



Auerbach Publications  
Taylor & Francis Group

# Mechanics of User Identification and Authentication

Fundamentals of  
Identity Management

**DOBROMIR TODOROV**

# Contents

<b>Acknowledgments .....</b>	<b>xix</b>
<b>About the Author .....</b>	<b>xxi</b>
<b>About This Book .....</b>	<b>xxiii</b>
<b>1 User Identification and Authentication Concepts.....</b>	<b>1</b>
1.1 Security Landscape .....	1
1.2 Authentication, Authorization, and Accounting.....	3
1.2.1 Identification and Authentication.....	4
1.2.2 Authorization .....	7
1.2.3 User Logon Process .....	8
1.2.4 Accounting.....	8
1.3 Threats to User Identification and Authentication .....	9
1.3.1 Bypassing Authentication .....	9
1.3.2 Default Passwords.....	10
1.3.3 Privilege Escalation .....	10
1.3.4 Obtaining Physical Access.....	11
1.3.5 Password Guessing: Dictionary, Brute Force, and Rainbow Attacks.....	12
1.3.6 Sniffing Credentials off the Network.....	14
1.3.7 Replaying Authentication.....	14
1.3.8 Downgrading Authentication Strength .....	15
1.3.9 Imposter Servers.....	15
1.3.10 Man-in-the-Middle Attacks.....	16
1.3.11 Session Hijacking .....	16
1.3.12 Shoulder Surfing.....	16
1.3.13 Keyboard Loggers, Trojans, and Viruses.....	17
1.3.14 Offline Attacks.....	17
1.3.15 Social Engineering.....	17
1.3.16 Dumpster Diving and Identity Theft .....	18

1.4	Authentication Credentials .....	18
1.4.1	Password Authentication .....	20
1.4.1.1	Static Passwords .....	20
1.4.1.2	One-Time Passwords .....	22
1.4.2	Asymmetric Keys and Certificate-Based Credentials .....	26
1.4.3	Biometric Credentials .....	34
1.4.4	Ticket-Based Hybrid Authentication Methods .....	37
1.5	Enterprise User Identification and Authentication Challenges .....	39
1.6	Authenticating Access to Services and the Infrastructure .....	43
1.6.1	Authenticating Access to the Infrastructure .....	43
1.6.2	Authenticating Access to Applications and Services .....	44
1.7	Delegation and Impersonation .....	45
1.8	Cryptology, Cryptography, and Cryptanalysis .....	45
1.8.1	The Goal of Cryptography .....	46
1.8.2	Protection Keys .....	47
1.8.2.1	Symmetric Encryption .....	49
1.8.2.2	Asymmetric Keys .....	51
1.8.2.3	Hybrid Approaches: Diffie-Hellman Key Exchange Algorithm .....	52
1.8.3	Encryption .....	54
1.8.3.1	Data Encryption Standard (DES/3DES) .....	55
1.8.3.2	Advanced Encryption Standard (AES) .....	57
1.8.3.3	RC4 (ARCFOUR) .....	58
1.8.3.4	RSA Encryption Algorithm (Asymmetric Encryption) .....	58
1.8.4	Data Integrity .....	59
1.8.4.1	Message Integrity Code (MIC) .....	60
1.8.4.2	Message Authentication Code (MAC) .....	61
<b>2</b>	<b>UNIX User Authentication Architecture .....</b>	<b>65</b>
2.1	Users and Groups .....	65
2.1.1	Overview .....	66
2.1.2	Case Study: Duplicate UIDs .....	67
2.1.3	Case Study: Group Login and Supplementary Groups .....	68
2.2	Simple User Credential Stores .....	69
2.2.1	UNIX Password Encryption .....	70
2.2.2	The /etc/passwd File .....	73
2.2.3	The /etc/group File .....	76
2.2.4	The /etc/shadow File .....	76
2.2.5	The /etc/gshadow File .....	79
2.2.6	The /etc/publickey file .....	80
2.2.7	The /etc/cram-md5.pwd File .....	81
2.2.8	The SASL User Database .....	82
2.2.9	The htpasswd File .....	82
2.2.10	Samba Credentials .....	83
2.2.11	The Kerberos Principal Database .....	84
2.3	Name Services Switch (NSS) .....	84

