



Open in 30 Seconds

Cracking One of the  
Most Secure Locks in America

Marc Weber Tobias  
Matt Fiddler

*in.*Security.Org

# LOCKS, LIES, and “HIGH” INSECURITY

- Dominant high security lock maker
- 40 year history of security
- Many expert attempts to crack with limited success, complicated tools
- Misstatements and disinformation
- 18 month research project results:

A Total compromise of security

# MEDECO HIGH SECURITY:

- UL, BHMA / ANSI, VdS Certified
- High level of protection against attack
- Picking: 10-15 minute resistance
- No bumping
- Forced Entry: 5 minutes, minimum
- Key control
  - Protect restricted and proprietary keyways
  - Stop duplication, replication, simulation of keys

# HIGH SECURITY LOCKS:

- Protect Critical Infrastructure, high value targets
- Stringent security requirements
- High security Standards
- Threat level is higher
- Protect against Forced, Covert entry
- Protect keys from compromise

# MEDECO HISTORY

- Dominant high security lock maker in U.S.
- Owns 70+ Percent of U.S. high security market for commercial and government
- Major government contracts
- In UK, France, Europe, South America
- Relied upon for highest security everywhere
- Considered almost invincible by experts

# WHY THE MEDECO CASE STUDY IS IMPORTANT

- Insight into design of high security locks
- Patents are no assurance of security
- Appearance of security v. Real World
- Undue reliance on Standards
- Manufacturer knowledge and Representations
- Methodology of attack
- More secure lock designs

# CONVENTIONAL v. HIGH SECURITY LOCKS

- **CONVENTIONAL CYLINDERS**
  - Easy to pick and bump open
  - No key control
  - Limited forced entry resistance
- **HIGH SECURITY CYLINDERS**
  - UL and BHMA/ANSI Standards
  - Higher quality and tolerances
  - Resistance to Forced and Covert Entry
  - Key control

# ATTACK METHODOLOGY

- Assume and believe nothing
- Ignore the experts
- Think “out of the box”
- Consider prior methods of attack
- Always believe there is a vulnerability
- **WORK THE PROBLEM**
  - Consider all aspects and design parameters
  - Do not exclude any solution



# HIGH SECURITY LOCKS: Critical Design Issues

- Multiple security layers
- More than one point of failure
- Each security layer is independent
- Security layers operate in parallel
- Difficult to derive intelligence about a layer

# HIGH SECURITY: Three Critical Design Factors

- Resistance against forced entry
- Resistance against covert and surreptitious entry
- Key control and “key security”

Vulnerabilities exist for each requirement

# BYPASS AND REVERSE ENGINEERING

- Weakest link in lock to bypass (Medeco)
- What locks the lock?
- What locking elements lock and in what order. Is there a primary element to bypass?
- Result if one layer fails: Can others be compromised?
- What intelligence needed to open the lock?
- Can Intelligence be simulated?

# SYSTEM BYPASS

- How strong is the sidebar(s) against forced attack
- Is the sidebar the only locking system?
- What if defeat one of two sidebars or security layers?
- Bitting design: spring biased?
- Ability to manipulate each pin or slider to set its code?

# SECONDARY SECURITY LAYERS

- Telescoping pins
- Sliders and wafers
- Sliders to set sidebars: Medeco
- Pseudo-sidebars = virtual keyways
- Sidebars
  - Most popular
  - Originated in America with GM locks
  - Many locking techniques

# LAYERS OF SECURITY AND BYPASS CAPABILITY

- How many
- Ability to exploit design feature?
- Integrated
- Separate
  - Primus = 2 levels, independent, complex locking of secondary finger pins
  - Assa = 2 levels, independent, simple locking, one level

# EXPLOITING FEATURES

- Codes: design, progression
- Key biting design
- Tolerances
- Keying rules
  - Medeco master and non-master key systems
- Interaction of critical components and locking systems
- Keyway and plug design

# EXPLOITING TOLERANCES

- Sidebar locking: Medeco 10 v. 20 degree
- Relation to codes
- Simulation of codes: Medeco
- Reverse engineer code progression of system from one or more keys?
  - Master key conventional v. positional system
  - Difficulty = replication of keys
  - Medeco v. MCS as example



# ATTACKS: Two Primary Rules

- “The Key never unlocks the lock”
  - Mechanical bypass
- Alfred C. Hobbs: “If you can feel one component against the other, you can derive information and open the lock.”

# METHODS OF ATTACK: High Security Locks

- Picking and manipulation of components
- Impressioning
- Bumping
- Vibration and shock
- Shim wire decoding (Bluzmanis and Falle)
- Borescope and Otoscope decoding
- Direct or indirect measurement of critical locking components

# ADDITIONAL METHODS OF ATTACK

- Split key, use sidebar portion to set code
- Simulate sidebar code
- Use of key to probe depths and extrapolate
- Rights amplification of key

# KEY CONTROL

- High security requirement



# KEY CONTROL and “KEY SECURITY”

- Duplicate
- Replicate
- Simulate

“Key control” and “Key Security” may not be synonymous!

# KEY SECURITY: A Concept

- Key control = physical control of keys
- Prevent manufacture and access to blanks
- Control generation of keys by code
- Patent protection
- Key security = compromise of keys
  - Duplication
  - Replication
  - Simulation

# KEYS: CRITICAL ELEMENTS

- Length = number of pins/sliders/disks
- Height of blade = depth increments = differs
- Thickness of blade = keyway design
- Paracentric design
- Keyway modification to accommodate other security elements
  - Finger pins
  - Sliders

# KEY CONTROL: Critical issues

- Simulation of code or key components
- Security of locks = key control and key security
  - All bypass techniques simulate actions of key
  - Easiest way to open a lock is with the key



# KEY CONTROL and “KEY SECURITY” ISSUES

- Most keys are passive: align = open
- Simulate components of key
- Replicate critical components
- Duplicate critical components
- Require interactive element for security
  - MUL-T-LOCK element
  - BiLock-NG, Everest Check Pins
  - MCS magnets

# KEY CONTROL: Design Issues

- Bitting design
- Bitting and sidebar issues and conflicts and limitations in differs
- Ability to decode one or more keys to break system
- Consider critical elements of the key: require to insure cannot be replicated
- Hybrid attacks using keys
  - Medeco mortise cylinder example

