LOCKS AND HIGH INSECURITY:
PROTECTING CRITICAL INFRASTRUCTURE

SECURITY VULNERABILITIES FOR MECHANICAL AND ELECTRONIC LOCKING SYSTEMS THAT ARE USED FOR PROTECTING CRITICAL ASSETS

CRITICAL FACILITIES

- TRANSPORTATION
  - AIRPORTS AND AIRPLANES
- FINANCIAL AND BANKING
- COMPUTRE SERVER CENTERS
- POWER GENERATION
- COMMUNICATIONS
- DEFENSE
- PUBLIC SAFETY

HIGH SECURITY FACILITIES: HIGHER THREAT LEVEL

- INTRUSION
- SABOTAGE and VANDALISM
- THEFT OF CRITICAL AND HIGH-VALUE ASSETS
- TERRORISM
- ACCESS TO INFORMATION
- IDENTITY THEFT
- INTERRUPTION OF CRITICAL ESSENTIAL SERVICES

LEGAL REQUIREMENTS:
STATE, FEDERAL, REGULATORY

- FEDERAL STATUTES AND REGULATIONS
- STANDARDS COMPLIANCE
- COMMERCIAL AND INSURANCE
- DEFENSE DEPARTMENT
- DEPARTMENT OF ENERGY
- BANKING AND TREASURY

LOCKS: FIRST LINE OF DEFENSE

CONVENTIONAL AND HIGH SECURITY

- LOCKING SYSTEM: CATEGORIES
  - MECHANICAL
  - ELECTRO-MECHANICAL
  - ELECTRONIC
- TREND: PHYSICAL SECURITY + I-T
- RELIANCE ON STANDARDS BY MOST FACILITIES TO SELECT WHICH LOCKS ARE SECURE ENOJUGH

STANDARDS: THE PROBLEM

- WHAT DO THEY MEASURE?
- WHY WE NEED STANDARDS
- NOT “REAL WORLD”
- LIMITED PROTOCOL, FEW TESTS
- MECHANICAL BYPASS
- SPECIAL ATTACK TECHNIQUES FOR CERTIFIED LOCKS
- LOCK BUMPING
- KNOWLEDGEABLE ATTACKS

LOCKS: SECURITY CRITERIA

- **STANDARDS DEFINE CONVENTIONAL AND HIGH SECURITY**
- THREAT CRITERIA
  - FORCED ENTRY
  - COVERT ENTRY
  - KEY CONTROL
- STANDARDS ARE BASED UPON:
  - TIME, TOOLS, TRAINING

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

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

STANDARDS: KEY CONTROL v. KEY SECURITY

- STANDARDS = LIMITED SECURITY
- ORGANIZATIONAL PROTECTION
  - DUPLICATION OF KEYS
  - KEYS BY CODE ON ORDER
- LEGAL PROTECTION
  - AVAILABILITY OF BLANKS
- NOT ADDRESS TECHNICAL SECURITY OF KEYS

CATEGORIES OF LOCKS

- CONVENTIONAL MECHANICAL LOCKS
- HIGH SECURITY MECHANICAL LOCKS
- ELECTRONIC CREDENTIALS
  - ELECTRO-MECHANICAL LOCKS
  - ELECTRONIC LOCKS
  - WIRED, WIRELESS, DATA ON CARD

LOCKS AND SECURITY: 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

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

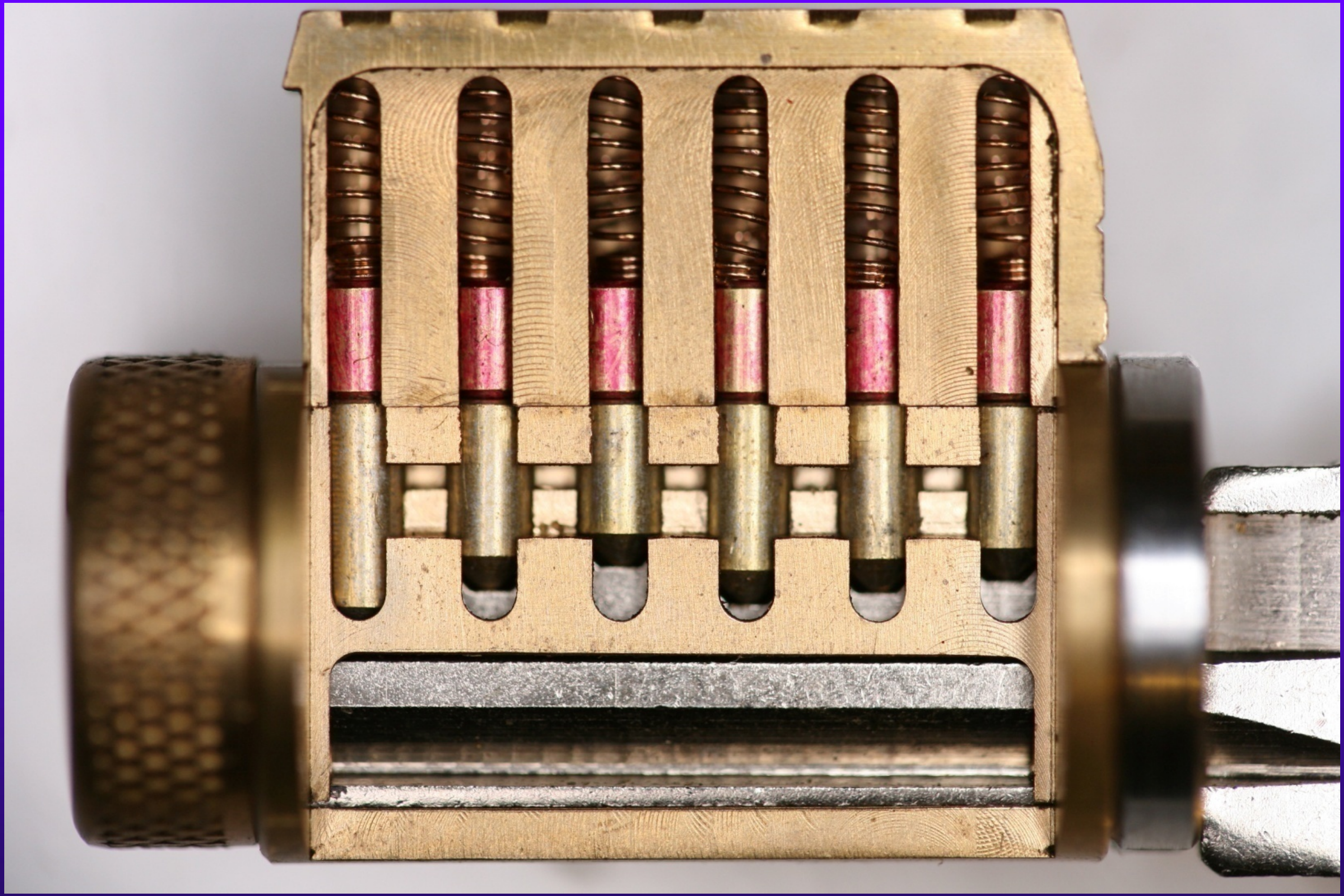
ALL MECHANICAL LOCKS: DESIGN LIMITATIONS

- GOOD FOR ONE PERSON, ONE KEY
- DON’T NEED TRACKING
- ADDING AND DELETING KEYS TO SYSTEM NOT AN ISSUE
- LOST, STOLEN OR COPIED KEYS, NO SECURITY
- MANIPULAITON OF KEYS: MUL-T-LOCK AND KEY INTERCHANGE

CONVENTIONAL LOCKS: THEIR FUNCTION

- RESTRICT WHO CAN ENTER
- PREVENT OR DELAY UNAUTHORIZED ACCESS
  - LOW TO MEDIUM SECURITY
  - NOT CERTIFIED
  - COVERT ENTRY OFTEN EASY

CONVENTIONAL LOCK: MODERN PIN TUMBLER



CONVENTIONAL LOCKS: VULNERABILITIES

- PICKING, BUMPING, DECODING
- KEY JIGGLING
- IMPRESSIONING
- MASTER KEY EXTRAPOLATION
- MECHANICAL BYPASS
- FAILURE OF KEY CONTROL
  - DUPLICATION OF KEYS
  - SIMULATION OF KEYS
  - REPLICATION OF KEYS

CONVENTIONAL LOCKS: WHY THEY ARE NOT ADEQUATE

- NO TRACKING OF ACCESS, ATTEMPTS, HOW OFTEN, WHEN
- ADD AND DELTE KEYS
- KEY SECURITY
- MASTER KEY SYSTEM INSECURITY
- NO EVIDENCE OF BREACH
- NO INTELLIGENCE IN LOCK OR KEY

HIGH SECURITY LOCKS: INCREASED PROTECTION?

