



شبكة المعلومات الجامعية

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ





شبكة المعلومات الجامعية



شبكة المعلومات الجامعية

التوثيق الالكتروني والميكرو فيلم

جامعة عين شمس

التوثيق الالكتروني والميكروفيلم



نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
على هذه الأفلام قد أعدت دون أية تغييرات



يجب أن

تحفظ هذه الأفلام بعيداً عن الغبار

في درجة حرارة من 15 – 20 مئوية ورطوبة نسبية من 20-40 %

To be kept away from dust in dry cool place of
15 – 25c and relative humidity 20-40 %



شبكة المعلومات الجامعية



بعض الوثائق الأصلية تالفة



شبكة المعلومات الجامعية



بالرسالة صفحات

لم ترد بالأصل

B.T. 114

SECURE ALGORITHM FOR REMOTE ACCESS SERVICES

By
Mohammed Attya Khaliefa

**A Thesis Submitted to the Faculty of Computers & Information
Cairo University
in Partial Fulfillment of the Requirements for Degree of Master of Science
in
Computer Science**

Under Supervision of

Prof. Dr. Aly Aly Fahmy

**Prof. Dr. Imane Aly
Saroit Ismail**

Dr. Tarek Abd El-Meged

Dean of Faculty of
Computers & Information,
Cairo University

Professor in Information
Technology Department,
Faculty of Computers &
Information., Cairo
University

Armed Force

**FACULTY OF COMPUTERS & INFORMATION
CAIRO UNIVERSITY - EGYPT**


May 2007

Certificate

I certify that this work has not been accepted in substance for any academic degree and is not being concurrently submitted in candidature for any other degree.

Any portions of this thesis for which I am indebted to other sources are mentioned and explicit references are given.

Student Name : Mohammed Attia Khaliefa.

Signature : 

SECURE ALGORITHM FOR REMOTE ACCESS SERVICES

By

Mohammed Attya Khaliefa

A Thesis Submitted to the Faculty of Computers & Information
Cairo University

in Partial Fulfillment of the Requirements for Degree of Master of Science
in Computer Science

Approved by the Examining Committee

Signature

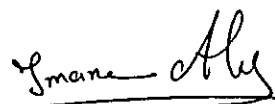
Prof. Dr. Aly Aly Fahmy, Main Advisor & Member.



Prof. Dr. Shrief El Kassas, Member.



Prof. Dr. Imane Aly Saroit Ismail, Advisor & Member.



A. Prof. Dr. Hesham Ahmed Hassan, Member.



FACULTY OF COMPUTERS & INFORMATION
CAIRO UNIVERSITY - EGYPT

May 2007

CONTENTS

<u>Title</u>	<u>Page</u>
LIST OF TABLES	viii
LIST OF FIGURES	ix
AKNOWLEDGMENT	xii
ABSTRACT	xiii
 Chapter 1: Introduction	
1.1 Introduction	1
1.2 Research Objective	1
1.3 Thesis Outlines	2
 Chapter 2: Remote Access Services Kinds and Solutions	
2.1 Electronic Mail (E-Mail): using Web email to develop a remote communication solution	4
2.1.1 What are the needs to implement E-Mail	6
2.1.2 Working Scenario	6
2.1.3 What it can be used for	7
2.2 Remote Control Software	7
2.2.1 What are the needs to implement Remote Control Software	8
2.2.2 Working Scenario	8
2.2.3 What it can be used for	9
2.2.4 Advantages of Remote Control Software	9
2.2.5 Disadvantages of Remote Control Software	9
2.3 Remote Access Services (RAS),Dialing-in to the office Local Area Network (LAN)	9
2.3.1 What are the needs to implement dialing into a LAN	10
2.3.2 Working Scenario	10
2.3.3 What it can be used for	11
2.3.4 Advantages of Dialing into a LAN	11
2.3.5 Disadvantages of Dialing into a LAN	11
2.4 Wide Area Networks (WANs)	12
2.4.1 What is needed to implement WAN	13
2.4.2 Working Scenario	13
2.4.3 What it can be used for	13
2.4.4 Advantages or WAN	14
2.4.5 Disadvantages or WAN	14
2.5 Virtual Private Networks (VPNs)	14
2.5.1 What is needed to implement VPN	15
2.5.2 Working Scenario	15
2.5.3 What it can be used for	16
2.5.4 Advantages of VPN	16
2.5.5 Disadvantages of VPN	16
2.6 Terminal Services	16
2.6.1 What is needed to implement Terminal Services	17
2.6.2 Working Scenario	18
2.6.3 What it can be used for	18