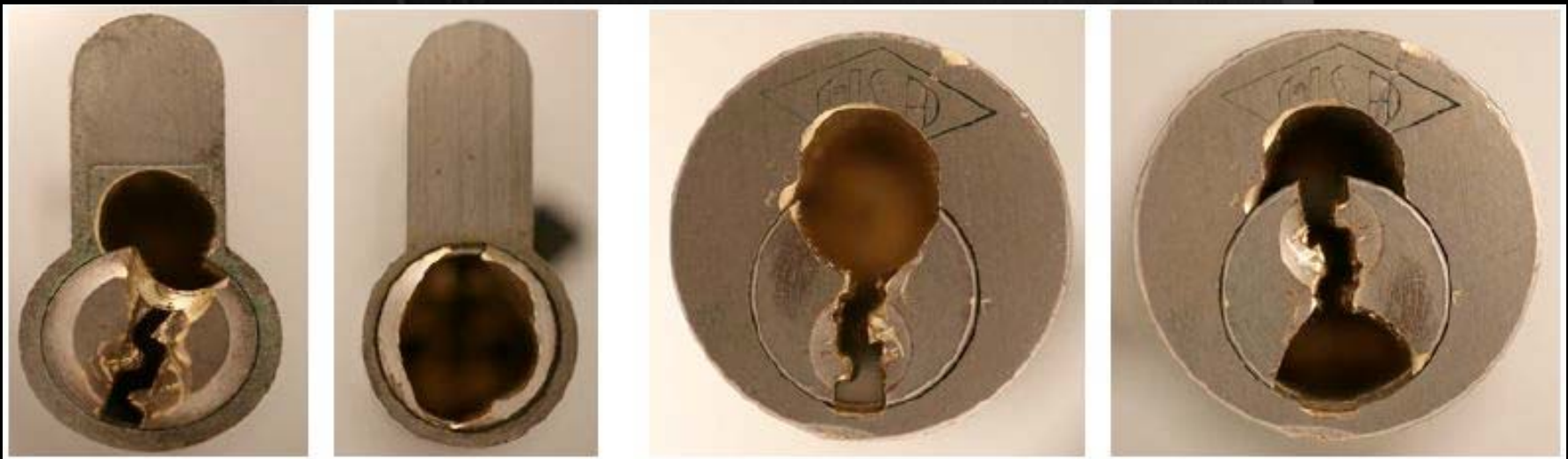
# DUPLICATION AND REPLICATION OF KEYS

- Key machine
- Milling machine: Easy Entry
- Clay and Silicone casting
- Key simulation: Medeco
- Rights amplification
- Alter similar keys



# COVERT and FORCED ENTRY RESISTANCE

- High security requirement



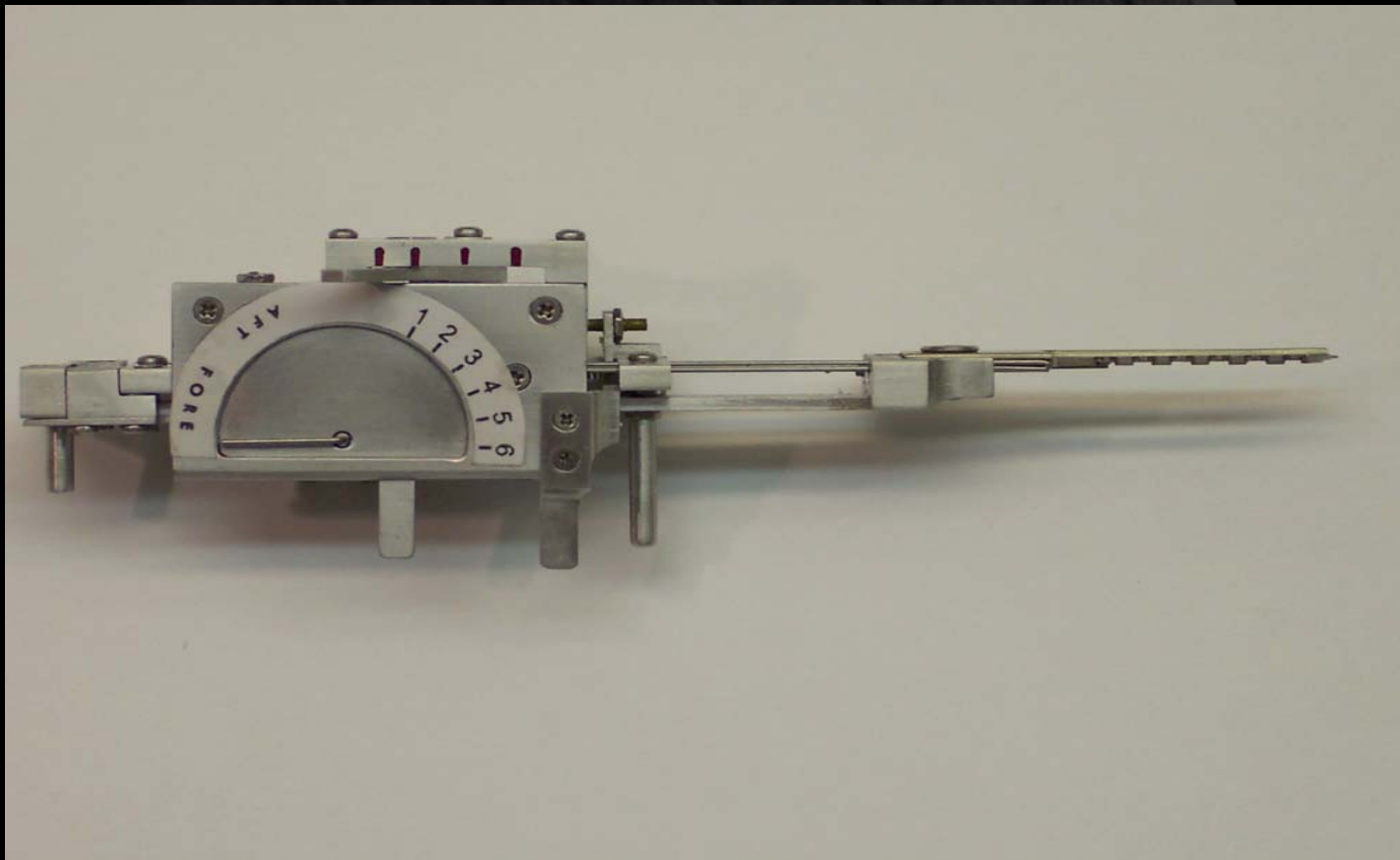
# STANDARDS REQUIREMENTS

- UL and BHMA/ANSI STANDARDS
- TIME is critical factor
  - Ten or fifteen minutes
  - Depends on security rating
- Type of tools that can be used
- Must resist picking and manipulation
- Standards do not contemplate or incorporate more sophisticated methods

