LOCKS AND HIGH SECURITY: 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

HIGH SECURITY LOCKS

- PROTECTION OF HIGH SECURITY FACILITIES
  - Critical infrastructure
  - Airports and transportation
  - Public Safety
  - Information
- HIGH SECURITY REQUIREMENTS
  - Key control
  - Covert and Surreptitious entry
  - Forced entry

LOCKS: FIRST LINE OF DEFENSE

- PHYSICAL SECURITY AND I-T INTEGRATION
- CONVENTIONAL V. HIGH SECURITY LOCK
- ELECTRONIC ACCESS CONTROL ISSUES
- RELIANCE ON STANDARDS
- RESULTS IF FAILURE OF SECURITY
  - Criminal activity, theft, collusion
  - Sabotage, unauthorized access
  - Compromise of information
  - Destruction of evidence

SECURITY SYSTEMS: LOCKS

- RESTRICT ACCESS
- TRACK PEOPLE AND THEIR ACCESS
- TRACK ENTRY AND ATTEMPTS

CRITICAL QUESTIONS

- WHAT IS SECURITY RE LOCKS
- IS IT SECURE ENOUGH
- WHAT DOES A HIGH SECURITY RATING MEAN
- CONCEPT OF KEY CONTROL , KEY SECURITY, AND WHY IMPORTANT
- CAN THE LOCK BE COMPROMISED AND HOW DIFFICULT
- REAL WORLD THREATS
- METHODS TO COMPROMISE AND BREAK

LOCKS AND SYSTEMS: CATEGORIES

- CONVENTIONAL LOCKS
- HIGH SECURITY LOCKS
- ELECTRONIC ACCESS CONTROL

MEDECO: WHO ARE THEY?

- 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
- Not easily compromised for 40 years

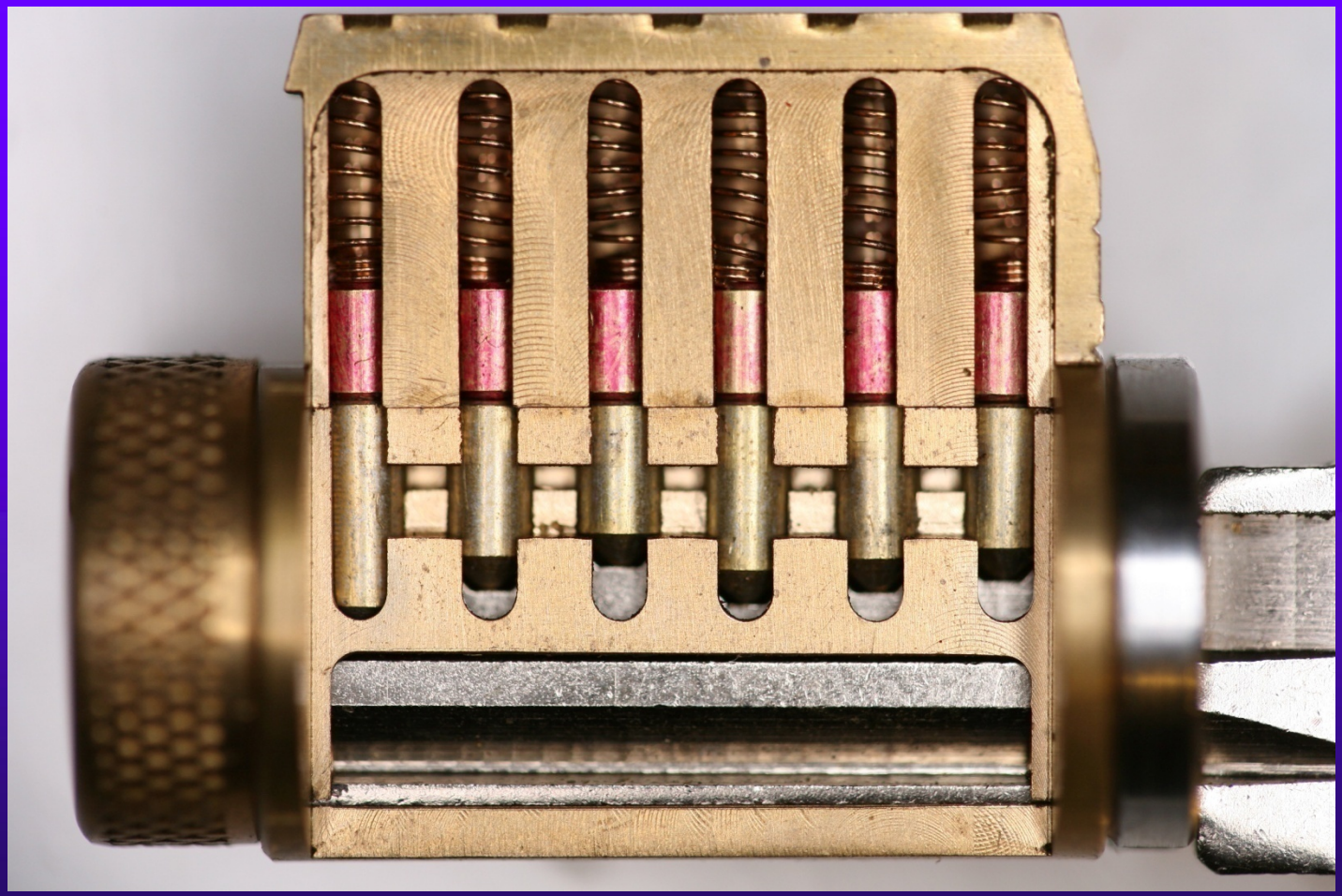
WHY THE MEDECO CASE STUDY IS IMPORTANT

- 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
    - UL 437 and BHMA/ANSI 156.30
  - Higher quality and tolerances
  - Resistance to Forced and Covert Entry
  - Key control

MODERN PIN TUMBLER



HIGH SECURITY LOCKS: Why Important?

