



MEDECO “VIRTUALLY RESISTANT” SECURITY

A Case Study in Real World

Security Vulnerabilities and Liability



LOCKS AND LIABILITY: WHY IMPORTANT

- ◆ PROTECTION OF ASSETS,
INFORMATION, PEOPLE
- ◆ PREVENT LOSSES
- ◆ UNAUTHORIZED ACCESS
- ◆ STATUTORY REQUIREMENTS
- ◆ STANDARDS: MINIMAL PROTECTION
- ◆ BYPASS OF LOCKS
- ◆ ELECTRONIC ACCESS CONTROL



MEDECO: One of the Most Secure Locks in America?

- ◆ FORTY YEARS: THE LEADER
- ◆ FIRST LINE OF PROTECTION
- ◆ CRITICAL INFRASTRUCTURE
- ◆ LEGAL REQUIREMENTS
- ◆ HIGHEST SECURITY RATINGS
 - UL 437 and BHMA/ANSI 156.30



MEDECO CASE STUDY: WHY IMPORTANT

◆ CONCEPT OF SECURITY

- Medeco locks are good, but not for everybody

◆ STANDARDS DO NOT PROTECT YOU

◆ CORPORATE ARROGANCE

- Medeco cannot open their own locks
- “Nobody else understands their locks”

◆ CAMPAIGN OF DISINFORMATION

- Misrepresentations, obfuscation, and misstatements



MEDECO: LESSONS LEARNED

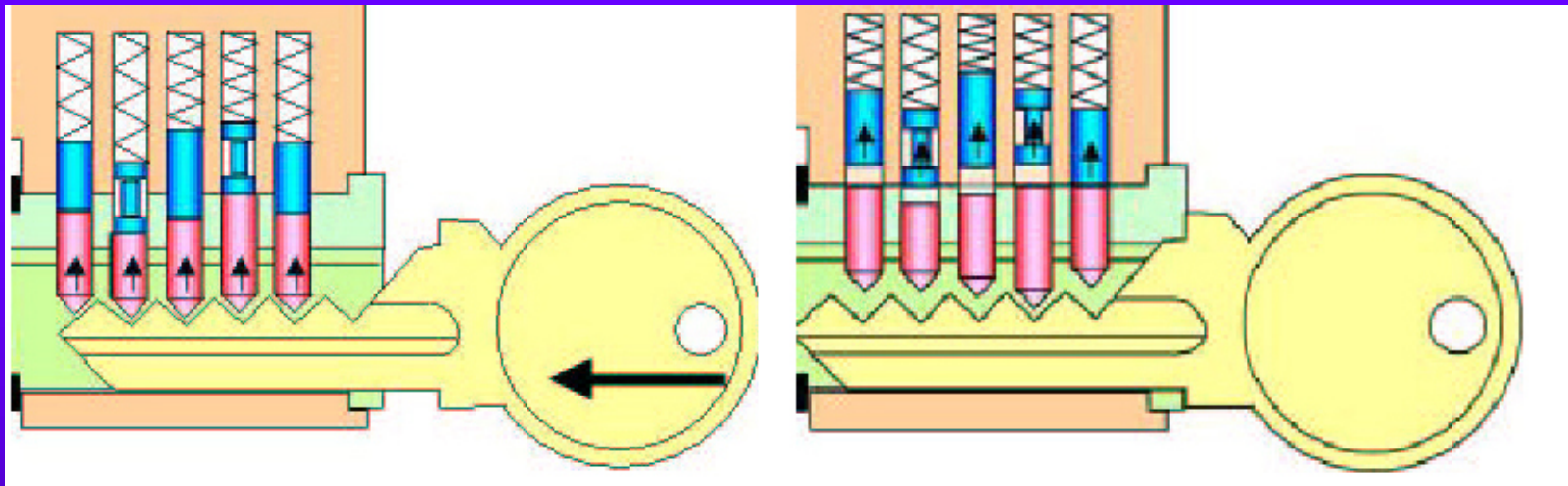
- ◆ PATENTS DO NOT MEAN ANYTHING
- ◆ STANDARDS: LIMITED VALUE
- ◆ SOME MANUFACTURERS WILL NOT TELL THE TRUTH OR DO NOT KNOW
- ◆ KEY CONTROL: THE MYTH
- ◆ SECURITY OF MECHANICAL LOCKS
- ◆ ELECTRONIC ACCESS CONTROL SECURITY ISSUES



LOCK BUMPING: WHERE IT ALL STARTED


- ◆ AUGUST 2006: JENNALYNN
 - Bumps a Kwikset pin tumbler lock
- ◆ AUGUST 2007: JENNALYNN
 - Bumps a Medeco Biaxial lock
- ◆ JUNE, 2008: OPEN IN THIRTY SECONDS
- ◆ AUGUST, 2008: JENNALYNN
 - Bumps a Medeco with ARX pins

LOCK BUMPING THEORY



JENNALYNN, AGE 11: OPENS KWIKSET





LOCK BUMPING: 2006

A SERIOUS THREAT

- ◆ INTRODUCED LOCK BUMPING
 - JennaLynn opens a Kwikset
- ◆ KNOWN TECHNIQUE: 1925
 - Refined in 2004 in Europe
- ◆ ALOA: NOT A PROBLEM
- ◆ MEDECO: BUMP-PROOF LOCKS
- ◆ POSTAL INSPECTION SERVICE
- ◆ CONVENTIONAL LOCKS AFFECTED



