

# Acknowledgment

At the beginning of this research, I held the opinion that this research would be too easy to finish it by myself without the help of others, but later the I realized that it was not so, and that every human being needs the help of others as well as that human being should help others in order to live in harmony and satisfied with this life.

It was found that this research needed beside the researcher's effort, the appropriate help of those who supervise, support, and encourage him to come up with a fruitful conclusion.

So the I expresses my deep thanks and appreciation to those who helped me, especially my supervisor **Dr. Yahia AbdAllah Mohamed, Dr. Mohamed Owad**, for their counseling and patience, also for **Eng. Gafar Wadidi** for his great support, and finally for kindly help of Data Center Staff ,computer center, Sudan university.

## **ABSTRACT**

Many Information Technology Departments in both large and small organizations use more than one operating system. Sudan University use Microsoft windows server for domain control as centralized identity management. License cost and client access one of the major problems of Microsoft server. In addition to this durability and batches require a reboot which made additional problem to the service.

This research use open-source software and non-commercial technologies in order to implement reliable solution which offers benefits of high availability. This research employed network of integrated (Light weight Directory Access Protocol LDAP as back end to centralized identity management, Samba as file and printer sharing, and Kerberos as authentication service).

By developing secure domain control, the licensing costs and management overhead has been reduced, in addition to that security performance and scalability has been improved

في كثير من شعب تكنولوجيا المعلومات في المؤسسات الكبيرة والصغيرة يستخدم اكثر من نظام تشغيل. تستخدم جامعة السودان للعلوم والتكنولوجيا مخدمات مايكروسوفت ويندوز للتحكم في مجال وحدة الادارة المركزية. ان تكاليف الترخيص و تكلفة ادخال اي زبون هي واحدة من اهم المشاكل في مخدمات مايكروسوفت. بالاضافة الي اعادة تشغيل النظام عند اضافة برامج جديدة مما يؤدي الي عدم استقراره.

لحل هذه المشاكل تم استخدام برامج مفتوحة المصدر وتكنولوجيا غير تجارية بتطبيق حل يمكن الاعتماد عليه بطريقة متاحة وذات كفاءة عالية. تم استخدام شبكة من المخدمات ( بروتوكول الدليل سريع الوصول باعتباره كوحدة ادارة مركزية, السامبا في مشاركة الملفات وبروتكول التحقق كيربيروز).

بالتحول الي مجال التحكم الامن المطور. حصلنا علي تقليل في التكلفة وادارة موحدة لمستخدمي الشبكة. بالاضافة الي تحسين في طريقة الوصول مع سرية في بيانات الشبكة.

## Table of Contents

|                       |  |     |
|-----------------------|--|-----|
| Acknowledgment        |  | II  |
| Abstract              |  | III |
| Abstract (in Arabic)  |  | IV  |
| Table of contents     |  | V   |
| List of figures       |  | IX  |
| List of tables        |  | XI  |
| List of abbreviations |  | XII |
| Chapter 1             | INTRODUCTION   |     |
| 1.1                   | Introduction   | 2   |
| 1.2                   | Problem Statement  | 3   |
| 1.3                   | Objectives of the Research   | 3   |
| 1.4                   | Implementation Phases  | 4   |
| 1.5                   | Thesis layout  | 5   |
| Chapter 2             | THE LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)   |     |
| 2.1                   | Introduction to LDAP   | 7   |
| 2.2                   | <i>Previous Studies</i>  | 8   |
| 2.2.1                 | <i>Manchester Metropolitan University has turned to Linux for the backbone of one the largest online learning projects in the UK</i> | 8   |
| 2.2.2                 | <i>Towards Automated Authorization Policy Enforcement</i>  | 8   |
| 2.3                   | <i>Directories</i>   | 5   |
| 2.4                   | <i>Directory versus database</i>   | 10  |
| 2.5                   | <i>LDAP: Protocol or directory</i>   | 12  |
| 2.6                   | <i>Directory clients and servers</i>   | 13  |
| 2.7                   | <i>Distributed directories</i>   | 14  |
| 2.8                   | <i>Advantages of using a directory</i>   | 15  |
| 2.9                   | <i>Network Information Service</i>   | 17  |
| 2.9.1                 | <i>X.500 the Directory Server Standard</i>   | 19  |
| 2.9.2                 | <i>Lightweight Access to X.500</i>   | 19  |
| 2.10                  | <i>LDAP concepts and architecture</i>  | 21  |
| 2.10.1                | <i>LDAP architecture</i>   | 21  |
| 2.10.2                | <i>The LDAP URL Format</i>   | 25  |
| 2.11                  | <i>The informational model</i>   | 26  |
| 2.12                  | <i>LDIF</i>  | 30  |
| 2.13                  | <i>LDAP schema</i>   | 31  |
| 2.13.1                | <i>Object classes</i>  | 31  |
| 2.13.2                | <i>Ldap attributes</i>   | 34  |
| 2.13.3                | <i>The naming model</i>  | 35  |
| 2.13.4                | <i>LDAP distinguished name syntax (DNs)</i>  | 36  |