- Protect high value targets
- Stringent security requirements
- High security Standards: UL, BHMA
- Threat level is higher
- Minimum security criteria
  - Attack times and resistance
  - More difficult to compromise

STANDARDS: THE PROBLEM

- WHAT DO THEY MEASURE?
- WHY WE NEED STANDARDS
- NOT REAL WORLD
- LIMITED TESTING, FEW TESTS
- MECHANICAL BYPASS
- SPECIAL ATTACK TECHNIQUES
- BUMPING

STANDAFORDS: CRITERIA

- COVERT ENTRY
- FORCED ENTRY
- KEY CONTROL

COVERT ENTRY PROTECTION: The Theory

- MINIMUM SECURITY CRITERIA IN UL 437 and BHMA/ANSI 156.30
- PROTECT AGAINST CERTAIN FORMS OF COVERT ENTRY
- ASSURE MINIMUM RESISTANCE TIMES TO OPEN: 10-15 Minutes
  - Picking, Decoding
  - Bumping (not covered)
  - Decoding and Master Key attacks

FORCED ENTRY PROTECTION: UL 437 and BHMA 156.30 Standards

- LOCKS ARE SECURE AGAINST FORCED METHODS OF ATTACK
- MINIMUM TIMES SPECIFIED IN UL 437 and BHMA/ANSI 156.30
  - ATTACK RESISTANCE: 5 MINUTES
- DOES NOT INCLUDE MANY METHODS OF ATTACK

PHYSICAL SECURITY: LEGAL REQUIREMENTS

- SARBANES OXLEY (2002)
- OTHER STATUTORY REQUIREMENTS
- HIPPA
  - PROTECTION OF INFORMATION
  - SANCTIONS FOR VIOLATION

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
  - Connect the dots

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
- *Mechanical bypass
  - * Not covered by UL or BHMA standards

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."

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 bypass each layer
- Difficult to derive intelligence about a layer
- Difficult to simulate the action of the key

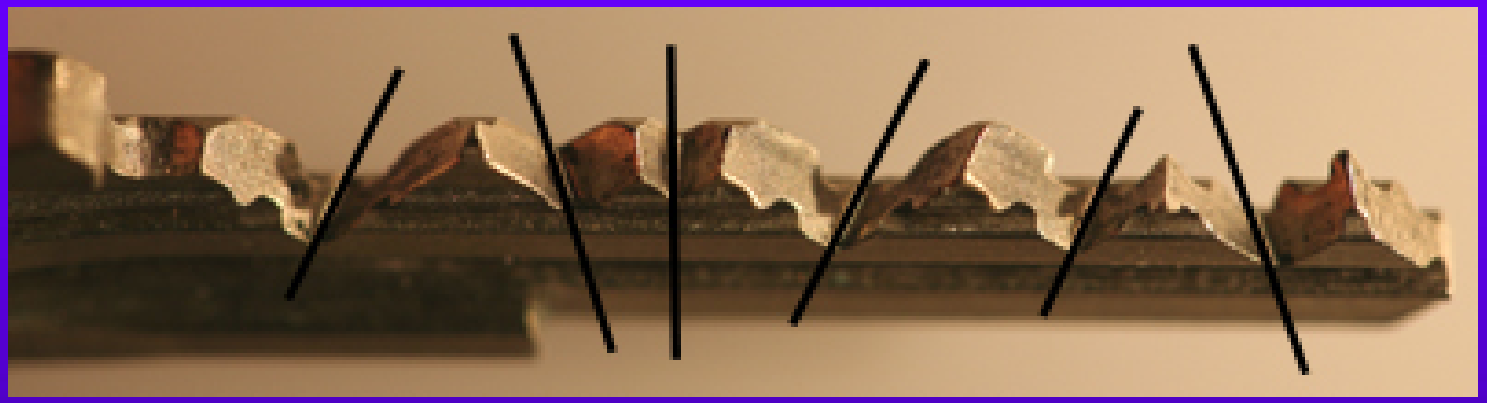
MEDECO HIGH SECURITY: What it means

- 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
  - If keys can be replicated: no security

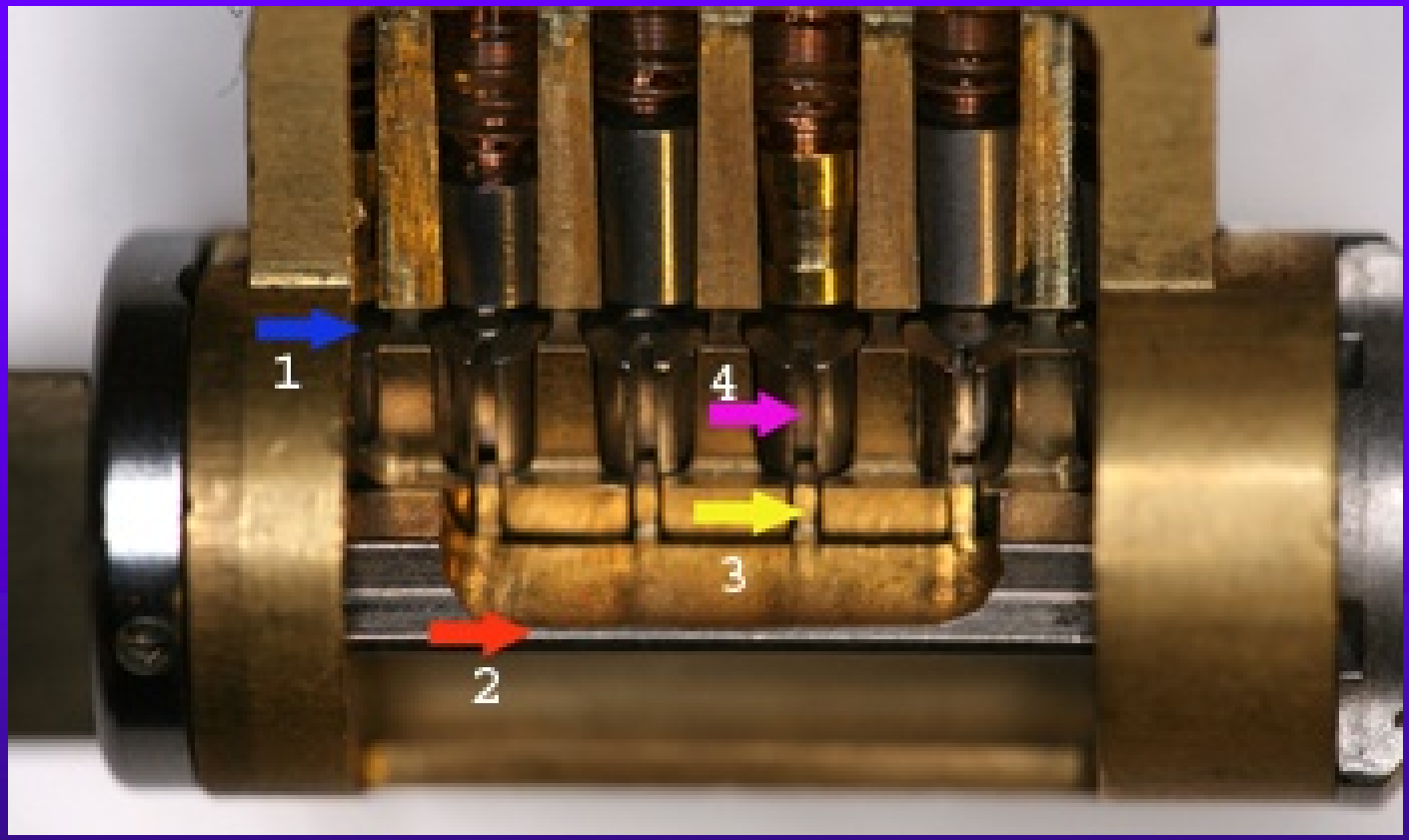
MEDECO LOCKS:
3 Independent Security Layers

