MEDECO “VIRTUALLY RESISTANT” SECURITY

A Case Study in Real World Security Vulnerabilities

HIGH SECURITY LOCKS

- 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

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 KIEY CONTROL and KEY SECURITY
  - Compromise of entire facility
  - Improper generation of keys

MEDECO INSECURITY: Key Control Protective Measures

- FACILITY RESTRICTIONS
  - No paper clips
  - No Copiers, scanners, cameras
  - No scissors or X-Acto knives
  - No plastic report covers
  - No Shrinky-Dink plastic
  - No printers
  - No email or Fax connections to outside world

MEDECO INSECURITY: Real World Threats - Keys

- NO KEY CONTROL OR KEY SECURITY
- All m3 and some Biaxial keyways
- Keyways (restricted and proprietary)
- M3 Step = no security
- Copy keys
- Produce any blank
- Generate Top Level Master Key
- Cut any key by code

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

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 INSECURITY: Key Control and Layers of Security

- THREE LAYERS OF SECURITY
  - Shear Line
  - Sidebar
  - Slider in m3
- HYBRID ATTACK: NEUTRALIZE EACH LAYER OF SECURITY
  - Shear line = Plastic key
  - Sidebar and Slider = Torque on plug

MEDECO KEY CONTROL: Appearance v. Reality

- WHAT IS IT SUPPOSED TO MEAN?
- ARE THE STANDARDS SUFFICIENT?
- REAL WORLD VULNERABILITIES
- [DO NOT DUPLICATE IMAGE]

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

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

SECURITY THREAT: Failure of Key Control: Replicate

- HIGH SECURITY LOCKS AND KEYS
- Designed to prevent replication
- REPLICATION TECHNIQUES
- EASY ENTRIE MILLING MACHINE
- SILINCONE 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

COMPROMISE THE SYSTEM: Obtaining the Critical Data

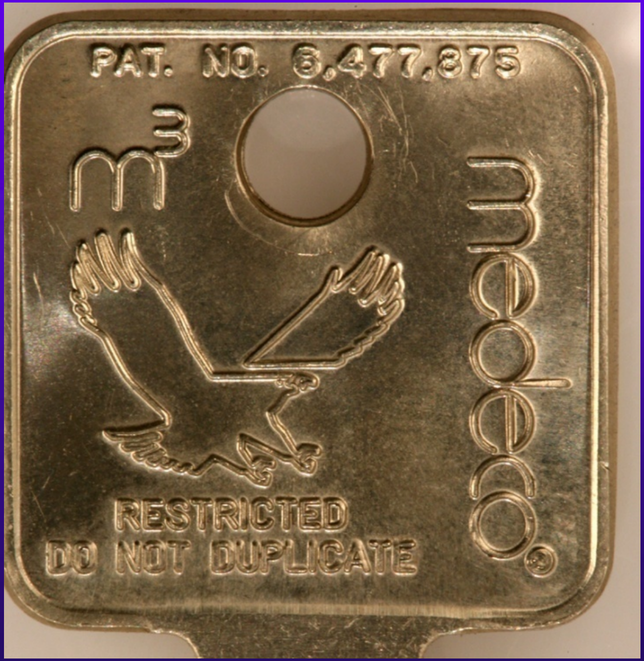
- TECHNIQUES TO OBTAIN KEY DATA
- Impressioning methods
- Decoding: visual and Key Gauges
- Photograph
- Scan keys
- Copy machine

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

- [medeco quote from adv]



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

- [medeco copier photo]