2.6.4 Advantages of Terminal Services	18
2.6.5 Disadvantages of Terminal Services	19
2.7 Database Replication	19
2.7.1 What is needed to implement Database Replication	20
2.7.2 Working Scenario	20
2.7.3 What it can be used for	20
2.7.4 Advantages of Database Replication	20
2.7.5 Disadvantages of Database Replication	21
2.8 Routing Remote Access Service (RRAS)	21
2.8.1 What is needed to implement RRAS	22
2.8.2 How it works	22
2.8.2.1 Understanding how routing work	22
2.8.2.2 How RRAS works	25
2.8.3 What it can be used for	27
2.8.4 Advantages of RRAS	27
2.9 Summary	28

Chapter 3: Remote Access Service Needs and Problems

3.1 Communications Links Needs and Problems	30
3.1.1 Capacity Needs	30
3.1.2 Bandwidth Needs and Problems	31
3.1.3 Choosing Appropriate Connectivity	33
3.2 What are supported services and to whom (Access Control)	36
3.2.1 Authentication	36
3.2.2 Logging and Auditing	37
3.2.3 Access to Your Network Resources	38
3.3 Network Devices Needs and Problems	39
3.3.1 Network Servers	40
3.3.2 Dedicated Devices	42
3.3.3 VPN Devices	42
3.3.4 Clients Devices and System	43
3.4 Summary	43

Chapter 4: Security Aspects and Issues

4.1 Confidentiality	45
4.1.1 Password Authentication Protocol (PAP)	46
4.1.1.1 PAP Messages Exchanges Scenario	47
4.1.1.2 PAP Advantages	47
4.1.1.3 PAP Disadvantages	48
4.1.2 Shiva Password Authentication Protocol (SPAP)	48
4.1.2.1 SPAP Messages Exchanges Scenario	49
4.1.2.2 SPAP Advantages	49
4.1.2.3 SPAP Disadvantages	50
4.1.3 Challenge Handshake Authentication Protocol (CHAP)	50
4.1.3.1 CHAP Messages Exchange Scenario	50
4.1.3.2 CHAP Advantages	51
4.1.3.3 CHAP Disadvantages	51

4.1.4 Microsoft Challenge Handshake Authentication (MS-CHAP)	52
4.1.4.1 MS-CHAP Messages Exchange Scenario	52
4.1.4.2 MS-CHAP Advantages	53
4.1.4.3 MS-CHAP Advantages	53
4.1.5 Extensible Authentication Protocol (EAP)	54
4.1.5.1 Difference between EAP and previous authentication protocols	54
4.1.5.2 Extensible Authentication Protocol using Message Digest5 (EAP-MD5)	55
4.1.5.3 Extensible Authentication Protocol using Remote Authentication Dial In User Server Method (EAP-RADIUS)	57
4.1.6 Remote Authentication Dial In User Server RADIUS Server (AAA)	59
4.1.6.1 RADIUS Message Exchange Scenario	59
4.1.6.2 RADIUS Advantages	60
4.1.6.3 RADIUS Disadvantages	61
4.2 Access Control	61
4.2.1 Access Matrix	62
4.2.1.1 Access Matrix Mechanism	62
4.2.1.2 Access Matrix Advantages	62
4.2.1.3 Access Matrix Disadvantages	62
4.2.2 Unix/Linux System	63
4.2.2.1 Unix/Linux System Mechanism	63
4.2.2.2 Unix/Linux System Advantages	64
4.2.2.3 Unix/Linux System Disadvantages	64
4.3 Privacy	64
4.3.1 Symmetric Algorithm (Private Key)	65
4.3.1.1 Symmetric Algorithm Scenario	66
4.3.1.2 Symmetric Algorithm Advantages	66
4.3.1.3 Symmetric Algorithm Disadvantages	67
4.3.2 Asymmetric Algorithm (Public Key)	67
4.3.2.1 Asymmetric Algorithm Message Scenario	68
4.3.2.2 Asymmetric Algorithm Advantages	68
4.3.2.3 Asymmetric Algorithm Disadvantages	69
4.3.2.4 More Security Issues	69
4.3.3 Tunneling for Virtual Private Network (VPN)	70
4.3.3.1 Point-to-Pont Protocol	71
4.3.3.2 Point-to-Point Tunneling Protocol (PPTP)	75
4.3.3.3 Layer 2 Tunneling Protocol (L2TP)	79
4.4 Integrity	84
4.4.1 Frame Check Sequence (FCS)	84
4.4.1.1 Frame Check Sequence (FCS) Scenario	85
4.4.1.2 Frame Check Sequence Advantages	85
4.4.1.3 Frame Check Sum Disadvantages	86
4.4.2 Message Authentication Code (MAC)	87
4.4.2.1 Message Authentication Code Scenario	87