- 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

MEDECO TWISTING PINS:
3 Angles + 2 Positions



MEDECO BIAXIAL (1985-2003)



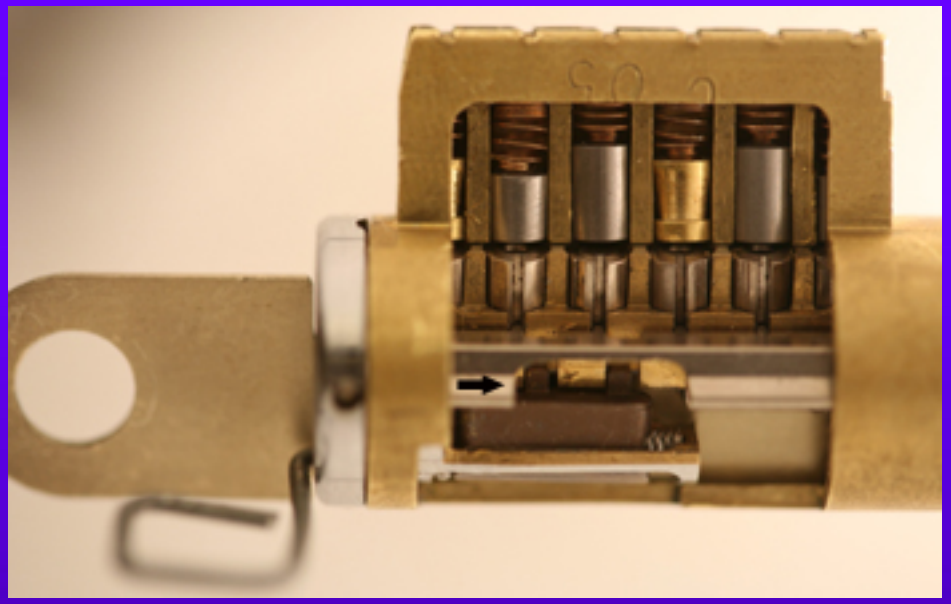
SECURITY CONCEPTS: Sidebar IS Medeco Security

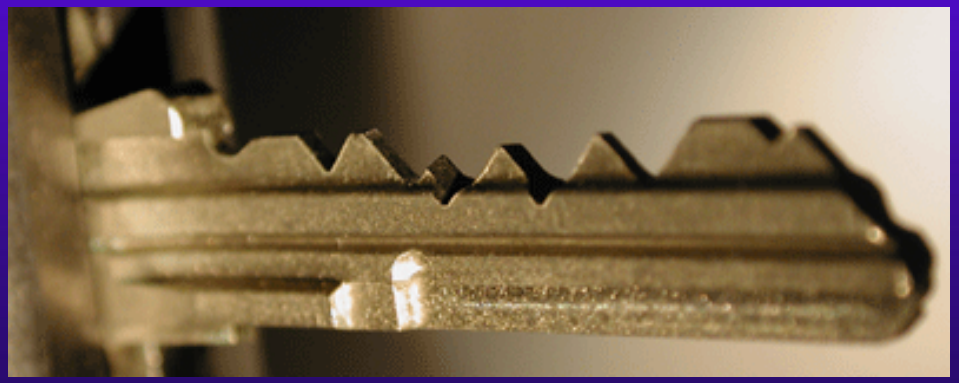
- GM locks, 1935, Medeco re-invented
- Heart of Medeco security and patents
- Independent and parallel security layer
- Integrated pin: lift and rotate to align
- Sidebar blocks plug rotation
- Pins block manipulation of pins for rotation to set angles

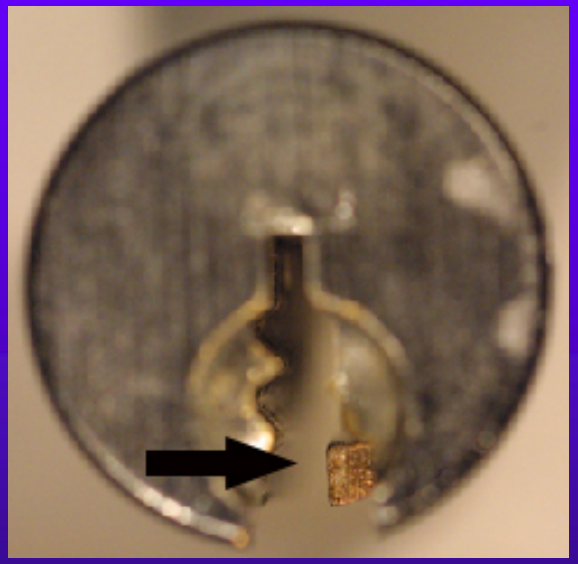
PLUG AND SIDEBAR: All pins aligned

PLUG AND SIDEBAR: Locked

MEDECO m3: The Slider (2003)

