OPENING LOCKS IN TEN SECONDS OR LESS: Is it a real threat to security?

Bumping as a method of covert entry

©2007 Marc Weber Tobias

ATTACK ON LOCKS: TWO THREATS TO SECURITY

- MECHANICAL LOCKS ARE SUBJECT TO BYPASS
- ACCESS CONTROL SYSTEMS UTILIZE MECHANICAL LOCKS
- THREE PRIMARY ISSUES FOR I-T:
  - Bumping
  - Master key extrapolation
  - Ability to replicate keys

A THREAT TO THE I-T ENVIRONMENT

- NON-SOPHISTICATED ATTACKS
- EASY TO ACCOMPLISH
- NO FORENSIC TRACES
- LOW RISK OF DETECTION
- 3T-2R RULE
- CAN COMPROMISE AN ENTIRE FACILITY OR CRITICAL LOCKS

LOCKS PROVIDE SECURITY

- Protect doors, safes and barriers from being opened
- They control movement of barriers to entry
- Relied upon as first level of security
- Most popular: pin tumbler designs

TYPES OF LOCKS

- WARDED
- LEVER
- WAFER AND DISK TUMBLER
- PIN TUMBLER
- HYBRID: COMBINED TECHNOLOGIES
- COMBINATION

PIN TUMBLER LOCK

- 4000 year old Egyptian design
- Re-invented by Linus Yale in 1860
- Modern pin tumbler: split pins
- 95% of locks
- Low to high security applications
- All based upon Yale design
  - Billions of locks
  - Many different configurations

OPENING LOCKS: Covert Methods of Entry

- PICKING
- IMPRESSIONING
- DECODING
- EXTRAPOLATION OF TMK
- BUMPING
  - Move all pins to shear line together or separately
  - Allow plug to turn without obstruction

CMOE AND SECURITY RATING

- SPECIAL TOOLS
- TRAINING AND EXPERTISE
- TIME REQUIRED
- RELIABILITY AND REPEATABILITY OF RESULTS
- DAMAGE TO LOCKS
- FORENSIC TRACE

WHAT IS SECURITY IN A LOCK

- Perfect world: cannot open without correct key or code;
- Reality: Levels of difficulty or resistance to forced and covert entry techniques
  - Type of mechanism
  - Secondary locking systems
  - Security enhancements

BUMPING: A NEW OLD THREAT

- KNOWN SINCE 1925
- WAS NOT SIGNIFICANT METHOD OF BYPASS
- NEW THREAT RAISED IN 2004
- TOOOL, BARRY WELS, OTHERS
- NOT POPULAR IN U.S. UNTIL 2006

NETHERLANDS TESTS

- CONSUMER REPORTS AND DUTCH LAW ENFORCEMENT AND TOOOL
- VALID AND COMPREHENSIVE
- MARCH, 2006 TEST OF ABOUT 70 MANUFACTURERS
- LARGE SAMPLE
- RELEVANT TO THE U.S. MARKET

NETHERLANDS TEST RESULTS

- MOST LOCKS COULD BE OPENED WITHOUT DIFFICULTY
- CONVENTIONAL AND HIGH SECURITY CYLINDERS OPENED
- MOST LOCKS NOT SECURE

THE THREAT FROM BUMP KEYS

- IF CAN OBTAIN A KEY THAT FITS THE LOCK THAT HAS ALREADY BEEN CUT
  - EASY TO LEARN BUMPING
  - ANYONE CAN OPEN A LOCK

BUMPING POSES A SERIOUS THREAT TO SECURITY

- AFFECTS MILLIONS OF LOCKS
- CRITICAL INFRASTRUCTURE OFTEN PROTECTED BY POOR LOCKS
- PROTECT PRIMARY PRIVACY AND COMMUNICATIONS
- FEDERAL REQUIREMENTS FOR INFORMATION SECURITY

BUMPING: CRITICAL ISSUES

- 95% OF LOCKS VULNERABLE
- EVERYONE WHO RELIES ON LOCKS MUST UNDERSTAND RISK SO CAN MAKE OWN JUDGMENT
- LEGAL ISSUES OF LIABILITY
- SECURITY ISSUES

WHY IS BUMPING A THREAT

- SIMPLEST FORM OF BYPASS
- 3T-2R RULE TO ASSESS SECURITY AGAINST COVERT ENTRY
  - TRAINING
  - TIME
  - TOOLS
    - REPEATABILITY
    - RELIABILITY

USPS LOCKS: 5 SECONDS TO IDENTITY THEFT

PRIMARY THREAT LEVELS

- SYSTEM INTELLIGENCE
- AVAILABILITY OF KEYS
  - SECURITY RISKS CHANGE SIGNIFICANTLY IF PRE-CUT
    - ONLY REQUIRES SLIGHT TRAINING

THREAT LEVEL 1: SYSTEM INTELLIGENCE

- NO INTELLIGENCE
  - STANDARD PIN TUMBLER LOCK
- PRIOR INTELLIGENCE
  - SECONDARY LOCKING SYSTEM
  - MEDECO, ASSA

THREAT LEVEL 2: KEYS

- PRODUCING A BUMP KEY
  - FROM BLANKS
  - FROM CUT KEYS
- BUYING A PRE-CUT BUMP KEY

CMOE AND SECURITY RATINGS

- SPECIAL TOOLS
- TRAINING AND EXPERTISE
- TIME REQUIRED
- RELIABILITY AND REPEATABILITY OF RESULTS
- DAMAGE TO LOCKS
- FORENSIC TRACE

