Π

[الذين آمنوا ولم يلبسوا إيمانهم بظلم أولئك لهم الأمن وهم مهتدون

صدق الله العظيم

الآية (82) من سورة الأنعام

الإهداء

إلى الصرحين العلميين التوأمين:

جامعة السودان للعلوم والتكنولوجيا (SUST)
وجامعة حضرموت للعلوم والتكنولوجيا (HUST)

إلى القائمين على إدارتيهما وتطويرهما
إلى الأساتذة والطلاب فيهما
إلى كل الشباب المتحمس للتقنية الحديثة

أهدي عملي المتواضع هذا

شكر وتقدير

الحمد لله رب العالمين والصلاة والسلام على أشرف الأنبياء والمرسلين وعلى آله وصحبه أجمعين، وبعد.

أحمد الله الذي أعانني على إتمام هذا البحث، ويسعدني أن أتقدم بالشكر الجزيل لكل من أسهم في إخراج هذه الرسالة وإتمامها على أحسن وجه. وأخص بالذكر أستاذي وأخي الدكتور أسامة عبدالوهاب ريس رئيس قسم الإلكترونيات بكلية الهندسة ورئيس مركز الحاسوب بصفته المشرف على هذه الرسالة على كل جهوده الكبيرة وتوجيهاته القيمة وسعة صدره خلال فترة الدراسة وحتى إخراجها على صورتها الحالية.

كما أتوجه بالشكر لأخي الدكتور يحيى عبدالله عميد كلية الحاسوب وتقانة المعلومات على ما قدمه من عون علمي صادق وتوجيهات أثرت البحث. وأخص بالشكر أيضاً كل العاملين في قسم الإلكترونيات بكلية الهندسة، ومركز الحاسوب بجامعة السودان للعلوم والتكنولوجيا.

كما أتوجه بالشكر لأساتذة قسم الرياضيات بكلية العلوم بجامعة السودان لتعاونهم معي في مناقشة الخلفية الرياضية لعلم التعمية (Cryptology) وخصوصاً الدكتور منصور الشيخ حسن.

كما أتوجه بالشكر للأخ أبوبكر شيخ رئيس مركز المعلومات بجامعة حضرموت للعلوم والتكنولوجيا على ما قدمه من معلومات وبيانات ومراجع ساعدت على إكمال البحث.

وفي الأخير أتوجه بالشكر والتقدير لكل من أسهم وساعد في إخراج هذه الدراسة مهما كانت درجة إسهامه.

والله الموفق ،،،

الباحث

ملخص الدراسة

يهدف هذا البحث لتقديم باقة متكاملة من المعلومات الأمنية التي يستطيع مستخدم التجارة الإلكترونية إستخدامها لتأمين موارده وثرواته على الإنترنت، وذلك بالتعرض لدراسة الإتجاهات المستقبلية في تقنيات أمن البيانات، والجهود المبذولة في مجالات تطوير المزايا الأمنية الداخلية في لغات الويب وجهود التطوير في هندسة البرمجيات وتقنيات كشف وتعقب الدخلاء.

وكذلك دراسة الجيل الجديد من مراسيم الإنترنت الأمنية المتعلقة بأمن المواقع التجارية والحساسة. ولإهتمامنا في موضوع البحث بعمليات التحويلات المالية على الإنترنت ركزنا على دراسة مرسومي طبقة المقابس الآمنة (SSL) ومرسوم الحركات المالية الآمنة (SET)، والتعرف على مزاياهما الأمنية، لمعرفة كيفية بناء الأنظمة المنيعة التي تصد أغلب الهجمات الموجهة.

وقد ثبت بالدراسة أن إستخدام اللغة العربية في تراسل البيانات عبر الشبكة يعزز من أمن التراسل لما تمتاز به من خصائص معلوماتية وتعموية جيدة، مثل معدل المعلومات والتكرارية ومعامل الصدفة ومقياس الخشونة وطول حد كسر التعمية مقارنة باللغة الإنجليزية.

أما منهجية البحث فقد إعتمدت على ثلاثة جوانب وهي: الجانب النظري وذلك بالرجوع الى المصادر العربية والأجنبية من كتب وبحوث ومقالات ودوريات ومواقع الإنترنت. ثم الجانب العملي وذلك لتطبيق هذه المفاهيم ببناء موقع حضرموت للأبحاث وأجرينا عليه بعض الإختبارات الأمنية وتم تسجيل النتائج المهمة. وأخيراً الجانب التحليلي وذلك بتحليل ومقارنتة النتائج مع نتائج دراسات سابقة للخروج باستنتاجات وتوصيات جديدة تثري موضوع البحث.

Abstract

This research aims to evaluate a complete security information that the user of e-commerce can use it to secure his source and wealths on internet, for the sake of studying prospective concepts in data security technique of exerted diligences in developing of the inner security protocols field in web language and diligences in developing programs of discovery technique engineer of following foreigners.

