DESCONSTRUCTING LAYERS OF INSECURITY: The Medeco Case Study

Cracking One of the Most Secure Locks in America

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

MECHANICAL LOCKS

- The First security barrier
- Often the only security
- Conventional or high security locks
- Are they secure?
  - Against what threat?
  - Protection of what?
  - Time and access?
  - Must consider in context

SECURITY: APPARENT OR ACTUAL

- Most locks appear secure
- Many are not
- Conventional or high security rated
  - UL 437
  - BHMA/ANSI 156.30
- Layers of security
- Manufacturer may not know of insecurity
- Manufacturer may not disclose defects

WHY IMPORTANT?

- Detailed information for
  - Security managers
  - Risk managers
  - IT directors
  - Critical protection
  - Security begins with locks

LOCKS: MECHANICAL PUZZLES

- More complex, more difficult to open
- Greater complexity = vulnerabilities
- All are apparently secure
- Many design flaws never discovered
- Manufacturers compromise on security
- Manufacturing and R&D Cost v. Security

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

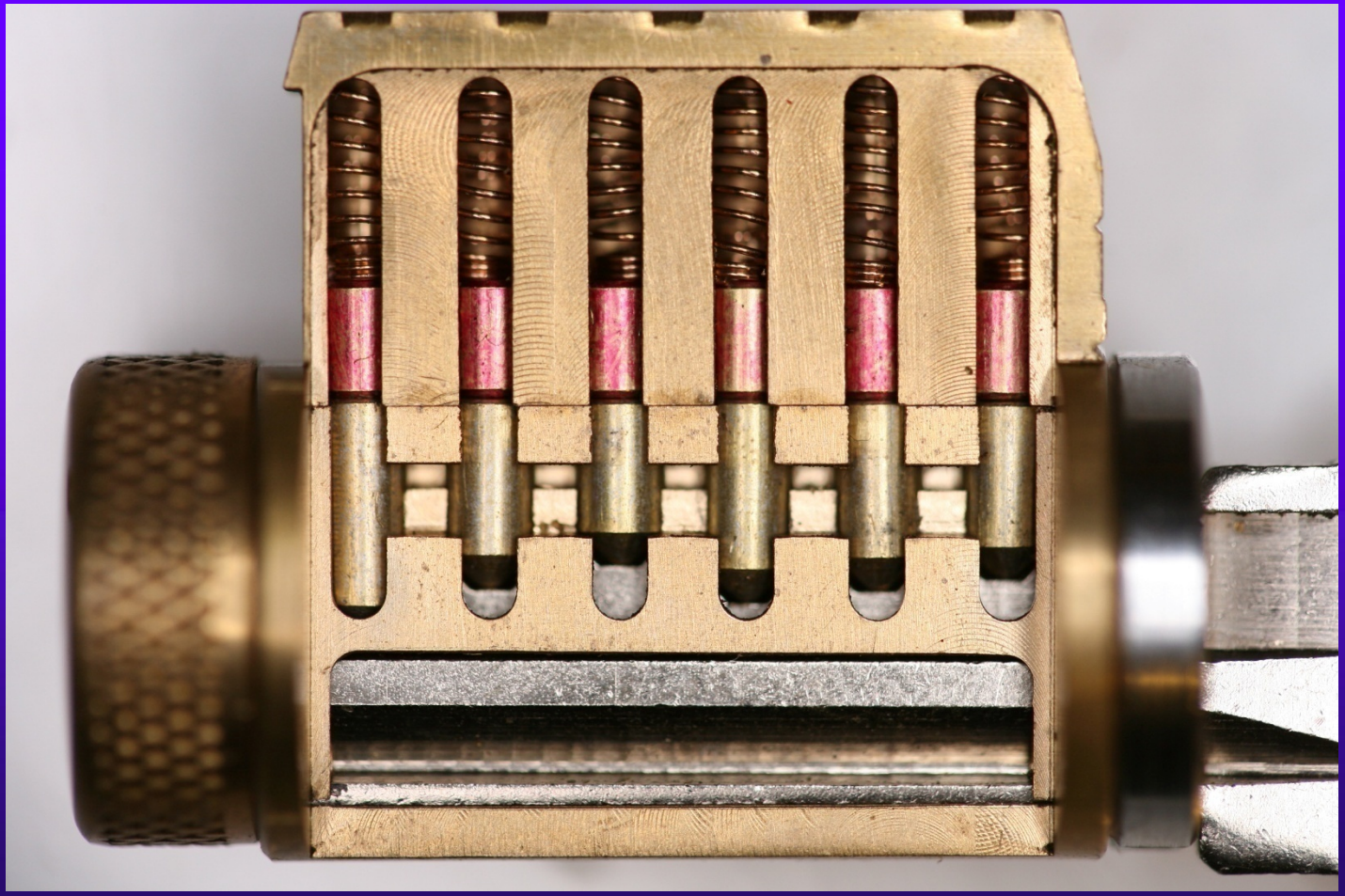
LAYERS OF SECURITY

- Independent and parallel
- Each a separate point of failure
- Add complexity to bypass
- Does not equal more security
- Conflicts possible
- Many different types:
  - Sliders
  - Sidebars

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

MODERN PIN TUMBLER



CONVENTIONAL LAYERS OF SECURITY = SHEAR LINE

- Keyways and their design
- sectional keyways
- Check pins
- Security pins, anti-bump pins
- High tolerances
- Key control: Everest and Medeco m3
- Master key systems

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

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 Design Factors

- Resistance against forced entry
- Resistance against covert and surreptitious entry
- Key control and “key security”
- Vulnerabilities for each 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 more sophisticated methods

ATTACK METHODOLOGY FOR HIGH SECURITY LOCKS

- 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

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."

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

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

DECONSTRUCTING LAYERS OF SECURITY: Medeco Locks

- Many lessons learned
- Discovered serious security vulnerabilities
- Applicable to residential, commercial, and government users
- Serious potential liability issues
- Resulted in a detailed book