|           |          |  |    |
|-----------|----------|--|----|
| 2.14      |          | <i>Functional model</i>                                | 37 |
|           | 2.14.1   | <i>Ldap queries</i>                                    | 38 |
|           | 2.14.2   | <i>Search filter syntax</i>                            | 40 |
|           | 2.14.2.1 | <i>Ldap compare</i>                                    | 41 |
|           | 2.14.2.2 | <i>Update operation</i>                                | 41 |
|           | 2.14.2.3 | <i>Authentication Operation</i>                        | 42 |
|           | 2.14.2.4 | <i>Control and Extended Operation</i>                  | 42 |
| 2.15      |          | <i>Security model</i>                                  | 43 |
| 2.16      |          | <i>Directory security</i>                              | 44 |
|           | 2.16.1   | <i>No authentication</i>                               | 45 |
|           | 2.16.2   | <i>Basic authentication</i>                            | 45 |
|           | 2.16.3   | <i>SASL (Simple Authentication Security Layer)</i>     | 46 |
|           | 2.16.4   | <i>SSL and TLS</i>                                     | 46 |
| Chapter 3 |          | <b>KERBEROS</b>  |    |
| 3.1       |          | <i>Introduction</i>                                    | 50 |
| 3.2       |          | <i>The Benefits of Kerberos</i>                        | 52 |
| 3.3       |          | <i>Hardware</i>  | 52 |
| 3.4       |          | <i>The Basics of Kerberos</i>                          | 53 |
| 3.5       |          | <i>The Ticket Granting Server</i>                      | 54 |
| 3.6       |          | <i>Cross-Realm Authentication</i>                      | 56 |
| 3.7       |          | <i>Kerberos and Public-Key Cryptography</i>            | 66 |
| 3.8       |          | <i>Public Key Infrastructure</i>                       | 70 |
| 3.11      |          | <i>GSSAPI</i>  | 73 |
| 3.12      |          | <i>SASL (Simple Authentication and Security Layer)</i> | 74 |
| 3.13      |          | <i>Changes for Version 5</i>                           | 58 |
|           | 3.13.1   | <i>Changes between Versions 4 and 5</i>                | 58 |
|           | 3.13.1.1 | <i>Use of Encryption</i>                               | 58 |
|           | 3.13.1.2 | <i>Network addresses</i>                               | 59 |
|           | 3.13.1.3 | <i>Message encoding</i>                                | 59 |
|           | 3.13.1.4 | <i>Ticket changes</i>                                  | 60 |
|           | 3.13.1.5 | <i>Naming principles</i>                               | 60 |
|           | 3.13.1.6 | <i>Inter-realm support</i>                             | 61 |
|           | 3.13.2   |  | 62 |
|           |          | <i>New protocol features in Version 5</i>              |    |
|           | 3.13.2.1 |  | 62 |
|           |          | <i>Tickets</i>   |    |
|           | 3.13.3   |  | 63 |
|           |          | <i>Authorization data</i>                              |    |
|           | 3.13.4   |  | 65 |
|           |          | <i>Pre-authentication data</i>                         |    |
|           | 3.13.5   |  | 65 |
|           |          | <i>Sub session key negotiation</i>                     |    |
|           | 3.13.6   |  | 66 |
|           |          | <i>Sequence numbers</i>                                |    |
| Chapter 4 |          | <b>THE PROPOSED FRAMEWORK</b>                          |    |
| 4.1       |          | <i>Sudan University Network Architecture</i>           | 76 |