WHY BUMPING IMPORTANT

- ◆ EXPOSED VULNERABILITY TO 95% OF PIN TUMBLER LOCKS
- ◆ PUBLIC AWARENESS
- ◆ LEGAL NOTICE AND LIABILITY
- ◆ HIGH SECURITY LOCKS
 - Manufacturers said locks were secure
 - Our locks are bump-proof
 - Assa Abloy Companies: “Smoke and mirrors”



BUMPING AND SECURITY

- ◆ NEED TO UNDERSTAND PROBLEM
- ◆ PROPERLY ASSESS SECURITY
- ◆ RESULTED IN BYPASS OF HIGH SECURITY LOCKS
 - MEDECO, MUL-T-LOCK, ASSA, OTHERS
- ◆ LEGAL LIABILITIES AND STATUTORY MANDATES FOR SECURITY



WHAT IS HIGH SECURITY: QUESTIONS TO ASK

- ◆ DO I HAVE HIGH SECURITY LOCKS
- ◆ DO I NEED HIGH SECURITY LOCKS
- ◆ CAN HIGH SECURITY LOCKS BE COMPROMISED
- ◆ WHAT CONSTITUTES A THREAT AND HOW DO LOCKS PROTECT MY FACILITY
- ◆ WILL ELECTRONIC ACCESS CONTROL BE SUFFICIENT



HIGH SECURITY LOCKS: A REVIEW

- ◆ SPECIFY FOR FACILITY PROTECTION
 - COVERT ENTRY
 - FORCED ENTRY
 - KEY CONTROL
- ◆ MINIMUM SECURITY CRITERIA
 - MINIMUM ATTACK TIMES
 - RESISTANCE TO CERTAIN FORMS OF ENTRY
 - UL 437 and BHMA/ANSI 156.30



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



COVERT ENTRY OF MEDECO LOCKS: RESULT

◆ BUMPING

- Modified change key
- Simulated key

◆ PICKING

- With change key
- With code setting keys

◆ EXTRAPOLATE TMK

◆ DECODE BILEVEL SYSTEM TO COMPROMISE m3 SYSTEM



MEDECO INSECURITY: Real World Threats - Covert

- ◆ FOUR KEYS TO PICK AND BUMP PRE-12/07 LOCKS
- ◆ SIXTEEN OR LESS KEYS FOR 2008 LOCKS
- ◆ PICKING IN AS LITTLE AS 27 SECONDS
 - Using any change key on same sidebar code
 - With code setting keys
 - Angle setting keys
 - ARX pins



MEDECO INSECURITY: Real World Threats - Covert

◆ BUMPING

- With correct blank and sidebar code
- With simulated blank
- With or without ARX pins

BUMPING MEDECO LOCKS





FORCED ENTRY PROTECTION: Theory

- ◆ LOCKS ARE SECURE AGAINST FORCED METHODS OF ATTACK
- ◆ MINIMUM TIMES SPECIFIED IN UL 437 and BHMA/ANSI 156.30
- ◆ ATTACK RESISTANCE: 5 MINUTES



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
 - Compromise of Top Level Master Key



MEDECO INSECURITY: The Threat from Within

- ◆ COMPROMISE OF KEY CONTROL + HYBRID ATTACK
 - Mortise, Rim, Interchangeable cores
- ◆ MEDECO KEY CONTROL v. CONVENTIONAL KEYS
 - Conventional keys = 1 layer of security
 - Medeco keys = 3 layers of security
 - Electronic Access Control issues: two levels of security



MEDECO INSECURITY:

The Threat from Within

- ◆ OBTAIN KEY DATA TO OPEN LOCKS BY HYBRID ATTACK
- ◆ KEY CONTROL IS CIRCUMVENTED
- ◆ BRIEF ACCESS TO A KEY FOR A TARGET LOCK
 - Compromise of the lock or system
 - By insiders
 - By criminals outside of an organization



MEDECO KEY CONTROL:

Appearance v. Reality

- ◆ WHAT IS IT SUPPOSED TO MEAN?
- ◆ ARE THE STANDARDS SUFFICIENT?
- ◆ REAL WORLD VULNERABILITIES
- ◆ IS ELECTRONIC ACCESS CONTROL ANY MORE SECURE?



KEY CONTROL: The Theory

- ◆ PROTECTION OF BLANKS OR CUT KEYS FROM ACQUISITION OR USE:
 - Unauthorized duplication
 - Unauthorized replication
 - Unauthorized simulation
 - restricted keyways
 - proprietary keyways
 - sectional keyways