# CONVENTIONAL PICKING



# TOBIAS DECODER: “Crackpot@security.org”



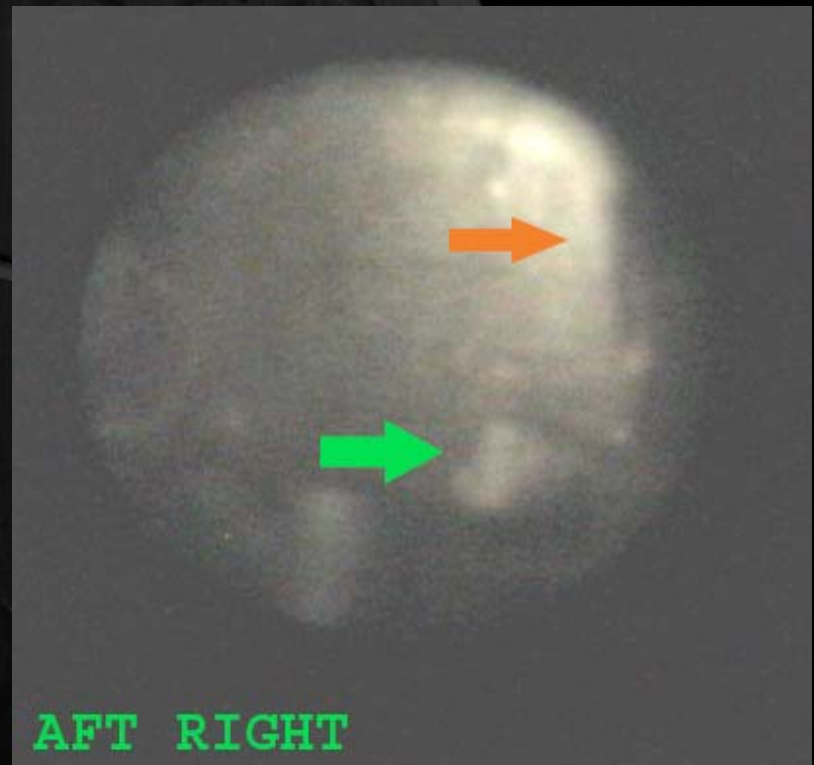
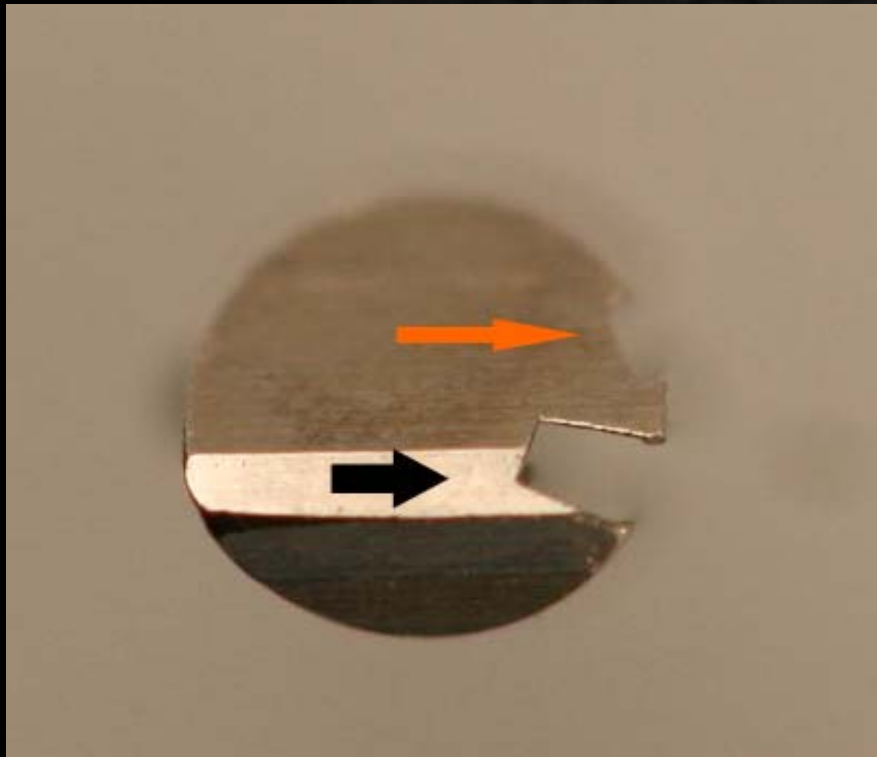
# SOPHISTICATED DECODERS

- John Falle: Wire Shim Decoder





# DECODE PIN ANGLES



# FORCED ENTRY RESISTANCE



# FORCED ENTRY ATTACKS: Deficiencies in standards

- Many types of attacks defined
- Mechanical Bypass - Not Contemplated
- Must examine weakest links
- Do not cover “hybrid attacks”
  - Medeco deadbolt attacks
  - Medeco mortise attack

# SIDEBAR: Bypass and Circumvention

- **Direct Access**
  - Decoding attacks
  - Manipulation
  - Simulate the sidebar code (Medeco)
  - Use of a key (Primus and Assa)
- **Indirect access**
  - Medeco borescope and otoscope decode issues

# SIDEBAR ATTACK: Physical Strength

- Independent protection
- Integrated with pin tumblers or other critical locking components
- Plug Compression
- Defeat of sidebar as one security layer: result and failures
- Anti-drill protection

# FORCED ENTRY ATTACKS

- Direct compromise of critical components
  - Medeco deadbolt 1 and 2 manipulate tailpiece
- Hybrid attack: two different modes
  - Medeco reverse picking
- Defeat of one security layer: result
  - Medeco Mortise and rim cylinders, defeat shear line

# MEDECO HIGH SECURITY: Lessons to be learned

- What constitutes security
- Lessons for design engineers
- Appearance v. reality

# MEDECO CASE HISTORY

- Exploited vulnerabilities
- Reverse engineer sidebar codes
- Analyze what constitutes security
- Analyze critical tolerances
- Analyze key control issues
- Analyze design enhancements for new generations of locks: Biaxial and m3 and Bilevel



# MEDECO MISTAKES

- Failed to listen
- Embedded design problems from beginning
- Compounded problems with new designs with two new generations: Biaxial and m3
- Failed to “connect the dots”
- Failure of imagination
- Lack of understanding of bypass techniques

# DESIGN = VULNERABILITIES

- Basic design: sidebar legs + gates
  - How they work: leg + gate interface
  - Tolerance of gates
- Biaxial code designation
- Biaxial pin design: aft position decoding
- M3 slider: geometry
- M3 keyway design
- Deadbolt design

# MEDECO DESIGN: Exploit design vulnerabilities

- EXPLOIT BEST DESIGN FEATURES
- Sidebar leg – true gate channel
- Code assignment: Biaxial 1985
- Gate – sidebar leg tolerance
- M3 design 2003
  - Widen keyway .007”
  - Slider geometry, .040” offset

# MEDECO DESIGNS: More vulnerabilities

- Biaxial pin design: fore and aft positions
- Borescope decode of aft angles
- Introduction of Bilevel in 2006
- Compromise by decoding

# MEDECO TIMELINE

- 1970 Original Lock introduced
- 1985 Biaxial, Second generation
- 2003 m3 Third generation

# August 2006: Bump Proof

About Medeco - MEDECO - THE BUMP PROOF LOCK

http://web.archive.org/web/20061016161749/www.medeco.com/about/whats\_new/

CONTACT: Ann McCrady  
859-689-5753  
amccrady@medeco.com

[What's New](#)  
[Map & Directions](#)  
[Training Schedule](#)  
[Careers At Medeco](#)  
[Trade Show Schedule](#)  
[Become a Medeco Dealer](#)  
[NCPC Projects](#)  
[Learn about Product Maintenance](#)

## Medeco Combats the Bump Key

*Law Enforcement and Security Dealers Educated in standard lock risks*

**Salem, Va., August 4, 2006** "Security flaw in your locks" asks a recent Newsweek.com headline. The term "Hackers" is typically associated with those who attempted to break into computer systems. Now Hackers are people attempting to defeat a wide range of protected systems including the locks on your doors.

Medeco, the industry's leading high security lock manufacturer, has expanded its acclaimed educational training module to explain the vulnerability that many locks face to a bumping attack. This training is offered to Crime Prevention associations and security dealers.

Medeco is commonly known as a "bump proof lock" by those who view picking as a sport. Standard locks utilize a single locking point, while high security locks such as Medeco utilize multiple locking technologies. To see why Medeco is not vulnerable to this type of attack, a short video is available at [www.medeco.com](http://www.medeco.com) in the Interactive Security Solutions link.

According to statistics provided by the National Crime Prevention Council (NCPC) and the Department of Justice, nearly 2/3 of all break-ins occur with no sign of forced entry. While some of these crimes may be a result of an unlocked door, most experts agree that lock bumping, picking or use of an unauthorized duplicate key are often the case.