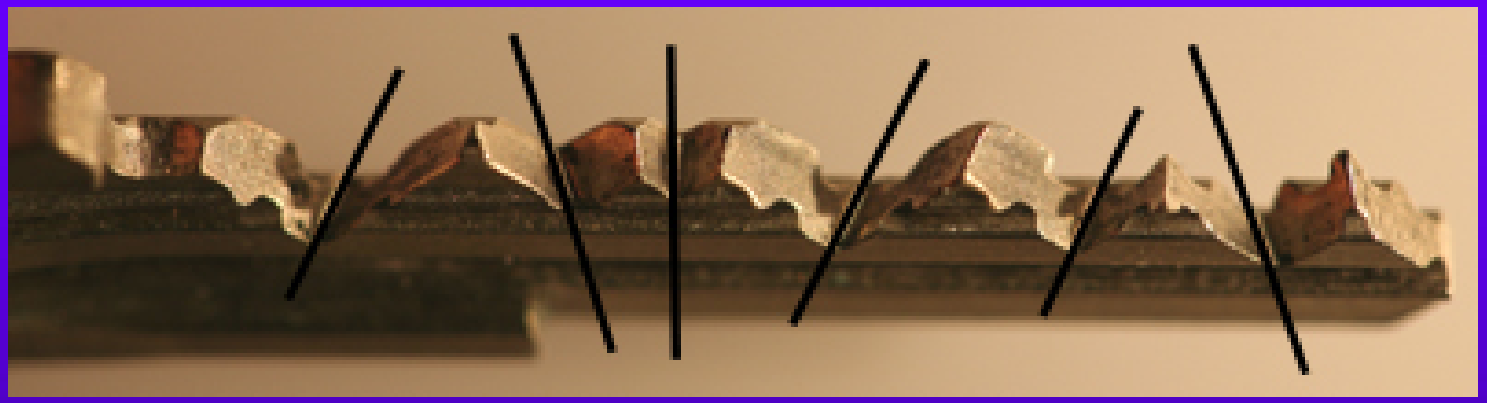
WHY THE MEDECO CASE STUDY IS IMPORTANT

- 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

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

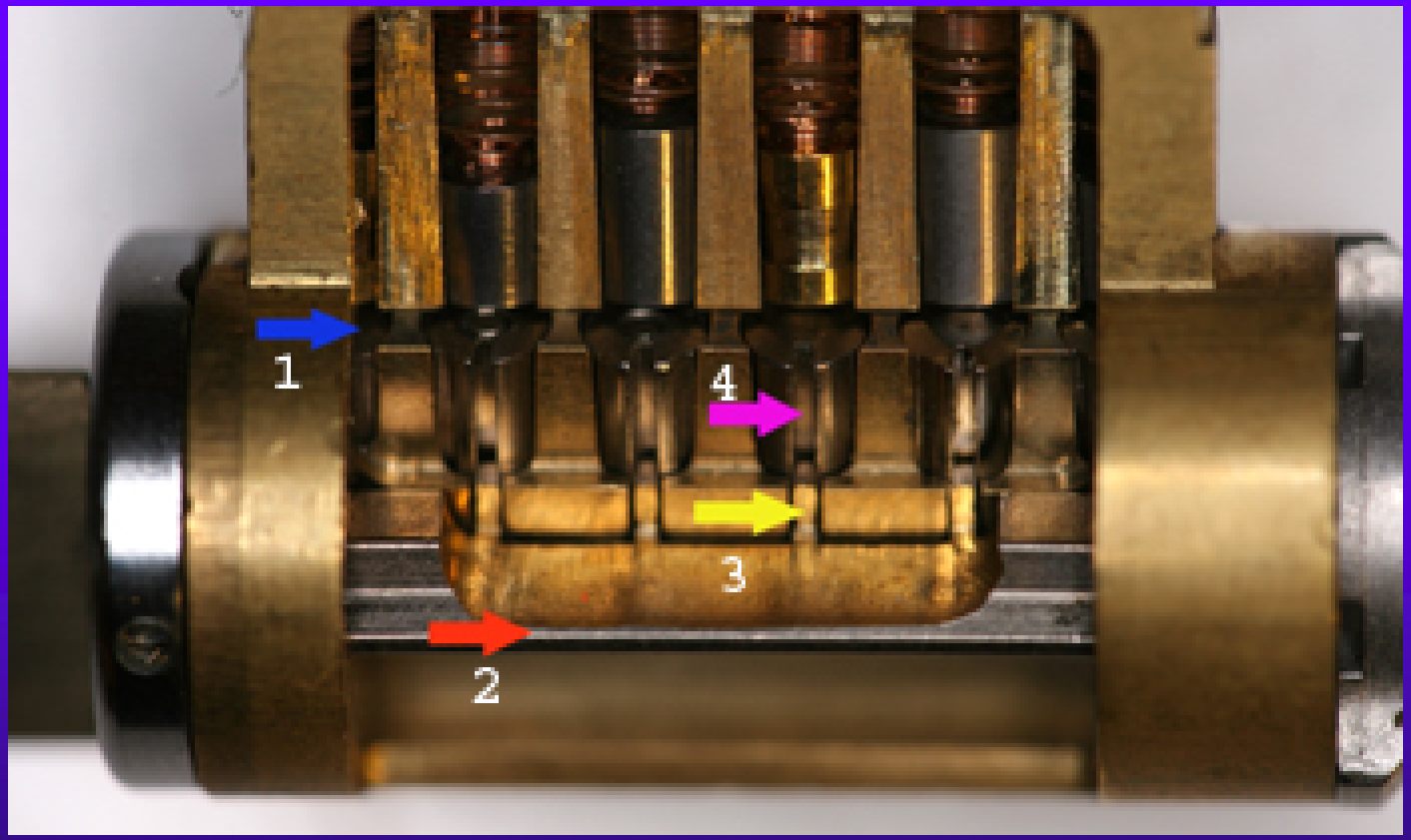
MEDECO TWISTING PINS: 3 Angles + 2 Positions



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
- False Gates, ARX Pins,
- High tolerance
- TO OPEN:
  - Lift the pins to shear line
  - Rotate each pin individually
  - Move the slider to correct position