Also to study the security protocols, which related to the sensitive e-commerce .Our interested in this research about the financial transaction process on Internet .We concentrat on studying Security Sockets Layer SSL and Security Electronic Transmision SET .To know more about its security diligences so as to build invincible systems, to face most dispatched attack .

It was preved that using Arabic language in sending reports via web to reinforce from security in sending ,because it has a good cryptographic characteristics: like Entropy, Redundancy, Index of Coincidence, Roughness Factor, and Unicity Distance comparing to English language .

So the research methodology depends on three parts

1- observation part: therefore referring to Arabic and foreign refrences like books, researches, essays, periodicals and web sites .
2- Practical part: therefore to practise these concepts by building Hadhramout for researches web site . We underwent some secure tests, and registered an important results .
3- Analytic part: so as to analyse and compare the out results with the former studying of results to extract new commendations and deductions so as to enrich the topic of the research.

جدول الإختصارات

البيان	الإختصار	الرقم
Automated Clearing House	ACH	1
Authentication Head	AH	2
Active Server Pages	ASP	3
Business To Business	B2B	4
Business To Customer	B2C	5
Customer To Business	C2B	6
Customer To Customer	C2C	7

Certificate Authority	CA	8
Challenge Handshake Authentication Protocol	CHAP	9
Data Encryption Standard	DES	10
Digital Signature Algorithm	DSA	11
Digital Signature Standard	DSS	12
Electronic Data Interchange	EDI	13
Electronic Fund Transfers	EFT	14
Electronic Fund Transfer at Point Of Sale	EFTPOS	15
File Transfer Protocol	FTP	16
Gross Domestic Product	GDP	17
سلسلة ثابتة وقصيرة من الأحرف تولد عشوائياً من نص صريح وتعرف ببصمة الرسالة وهي أيضاً تعد دالة الإتجاه الواحد .	Hash	18
Hypertext Transport Protocol	HTTP	19
Internet Control Message Protocol	ICMP	20
International Data Corporation	IDC	21
Internet Service	IIS	22
Internet Messaging Access Protocol	IMAP	23
Internet Protocol	IP	24
Internet Protocol new generation	IP ng	25
Internet Protocol security	IP sec	26
Internet Protocol version 6	IP v6	27
Internet Service Provider	ISP	28
Integrity Service Digital Network	ISDN	29
Internet Task Engineering Force	ITEF	30
Key Exchange Algorithm	KEA	31
أشهر برنامج للتحقق من هوية مستخدمي الشبكة، والإسم عند اليونان عبارة عن حيوان خرافي متعدد الرؤوس .	Kerberos	32
Message Authentication Code	MAC	33
Message Digest Algorithm	MD5	34
Network File System	NFS	35
Non-Sufficient Fund	NSF	36
Password Authentication Protocol	PAP	37
Pretty Good Privacy	PGP	38
Post Office Protocol	POP3	39

Point to Point Tunneling Protocol	PPTP	40
Remote Authentication Dial-In User Service	RADIUS	41
Remote Access Server	RAS	42
Rivest & Shamir & Adleman	RSA	43
Secure Multi-purpose Internet Mail Extension	S/MIME	44
System Design Document	SDD	45
Secure Electronic Transactions	SET	46
Secure Hash Algorithm	SH-1	47
طريقة تشفير تقليدية بمفتاح متماثل	SKIPJAC	48
Simple Mail Transfer Protocol	SMTP	49
Simple Network Management Protocol	SNMP	50
System Requirements Specifications	SRS	51
Secure Sockets Layer	SSL	52
Transmission Control Protocol	TCP	53
Terminal Emulation Protocol	Telnet	54
Ticket Grant Server	TGS	55
Transport Layer Security	TLS	56
User Datagram Protocol	UDP	57
Unified Modeling Language	UML	58
Universal Resource Locator	URL	59
Value Added Network	VAN	60
Virtual Private Network	VPN	61
شهادات معيارية تستخدمها مراسيم SSL و SET	X.509	62

فهرس المحتويات

	الموضوع	رقم الصفحة
	الإهداء	ب
	شكر وتقدير	ج
	ملخص الدراسة باللغة العربية	د
	ملخص الدراسة باللغة الإنجليزية	هـ
	جدول الإختصارات	و
	فهرس المحتويات	ح
	الفصل الأول	
	مدخل الدراسة	
1-1	مقدمة	2
1-2	مشكلة البحث	2
1-3	فروض البحث	2
1-4	أهداف البحث	3
1-5	أهمية البحث	3
1-6	منهجية البحث	3
1-7	دراسات سابقة	4
	الفصل الثاني	
	تقنية أمن البيانات	
2-1	أمن الإنترنت	7
2-1-1	نظرة عامة	7
2-1-2	مفاهيم الأمن الأساسية	8
2-1-3	أهمية أمن المعلومات	9
2-1-4	حوادث أمن الإنترنت	10
2-1-5	مصادر الحوادث	10
2-1-6	أنواع الحوادث	11
2-1-7	مقاصد الحوادث وغاياتها	14
2-1-8	الإتجاهات المستقبلية للأمن	14
2-2	مفاهيم في علم التعمية	19
2-2-1	الحاجة لعلم التعمية	20
2-2-2	علم التعمية التطبيقي	21
2-2-3	التشفير المعتمد على المفاتيح	21