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

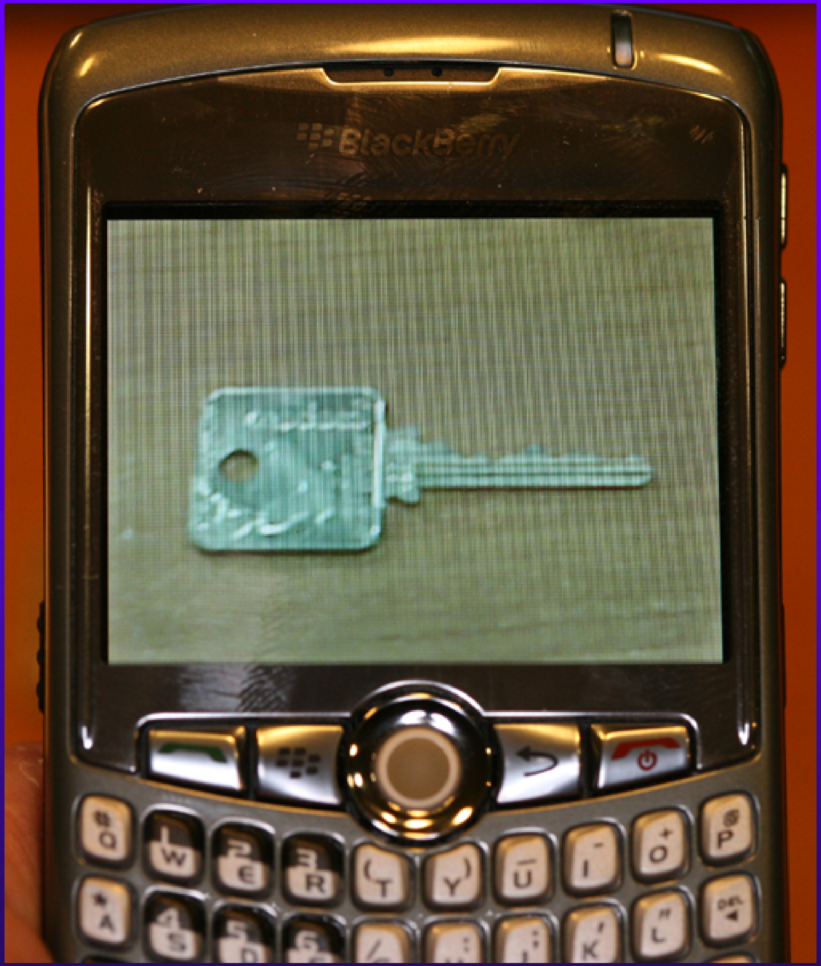
OBTAIN DATA - COPIER

OBTAIN DATA

- SCANNER

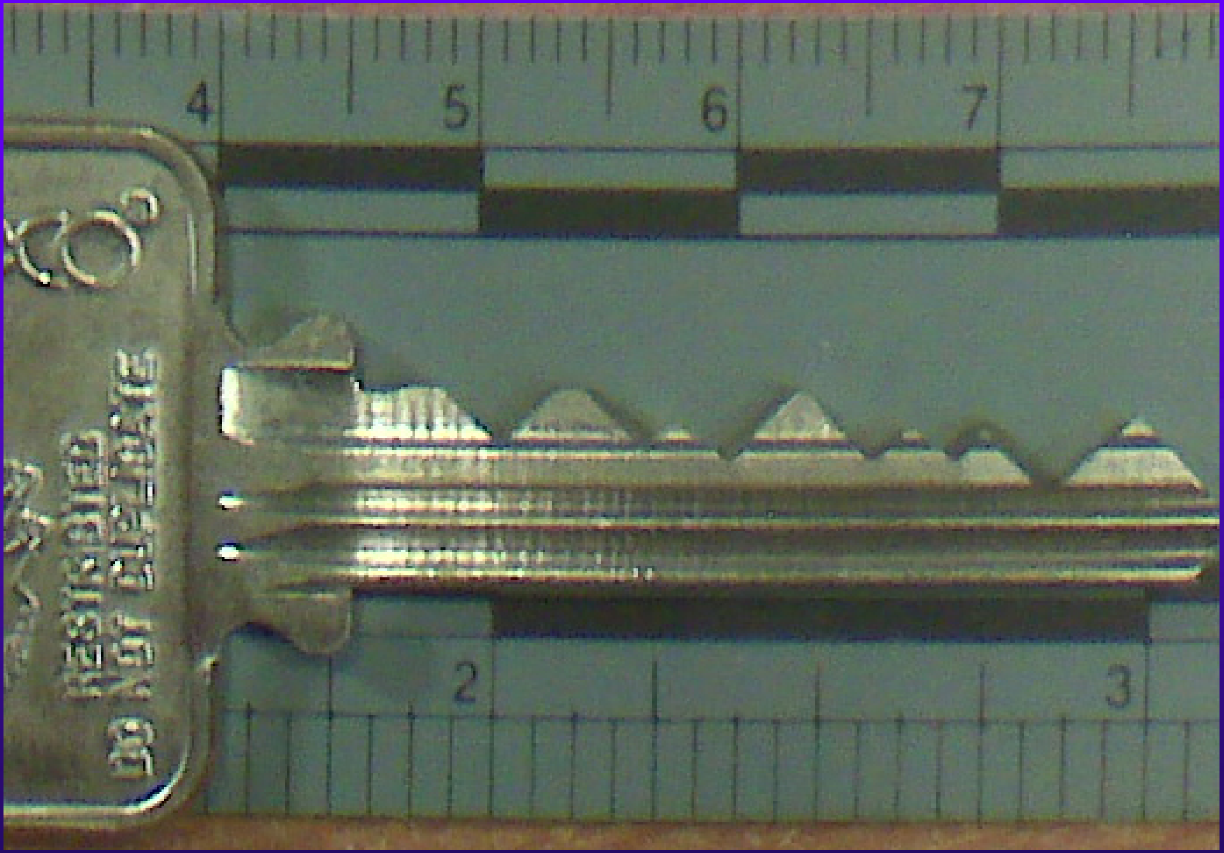
OBTAIN DATA

- CELL PHONE



BLACKBERRY CURVE

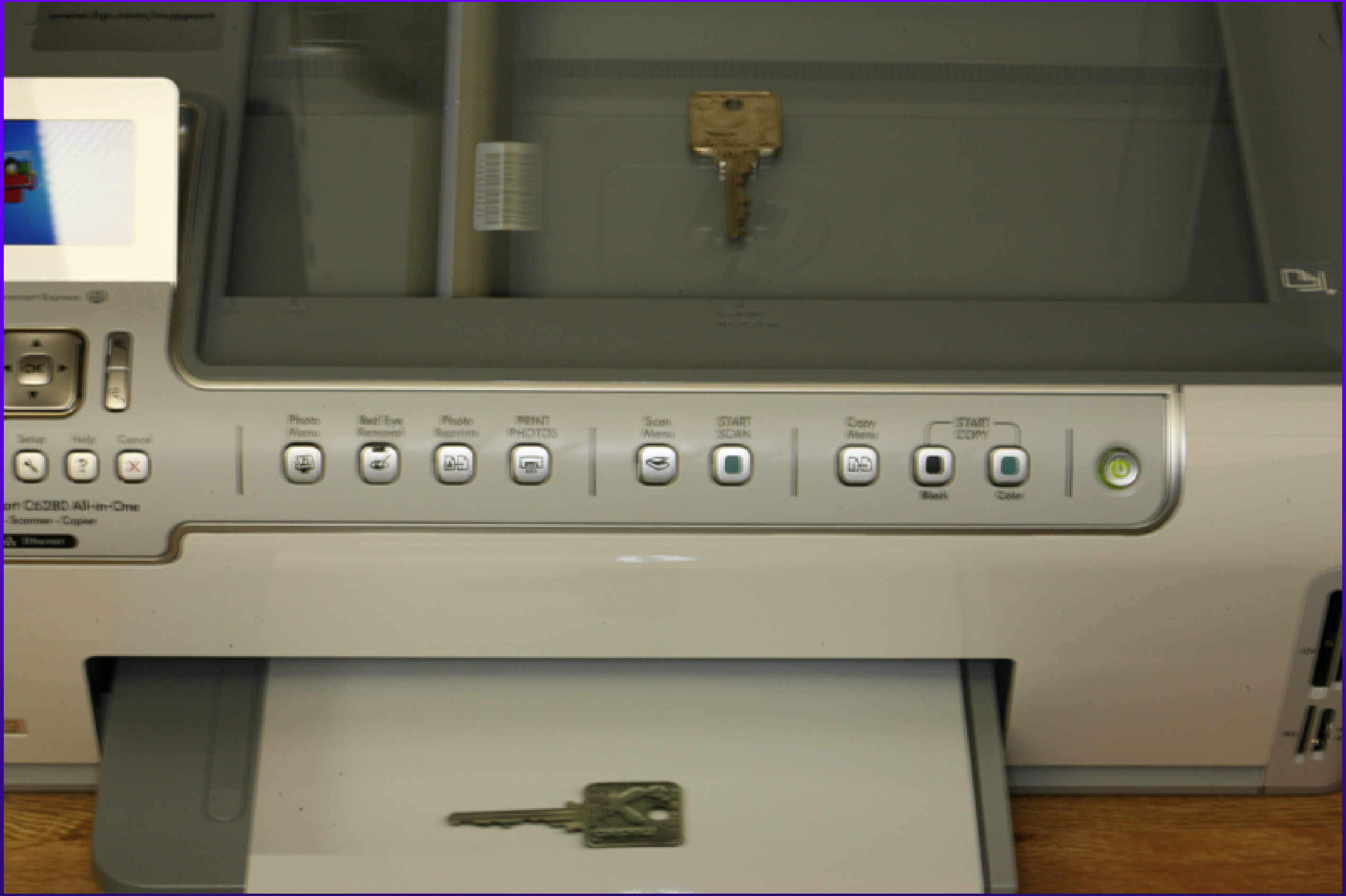
