخت افزار	۴۱
۱- دستگاه های ورودی یا واحد ورودی (Input Unit)	۴۱
۲- دستگاه های خروجی یا واحد خروجی (Output Unit)	۴۱
۳- واحد پردازش مرکزی	۴۱
۴- حافظه (Memory or Storage)	۴۱

۴۲	 دستگاه‌های ورودی و خروجی
۴۳	 DMA
۴۶	 وظایف رجیسترها
۴۶	 واکنشی
۴۶	 Decode یا کدگشائی دستورالعمل‌ها
۴۷	 Execute یا اجرای دستورات
۴۷	 انواع رجستر در پردازنده
۴۷	 PC
۵۱	 Data رجستر
۵۱	 وقفه یا Interrupt
۵۱	 مکانیسم وقفه
۵۳	 دسته بندی وقفه‌ها
۵۳	 وقفه‌های داخلی
۵۳	 وقفه‌های خارجی
۵۳	 وقفه‌های نرم افزاری
۵۳	 مثال هایی از انواع وقفه‌ها
۵۴	 وقفه‌های زمان سنج (Timer)
۵۴	 وقفه‌های I/O
۵۴	 وقفه‌های نقص سخت افزار یا وقفه‌های (Machine Check)
۵۴	 وقفه Super Visor Call

۵۴	وقفه Restart
۵۴	وقفه نرم افزار
۵۵	Power failure
۵۵	Buffer Overflow
۵۶	Buffer Underflow
۵۷	Exceptions یا استثناءها
۵۸	ورودی - خروجی برنامه ریزی شده
۵۹	IEEE1394 و USB
۶۰	نسل های USB
۶۰	USB 2
۶۱	USB 3
۶۲	انواع پورت های USB
۶۲	USB-type A
۶۲	USB-type B
۶۳	Mini& Micro USB-type A and B
۶۵	مزیت های پورت USB
۶۵	IEEE1394
۶۷	Hot Plug
۶۸	Hot Swap
۶۸	کارت واسط شبکه
۶۹	کارت شبکه از منظر سخت افزاری
۶۹	Wired
۷۰	سرعت انتقال کارت های شبکه

۷۲	 واسطه های KVM
۷۲	 صفحه کلید
۷۲	 انواع کلیدهای صفحه کلید
۷۸	 انواع صفحه کلید
۷۸	 صفحه کلید مخصوص تایپ (Office)
۷۸	 صفحه کلید مالتی مدیا
۷۸	 صفحه کلید چند منظوره
۷۹	 کداسکی
۷۹	 انواع کداسکی
۷۹	 Mouse
۸۰	 انواع ماوس و نحوه کار آن
۸۰	 ماوس نوری یا لیزری
۸۲	 ماوس تویی یا غلتکی
۸۳	 کارت گرافیک ویدیویی
۸۴	 DVI
۸۵	 HDMI
۸۷	 VGA
۸۸	 نکات امنیت I/O
۸۹	 ورودی / خروجی حافظه ای و ورودی / خروجی درگاهی
۹۱	 فصل دوم: واحد پردازش مرکزی یا CPU و گذرگاه های آن
۹۲	 تعریف پردازنده

۹۲		نسل پردازنده
۹۳		علل بوجود آمدن پردازنده ها
۹۴		کار پردازنده
۹۶		زبان اسمبلی
۹۸		انواع پردازنده ها از نظر ساختار دستورالعمل
۹۹		اجزای داخل پردازنده
۱۰۰		واحد حسابات و منطق
۱۰۰		واحد پردازش اعشاری
۱۰۲		انواع کامپیوتر
۱۰۳		علل پیشرفت تکنولوژی کامپیوتر
۱۰۴		Mainframe
۱۰۴		Minicomputer
۱۰۴		کامپیوترهای رومیزی
۱۰۶		Internet
۱۰۶		Cell phone
۱۰۶		سرویس دهنده ها
۱۰۶		مشخصات سرورها
۱۰۷		دو نقش اساسی سرورها
۱۰۷		کامپیوترهای همراه یا جاسازی شده
۱۰۸		مجموعه دستورالعمل ها یا ISA
۱۰۹		کلاس های ISA

