

THE COMPROMISE OF MEDECO® HIGH SECURITY LOCKS: New Techniques of Forced, Covert, and Surreptitious Entry



LSS-701: The High Security Supplement to Locks, Safes, and Security

Version 08-117

Locks, Safes, and Security was first published in 1970 by Charles C. Thomas Publishers, Springfield, Illinois. The Second Edition was released in 2000. Supplementary materials can be found at www.security.org. This Infobase contains supplementary multimedia materials for *Locks, Safes, and Security*, electronic Infobase edition. Medeco® is a registered trademark of Medeco Security Locks, Inc.

Created by Marc Weber Tobias, B.S., J.D.

Member: ABA, ASIS, AFTE, ALOA, SAVTA, APA, AAFS, IAIL

and **Tobias Bluzmanis**

(c)1999-2008, Marc Weber Tobias, All Rights Reserved. This Infobase may not be copied, reproduced, transmitted, or regenerated in any form without the express written permission of the authors.

Table of Contents

Piracy Warning

Waivers and Disclaimers

Editions of this Book and Security Levels

Trademarks

Foreword by Barry Wels

Foreword by Harry Sher

Acknowledgements

Preface

PART I CONVENTIONAL AND HIGH SECURITY LOCKS

PART II THEORY: ACHIEVING THE COMPROMISE OF THREE LAYERS OF MEDECO SECURITY

PART III TACTICAL APPLICATIONS: COVERT ENTRY, FORCED ENTRY, AND THE
BYPASS OF KEY CONTROL

Epilogue
Appendices
Master Exhibit Index
Master Table Index
Master Video Index

About the Authors

CHAPTER OUTLINE

PART I CONVENTIONAL AND HIGH SECURITY LOCKS

CHAPTER ONE Conventional and High Security Locks: An Overview
CHAPTER TWO Standards for Conventional and High Security Locks
CHAPTER THREE Security Vulnerabilities of Conventional Locks
CHAPTER FOUR Medeco, Assa®, Schlage Primus®, and EVVA MCS: A
Comparison of Four High Security Lock Designs
CHAPTER FIVE Compromising Medeco Security: An Overview

PART II THEORY: ACHIEVING THE COMPROMISE OF THE THREE LAYERS OF MEDECO SECURITY

CHAPTER SIX Locked and Apparently Secure: The Road from High
Security to High Insecurity
CHAPTER SEVEN The Medeco Sidebar Design: Building Blocks to
Insecurity
CHAPTER EIGHT The Modern Enigma: Cracking Medeco Codes

PART III TACTICAL APPLICATIONS: COVERT ENTRY, FORCED ENTRY, AND THE BYPASS OF KEY CONTROL

CHAPTER NINE	The m3® Meets the Perilous Paper Clip: The Complete Compromise of Medeco Key Control
CHAPTER TEN	LISTENING TO THE LOCK: Techniques of Decoding to Gather Sidebar Code Intelligence
CHAPTER ELEVEN	Things that go Bump in the Night: "Our Locks Are Bump-proof, Virtually Bump-proof, and Virtually Resistant"
CHAPTER TWELVE	Methods of Picking Medeco Cylinders
CHAPTER THIRTEEN	Forced Entry: Three Strikes and You're In
CHAPTER FOURTEEN	Compromising Medeco Master Key Systems with Multiple sidebar Codes

Epilogue

APPENDICES

Appendix 1	Definitions
Appendix 2	Cast of Characters
Appendix 3	Code data tables
Appendix 3A	Key cutting data for HPC 1200 key machine
Appendix 4	Key-interchange conflict tables
Appendix 5	Protecting a System with Safe sidebar codes
Appendix 6	Legal waivers and disclaimers

About the Authors

Index

MASTER EXHIBIT INDEX

CHAPTER ONE

Figure 101 Two examples of Egyptian pin tumbler locks

Figure 102 Original Egyptian pin tumbler lock
Figure 103 Diagram of pin tumbler lock and key
Figure 104 A modern pin tumbler cylinder has three primary components
Figure 105 A six pin lock with three security pins