- ♦ CAPTURED IMAGE



RESULTING IMAGE

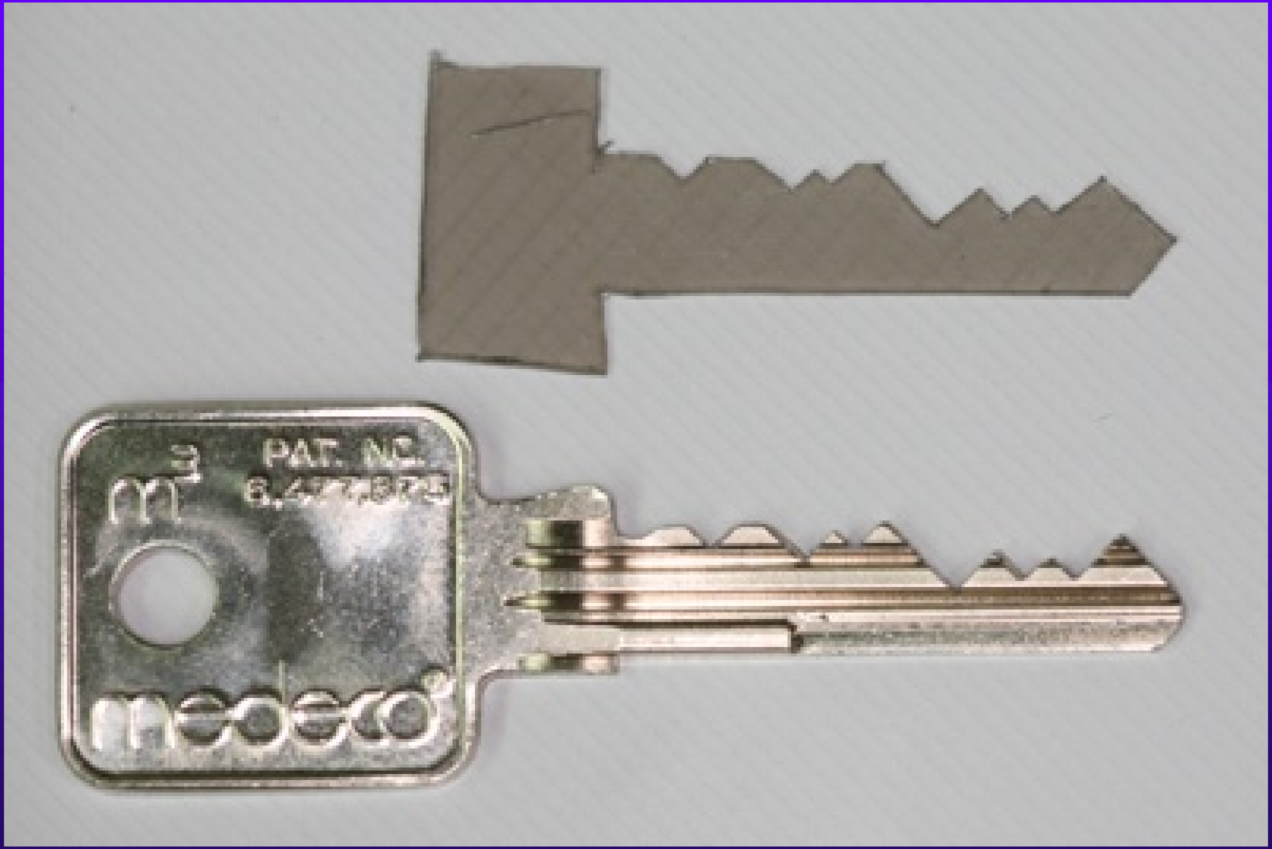
- REPRODUCE THE IMAGE
  - On Paper
  - On plastic sheet
  - On Adhesive Labels
  - On Shrinky dinks® plastic
  - On a piece of copper wire
  - On a simulated metal key