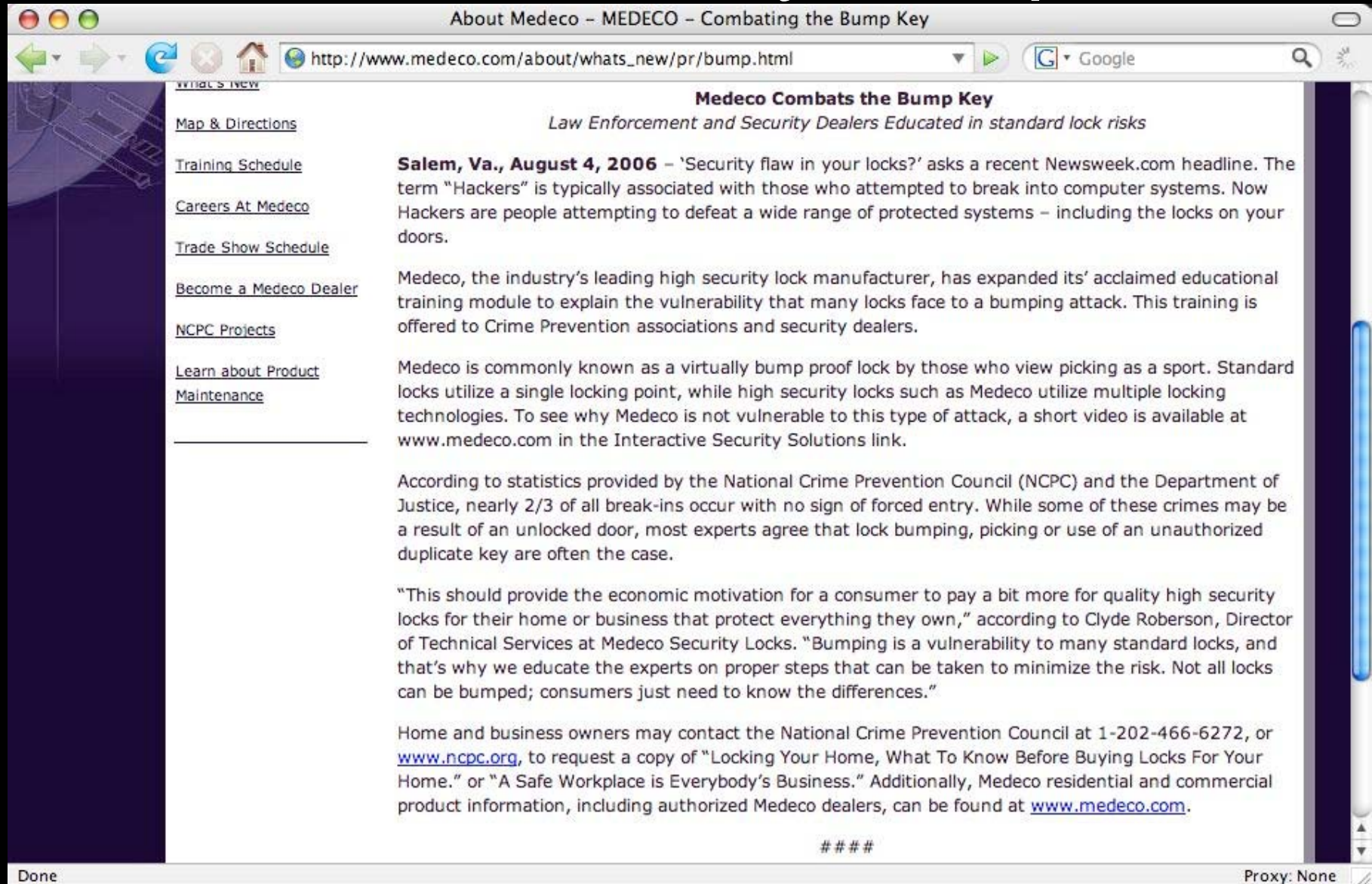
"This should provide the economic motivation for a consumer to pay a bit more for quality high security locks for their home or business that protect everything they own," according to Clyde Roberson, Director of Technical Services at Medeco Security Locks. "Bumping is a vulnerability to many standard locks, and that's why we educate the experts on proper steps that can be taken to minimize the risk. Not all locks can be bumped; consumers just need to know the differences."

Home and business owners may contact the National Crime Prevention Council at 1-202-466-6272, or [www.ncpc.org](http://www.ncpc.org), to request a copy of "Locking Your Home, What To Know Before Buying Locks For Your Home" or "A Safe Workplace is Everybody's Business." Additionally, Medeco residential and commercial product information, including authorized Medeco dealers, can be found at [www.medeco.com](http://www.medeco.com).

####

Done Proxy: None

# Feb 2007: Virtually BumpProof



The screenshot shows a web browser window with the following elements:

- Browser Title Bar:** "About Medeco - MEDECO - Combating the Bump Key"
- Address Bar:** "http://www.medeco.com/about/whats\_new/pr/bump.html"
- Search Bar:** "Google"
- Left Sidebar (Navigation Links):**
  - WHAT'S NEW
  - [Map & Directions](#)
  - [Training Schedule](#)
  - [Careers At Medeco](#)
  - [Trade Show Schedule](#)
  - [Become a Medeco Dealer](#)
  - [NCPC Projects](#)
  - [Learn about Product Maintenance](#)
- Main Content Area:**
  - Section Header:** **Medeco Combats the Bump Key**
  - Sub-header:** *Law Enforcement and Security Dealers Educated in standard lock risks*
  - Text:**

**Salem, Va., August 4, 2006** - 'Security flaw in your locks?' asks a recent Newsweek.com headline. The term "Hackers" is typically associated with those who attempted to break into computer systems. Now Hackers are people attempting to defeat a wide range of protected systems - including the locks on your doors.

Medeco, the industry's leading high security lock manufacturer, has expanded its' acclaimed educational training module to explain the vulnerability that many locks face to a bumping attack. This training is offered to Crime Prevention associations and security dealers.

Medeco is commonly known as a virtually bump proof lock by those who view picking as a sport. Standard locks utilize a single locking point, while high security locks such as Medeco utilize multiple locking technologies. To see why Medeco is not vulnerable to this type of attack, a short video is available at [www.medeco.com](http://www.medeco.com) in the Interactive Security Solutions link.

