MEDECO CASE STUDY

Cracking One of the Most Secure Locks in America

Lessons learned from embedded design deficiencies, a failure of imagination, and a failure to connect the dots, and a belief in invincibility

MEDECO PRESENTATION

- HIGH SECURITY LOCKS
  - Attack methodology
- MEDECO LOCKS
  - High security: Why secure?
  - Sidebar IS security
  - Case history
  - ID Vulnerabilities
  - Codes

MEDECO PRESENTATION

- HIGH SECURITY REQUIREMENTS
  - Key control
  - Covert and Surreptitious entry
  - Forced entry
- RESULTS OF RESEARCH PROJECT

ATTACK METHODOLOGY FOR HIGH SECURITY LOCKS

- Assume and believe nothing
- Ignore the experts
- Think “out of the box” and “inside the lock”
- 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 for each requirement

MEDECO HIGH SECURITY

MEDECO HIGH SECURITY: What it means

- UL, BHMA/ANSI, Vd.S 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

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

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

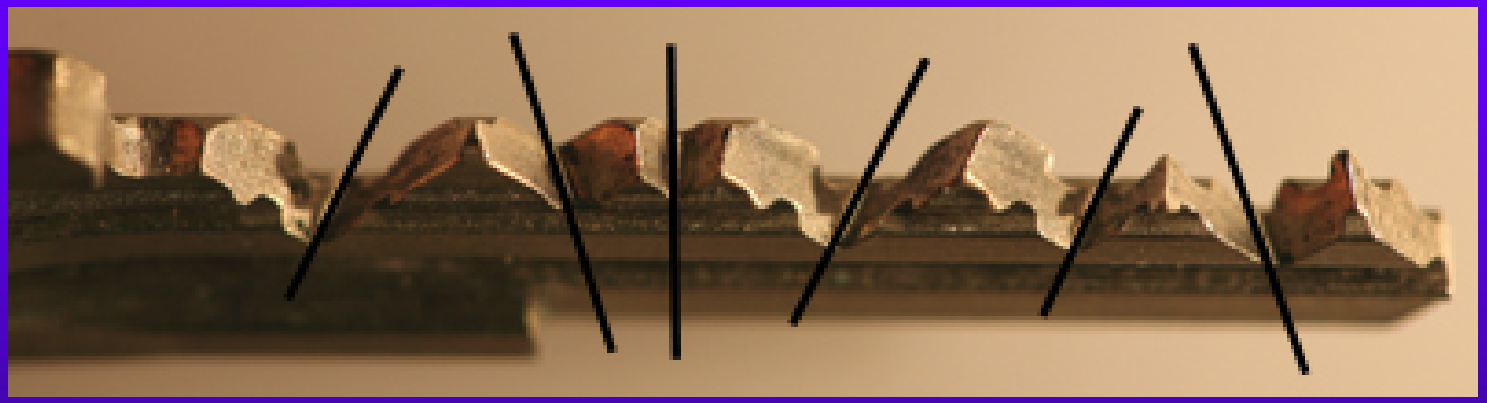
MEDECO LOCKS:
3 Independent Security Layers

- Layer 1: PIN TUMBLERS to shear line
- Layer 2: SIDEBAR: 3 angles x 2 positions
- Layer 3: SLIDER – 26 positions
- TO OPEN:
  - Lift the pins to shear line
  - Rotate each pin individually
  - Move the slider to correct position

HIGH SECURITY LOCKS: Why Important?

- 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 TWISTING PINS:
3 Angles + 2 Positions