PRINT IMAGE ON PLASTIC OR PAPER

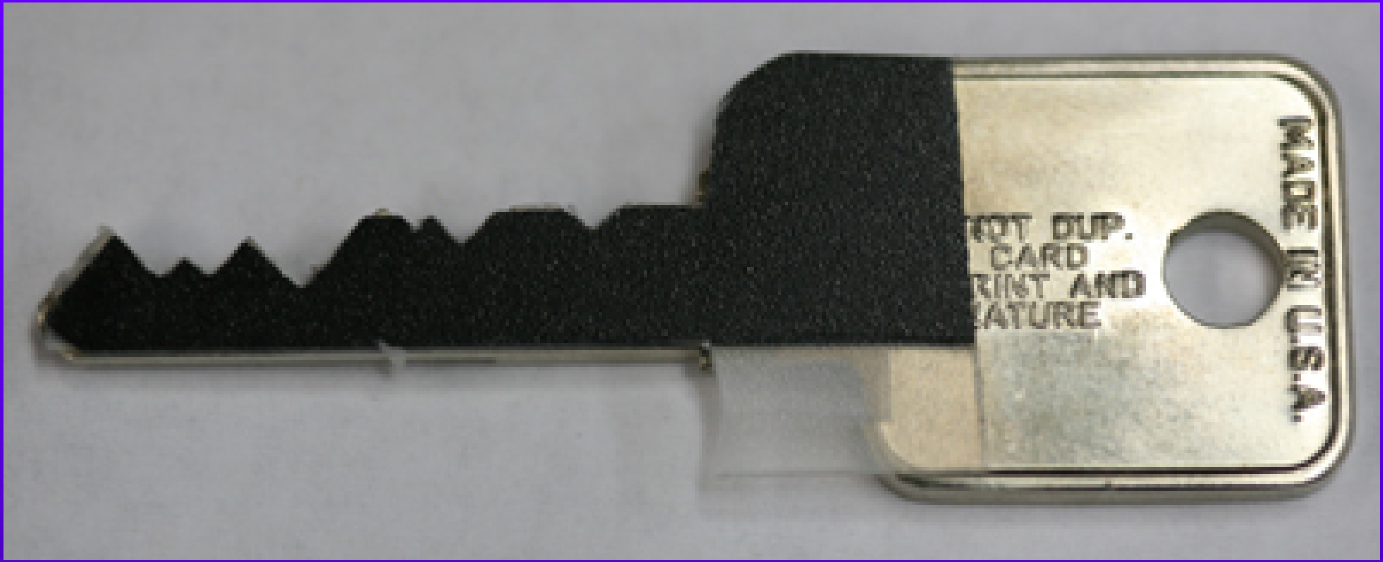


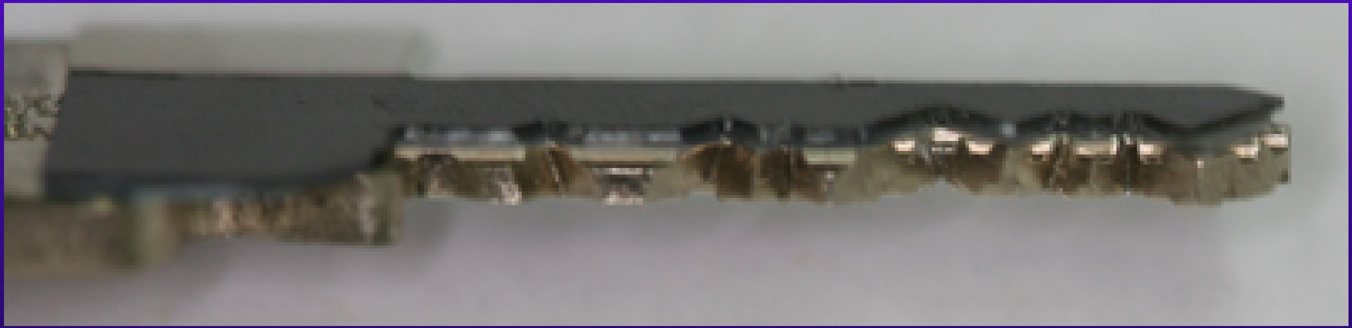
SET THE SHEAR LINE

- ♦ PLASTIC KEY SETS SHEAR LINE

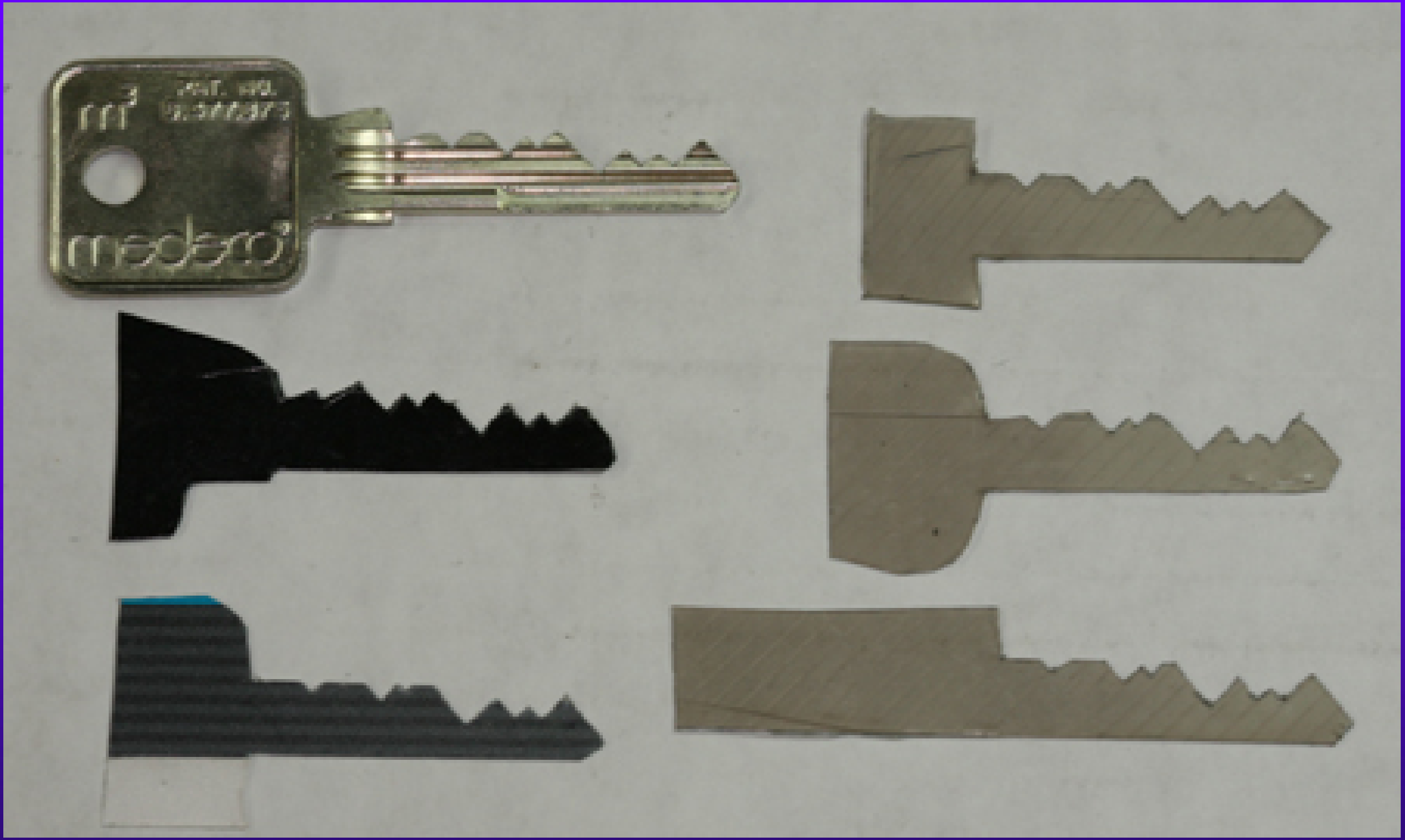


SET THE SHEAR LINE



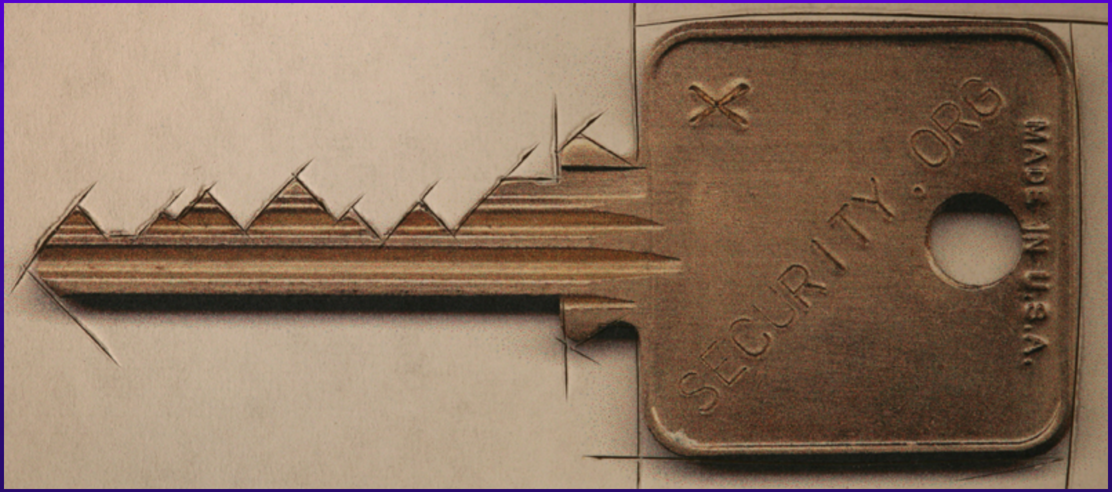


SET THE SHEAR LINE

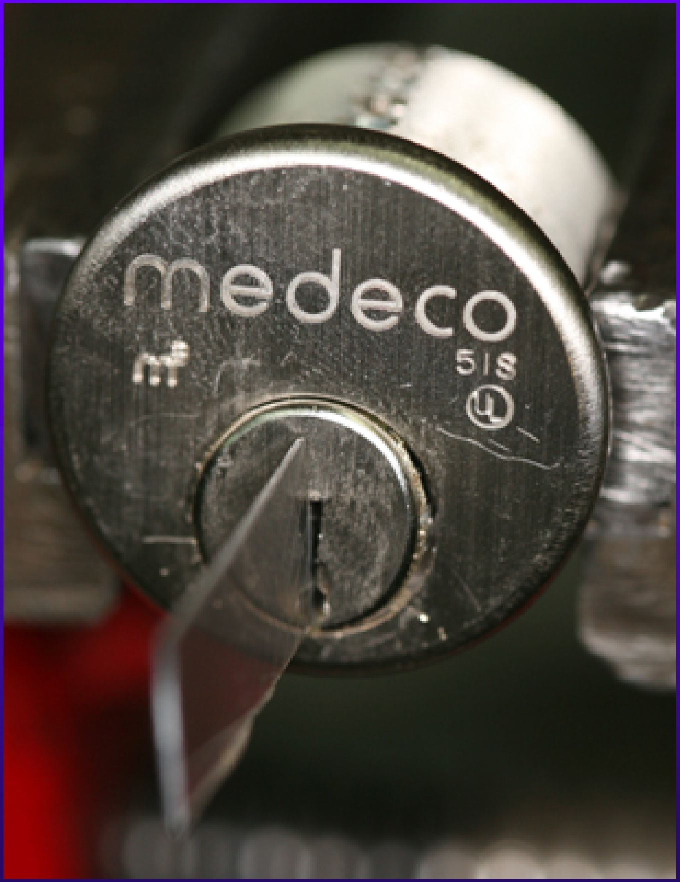


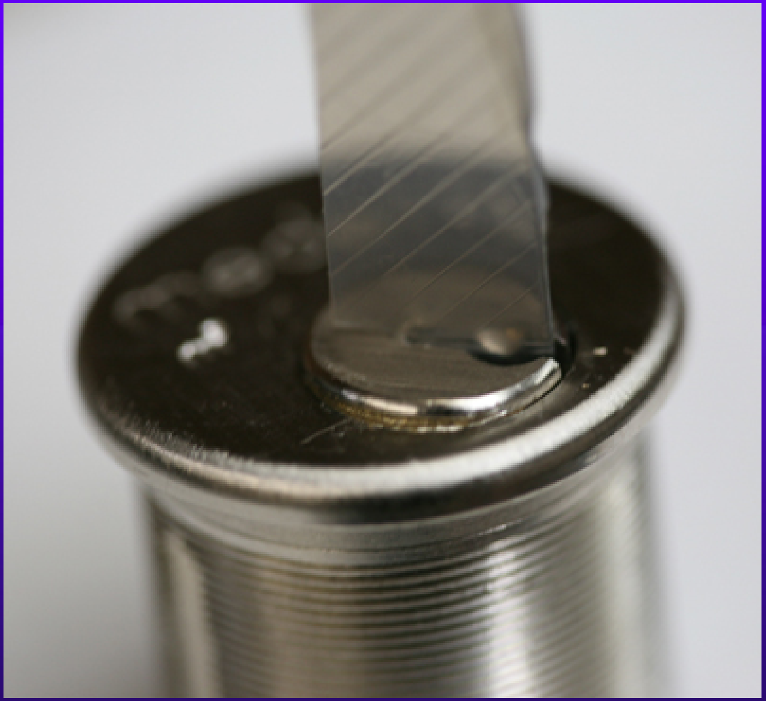
CUT A FACSIMILE OF KEY

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