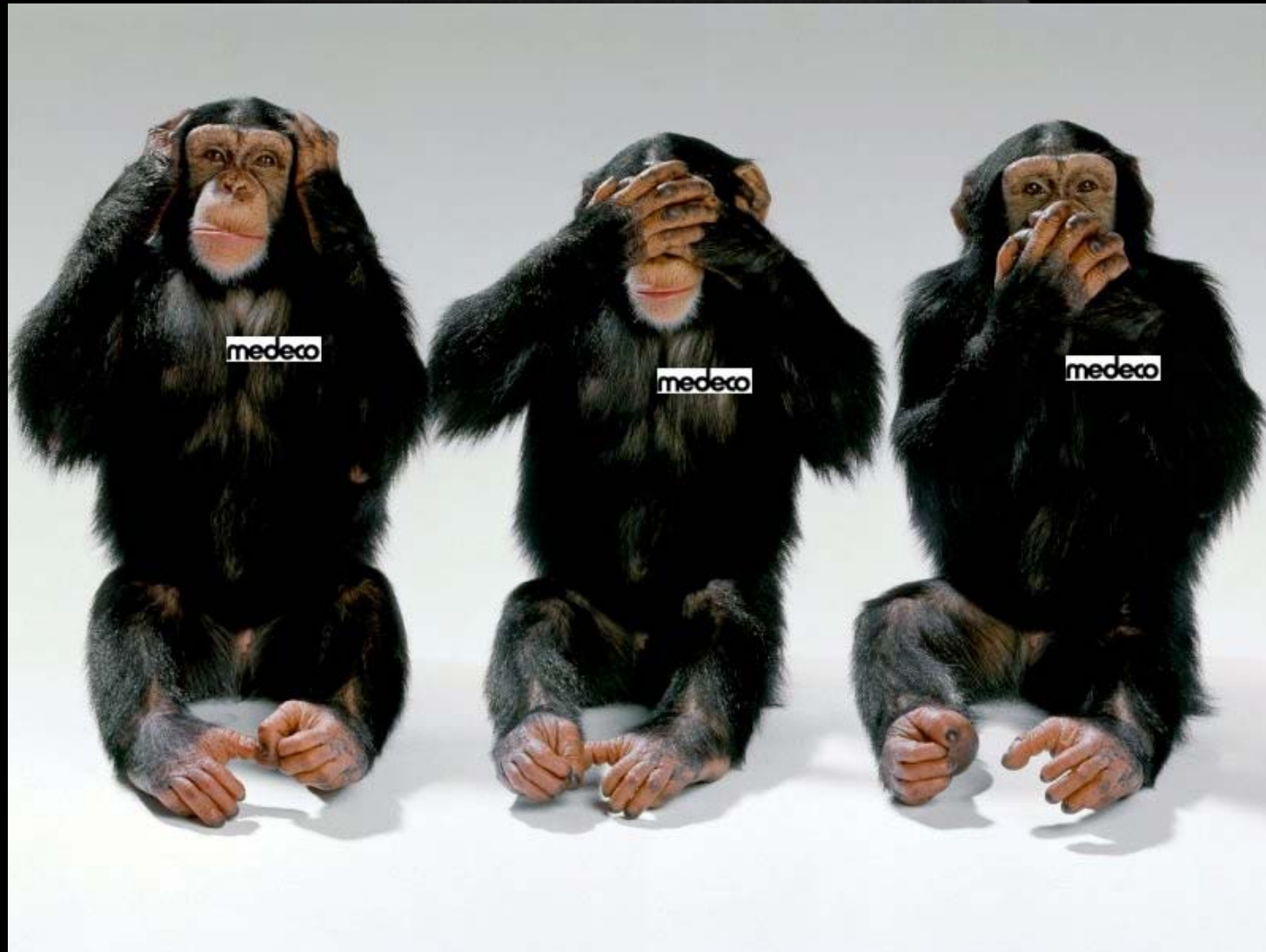
According to statistics provided by the National Crime Prevention Council (NCPC) and the Department of Justice, nearly 2/3 of all break-ins occur with no sign of forced entry. While some of these crimes may be a result of an unlocked door, most experts agree that lock bumping, picking or use of an unauthorized duplicate key are often the case.

"This should provide the economic motivation for a consumer to pay a bit more for quality high security locks for their home or business that protect everything they own," according to Clyde Roberson, Director of Technical Services at Medeco Security Locks. "Bumping is a vulnerability to many standard locks, and that's why we educate the experts on proper steps that can be taken to minimize the risk. Not all locks can be bumped; consumers just need to know the differences."

Home and business owners may contact the National Crime Prevention Council at 1-202-466-6272, or [www.ncpc.org](http://www.ncpc.org), to request a copy of "Locking Your Home, What To Know Before Buying Locks For Your Home." or "A Safe Workplace is Everybody's Business." Additionally, Medeco residential and commercial product information, including authorized Medeco dealers, can be found at [www.medeco.com](http://www.medeco.com).
  - Text:** #####

Done Proxy: None

2008:





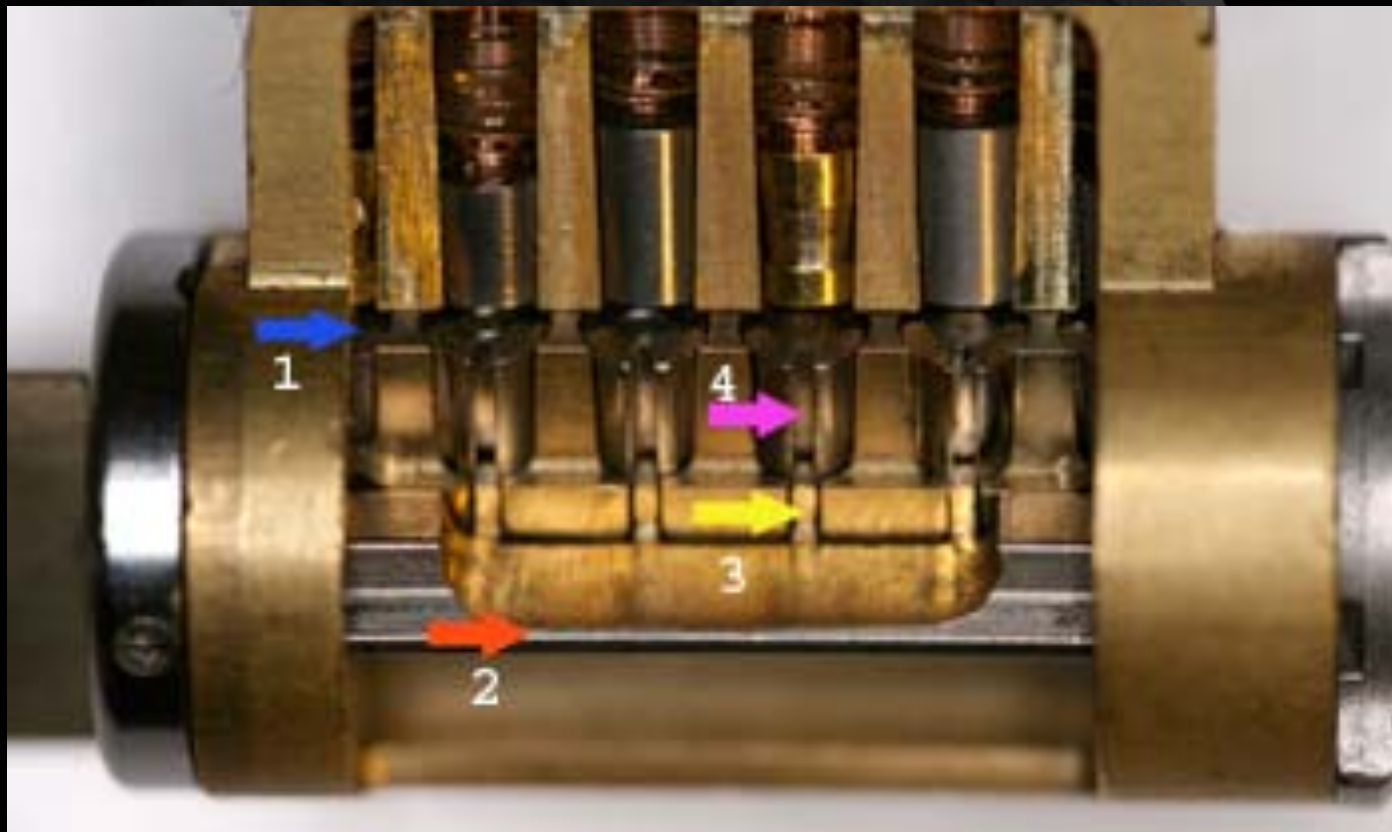
# MEDECO LOCKS: Why are they Secure?