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

STORY OF 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

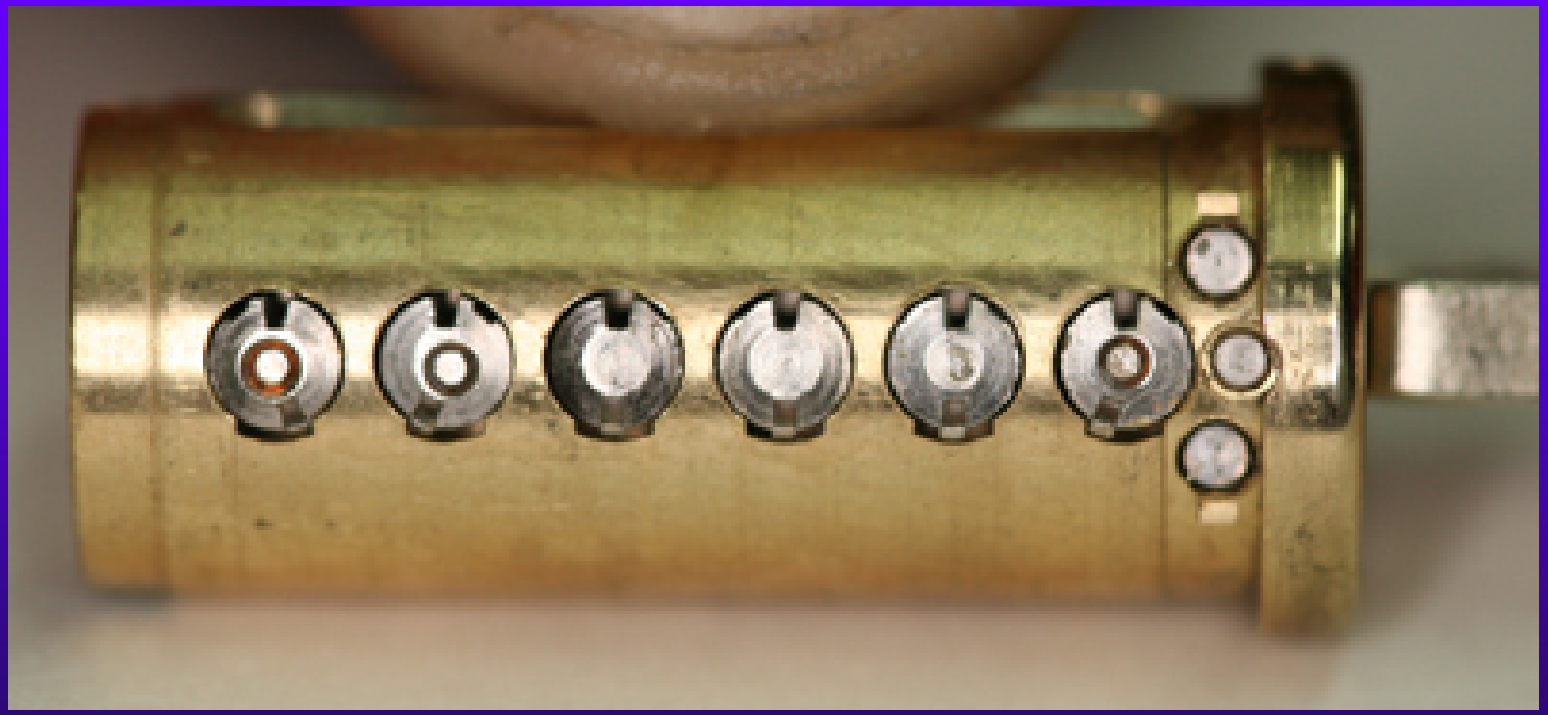
Misstatements and disinformation

18 month research project results:

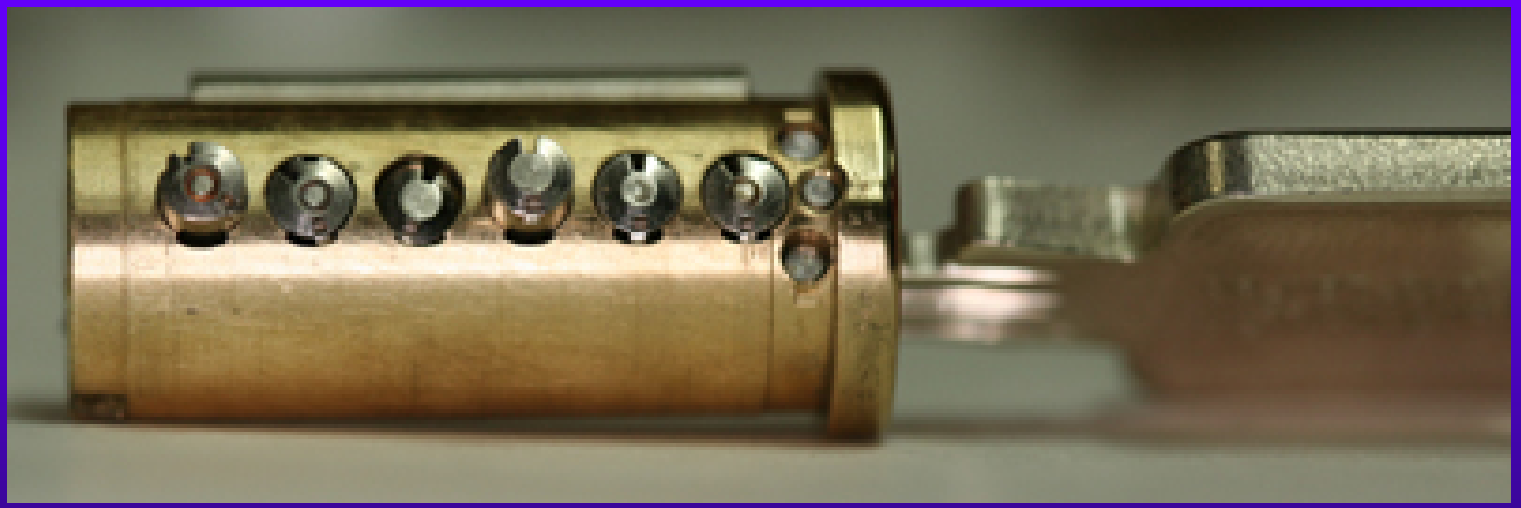
Total compromise of security

PLUG AND SIDEBAR: All pins aligned

SIDEBAR RETRACTED



PLUG AND SIDEBAR: Locked



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

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 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

CRACKING MEDECO LOCKS:

Exploit Design Features and System Parameters

- Codes: design, progression
- Key bitting design: double-cutting
- Keying rules: Extrapolation of the TMK
  - Medeco master and non-master key systems
- Tolerances: 20 degree rotation
  - Sidebar leg – true gate tolerance

CRACKING MEDECO LOCKS:

Exploit Design Features and System Parameters

- Interaction of critical components and locking systems: Sidebar leg – gate
- Keyway and plug design
- Slider design and geometry
- Wider keyway

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
- December, 2007: Add 2500 codes

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

QUESTIONS: 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: More Questions

- 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?

