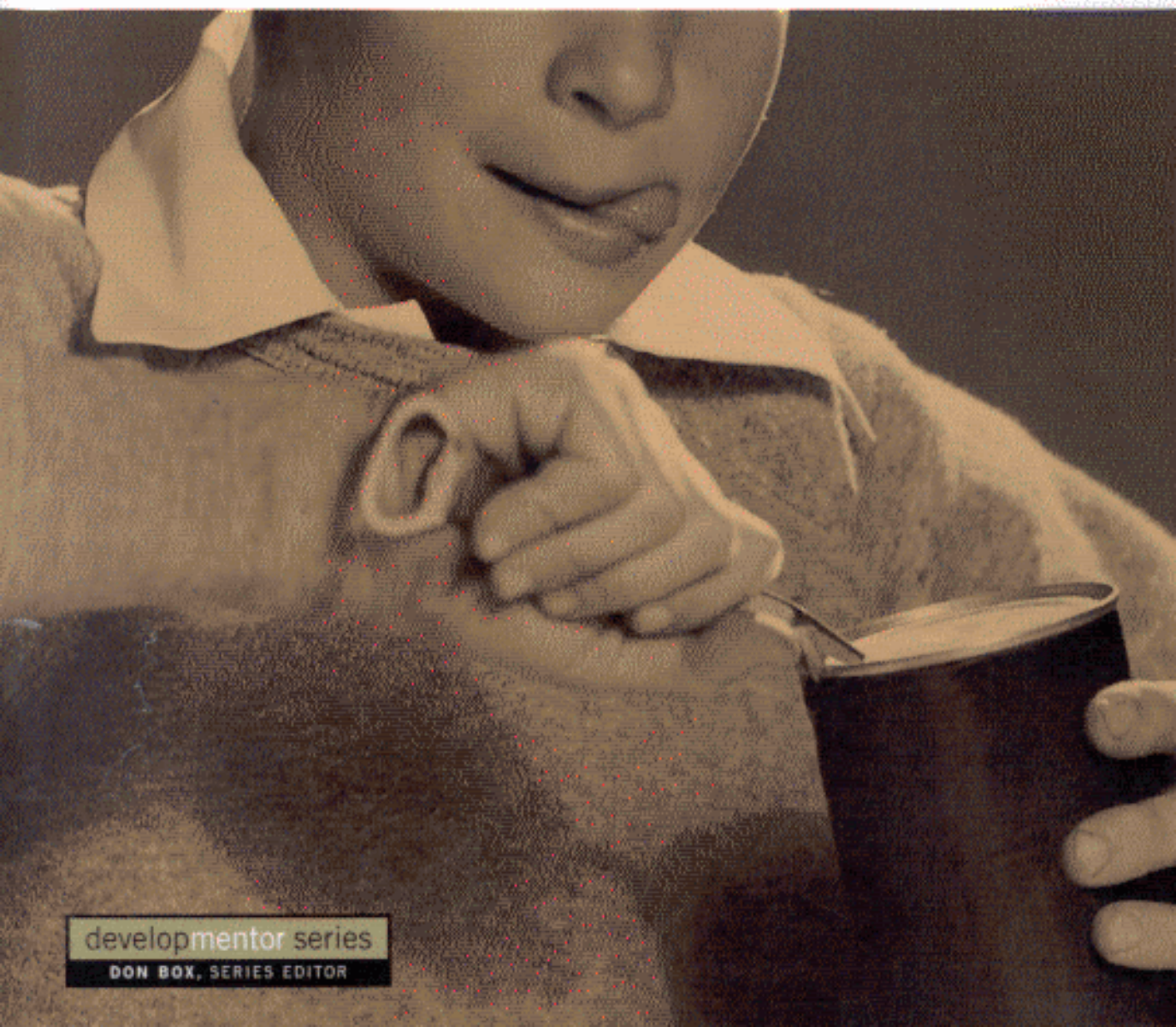


# Programming Windows Security

Keith Brown



developmentor series

DON BOX, SERIES EDITOR

# Contents

<b>Preface</b>	<b>xi</b>
----------------	-----------

<b>PART 1 ★ MODEL</b>	<b>1</b>
-----------------------	----------

<b>1 The Players</b>	<b>3</b>
----------------------	----------

Principals	3
Authorities	10
Machines as Principals	12
Authentication	12
Trust	18
Summary	24