- 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
  - Higher key control

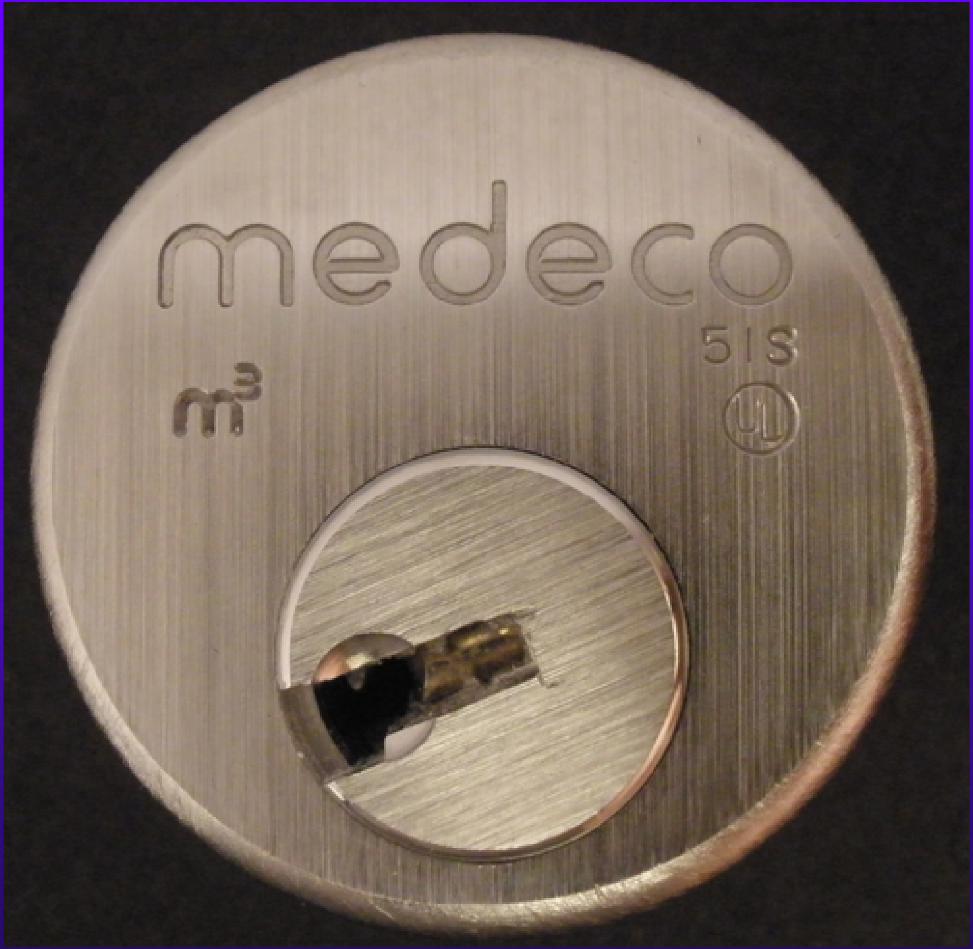
HIGH SECURITY MECHANICAL LOCKS: PRIMARY FUNCTIONS

- RESTRICT ACCESS
- ADDED RESISTANCE TO FORCED, COVERT ENTRY, AND KEY CONTROL
- NO ABILITY TO:
  - TRACK PEOPLE AND THEIR ACCESS
  - TRACK ENTRY AND ATTEMPTS
  - CONTROL ACCESS BY TIME, DATE, USER GROUP

HIGH SECURITY LOCKS: Critical Design Differences

- 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: WAS THE U.S. MODEL FOR HIGH ECURITY



MEDECO: WHO ARE THEY and WHY IMPORTANT?