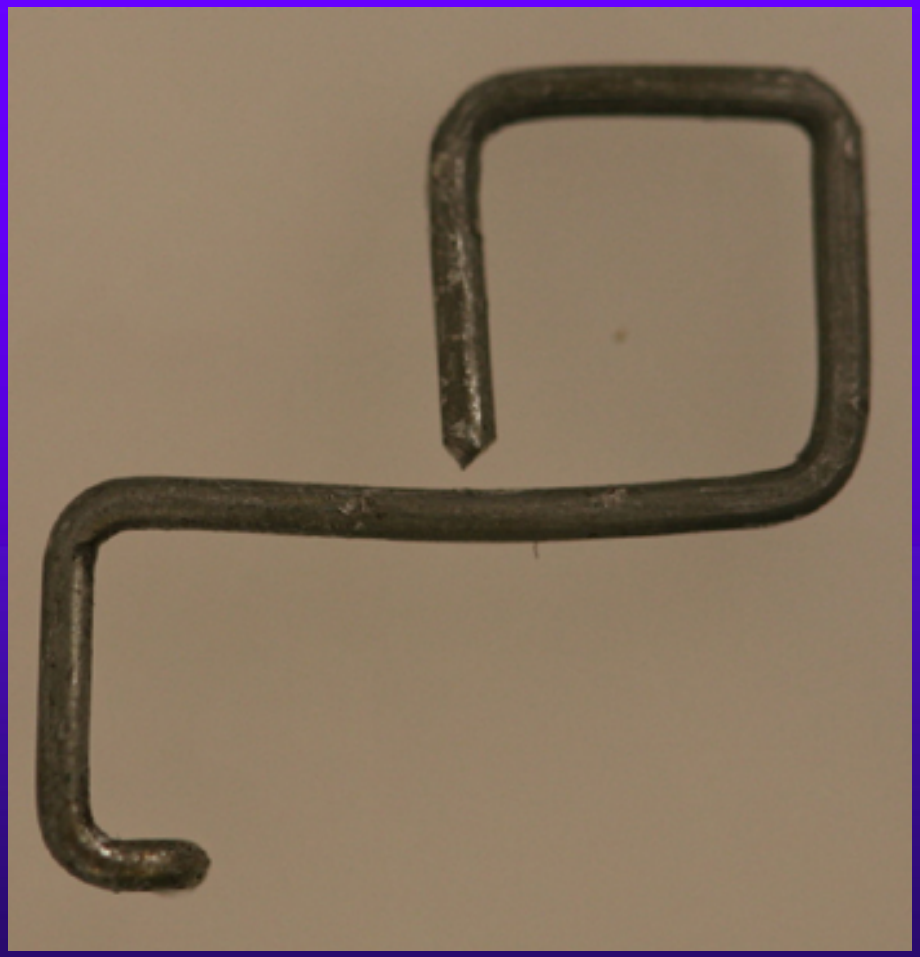






M3 SLIDER: (Not secure) Bypass with a Paper clip

SECURITY OF m3: High Tech Wire!



MEDECO RESEARCH: WHAT WE DID

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

MEDECO INSECURITY: Real World Threats - Covert

- PICKING AND BUMPING
  - With correct blank and sidebar code
  - With simulated blank
  - With or without ARX pins
- INSIDE ATTACKS
  - Change key picking
  - Keymail
- MASTER KEY ATTACKS
- VISUAL DECODING

MEDECO INSECURITY: Real World Threats – Forced

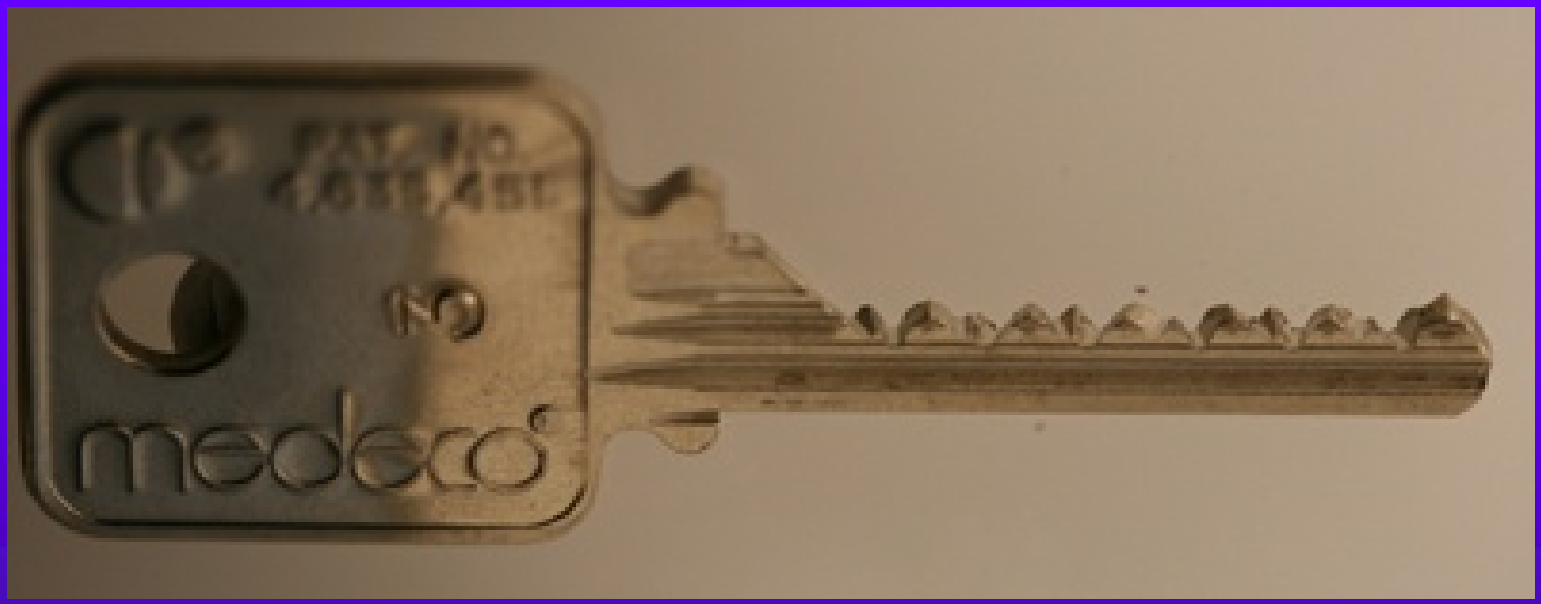
- DEADBOLT Pre-12/2007
  - Thirty seconds
  - Complete circumvention of security
  - Simple tools, easy to accomplish
- DEADBOLT 2008
  - Reverse picking attack
- MORTISE, RIM, ICORE
  - Hybrid attack, compromise of key control

MEDECO INSECURITY: Real World Threats - Keys

- VIOLATION OF KEY CONTROL and KEY SECURITY
  - Compromise of entire facility
  - Improper generation of keys
  - Use to open locks
  - Decode Top Level Master Key
  - Forced and covert entry techniques