|           |       |   |     |
|-----------|-------|---|-----|
| 4.2       |       | <i>Wireless Point to Point Campus</i>               | 79  |
| 4.3       |       | <i>SUST Data Center Architecture</i>                | 81  |
| 4.4       |       | <i>Proposed framework</i>                           | 84  |
| 4.5       |       | <i>Implementation</i>                               | 84  |
| 4.6       |       | <i>Domain control using samba</i>                   | 91  |
| 4.7       |       | <i>Authentications Kerberos and Ldap</i>            | 93  |
| 4.8       |       | <i>Configuration of Master Domain</i>               | 94  |
|           | 4.8.1 | <i>Configure the SUST LDAP Server files</i>         | 94  |
|           |       | 4.8.1.1 <i>Configure the ldap.conf</i>              | 94  |
|           |       | 4.8.1.2 <i>Configure the slapd.conf</i>             | 95  |
|           |       | 4.8.1.3 <i>Configure the /etc/nsswitch.conf</i>     | 95  |
|           | 4.8.2 | <i>Configure the SUST Kerberos Server files</i>     | 95  |
|           | 4.8.3 | <i>Configure the SUST Samba Server files</i>        | 97  |
|           |       | 4.8.3.1.1 <i>The global section</i>                 | 97  |
|           |       | 4.8.3.1.2 <i>The home section</i>                   | 98  |
|           | 4.8.4 | <i>Start the domain smb, winbind, ldap services</i> | 98  |
|           | 4.8.5 | <i>Joining the sust samba domain</i>                | 98  |
| Chapter 5 |       | <b>IMPLEMENTATION AND RESULTS</b>                   |     |
| 5.1       |       | <i>Implementation Steps</i>                         | 100 |
| 5.2       |       | <i>Joining the Linux client to sust domain</i>      | 102 |
| 5.3       |       | <i>Joining The Windows Client to Sust Domain</i>    | 103 |
| 5.4       |       | <i>Result</i>                                       | 103 |
| 5.5       |       | <i>Implementation problem</i>                       | 104 |
|           |       | <b>Chapter 6</b>                                    |     |
|           |       | <b>Summary and Recommendations</b>                  |     |
| 6.1       |       | <i>summary</i>                                      | 106 |
| 6.2       |       | <i>Recommendation</i>                               | 107 |
|           |       | <i>Appendix</i>                                     | 108 |
|           |       | <i>References</i>                                   | 121 |

## LIST OF FIGURES

| <b>FIGURE<br/>NO</b> |  | <b>PAGE</b> |
|----------------------|--|-------------|
| Figure 2.1           | <i>Several applications using attribute of the same entry</i>      | 16          |
| Figure 2.2           | <i>Relation between a directory Entries, attributes and values</i> | 26          |
| Figure 2.3           | <i>Directory Information Tree (DIT)</i>                            | 34          |
| Figure 3.1           | <i>SUST Kerberos Authentication Server</i>                         | 55          |
| Figure 3.2           | <i>Cross Realm Authentication</i>                                  | 56          |
| Figure 3.3           | <i>Inter Realm Diagram</i>   | 60          |
| Figure 3.4           | <i>Key Management</i>  | 68          |
| Figure 3.5           | <i>GSSAPI Mechanism Diagram</i>                                    | 73          |
| Figure 4.1           | <i>main Zone Diagram</i>   | 76          |
| Figure 4.2           | <i>wireless point-to-point connection Diagram</i>                  | 78          |
| Figure 4.3           | <i>Wireless Point To Point Campus Design</i>                       | 79          |
| Figure 4.4           | <i>Wireless Point To Point Campus Design Two</i>                   | 79          |
| Figure 4.5           | <i>Wireless Point to Point Campus Design Three</i>                 | 80          |
| Figure 4.6           | <i>Main SUST Servers</i>   | 81          |
| Figure 4.7           | <i>suggested Design Scenario for the sust Server</i>               | 83          |
| Figure 4.8           | <i>SUST Domain Architecture</i>                                    | 87          |
| Figure 4.9           | <i>Sust Domain Control Using Samba</i>                             | 88          |
| Figure 4.10          | <i>Integration of SUST LDAP, UNIX Accounts and Samba Accounts</i>  | 90          |
| Figure 4.11          | <i>SUST LDAP Authentication Using Samba Server</i>                 | 91          |
| Figure 5.1           | <i>Windows System Properties</i>                                   | 101         |

|            |                               |     |
|------------|-------------------------------|-----|
| Figure 5.2 | <i>Adding Domain Name</i>     | 102 |
| Figure 5.3 | <i>Joining domain Screen</i>  | 102 |
| Figure 5.4 | <i>Domain Joining Message</i> | 103 |
| Figure 5.5 | <i>Restarting windows</i>     | 103 |
| Figure 5.5 | <i>System properties</i>      | 104 |

