

CDD 005.8

نوع 370

069206

③



المدخل الى أمن المعلومات والحاسوب

عبيد صالح عبد العزيز

الطبعة الأولى

2024



المحتويات

15تهديد
	الفصل الاول : مقدمة إلى أنظمة أمن الحاسوب
	Introduction to Computer System Security
211-1 مقدمة عامة Introduction
261-2 المكونات الأساسية لأمن الحاسوب ونظامه
	Basic Components of Computer Security
341-3 التهديدات Threats
391-4 أهداف الأمن Goals of Security
391-5 الحاجة إلى الأمن
411-6 القضايا الأساسية للأمن على الإنترنت
471-7 أنواع التهديدات والهجوم عبر الحاسوب والإنترنت
501-8 الأنواع المختلفة للتهديدات والهجمات
521-9 قرصنة رفض الخدمة الموزعة
	Distributed Denial of Service Attacks (DDoS)
541-10 الكود الفيروسي الإرهابي (الدودة وأحصنة طروادة)....
571-11 النقل الإلكتروني الآمن SET وطبقة المنفذ الآمن SSL .
601-12 بروتوكولات نقل النصوص المتشعبة الآمنية SHTTP ...
601-13 الشهادات الرقمية Digital Certificates
611-14 أنظمة الكشف عن الدخلاء IDS والشبكات الخاصة الافتراضية VPN
641-15 ضبط كلمات المرور
651-16 أهداف الحماية

الفصل الثاني: أنظمة الحماية الحيوية (البيولوجية)

Biologic Protection Systems

- 71 أنظمة التحقق البيولوجية 1-2-1
- 76 Authentication Technologies: تقنيات التحقق 1-2-1
- 79 هدف وأداء القياسات البيولوجية 3-2-1
- Goal and Performance of Biometrics
- 81 Biometric System نظام القياسات البيولوجية 4-2-1
- 83 القضايا المتعلقة بتصميم وأداء النظام 5-2-1
- System Performance and Design Issues
- 85 Biometric Identification تعريف القياسات البيولوجية 6-2-1
- 86 Biometric Verification اثبات القياسات البيولوجية 7-2-1
- 87 Biometric Enrollment تسجيل القياسات البيولوجية 8-2-1
- 89 Biometric System أمنية نظام القياسات البيولوجية 9-2-1
- Security
- 89 Good Biometric القياس البيولوجي الجيد 10-2-1
- 91 The Common القياسات البيولوجية الاعتيادية 11-2-1
- Biometrics
- 102 قياسات بيولوجي أخرى 12-2-1
- 103 أسئلة الفصل

الفصل الثالث: تكنولوجيا شبكات الحاسوب والانترنت

Computer Networks & Internet Technologies

- 107 Introduction. المقدمة 1-3-1
- 108 Computer Network شبكة الحاسوب 2-3-1
- 111 Protocols البروتوكولات (أصول) الشبكات 3-3-1
- 117 Move Data Packets بروتوكولات نقل حزم البيانات 4-3-1

 Protocols data
117 5-3 عنوان الجهاز المادي Hardware Address
122 6-3 مشاكل طبقة IP
123 7-3 بروتوكولات السيطرة على الإرسال
	(TCP) Transmission Control Protocol
124 8-3 الأمن في بروتوكول TCP/IP
125 9-3 المنافذ ونقاط التوصيل. Ports and Sockets
126 10-3 بروتوكول نقل الملف (FTP) File Transfer Protocol
127 11-3 بروتوكولات نقل النص التشعبي
	(HTTP) Hypertext Transfer Protocol
127 12-3 أنواع الشبكات Types of Network
131 13-3 تقنيات ربط الشبكات Network Topologies
133 14-3 تهديدات الشبكات Threats in Networks
138 15-3 نموذج أمن الشبكات Model For Network Security
140 16-3 الشبكات اللاسلكية Wireless Networks

الفصل الرابع: نظام كشف التطفل

Intrusion Detection System (IDS)