CODE SETTING KEYS:
Four Keys to the Kingdom

MEDECO BUMP KEY



REAL WORLD ATTACK: Bumping a Medeco Lock

BUMPING + 4 ARX PINS

PICKING A MEDECO LOCK

MEDECO PICKING: OPEN IN 23 SECONDS

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

MORTISE CYLINDER

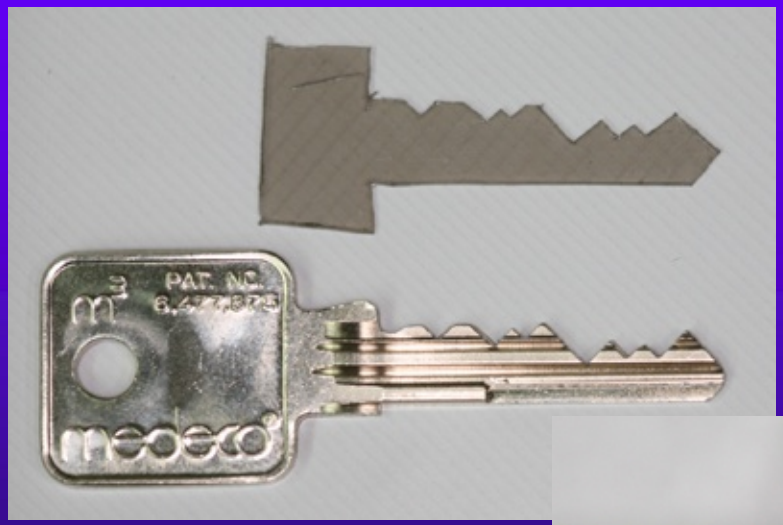
MORTISE ATTACK: Sources of Key Data

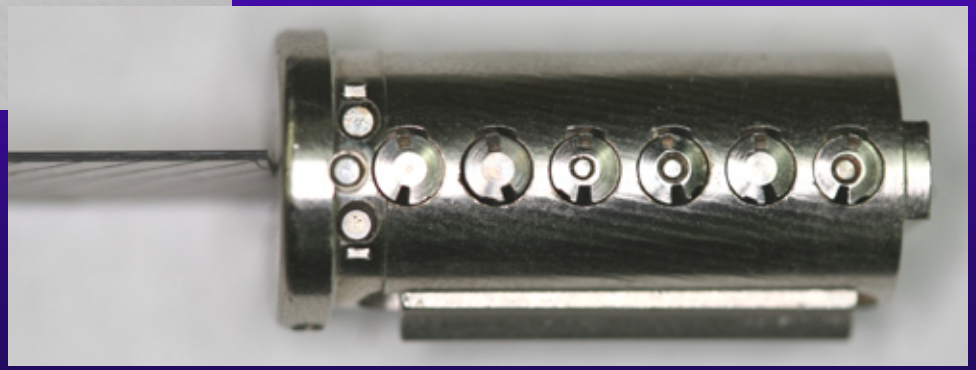
- Copy machine
- Scanner
- Cell phone camera
- Plastic sheets: Shrinky Dink
- X-acto knife

SET THE SHEAR LINE: OPEN THE LOCK

SET THE SHEAR LINE

- PLASTIC KEY SETS SHEAR LINE
- SIDEBAR IS IRRELEVANT





MORTISE ATTACK

KEYS and KEY CONTROL

- KEYS ARE THE EASIEST WAY TO OPEN LOCKS
  - Change key or master key
  - Duplicate correct bitting
  - Bump keys
  - Rights amplification: modify keys
- PROTECTION OF KEYS
  - Side bit milling: Primus and Assa
  - Interactive elements: Mul-T-Lock
  - Magnets: EVVA MCS

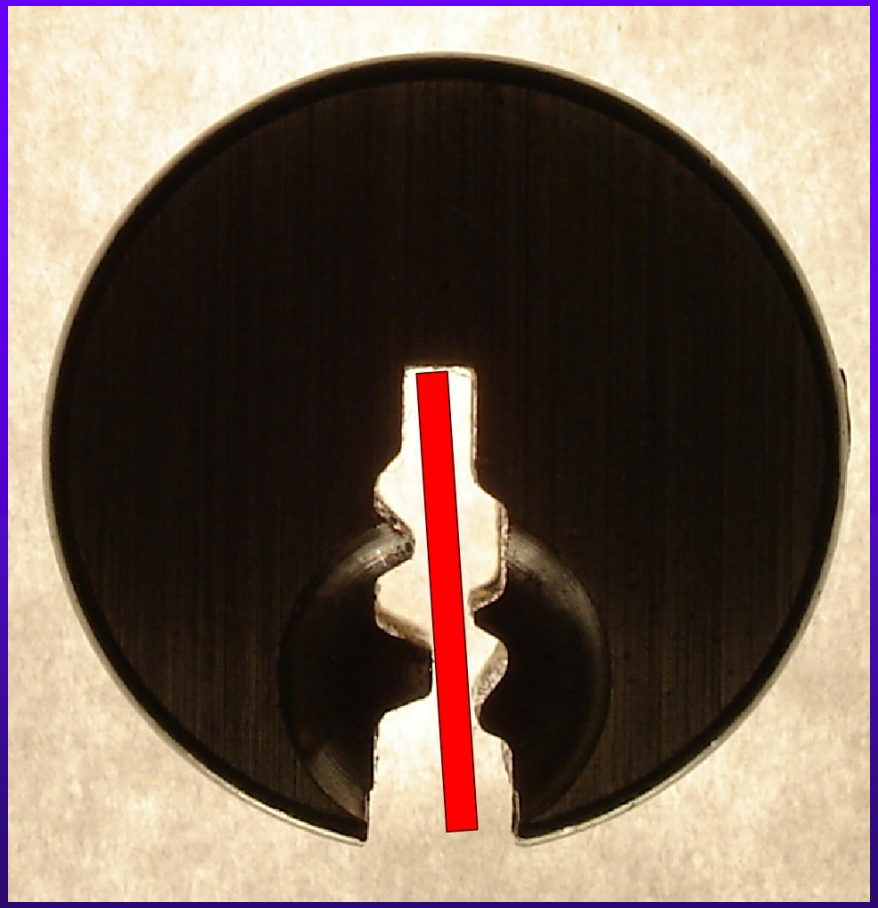
KEY CONTROL: Why Most Keys are Vulnerable

- CONVENTIONAL LOCKS: Single Layer
  - KEYWAY = KEY CONTROL
- LEGAL PROTECTION DOES NOT PREVENT REAL WORLD ATTACKS
  - KEYS = BITTING HEIGHT + KEYWAY
  - Bypass the keyway
  - Raise pins to shear line

MEDECO KEY SECURITY: The Problem

- CIRCUMVENTING SECURITY LAYERS
  - Keyways can be bypassed
  - Blanks can be simulated
  - Sidebar codes are simulated
  - Slider can be bypassed
- NO REAL LEGAL PROTECTION EXCEPT FOR M3 STEP

SIMULATED BLANKS: Any m3 and Many Biaxial Locks



SIMULATED BLANKS

COMPROMISE THE SYSTEM: Obtaining the Critical Data

- TECHNIQUES TO OBTAIN KEY DATA
  - Impressioning methods
  - Decoding: visual and Key Gauges
  - Photograph
  - Scan keys
  - Copy machine

"KEYMAIL": The New Security Threat from Within

- NEW AND DANGEROUS THREAT
- THE NEW MULTI-FUNCTION COPIER
  - It scans, copies, prints, and allows the production of MEDECO keys
- DUPLICATE COMPETE KEY
  - Open the lock
- DUPLICATE BITTING
  - Hybrid attack

KEYMAIL: How It Works for Mortise, IC, and Rim Cylinders

- ACCESS TO THE TARGET KEY
- CAPTURE AN IMAGE
- PRINT THE IMAGE
- PRODUCE A KEY
- OPEN THE LOCK

PLASTIC KEYS: PROCEDURE

- OBTAIN IMAGE OF THE KEY
  - Scan, copy, or photograph a Medeco key
  - Email and print the image remotely
  - Print 1:1 image on paper or plastic Shrinky Dinks
  - Trace onto plastic or cut out the key bitting
- INSERT KEY INTO PLUG
  - Neutralize three layers of security
  - Produce working key
  - Open Mortise, Rim, IC cylinders