4.4.2.2 Message Authentication Code Advantages	88
4.4.2.3 Message Authentication Code Requirements	88
4.4.2.4 Message Authentication Code Security	90
4.4.3 Hashing Algorithm	91
4.4.3.1 Hashing Messaging Scenario	91
4.4.3.2 Hash Function Advantages	92
4.4.3.3 Hash Function Disadvantages	92
4.4.3.4 Hash function Requirements	92
4.4.3.5 Simple Hash Function	93
4.4.3.6 Other Scenarios for Hash function	93
4.5 Non-Repudiation and Network Management	95
4.5.1 Network Traffic Management	96
4.5.1.1 Network Management Mechanism	96
4.5.1.2 Network Management Scenario Advantages	97
4.5.1.3 Network Management Scenario Disadvantages	98
4.5.2 Accounting	98
4.5.2.1 Accounting Message Scenario	98
4.5.2.2 RADIUS Scenario Advantages	99
4.5.2.3 RADIUS Scenario Disadvantage	99
4.5.2.4 Accounting Attributes	99
4.6 Summary	101

Chapter 5: Bandwidth Allocation Algorithms and Strategies

5.1 What Are Network Services Problems?	102
5.2 Bandwidth Allocation Requirements and Measurements	103
5.2.1 Max-Min Fairness	104
5.2.1.1 Advantages of Max-Min Fairness	104
5.2.1.2 Disadvantages of Max-Min Fairness	104
5.2.2 Utility Max-Min Fairness	105
5.2.2.1 Advantages of Utility Max-Min Fairness	105
5.2.2.2 Disadvantages of Utility Max-Min Fairness	106
5.2.3 Proportional Fairness (Utility Approach)	106
5.2.3.1 Advantages of Proportional Fairness	107
5.3 Bandwidth Allocation Algorithms	107
5.3.1 Complete Sharing Algorithm	107
5.3.2.1 Complete Sharing Algorithm Advantages	109
5.3.2.2 Complete Sharing Algorithm Disadvantages	109
5.3.2 Complete Partitioning Algorithm	109
5.3.2.1 Complete Portioning Advantages	112
5.3.2.2 Complete Portioning Disadvantages	112
5.3.3 Dynamic Bandwidth Partitioning Algorithm	112
5.3.3.1 Dynamic Portioning Algorithm Advantages	114
5.4 Summary	114

Chapter 6: Proposed Model for Securing Proposed Remote Access Services

6.1 Remote Access Services Structure	116
6.1.1 Desktop Management Service	117
6.1.2 File Management Service	117
6.1.3 Process Management Service	118
6.2 Remote Access Services System Requirements	118
6.3 Remote Access Services System Design	119
6.3.1 Client Side	119
6.3.2 Server Side	119
6.4 Remote Access Services System Work-Flow	121
6.5 proposed Security Service Modules	123
6.6 Proposed Confidentiality Module	123
6.6.1 Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) Message Passing Scenario	124
6.6.2 Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) Advantages	125
6.7 Proposed Access Control Module	126
6.7.1 Access Control Module Structure	127
6.7.2 Authorization Scenario	127
6.7.3 Combined Approach advantages	129
6.8 Proposed Privacy Module	129
6.8.1 RSA Algorithm Scenario	130
6.8.2 RSA Algorithm Scenario Advantages	131
6.8.3 RSA Algorithm Scenario Disadvantages	132
6.8.4 AES Algorithm Scenario	132
6.8.5 AES Algorithm Scenario Advantages	133
6.9 Proposed Integrity Module	133
6.9.1 Advantages of MAC	133
6.9.2 Used Approach for MAC	134
6.9.3 HMAC Algorithm	136
6.9.3.1 HMAC Algorithm Design and Elements	136
6.9.3.2 HMAC Algorithm	137
6.9.3.3 HMAC Advantages and Security	138
6.10 Non-Repudiation	138
6.10.1 Non-Repudiation Message Passing Scenario	139
6.10.2 Advantages of Central Auditing Server Approach	142
6.10.3 Disadvantages of Central Auditing Server Approach	142
6.11 Summary	142

Chapter 7: Experimental Results of Applying Proposed Security Model upon Remote Access Services system

7.1 Experimental Measurements and Environment	143
7.1.1 Investigation Parameters	143
7.1.2 Experimental Environment	144
7.2 Testing Confidentiality Module	144