BUMPING: A METHOD OF COVERT ENTRY

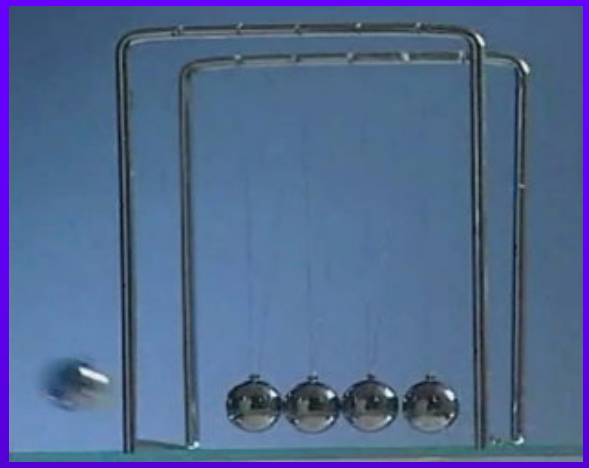
- METHOD TO OPEN LOCKS IN SECONDS
- FASTEST AND EASIEST WAY TO OPEN
- VIRTUALLY NO SKILL REQUIRED
- EASY TO LEARN
- NO SPECIAL TOOLS
- 95% OF LOCKS CAN BE BYPASSED
- OPEN SOME HIGH SECURITY LOCKS
- USUALLY NO TRACE OR DAMAGE
- RELIABILITY OF RESULTS
- REPEATABILITY OF THE PROCESS

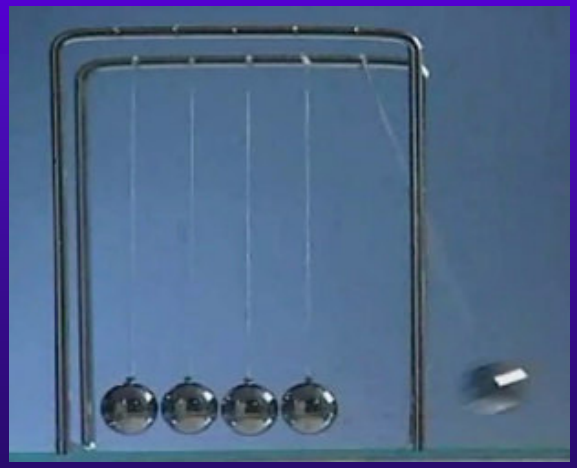
YALE + NEWTON = BUMPING

- VIRTUALLY ALL TRADITIONAL YALE LOCKS CAN BE OPENED BY BUMPING
- RELIABLE
- REPEATABLE
- SIMPLE TO LEARN

THE PHYSICS OF BUMPING: SIR ISAAC NEWTON: 1650

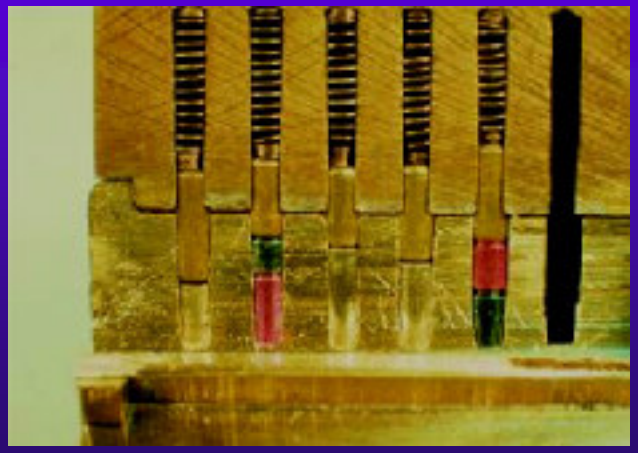
- THE FATHER OF BUMPING OF LOCKS
- THIRD LAW OF MOTION:
  - "For every action, there is an equal and opposite reaction"