KEYS and KEY CONTROL

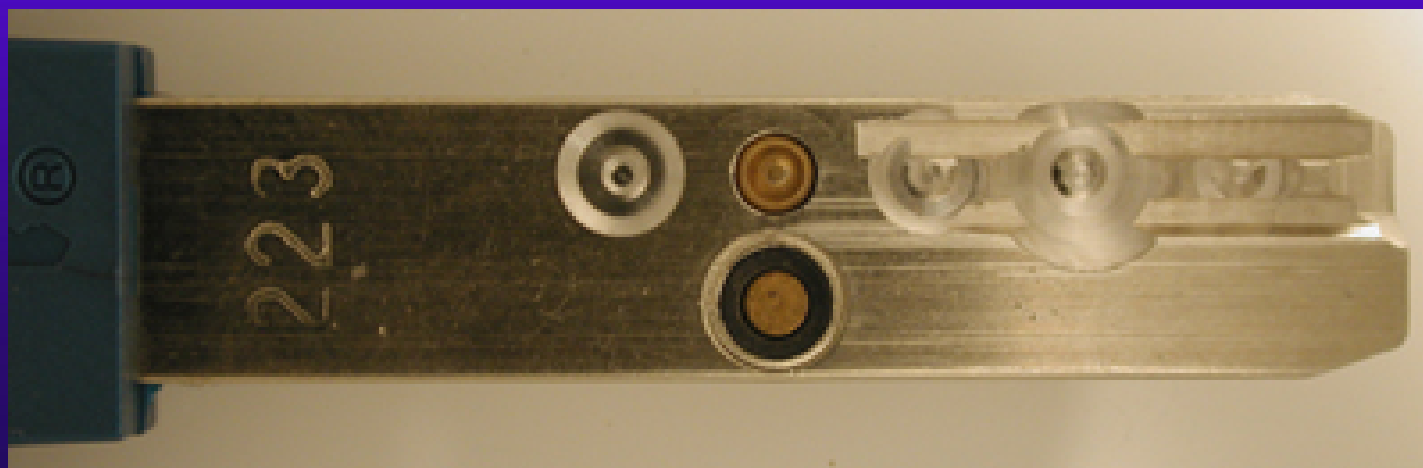
◆ KEYS ARE THE EASIEST WAY TO OPEN LOCKS

- Change key or master key
- Duplicate correct bitting
- Bump keys
- Rights amplification: modify keys

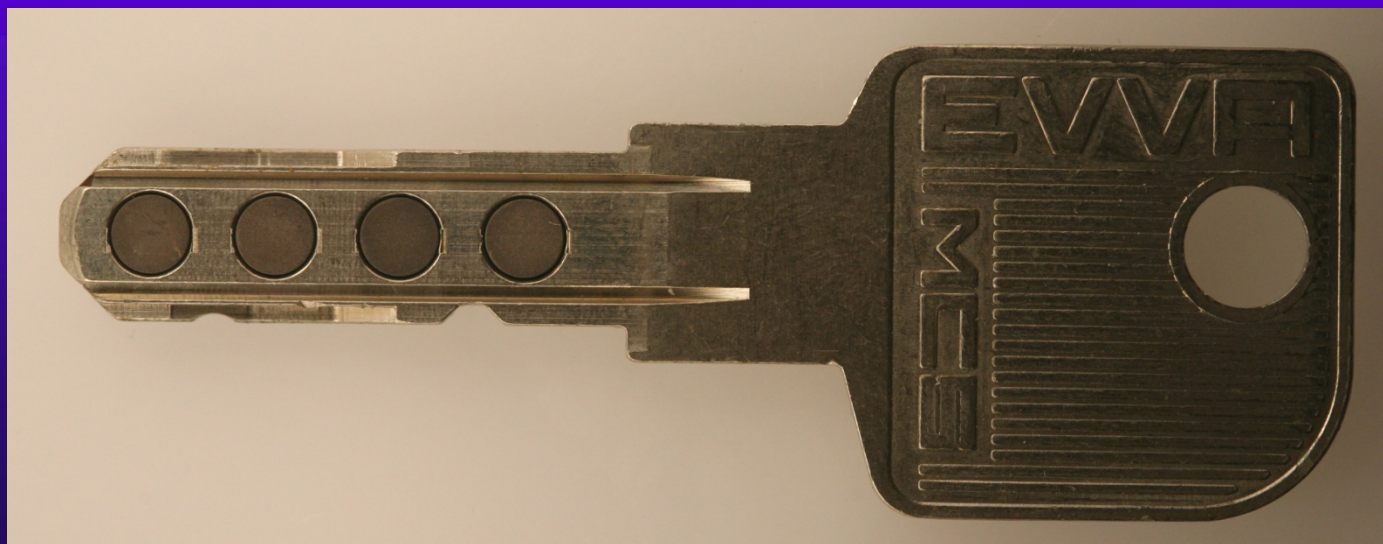
◆ PROTECTION OF KEYS

- Side bit milling: Primus and Assa
- Interactive elements: Mul-T-Lock
- Magnets: EVVA MCS