- 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

MEDECO HIGH SECURITY: What it is supposed to mean

- 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

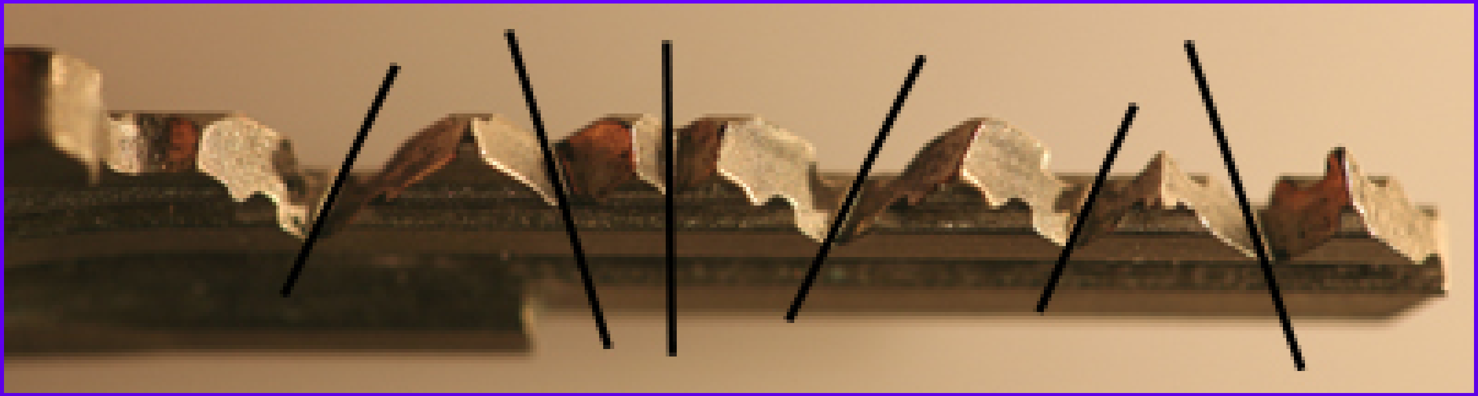
WHY THE MEDECO CASE STUDY IS IMPORTANT

- 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

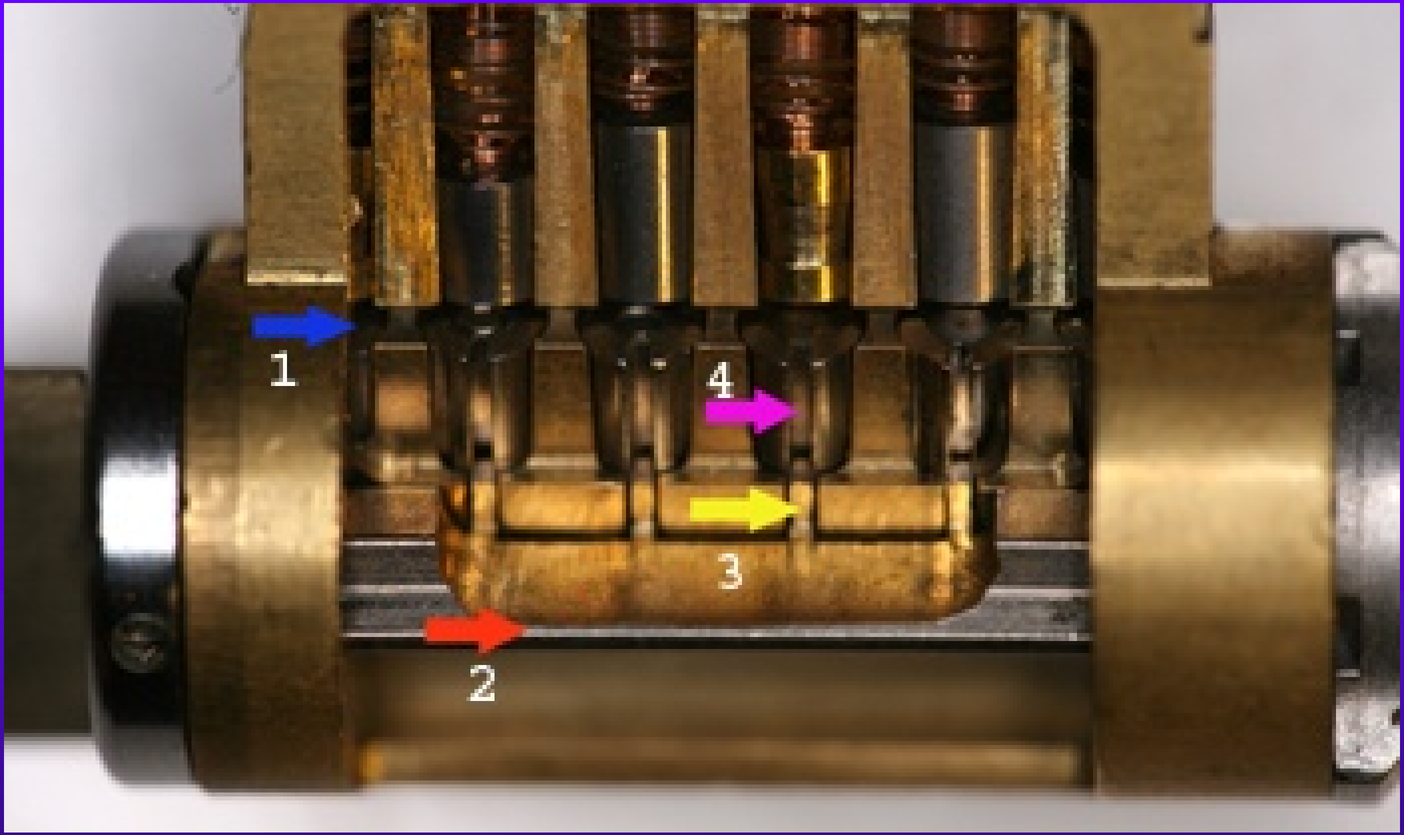
MEDECO LOCKS:
3 Independent Security Layers

- 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

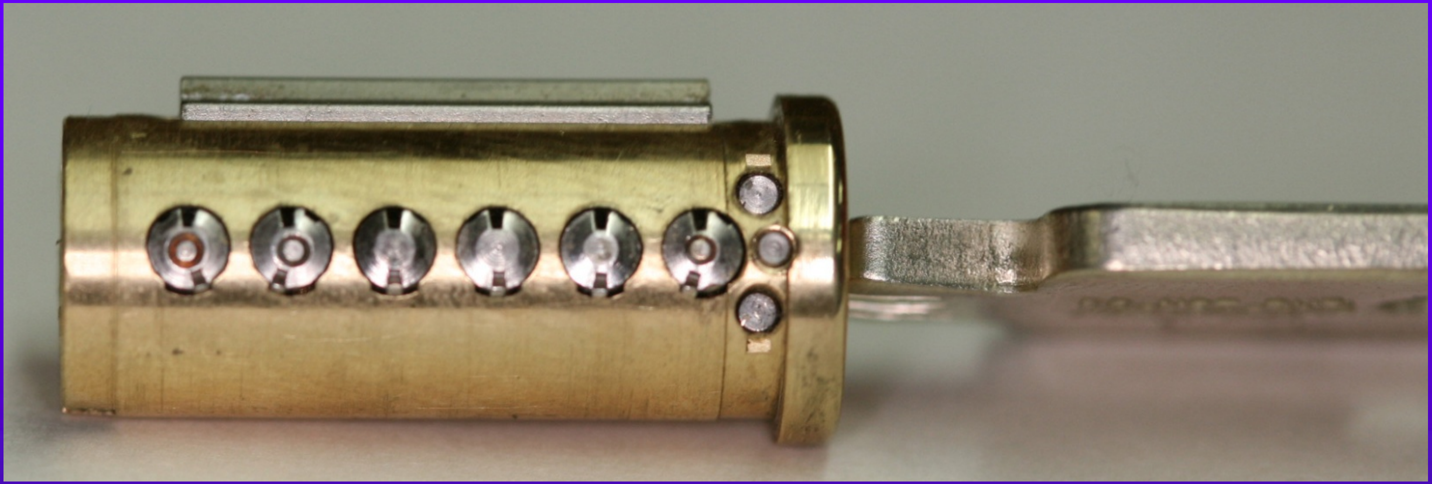
MEDECO TWISTING PINS: 3 Angles + 2 Positions



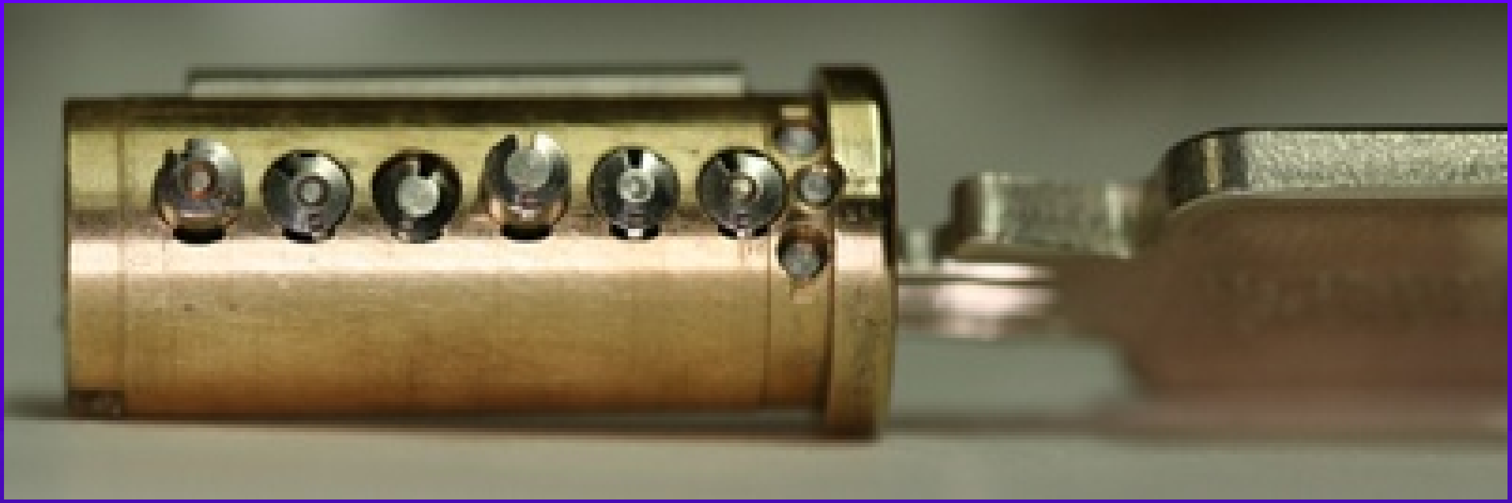
MEDECO BIAXIAL (1985-2003)