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: Analyze 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

MEDECO KEY CONTROL: Critical Issues

- MEDECO: Simulation of code or key components
  - Bitting for particular lock
  - Sidebar code
- 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

MEDECO KEY CONTROL

- Bypass all m3 keyways
  - Simulate blanks
  - Some Biaxial keyways
- Set shear line
  - Plastic keys
- Hybrid attacks
  - Mortise, Rim, IC

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
  - 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 Entrie
- Clay and Silicone casting
- Key simulation: Medeco
- Rights amplification
- Alter similar keys

COVERT and FORCED ENTRY RESISTANCE

High Security Requirement

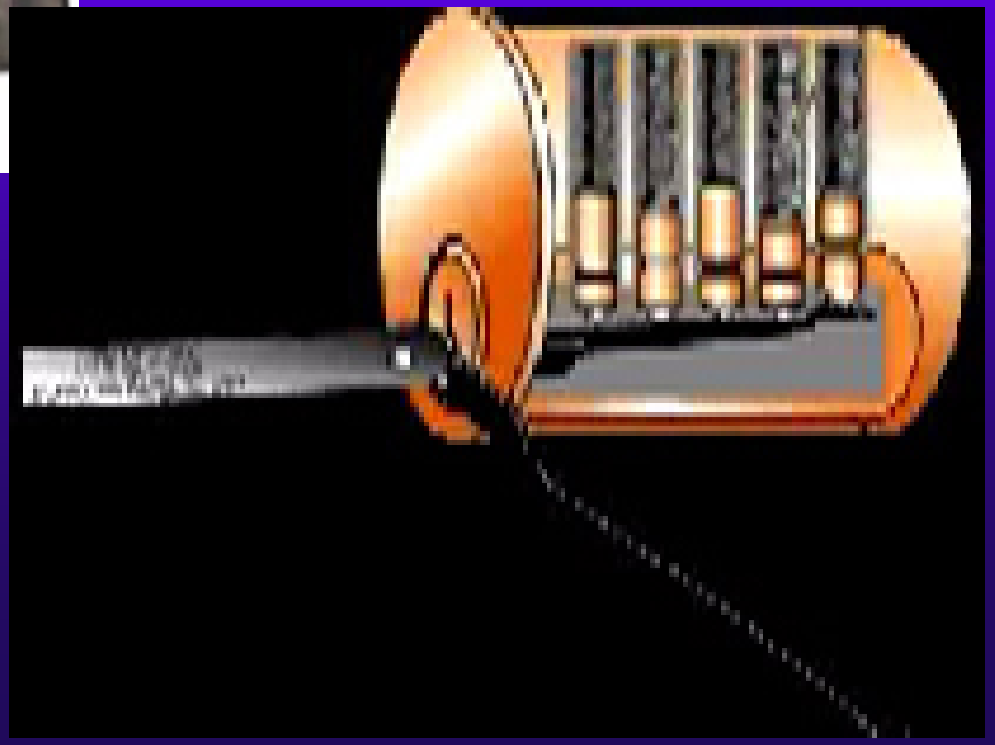
CMOE: Covert Methods of Entry

- Picking
  - Set the sidebar code
  - Code setting keys
  - Any change key
- Bumping
- Decoding
  - Otoscope
  - Borescope