7.2.1 Before Applying the Confidentiality Module	144
7.2.2 After Applying the Confidentiality Module	145
7.3 Testing Access Control Module	146
7.3.1 Before Applying the Access Control Module	146
7.3.2 After Applying the Access Control Module	146
7.4 Testing Privacy Module	147
7.4.1 RSA Algorithm upon Process Management Service	148
7.4.1.1 Before Applying RSA Algorithm	148
7.4.1.2 After Applying RSA Algorithm	149
7.4.2 RSA Algorithm upon File Management Service	150
7.4.2.1 Before Applying the RSA Algorithm	151
7.4.2.2 After Applying the RSA Algorithm	151
7.4.2.3 Modifications for using RSA Algorithm	153
7.4.2.4 More Modifications to Solve Time Delay Problem	155
7.4.3 RSA Algorithm upon Desktop Management Service	157
7.4.3.1 Before Applying RSA Algorithm	157
7.4.3.2 After Applying RSA Algorithm	157
7.4.3.3 Modifications of using RSA Algorithm	159
7.4.4 AES Algorithm upon Process Management Service	160
7.4.4.1 Before Applying AES Algorithm	161
7.4.4.2 After Applying AES Algorithm	161
7.4.5 AES Algorithm upon File Management Service	162
7.4.5.1 Before Applying AES Algorithm	162
7.4.5.2 After Applying AES Algorithm	162
7.4.6 AES Algorithm upon Desktop Management Service	163
7.4.6.1 Before Applying RSA Algorithm	163
7.4.6.2 After Applying AES Algorithm	163
7.5 Testing the Proposed Integrity Module	163
7.6 Testing Non-Repudiation Module	164
7.8 Conclusion	164

Chapter 8: Experimental Results of Applying Bandwidth Allocation Algorithms upon Remote Access Services System

8.1 Experimental Measurements and Environment	168
8.1.1 Investigation Parameters	168
8.1.2 Experimental Environment	169
8.2 Testing Complete Sharing Algorithm	169
8.2.1 Applying Complete Sharing upon Desktop Management Service	170
8.2.1.1 Bandwidth Usage and Utilization	170
8.2.1.2 Time Response	171
8.2.2 Applying Complete Sharing upon File Management Service	171
8.2.2.1 Bandwidth Usage and Utilization	172
8.2.2.2 Time Response	173
8.2.3 Applying Complete Sharing upon Process Management Service	173
8.2.3.1 Bandwidth Usage and Utilization	174

8.2.3.2 Time Response	174
8.2.4 Overall Used Bandwidth for Complete Sharing	174
8.3 Testing Complete Partitioning After RSA Algorithm	176
8.3.1 Applying Complete Partitioning upon Desktop Management Service	176
8.3.1.1 Bandwidth Usage and Utilization	177
8.3.1.2 Time Response	178
8.3.2 Applying Complete Partitioning upon File Management Service	179
8.3.2.1 Bandwidth Usage and Utilization	179
8.3.2.2 Time Response	180
8.3.3 Applying Complete Partitioning upon Process Management Service	180
8.3.4 Overall Used Bandwidth for Complete Partitioning	180
8.4 Testing Dynamic Partitioning After RSA Algorithm	181
8.4.1 Applying Dynamic Partitioning upon Desktop Management Service	182
8.4.1.1 Used Bandwidth and Utilization	182
8.4.1.2 Time Response	184
8.4.2 Applying Dynamic Partitioning upon File Management Service	184
8.4.2.1 Used Bandwidth and Utilization	185
8.4.2.2 Time Response	186
8.4.3 Applying Dynamic Partitioning upon Process Management Service	186
8.4.4 Overall Used Bandwidth for Dynamic Bandwidth Partitioning	187
8.5 Testing Complete Sharing Algorithm after AES Algorithm	188
8.5.1 Applying Complete Sharing upon Desktop Management Service	188
8.5.1.1 Bandwidth Usage and Utilization	189
8.5.1.2 Time Response	190
8.5.2 Applying Complete Sharing upon File Management Service	190
8.5.2.1 Bandwidth Usage and Utilization	190
8.5.2.2 Time Response	192
8.5.3 Applying Complete Sharing upon Process Management Service	192
8.5.3.1 Bandwidth Usage and Utilization	192
8.5.3.2 Time Response	192
8.5.4 Overall Used Bandwidth for Complete Sharing	193
8.6 Conclusion	194
Chapter 9: Conclusion and Future Work	
9.1 Conclusion	198
9.2 Future Work	202
References	204
Outcome From The Thesis	209