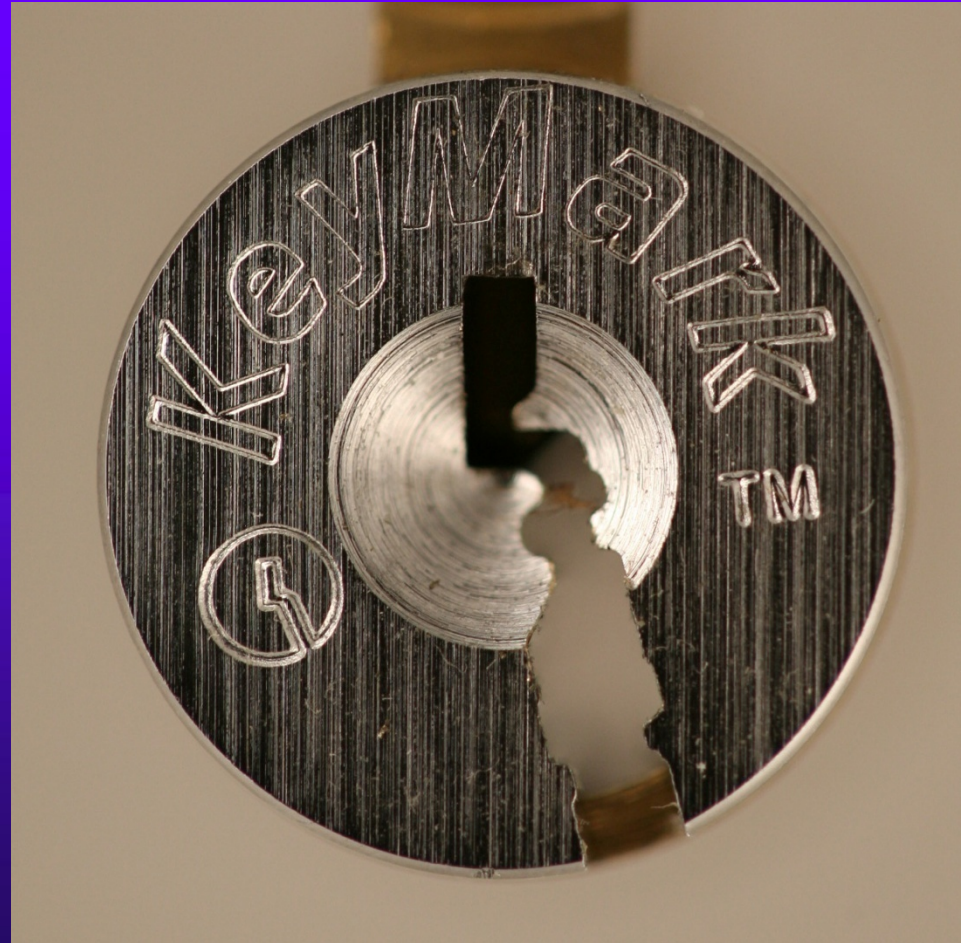
PROTECTION OF KEYS



PROTECTION OF KEYS



MEDECO KEYMARK: ABSOLUTE KEY CONTROL!



MEDECO KEYMARK X4



KEYMARK TAKES PLASTIC





SECURITY THREAT:

Failure of Key Control: Duplicate

- ◆ IMPROPER ACQUISITION OR USE OF KEYS BY EMPLOYEES OR CRIMINALS
- ◆ Unauthorized access to facilities or areas
- ◆ Bump keys
- ◆ Use for rights amplification
- ◆ Compromise master key systems

KWIKSET: CONVENTIONAL LOCKS AND KEYS





SECURITY THREAT:

Failure of Key Control: Replicate

- ◆ HIGH SECURITY LOCKS AND KEYS
 - Designed to prevent replication
- ◆ REPLICATION TECHNIQUES
- ◆ EASY ENTRY MILLING MACHINE
- ◆ SILICON CASTING
- ◆ PLASTIC AND EPOXY

SECURITY THREAT:

Failure of Key Control: Simulate

◆ M3 KEYWAY

- Wider than Biaxial
- No paracentric keyway

◆ COMPONENTS OF MEDECO KEYS

- Ward pattern and paracentric keyway
- Bitting
- M3 Slider

◆ SECURITY THREAT

- Bypass wards in paracentric keyway
- Create new blanks





RESULT: Failure of Key Control

- ◆ Restricted and proprietary keyways
- ◆ M3 Slider: bypass with paper clip
- ◆ Sabotage potential
- ◆ Make keys to open your locks
- ◆ Duplicate from codes or pictures
- ◆ TMK extrapolation
- ◆ Set the sidebar code

DUPLICATING MEDECO



KEYS AND FORCED ENTRY





COMPROMISE THE SYSTEM: Obtaining the Critical Data

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

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 CONTROL: Virtually Impossible to Copy

- ◆ “If there is no key control, then it does not matter what security enhancements are in the lock”





MEDECO KEY CONTROL: 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

MORTISE, RIM, IC: A Special Form of Attack

- ◆ HYBRID ATTACK
- ◆ Will damage the lock
- ◆ Entry in ten seconds
- ◆ Millions of Locks affected





“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



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 Dink
- Trace onto plastic or cut out the key bitting