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 more sophisticated methods

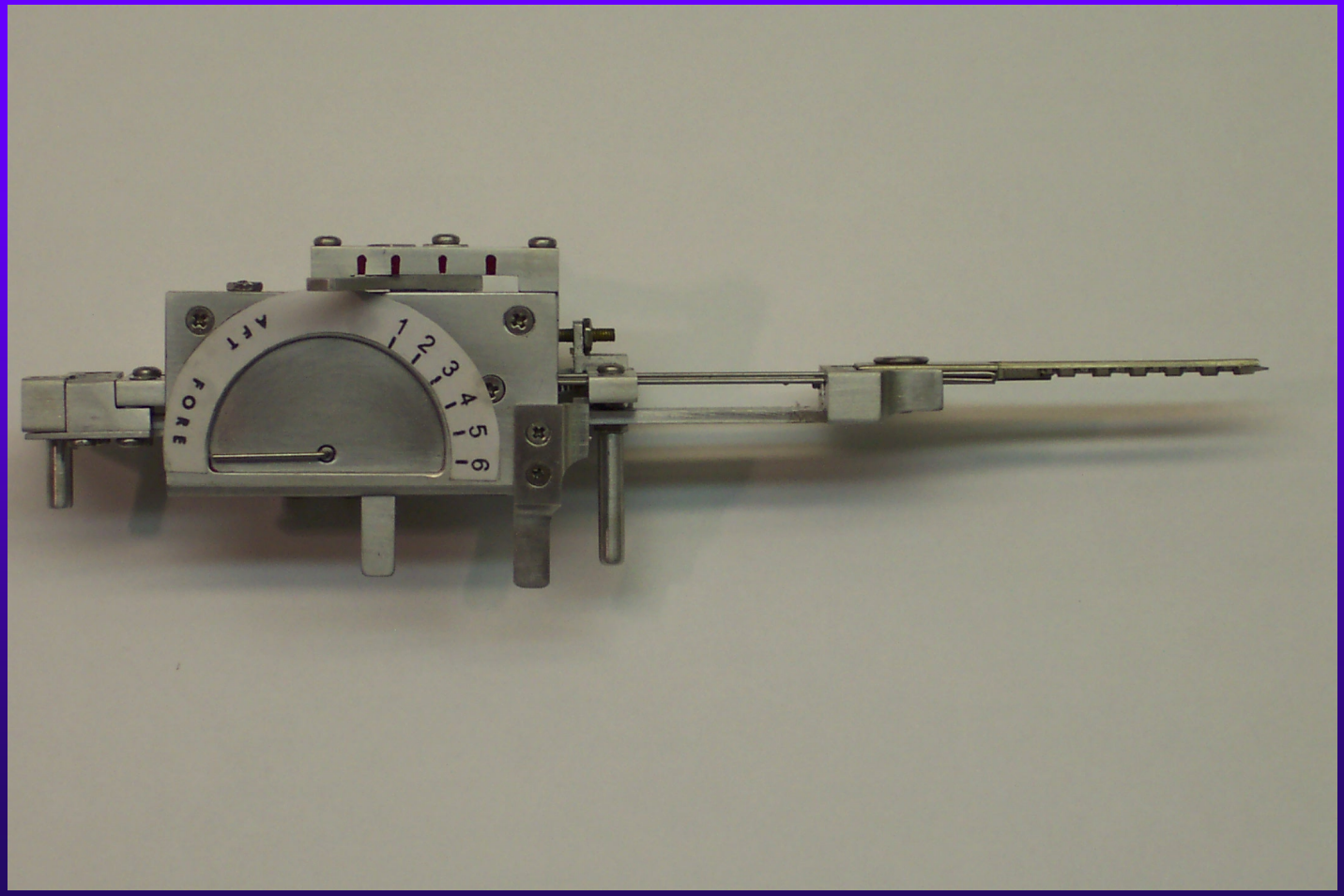
MEDECO: CONVENTIONAL PICKING



PICKING MEDECO LOCKS

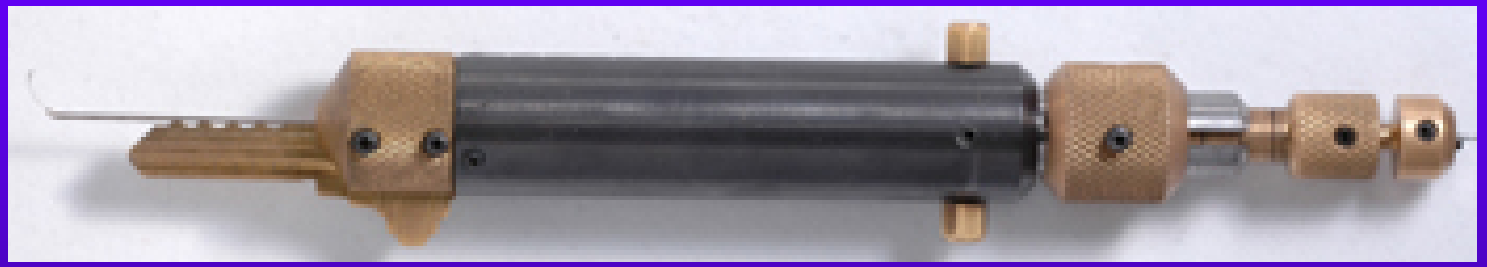
- Change key
- Code setting key
  - Set the code and pick or bmp the lock
- Original blanks
- Simulated blanks

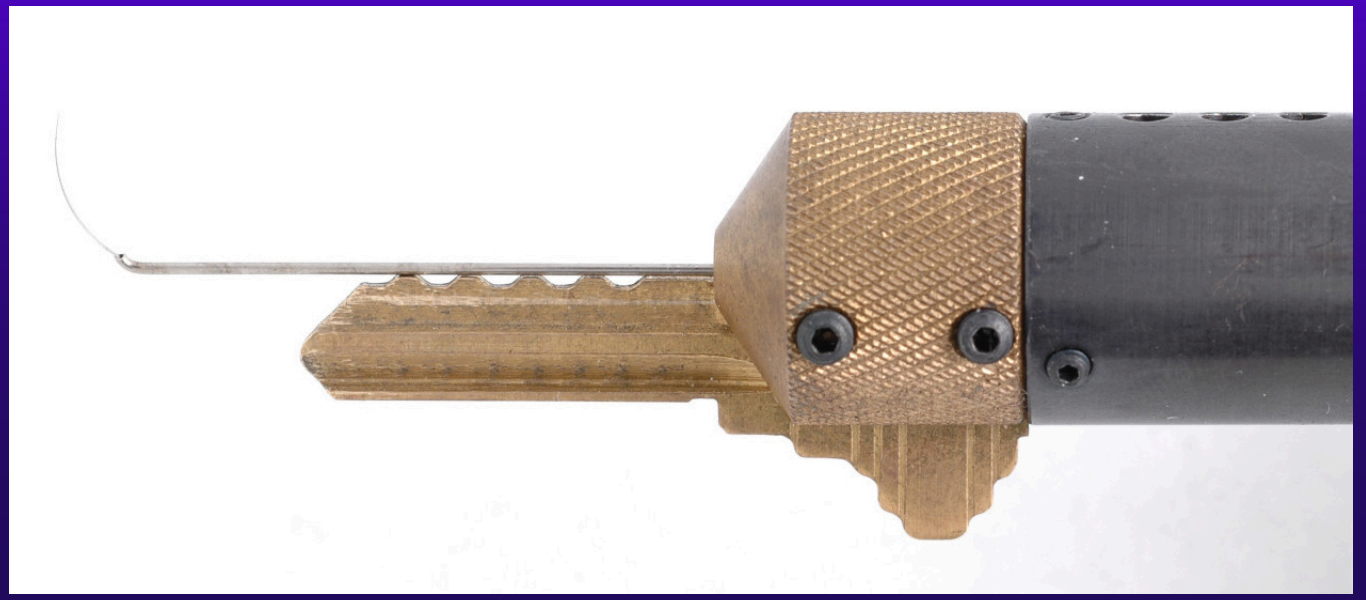
TOBIAS DECODER:
Medeco decoder: by “Crackpot!”