CHAPTER TWO

Figure 201 Creating a new shear line by drilling
Figure 202 Drilling a profile cylinder
Figure 203 Drilling the plug of a profile cylinder
Figure 204 Anti-drill pins are designed to stop a drilling attack
Figure 205 Pulling a profile cylinder with a metal screw
Figure 206 A Medeco Biaxial® plug with anti-drill pins to protect it



Forced entry attack: pulling the EVVA 3KS profile cylinder by Paul Crowel



Forced entry attack: drilling the EVVA 3KS shear line by Paul Crowel



Forced entry attacks: a discussion of pulling plugs by Paul Crowel



Forced entry attack: drilling the EVVA 3KS plug by Paul Crowel



Forced entry attack: drilling the shear line in conventional locks by Paul Crowel



Forced entry attack: detailed discussion of drilling the plug in conventional locks by Paul Crowel

CHAPTER THREE

Figure 301 Easy Entrie milling machine
Figure 302 Profiles are probed by the Easy Entrie

CHAPTER FOUR

Figure 401 Key for Assa V10
Figure 401A Assa sidebar detail
Figure 401B Assa right and left contact of finger pins
Figure 402 Key for Schlage Primus
Figure 403 Primus finger pins
Figure 404 Primus finger pin detail
Figure 405 Medeco bitting angles
Figure 406 Medeco bottom pins aligned with sidebar legs
Figure 407 Diagram of Medeco Biaxial
Figure 408 Identification of six angles for Medeco pins
Figure 409 Medeco Biaxial cylinder diagram with the sidebar
Figure 410 Medeco Biaxial cutaway

Figure 411 Diagram of Medeco fore and aft angles
Figure 412 Diagram of Medeco pin angles and sidebar alignment
Figure 413 Medeco m3 cutaway
Figure 414 Medeco m3 slider alignment with wire offset
Figure 415 Medeco m3 cutaway and the action of the slider
Figure 416 Medeco slider from the m3
Figure 417 Medeco m3 slider detail
Figure 418 Medeco Bilevel® and Biaxial pins
Figure 419 EVVA MCS key, rotor and lock
Figure 420 EVVA MCS top and bottom track on key for sliders
Figure 421 EVVA MCS magnetic film overlay showing different magnetic fields
Figure 422 Examples of ARX pins
Table 4_2.3.1 Angle identification table for fore and aft rotations

CHAPTER FIVE

No images

CHAPTER SIX

Figure 600 Tobias Bluzmanis decoder for Medeco locks
Figure 601 Diagram of a six pin Medeco lock where the sidebar is not aligned
Figure 602 Diagram of a Medeco plug with the sidebar aligned
Figure 603 Medeco key card that contains the bitting and sidebar code
Table 6_2.5 Matrix of keys for methods of entry: normal, covert, forced

CHAPTER SEVEN

Figure 701 Three generations of Medeco locks and distinctive logos

CHAPTER EIGHT

Figure 801 Code space definition
Figure 802 Four code setting keys for Medeco Biaxial and m3 cylinders
Figure 803 Depth and spacing definition for Medeco Biaxial and m3
Figure 804 Double-cut keys for Medeco Biaxial and m3 locks
Figure 805 Sidebar code identifier for Medeco Biaxial and m3
Figure 806 Vertical channel or true gate
Figure 807 True and false gates on pins
Figure 808 Fore and aft tip positions
Figure 809 Gate tolerance diagram for sidebar legs
Figure 810 Code space diagram
Figure 811 Diagram showing three types of cuts: original, fore-aft, and offset
Figure 812 Keys with offset cuts for alternate code setting keys
Figure 813 Bump keys with offset cuts for alternate method of bumping

Table 8_2.0A Generation-2 angles for code setting keys

Table 8_2.0B Generation-3 angles for code setting keys

Table 8_3.4.2 Maximum Adjacent Cut angle table (MACS)
Table 8_4.4.2.1A Fore and aft conflicts for Biaxial and m3
Table 8_4.4.2.1B Fore and aft conflicts in modified bitting
Table 8_4.9 Code setting key simulated angles
Table 8_5.0 Comparison of Generation-2 and Generation-3 angle allocation



