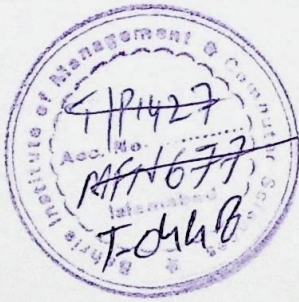


KSCRTS

Kerberos Secure Communication in Real Time System



Developed by:

Mobeen Akhtar (244002-008-CS/MCS)

(Year 2004)

Supervised by:

Madam Farzana Khan

Department of Computer Sciences
Bahria Institute of Management & Computer Sciences
Islamabad



**Bahria Institute of Management & Computer Sciences,
Islamabad.**

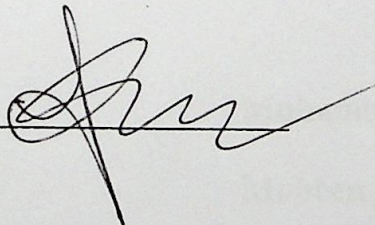
March 26, 2004

Final Approval

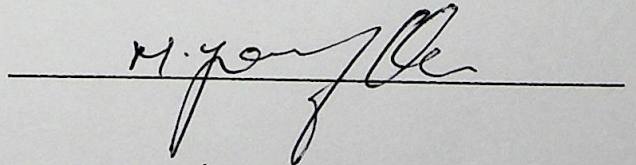
It is certified that I have read the project titled "KSCRTS" submitted by Muhammad Reahan and Mobeen Akhtar. It is my judgment that this project is of sufficient standard to warrant its acceptance by Behria University for the Master degree in computer sciences.

Committee

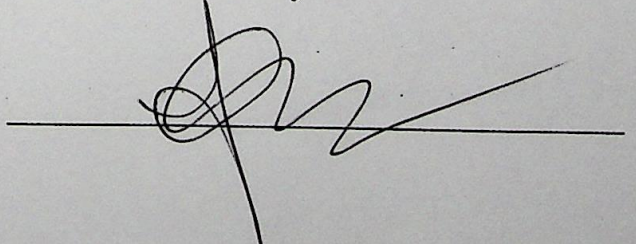
Head of Department:



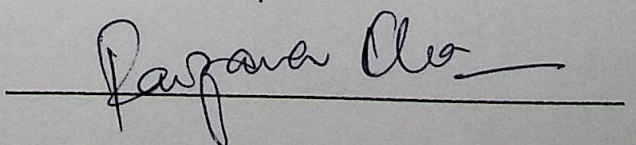
External Examiner:



Internal Examiner:



Supervisor:



Madam Farzana Khan
Department of Computer Sciences
Bahria Institute of Management & Computer Sciences Islamabad

DECLARATION

We, hereby declare that “KSCRTS” software, neither as a whole nor as a part of has been copied out from any source. It is further declared that we have developed this software and the accompanied report entirely on the basis of our personal efforts made under the guidance of kind supervisors & PAF Engineers. No portion of the work presented in this report has been submitted in support of any application for any other degree or qualification of this or any other university or institute, if found we will stand responsible.

Muhammad Reahan

Mobeen Akhtar

DEDICATED TO

Our parents

For their love, prayers and much more...

&

Our teachers

For their valuable guidance, assistance and much more...

ACKNOWLEDGEMENTS

No words can express our gratitude to Almighty ALLAH who bestowed his kindness upon us, enabling us to complete this tedious and challenging task in time.

We would like to pay our heartiest tribute to our supervisor Madam Farzana Khan, for providing the skills and imparting the knowledge, necessary to coup up with the challenges to build this software and making this idea to reality world. Her all time appreciation has been the motivating force behind the successful completion of this software

We would also like to thank System Engineers Sqd Leader Abdullah and Sqd Leader Adeel from Pakistan Air Force for providing all the necessary assistance, guidance facts and figures to the best of their knowledge & special thanks to the Director of the Project Vision for his kind propensity.

Salutations to my loving parents for their invaluable prays, salutary advises and emboldening attitude kept our spirit alive to strive for knowledge and integrity, which enabled us to reach this milestone.