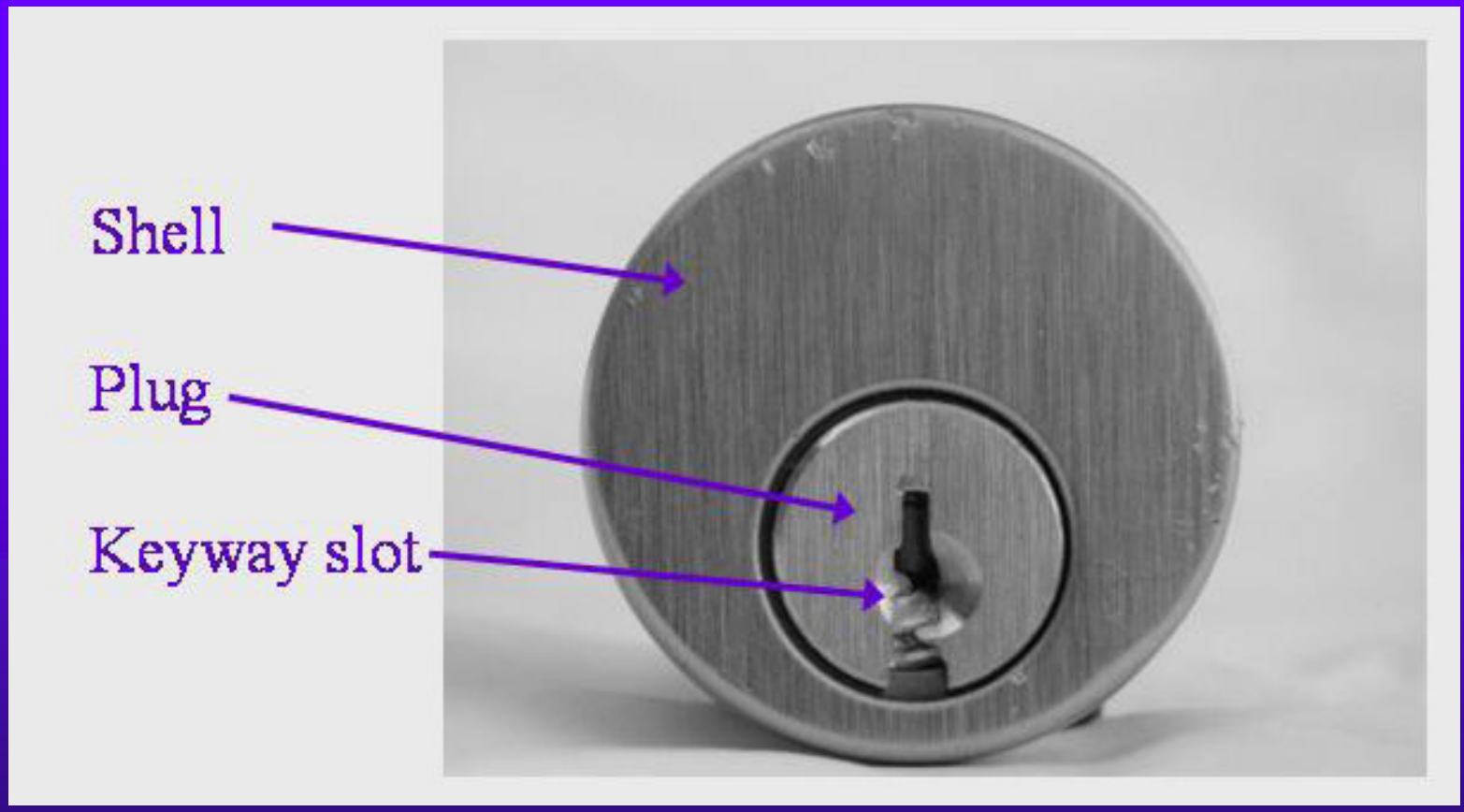


1860: YALE PIN TUMBLER LOCK

- Modernized the Egyptian single pin design
- Utilized two pins for locking
- Double-detainer theory of locking
- Created shear line



MODERN PIN TUMBLER LOCK



BUMPING: BACKGROUND

- ENGLAND: 1925, GEORGE BARON
- 999, CODE 12, PERCUSSION KEY
- DENMARK, 25 YEARS AGO
- DEVELOPED BY LOCKSMITHS TO RAP OPEN A CYLINDER
- ORIGINAL TECHNIQUE HAS BEEN IMPROVED UPON TO MAKE BUMPING A SIGNIFICANT THREAT

BUMPING: SIX CRITICAL ELEMENTS

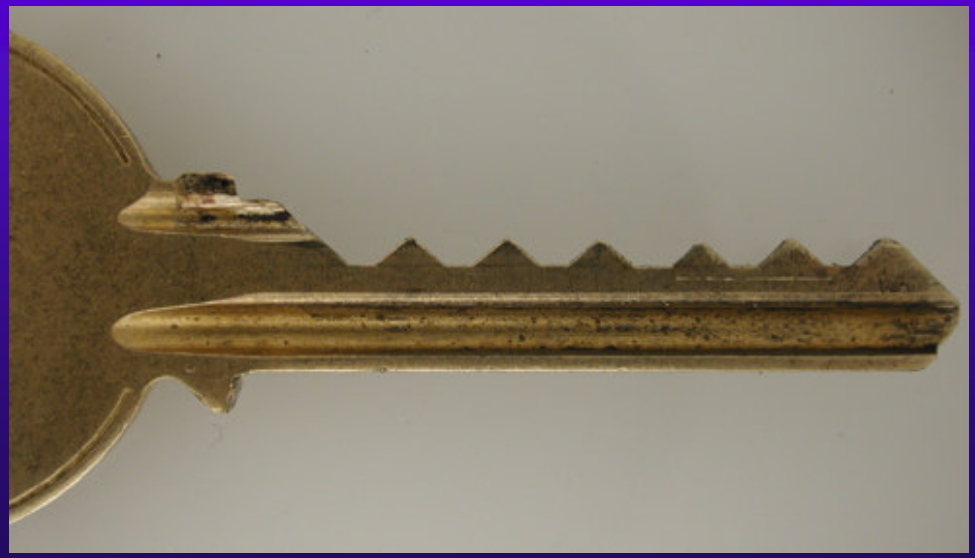
1. KEY WITH CORRECT KEYWAY
2. CUT TO ALL “9” DEPTHS
3. BUMPING TECHNIQUE
4. METHOD TO APPLY ENERGY TO PINS
5. TORQUE AND TIMING
6. TRAINING

1: KEY WITH CORRECT KEYWAY

- SOURCES
  - COMMERCIAL STORES
  - LOCKSMITHS
  - INTERNET
  - KEY TO ANY LOCK IN A FACILITY
  - MODIFIED KEY: MILLED BLANK