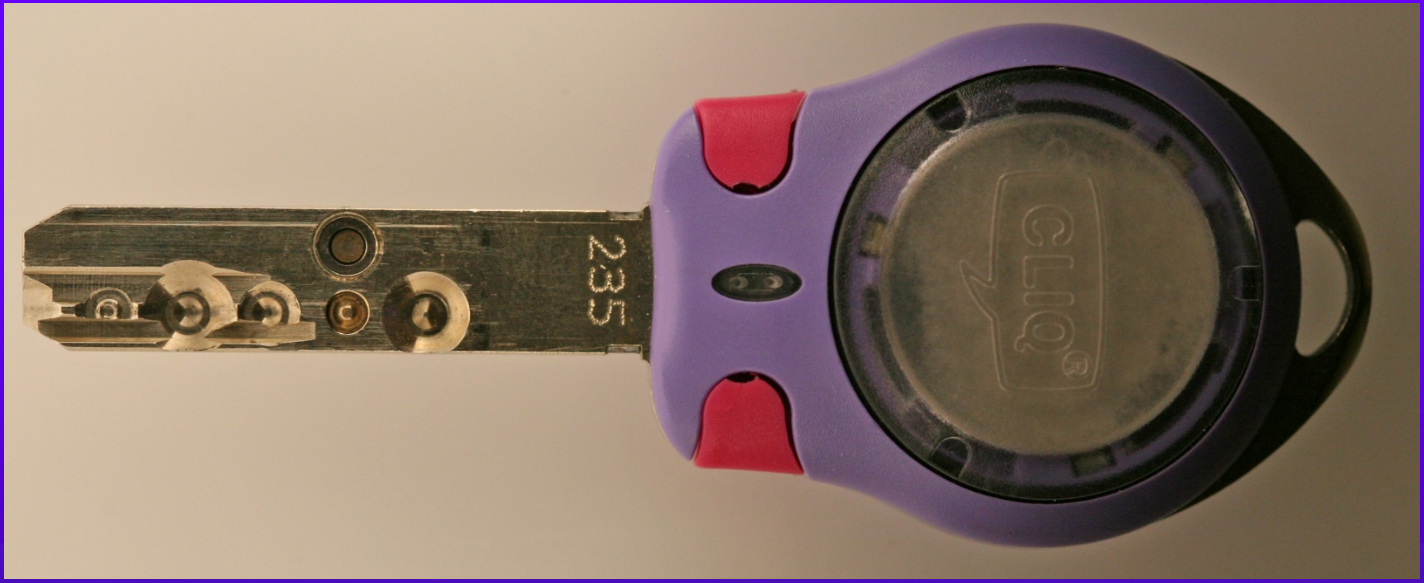
PLUG AND SIDEBAR: All pins aligned

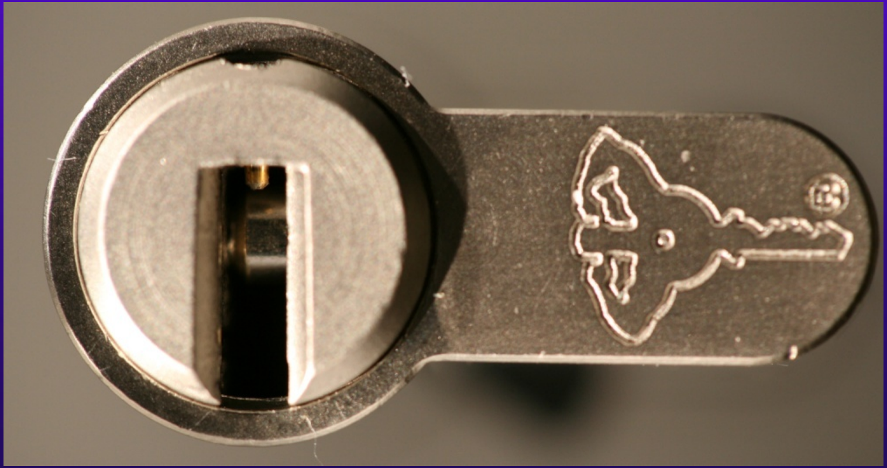


PLUG AND SIDEBAR: Locked



ELECTRONIC LOCKS: The Security Solution???





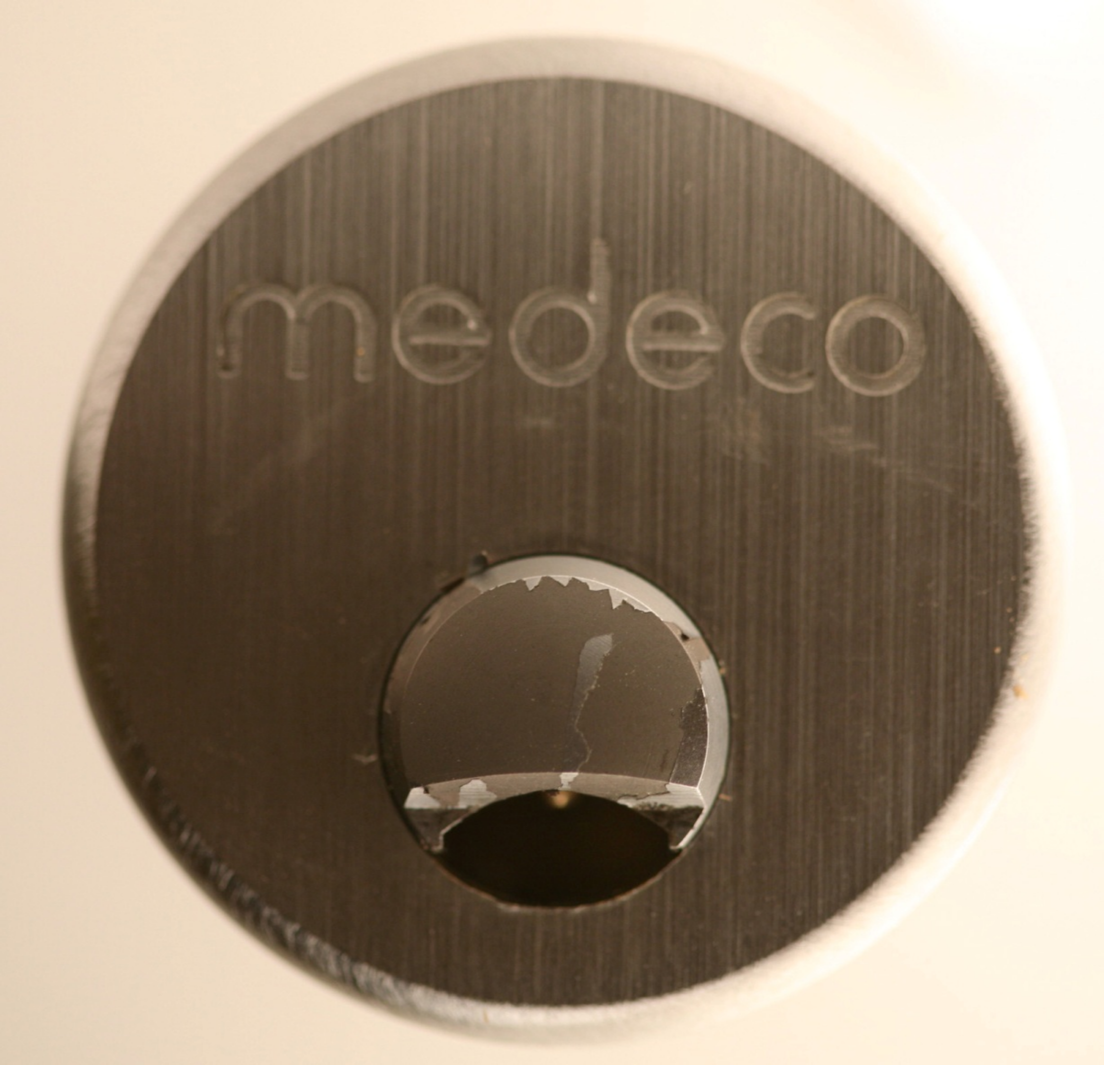
ELECTRO-MECHANICAL SELF-CONTAINED LOCKS

- MECHANICAL LOCKS +
- ELECTRONIC CREDENTIALS
  - STILL MECHANICAL LOCKS
- TWO PARALLEL LOCKING SYSTEMS
  - MECHANICALLY KEYED ALIKE
  - MECHANICALLY MASTER KEYED
  - KEY BITTING ASSIGNED TO EACH CUSTOMER