- ۱۰۹..... کدگذاری یک ISA
- ۱۱۰..... اجزای دستورالعمل ها
- ۱۱۲..... انواع دستورالعمل های حافظه و رجیسترها
- ۱۱۳..... کپی کردن بیت ها
- ۱۱۳..... دستورالعمل های منطقی
- ۱۱۳..... براساس بیت منطقی (NOT, AND, OR, XOR)
- ۱۱۳..... jump یا پرش
- ۱۱۳..... jump
- ۱۱۳..... jmp target
- ۱۱۴..... دستورالعمل های MOV
- ۱۱۵..... دستورالعمل های stack یا پشته
- ۱۱۵..... PUSH
- ۱۱۶..... قرار دادن همه رجیسترها به طور همزمان در پشته
- ۱۱۶..... POP
- ۱۱۶..... POPA
- ۱۱۶..... دستورات شیفت
- ۱۱۷..... شیفت منطقی
- ۱۱۸..... شیفت حسابی یا محاسباتی
- ۱۱۹..... شیفت چرخشی
- ۱۲۳..... دستور Call
- ۱۲۳..... دستور Return

۱۲۳.....	دستورات حلقه
۱۲۳.....	Zero Flag یا Zflag
۱۲۳.....	LOOP
۱۲۵.....	امنیت پردازنده
۱۲۷.....	ملاحظات امنیتی پردازنده
۱۲۷.....	تحلیل کانال جانبی
۱۲۸.....	Tamper-Resistant cpu
۱۲۹.....	پردازنده مجاز
۱۳۰.....	ویژگی های VM
۱۳۱.....	تعریف گذرگاه یا Bus
۱۳۲.....	انواع گذرگاه
۱۳۲.....	پهنای باند
۱۳۳.....	گذرگاه آدرس
۱۳۳.....	گذرگاه کنترل
۱۳۴.....	سیگنال های کنترلی مربوط به وقفه
۱۳۴.....	سیگنال های کنترلی مربوط به کنترل گذرگاه
۱۳۵.....	اجزای یک گذرگاه کنترلی
۱۳۵.....	تقسیم بندی گذرگاه ها از نقطه نظر داخلی یا خارجی بودن
۱۳۵.....	داخلی یا محلی یا Local یا Internal
۱۳۵.....	خارجی یا External

۱۳۵.....	ارتباط موازی یا parallel
۱۳۶.....	انواع ارتباط و پورت ها
۱۳۶.....	Parallel Port
۱۳۸.....	Serial Port
۱۴۰.....	انواع ارتباط بین فرستنده و گیرنده در روش انتقال سریال
۱۴۰.....	روش یک طرفه ساده یا Simplex
۱۴۰.....	روش نیم در طرفه یا Half Duplex
۱۴۱.....	روش دو طرفه یا Full Duplex
۱۴۱.....	روش های انتقال داده های سریال
۱۴۱.....	سنکرون
۱۴۱.....	آسنکرون
۱۴۳.....	تفاوت ارتباط سریال سنکرون و آسنکرون
۱۴۳.....	Handshaking یا دست تکانی
۱۴۴.....	تفاوت ارتباط سریال و موازی
۱۴۵.....	پردازنده های دو هسته ای یا Dual Core
۱۴۷.....	ملاحظات امنیتی گذرگاهها
۱۴۷.....	غیر فعال کردن پورت ها از دیوایس Manager
۱۴۸.....	Dual گذرگاه Interface
۱۴۸.....	Dual Channel Architecture
۱۴۹.....	Triple Channel Architecture
۱۵۰.....	فصل سوم: زبان اسمبلی و سیستم عامل و مدارات منطقی

۱۵۱	 مقدمه
۱۵۱	 تعریف زبان اسمبلی
۱۵۲	 تفاوت اسمبلی با زبان ماشین
۱۵۳	 شباهت های زبان ماشین و زبان اسمبلی
۱۵۳	 سیستم عامل
۱۵۵	 انواع ، سیستم عامل
۱۵۶	 سیستم عامل بلا درنگ
۱۵۶	 سیستم های یجیتال
۱۵۹	 اصول جبر بول
۱۶۱	 تقدم عملگر ها در جبر بول
۱۶۱	 قوانین دموورگان
۱۶۱	 محاسباتی و تریبی
۱۶۲	 FPGA
۱۶۴	 گیت های منطقی
۱۶۶	 جداول درستی (Truth Table)
۱۶۷	 جدول کارنو
۱۶۹	 کد گری
۱۷۰	 مینترم
۱۷۰	 ماکستریم
۱۷۰	 MSOP و MPOS