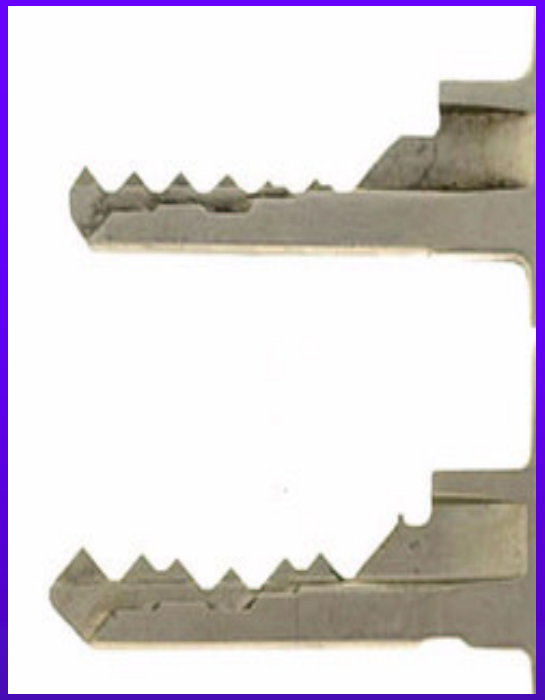
2: CUT TO ALL “9” DEPTHS

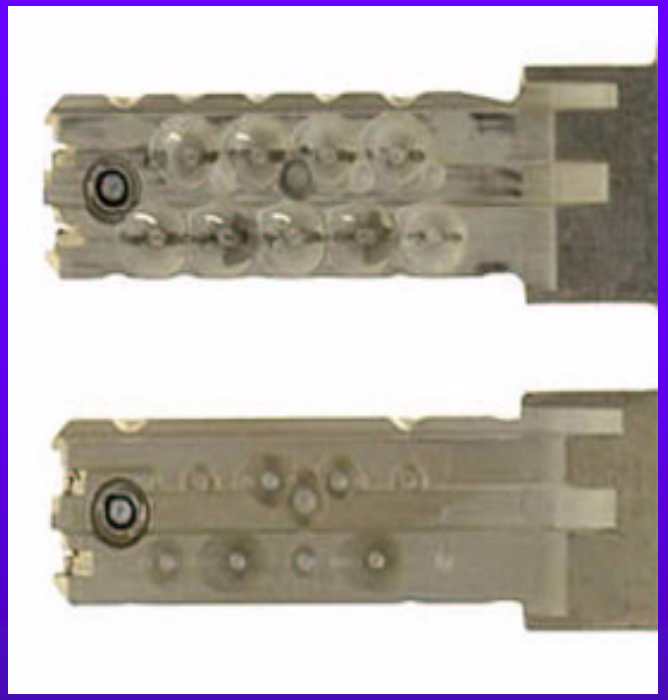
- HAND-CUT WITH FILE
- CODE CUT WITH PUNCH OR MACHINE
- INTERNET SITES
  - ALL KEYS OF SAME KEYWAY CAN BE MADE TO WORK