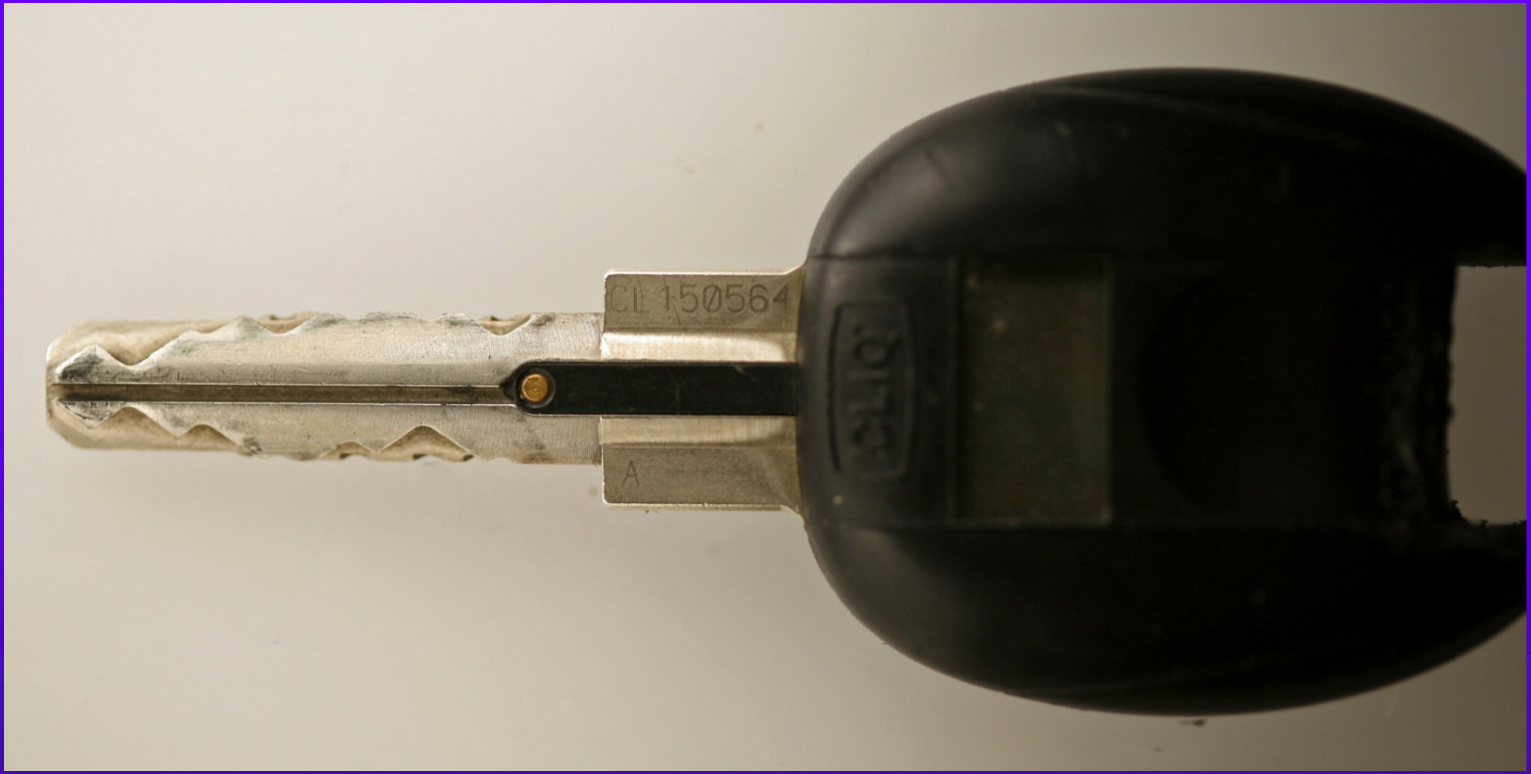
ELECTRONIC ACCESS CONTROL SYSTEMS

- MECHANICAL LOCK DESIGNS
- ELECTRONIC CREDENTIALS
  - I-BUTTON, RFID, SMART CARD
  - MANY DIFFERENT PROTOCOLS
- SECURITY LAYERS
  - PROTOCOL
  - MECHANICAL LOCKING SYSTEM
  - AUDIT FUNCTIONS
  - KEY SECURITY

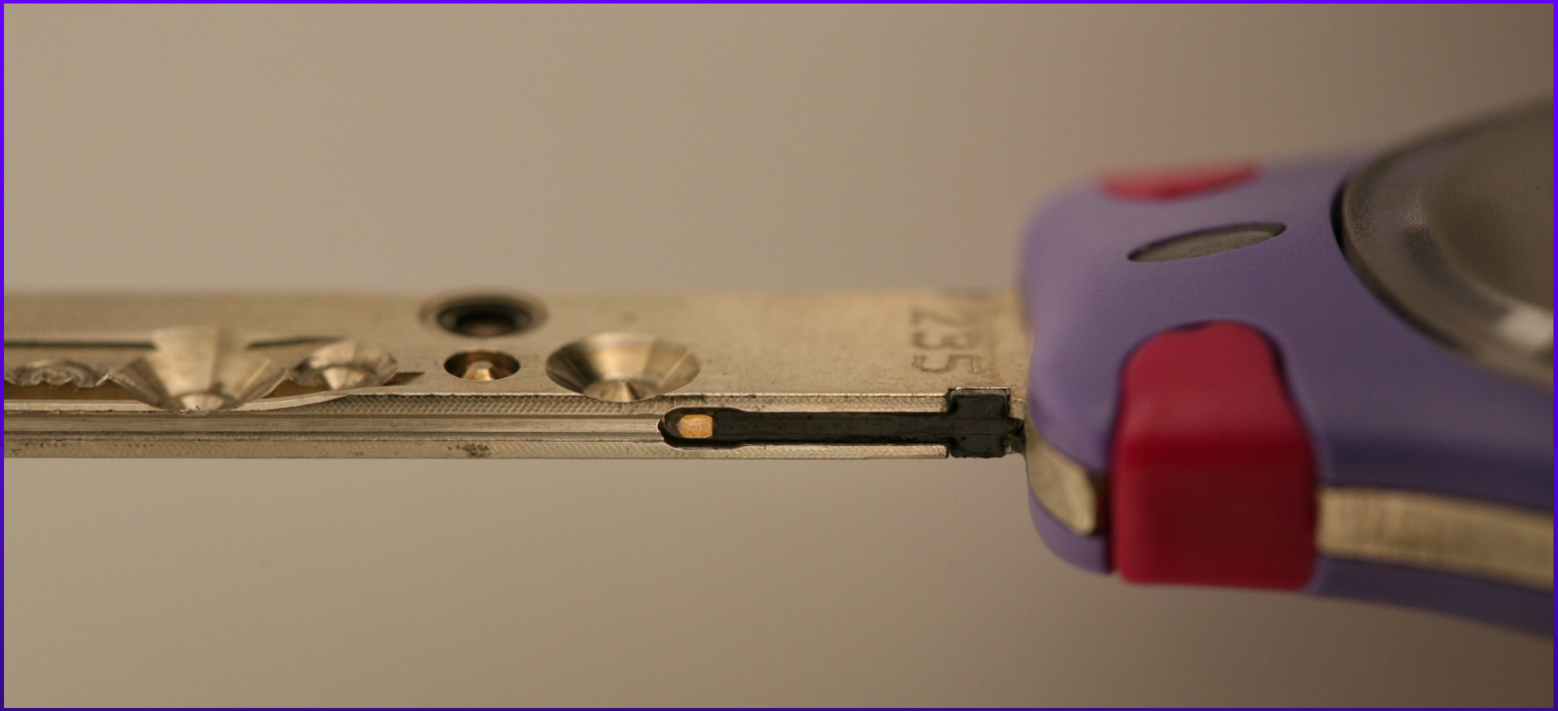
MEDECO LOGIC CYLINDER: HIGHER SECURITY?