۱۷۱	 don't-care و حالات
۱۷۱	 Numbering System یا سیستم اعداد
۱۷۳	 روش تقسیم‌های متوالی بر ۲
۱۷۳	 سیستم شماره‌گذاری دهدهی
۱۸۴	 تبدیل BCD به دهدهی
۱۸۷	 Accessing Direct مکان‌های مستقیم یا
۱۸۷	 آدرس‌های غیر مستقیم
۱۸۸	 Stack یا پشته
۱۸۹	 تفاوت پشته و حافظه
۱۹۰	 اجزای برنامه
۱۹۱	 انواع برنامه‌های فرعی
۱۹۱	 توابع آماده (Supplied Functions)
۱۹۱	 زیر روال‌ها (Procedure)
۱۹۱	 انواع زیر برنامه
۱۹۱	 Intrasegment یا داخلی
۱۹۲	 Intersegment یا خارجی
۱۹۲	 Near call
۱۹۲	 Far call
۱۹۳	 Stack Protection
۱۹۳	 کرنل یا هسته
۱۹۴	 BIOS یا سامانه ورودی/خروجی پایه‌ای

۱۹۵	وظایف بایوس
۱۹۵	POST
۱۹۵	درايوه‌های بایوس
۱۹۵	راه اندازی سیستم عامل
۱۹۶	فعال کردن بایوس سایر قطعات
۱۹۷	کنترل قطعات سخت افزاری
۱۹۷	Boot strap
۱۹۷	Boot Loader
۱۹۷	Coprocessor
۱۹۹	فصل چهارم: معماری کامپیوتر
۲۰۰	مقدمه
۲۰۱	سیر تکامل معماری کامپیوتر
۲۰۲	پردازش فراگیر یا Ubiquitous Computing
۲۰۳	Multiprocessor ها یا چند پردازندگی
۲۰۴	Multiprocessor
۲۰۸	پردازنده‌های چند هسته‌ای
۲۱۰	معماری سیستم های چند هسته‌ای
۲۱۱	چند نخه یا Hyperthreading
۲۱۱	نخ یا Thread
۲۱۲	تک نخه
۲۱۲	چند نخه یا Multithreading

۲۱۵	پایلاین یا موازی سازی
۲۱۷	انواع هازاردها
۲۱۸	هازاردهای ساختاری
۲۲۱	هازارد های داده ای
۲۲۵	شگرد پیش فرستادن (هدایت رو به جلو)
۲۲۵	مرآحل Forwarding
۲۳۱	هازاردهای کنترلی
۲۳۲	متوقف کردن یا Stall دادن
۲۳۴	پیش بینی رش Branch prediction
۲۳۵	پیش گویی به روش ایستای Static
۲۳۵	پیش گویی به روش پویای Dynamic
۲۳۶	راه حل هازاردهای کنترلی
۲۳۶	delayed decision
۲۳۷	زمان بندی پویا
۲۳۸	مزایا و معایب زمان بندی پویا
۲۳۸	مشکلات ناشی از اجرای خارج از ترتیب دستورات برنامه
۲۳۹	Dynamically- scheduled پایلاین
۲۴۰	Static- scheduling پایلاین
۲۴۶	حافظه نهان یا کش
۲۴۶	انواع کش

۲۴۶.....	Caching	مبانی
۲۵۰.....	cache با حافظه رجیستر در پردازنده	فرق بین حافظه
۲۵۰.....	نحوه کار حافظه کش	
۲۵۱.....	مبانی عملیاتی کش	
۲۵۵.....	Cash Mapping Policy	
۲۵۵.....	Direct Map	نگاشت مستقیم یا
۲۶۱.....	MISS	انواع و علت های
۲۶۱.....	Compulsory	اجباری
۲۶۱.....	Capacity	ظرفیت یا
۲۶۲.....	Conflict	
۲۶۲.....	Conflict Misses	انواع
۲۶۲.....	Eight way	
۲۶۲.....	Four way	
۲۶۲.....	2-way	
۲۶۲.....	One-way	
۲۶۳.....	روش های بهینه سازی کارایی کش	
۲۷۸.....	blockهای جدید در کش	نحوه جایگذاری
۲۷۸.....	Write-back Policy	
۲۷۹.....	Write-through Policy	
۲۸۰.....	واقعیت افزوده	
۲۸۱.....	تفاوت واقعیت افزوده و واقعیت کامپیوتری	
۲۸۳.....	محاسبات سیار	