147 1-4 المقدمة
148 2-4 المتطفلين Intruders
149 3-4 نظام كشف التطفل (IDS) Intrusion Detection System
151 4-4 تقنيات كشف التطفل Intrusion Detection Techniques
154 5-4 سيناريو التطفل Intrusion Scenario
157 6-4 لماذا نحتاج إلى كشف التطفل
160 7-4 كشف التطفل Intrusion Detection
164 8-4 مقارنة كشف الشذوذ مع إساءة الاستخدام

166Audit Records	9-4- سجلات التدقيق
169	Statistical Anomaly	10-4- كشف الشذوذ الإحصائي
	Detection
172	11-4- كشف التطفل المستند على القواعد
	Rule-Based Intrusion Detection	
175	Classification of Intrusion	12-4- أصناف كشف التطفل
	Detection
177	Distributed Intrusion detection	13-4- كشف التطفل الموزع
179	14-4- قارورة العسل Honey pots
الفصل الخامس: منطق البرامج التخريبية		
Viruses Logic		
187	1-5- مقدمة عامة Introduction
188	2-5- أحصنة طروادة Trojan Horses
189	3-5- فيروسات الحاسوب
192	4-5- ملوثات مقاطع التحميل
193	5-5- ملوثات البرامج التنفيذية Executable Infectors
194	6-5- الفيروس المتعدد التأثير Multipartite Viruses
194	7-5- فيروس تي أس آر TSR
194	8-5- فيروسات ستيلث Stealth Viruses
195	9-5- الفيروسات المشفرة Encrypted Viruses
196	10-5- دودة الحاسوب
196	11-5- البكتيريا والأرانب Rabbits and Bacteria
197	12-5- أنظمة الدفاع ضد الكود التخريبي Defenses

الفصل السادس : علم التشفير

Cryptography

- 203 المقدمة 1-6
- 206 Encryption Algorithms خوارزميات التشفير 2-6
- 209 Breakable Encryption التشفير القابل للحرق 3-6
- 210 Representation of Characters تمثيل الرموز 4-6
- 212 Symmetric Cipher التشفير المتناظر 5-6
- 215 Cryptanalysis تحليل النص المشفر 6-6
- 219 Substitution Cipher التشفير بطريقة التعويضية 7-6
- 220 The Caesar Cipher تشفير قيصر 1-7-6
- 223 التشفير بطريقة التعويض المتعددة الحروف 2-7-6
- Polyalphabetic Cipher
- 227 Vernam Cipher تشفير فيرنام 3-7-6
- 229 Hill Cipher تشفير هيل 4-7-6
- 231 Play Fair طريقة تشفير 5-7-6
- 234 ASCII نظام الاسكي 6-7-6
- 235 Multiplicative Cipher التشفير الضربي 7-7-6
- 236 Transposition Cipher التشفير الابدالي 8-6
- 237 Columnar Transposition الإبدال العمودي 1-8-6
- 239 Fixed Period طريقة تشفير الفترة الثابتة 2-8-6

الفصل السابع : أمن البيانات والرياضيات

Data Security and Mathematical

- 249 المقدمة 1-7
- 249 Prime Numbers الأعداد الأولية 2-7
- 250 القاسم المشترك الأكبر 3-7

Greatest Common Divisor(GCD)

252 4-7- المضاعف المشترك الأصغر

(LCM) Least Common Multiple

253 5-7- باقي القسمة Modular

256 6-7- دالة أويلر Euler Function

257 7-7- خوارزمية المعكوس Inverse Algorithm (inv)