◆ INSERT KEY INTO PLUG

- Neutralize three layers of security
- Open Mortise, Rim, IC cylinders



ACCESS TO TARGET KEY

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



CAPTURE AN IMAGE

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

OBTAIN DATA - COPIER



OBTAIN DATA

◆ SCANNER



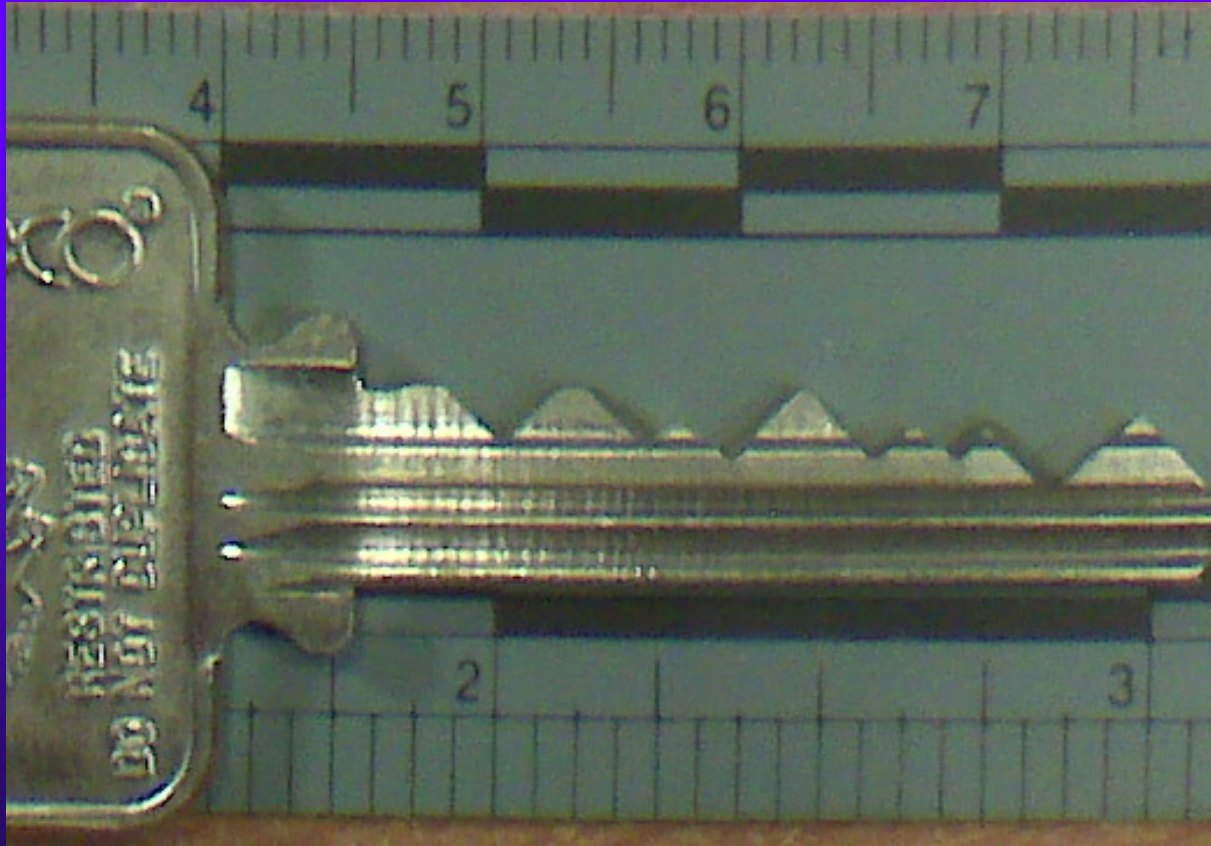
OBTAIN DATA

◆ CELL PHONE



BLACKBERRY CURVE

◆ CAPTURED IMAGE





RESULTING IMAGE

◆ REPRODUCE THE IMAGE

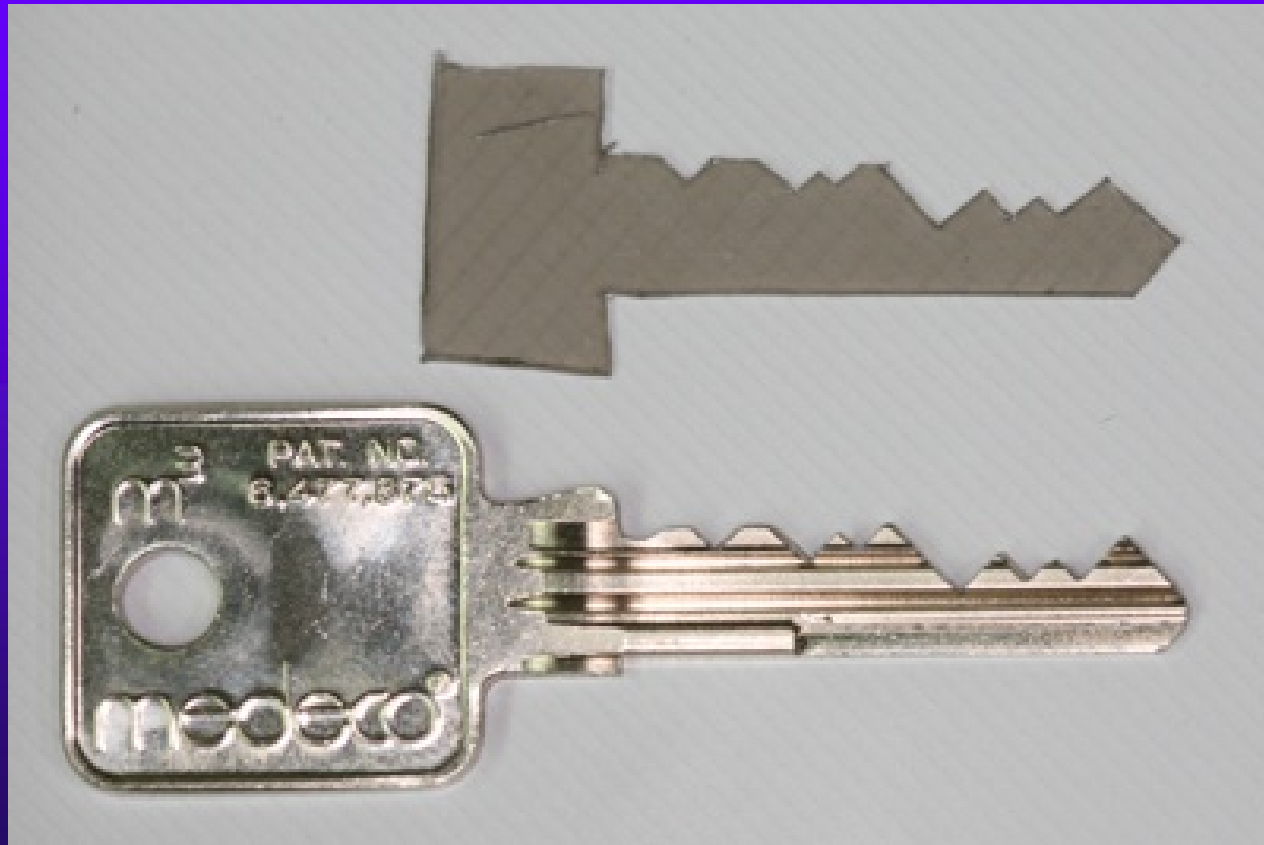
- On Paper
- On plastic sheet
- On Adhesive Labels
- On Shrinky dinks® plastic
- On a piece of copper wire
- On a simulated metal key