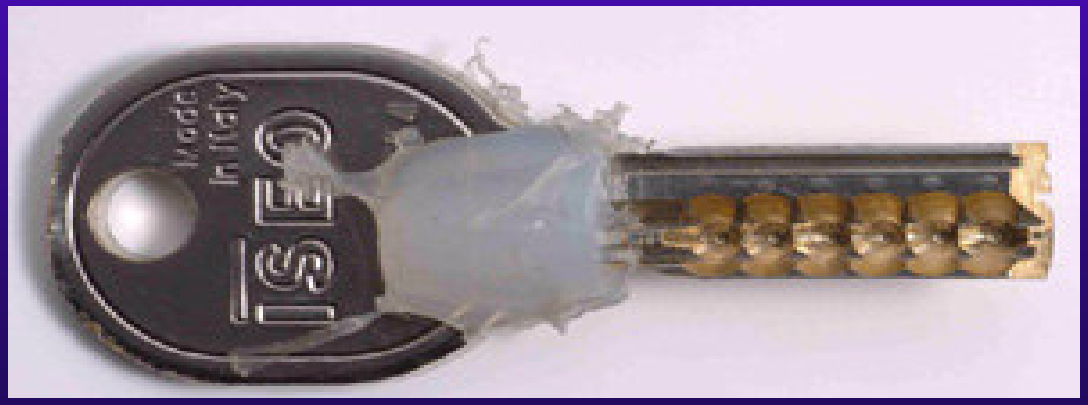


NEGATIVE SHOULDER

BUMP KEYS



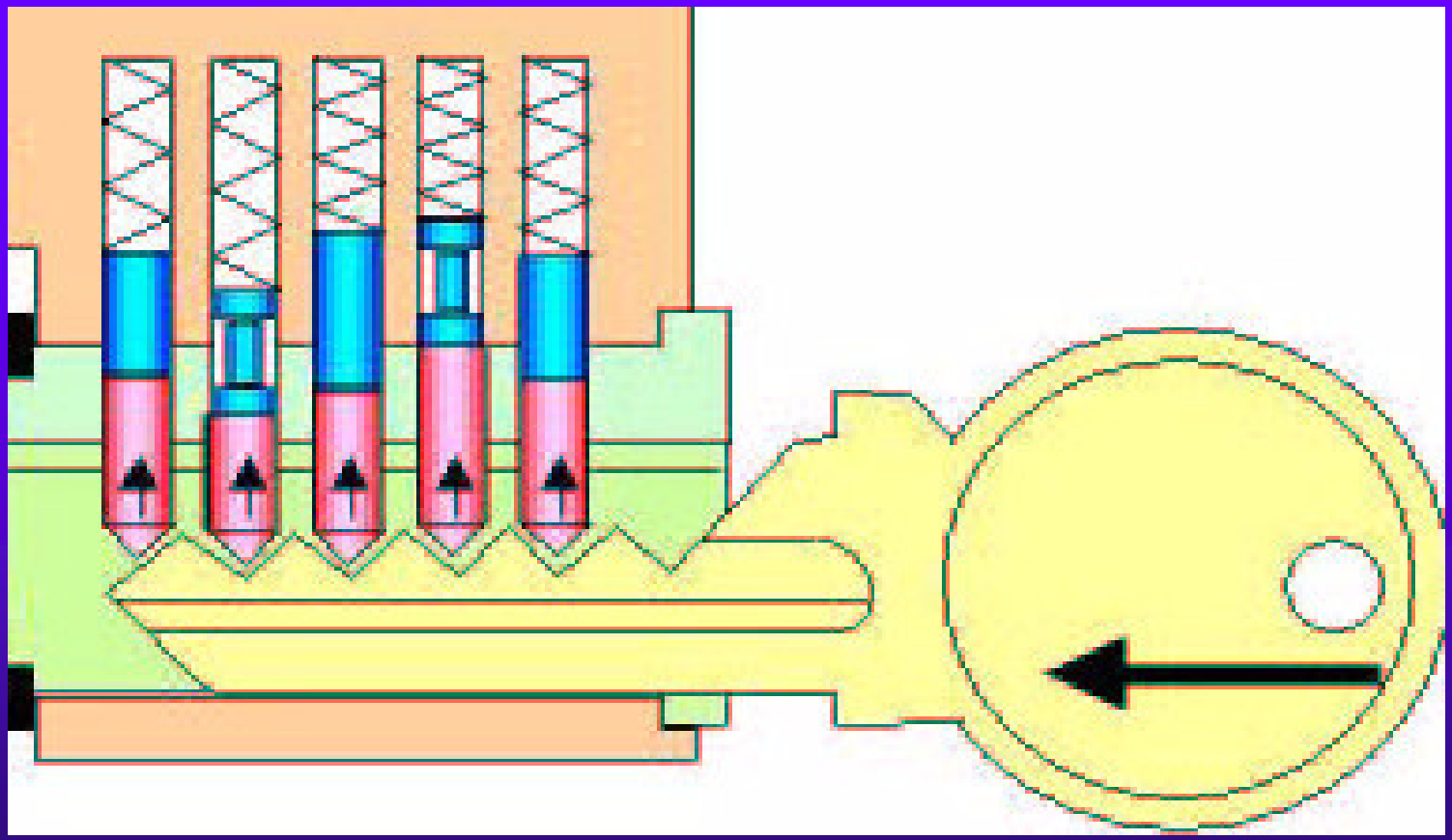




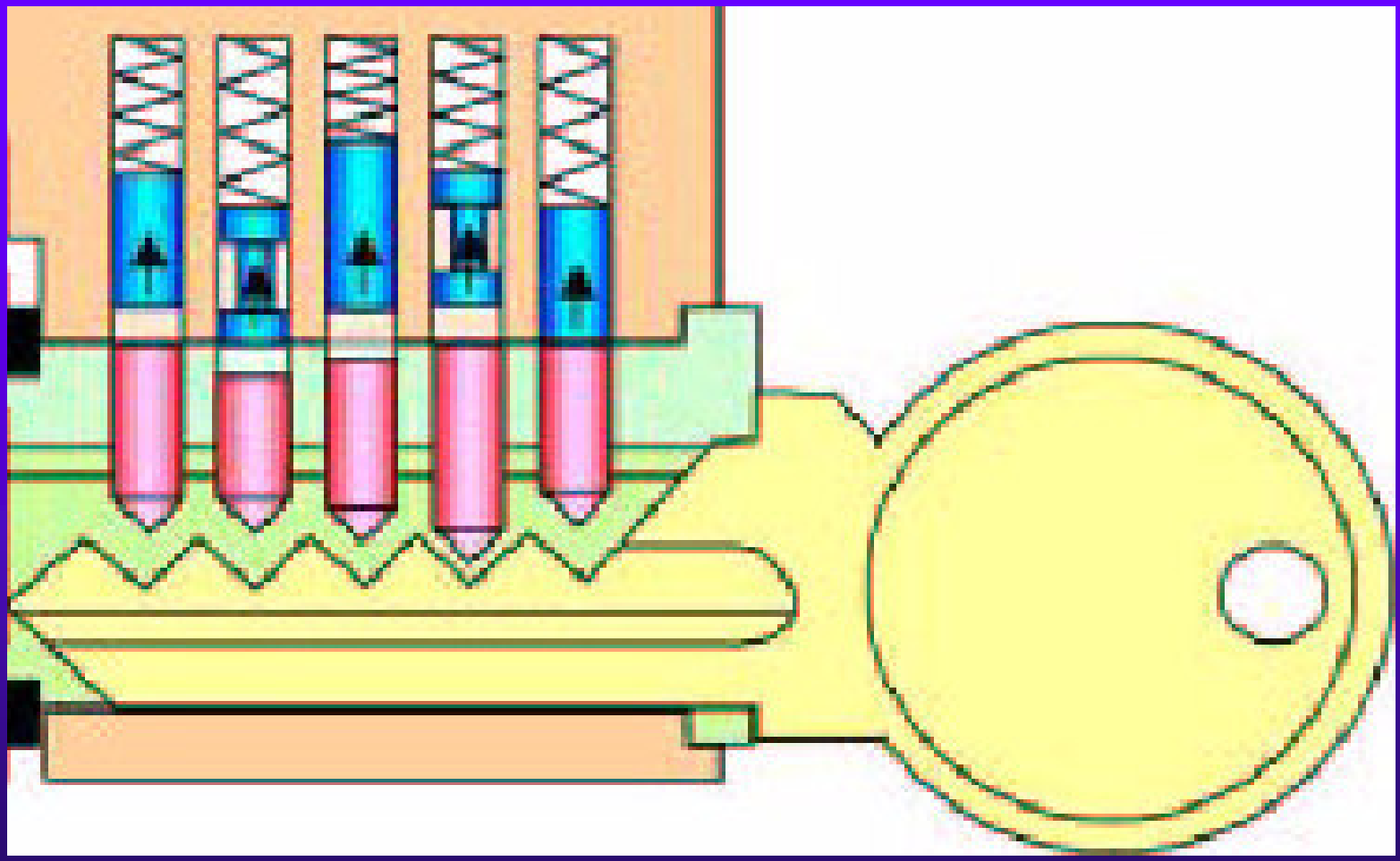
3: BUMPING TECHNIQUE

- TWO TECHNIQUES FOR BUMPING
  - WITHDRAW KEY ONE POSITION
    - NO MODIFICATION REQUIRED
  - NEGATIVE SHOULDER METHOD
    - REDUCE SHOULDER BY .25 mm
- DESIGN OF KEY DEPENDS UPON TECHNIQUE OF BUMPING