ACCESS TO TARGET KEY

- BORROW BRIEFLY
- AUTHORIZED POSSESSION
- AUTHORIZED USE
- COLLUSION WITH EMPLOYEE WHO HAS ACCESS TO A KEY
- PARKING VALET

CAPTURE AN IMAGE

- COPIER
- TRACE THE KEY
- CELL PHONE CAMERA
- SCANNER

OBTAIN DATA - COPIER

OBTAIN DATA

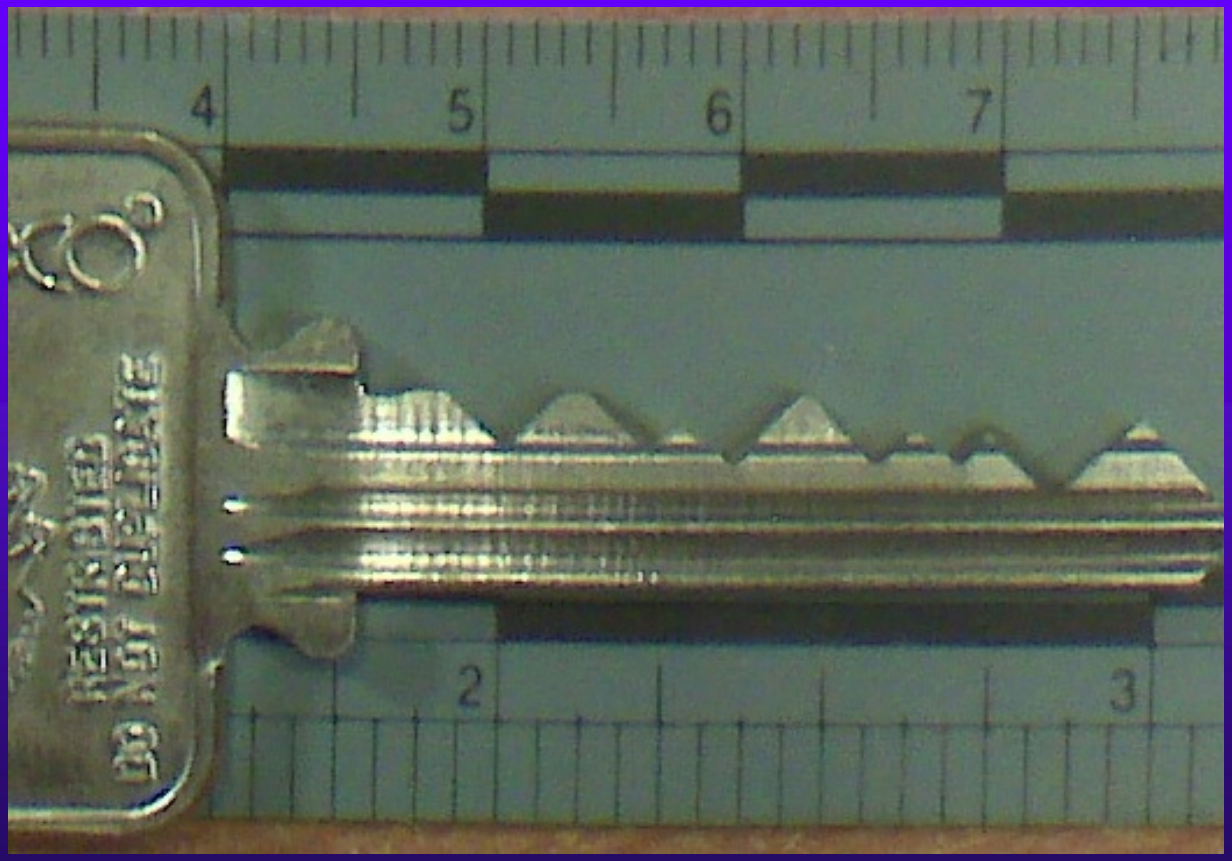
- SCANNER

OBTAIN DATA

- CELL PHONE

BLACKBERRY CURVE

- CAPTURED IMAGE



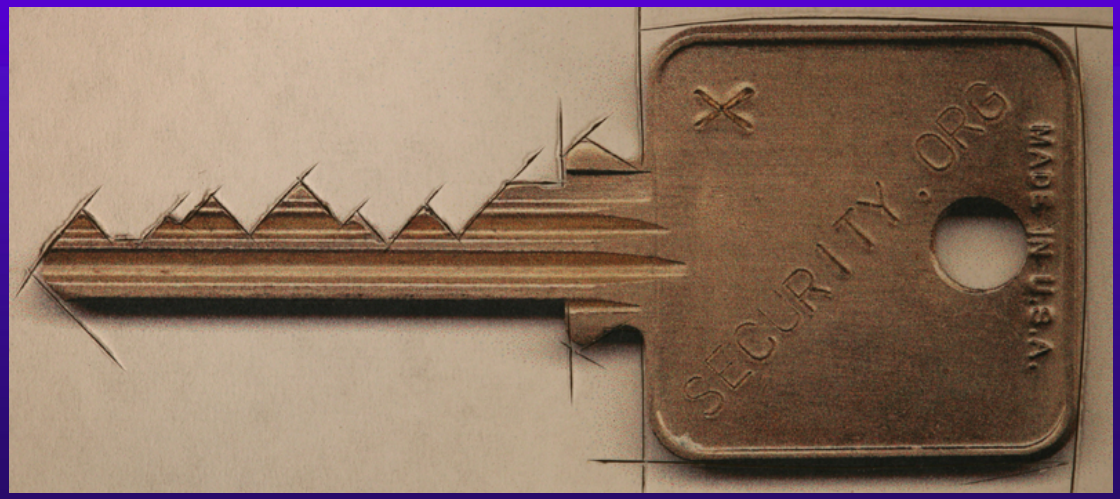
RESULTING IMAGE

- REPRODUCE THE IMAGE
  - On Paper
  - On plastic sheet
  - On Adhesive Labels
  - On Shrinky dinks® plastic
  - On a piece of copper wire
  - On a simulated metal key
  - On plastic credit card