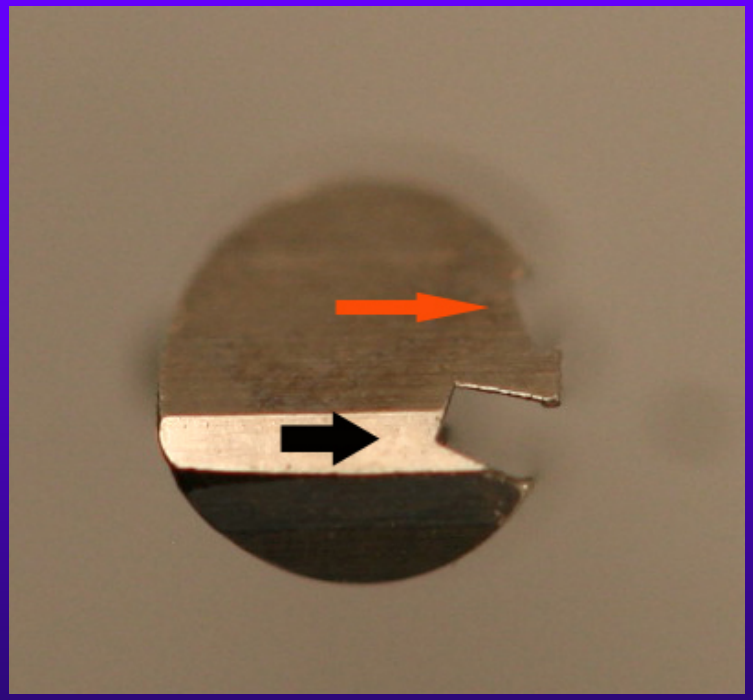
SOPHISTICATED DECODERS

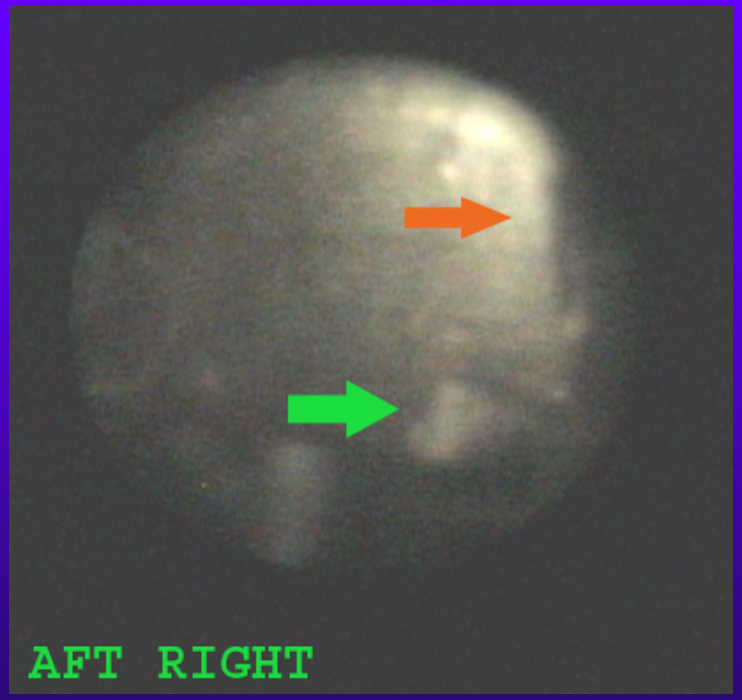
- John Falle: Wire Shim Decoder





AFT PINS: Decode Angles for Biaxial, m3, and Bilevel





FORCED ENTRY RESISTANCE

High Security Requirement

FORCED ENTRY ATTACKS: Deficiencies in standards

- Many types of attacks defined
- Do not contemplate mechanical bypass
- Must examine weakest linkis
- 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
- Compress plug
- 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