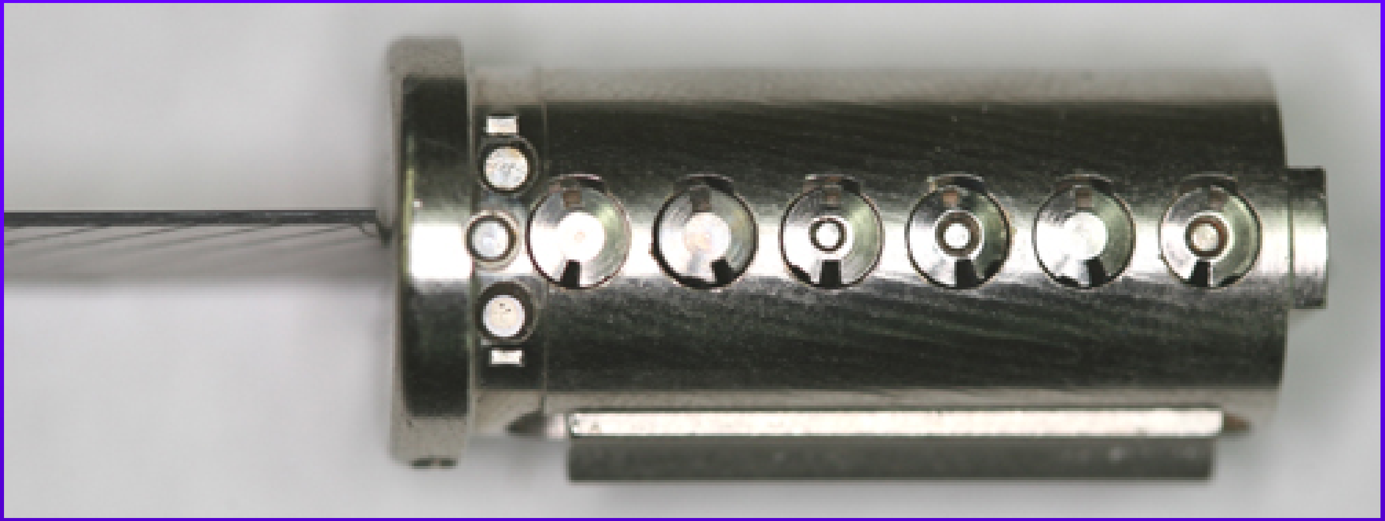


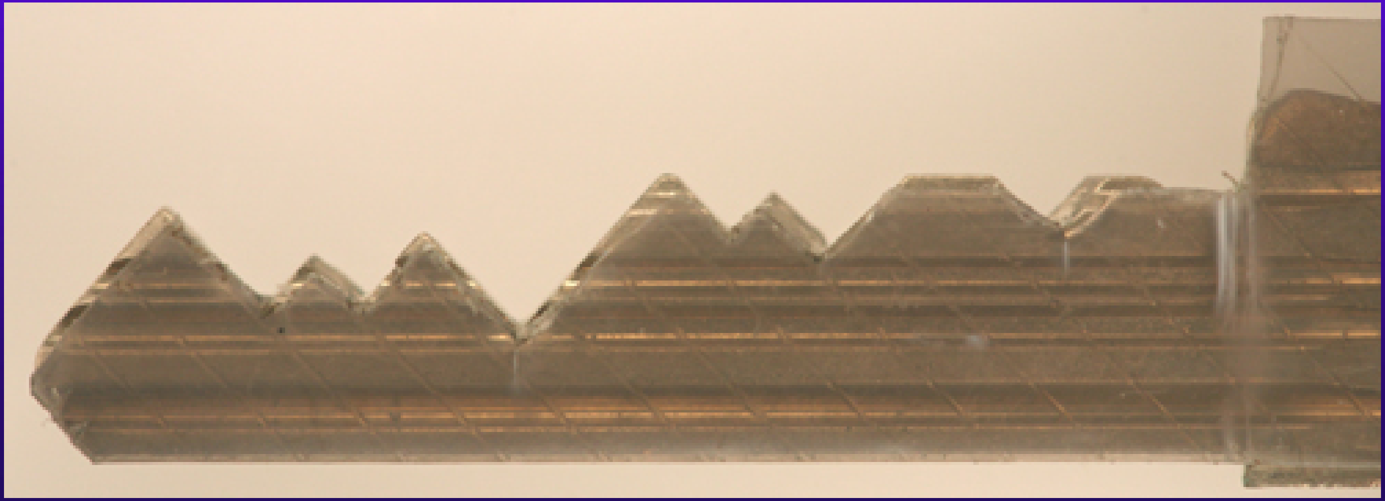
SET THE SHEAR LINE: OPEN THE LOCK





NEUTRALIZE SHEAR LINE





LOCKS, LIES, AND VIDEOTAPE: MEDECO CASE STUDY

- **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 RECOGNIZES LOCKSPORT: NDE: May, 2008

- BASED ON RESPONSIBLE DISCLOSURE ABOUT MEDECODER
  - Give Medeco time to fix the vulnerability
  - Right result, wrong reason
  - No t new: 15 year old bypass
  - Problem in millions of locks
  - Concept not applicable

KNOWN VULNERABILITIES IN MEDECO LOCKS

- RESPONSIBLE DISCLOSURE v. IRRESPONSIBLE NON-DISCLOSURE
  - Serious vulnerabilities disclosed
  - Notice to manufacturer for 18 months
  - Failure to disclose to dealers or customers
  - Misrepresentation, half truth, misleading advertising and use of language that means nothing

RESPONSIBLE DISCLOSURE: It is a Two-Way Street

- DISCOVERY OF VULNERABILITY
  - Locksport, hacker, security expert disclosure to manufacturers
  - Manufacturers to dealers and consumers
- SIGNIFICANT QUESTIONS
  - When discovered
  - New lock or embedded base
  - Number of users affected
  - National security issues

RESPONSIBILITIES

- **Locksport and hacker responsibility**
  - Disclose vulnerability in new lock design or upgrade
  - What about current locks that are installed
  - Give time to fix? When relevant?