BUMPING: INSERT THE KEY

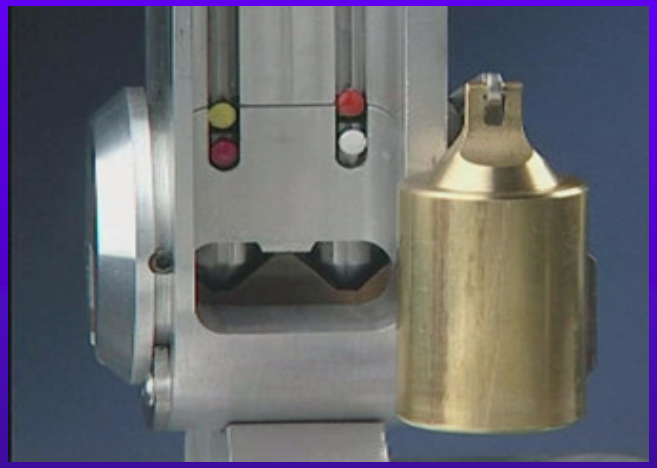


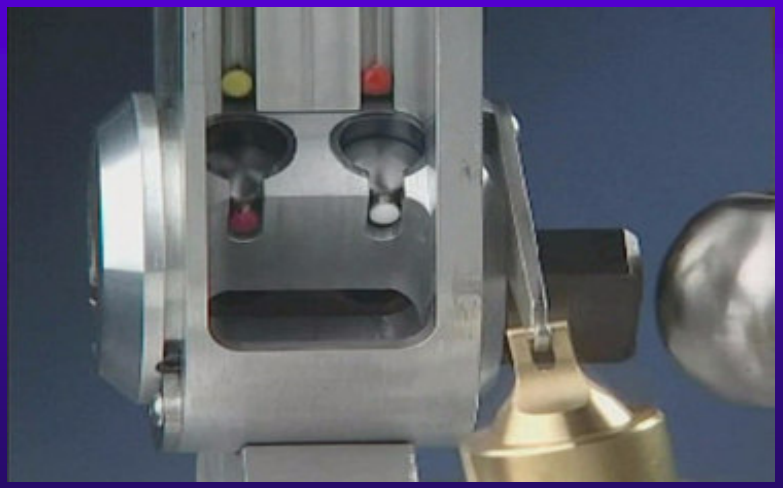
BUMPING: APPLY ENERGY



HOW BUMPING WORKS

- DOLEV MODEL



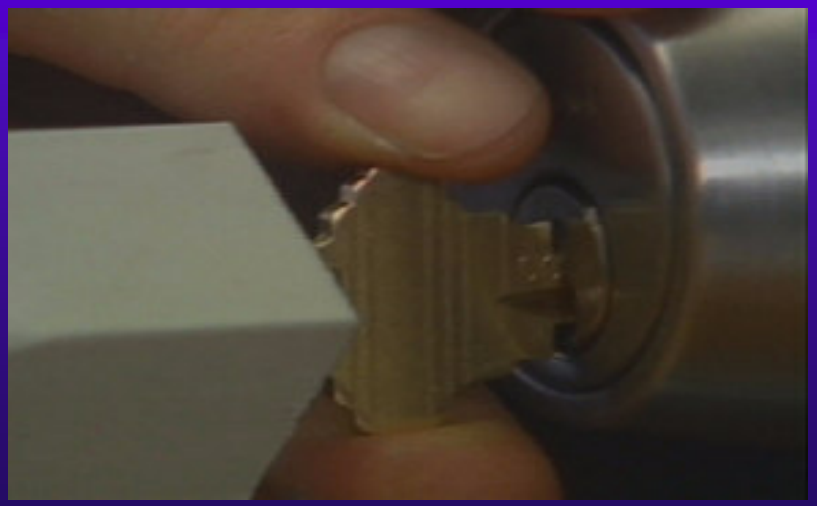


4: METHOD TO APPLY ENERGY

- STRIKE HEAD OF KEY
  - "TOMAHAWK"
  - SCREWDRIVER HANDLE
  - WOODEN OR PLASTIC MALLET
  - WOODEN STICK
  - OTHER TOOLS

5: TORQUE + TIMING

- TWO METHODS TO APPLY TORQUE
- REQUIRED TO TURN THE PLUG AT THE RIGHT MOMENT
  - TORQUE + ENERGY TO KEY
  - ENERGY TO KEY THEN TORQUE



6: TRAINING

- EASY TO LEARN
- LESS THAN ONE HOUR
- NETHERLANDS TESTS
- KELO-TV REPORTER, TEN SECONDS

BUMPING DEMONSTRATION

- INSERT BUMP KEY
  - TWO METHODS OF BUMPING
    - Withdraw one position and strike
    - Negative shoulder method
- APPLY TORQUE
- APPLY ENERGY TO HEAD OF KEY
- BOUNCE PINS
- TURN THE PLUG

MBE SECURITY: 5 SECONDS

HIGH SECURITY MANUFACTURERS: OUR LOCKS ARE "BUMP-PROOF" !