2-2-4	التوقيع الإلكتروني	23
2-2-5	ملخّص الرسالة	23
2-3	الخصائص التعموية للغة العربية	24

الفصل الثالث
التجارة الإلكترونية

3-1	مقدمة	28
3-2	تعريفات ومصلحات التجارة الإلكترونية	29
3-3	التجارة الإلكترونية من خلال طبيعة المعاملات	31
3-4	الأسواق الإلكترونية	32
3-5	وسائل ونظم الدفع الإلكترونية	33
3-5-1	بطاقات الإئتمان	33
3-5-2	النقود الرقمية أو الإلكترونية	36
3-5-3	الشيكات الإلكترونية	38
3-5-4	البطاقات الذكية	39
3-6	حلول التجارة الإلكترونية	40
3-6-1	المجمعات الانترنتية	41
3-6-2	مزودي خدمة الإنترنت	42
3-7	فوائد التجارة الإلكترونية للشركات والمؤسسات	43
3-8	فوائد التجارة الإلكترونية للمستهلكين	44
3-9	فوائد التجارة الإلكترونية للمجتمع	44
3-10	معوقات التجارة الإلكترونية	45
3-11	جوانب القصور في التجارة الإلكترونية	45
3-12	تحديات التجارة الإلكترونية	46
3-13	إحصاءات هامة تتعلق بالتجارة الإلكترونية	47

الفصل الرابع
الشبكات الخاصة الوهمية

4-1	الشبكة الخاصة الوهمية	51

4-2	خدمة التحقق من المتصل عن بعد RADIUS	56
4-3	مرسوم الإنترنت السري IPsec	60
4-3-1	فوائد IPsec	60
4-4	Kerberos	61

الفصل الخامس

مرسوم التحويلات المالية الآمنة SET

5-1	مقدمة	64
5-2	نظرة عامة على مراسيم الشبكة	64
5-2-1	مجموعة المراسيم (TCP/IP)	64
5-2-2	مرسوم تيلنت	64
5-2-3	مرسوم نقل الملفات	65
5-2-4	مرسوم (NFS)	65
5-2-5	مرسوم (SMTP)	65
5-2-6	المرسوم (SNMP)	66
5-2-7	المرسوم (HTTP)	66
5-2-8	مرسوم (TCP)	68
5-2-9	المرسوم (UDP)	68
5-2-10	المرسوم (IP)	68
5-3	تعريف مرسوم الحركات المالية الآمنة	69
5-4	أطراف عملية الشراء وفقاً لـ SET	70
5-5	إجراء الحركات المالية وفقاً لـ SET	72

5-6	التوقيع المزدوج	73
5-7	مرسوم SET بين التاجر والزبون	74
5-8	نظام التحويلات المالية الإلكترونية	74
5-8-1	تعريف نظام التحويلات المالية الإلكترونية	75
5-8-2	كيف تتمّ عملية التحويل المالي الإلكتروني	75
5-8-3	منافع نظام التحويلات المالية الإلكترونية	77
5-9	نظام تبادُل البيانات إلكترونياً	77
5-9-1	برمجيات تبادُل البيانات إلكترونياً	78
5-9-2	كيف يعمل نظام تبادُل البيانات إلكترونياً	79
5-9-3	فوائد نظام تبادُل البيانات إلكترونياً	80

الفصل السادس

مرسوم طبقة المقابس الآمنة SSL

6-1	مقدمة	83
6-2	أهداف التعاملات الآمنة	84
6-3	المقياس العملي	85
6-4	تطبيقات SSL	85
6-5	معمارية SSL	86
6-5-1	The SSL Record Protocol	88
6-5-2	The SSL Handshake protocol	88
6-6	توثيق الخادم	88
6-7	توثيق العميل	98
6-8	التشفير في إتصالات SSL	98
6-9	خوارزميات التشفير المستخدمة في SSL	89
6-10	شهادات SSL الإلكترونية	98
6-11	إنشاء جلسة SSL	100
6-12	تهيئة SSL	101

6-13 توثيق الشهادة الخارجي 101

الفصل السابع
الجانب العملي
موقع حضرموت للأبحاث

7-1 وصف عام للموقع 103
7-2 خواص الموقع 104
7-3 وثيقة تحرير خطوات المشروع 108
7-4 إستعراض النظام 110
7-5 الصياغة الأولية 113
7-6 وثيقة مواصفات متطلبات النظام SRS 123
7-7 وثيقة تصميم النظام SDD 131
7-8 الإستنتاجات والتوصيات 136
المراجع 138
الملاحق 141