PRINT IMAGE ON PLASTIC OR PAPER

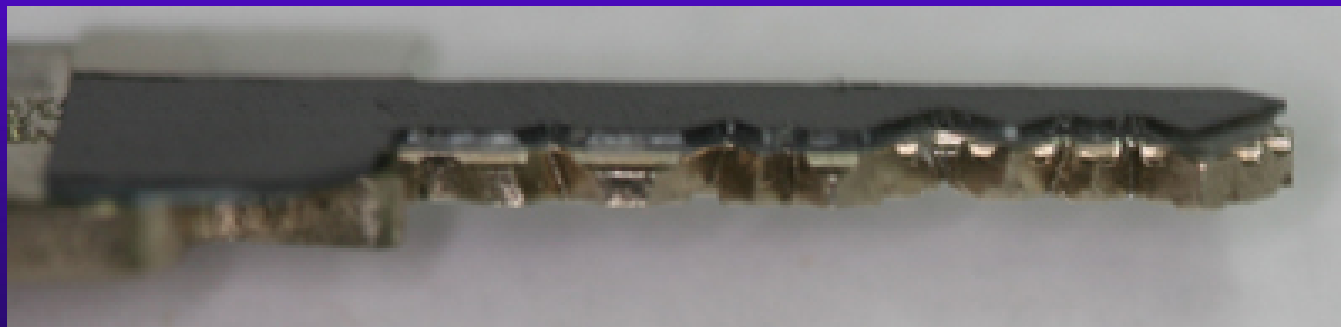
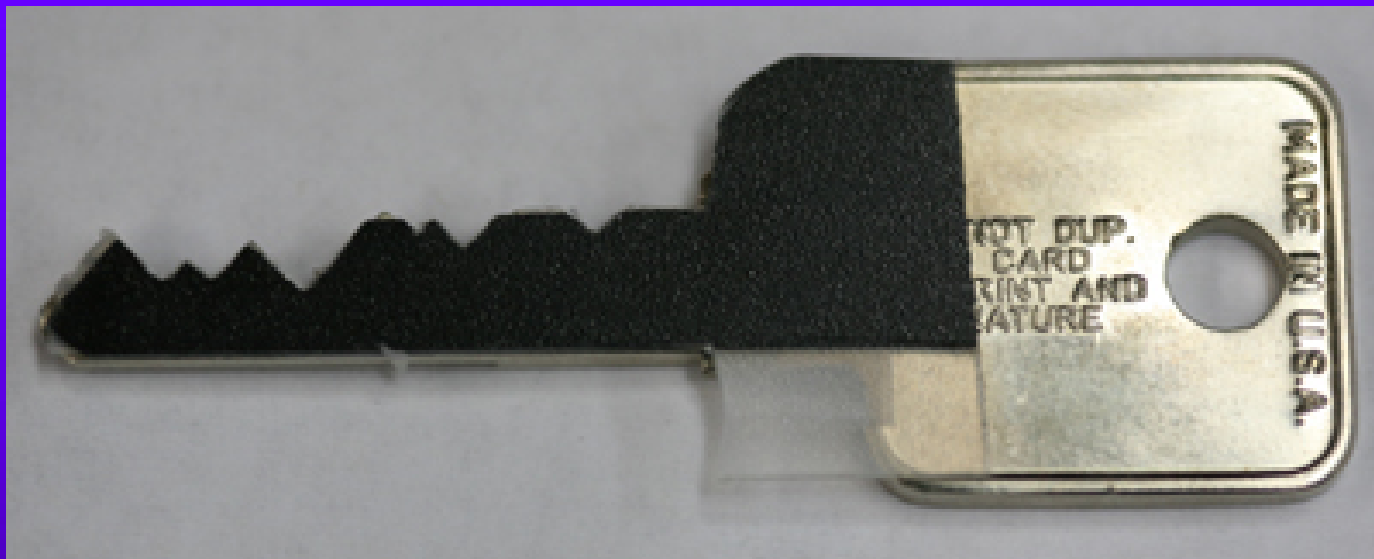