۲۸۴.....	شبکه های محاسباتی یا Grid Computing
۲۸۵.....	محاسبات ابری یا Cloud Computing
۲۸۵.....	تعریف رایانش ابری
۲۸۸.....	نمونه هایی از سرویس های مبتنی بر پردازش ابری
۲۸۸.....	Evernote
۲۸۸.....	Dropbox
۲۸۹.....	PandaCloudAntivirus
۲۸۹.....	GoogleDocs
۲۹۰.....	تاریخچه سرویس های ابری
۲۹۱.....	مدل های بکارگیری رایانش ابری
۲۹۱.....	ابزارهای عمومی
۲۹۱.....	ابزار خصوصی
۲۹۱.....	ابزار ترکیبی
۲۹۲.....	مدل های ارائه خدمات در رایانش ابری
۲۹۲.....	زیر ساخت به عنوان خدمت
۲۹۲.....	بستر به عنوان خدمت
۲۹۳.....	نرم افزار به عنوان خدمت
۲۹۳.....	مزایای برجسته رایانش ابری
۲۹۶.....	چالش های رایانش ابری
۲۹۷.....	ملاحظات امنیتی در ابر
۳۰۲.....	محاسبات اینترنت یا Internet Computing

- ۳۰۴..... مجازی سازی یا virtualization
- ۳۰۷..... مزایای مجازی سازی
- ۳۰۷..... کامپیوترهای DNA
- ۳۱۱..... فصل پنجم: امنیت سیستم های کامپیوتری
- ۳۱۲..... امنیت اطلاعات
- ۳۱۵..... بررسی کلی امنیت کامپیوتر
- ۳۱۷..... ضریب e-حکد یا work factor
- ۳۱۸..... مراحل اولیه ایجاد امنیت در شبکه
- ۳۱۸..... سیاست امنیتی
- ۳۲۰..... رمز عبور
- ۳۲۲..... ایجاد محدودیت در برخی از سمات سیستم الکترونیکی
- ۳۲۳..... بایبندی به مفهوم کمترین امتیاز
- ۳۲۴..... ممیزی برنامه ها
- ۳۲۵..... چاپگر شبکه
- ۳۲۵..... تست امنیت شبکه
- ۳۲۵..... هک (Hack)
- ۳۲۵..... انواع هکرها
- ۳۲۶..... انواع هکرها از منظر مهارت، دانش و تجربه
- ۳۲۶..... هکرها نوبا یا نوب (Newbie ، Noob، Neophyte) یا مبتدی
- ۳۲۶..... بچه اسکریپتی ها (Script Kiddy)

- هکرهاي خبره-نخبه (Elite) ۳۲۷
- هکرهاي کلاه سفيد (White Hat) ۳۲۸
- هکرهاي کلاه صورتي ۳۲۸
- هکرهاي کلاه سياه (Black Hat) ۳۲۸
- هکرهاي کلاه خاکستري (Grey Hat) ۳۲۹
- هکرهاي کلاه قرمز (Red Hat) ۳۲۹
- هکرهاي کلاه آبي (Blue Hat) ۳۲۹
- هک نيويست (Hacktivist) ۳۳۰
- فريکتر (Pirater) ۳۳۰
- هکر علمي (Academic) ۳۳۱
- هکر انتحاري (Suicide) ۳۳۱
- متدولوژي هاي معمول حملات هکري ۳۳۱
- متدولوژي انجام حملات هکري ۳۳۲
- مقايسه مثلث امنيت اطلاعات يا CIA و مثلث هکري يا DDD ۳۳۴
- افشا سازي ۳۳۵
- تست جعبه سفيد ۳۳۸
- تست جعبه سياه ۳۳۸
- تست جعبه خاکستري ۳۳۹
- تست نفوذ پذيري ۳۴۰
- انواع تست آسيب پذيري (تست نفوذ) و ارزيابي امنيتي ۳۴۰

۳۴۱		بازیابی رمز عبور
۳۴۱		شکستن پسورد به صورت دستی
۳۴۱		کرم کردن رمز عبور به روش GPU
۳۴۲		روش Brute Force Password Cracking
۳۴۳		حمله Dictionary Attack
۳۴۴		جدول نگین کمان
۳۴۶		اصول شبکه و لایه بندی (مرور مدل OSI و TCP/IP)
۳۴۶		Tcp/ip
۳۴۷		لایه ها در مدل TCP/IP
۳۴۸		OSI
۳۴۹		لایه های OSI
۳۵۰		پروتکل های پشته ای
۳۵۱		پروتکل یا سرویس های شبکه
۳۵۲		ARP
۳۵۲		DHCP
۳۵۲		DNS
۳۵۳		FTP
۳۵۳		SMB
۳۵۴		پروتکل SNMP
۳۵۴		انواع حملات و تهدیدات
۳۵۷		مفاهیم و اصطلاحات اولیه
۳۵۷		حمله (Attack)