MEDECO LOGIC KEYS



MUL-T-LOCK CLIQ: SIMILAR TECHNOLOGY



EAC: CRITICAL APPLICATIONS IMPLEMENTATION EXAMPLES

- AVIATION
- CARGO
- POWER
- COMPUTER SERVERS AND DATA PROTECTION

CRITICAL INFRASTRUCTURE: AIRPORTS AND AIRCRAFT

CRITICAL INFRASTRUCTURE: AIRCRAFT

U.S. LAWS AFTER 9-11: TRANSPORTATION SECURITY

- ♦ AVIATION TRANSPORTATION SECURITY ACT (2001)
- ♦ SECURITY OF AIRPORTS, HIGHWAYS, BUSSES, PORTS, MASS TRANSIT
  - – CONTROL PHYSICAL ACCESS TO 450 AIRPORTS
  - – CONTROL, TRACK, ANALYZE INDIVIDUAL ACCESS AND ATTEMPTS TO SECURE AREAS

AIRPORT SECURITY

- SECTION 106: AIRPORT PERIMITER PROTECTION
- SECURITY TECHNOLOGY TO MANAGE ACCESS CONTROL
- POSTIVIELY VERIFY THE IDENTIFY OF EACH EMPLOYEE AND LAW ENFORCEMENT OFFICER
- TEST AND ASSURE COMPLIANCE

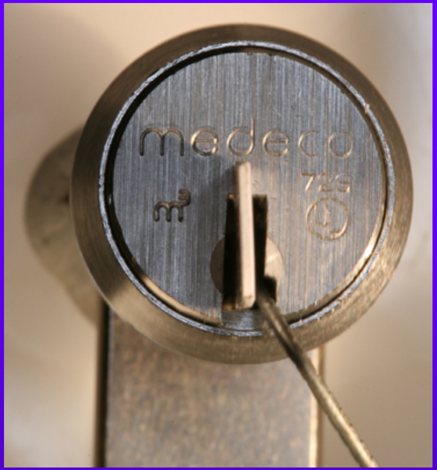
AIRPORT SECURITY

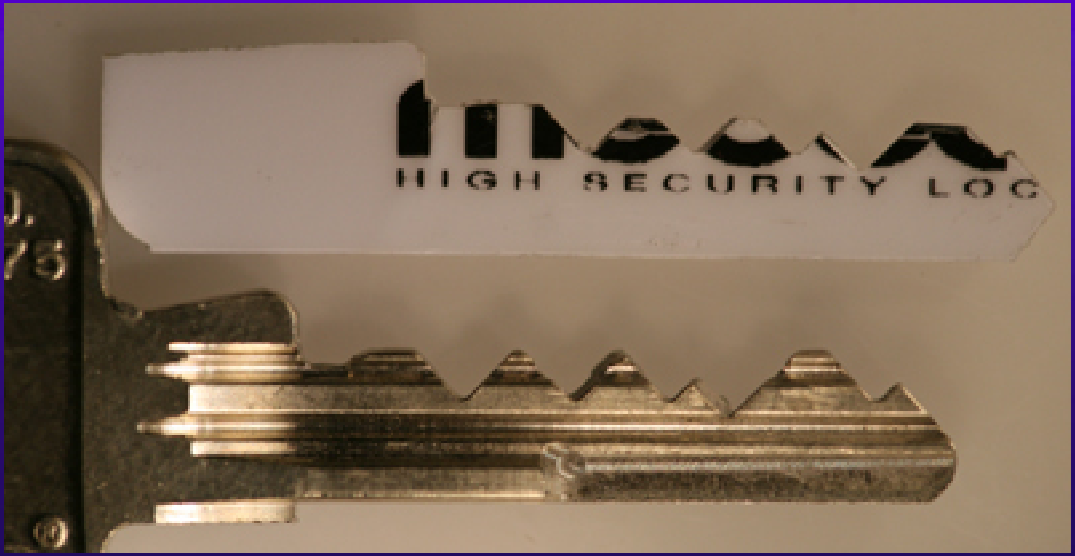
- LAYERED SECURITY APPROACH
- ACCESS CONTROL
- PHYSICAL SECURITY OF FIXED ASSETS
- BREACHES: TRACE TO LOCKS AND USER VIOLAITONS
- PREVENT COPYING OF KEYS

CONVENTIONAL LOCKS NOT SECURE FOR AIRPORT PROTECTION

- DUPLICATION OF KEYS OR CREDENTIALS
- NO AUDIT INFORMATION
- NO SECHEDULING OF PERSONNEL
- MASTER KEY SYSTEMS: NO IDENTIFICATION OF EMPLOYEE, NOR ABILITY TO TEST SYSTEM

PRIVATE AIRCRAFT: MEDECO CAM LOCKS



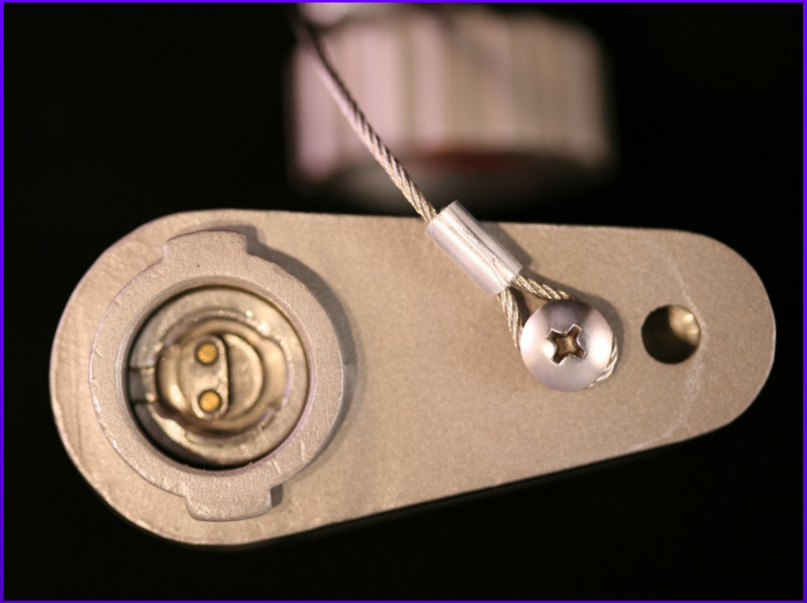


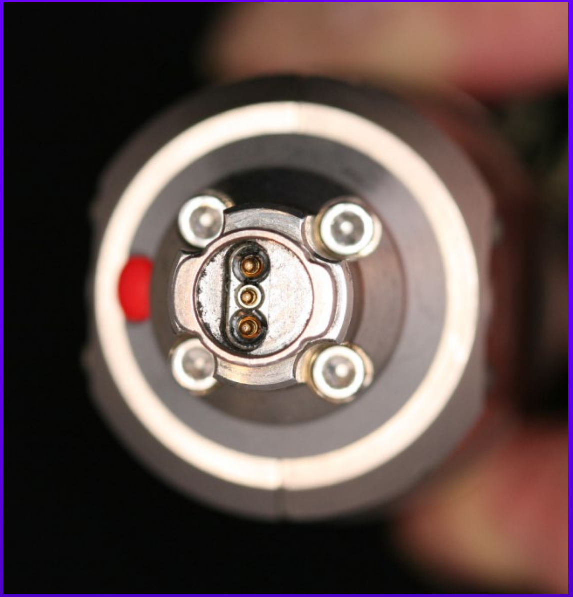
CRITICAL INFRASTRUCTURE: CARGO AREAS / CONTAINERS