- 2 shear lines and sidebar for Biaxial
- 3 independent security layers: m3
- Pins = 3 rotation angles, 6 permutations
- Physical pin manipulation difficult
- False gates and mushroom pins
- ARX special anti-pick pins
- High tolerance

# MODERN PIN TUMBLER



# MEDECO BIAXIAL

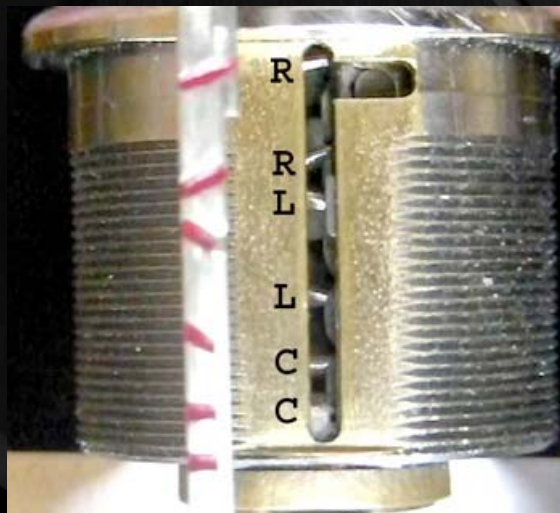


# MEDECO LOCKS: 3 Independent Layers

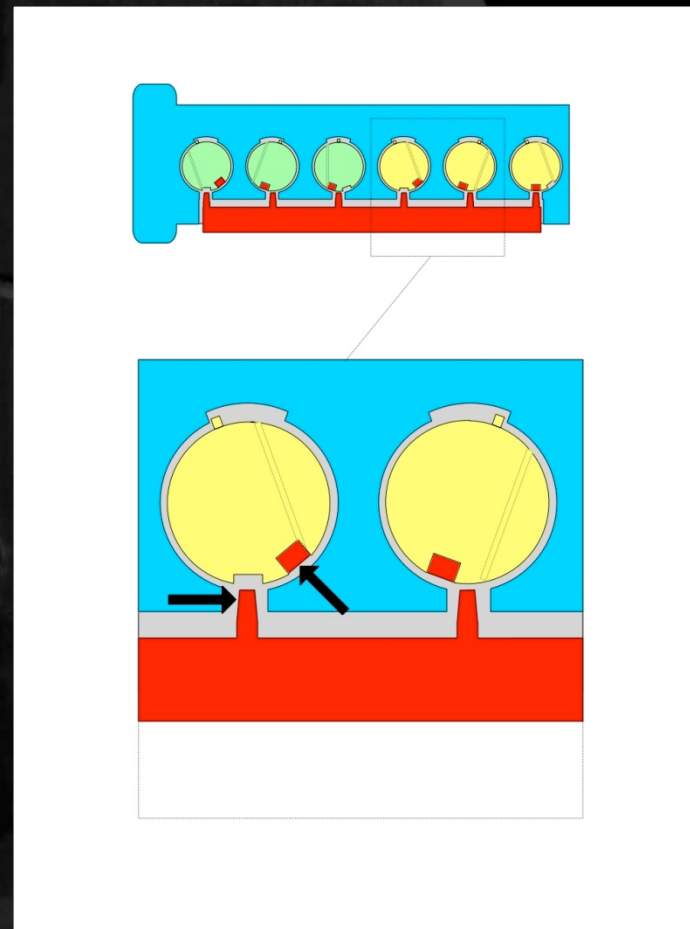
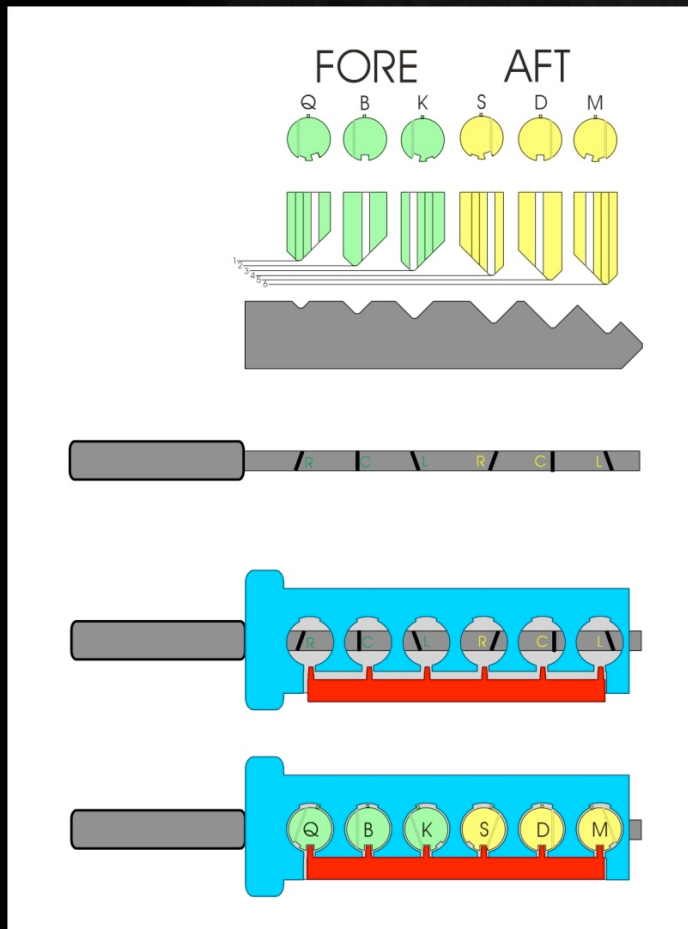
- Layer 1: PIN TUMBLERS to shear line
- Layer 2: SIDEBAR: 3 angles x 2 positions
- Layer 3: SLIDER – 26 positions

Opened By;  
Lifting the pins to shear line  
Rotating each pin individually  
Moving the slider to correct position

# MEDECO TWISTING PINS: 3 Angles + 2 Positions



# MEDECO ROTATING TUMBLER



# SIDEBAR Technology

- Block rotation of the plug
- One or two sidebars
- Primary or secondary locking
- Only shear line or secondary
- Integrated or separate systems
  - Assa, Primus , MT5 (M5), MCS= split
  - Medeco and 3KS = integrated
- Direct or indirect relationship and access by key biting

# SIDEBAR LOCKING: How does it work

- One or two sidebars
- Interaction during plug rotation
- Direct or indirect block plug rotation
- Sidebar works in which modes
  - Rotate left or right
  - Pull or push
- Can sidebar be neutralized: i.e. Medeco
  - Setting sidebar code
  - Pull plug forward, not turn



# SIDEBAR LOCKING

## DESIGN: Information from the lock?

- Feel picking: sense interactions
- Medeco, 3KS, Primus, Assa = direct link
- MCS = indirect link: sidebar to component
- Sidebar + pins/sliders interaction to block each other: ability to apply torque?