۳۵۷		رخنه (Breach)
۳۵۷		نفوذ (Intrusion)
۳۵۷		آسیب پذیری (Vulnerability)
۳۵۷		دسته بندی حملات
۳۵۸		تهدیدات
۳۵۸		حملات لایه کاربرد
۳۵۹		Exploitation
۳۵۹		سرمیز بافر یا پشته
۳۶۰		Malware
۳۶۰		انواع malware
۳۶۰		اسب تروا
۳۶۱		ویروس
۳۶۱		روش انتشار ویروس ها
۳۶۱		بوت سکتور
۳۶۲		انواع ویروس ها
۳۶۲		ویروس های پنهانی یا Stealth Virus
۳۶۲		Memory Resident Virus و Macro Virus
۳۶۳		Polymorphic Virus یا چند ریختی
۳۶۳		کرم ها یا Worms
۳۶۶		DDOS
۳۶۶		روش های ایجاد کانال های پنهان

۳۶۶	از طریق بسته های ICMP
۳۶۶	استفاده از Web Browsing Shell ها به صورت معکوس
۳۶۷	استفاده از Telnet Shell ها به صورت معکوس
۳۶۸	اسب تروا
۳۶۸	انواع اسب تروا
۳۶۹	Sniffer ها
۳۷۰	دوروش هم برای sniffing و استراق سمع یا Eavesdropping
۳۷۰	تهدیدات و حملات لایه فیزیکی، لایه پیوند داده ها، شبکه و انتقال
۳۷۰	خواباندن شبکه در اثر اشباع کابل
۳۷۱	سوییچ های غیر فعال یا Passively
۳۷۱	پورت های فعال
۳۷۱	Mac flooding یا اشباع سوییچ
۳۷۲	ARP spoofing
۳۷۳	حمله DNS Spoofing
۳۷۳	عملکرد سوییچ های فعال
۳۷۳	روش های کلی مقابله با حملات
۳۷۴	حملات لایه دو
۳۷۶	تهدیدات لایه دو
۳۷۶	VLAN Hopping
۳۷۶	MAC Flooding
۳۷۸	DHCP Attacks

۳۷۸.....	Rogue DHCP و DHCP Starvation
۳۷۹.....	ARP Table Poisoning
۳۷۹.....	ARP Table Poisoning : شکل ۹۱
۳۸۰.....	Spoofing Attacks
۳۸۰.....	MAC Spoofing
۳۸۱.....	MAC Spoofing : شکل ۹۳
۳۸۲.....	IP Spoofing
۳۸۳.....	STP Attacks
۳۸۴.....	CDP Attacks
۳۸۵.....	CDP Attacks : شکل ۹۶
۳۸۵.....	راهکارهای جلوگیری از حملات لایه دو
۳۸۵.....	VLAN Hopping : حملات از
۳۸۶.....	Trunk Port
۳۸۷.....	Native VLAN پورت
۳۸۷.....	راهکارهای جلوگیری از MAC Attacks
۳۸۸.....	DHCP Attacks از جلوگیری
۳۸۸.....	راهکارهای جلوگیری از ARP Attacks
۳۸۸.....	DAI (Dynamic ARP Inspection)
۳۸۹.....	IP/MAC Spoofing Attacks از جلوگیری
۳۸۹.....	IP Source Guard
۳۸۹.....	IPSG (IP Source Guard)
۳۸۹.....	راهکارهای جلوگیری از حملات مبتنی بر STP
۳۸۹.....	Root Guard