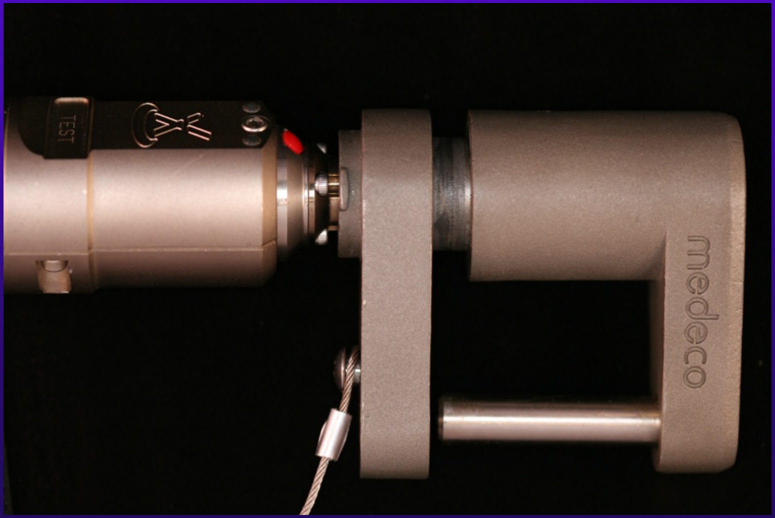
CARGO ACCESS

- ELECTRONIC ACCESS CONTROL SYSTEMS
- ELECTRONIC PADLOCKS WITH AUDIT CONTROL
  - DETERMINE TAMPERING
  - TERRORIST ACTS
  - CONTRABAND

MEDECO NEXGEN







CRITICAL INFRASTRUCTURE: POWER GENERATION

SECURITY REQUREMENTS

- PREVENT ATTACKS, PHYSICAL AND ELECTRONIC
- ACCESS TO DATA AND EQUIPMENT
  - HARD ASSETS: GENERATING PLANTS, EQUIPMENT, TRANSMISSION, NETWORKS
- PHYSICAL ACCESS AND ATTEMPTS

PREVENT UNAUTHORIZED ACCESS

- TERRORISTS, DISGRUNTLED FORMER EMPLOYEES, TEENAGERS
- DISRUPTION OF LOCAL OR NATIONAL POWER AND TRANSMISSION
- REMOTE ACCESS AND SABOTAGE
- PROBLEM: LOCAL OR REMOTE ACCESS

CRITICAL INFRASTRUCTURE: COMPUTER SERVER ROOMS

SERVER SECURITY AND MECHANICAL LOCKS

- ♦ MECHANICAL LOCKS: WILL NOT PROTECT ELECTRONIC DATA
- ♦ NOT ENOUGH SECURITY TO ALLOW MANAGEMENT TO “ASSESS AND EVALUATE” INTERNAL CONTROLS
- ♦ REQUIRES A SYSTEM
  - – RESTRICT ACCESS
  - – TRACK PEOPLE ACCESS
  - – ENTRY AND ATTEMPTS

PROTECTION OF FINANCIAL DATA: SPECIAL NEEDS

- SARBANES-OXLEY ACT (2002)
  - FINANCIAL REPORTING FOR PUBLIC CORPORATIONS
  - QUALITY OF FINANCIAL REPORTING
  - INTERNAL CONTROLS
  - SERVER ROOM ACCESS SECURITY
- SECURITY
  - FOR CORPORATION
  - FOR COMPLIANCE
  - FOR PUBLIC

SERVER SECURITY: PHYSICAL ACCESS

- PHYSICAL SECURITY IS VITAL
- EQUIPMENT AND INFORMATION
- PREVENT SERVER THEFT
- MECHANICAL LOCKS NOT SUFFICIENT

- KEY CONTROL AND KEY SECURITY
- LOG ACCESS
- **SERVER ROOM SECURITY BEGINS WITH CONTROLLING ACCESS TO FACILITY**

FAILURE TO PROTECT SERVERS AND DATA

- THEFT OF PERSONAL DATA
- THEFT OF SERVERS AND COMPUTERS
- SIGNIFICANT LIABILITY TO ACCOUNT HOLDERS
- COMPROMISE OF CLASSIFIED DATA

FAILURE OF SECURITY: POSSIBLE RESULTS

- INTERRUPTION OF SERVICES
- SABOTAGE, UNAUTHORIZED ACCESS
- LOSS OF LIFE
- COMPROMISE OF CRITICAL DATA
- DESTRUCTION OF FACILITIES AND EVIDENCE
- TERROR ATTCKS
- EXTENSIVE LIABILITY
- CRIMINAL ACTIVITY, THEFT, COLLUSION

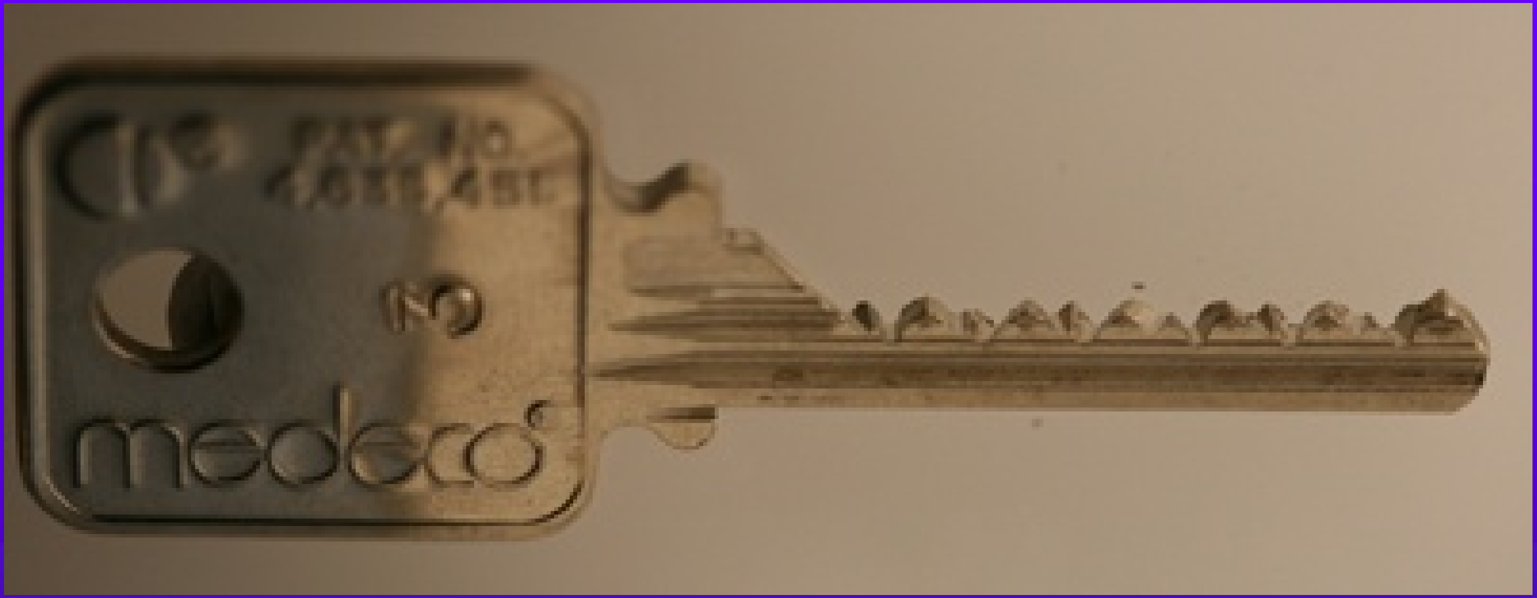
METHODS OF ATTACK: High Security Mechanical Locks