A DISSERTATION SUBMITTED TO THE
DEPARTMENT OF COMPUTER SCIENCE
BAHRIA INSTITUTE OF MANAGEMENT AND COMPUTER
SCIENCES, ISLAMABAD
AS
A PARTIAL FULFILMENT OF THE REQUIREMENTS
FOR THE AWARD OF DEGREE OF
MASTER OF COMPUTER SCIENCE

PROJECT IN BRIEF

Project Title:	KSCRTS
Objective:	To develop a Kerberos Secure Communication System that will be used for Resource Administration & Monitoring over PPP Link.
Undertaken By:	Muhammad Reahan & Mobeen Akhtar
Supervised By:	Madam Farzana Khan
Controlled By:	Madam Farzana Khan
Verified By:	Madam Farzana Khan
Version:	1.0.00
For:	BIMCS (Bahria Islamabad)
Tools & Technologies:	QT Designer Forte Developer Workshop C++.
Operating System:	Solaris 8.
Date Started:	June 14, 2003
Date Completed:	March 26, 2004
System Used:	Sun Blade 100 (2)

ABSTRACT

Security and quality of service in Real Time System networks is the basic requirements which contribute to provide realistic parameters. The software will be used in administration and monitoring of the network resources in a secure manner. Network resources belong to different component of the Real Time System. There are two major parts of the application. One part will purely be used for administrative purposes. The second part is monitoring of different component of the system. It is highly required to have an application for the Centralized Resource Management. Our application is used for Secure Centralized Resource Management. The KSCRTS is a UNIX based system. The entire system as a whole, the individual servers, and the individual sessions all are secured. All of the communication between Side B and Side C is on Legacy system leased lines by using the Asynchronous modems. Our application is capable to meet all the desired requirements.

Table of Contents

Contents	Page No.
Acknowledgements -----	v
Project Brief-----	vii
Abstract -----	viii
Table of Contents-----	ix
List of Figures-----	xix

Chapter No. 1

1. INTRODUCTION & BACKGROUND-----	1
1.1 SYSTEM ANALYSIS OVERVIEW -----	1
1.2 PROPOSED SYSTEM -----	2
1.3 PROJECT DEFINITION-----	2
1.4 PROJECT SCOPE -----	3
1.5 EFFICIENCY -----	3
1.6 RELIABILITY -----	3
1.7 USER FRIENDLINESS -----	3
1.8 ASSUMPTIONS AND DEPENDENCIES -----	3
1.9 ADVANTAGES OF THE PROPOSED SYSTEM-----	4
1.10 INTENDED AUDIENCE OF KSCRTS-----	5
1.10.1 End Users-----	5
1.10.2 Developers-----	5
1.10.3 External Supervisor -----	5
1.10.4 Internal Supervisor-----	6

<u>Contents</u>	<u>Page No.</u>
 CHAPTER NO. 2	
2 PRELIMINARY INVESTIGATION-----	7
2.1 PROCESS MODEL ARCHITECTURE-----	7
2.1.1 PROCESS MODEL-----	8
2.1.2 SOFTWARE DEVELOPMENT APPROACH-----	10
2.1.3 PHASES OF SPIRAL MODEL-----	10
2.2 BASIC CONCEPTS-----	12
2.2.1 Radar Overview-----	13
2.3 RADAR NATURE-----	13
2.3.1 Common Radar Operations-----	14
2.3.2 Doppler Effect-----	14
2.3.3 Radar Frequencies-----	14
2.3.4 Target Detection-----	15
2.4 DISTRIBUTED SYSTEMS SECURITY-----	17
2.5 KEY SECURITY CONCEPTS-----	19
2.5.1 Underlying security Concepts-----	19
2.5.2 Kerberos Security Model-----	20
2.5.3 Key Distribution Center (KDC)-----	21
2.5.4 principal Database-----	21
2.5.5 Realm-----	21
2.5.6 Tickets-----	22
2.5.7 A Shared Secret-----	22
2.5.8 Trusted Third Party Arbitration-----	22
2.5.9 Kerberos Network Architecture-----	22
2.5.10 Phases of Authentication-----	23
2.5.11 Authentication Service Message Exchange-----	24

Contents	Page No.
2.5.12 Ticket-Granting Service Message Exchange-----	25
2.5.13 Application Message Exchange -----	25
2.5.14 Credential Attributes -----	25
2.6 INTRODUCTION TO KERBEROS-----	26
2.6.1 Session Messages-----	26
2.7 KERBEROS SECURITY SERVICES -----	28
2.7.1 Authentication-----	28
2.7.2 Access Control-----	29
2.7.3 UNIX Permission -----	29
2.7.4 Role-Based Access Control-----	29
2.7.5 Device Allocation -----	29
2.7.6 Security Enhancement -----	29
2.8 SECURE COMMUNICATION -----	29
2.8.1 Sun Enterprise Authentication Module (SEAM) -----	30
2.8.2 Internet Protocol Security Architecture (IPsec) -----	30
2.8.3 Solaris Secure Shell-----	30
2.8.4 DES Encryption-----	30
2.8.5 Diffie Hellmann Authentication-----	31