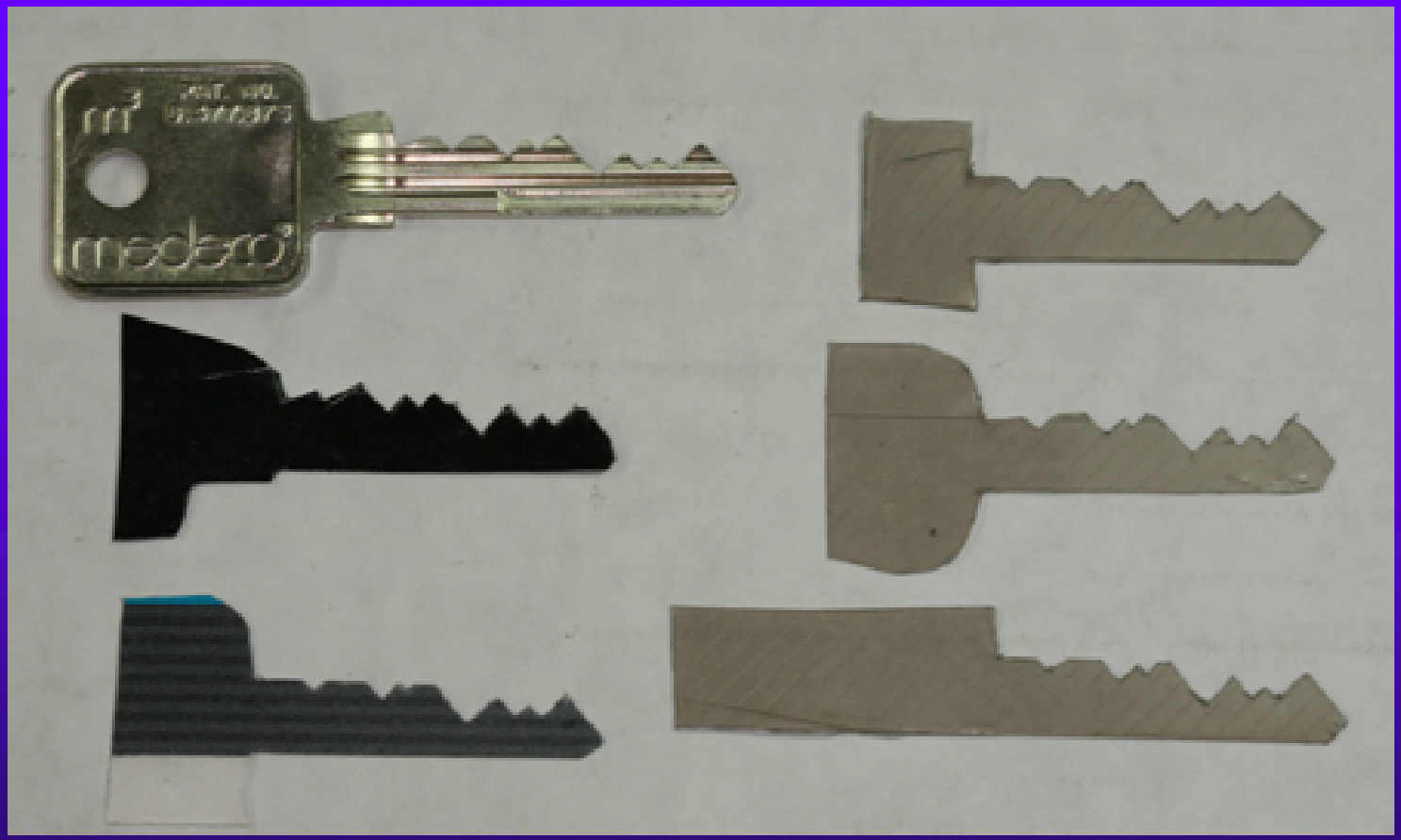
PRINT IMAGE ON PLASTIC OR PAPER

CUT A FACSIMILE OF KEY

- KEY REQUIREMENTS
  - Vertical bitting only
  - No sidebar data
  - No slider data



SET THE SHEAR LINE



OPEN THE LOCK: Replicate the Key in Plastic

- MEDECO TAKES PLASTIC!

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

MECHANICAL LOCKS: NOT ENOUGH PROTECTION

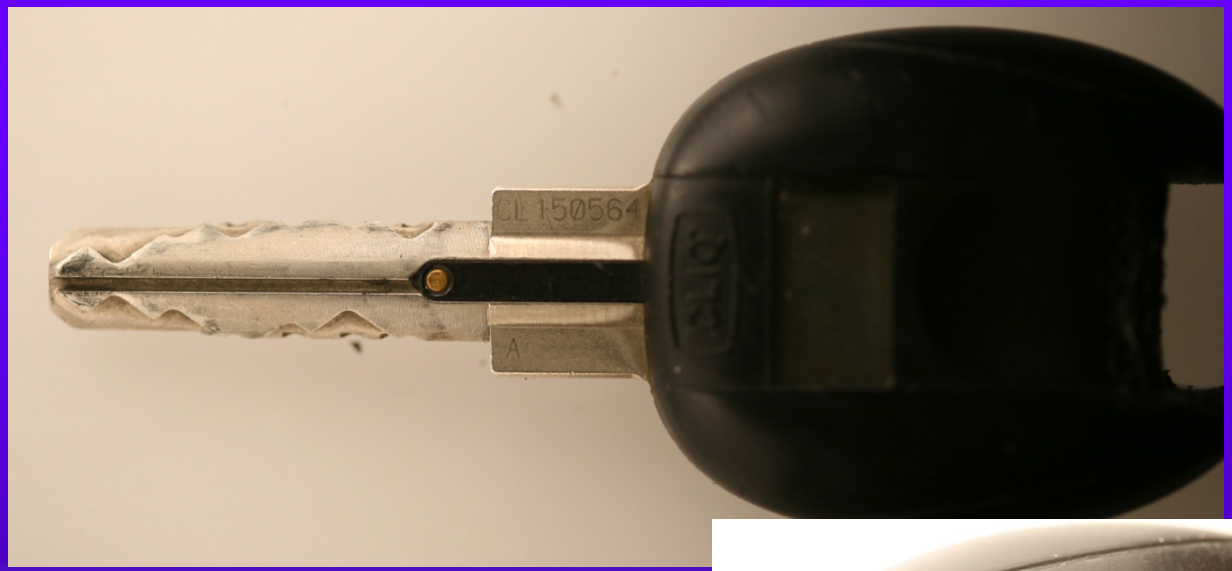
- GOOD FOR ONE PERSON, ONE KEY
- WHERE DON'T NEED TRACKING
- ADD DELETE KEYS NOT AN ISSUE
- LOST KEYS
- COPIED OR STOLEN KEYS