# SIDEBAR CODING

- Total number: real and theoretical
- Restrictions and conflicts
- Rules to establish
- Can we use rules to break system
  - Medeco TMK multiple
  - Assa V10 multiplex coding

# SECURITY CONCEPTS:

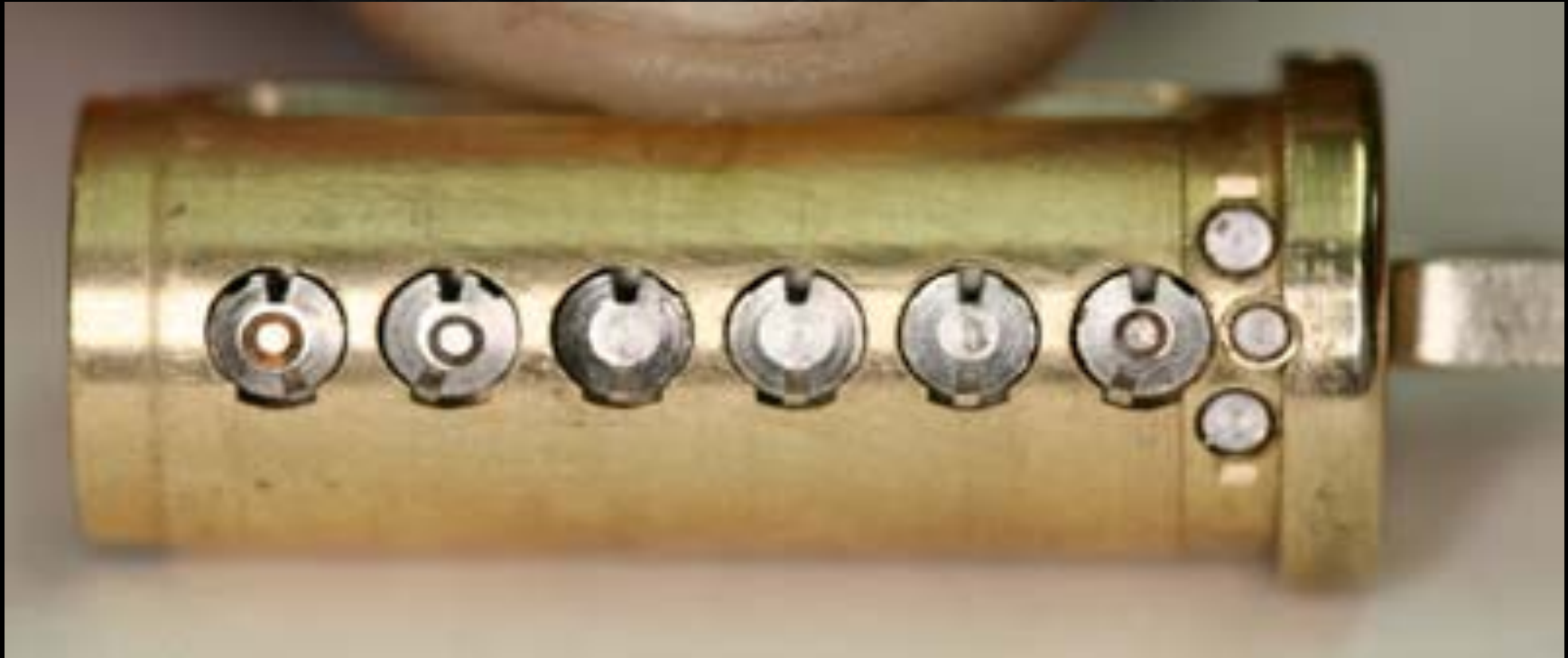
## Sidebar “IS” Medeco Security

- GM locks, 1935, Medeco re-invented
- Heart of Medeco security and patents
- Independent and parallel security layer
- Integrated pin: lift and rotate to align
- Sidebar blocks plug rotation
- Pins block manipulation of pins for rotation to set angles

# PLUG AND SIDEBAR: All pins aligned



# SIDEBAR RETRACTED



# PLUG AND SIDEBAR: Locked



# MEDECO CODEBOOK: At the heart of security

- All locksmiths worldwide must use
- All non-master keyed systems
- New codes developed for Biaxial in 1983
- Chinese firewall: MK and Non-MK
- Codebook defines all sidebar codes

# KEY CODES: Vertical Bitting and Sidebar

- Vertical bitting = 6 depths .025" increments
- Sidebar Pins: 3 angles, 2 positions = 6 permutations

	ORIGINAL	FORE	AFT
Left	L	K	M
Center	C	B	D
Right	R	Q	S



# MEDECO RESEARCH: Results of Project

- Covert and surreptitious entry in as little as 30 seconds: standard requires 10-15 minutes
- Forced entry: four techniques, 30 seconds, affect millions of locks
- Complete compromise of key control
  - Duplication, replication, simulation of keys
  - Creation of bump keys and code setting keys
  - Creation of top level master keys

# RESULTS OF PROJECT: Bumping

- Reliably bump open Biaxial and m3 locks
- Produce bump keys on Medeco blanks and simulated blanks
- Known sidebar code
- Unknown sidebar code

