



KEY CONTROL: 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



MEDECO INSECURITY: Real World Threats - Keys

- ◆ VIOLATION OF KEY 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 ENTRY MILLING MACHINE
- ◆ SILINONE 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



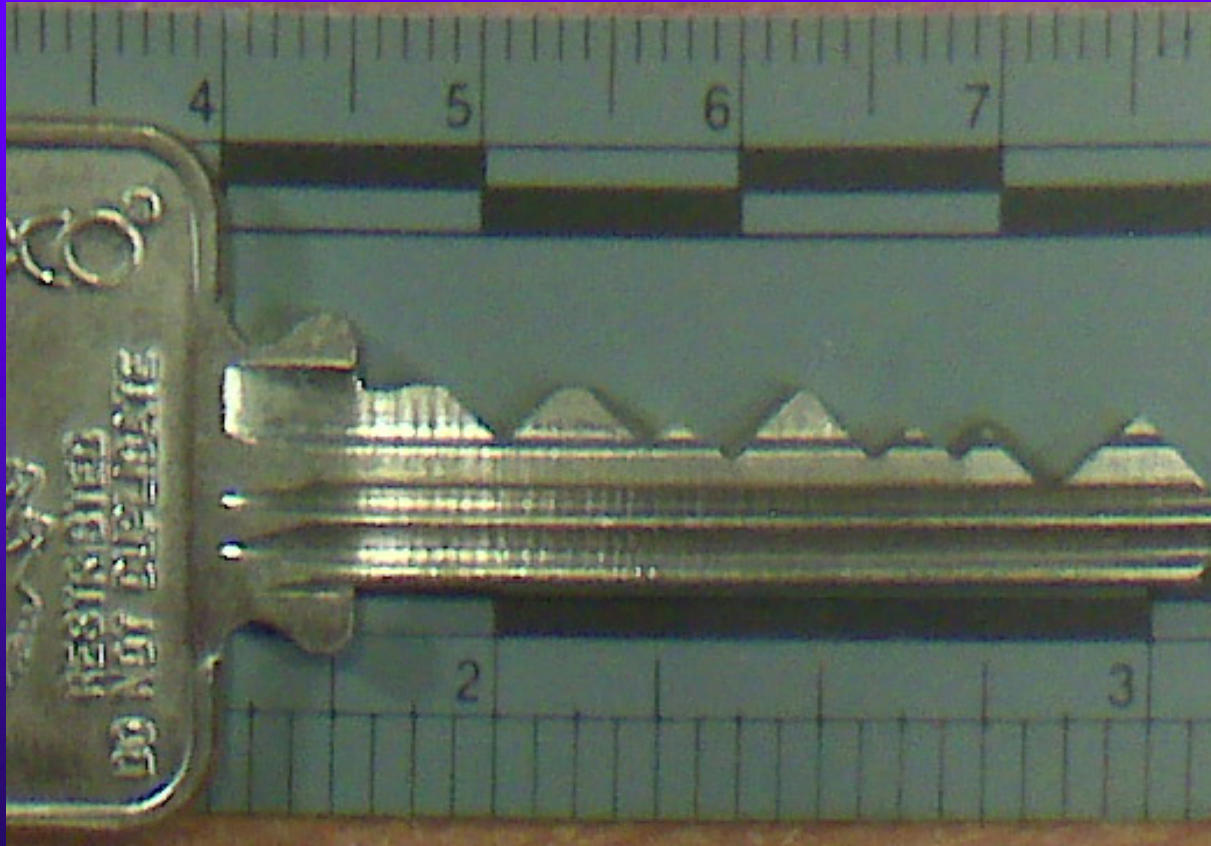
OBTAIN DATA

◆ CELL PHONE



BLACKBERRY CURVE

◆ CAPTURED IMAGE





RESULTING IMAGE

◆ REPRODUCE THE IMAGE

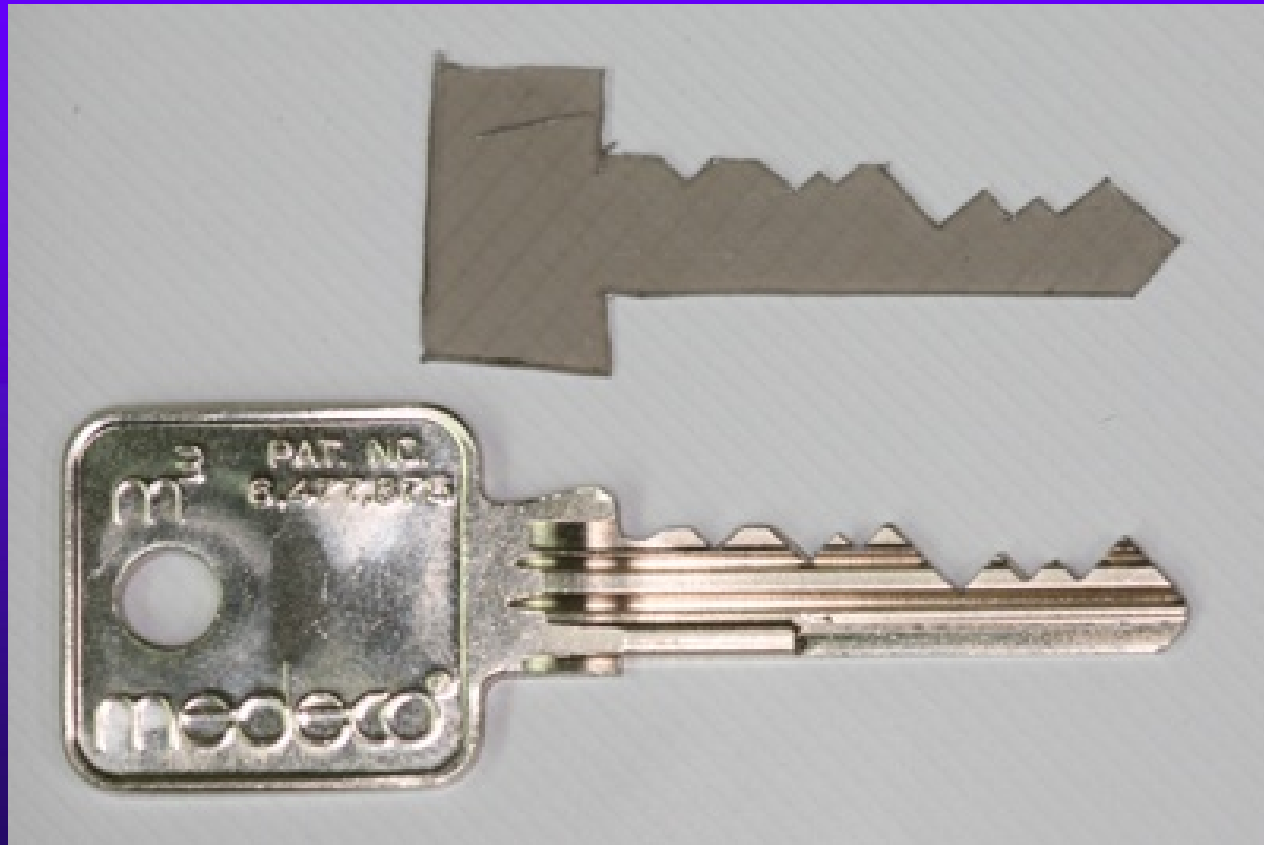
- On Paper
- On plastic sheet
- On Adhesive Labels
- On Shrinky dinks® plastic
- On a piece of copper wire
- On a simulated metal key