<b>2 The Environment</b>	<b>27</b>
--------------------------	-----------

Logon Sessions	28
Tokens	32
The System Logon Session	35
Window Stations	37
Processes	41
Summary	42

<b>3 Enforcement</b>	<b>45</b>
----------------------	-----------

Authorization	45
Discovering Authorization Attributes	51
Distributed Applications	52
Objects and Security Descriptors	54
Access Control Strategies	56
Choosing a Model	62
Caching Mechanisms	63
Summary	69

<b>PART II ★ MECHANICS</b>	<b>71</b>
----------------------------	-----------

<b>4 Logon Sessions</b>	<b>73</b>
-------------------------	-----------

Logon Session 999	76
Daemon Logon Sessions	80

Network Logon Sessions	83
Interactive Logon Sessions	84
Network Credentials	86
Tokens	86
Memory Allocation and Error Handling Strategies	105
Using Privileges	106
Impersonation	112
Restricting Authorization Attributes	128
Terminating a Logon Session	133
Summary	134

## **5 Window Stations and Profiles 137**

What Is a Window Station?	137
Window Station Permissions	140
Natural Window Station Allocation	142
Daemons in the Lab	146
Other Window Stations	147
Exploring Window Stations	150
Closing Window Station Handles	152
Window Stations and Access Control	153
Desktops	154
Jobs, Revisited	164
Processes	165
Summary	177

## **6 Access Control and Accountability 179**

Permissions	180
Anatomy of a Security Descriptor	184
Where Do Security Descriptors Come From?	188
Security Descriptor Usage Patterns	191
How ACLs Work	194
Security Descriptors and Built-in Objects	206
Security Descriptors and Private Objects	208
Hierarchical Object Models and ACL Inheritance	210
ACL Programming	235
Handles	247
Summary	249

## **PART III ★ DISTRIBUTION 253**

### **7 Network Authentication 255**

The NTLM Authentication Protocol	256
----------------------------------	-----

The Kerberos v5 Authentication Protocol	273
SSPI	300
SPNEGO: Simple and Protected Negotiation	306
Summary	307
<b>8 The File Server</b>	<b>309</b>
Lan Manager	309
Lan Manager Sessions	310
Clients and Sessions	315
Use Records	318
NULL Sessions	325
Dealing with Conflict	327
Drive Letter Mappings	328
Named Pipes	329
SMB Signing	333
Summary	334
<b>9 COM(+)</b>	<b>337</b>
The MSRPC Security Model	338
The COM Security Model	355
COM Interception	370
Activation Requests	377
More COM Interception: Access Control	383
Plugging Obscure Security Holes	385
Security in In-process Servers?	386
Surrogates and Declarative Security	387
COM Servers Packaged as Services	390
Legacy Out-of-Process Servers	392
Launching Servers via the COM SCM	394
A Note on Choosing a Server Identity	399
Access Checks in the Middle Tier	400
The COM+ Security Model: Configured Components	401
Catalog Settings	404
Applications and Role-Based Security	407
Making Sense of COM+ Access Checks	416
Which Components Need Role Assignments?	422
Security in COM+ Library Applications	423
Fine-Grained Access Control: IsCallerInRole	426
Call Context Tracking	428
Tips for Debugging COM Security Problems	429
Summary	432

<b>10 IIS</b>	<b>435</b>
Authentication on the Web	436
Public Key Cryptography	440
Certificates	442
Secure Sockets Layer	448
Certificate Revocation	452
From Theory to Practice: Obtaining and Installing a Web Server Certificate	453
Requiring HTTPS via the IIS Metabase	457
Managing Web Applications	460
Client Authentication	465
Server Applications	475
IIS as a Gateway into COM+	482
Miscellaneous Topics	486
Where to Get More Information	489
Summary	490
<b>Appendix: Some Parting Words</b>	<b>493</b>
Well-Known SIDs	494
Printing SIDs in Human Readable Form	495
Adding Domain Principals in Windows 2000	498
Adding Groups in Windows 2000	500
Adding Local Accounts and Aliases	504
Privileges and Logon Rights	505
Secrets: The Windows Password Stash	507
<b>Glossary</b>	<b>517</b>
<b>Bibliography</b>	<b>541</b>
<b>Index</b>	<b>543</b>