Chapter No. 3

3 DETAIL SYSTEM ANALYSIS -----	32
3.1 WHAT IS SEAM -----	32
3.1.1 HOW SEAM WORKS-----	33
3.1.2 AUTHENTICATION SYSTEM-----	34
3.1.3 GAINING ACCESS TO A SERVICE USING SEAM -----	34
3.1.4 OBTAINING A CREDENTIAL FOR THE TICKET-GRANTING SERVICE-----	34
3.1.5 OBTAINING A CREDENTIAL FOR A SERVER -----	36

<u>Contents</u>	<u>Page No.</u>
3.1.6 OBTAINING ACCESS TO A SPECIFIC SERVICE -----	37
3.1.7 USING THE GSSCRED TABLE-----	38
3.2 PRINCIPALS-----	38
3.2.1 REALMS-----	39
3.2.2 REALMS AND SERVERS-----	40
3.3 SEAM SECURITY SERVICES -----	40
3.3.1 DATABASE PROPAGATION-----	41
3.3.2 CLOCK SYNCHRONIZATION-----	41
3.3.3 PASSWORD MANAGEMENT-----	41
3.4 ADVICE ON CHOOSING A PASSWORD -----	42
3.5 SPECIFIC TERMINOLOGY -----	43
3.5.1 AUTHENTICATION-SPECIFIC TERMINOLOGY-----	43
3.5.2 TYPES OF TICKETS -----	44
3.5.3 FORWARDABLE -----	44
3.5.4 INATIAL -----	45
3.5.5 INVALID-----	45
3.5.6 POST DATEABLE-----	45
3.5.7 PROXIABLE/PROXY -----	46
3.5.8 TICKET LIFETIMES-----	46
3.6 PRODUCT FUNCTIONS -----	47
3.7 REEQUIREMENT ANALYSIS SIGNIFICANCE -----	48
3.7.1 FUNCTIONAL REQUIREMENT -----	49
3.7.2 NON-FUNCTIONAL REQUIREMENTS-----	49
3.7.3 SYSTEM INTERFACES-----	49
3.7.4 USER INTERFACES -----	49
3.7.5 HARDWARE INTERFACES-----	50
3.7.6 SOFTWARE INTERFACES-----	50

<u>Contents</u>	<u>Page No.</u>
3.7.7 COMMUNICATION INTERFACES-----	50
3.8 EFFICIENCY -----	50
3.8.1 PERFORMANCE-----	50
3.8.2 CONSTRAINTS -----	50
Chapter No. 4	
4. SYSTEM DESIGN -----	51
4.1 DESIGN OBJECTIVES-----	51
4.1.1 Design Characteristics -----	52
4.1.2 Design Approaches -----	52
4.1.3 Structure Approach -----	52
4.1.4 Object-Oriented Approach -----	52
4.2 TOOL FOR DEVELOPMENT-----	53
4.3 DESIGN MODEL -----	54
4.4 CLASS AND OBJECTS IDENTIFICATION -----	54
4.5 HARDWARE AND SOFTWARE RESOURCES -----	55
4.5.1 Hardware-----	55
4.5.2 Software -----	56
4.5.3 Reusable Software Components -----	56
4.5.4 Human Resource-----	56
4.5.5 Software Skill-----	57
4.5.6 Number of People Required -----	57
4.6 REQUIREMENTS OF DATA COMMUNICATION -----	57
4.6.1 Designed Communication Medium-----	58
4.6.2 PSTN Network & Data -----	59
4.7 USE CASE ANALYSIS -----	60
4.7.1 Identifying the Actors-----	61