۳۹۰.....	BPDUGuard
۳۹۳.....	راهکارهای جلوگیری از حملات مبتنی بر CDP
۳۹۳.....	حملات لایه شبکه
۳۹۳.....	IP spoofing
۳۹۳.....	Ping Of Death
۳۹۳.....	JOLT2
۳۹۴.....	Tear drop
۳۹۴.....	حملات لایه انتقال
۳۹۴.....	Syn flooding
۳۹۴.....	Fraggle
۳۹۵.....	Land
۳۹۵.....	Latteria
۳۹۵.....	ICMP Smurfing
۳۹۶.....	سایر حملات متداول
۳۹۶.....	حمله جلوگیری از سرویس (DOS)
۳۹۷.....	استراق سمع
۳۹۷.....	تحلیل ترافیک
۳۹۷.....	دستکاری پیام ها و داده ها
۳۹۷.....	جعل هویت
۳۹۸.....	Back Door Attack
۳۹۸.....	Spoofing

۳۹۸		Man in the Middel Attack
۳۹۹		Replay
۳۹۹		TCP/IP Hijacking
۴۰۰		DNS Poisoning
۴۰۰		Engineering Social یا اجتماعی
۴۰۰		Birthday
۴۰۰		Software Exploitation
۴۰۱		War Dialing
۴۰۱		Smurfing
۴۰۱		Sniffing
۴۰۲		پویش پورت
۴۰۲		(Fragmentation Attack) حملات قطعه قطعه کردن
۴۰۲		دسترسی فیزیکی
۴۰۳		SQL حملۀ تزریق
۴۰۳		Phishing حملۀ
۴۰۴		HOAX (گول زنگ‌ها)
۴۰۶		Sulfnbk یک ویروس، یک شوخی و یا هردو
۴۰۷		پیام SOAP
۴۱۰		(Wrapping Attack) SOAP حملۀ بسته پیام
۴۱۰		SOAP در XPATH حملۀ تزریق
۴۱۱		Oauth پروتکل
۴۱۲		DRAM سرقت اطلاعات حساس از ماشین مجازی با حملات آدرس دهی

۴۱۴.....	جاسوس افزار اندرویدی Exasp
۴۱۶.....	کاو کتیف
۴۱۸.....	آسیب پذیری ION با نام (Drammer AKA)
۴۱۸.....	تروجان بانگی با نام Svpeng
۴۱۹.....	نرم افزارهای کاربردی در حملات
۴۱۹.....	Back Orifice
۴۱۹.....	Net
۴۱۹.....	(Sub 7) SubSeven
۴۲۰.....	(Virtual Network Computing)VNC
۴۲۰.....	PCAnywhere
۴۲۱.....	Nmap
۴۲۱.....	John The Ripper
۴۲۱.....	Aircrack-ng
۴۲۱.....	Services Terminal
۴۲۳.....	انواع مشکلات سیستم های دارای فایروال
۴۲۳.....	راهکارهای حفظ امنیت سخت افزار
۴۲۳.....	OTP یا رمزهای یک بار مصرف (One Time Password)
۴۲۴.....	کاربردهای OTP
۴۲۶.....	فناوری RFID
۴۲۸.....	مزایای RFID
۴۲۹.....	منابع

مقدمه مؤلف

آلبرت انیشتین: "به خاطر داشته باشید هر چه در مدارس خود یاد می گیرید نتیجه کار نسل های بیشماری است که در اثر کوشش آرزومندانه همه مردم جهان به ثمر رسیده است و سپرده ای است در دست شما، از آن استفاده ببرید و به آن بیفزایید تا روزی که آنرا با کمال امانت و وفاداری به فرزندانتان بسپارید. • بزرگ ترین فناوری که در طول تاریخ توانسته است اطلاعات مورد نیاز صنعت، بازرگانی، پژوهش و قشرهای مختلف جامعه را در کمترین زمان فراهم ساخته، مرزهای جغرافیایی را درهم نوردیده و ملت ها را در یک جامعه جهان گرا هم آورد آن ها را به سوی دهکده جهانی سوق دهد اینترنت می باشد. فناوری اینترنت مانند سایر نوآوری های دیگر همچون سکه دو رو است: فرصت و تهدید. اگر به همان اندازه که به توسعه و فراگیر شدن آن توجه می شود به مصدق امنیتی آن پرداخته نگردد می تواند به یک فاجعه بزرگ مبدل شود. منابع آکادمی علمی به زبان فارسی در زمینه امنیت سیستم های کامپیوتری و مخاطرات متدنیهای سایبری و نیاز شدید دانشجویان به این دست داده ها ما را بر آن داشت در زمینه آسان سازی فرآیند علم ورزی قلمی و قدمی برداشته و این کتاب را تقدیم حضور نماییم.

فاطمه صالح احمدی

فاطمه حاجی علی عسگری