259 8-7- خوارزمية الأسس السريعة

261 9-7- القوانين العامة لباقي القسمة

262 10-7- معكوس المصفوفة

266 11-7- الجذر الأولي Primitive root

الفصل الثامن: التشفير بالفتاح العام

Public Key Cipher

273 1-8- المقدمة

274 2-8- مبادئ شفرة المفتاح العام

277 3-8- تطبيقات نظام التشفير المفتاح العام

278 4-8- متطلبات شفرة المفتاح العام

279 5-8- خوارزمية شفرة المفتاح العام

284 6-8- إدارة المفاتيح Key Management

288 7-8- تبادل المفتاح بطريقة ديفي - هبمن

293 8-8- نابسك Knapsack cipher

296 9-8- اثبات صحة الرسالة Authentication Requirements

297 10-8- دالات إثبات الرسالة

298 11-8- إثبات أصالة الرسالة

الفصل التاسع: تشفير البيانات القياسي (DES)

309 1-9- متطلبات التشفير الآمن

- 310 Characteristics of "Good " Cipher الخصائص الشفرة الجيدة 2-9
- 312Confusion and Diffusion التشويش والانتشار 3-9
- 313Feistel Cipher Structure هيكله شفرة فيستال 4-9
- 316 DES))Data Encryption Standard التشفير القياسي للبيانات 5-9
- 316 1-5-9 نبذة تاريخية
- 318DES 2-5-9 نظام التشفير بـ
- 319 3-5-9 هياكل البيانات المستخدمة
- 319 Initial Permutation IP جدول التبدل الاولي 4-5-9
- 321 Expansion Permutation E جدول التوسيع 1-
- 322 PC-1 جدول اختيار 2-
- 323(Left Shift) LS جدول الإزاحة 3-
- 324 ... Permuted Choice-2 PC-2 جدول الترتيب الاختياري 4-
- 326 ... Substitution Boxes S-boxes صناديق التعويض 5-
- 327Permutation P جدول الترتيب 6-
- 331 Permutation inverse IP^{-1} جدول الترتيب الأولي المعكوس 7-
- 334 8- مثال تطبيقي
- 340 5-5-9 مواصفات الشفرة الكتلية المتناظرة المتقدمة
- 340The Avalanche Effect تأثير الانهيار 6-9
- 342DES 7-9 تكرار
- 342 Double DES التشفير المتكرر الثنائي 1-7-9
- 343Triple DEA التشفير المتكرر الثلاثي 2-7-9
- 345 3-7-9 خوارزمية تشفير البيانات الدولية
- 345 The International Data Encryption BLOWFISH بلو فيش 4-7-9

346 RC 5: 5-7-9 آر سي 5

347 CAST -128 128 -6-7-9 كاست

الفصل العاشر: دالة هاش

Hash Function

353 1-10 المقدمة

354 2-10 أمنية دالة هاش

356 3-10 دالة هاش البسيطة

357 4-10 خوارزمية ملخص الرسالة MD5

359 5-10 خوارزمية دالة هاش الأمانة Secure Hash Algorithm

..... (SHA)

361 6-10 خوارزمية RIPEMD-160

364 7-10 خوارزمية Hash Message Authentication Code

..... ((HMAC

369 أسئلة الفصل

الفصل الحادي عشر: التوقيع الرقمي وسياقات التحقق

Digital Signature and Authentication Protocol

373 1-11 مقدمة عامة

374 2-11 تعريف التوقيع الالكتروني الرقمي Digital Signature ..

378 3-11 التوقيع الرقمي المباشر Direct Digital Signature

380 4-11 التوقيع الرقمي المحكم Arbitrated Digital Signature ...

384 5-11 التوقيع الرقمي القياسي Digital Signature Standard ..

388 6-11 بروتوكولات التحقق من الهوية Authentication

..... Protocols

388 1-6-11 التحقق المتبادل من الهوية Mutual Authentication ...