MEDECO BIAXIAL

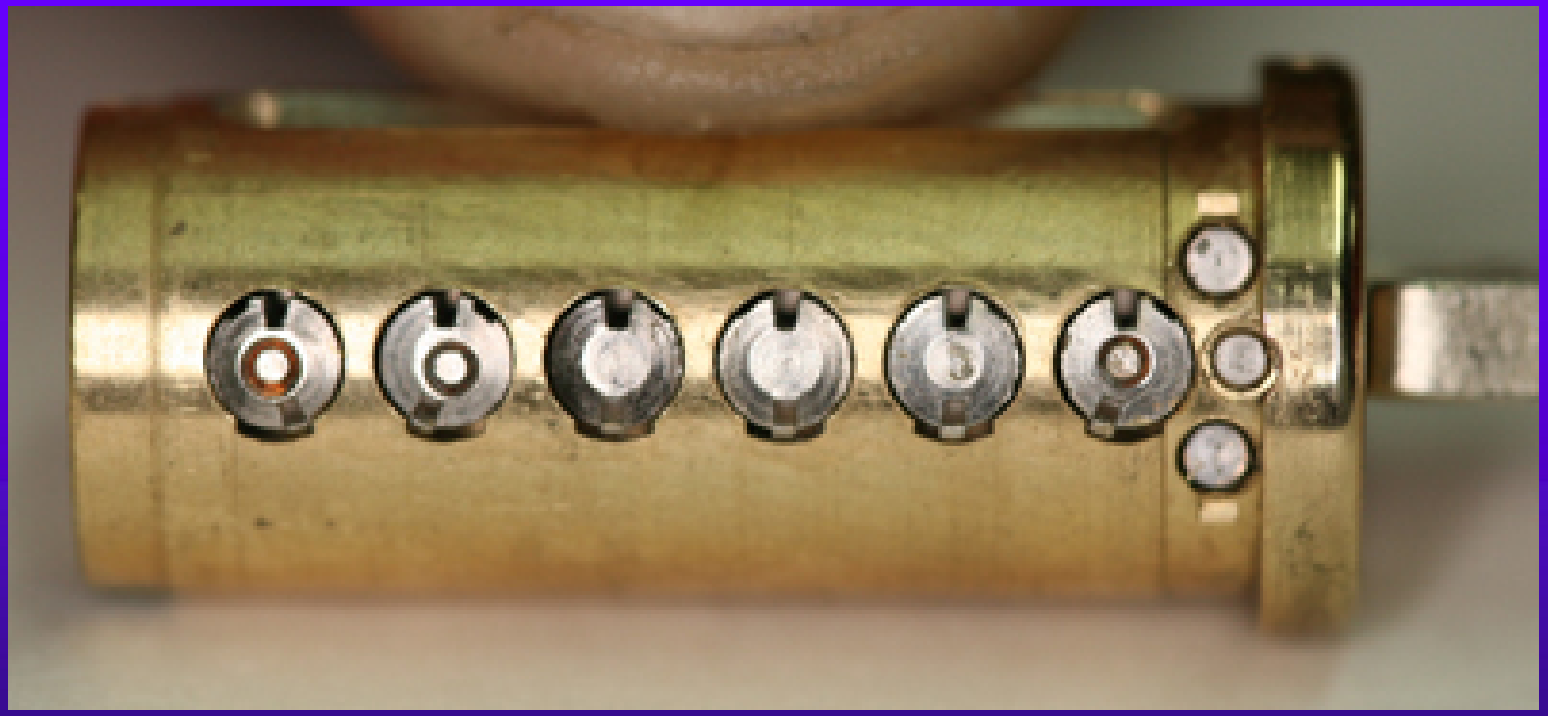


SECURITY CONCEPTS: Sidebar IS Medeco Security

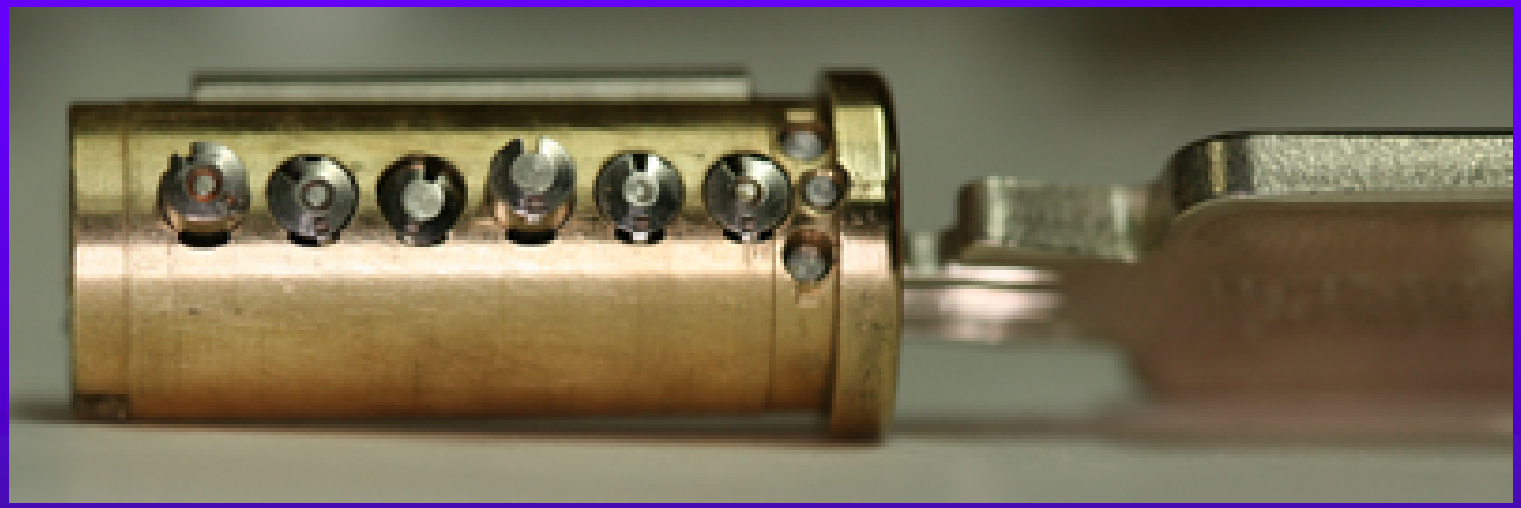
- GM locks, 1935, Medeco re-invented
- Heart of Medeco security and patents
- Independent and parallel security layer
- Integrated pin: lift and rotate to align
- Sidebar blocks plug rotation
- Pins block manipulation of pins for rotation to set angles

PLUG AND SIDEBAR:
All pins aligned

SIDEBAR RETRACTED



PLUG AND SIDEBAR: Locked



MEDECO 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

EXPLOIT DESIGN FEATURES AND SYSTEM PARAMETERS

- Codes: design, progression
- Key bitting design
- Tolerances
- Keying rules
  - Medeco master and non-master key systems
- Interaction of critical components and locking systems: Sidebar leg and gates
- Keyway and plug design
- M3 design: wider keyway

MEDECO RESEARCH: Results of Project

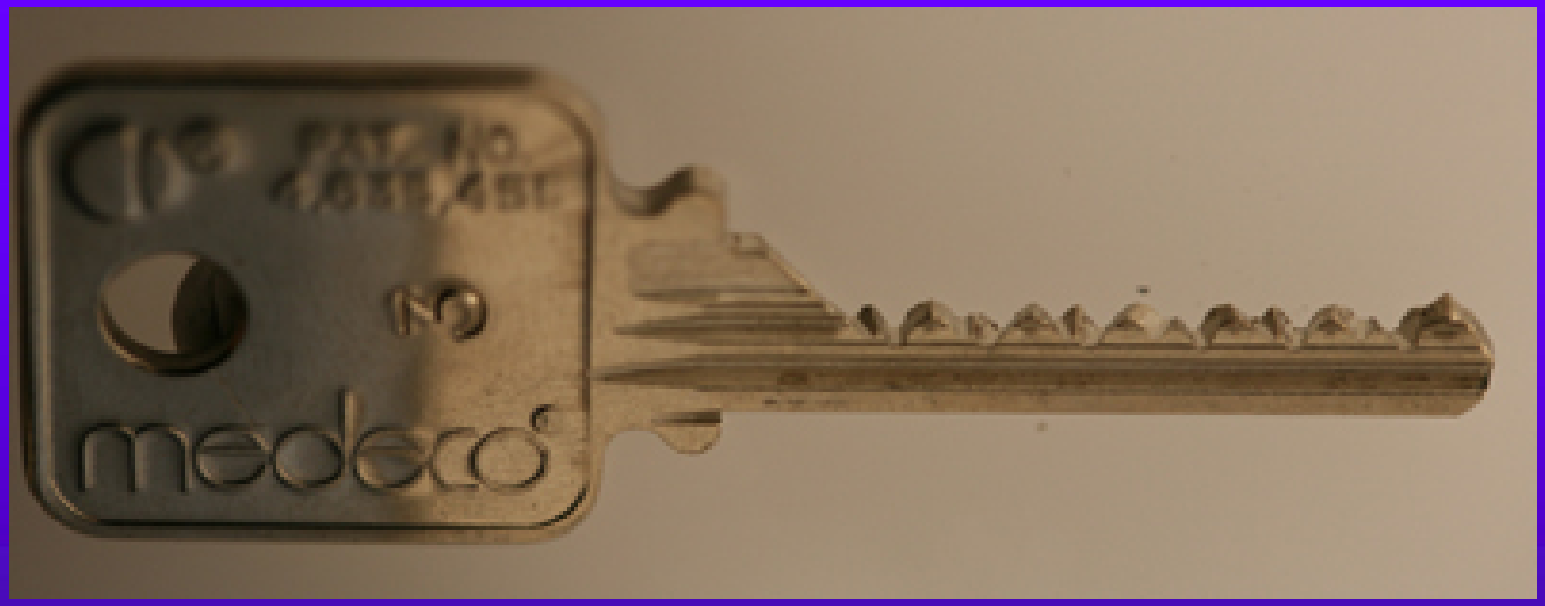
- Covert and surreptitious entry in as little as 30 seconds: standard requires 10-15 minutes
- Forced entry: four techniques, 30 seconds, affect millions of locks
- Complete compromise of key control
  - Duplication, replication, simulation of keys
  - Creation of bump keys and code setting keys
  -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