SET THE SHEAR LINE

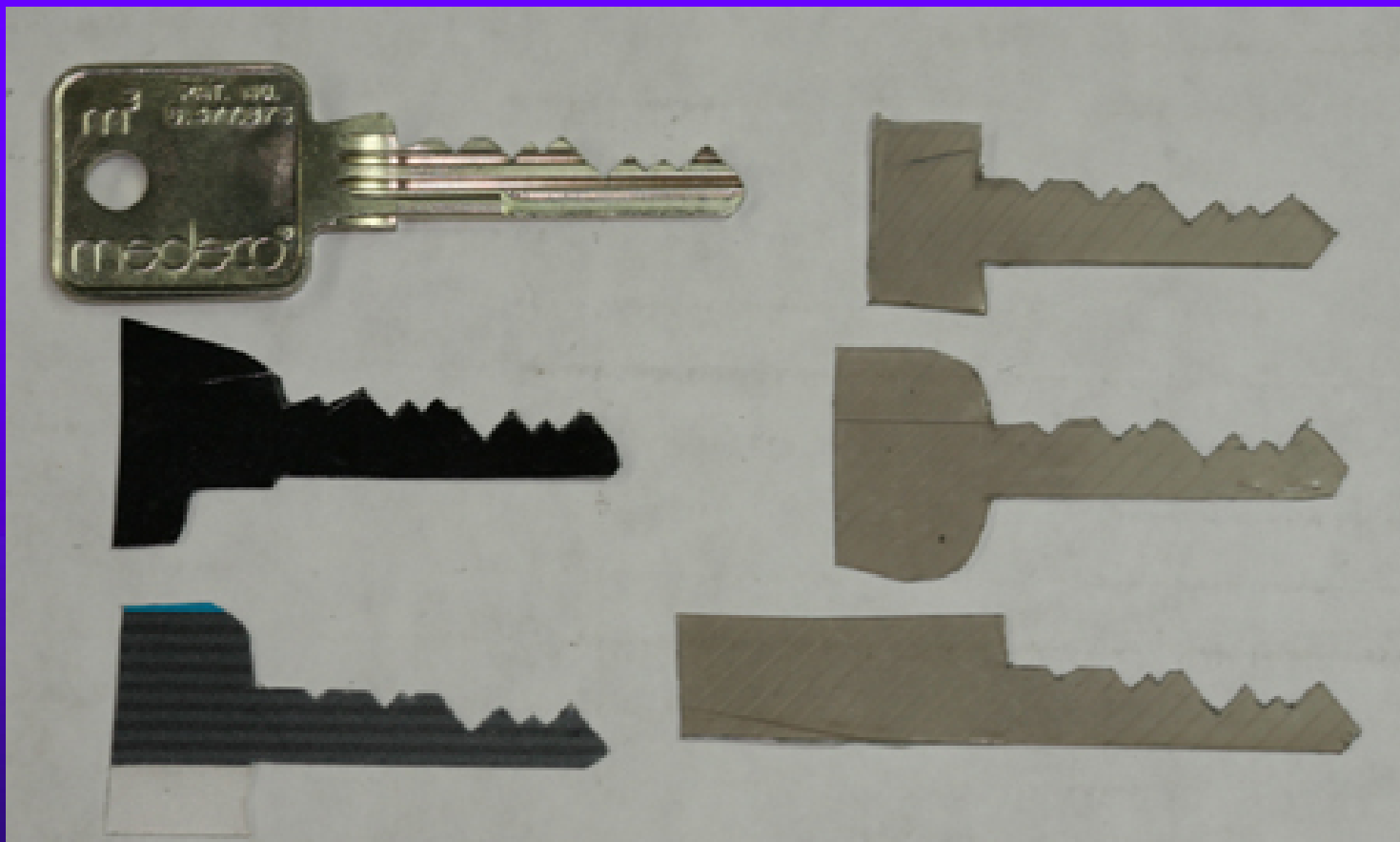
- ◆ PLASTIC KEY SETS SHEAR LINE



SET THE SHEAR LINE



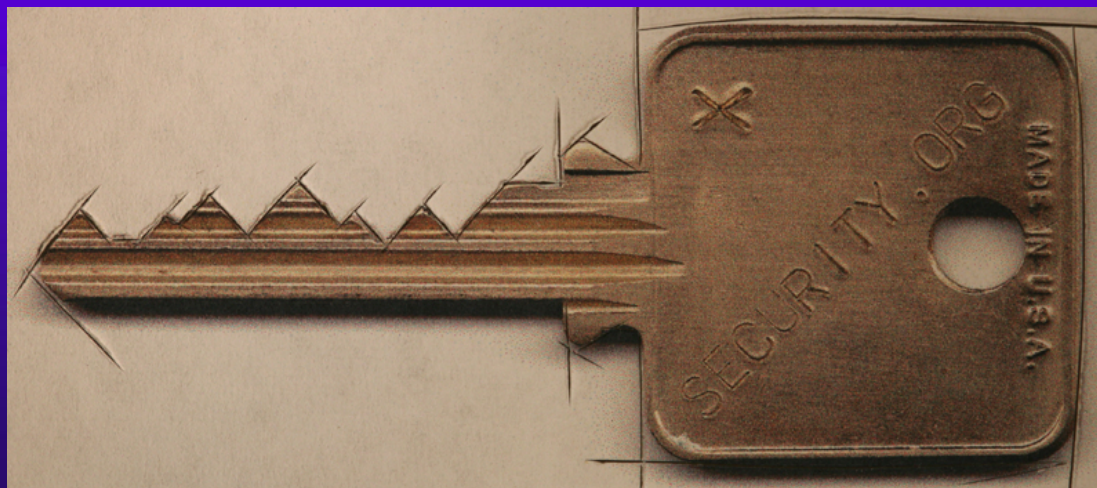
SET THE SHEAR LINE



CUT A FACSIMILE OF KEY

◆ KEY REQUIREMENTS

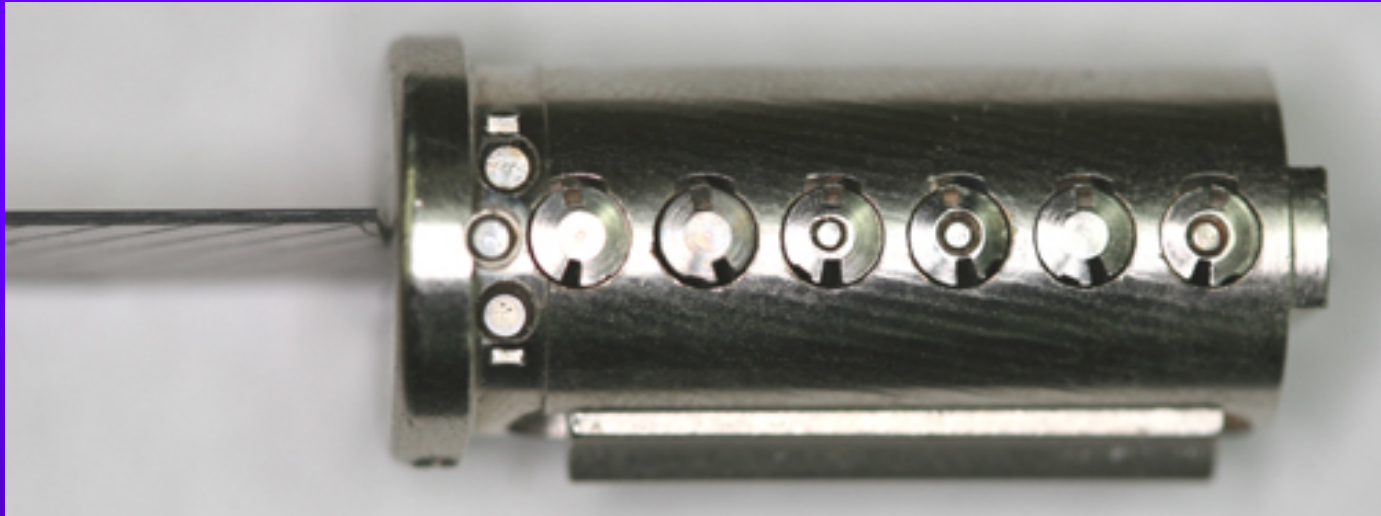
- Vertical biting only
- No sidebar data
- No slider data




SET THE SHEAR LINE: OPEN THE LOCK



NEUTRALIZE SHEAR LINE





HIGH SECURITY LOCK MANUFACTURERS

- ◆ LEGAL RESPONSIBILITY
- ◆ ETHICAL RESPONSIBILITY
 - NOTIFY OF VULNERABILITIES
 - PROPER PRODUCT DESIGNS
 - FIX PROBLEMS



LOCKS, LIES, AND VIDEOTAPE: MEDECO CASE STUDY

◆ LOCK BUMPING: WHERE IT BEGAN

◆ MEDECO CASE STUDY

- Medeco security: “Our locks are bump-proof, virtually bump-proof, and Virtually Resistant”
- We Never claimed our Locks were bump-proof!
- Our deadbolts are secure, no problem!
- We have spent hundreds of hours and cannot replicate any of the Tobias attacks!



MEDECO BUMPING CLAIM: “We never said it: Others did!”

◆ WHAT IS THE TRUTH?

- August 4, 2006 press release: “Bump-proof”
- 2007 - Retroactively changed the language: “Virtually Bump-proof”
- The Medeco Problem: **www.archive.org**

- ◆ TV, Advertising, DVD, Medeco website
- ◆ The Smoking Gun: August 12, 2006



WE NEVER SAID OUR LOCKS WERE BUMP-PROOF

- ◆ AUGUST 15, 2006
- ◆ U.S. Patent and Trademark Office filing by Medeco Security Locks, Inc. lawyer G. Franklin Rothwell, Application 78952460
- ◆ Word mark: BUMP PROOF
- ◆ Abandoned: February 9, 2007



BUMP PROOF: USPTO FILING FOR THE WORD MARK

BUMP PROOF

Word Mark	BUMP PROOF
Goods and Services	(ABANDONED) IC 006. US 002 012 013 014 023 025 050. G & S: CYLINDER LOCKS OF METAL AND KEYS THEREFOR