2.4	Pluggable Authentication Modules (PAM).....	88
2.5	The UNIX Authentication Process .....	95
2.6	User Impersonation.....	96
2.7	Case Study: User Authentication against LDAP .....	104
2.7.1	Preparing Active Directory .....	105
2.7.2	PADL LDAP Configuration.....	105
2.7.3	User Authentication Using NSS LDAP .....	108
2.7.4	User Authentication Using PAM LDAP.....	124
2.8	Case Study: Using Hesiod for User Authentication in Linux .....	129
<b>3</b>	<b>Windows User Authentication Architecture .....</b>	<b>139</b>
3.1	Security Principals .....	140
3.1.1	Security Identifiers (SIDs).....	140
3.1.2	Users and Groups .....	140
3.1.3	Case Study: Group SIDs.....	152
3.1.4	Access Tokens .....	153
3.1.5	Case Study: SIDs in the User Access Token .....	155
3.1.6	User Rights.....	157
3.2	Stand-Alone Authentication .....	160
3.2.1	Interactive and Network Authentication .....	161
3.2.2	Interactive Authentication on Windows Computers .....	162
3.2.3	The Security Accounts Manager Database.....	165
3.2.4	Case Study: User Properties — Windows NT Local User Accounts .....	168
3.2.5	Case Study: Group Properties — Windows Local Group Accounts .....	169
3.2.6	SAM Registry Structure .....	170
3.2.7	User Passwords .....	173
3.2.8	Storing Password Hashes in the Registry SAM File .....	174
3.2.8.1	LM Hash Algorithm.....	174
3.2.8.2	NT Hash Algorithm.....	178
3.2.8.3	Password Hash Obfuscation Using DES.....	178
3.2.8.4	SYSKEY Encryption for Storing Password Hashes in the SAM .....	179
3.2.8.5	Case Study: The SYSKEY Utility, the System Key, and Password Encryption Key.....	181
3.2.8.6	Threats to Windows Password Hashes.....	185
3.2.8.7	Tools to Access Windows Password Hashes.....	188
3.2.8.8	Case Study: Accessing Windows Password Hashes with pwdump4.....	188
3.2.9	LSA Secrets .....	190
3.2.9.1	Case Study: Exploring LSA Secrets on a Windows NT 4.0 Domain Controller That Is an Exchange 5.5 Server.....	192
3.2.10	Logon Cache.....	197
3.2.11	Protected Storage .....	199
3.2.12	Data Protection API (DPAPI) .....	200

3.2.13	Credential Manager .....	205
3.2.14	Case Study: Exploring Credential Manager.....	208
3.3	Windows Domain Authentication .....	210
3.3.1	Domain Model.....	210
3.3.2	Joining a Windows NT Domain .....	214
3.3.3	Computer Accounts in the Domain .....	215
3.3.4	Domains and Trusts .....	217
3.3.5	Case Study: Workstation Trust and Interdomain Trust .....	219
3.3.6	SID Filtering across Trusts.....	220
3.3.7	Migration and Restructuring.....	222
3.3.8	Null Sessions .....	224
3.3.9	Case Study: Using Null Sessions Authentication to Access Resources .....	227
3.3.10	Case Study: Domain Member Start-up and Authentication.....	230
3.3.11	Case Study: Domain Controller Start-up and Authentication.....	233
3.3.12	Case Study: Windows NT 4.0 Domain User Logon Process .....	233
3.3.13	Case Study: User Logon to Active Directory Using Kerberos.....	235
3.3.14	Windows NT 4.0 Domain Model.....	235
3.3.14.1	User Accounts .....	235
3.3.14.2	Group Accounts and Group Strategies .....	236
3.3.14.3	Authentication Protocols: NTLM and LM.....	237
3.3.14.4	Trust Relationships.....	237
3.3.15	Active Directory.....	240
3.3.15.1	Active Directory Overview .....	240
3.3.15.2	Logical and Physical Structure .....	240
3.3.15.3	Active Directory Schema .....	244
3.3.15.4	Database Storage for Directory Information.....	245
3.3.15.5	Support for Legacy Windows NT Directory Services .....	246
3.3.15.6	Hierarchical LDAP-Compliant Directory.....	249
3.3.15.7	Case Study: Exploring Active Directory Using LDP.EXE .....	249
3.3.15.8	User Accounts in AD.....	252
3.3.15.9	Case Study: User Logon Names in Active Directory .....	257
3.3.15.10	Case Study: Using LDAP to Change User Passwords in Active Directory.....	259
3.3.15.11	Case Study: Obtaining Password Hashes from Active Directory.....	262
3.3.15.12	Group Accounts and Group Strategy in AD .....	262
3.3.15.13	Case Study: Exploring the Effects of Group Nesting to User Access Token.....	266
3.3.15.14	Computer Accounts in AD.....	270