391 2-6-11 التحقق ذو الاتجاه الواحد One-Way Authentication

391	7-11 - إدارة المفاتيح Key Management
393	8-11 - استخدام المفتاح العام لتوزيع المفاتيح السرية
394	أسئلة الفصل
الفصل الثاني عشر: أمانة الانترنت والبريد الالكتروني		
Internet and E-mail Security		
399	1-12 - المقدمة
400	2-12 - الشبكة العنكبوتية - الويب History of the world wide web
402	3-12 - قضية الأمن في الدفع المالي الالكتروني Security in e-payment
406	4-12 - معايير التصميم Design Standardization:
407	5-12 - أمن موقع الويب Web Site Security:
408	6-12 - تهديدات أمانة الويب Web Site Security Threats:
410	7-12 - أنواع التهديدات والهجوم عبر الانترنت
411	8-12 - الأنواع المختلفة للتهديدات عبر الانترنت
412	9-12 - الهجوم الغير فني: الهندسة الاجتماعية
416	10-12 - الهجوم التقني أو الفني
417	11-12 - حماية شبكات الانترنت و التجارة الالكترونية
417	1-11-12 - حماية وضبط تداول البيانات والتحقق من هوية المتصل
419	12-12 - أمن البريد الالكتروني
420	13-12 - تشفير البريد الالكتروني E-mail Encryption:
421	14-12 - كيف يعمل الخداع ؟ How Spoofing Works:
422	15-12 - كيف يعمل الفيروس في البريد الالكتروني
422	16-12 - برنامج Pretty Good Privacy PGP

425 أسئلة الفصل
	الفصل الثالث عشر: أمن التعليم الالكتروني
	E-Learning Security
429Introduction مقدمة عامة 1-13
431 أهمية التعليم الالكتروني 2-13
436 ما هو التعليم عبر الهاتف الخليوي المحمول 3-13
437 عوائق ومحددات التعليم الالكتروني 4-13
	Obstacles and Limitation of E-Learning
439 القضايا الأمنية للتعليم الالكتروني 5-13
442	Secure E-Learning نموذج أمن مثالي للتعليم الالكتروني 6-13
Model
445	Viewing e-courses آلية استعراض المساقات الالكترونية 7-13
446 آلية التوقيع الالكتروني في النظام 8-13
448	Secure m-phone learning نظام أممي للتعليم عبر الموبايل 9-13
 system

تمهيد

"يستطيع ثلاثة أشخاص أن يحافظوا على السرّ إذا وفقط إذا كان اثنان منهم متوفيان"

أديب غربي

إن هذا العصر الذي نعيش فيه يسمى في الوقت الحالي بعصر المعلومات، عصر الإنترنت، عصر الكمبيوتر، عصر المنظمات، عصر العولمة، عصر الاتصالات، عصر التغيير فكلّ شيء وكلّ فرد وكل مؤسسة قائمة على المعلومات، فالجامعات قائمة لنشر المعلومات وتعليمها، وكذلك المدارس، وكل المؤسسات التعليمية الأخرى، أيضاً فإن كل شخص في هذا العصر لا بد أن يكون لديه معلومات معينة حتى يستطيع أن يعايش عصره، فلا بد للسائق أن يكون لديه معلومات عن السيارة وصيانتها وعن العناوين والطرق وقوانين المرور وغيرها، وكذلك الطبيب والمهندس وكل المهن الأخرى، المؤسسات الخاصة والعامة كلها مبنية على تداول وتبادل المعلومات. ومع ذلك قال الله تعالى:

1- "وما أوتيتم من العلم إلا قليلاً"

2- "قل هل يستوي الذين يعلمون والذين لا يعلمون"

3- "أما يخشى الله من عباده العلماء"

لذا فإن المعلومات هي المقياس الذي نقيس به قوة الدولة والشعب والفرد، فمن يمتلك المعلومات في هذا العصر يمتلك القوة والمال والسيطرة والسلاح القوي الذي يوصل الشعوب إلى النصر أو الهزيمة والذي يوصل الأشخاص إلى تحقيق أهدافهم ويوصل الشركات إلى الريادة والسيادة والسيطرة على الأسواق فمن لديه العلم سوف يسيطر ويظهر على غيره ولو بعد حين.

بالإضافة إلى المعلومات الضخمة والتي يتم تبادلها تحتاج إلى أدوات وأجهزة تقوم بمعالجتها وتنظيمها وحفظها واسترجاعها عند الحاجة بالسرعة الممكنة