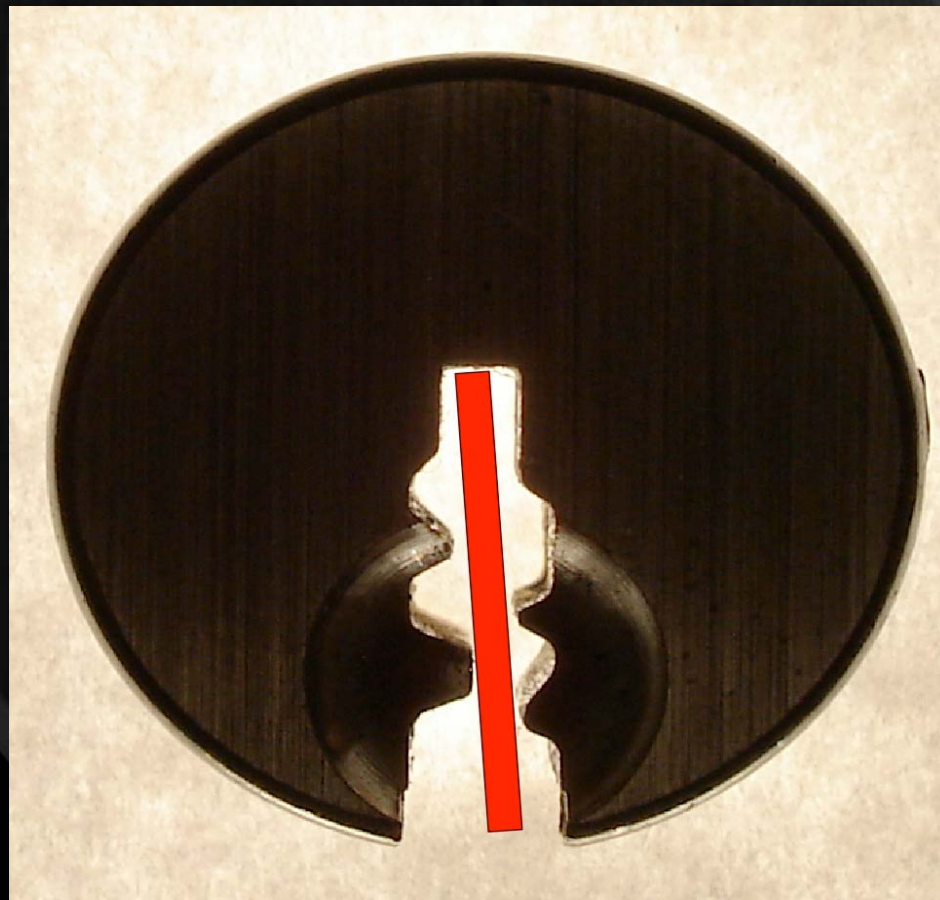
# MEDECO BUMP KEY



# RESULTS OF PROJECT: Key Control and Key Security

- Total compromise of key control and key security, vital to high security locks
  - Duplicate, replicate, simulate keys for all m3 and some Biaxial keyways
    - Restricted keyways, proprietary keyways
    - Government and large facilities affected
  - Attack master key systems
  - Produce bump keys
  - Produce code setting keys

# SIMULATED BLANKS: Any m3 and Many Biaxial Locks



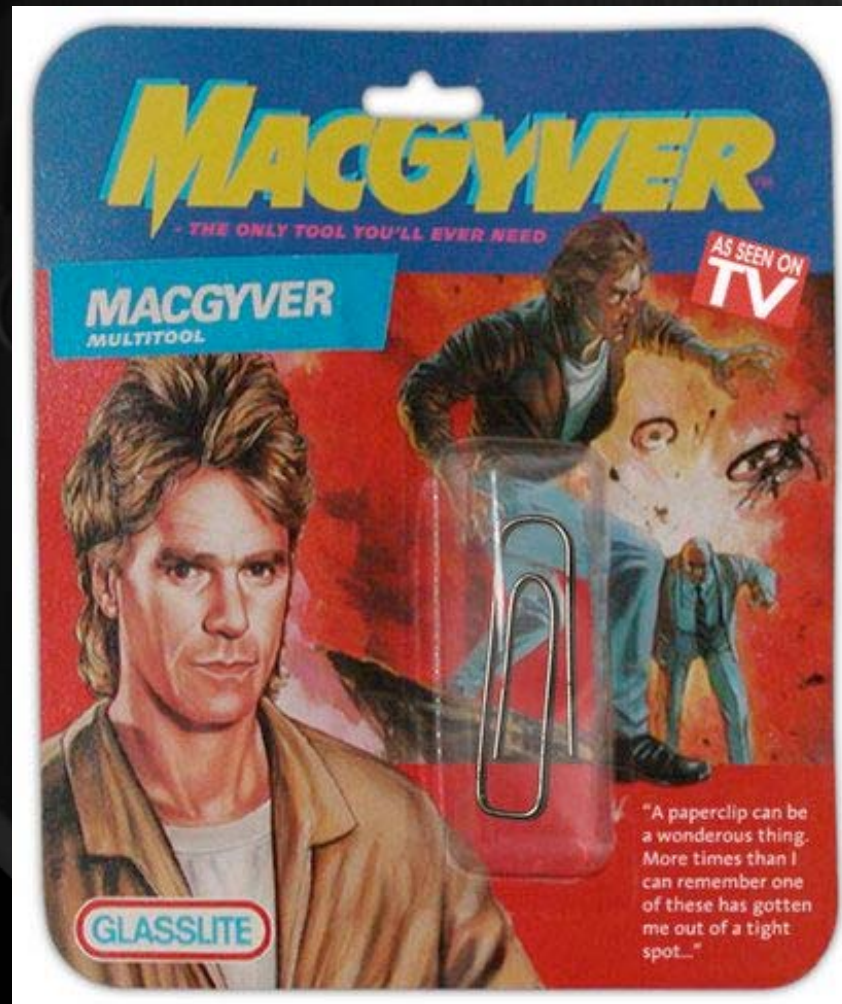
# SIMULATED BLANKS



# M3 SLIDER: Bypass with a Paper clip



# SECURITY OF m3:





# RESULTS OF PROJECT: Picking

- Pick the locks in as little as 30 seconds
- Standard picks, not high tech tools
- Use of another key in the system to set the sidebar code
- Pick all pins or individual pins
- Neutralize the sidebar as security layer

# PICKING A MEDECO LOCK



# Video Demo:

- Picking Medeco Locks

# RESULTS OF PROJECT: Decode Top Level Master Key

- Determine the sidebar code in special system where multiple sidebar codes are employed to protect one or more locks
- Decode the TMK
- PWN the system



# RESULTS OF PROJECT: Forced Entry Techniques

- **Deadbolt attacks on all three versions**
  - Deadbolt 1 and 2: 30 seconds
  - Deadbolt 3: New hybrid technique of reverse picking
- **Mortise and rim cylinders**
  - Prior intelligence + simulated key
- **Interchangeable core locks**

# DEADBOLT ATTACK



# DEADBOLT BYPASS: 2\$ Screwdriver + \$.25 materials



# Video Demo:

- **Deadbolt Bypass**



# MORTISE CYLINDER



# MORTISE ATTACK



# Video Demo:

- Mortise Cylinder Bypass

# CONNECTING THE DOTS

- CRITICAL FAILURES
- Original → Biaxial
  - pin design
  - code assignment
- Biaxial → m3 design
  - M3 slider geometry = .040" offset
  - Key simulation
  - .007" keyway widening

# MORE DOTS!

- **FORCED ENTRY**
- Original Deadbolt design
- Fatal design flaw: 30 seconds bypass
- Later deadbolt designs: new attacks
- Mortise and rim cylinders
- Inherent design problem: .065" plug

# MORE DOTS: BILEVEL LOCK

- 2007 Bilevel locks introduced
- Integrate low and high security to compete
- Flawed design, will affect system security when integrated into high security system
- Borescope decoding of aft pins to compromise security of entire system

# CONNECTING THE DOTS: The Results

- Biaxial Code assignment: Reverse Engineer for all non-master key systems
- Gate tolerance: 4 keys to open
- NEW CONCEPT: Code Setting keys
- Sidebar leg-gate interface: NEW CONCEPT: Setting sidebar code
- M3 Wider keyway: Simulated blanks
- Slider design: paper clip offset

# 4 KEYS TO THE KINGDOM





# Video Demo:

- Code Setting Keys

# Video Demo:

- Bump Proof...
- Virtually Bump Proof...
- Virtually Bump Resistant...

# LESSONS TO BE LEARNED

- Patents do not assure security
- Apparent security v. actual security
- 40 years of invincibility means nothing
- New methods of attack
- Corporate arrogance and misrepresentation
- “If it wasn’t invented here” mentality
- All mechanical locks have vulnerabilities

# COUNTERMEASURES: Primary Design Rules

- ARX pin design
- Dual State Locking: 3KS
- Interactive key elements (MCS)
- 2 or 3 security layers
- No direct intelligence from manipulation
- Cannot defeat one layer and bypass others

# Video Demo

- Bypass...Medeco Gen4

Thank You!



*in.*Security.Org

[mwtobias@security.org](mailto:mwtobias@security.org)

[mjfiddler@security.org](mailto:mjfiddler@security.org)

© 2008 Marc Weber Tobias