

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	ii
	ACKNOWLEDGMENT	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	xiii
	LIST OF FIGURES	xiv
	LIST OF APPENDICES	xvi
1	OVERVIEW	1
	1.1 Introduction	1
	1.2 Background problem	2
	1.3 Problem statement	4
	1.4 Project objective	4
	1.5 Project scope	5
	1.6 Importance of the Study	6
	1.7 Summary	7
2	LITERATURE REVIEW	8
	2.1 Introduction	8
	2.2 Computer network	9
	2.3 Network topology	9
	2.3.1 Bus topology	10
	2.3.2 Ring topology	11
	2.3.3 Star topology	12

2.3.4 Mesh topology	13
2.3.5 Consideration when choosing topology	14
2.4 Network security	14
2.4.1 Overview of network security	15
2.4.2 Overview of OSI Technology	16
2.5 The Five layers of security model	17
2.5.1 Authentication	18
2.5.2 Authorization	18
2.5.3 Encryption	19
2.5.4 Integrity	19
2.5.5 Audit	20
2.6 General security threats and attacks on LANs	21
2.6.1 Passive attacks	22
2.6.2 Active attacks	23
2.6.3 Man-in-the middle attack	24
2.6.4 Jamming attack	24
2.7 Authentication in network	24
2.7.1 Authentication elements	26
2.8 Network access control	27
2.8.1 Types of network access control	28
2.8.1.1 Discretionary access control (DAC)	28
2.8.1.2 Mandatory access control (MAC)	29
2.8.1.3 Role-based access control (RObAC)	30
2.8.1.4 Rule-based access control (RUbAC)	31
2.8.1.5 Quandary of network access control	32
2.8.1.6 Security issue in network access control	33
2.9 Planning network access controls	33
2.10 IEEE 802.1x technology	35
2.10.1 Elements of 802.1X	36
2.10.2 Supplicant	37
2.10.3 Pass-through authenticator	37
2.10.4 Authentication server	37

2.10.5 Controlled and uncontrolled ports	39
2.10.6 Security Provided by IEEE 802.1x	39
2.10.7 Advantages of using IEEE 802.1x	40
2.10.8 Limitations and vulnerabilities on using ieee 802.1x	42
2.10.9 The absence of mutual authentication	42
2.10.10 Session hijacking	44
2.11 Extensible authentication protocol (EAP)	45
2.11.1 General concepts of extensible authentication protocol (EAP)	45
2.11.2 EAP-MD5	47
2.11.3 EAP-TLS	49
2.11.4 EAP-TTLS	51
2.11.5 EAP-PEAP	53
2.11.6 Comparison between previous four EAP methods	54
2.12 IPsec technology	57
2.12.1 IPsec security properties	57
2.12.2 How IPsec protects IP traffic	59
2.12.3 Authentication header (AH)	60
2.12.4 Encapsulating security payload (ESP)	60
2.12.5 Security provided by IPsec	62
2.12.6 Some limitation of the IPsec with network quarantine	63
2.13 Comparing 802.1x for wired network with IPsec	63
2.13.1 Compression summary	66
2.14 Network access quarantine	67
2.14.1 Benefit of network quarantine	68
2.14.2 How network access quarantine works	68
2.14.3 Quarantine Mode	69
2.14.4 Components of Network access quarantine control	70
2.14.5 Important of network access quarantine control	71
2.14.6 Network Quarantined Resources	72

2.14.6.1	DNS	72
2.14.6.1.1	Benefits of adding a third-party DNS server	72
2.14.6.2	DHCP	73
2.15	Types & Comparison between different authentication mechanisms used	74
2.15.1	Null authentication	75
2.15.2	Virtual Private Network	75
2.15.3	Media Access control (MAC) based authentication	77
2.15.4	Wired equivalent privacy (WEP)	77
2.16	Network access quarantine implementation method	79
2.16.1	Network quarantine with VPN	79
2.16.2	Network quarantine with IPsec	80
2.16.4	Network quarantine with DHCB	81
2.16.5	Network quarantine with IEEE802.1x	81
2.16.5.1	Benefit of Network quarantine with IEEE802.1x	82
2.17	Best authentication choice based on organizations types	84
2.17.1	Home network security	84
2.17.2	Small business security	84
2.17.3	Medium to large enterprise security	85
2.17.3	Military grade maximum level security	86
2.18	Summary	86
3	RESEARCH METHODOLOGY	88
3.1	Introduction	88
3.2	Project framework	88
3.3	Observations and problem formulation	90
3.4	Literature review	90
3.5	Requirement specification	91
3.5.1	Hardware requirement specification	91
3.5.2	Software requirement specification	93
3.6	Scheme design	93
3.7	System implementation	94
3.8	Testing the system	95