ELECTRONIC ACCESS CONTROL: THE NEW SOLUTION

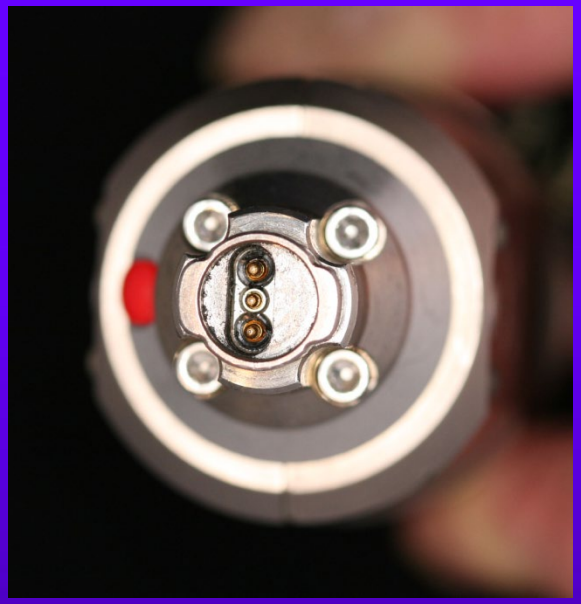
- THE ANSWER TO MECHANICAL LOCKS?
- CURRENT SYSTEMS
  - MECHANICAL + ELECTRONIC
  - ALL ELECTRONIC
    - WIRED
    - DATA ON CARD
    - WIRELESS

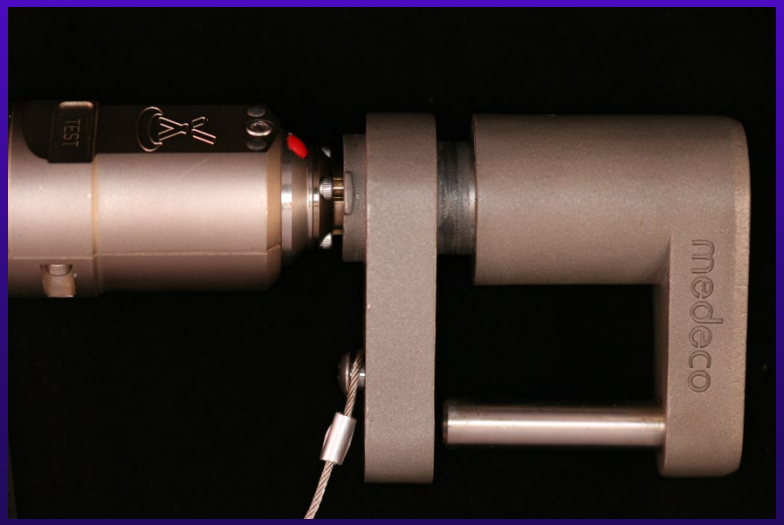
LOGIC CYLINDER

MEDECO LOGIC

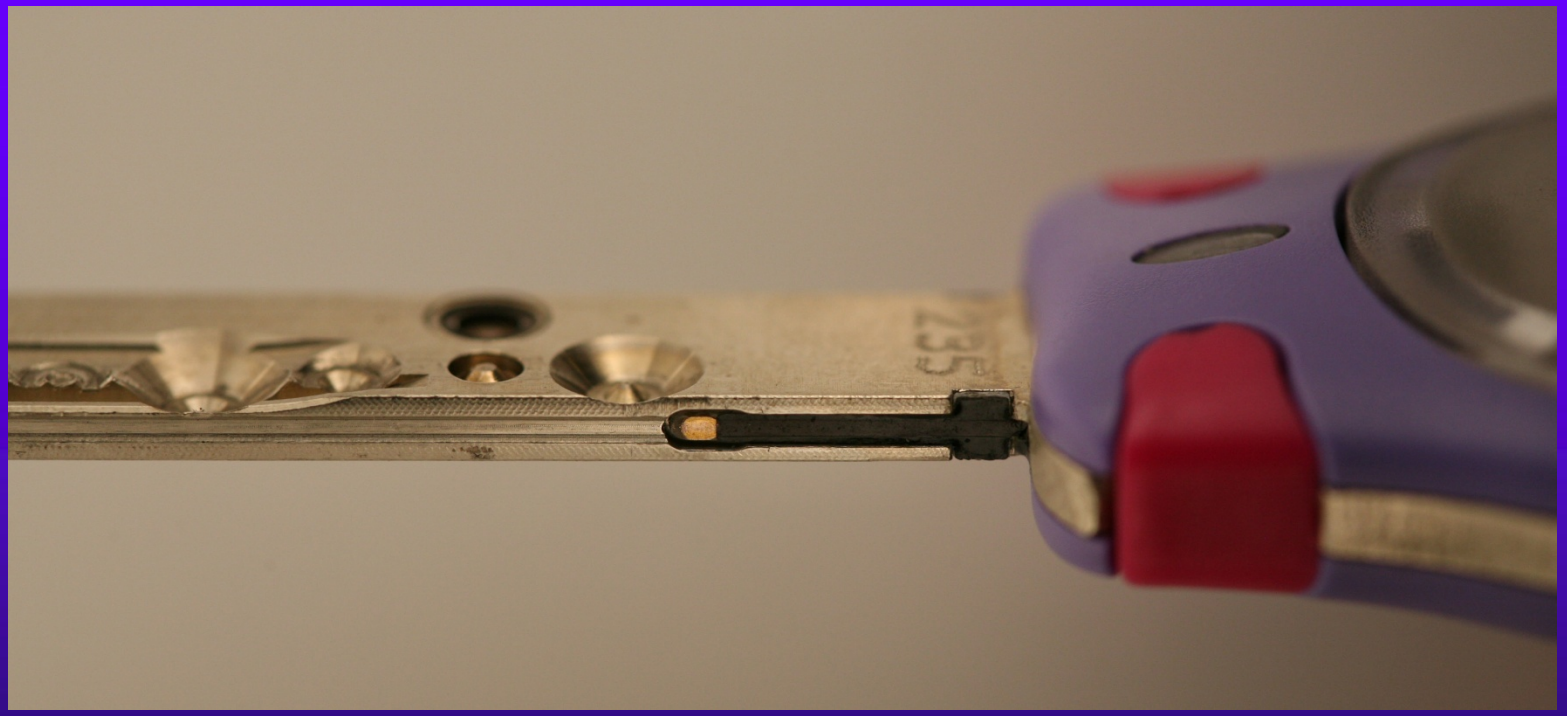


MEDECO NEXGEN





MUL-T-LOCK CLIQ



POTENTIAL SECURITY VULNERABILITIES?

- BYPASS OF MECHANICAL OR ELECTRONIC SYSTEM
- AUDIT TRAIL DEPENDS ON READING THE KEY
- WHAT IF ONE LAYER IS BYPASSED

ELECTRONIC ACCESS CONTROL: SERIOUS ISSUES

- FALSE SENSE OF SECURITY
- FALSE BLAME OF EMPLOYEES
- NO EVIDENCE OF ENTRY FOR SECRET INFORMATION
- SECRETS COMPROMISED
- FALSE SENSE OF SECURITY
- EVIDENCE: CHAIN OF CUSTODY

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

www.security.org

mwtobias@security.org