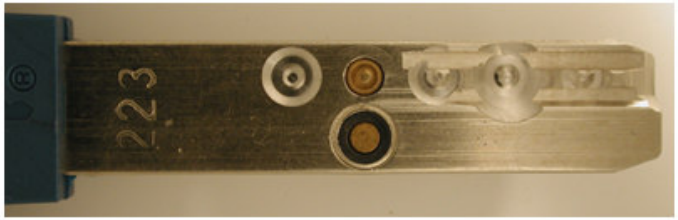
- Manufacturer's Claims:
  - Bumping does not work
  - Our locks are bump-proof
- Sidebar Locks that are Secure: Maybe
  - Medeco Biaxial and M3
  - Assa
  - Mul-T-Lock: Classic, 7x7, Interactive
  - Other Sidebar designs

HIGH SECURITY LOCK DESIGNS

KWIKSET

ASSA V10

SCHLAGE PRIMUS

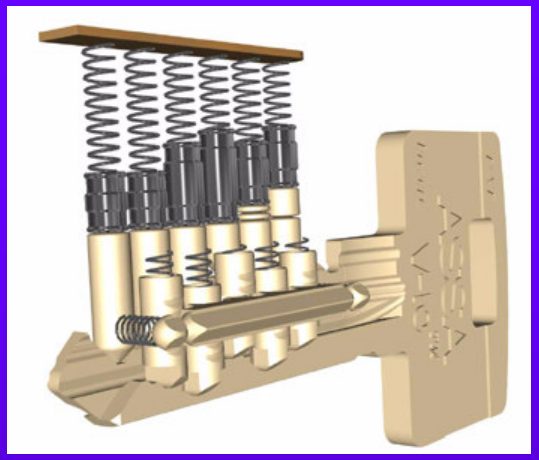


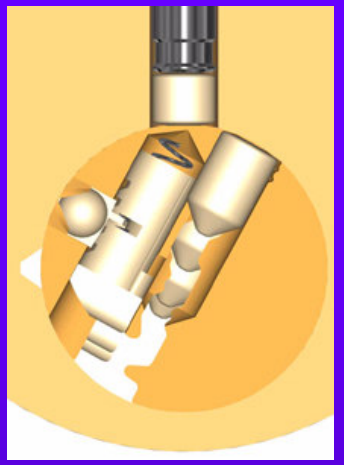
MUL-T-LOCK INTERACTIVE

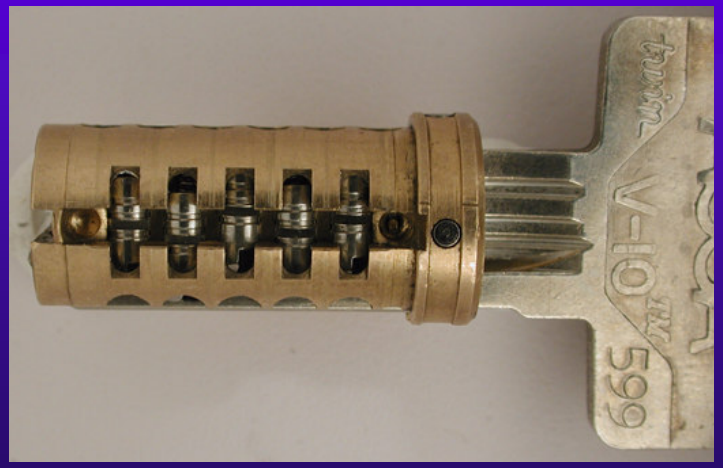
MEDECO BIAXAIL

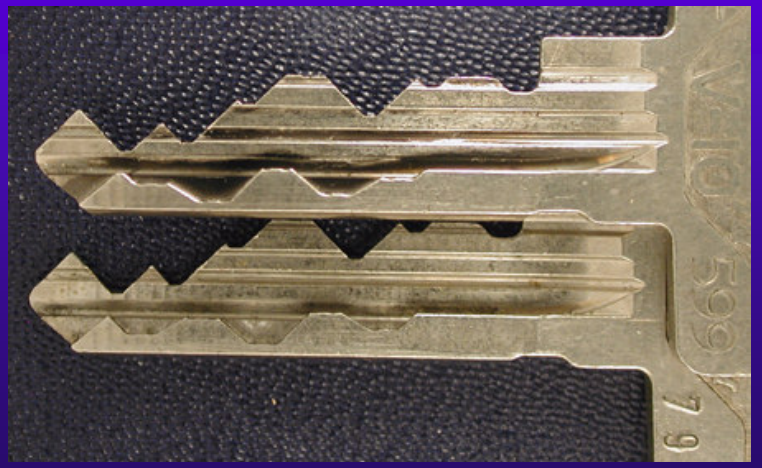
MUL-T-LOCK MT5

SIDEBAR LOCKS - ASSA



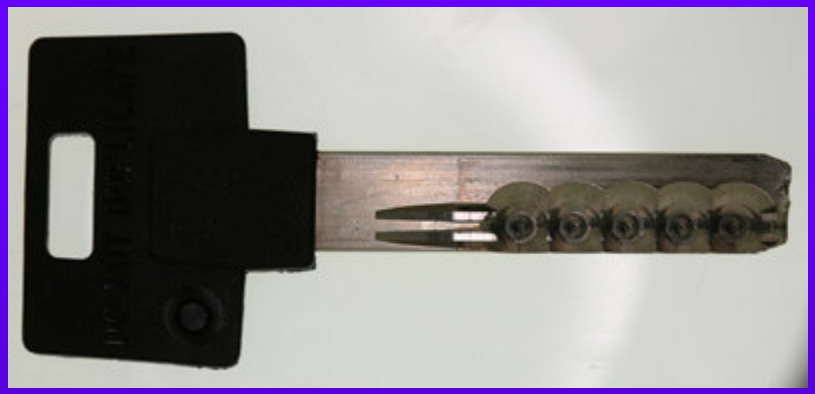


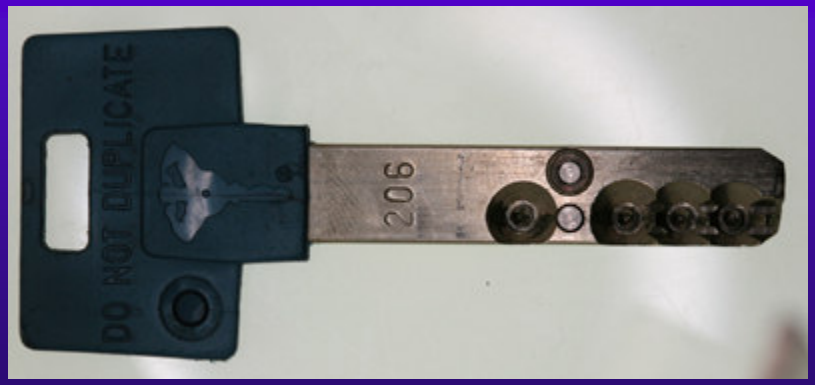




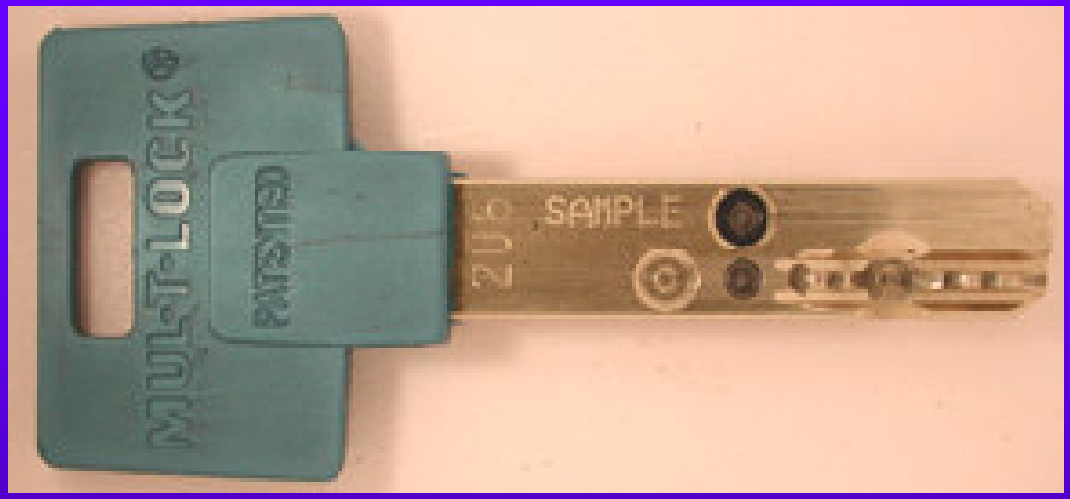
ASSA HIGH SECURITY?

MUL-T-LOCK HIGH SECURITY?





MUL-T-LOCK INTERACTIVE



MUL-T-LOCK MT5

GENERIC LOCKS THAT CANNOT BE BUMPED OPEN

- WARDED
- LEVER
- WAFER AND DISK WAFER
- COMBINATION

EVVA 3KS SLIDER

COMPLICATING FACTORS

- SECONDARY LOCKING MECHANISM
  - SIDEBARS
  - INTERACTIVE COMPONENTS
- DIRT AND DEBRIS
- SPECIAL PINS
- BROKEN SPRINGS
- PIN STACK LENGTH
- RESTRICTED BLANKS