Sidebar leg-gate 10° tolerance

CHAPTER NINE

Figure 901 Mosler 1095A simulated key
Figure 902 Simulated key for Medeco lock
Figure 903 Third party and knock-off blanks for Medeco locks
Figure 904 A slider is positioned to the right side of the keyway
Figure 905 Diagram of slider and the different step positions
Figure 906 Biaxial and m3 keyways showing operation of simulated blank
Figure 907 Cutaway diagram of the m3 with a wire inserted, tabs aligned
Figure 908 An m3 with a wire offsetting the slider
Figure 909 A paper clip inserted into the keyway to offset the slider
Figure 910 A paper clip and key inserted into an m3 keyway
Figure 911 A wire can be lodged between the slider and plug to sabotage the lock
Figure 912 The m3 with a fixed wire will still function normally
Figure 913 A simulated key
Figure 914 A simulated key in a Biaxial cutaway
Figure 915 A simulated blank inserted into a keyway must pass all the wards
Figure 916 A pick has the same thickness as a simulated key
Figure 917 Measuring the Mosler 1095A with a micrometer showing .040" thickness
Figure 918 The material on the simulated blank is reduced with sand paper
Figure 919 Two key machines to produce code setting keys: ITL 9700 and Medeco
Figure 920 Biaxial key machine by Medeco showing the insertion of a shim
Figure 921 Two stacked simulated blanks are used to properly cut the keys

Table 9_3.3.2.1 Biaxial and m3 key blank measurements
Table 9_3.3.2.1A Biaxial and m3 key blade measurements
Table 9_3.3 Simulated key blank measurements



Bypass of the Medeco m3 slider



Simulation of keys for the Medeco m3 and Biaxial

CHAPTER TEN

Figure 1001 Fore and aft pin geometry
Figure 1002 Oscope for viewing internal components
Figure 1003 An oscope has several different viewing ranges
Figure 1004 An Olympus borescope with a .87mm probe can view the gate angles
Figure 1005 Gate identification for fore pins
Figure 1006 Gate identification for aft pins
Figure 1007 Gate angles as decoded with Olympus borescope

Figure 1008 John Falle shim decoder tool
Figure 1009 Code space decoder

Table 10_3.1.1A Generation-2 code data for one and two code spaces
Table 10_3.1.1B Matrix for Generation-2 to select code setting keys
Table 10_3.2.3A Known number of angles and code setting keys for Gen-3
Table 10_3.2.3B Known number of angles for specific chambers for Generation-3



Decoding with an Olympus borescope

CHAPTER ELEVEN

Figure 1101 A conventional bump key for Kwikset® locks
Figure 1102 A diagram for bumping using the pull-back method
Figure 1103 A tomahawk and Peterson Manufacturing bump hammer
Figure 1104 Sir Isaac Newton postulated the theory for bumping
Figure 1105 A bump key that was produced for the Assa V10
Figure 1106 A diagram showing a double-cut bump key with different fore and aft depths
Figure 1107 Eleven year old JennaLynn bumps open a Kwikset lock at Defcon 14
Figure 1108 Medeco provided these macro-photographs of a cylinder that was bumped
Figure 1109 Forensic indication that a Bilevel cylinder was bumped
Figure 1109A A Biaxial change key that has been modified to work as a bump key
Figure 1110 A milled m3 blank, showing the removal of the step protrusion
Figure 1110A Diagram with all possible angle rotations
Figure 1111 A bump key on a simulated blank
Table 11_3.1.2.1A Bump key for known sidebar code depth measurements
Table 11_3.1.2.2 Depth measurements for bump key for an unknown sidebar code
Table 11_5.1.1 Generation-2 code table for code setting keys
Table 11_5.1.2 Generation-3 code table for code setting keys
Table 11_5.1.2.1 Selection of keys for Generation-3 for chambers 2-3