3.9	Report writing	96
3.10	Summary	97
4	SYSTEM DESIGN	98
4.1	Introduction	98
4.2	Selected operating system	98
4.3	Overall system design	99
4.4	DC server	100
4.4.1	Infrastructure services	101
4.4.1.1	Active directory (AD)	102
4.4.1.2	Domain name system (DNS)	103
4.4.1.3	Dynamic host configuration protocol (DHCP)	103
4.5	NPS server	103
4.6	The entire network	105
5.7	The overall authentication process of the designed system	105
4.8	Summary	106
5	SYSTEM IMPLEMENTATION AND TESTING	108
5.1	Introduction	108
5.2	Infrastructure server	108
5.2.1	Infrastructure and service installation and configuration	109
5.2.1.1	Active directory & DNS (DC server)	109
5.2.1.2	Certification authority (DC server)	110
5.2.1.3	IPSec	111
5.2.1.4	Dynamic host configuration protocol (DHCP)	112
5.2.1.5	Network policy server	113
5.2.2	IEEE802.1X technology	114
5.3	Testing the system	115
5.3.1	Testing the authentication	116
5.4	Summary	117
6	DISCUSSION FUTURE WORK AND CONCLUSION	118

6.1 Introduction	118
6.2 Discussion	118
6.2.1 Justification of choosing windows as an operating system in this project	119
6.2.2 Justification of the authentication level in this project	120
6.2.3 Features of the implemented authentication in this project	121
6.2.4 Comparing UTM authentication with proposed project solution	122
6.3 Future works	123
6.4 Conclusion	124
Reference	125
Appendix	Xvi

LIST OF TABLES

TABLE NO.	TITLE	PAGE
2.1	Comparison between EAP methods	55
2.2	Summary between 802.1X and IPsec	63
2.3	Compare between different Network quarantine implementation method	64
2.4	Comparison between different authentication mechanisms	83
3.1	The servers' requirements	92
3.2	The client desktop/laptop minimum requirement	92
6.1	Comparisons between UTM authentication & network quarantine using IEEE802.1x and IPsec	123

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
Figure 1.1:	Machine is not accessing the network because it's not authenticate & validate from the server	2
Figure1.2:	PC0 only can access the network if the machine fulfills the security Requirement	5
Figure 1.3:	(a) Unauthorized state port (b) Authorized state port	6
Figure 2.1:	Bus topology	10
Figure 2.2:	Ring topology	11
Figure 2.3:	Star topology	12
Figure 2.4:	Mesh topology	13
Figure 2.5:	802.11 Network and The OSI model	16
Figure 2.6:	Security Pyramid	20
Figure 2.7:	Security incidents or attacks on network in 2002	22
Figure 2.8:	Discretionary access control	29
Figure 2.9:	Mandatory access control	30
Figure 2.10:	Role-based access control	31
Figure 2.11:	Rule-based access control	32
Figure 2.12:	Shows these components for a wired network	36
Figure 2.12.1:	Shows the interaction between supplicant and server	37
Figure 2.13:	Shows the different types of ports	39
Figure 2.14:	Man-in-the middle attack	43
Figure 2.15:	Session Hijacking Attack	44
Figure 2.16:	EAP packet format	46
Figure 2.17:	EAP-MD5 process details	49
Figure 2.18:	EAP-TLS process details	51
Figure 2.19:	EAP-TTLS process detail	52

Figure 2.20: PEAP process detail	54
Figure 2.21: An IP packet without any IPsec protection	59
Figure 2.22: An IP packet without any IPsec protection	60
Figure 2.23: An IP packet with ESP and encryption protection	61
Figure 2.24: An IP packet with ESP and no encryption protection	61
Figure 2.25: Components of windows access for network access Quarantine Control	70
Figure 2.26: VPN authentication	76
Figure 2.27: Shows virtual private network	80
Figure 2.28: Network quarantine with IEEE802.1x	82
Figure 3.1: Project framework	89
Figure 3.2: System architecture	94
Figure 4.1: Overall system implementation plan	99
Figure 4.2: Overall system design	100
Figure 4.3: DC server	101
Figure 4.4: The project domain namespace	103
Figure 4.5: NPS server	104
Figure 4.6: The sequence of the authentication process	105
Figure 5.1: Active directory users and computers	110
Figure 5.2: Shows the Certificate Authority	111
Figure 5.3: Shows the DHCP	112
Figure 5.4: Network policy server set up	113
Figure 5.6: Switch software	114
Figure 5.7: Show the policy you can set to your network	115
Figure 5.8: Show's the client is not comply with network policy	116
Figure 5.9: Client comply with policy & connects to the network	117
Figure 6.1: OSI layer	121
Figure 6.2: Snapshot of the SMAC V2.0 tool	122

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Step by step system implementation	132