- REQUIRES MORE THAN ONE MINUTE

U.S. LAWS

- 60 YEAR OLD FEDERAL STATUTE CONTROLS “NON-MAILABLE MATTER”
- SOME JURISDICTIONS: NO LAWS
- BUMP KEYS EXEMPTED
- INTERNET SITES SELLING PRE-CUT BUMP KEYS AND “TOMAHAWK”

PREVENTING BUMPING

- SPECIAL PINS AND MECHANISMS
- SECONDARY SECURITY: SIDEBARS
- SPRING BIAS DIFFERENCE
- SHORTER BORES
- EMPLOY CERTAIN HIGH SECURITY LOCKIS

NEEDED LEGISLATION

- PREVENT TRAFFICKING IN PRE-CUT BUMP KEYS
- CHANGE POSTAL REGULATIONS

MK SYSTEM DESIGN

- Most are easy to compromise
- Extrapolation: What is it?
- 3T-2R Rule
- Types of locks
- Restricted keyways
- Advanced protection

© 2007 Marc Weber Tobias
mwtobias@security.org

ADDITIONAL REFERENCE MATERIAL

www.security.org

- **OPENING LOCKS BY BUMPING IN FIVE SECONDS OR LESS: IS IT REALLY A THREAT TO PHYSICAL SECURITY?**
  - www.security.org/bumping_040206.pdf
- **BUMPING OF LOCKS: LEGAL ISSUES IN THE U.S.**
  - www.security.org/bumping_legal_mwt.pdf

- ***Locks, Safes and Security: An International Police Reference,*** Marc Weber Tobias, 2001
- ***LSS+ The Multimedia Edition,*** 2006

www.toool.nl