PRINT IMAGE ON PLASTIC OR PAPER

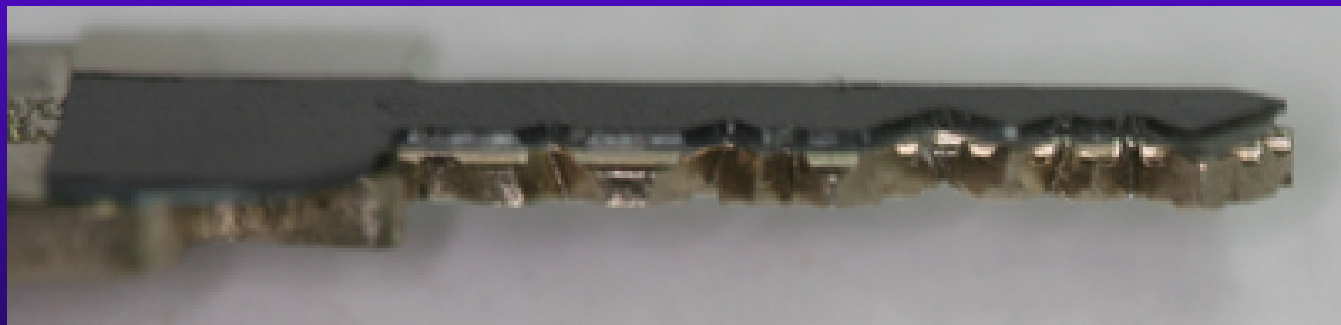
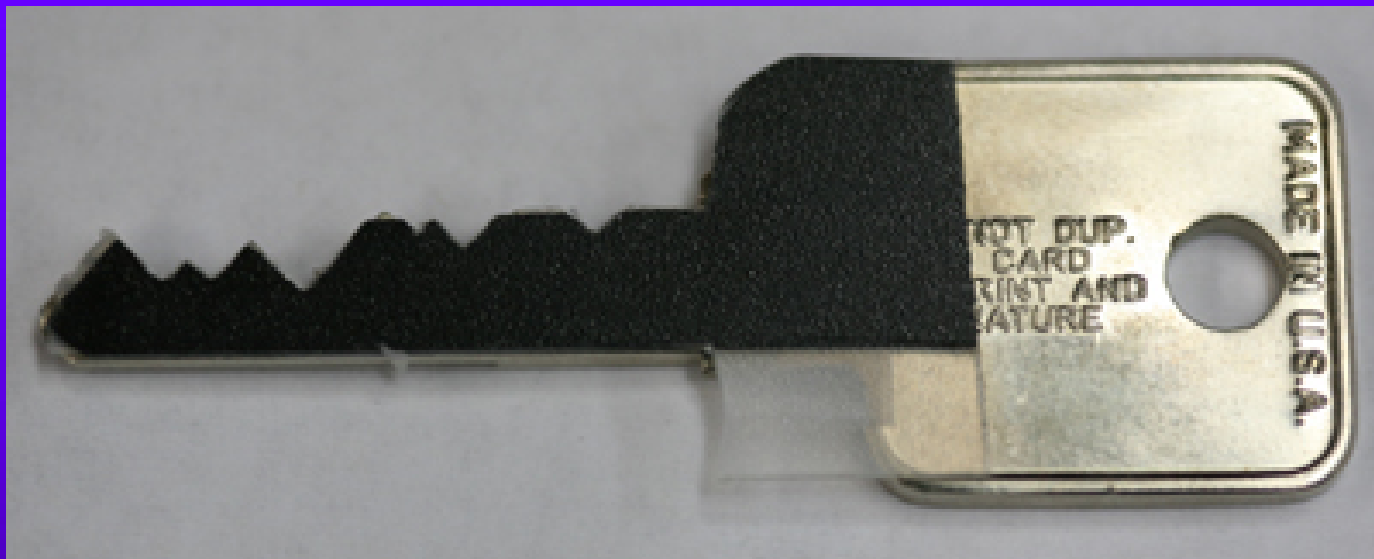