Standard Characters Claimed	
Mark Drawing Code	(4) STANDARD CHARACTER MARK
Serial Number	78952460
Filing Date	August 15, 2006
Current Filing Basis	1B
Original Filing Basis	1B
Owner	(APPLICANT) Medeco Security Locks, Inc. CORPORATION VIRGINIA PO Box 3075 Salem VIRGINIA 24153
Attorney of Record	G. Franklin Rothwell
Type of Mark	TRADEMARK
Register	PRINCIPAL
Live/Dead Indicator	DEAD
Abandonment Date	February 9, 2007



ABOUT CLAIMS OF PICKING MEDECO LOCKS

- ◆ NOBODY HAS PROVED THEY CAN PICK OUR LOCKS IN 40 YEARS
 - False demonstrations, special locks
 - They are lying
 - We cannot replicate anything
- ◆ THE REAL PROBLEM
 - They cannot open their own locks
 - Failure of imagination



RESPONSIBLE DISCLOSURE BY LOCK MANUFACTURERS

- ◆ KNOWLEDGE OF VULNERABILITY
- ◆ Known or suspected
- ◆ Make responsible notifications
- ◆ Let users and dealers assess risks
- ◆ Duty to tell the truth
- ◆ Duty to fix the problem



VULNERABILITIES:

Full Disclosure Required

- ◆ SECURITY BY OBSCURITY
- ◆ It does not work with Internet
- ◆ It is the User's security
- ◆ They have a right to assess their own risks
- ◆ Criminals already have information
- ◆ Disclosure: benefits outweigh risks
- ◆ Liability for failure to disclose



LESSONS LEARNED

- ◆ THE MEDECO CASE
- ◆ Nothing is impossible
- ◆ Corporate arrogance does not work
- ◆ HIGH SECURITY LOCK MAKERS
- ◆ Engineering, Security, Integrity
- ◆ Duty to tell the truth



OPEN IN THIRTY SECONDS

- ◆ © 2008 Marc Weber Tobias, Matt Fiddler
- ◆ <http://www.security.org>
- ◆ <http://in.security.org>
- ◆ mwtobias@security.org
- ◆ mjfiddler@security.org
- ◆ tbluzmanis@security.org