4 KEYS TO THE KINGDOM

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

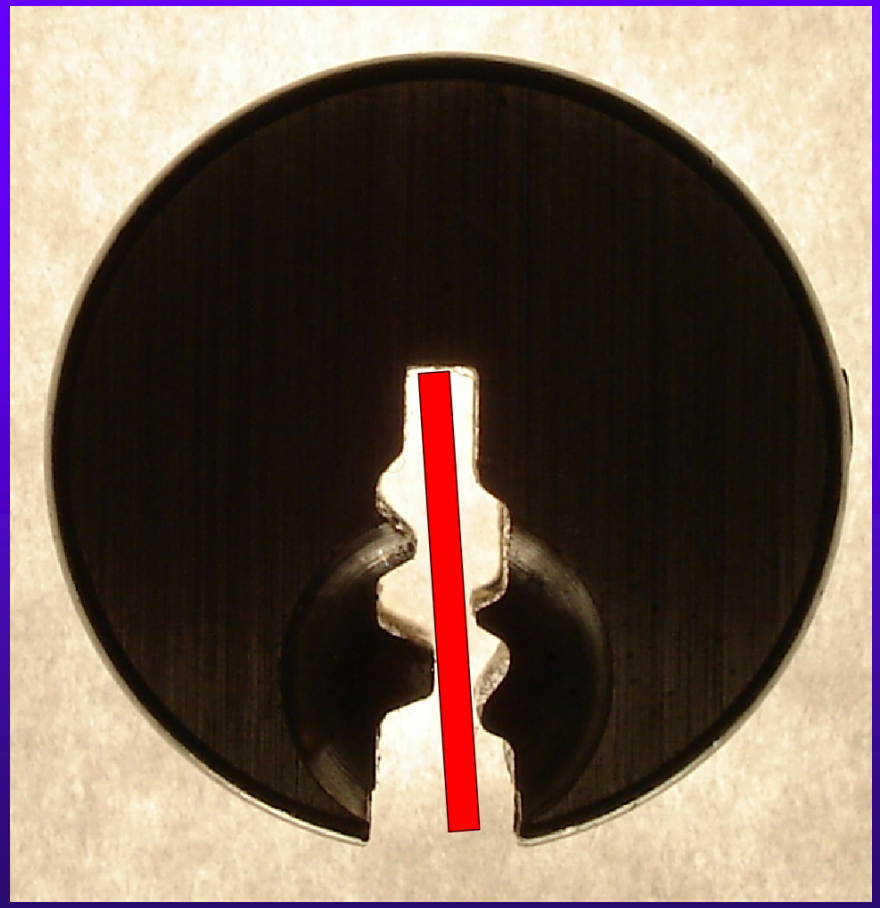


REAL WORLD ATTACK: Bumping a Medeco Lock

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

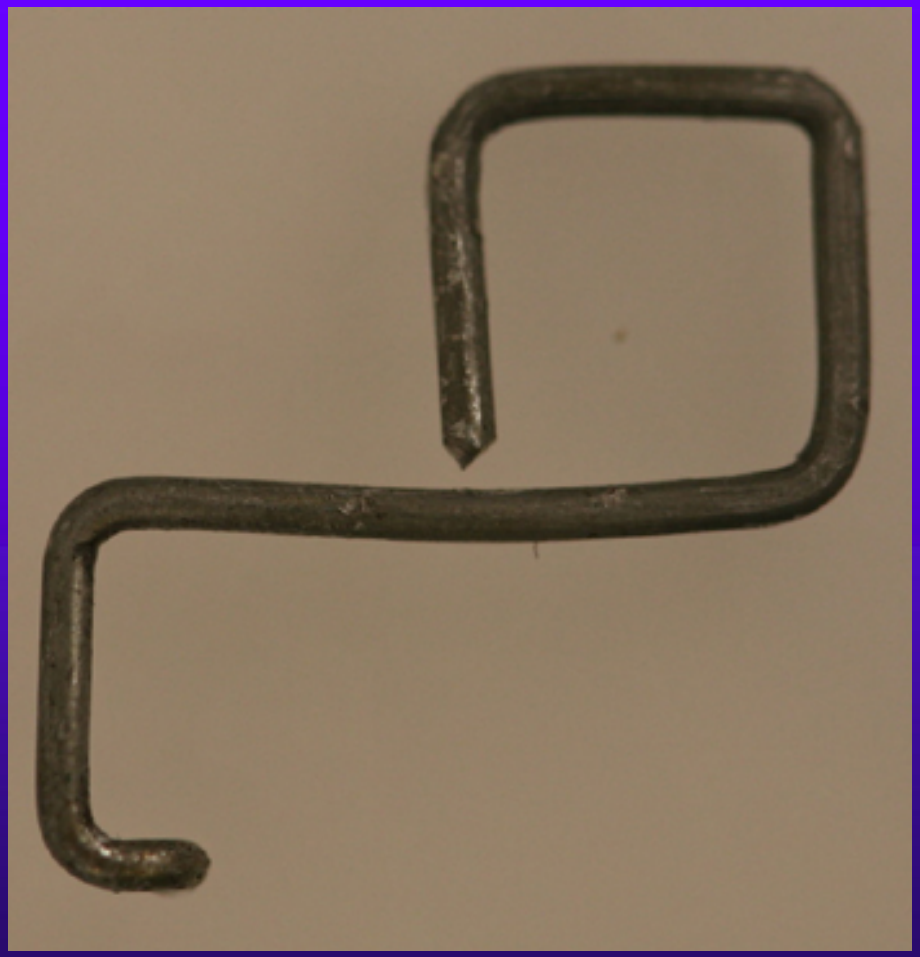
SIMULATED BLANKS: Any m3 and Many Biaxial Locks



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

PICKING A MEDECO LOCK

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

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

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

RESPONSIBLE DISCLOSURE

- Medeco announced their locks were bump-proof
  - Medeco learned they were not
- Medeco was shown how their locks could be picked with four keys
- Medeco was shown how their key control could be compromised
- Medeco knew their deadbolts could be opened in seconds

IRRESPONSIBLE NON-DISCLOSURE?

- Should they have advised their customers when they believed their locks could be compromised?
- Should they have warned their dealers regarding their deadbolt issue before they fixed it?
- Do they have an affirmative duty to disclose vulnerabilities that could affect their customers?

RESPONSIBLE DISCLSOURE BY A MANUFACTURER?

- Should a lock manufacturer disclose vulnerabilities to the public
- Should they promote Security by Obscurity
- Does the public have a right to know
  - There are security vulnerabilities
  - The details of those vulnerabilities
  - How much of a risk

HIGH SECURITY LOCK MANUFACTURERS: Special Duties to Customers?

- Nature of product
- What is at risk
- Disclosure to customer v. educating criminals: Which is more important?
- Does the dealer and customer need to know
- Liability for non-disclosure?

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

www.security.org

mwtobias@security.org