Harry Sher discusses conventional bumping theory



Bumping open different Assa high security cylinders



Bumping the Medeco Biaxial by JennaLynn at Defcon 15, full interview



Bumping open a Medeco Biaxial

CHAPTER TWELVE

Figure 1201 Diagram of a conventional pin tumbler lock and rake pick
Figure 1202 Medeco pins have true and false gates
Figure 1203 Four code setting keys for Generation-2 codes
Figure 1204 The bottom pins are scrambled when the key is removed from the lock
Figure 1205 A code setting key with double-cut bitting
Figure 1206 The theory for setting the sidebar code: pins retain their angles with torque

Figure 1207 Picking sequence for Medeco cylinders
Figure 1207A Cutaways of mortise cylinder, showing pin rotations
Figure 1208 Setting the sidebar code when picking
Figure 1209 A cylinder that has been picked
Figure 1210 Special advanced code setting keys for manipulating individual angles
Table 12_3.10.3 Depth, spacing, and angles for advanced code setting picks



Picking technique for the Medeco Biaxial and m3



Introduction to the theory of picking a Medeco cylinder



Demonstration of the theory of setting the sidebar code



Setting the sidebar code with code setting keys



Setting the sidebar code with a change key with the same code



Setting individual rotations with angle setting keys



Setting the sidebar code and setting individual angles

CHAPTER THIRTEEN

Figure 1301 High security locks employ anti-drill pins to protect vital areas
Figure 1302 The m3 deadbolt can be rapidly compromised with a variety of methods
Figure 1303 Two screws form the entire security of the Medeco deadbolt cylinder
Figure 1304 The screws are sheared with a special breaker tool
Figure 1305 The screws are sheared with a piece of spring steel held by vice grip
Figure 1306 The tailpiece is linked to the plug through the end-cap and two screws
Figure 1307 A modified screwdriver tip at the end of the plug to control the tailpiece
Figure 1308 The design of the modified screwdriver to manipulate the tailpiece
Figure 1309 The interim fix for the defective tailpiece design of the Biaxial and m3
Figure 1310 The interim design required a long pin to be inserted into the plug
Figure 1311 The final tailpiece design that was introduced in December, 2007
Figure 1312 A plug with sheared screws from an m3 with the final deadbolt design
Figure 1313 Reverse picking of the m3 deadbolt with the final tailpiece design
Figure 1314 A screwdriver and paperclip are used in the reverse picking attack
Figure 1315 The sidebar channel runs the length of the cylinder
Figure 1316 Reverse picking sequence
Figure 1317 Actuation of the deadbolt can be accomplished by a flat blade screwdriver
Figure 1318 Modified sidebar to prevent reverse picking attacks
Figure 1319 A mortise cylinder and protruding plug
Figure 1320 A plastic key can set the pins at shear line in the mortise cylinder
Figure 1321 Torque is applied to the plug with a 10" vice grip
Figure 1322 Plastic keys can be easily created to set the pins at shear line
Figure 1323 A plastic key can be produced by overlaying and tracing an original
Figure 1324 Special vice grip and plug showing compression of the keyway

Figure 1325 A compressed plug allows the sidebar to retract
Figure 1326 An interchangeable core key-in-knob lock can also be compromised
Figure 1327 An Assa Twin® with a protruding plug cannot be compromised in the same way



Shearing deadbolt screws



Bypass of the Medeco mortise cylinder



Bypass of the Medeco Biaxial and m3 deadbolt original design



Reversed picking attack on the Biaxial and m3 deadbolt



Bypassing the interim deadbolt fix

CHAPTER FOURTEEN

Figure 1401 Diagrams of a master keyed and non-master keyed cylinder
Figure 1402 Cylinder with a master pin in the pin stack and diagram
Figure 1403 Levels of master key systems
Figure 1404 Example of two-pin lock with master and change key
Figure 1405 Four keys will open the two-pin master keyed lock
Table 14_162A Multiple sidebar code system showing complementary angles
Table 14_162B Multiple sidebar code #2 available angles
Table 14_162C Multiple sidebar code #3 available angles
Table 14_162D Top level master key angle matrix for multiple code system
Table 14_1.7A Angle table for extrapolation of TMK from a change key
Table 14_1.7B Sidebar code permutations from a change key