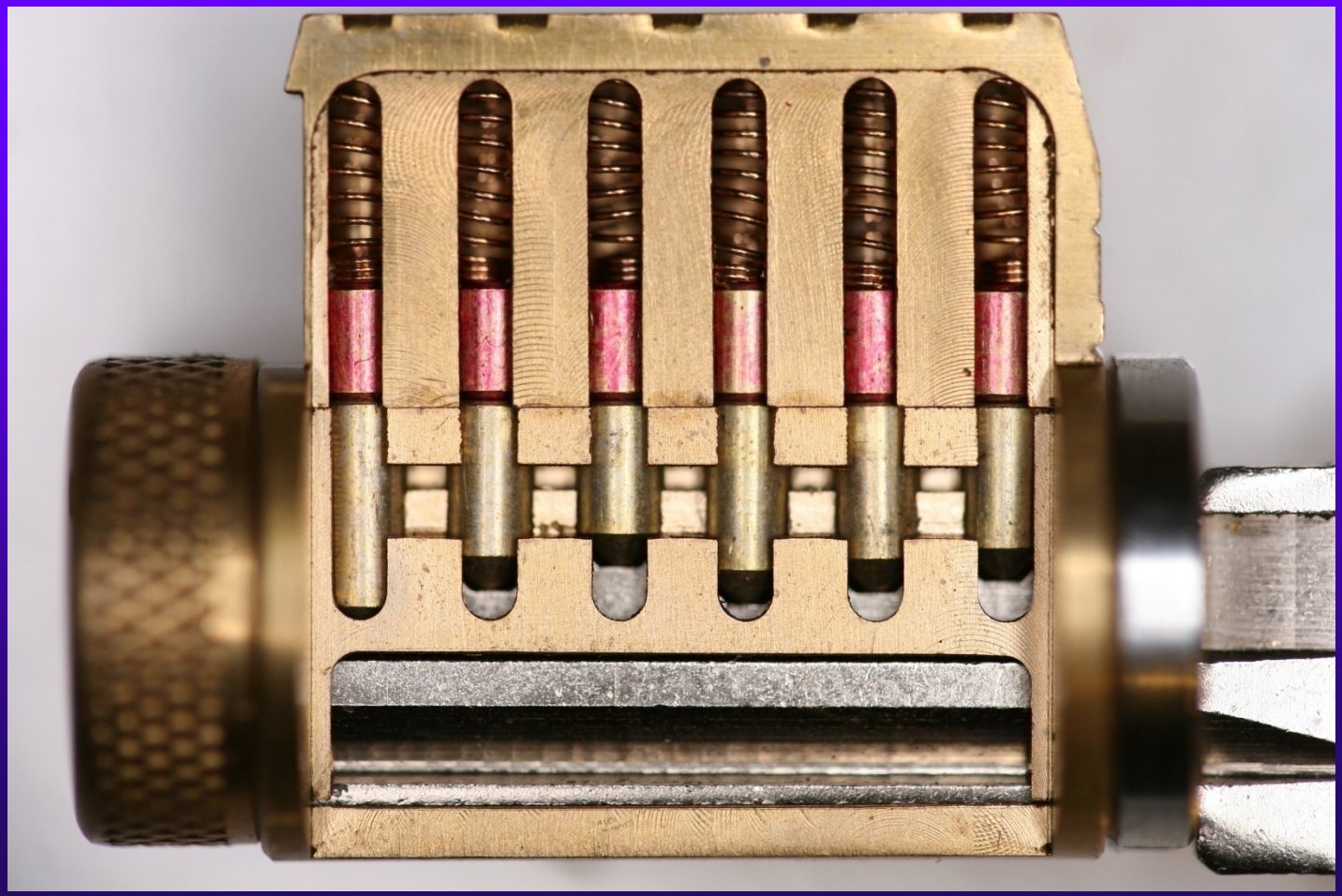
MEDECO MISTAKES

- 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

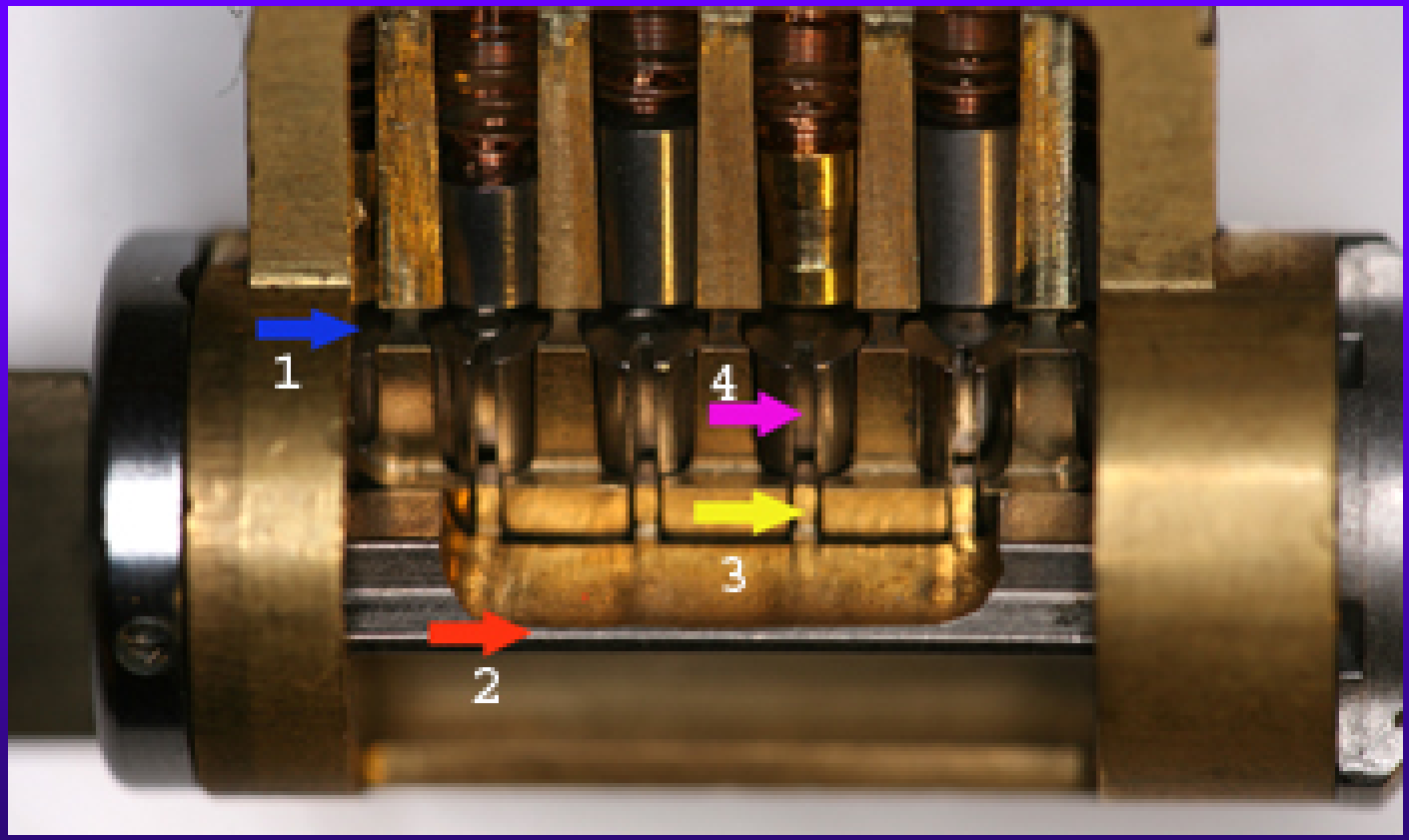
MEDECO TIMELINE

- 1970 Original Lock introduced
- 1985 Biaxial, Second generation
- 2003 m3 Third generation
- 2006 Bumping introduced to America
  - Medeco announces “Bump-Proof”
- 2007 Revised to “Virtually Bump-Proof”
- 2007 Revised to “Virtually Resistant”
- 2008 No public statements by Medeco

MODERN PIN TUMBLER



MEDECO BIAXIAL



SIDEBAR AS A GENERIC SECURITY CONCEPT

- 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, MCS= split
  - Medeco and 3KS = integrated
- Direct or indirect relationship and access by key bitting