3.3.15.15	Trees, Forests, and Intra-forest Trusts .....	270
3.3.15.16	Case Study: User Accesses Resources in Another Domain in the Same Forest .....	275
3.3.15.17	Trusts with External Domains .....	279
3.3.15.18	Case Study: Exploring External Trusts .....	281
3.3.15.19	Case Study: Exploring Forest Trusts .....	283
3.3.15.20	Selective Authentication .....	285
3.3.15.21	Case Study: Exploring Authentication Firewall and User Access Tokens .....	287
3.3.15.22	Protocol Transition .....	290
3.4	Federated Trusts .....	291
3.5	Impersonation .....	291
3.5.1	Secondary Logon Service .....	292
3.5.2	Application-Level Impersonation .....	294
<b>4</b>	<b>Authenticating Access to Services and Applications .....</b>	<b>301</b>
4.1	Security Programming Interfaces .....	301
4.1.1	Generic Security Services API (GSS-API) .....	302
4.1.1.1	Kerberos Version 5 as a GSS-API Mechanism .....	306
4.1.1.2	SPNEGO as a GSS-API Mechanism .....	308
4.1.2	Security Support Provider Interface (SSPI) .....	310
4.1.2.1	SSP Message Support .....	311
4.1.2.2	Strong Keys and 128-bit Encryption .....	312
4.1.2.3	SSPI Signing .....	314
4.1.2.4	SSPI Sealing (Encryption) .....	314
4.1.2.5	Controlling SSP Behavior Using Group Policies .....	314
4.1.2.6	Microsoft Negotiate SSP .....	315
4.1.2.7	GSS-API and SSPI Compatibility .....	330
4.2	Authentication Protocols .....	331
4.2.1	NTLM Authentication .....	331
4.2.1.1	NTLM Overview .....	331
4.2.1.2	The Concept of Trust and Secure Channels .....	332
4.2.1.3	Domain Member Secure Channel Establishment .....	334
4.2.1.4	Domain Controller Secure Channel Establishment across Trusts .....	338
4.2.1.5	SMB/CIFS Signing .....	339
4.2.1.6	Case Study: Pass-through Authentication and Authentication Piggybacking .....	342
4.2.1.7	NTLM Authentication Mechanics .....	344
4.2.1.8	Case Study: NTLM Authentication Scenarios .....	362
4.2.1.9	NTLM Impersonation .....	387
4.2.2	Kerberos Authentication .....	387
4.2.2.1	Kerberos Overview .....	387
4.2.2.2	The Concept of Trust in Kerberos .....	388
4.2.2.3	Name Format for Kerberos Principals .....	389