Contents	Page No.
4.7.2 Identifying the Use Case-----	61
4.7.3 Uses-Case Diagram-----	61
4.7.4 Actors-----	62
4.8 USE-CASE DESCRIPTION-----	62
4.8.1 Logon Console-----	64
4.8.2 Acquire Credential-----	64
4.8.3 Connect to Server-----	64
4.8.4 Radar State-----	65
4.8.5 Pulse Info-----	65
4.8.6 Noise Indication-----	65
4.8.7 Detail Pulse Info-----	65
4.8.8 Session Timer-----	65
4.8.9 Loop Back Test-----	65
4.8.10 Restart Client-----	65
4.8.11 Site Link Noise Indication-----	66
4.8.12 Detail in Range Object Info-----	66
4.8.13 Reboot Console-----	66
4.8.14 Kill Consol Session-----	66
4.8.15 Change Background Color-----	66
4.8.16 Kerberos Client State-----	66
4.8.17 Lost Token Info-----	66
4.9 CLASS DIAGRAMS OF KSCRTS-----	68
4.10 WORK BREAKDOWN STRUCTURE-----	69
SCHEDULING-----	69
4.10.1 Task Identification-----	69
4.10.2 PERT-----	72
4.10.3 Pert Network-----	73
4.11 CRITICAL PATH-----	74

Contents	Page No.
4.11 RISK ANALYSIS -----	75
4.12.1 Quality Management-----	76
4.12.2 Quality Management Activities -----	76
4.12.3 Modern Quality Management-----	76
4.12.4 Statistical Quality-----	77
4.12.5 Phases -----	77
4.12.6 Requirements Phase-----	78
4.12.7 Analysis Phase-----	78
4.12.8 Design Phase-----	78
4.12.9 Detailed Design Phase -----	79
4.12.10 Implementation Phase -----	79
4.12.11 Installation & Testing Phase -----	80
 Chapter No. 5	
DETAIL SYSTEM DESIGN-----	84
5. SECURITY MODEL-----	84
5.1 SECURITY STEPS B/W APPLICATIONS -----	85
5.2 GETTING NAMES-----	86
5.3 ACQUIRING CREDENTIALS -----	86
5.4 ESTABLISHING A SECURITY CONTEXT-----	88
5.5 EXCHANGING MESSAGES-----	90
5.6 USING GSS_GET_MIC () AND GSS_VERIFY_MIC ()-----	93
5.7 USING GSS_WRAP () AND GSS_UNWRAP ()-----	94
5.8 TERMINATING THE SECURITY CONTEXT -----	95
5.9 RUNNING IP APPLICATIONS OVER PPP -----	96
5.10 SYNCHRONOUS CONNECTIONS -----	96

<u>Contents</u>	<u>Page No.</u>
5.11 ESTABLISHING IP OVER PPP -----	97
Chapter No. 6	
6. INTRODUCTION -----	99
6.1 SYSTEM IMPLEMENTATION-----	99
6.1.1 Tool Selection-----	100
6.1.2 Operating System Selection-----	100
6.1.3 Programming Language Selection-----	100
6.2 COMMUNICATION INTERFACES -----	101
6.2.1 System Requirements -----	102
6.2.2 System Implementation-----	103
6.3 THE CONCEPT OF REMOTE MONITORING -----	103
6.4 RADAR & REMOTE MONITORING-----	105
6.4.1 Network Resource Monitoring -----	105
6.5 FUNCATION DESCRIPTION -----	106
Chapter No. 7	
7. TESTING -----	108
7.1 FAILURE, ERROR AND DEFECT -----	108
7.2 TESTING STRATEGIES -----	108
7.2.1 UNIT TESTING-----	108
7.2.2 BLACK BOX TESTING -----	108
7.2.3 SPECIFICATION TESTING -----	109
7.2.4 WHITE BOX TESTING -----	109
7.2.5 REGRESSION TESTING -----	109
7.2.6 ACCEPTANCE TESTING -----	109
7.2.7 ASSERTION TESTING -----	109

Contents	Page No.
7.2.8 SYSTEM TESTING -----	110
7.3 TESTING KSCRTS -----	110
7.4 TEST CASES ARCHITECTURE -----	110
7.5 CONVERSION -----	112
7.5.1 PILOT APPROACH -----	112
7.5.2 DIRECT CUT-OVER -----	112
7.5.3 PARALLEL APPROACH -----	112
7.6 TEST PLAN -----	112
7.7 FUNCTIONALITY -----	113
7.8 MISSING FUNCTION -----	113
7.9 WRONG FUNCTION -----	113
7.10 COMMUNICATION -----	113
7.11 MISSING INFORMATION -----	113
7.12 MISLEADING OR CONFUSING INFORMATION -----	113
7.13 PERFORMANCE -----	113
7.14 DIALOG LAYOUT -----	113
7.15 MISUSE OF COLOR -----	114
7.16 INCONSISTENT ABBREVIATIONS -----	114
7.17 VERSIONS -----	114
7.18 MESSAGE PROBLEM -----	115
7.19 PUBLIC DOCUMENTATIONS -----	115
7.20 SYSTEM EVALUATION -----	116