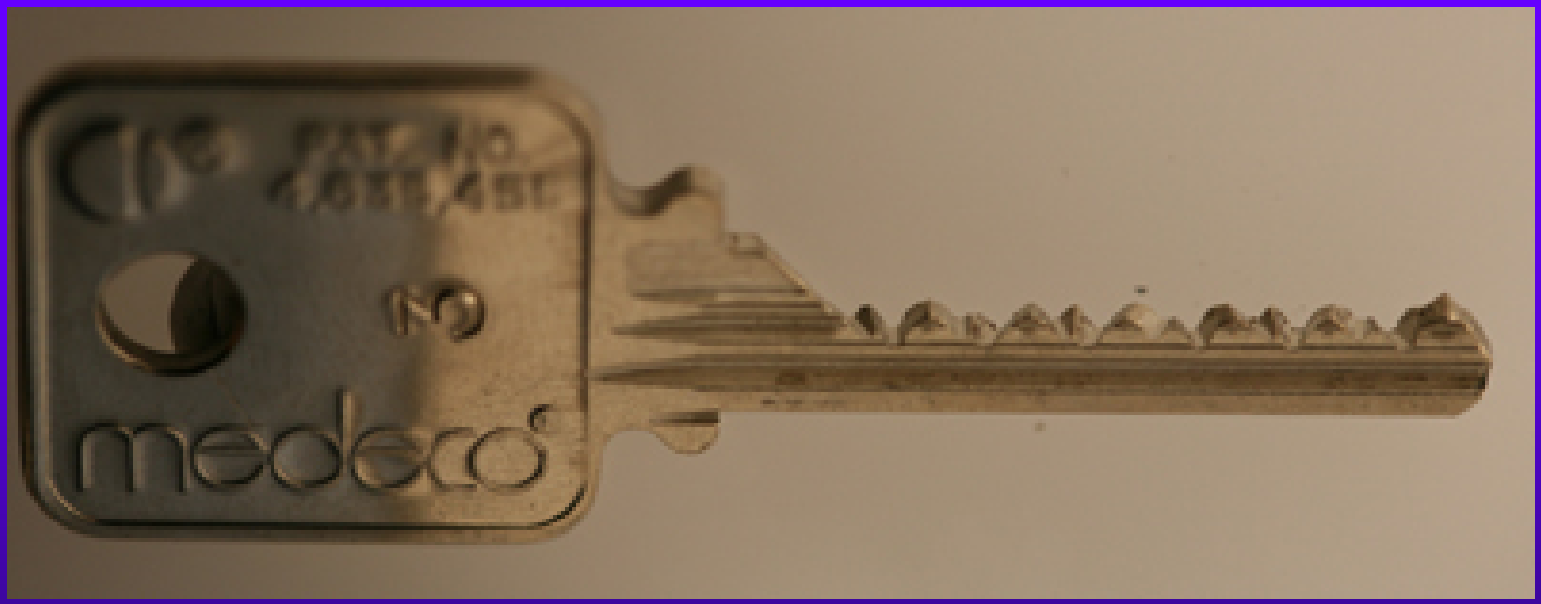
MEDECO RESEARCH: Results of Project

- 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

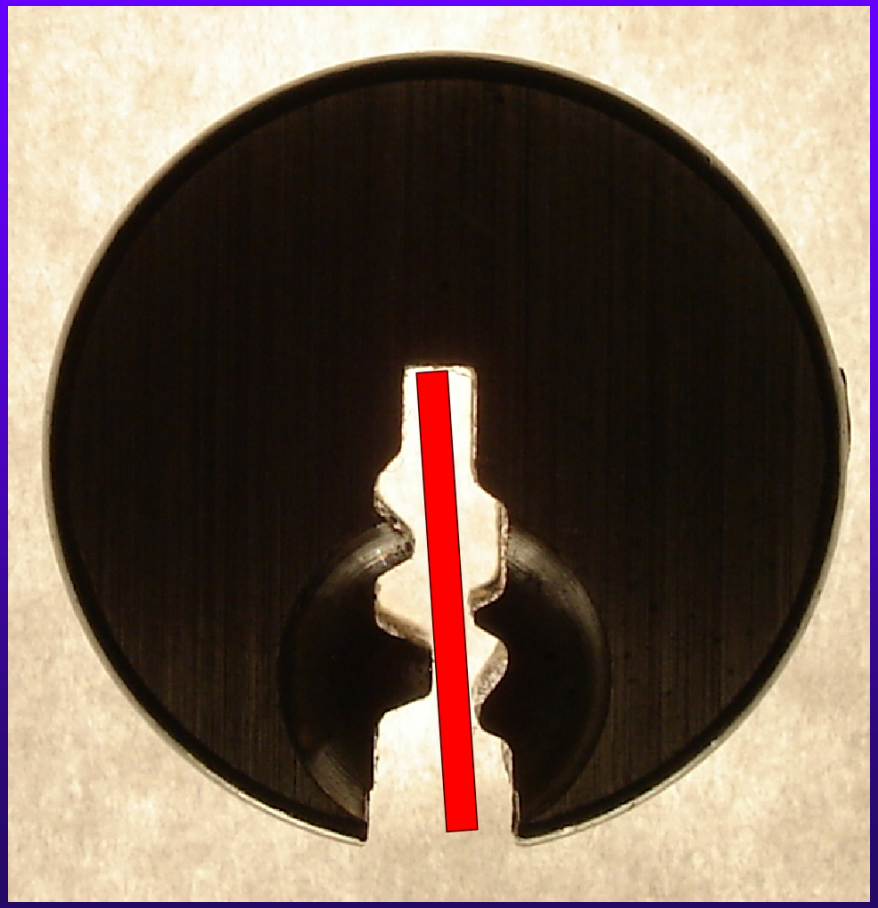
MEDECO BUMP KEY



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

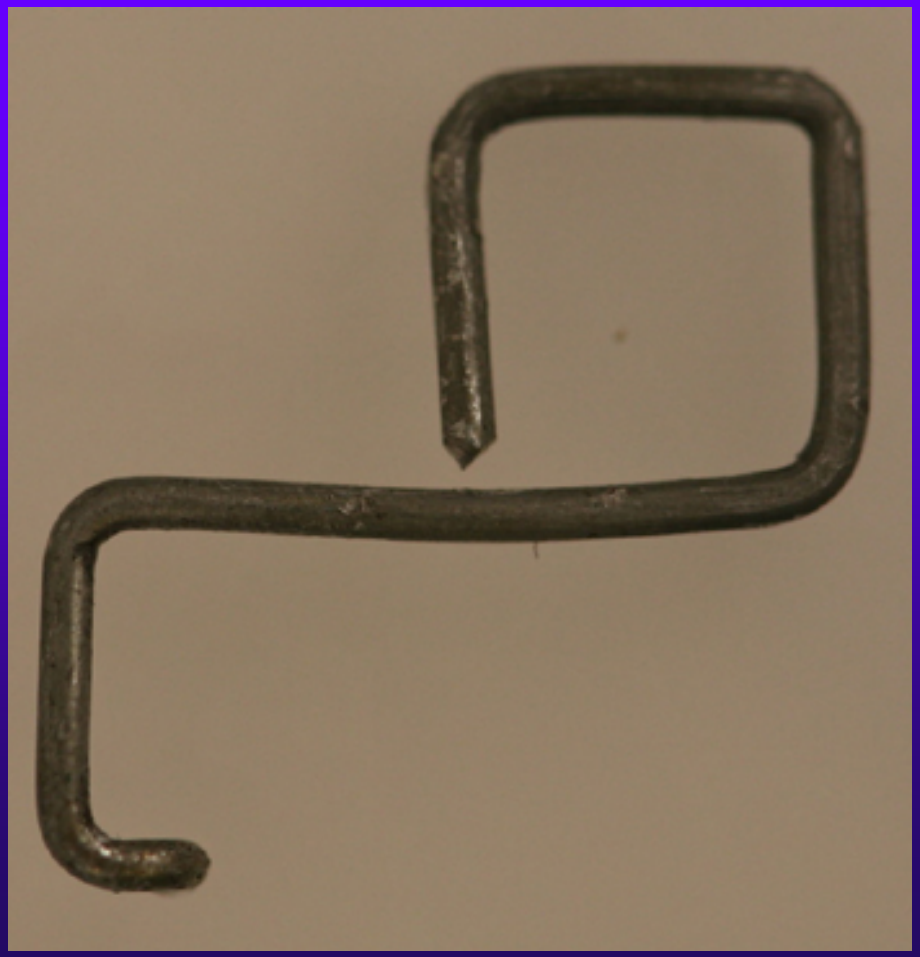
SIMULATED BLANKS: Any m3 and Many Biaxial Locks



SIMULATED BLANKS

M3 SLIDER:
Bypass with a Paper clip

SECURITY OF m3: High Tech Wire!



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

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

MORTISE CYLINDER

MORTISE ATTACK

MORTISE ATTACK

- Copy machine
- Scanner
- Cell phone camera
- Plastic sheets: Shrinky Dink
- X-acto knife

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

CODE SETTING KEYS:
Four Keys to the Kingdom

OPEN IN THIRTY SECONDS

- Setting the Sidebar Code
- Conventional pick tools

PICKING A MEDECO LOCK

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

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
- OWN the system

REAL WORLD ATTACK: Bumping a Medeco Lock

OPEN IN THIRTY SECONDS: Cracking one of the most secure locks in America

www.security.org

mwtobias@security.org