### **LIST OF TABLES**

|           |   |    |
|-----------|---|----|
| Table 2.1 | <i>LDAP attribute syntaxes</i>                        | 22 |
| Table 2.2 | <i>Common LDAP attributes</i>                         | 27 |
| Table 2.3 | <i>LDAP common Schema(Object classes and required</i> | 28 |



|           |   |    |
|-----------|---|----|
|           | <i>attributes</i>                       |    |
| Table 2.6 | <i>LDAP Update operations</i>           | 40 |
| Table 2.7 | <i>LDAP Authentication operations</i>   | 41 |
| Table 4.1 | <i>Total PCs, Student and Employees</i> | 79 |

## **LIST OF ABBREVIATIONS**

|              |   |
|--------------|---|
| <i>ADSI</i>  | <i>Active Directory Service Interface</i> |
| <i>AFS</i>   | <i>Andrew File System</i>                 |
| <i>API</i>   | <i>Application Programming Interface</i>  |
| <i>AS</i>    | <i>Authentication Server</i>              |
| <i>ASN.1</i> | <i>Abstract Syntax Notation One</i>       |

|               |  |
|---------------|--|
| <i>BDB</i>    | <i>Berkley database</i>  |
| <i>CAL</i>    | <i>Client Access License</i>                                       |
| <i>CBC</i>    | <i>Cipher Block Chaining</i>                                       |
| <i>CRL</i>    | <i>Certificate Revocation List</i>                                 |
| <i>DC</i>     | <i>distinct common</i>   |
| <i>DCE</i>    | <i>Distributed Computing Environment</i>                           |
| <i>DES</i>    | <a href="#"><u>Data Encryption Standard</u></a>                    |
| <i>EDU</i>    | <i>Education</i>   |
| <i>FTP</i>    | <i>File Transfer Protocol</i>                                      |
| <i>GID</i>    | <i>Group ID</i>  |
| <i>GSSAPI</i> | <i>Generic Security Services Application Programming Interface</i> |
| <i>HTTP</i>   | <i>Hyper Text Terminal Protocol</i>                                |
| <i>IBM</i>    | <i>International Business Machine</i>                              |
| <i>ID</i>     | <i>Identity</i>  |
| <i>IETF</i>   | <i>Internet Engineering Task Force</i>                             |
| <i>JNDI</i>   | <i>Java Naming and Directory Interface</i>                         |
| <i>KDC</i>    | <i>key distribution center</i>                                     |
| <i>KRB</i>    | <i>Kerberos</i>  |
| <i>LDAP</i>   | <i>Lightweight Directory Access Protocol</i>                       |
| <i>MIT</i>    | <a href="#"><u>Ministry of Information Technology</u></a>          |
| <i>NFS</i>    | <i>New Technology File System</i>                                  |
| <i>NSS</i>    | <a href="#"><u>Name Services Switch</u></a>                        |
| <i>OS</i>     | <i>Operating System</i>  |
| <i>OTP</i>    | <i>one-time passwords</i>  |
| <i>PACs</i>   | <a href="#"><u>Programmable Automation Controls</u></a>            |
| <i>PAM</i>    | <i>Pluggable authentication modules</i>                            |
| <i>PDC</i>    | <i>Primary Domain Control</i>                                      |
| <i>PGP</i>    | <i>Pretty Good Privacy</i>   |

|               |   |
|---------------|---|
| <i>PKI</i>    | <i>Public Key Infrastructure</i>  |
| <i>PKIX</i>   | <i><a href="#">Public-Key Infrastructure (X.509)</a></i>  |
| <i>RFC</i>    | <i>Request for Comments</i>   |
| <i>RTGS</i>   | <i>Remote Ticket Granting Service</i>   |
| <i>SASL</i>   | <i>Simple Authentication and Security Layer</i>   |
| <i>SDSI</i>   | <i>Simple Distributed Security Infrastructure</i>   |
| <i>SESAME</i> | <i>Secure European System for Applications in a Multi-vendor Environment</i>  |
| <i>SID</i>    | <i>Windows identity</i>   |
| <i>SMB</i>    | <i>Server Message Block</i>   |
| <i>SOLGSS</i> | <i>GSS-API Programming Guide</i>  |
| <i>SPKI</i>   | <i>Simple Public Key Infrastructure</i>   |
| <i>SQL</i>    | <i>Structured Query Language</i>  |
| <i>SUST</i>   | <i>Sudan University of Science and Technology</i>   |
| <i>TCO</i>    | <i>Total cost of ownership</i>  |
| <i>TGS</i>    | <i>Ticket Granting Service</i>  |
| <i>UID</i>    | <i>Unique ID</i>  |
| <i>X.509</i>  | <i>is an <a href="#">ITU-T</a> standard for a (PKI) and <a href="#">Privilege Management Infrastructure (PMI)</a></i> |