Master Table Index

Table 4_2.3.1 Angle identification table for fore and aft rotations

Table 6_2.5 Matrix of keys for methods of entry: normal, covert, forced

Table 8_2.0A Generation-2 angles for code setting keys

Table 8_2.0B Generation-3 angles for code setting keys

Table 8_3.4.2 Maximum Adjacent Cut angle table (MACS)

Table 8_4.4.2.1A Fore and aft conflicts for Biaxial and m3

Table 8_4.4.2.1B Fore and aft conflicts in modified bitting

Table 8_4.9 Code setting key simulated angles

Table 8_5.0 Comparison of Generation-2 and Generation-3 angle allocation

Table 9_3.3.2.1 Biaxial and m3 key blank measurements

Table 9_3.3.2.1A Biaxial and m3 key blade measurements

Table 9_3.3 Simulated key blank measurements

Table 10_3.1.1A Generation-2 code data for one and two code spaces

Table 10_3.1.1B Matrix for Generation-2 to select code setting keys

Table 10_3.2.3A Known number of angles and code setting keys for Gen-3

Table 10_3.2.3B Known number of angles for specific chambers for Generation-3

Table 11_3.1.2.1A Bump key for known sidebar code depth measurements

Table 11_3.1.2.2 Depth measurements for bump key for an unknown sidebar code

Table 11_5.1.1 Generation-2 code table for code setting keys

Table 11_5.1.2 Generation-3 code table for code setting keys

Table 11_5.1.2.1 Selection of keys for Generation-3 for chambers 2-3

Table 14_162A Multiple sidebar code system showing complementary angles

Table 14_162B Multiple sidebar code #2 available angles

Table 14_162C Multiple sidebar code #3 available angles

Table 14_162D Top level master key angle matrix for multiple code system

Table 14_1.7A Angle table for extrapolation of TMK from a change key

Table 14_1.7B Sidebar code permutations from a change key

Master Video Index



Harry Sher discusses conventional bumping theory



Bypass of the Medeco m3 slider



Bypass of the Medeco mortise cylinder



Bypass of the Medeco Biaxial and m3 deadbolt original design



Picking technique for the Medeco Biaxial and m3



Simulation of keys for the Medeco m3 and Biaxial



Reversed picking attack on the Biaxial and m3 deadbolt



Forced entry attack: pulling the EVVA 3KS profile cylinder by Paul Crouwel



Forced entry attack: drilling the EVVA 3KS shear line by Paul Crouwel



Forced entry attacks: a discussion of pulling plugs by Paul Crouwel



Forced entry attack: drilling the EVVA 3KS plug by Paul Crouwel



Forced entry attack: drilling the shear line in conventional locks by Paul Crouwel



Forced entry attack: detailed discussion of drilling the plug in conventional locks by Paul Crouwel



Bumping open different Assa high security cylinders



Bumping of a Kwikset lock by eleven year old JennaLynn



Bumping the Medeco Biaxial by JennaLynn at Defcon 15, full interview



Bumping of the Medeco Biaxial by JennaLynn at Defcon 15



Shearing deadbolt screws



Bypassing the interim deadbolt fix



Decoding with an Olympus borescope



Setting the sidebar code with a change key with the same code



Setting the sidebar code with code setting keys



Bumping open a Medeco Biaxial



Introduction to the theory of picking a Medeco cylinder



Demonstration of the theory of setting the sidebar code



Setting individual rotations with angle setting keys



Setting the sidebar code and setting individual angles



Sidebar leg-gate 10° tolerance



LSS206: Harry Sher on impressioning Medeco locks



LSS206: Detailed discussion of sidebar leg-gate tolerance



LSS206: Bypass of the Bilevel



LSS206: Medeco tip probe