4.2.2.4	Kerberos Authentication Phases .....	389
4.2.2.5	Kerberos Tickets.....	391
4.2.2.6	Kerberos Authentication Mechanics .....	394
4.2.2.7	Case Study: Kerberos Authentication: CIFS .....	403
4.2.2.8	Authorization Information and the Microsoft PAC Attribute .....	414
4.2.2.9	Kerberos Credentials Exchange (KRB_CRED) .....	416
4.2.2.10	Kerberos and Smart Card Authentication (PKInit).....	416
4.2.2.11	Kerberos User-to-User Authentication .....	418
4.2.2.12	Kerberos Encryption and Checksum Mechanisms .....	420
4.2.2.13	Case Study: Kerberos Authentication Scenarios .....	423
4.2.2.14	Kerberos Delegation .....	428
4.2.3	Simple Authentication and Security Layer (SASL).....	430
4.2.3.1	Kerberos IV .....	432
4.2.3.2	GSS-API.....	433
4.2.3.3	S/Key Authentication Mechanism .....	433
4.2.3.4	External Authentication .....	433
4.2.3.5	SASL Anonymous Authentication.....	433
4.2.3.6	SASL CRAM-MD5 Authentication .....	434
4.2.3.7	SASL Digest-MD5 Authentication .....	437
4.2.3.8	SASL and User Password Databases .....	445
4.3	Transport Layer Security (TLS) and Secure Sockets Layer (SSL) ....	446
4.3.1	Hello Phase .....	449
4.3.2	Server Authentication Phase.....	450
4.3.3	Client Authentication Phase .....	451
4.3.3.1	Calculate the Master Secret.....	452
4.3.3.2	Calculate Protection Keys.....	453
4.3.4	Negotiate Start of Protection Phase.....	454
4.3.5	Resuming TLS/SSL Sessions.....	454
4.3.6	Using SSL/TLS to Protect Generic User Traffic .....	454
4.3.7	Using SSL/TLS Certificate Mapping as an Authentication Method .....	455
4.4	Telnet Authentication .....	464
4.4.1	Telnet Login Authentication .....	465
4.4.2	Telnet Authentication Option.....	470
4.5	FTP Authentication.....	479
4.5.1	FTP Simple Authentication.....	480
4.5.2	Anonymous FTP.....	481
4.5.3	FTP Security Extensions with GSS-API .....	481
4.5.4	FTP Security Extensions with TLS .....	485
4.6	HTTP Authentication.....	486
4.6.1	HTTP Anonymous Authentication .....	487
4.6.2	HTTP Basic Authentication .....	489
4.6.3	HTTP Digest Authentication.....	492

4.6.4	HTTP GSS-API/SSPI Authentication Using SPNEGO and Kerberos.....	495
4.6.5	HTTP NTLMSSP Authentication .....	501
4.6.6	HTTP SSL Certificate Mapping as an Authentication Method.....	501
4.6.7	Form-Based Authentication .....	506
4.6.8	Microsoft Passport Authentication .....	506
4.6.9	HTTP Proxy Authentication .....	509
4.7	POP3/IMAP Authentication .....	510
4.7.1	POP3/IMAP Password Authentication .....	510
4.7.2	POP3/IMAP Plain Authentication.....	511
4.7.3	POP3 APOP Authentication .....	511
4.7.4	POP3/IMAP Login Authentication.....	513
4.7.5	POP3/IMAP SASL CRAM-MD5 and DIGEST-MD5 Authentication.....	513
4.7.6	POP3/IMAP and NTLM Authentication (Secure Password Authentication).....	513
4.8	SMTP Authentication.....	515
4.8.1	SMTP Login Authentication.....	517
4.8.2	SMTP Plain Authentication.....	519
4.8.3	SMTP GSS-API Authentication.....	519
4.8.4	SMTP CRAM-MD5 and DIGEST-MD5 Authentication .....	520
4.8.5	SMTP Authentication Using NTLM .....	520
4.9	LDAP Authentication.....	520
4.9.1	Simple Authentication.....	522
4.9.2	LDAP Anonymous Authentication .....	522
4.9.3	LDAP SASL Authentication Using Digest-MD5 .....	522
4.9.4	LDAP SASL Authentication Using GSS-API.....	526
4.10	SSH Authentication.....	533
4.10.1	SSH Public Key Authentication.....	535
4.10.2	SSH Host Authentication .....	538
4.10.3	SSH Password Authentication .....	539
4.10.4	SSH Keyboard Interactive Authentication .....	541
4.10.5	SSH GSS-API User Authentication .....	541
4.10.6	SSH GSS-API Key Exchange and Authentication .....	543
4.11	Sun RPC Authentication.....	544
4.11.1	RPC AUTH_NULL (AUTH_NONE) Authentication .....	545
4.11.2	RPC AUTH_UNIX (AUTH_SYS) Authentication.....	549
4.11.3	RPC AUTH_SHORT Authentication .....	553
4.11.4	RPC AUTH_DES (AUTH_DH) Authentication.....	553
4.11.5	RPC AUTH_KERB4 Authentication .....	558
4.11.6	RPCSEC_GSS Authentication .....	558
4.12	SMB/CIFS Authentication.....	560
4.13	NFS Authentication.....	561
4.14	Microsoft Remote Procedure Calls.....	561
4.15	MS SQL Authentication .....	562
4.15.1	MS SQL Authentication over the TCP/IP Transport.....	563