SET THE SHEAR LINE

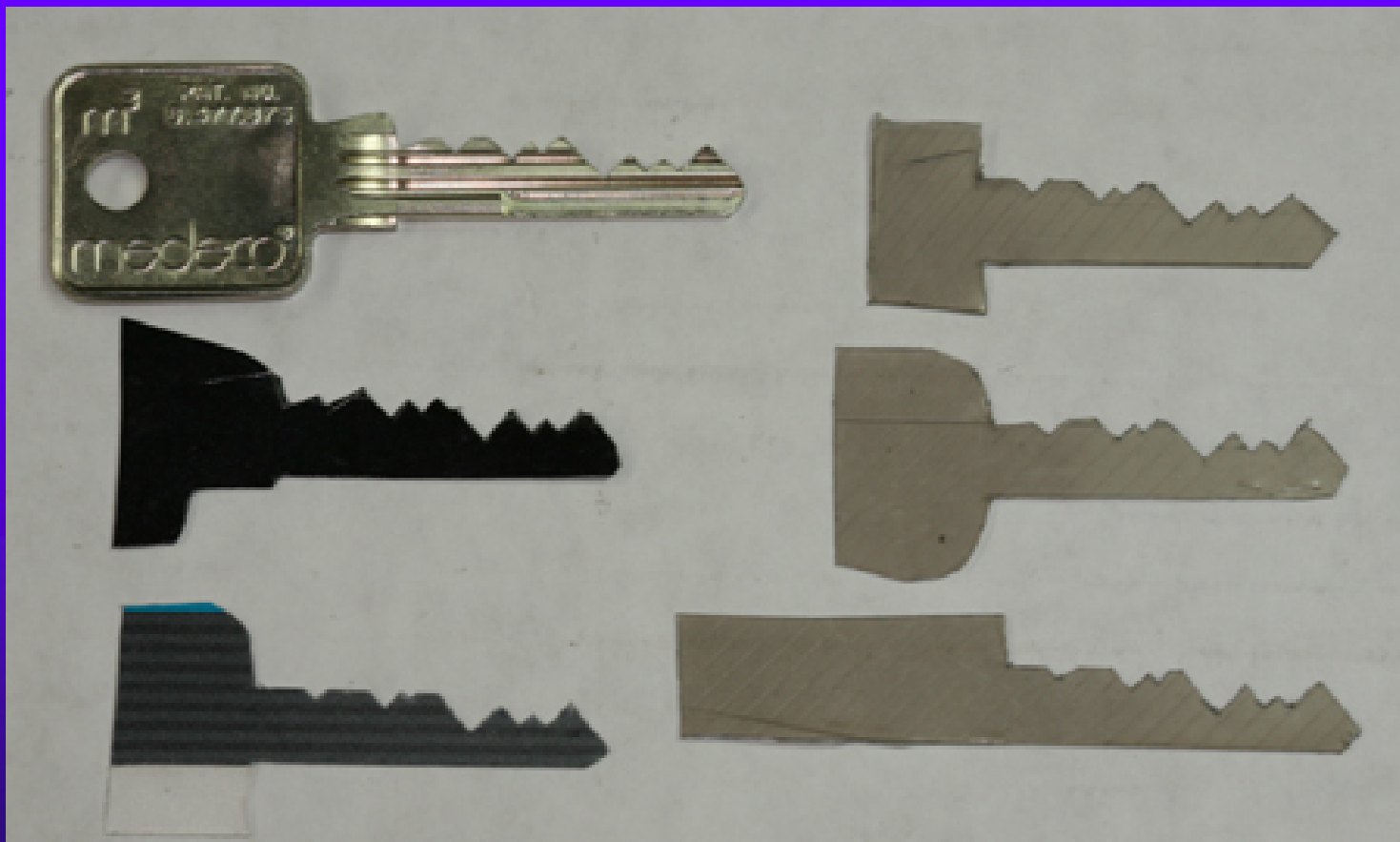
- ◆ PLASTIC KEY SETS SHEAR LINE



SET THE SHEAR LINE



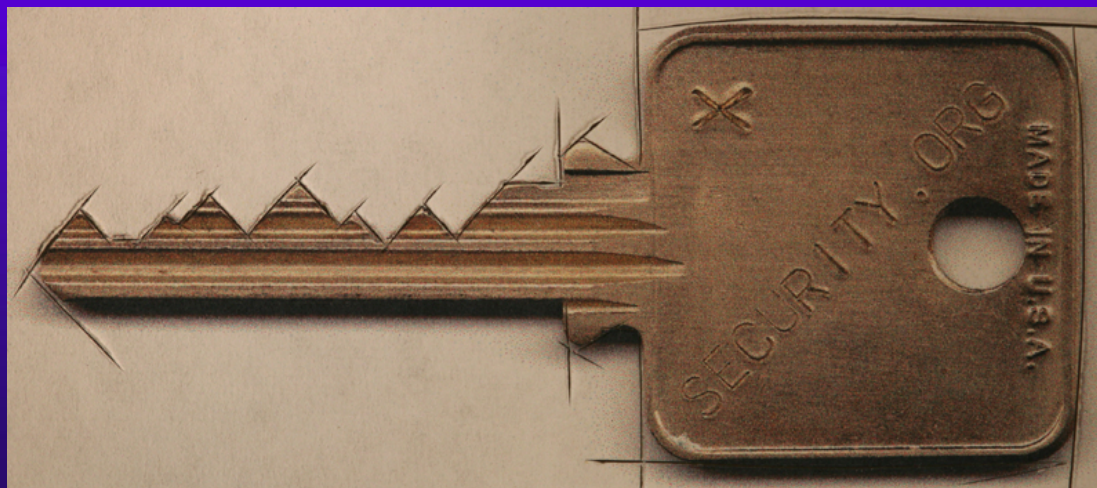
SET THE SHEAR LINE



CUT A FACSIMILE OF KEY

◆ KEY REQUIREMENTS

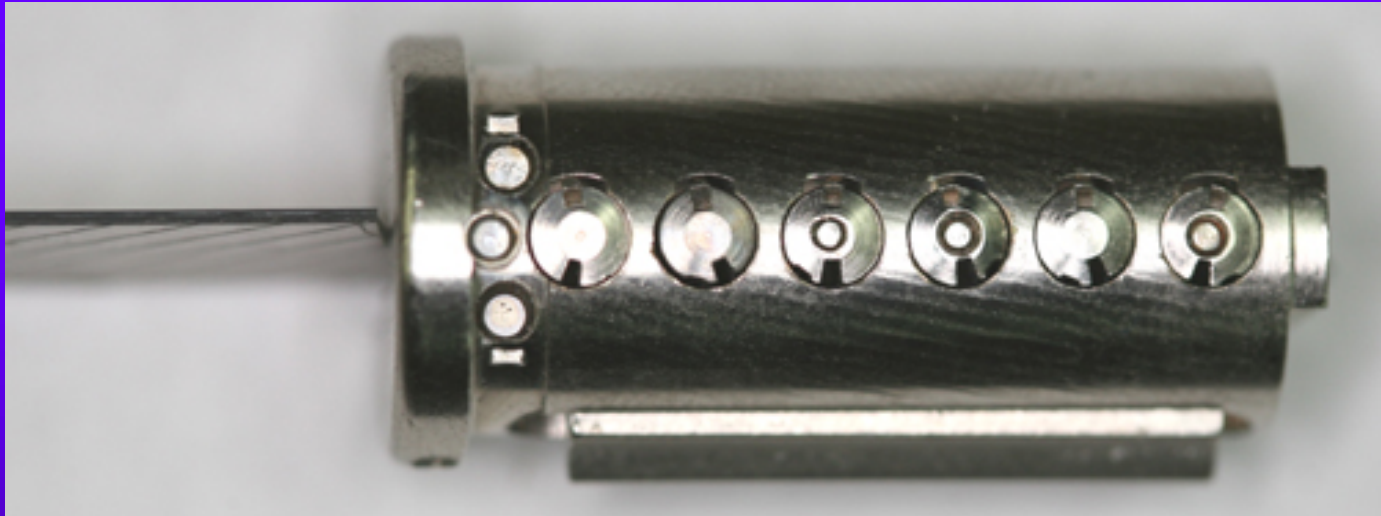
- Vertical biting only
- No sidebar data
- No slider data



SET THE SHEAR LINE: OPEN THE LOCK



NEUTRALIZE SHEAR LINE



EASY ENTRY: SIMULATED KEY BLANKS



OPEN THE LOCK: Replicate the Key in Plastic

◆ MEDECO TAKES PLASTIC!



KEYS FROM CREDIT CARDS



M3 PLASTIC KEYS: OPEN THE LOCK





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