HIGH SECURITY LOCK MANUFACTURERS

- **Responsibility of high security lock manufacturer are different**
  - High security is different than normal mfg or corporation
  - Protect high value targets, critical infrastructure
- **Duties**
  - Tell the truth
  - Disclose security vulnerabilities to customers and dealers

RESPONSIBLE DISCLOSURE: REALITY, AND LIABILITY

- WHAT TO DISCLOSE AND TO WHOM
- TWO COMPONENTS
- PUBLIC RIGHT AND NEED TO KNOW
  - SECURITY BY OBSCURITY
  - ASSUME THE RISK, ONLY CAN BE BASED UPON KNOWLEDGE
  - BAD GUYS KNOW
- LOCKS NOT LIKE SOFTWARE
  - NOTICE ONLY PROSPECTIVE TO FIX PROBLEMS

DISCLOSURE TO MANUFACTURER: Prospective or Retroactive Effect

- PROSPECTIVE IMPLEMENTATION OF FIX BY MANUFACTURER
  - Only applies to new locks or new product
  - Does not apply to embedded base
  - Does not help the consumer unless manufacturer does a recall or field fix
- QUESTION OF LIABILITY AND COST
  - Who will pay for retroactive upgrade?
  - "Enhancement" to new bypass technique or liability to remedy?

MEDECO TIMELINE

- 1994 ARX pins and John Falle decoder
- 2006 Bumping of conventional locks
  - Medeco issues press release: Bump-Proof
- 2006-2007 Data to Medeco regarding bumping, picking, and key control
- 2007 Tobias Deadbolt attack
- 2007 JennaLynn Bumps a Biaxial
- 2008 Jon King Medecoder and Medeco recognition of Locksport community

MEDECO: Responsible or Irresponsible Actions?

- BUMPING CLAIMS BY MEDECO
- August 4, 2006 Press Release: “Our Locks are Bump-Proof!”
- 2007: Retroactive change, “Our Locks are Virtually Bump-Proof”
- 2007: “Our locks are virtually resistant!”

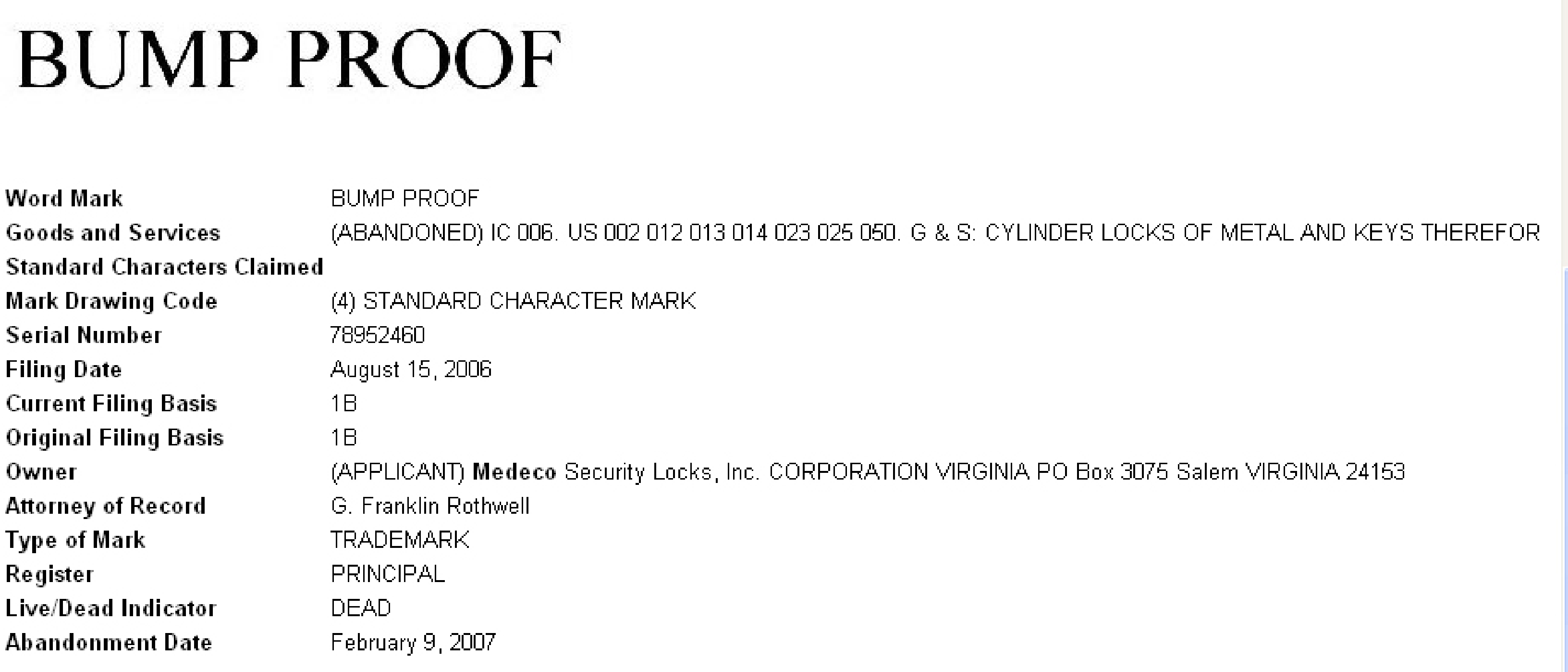
MEDECO BUMPING CLAIM: "We never said it: Others did!"

- 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

MEDECO LOCKS ARE VULNERABLE

- MEDECO KNOWS
- Vulnerability from Bumping, Picking, Key control, Forced Entry techniques
- Should be candid with dealers and users so they understand the potential risks
- Failure to tell the truth = irresponsible non-disclosure
- Dealers and customers have a need and a right to know

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

- http://www.security.org
- http://in.security.org

- mwtobias@security.org
- mjfiddler@security.org
- tbluzmanis@security.org