4.15.2	MS SQL Server Authentication over Named Pipes.....	564
4.15.3	MS SQL Server Authentication over Multiprotocol.....	565
4.15.4	MS SQL Server and SSL.....	566
4.16	Oracle Database Server Authentication.....	567
4.16.1	Oracle Legacy Authentication Database.....	567
4.16.2	Legacy OracleNet Authentication.....	568
4.16.3	Oracle Advanced Security Mechanisms for User Authentication.....	570
4.17	MS Exchange MAPI Authentication.....	571
4.18	SAML, WS-Security, and Federated Identity.....	571
4.18.1	XML and SOAP.....	572
4.18.2	SAML.....	572
4.18.2.1	SAML and Web Single Sign-On.....	575
4.18.2.2	Case Study: Web Single Sign-On Mechanics.....	577
4.18.2.3	SAML Federated Identity.....	578
4.18.2.4	Account Linking.....	578
4.18.3	WS-Security.....	580
<b>5</b>	<b>Authenticating Access to the Infrastructure.....</b>	<b>583</b>
5.1	User Authentication on Cisco Routers and Switches.....	583
5.1.1	Authentication to Router Services.....	584
5.1.2	Local User Database and Passwords.....	585
5.1.3	Centralizing Authentication.....	588
5.1.4	New-Model AAA.....	589
5.2	Authenticating Remote Access to the Infrastructure.....	590
5.2.1	SLIP Authentication.....	590
5.2.2	PPP Authentication.....	590
5.2.3	Password Authentication Protocol (PAP).....	591
5.2.4	CHAP.....	593
5.2.5	MS-CHAP Version 1 and 2.....	594
5.2.6	Extensible Authentication Protocol (EAP).....	600
5.2.7	EAP-TLS.....	603
5.2.8	EAP-TTLS.....	604
5.2.9	Protected EAP (PEAP).....	605
5.2.10	Lightweight EAP (LEAP).....	606
5.2.11	EAP-FAST.....	607
5.2.11.1	EAP-FAST Automatic Provisioning (EAP-FAST Phase 0).....	608
5.2.11.2	Tunnel Establishment (EAP-Phase 1).....	610
5.2.11.3	User Authentication (EAP-FAST Phase 2).....	610
5.3	Port-Based Access Control.....	611
5.3.1	Overview of Port-Based Access Control.....	613
5.3.2	EAPOL.....	614
5.3.3	EAPOL Key Messages.....	616
5.4	Authenticating Access to the Wireless Infrastructure.....	623
5.4.1	Wi-Fi Authentication Overview.....	624
5.4.2	WEP Protection.....	625

5.4.3	Open Authentication.....	627
5.4.4	Shared Key Authentication.....	633
5.4.5	WPA/WPA2 and IEEE 802.11i .....	639
5.4.6	WPA/WPA2 Enterprise Mode .....	641
5.4.7	WPA/WPA2 Preshared Key Mode (WPA-PSK).....	643
5.5	IPSec, IKE, and VPN Client Authentication .....	644
5.5.1	IKE Peer Authentication .....	644
5.5.1.1	IKE and IPSec Phases.....	645
5.5.1.2	Preshared Key Authentication.....	648
5.5.1.3	IKE Signature-Based Authentication .....	649
5.5.1.4	IKE Public Key Authentication, Option 1.....	650
5.5.1.5	IKE Public Key Authentication, Option 2.....	652
5.5.2	IKE XAUTH Authentication and VPN Clients.....	654
5.6	Centralized User Authentication.....	670
5.6.1	RADIUS .....	672
5.6.1.1	Overview.....	672
5.6.1.2	The Model of Trust in RADIUS .....	674
5.6.1.3	RADIUS Authentication Requests from Edge Devices.....	676
5.6.1.4	RADIUS and EAP Pass-through Authentication...	678
5.6.2	TACACS+ .....	682
5.6.2.1	Overview.....	683
5.6.2.2	TACACS+ Channel Protection .....	684
5.6.2.3	TACACS+ Authentication Process .....	684

## Appendices

<b>A</b>	<b>References .....</b>	<b>691</b>
	Printed References .....	691
	Online References.....	692
<b>B</b>	<b>Lab Configuration .....</b>	<b>701</b>
<b>C</b>	<b>Indices of Tables and Figures .....</b>	<b>705</b>
	Index of Tables.....	705
	Index of Figures.....	709
	<b>Index.....</b>	<b>713</b>