<u>Contents</u>	<u>Page No.</u>
Chapter No. 8	
8. USER GUIDE -----	117
8.1 SYSTEM REQUIREMENTS-----	117
8.1.1 How to Use the Software?-----	117
8.1.2 Running the Server-----	117
8.1.3 Running the Client -----	118
8.2 KSCRTS APPLICATION -----	119
8.2.1 Kerberos Client -----	119
8.2.2 Data Recording-----	120
8.2.3 Mobile Pulse Doppler Radar (MPDR)-----	120
8.2.4 In Range Objects -----	121
8.2.5 Channel Links -----	122
8.2.6 Consoles -----	122
8.3 FUTURE RECOMENNDATIONS -----	123
8.4 CONCLUSION-----	123
9. REFERENCES & BIBLIOGRAPHY-----	125

List of Figures

<u>Contents</u>	<u>Page No.</u>
2 PRELIMINARY INVESTIGATION.....	7
FIGURE 2.1 FROM IDEA TO COMPLETE PRODUCT.....	7
FIGURE 2.2 IDEA TO PRODUCT.....	9
FIGURE 2.3 PHASES OF SPIRAL MODEL.....	11
FIGURE 2.4 PRESPECTIVE OF SPIRAL MODEL.....	12
FIGURE 2.5 DOPPLER FREQUENCY	15
FIGURE 2.6 FREQUENCY MODULATION OF CS.....	16
3 DETAIL SYSTEM ANALYSIS.....	32
FIGURE 3.1. CREDENTIAL GRANTING SERVICE	35
FIGURE 3.2 OBTAINING A CREDENTIAL FOR A SERVER	36
FIGURE 3.3 OBTAINING ACCESS TO A SPECIFIC SERVICE.....	37
4. SYSTEM DESIGN	57
FIGURE 4.1 CLASS HIERARCHY	53
FIGURE 4.2 QT DESIGNER.....	56
FIGURE 4.3 COMMUNICATION	58

FIGURE 4.4 DATA DISTRIBUTION	58
FIGURE 4.5 TELECOMMUNICATION NETWORK	60
FIGURE 4.6 ACTORS.....	62
FIGURE 4.7 USE CASE.....	63
FIGURE 4.8 USE CASE DIAGRAM	67
FIGURE 4.9 CLASS DIAGRAM	68
FIGURE 4.10 SEQUENCE DIAGRAM PULSE INFO	69
FIGURE 4.11 SEQUENCE DIAGRAM INRANGE OBJECT.....	70
FIGURE 4.12 SEQUENCE DIAGRAM CHANNEL STATUS	71
FIGURE 4.13 TASK IDENTIFICATION.....	74
FIGURE 4.14 PERT NETWORK	76
FIGURE 4.15 RISK ANALYSIS	78
5. DETAIL SYSTEM DESIGN	81
FIGURE 5.1 SECURITY STEP 1	85
FIGURE 5.2 ACQUIRE CREDENTIAL PROCESS.....	87
FIGURE 5.3 ESTABLISHING SECURITY CONTEXT	89
FIGURE 5.4 ENCRYPTING A PART OF MESSAGE IN TOKEN	92

FIGURE 5.5 DATA & SIGNATURE TOKEN	93
FIGURE 5.6 VERIFICATION OF SIGNATURE	94
FIGURE 5.7 WRAPPING & UNWRAPPING TOKEN	95
FIGURE 5.8 LAYERS OF IP APPLICATION ON PPP	96
FIGURE 5.9 PPP & PUBLIC TELEPHONE NETWORK	97
FIGURE 5.10 POINT TO POINT IP CONNECTION	98
6. IMPLEMENTATION	99
FIGURE 6.1 REMOTE MONITORING	104
FIGURE 6.2 INFORMATION FLOW ARCHITECTURE	106
8. USER GUIDE	117
FIGURE 8.1 RUNNING SERVER SOFTWARE	118
FIGURE 8.2 RUNNING CLIENT SOFTWARE	118
FIGURE 8.3 KERBEROS CLIENT STATUS	119
FIGURE 8.4 DATA RECORDING STATUS	120
FIGURE 8.5 MPDR STATUS	121
FIGURE 8.6 IN RANGE OBJECT INFORMATION	121
FIGURE 8.7 CHANNEL LINK STATUS	122

FIGURE 8.8 CONSOLE ADMINISTRATION..... 122