- 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

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

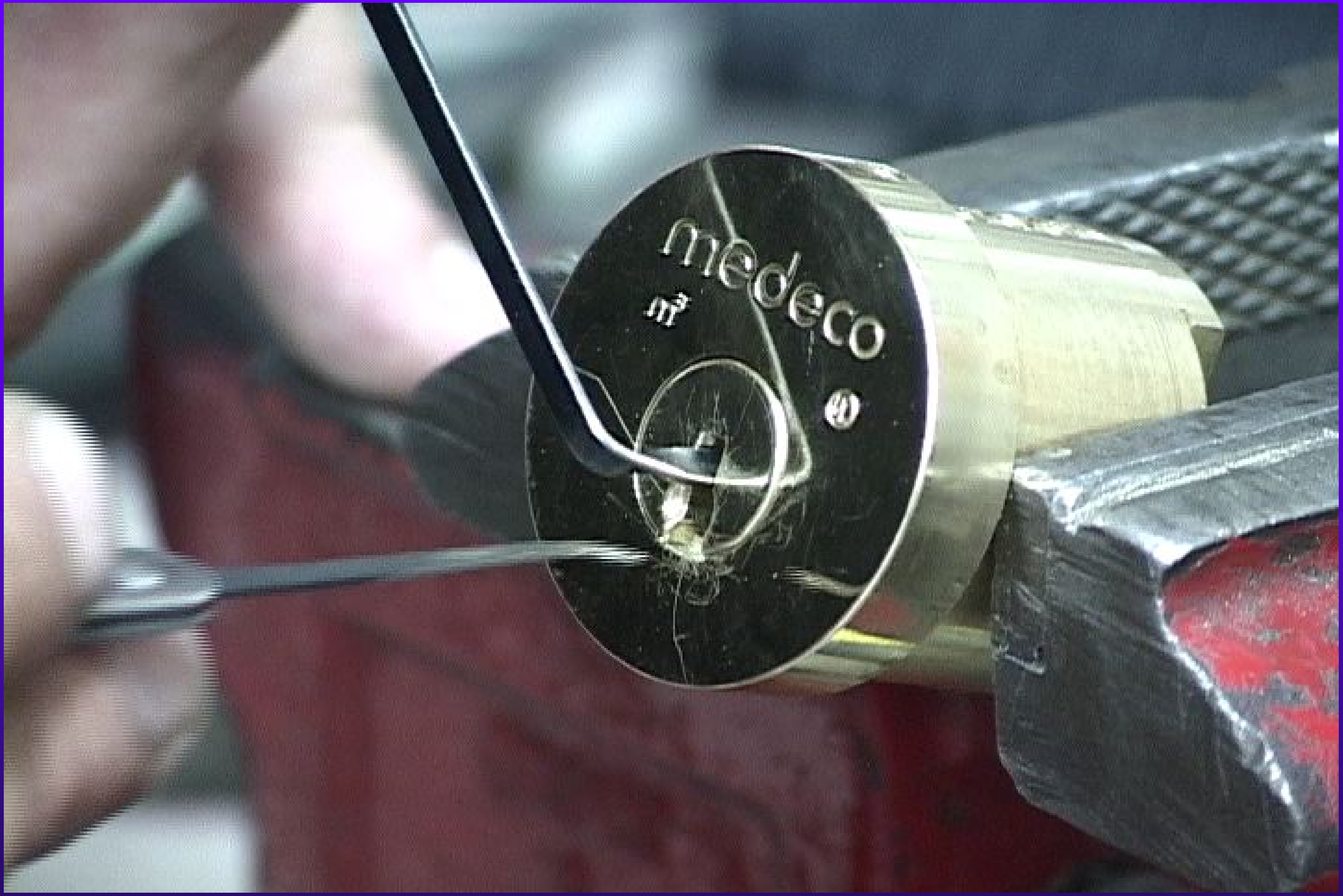
MEDECO BUMP KEY



REAL WORLD ATTACK: Bumping a Medeco Lock

FEBRUARY, 2009: WIRED MAGAZINE BUMPING TEST

PICKING A MEDECO LOCK



MEDECO PICKING: OPEN IN 23 SECONDS

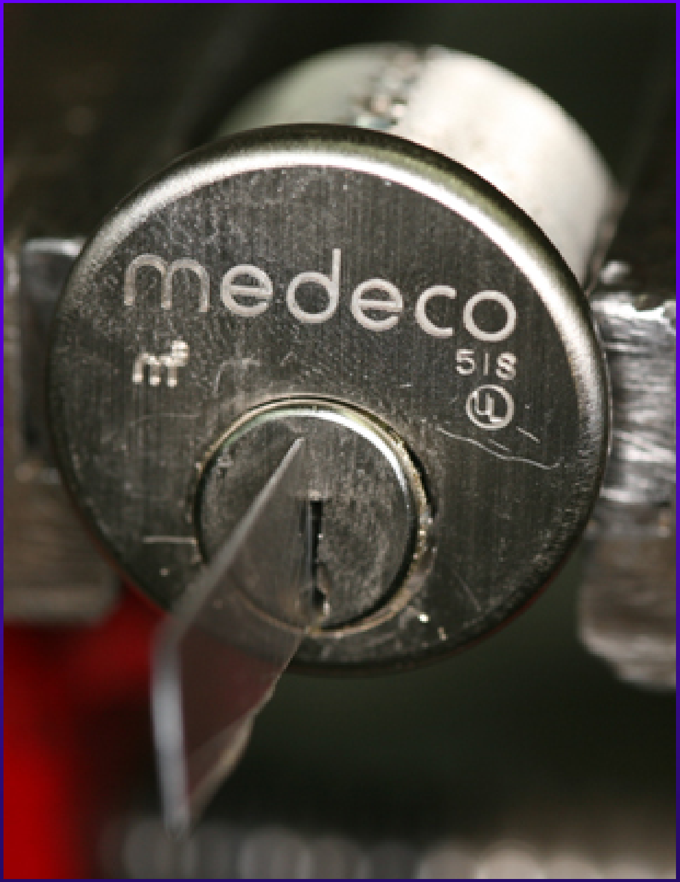
MEDECO INSECURITY: Real World Threats – Forced

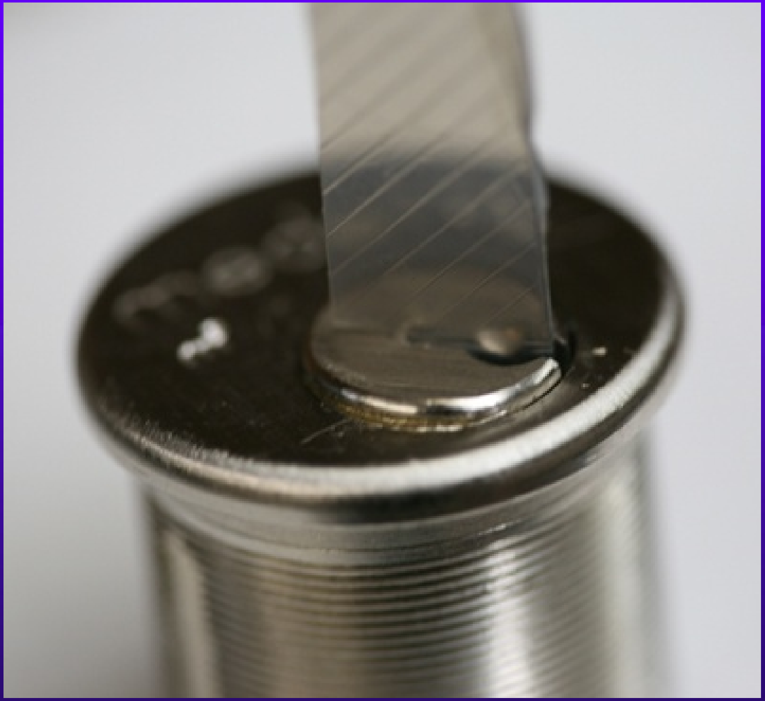
- DEADBOLT Pre-12/2007
  - Thirty seconds
  - Complete circumvention of security
  - Simple tools, easy to accomplish
- DEADBOLT 2008
  - Reverse picking attack
- MORTISE, RIM, ICORE
  - Hybrid attack, compromise of key control

DEADBOLT ATTACK

MORTISE CYLINDER

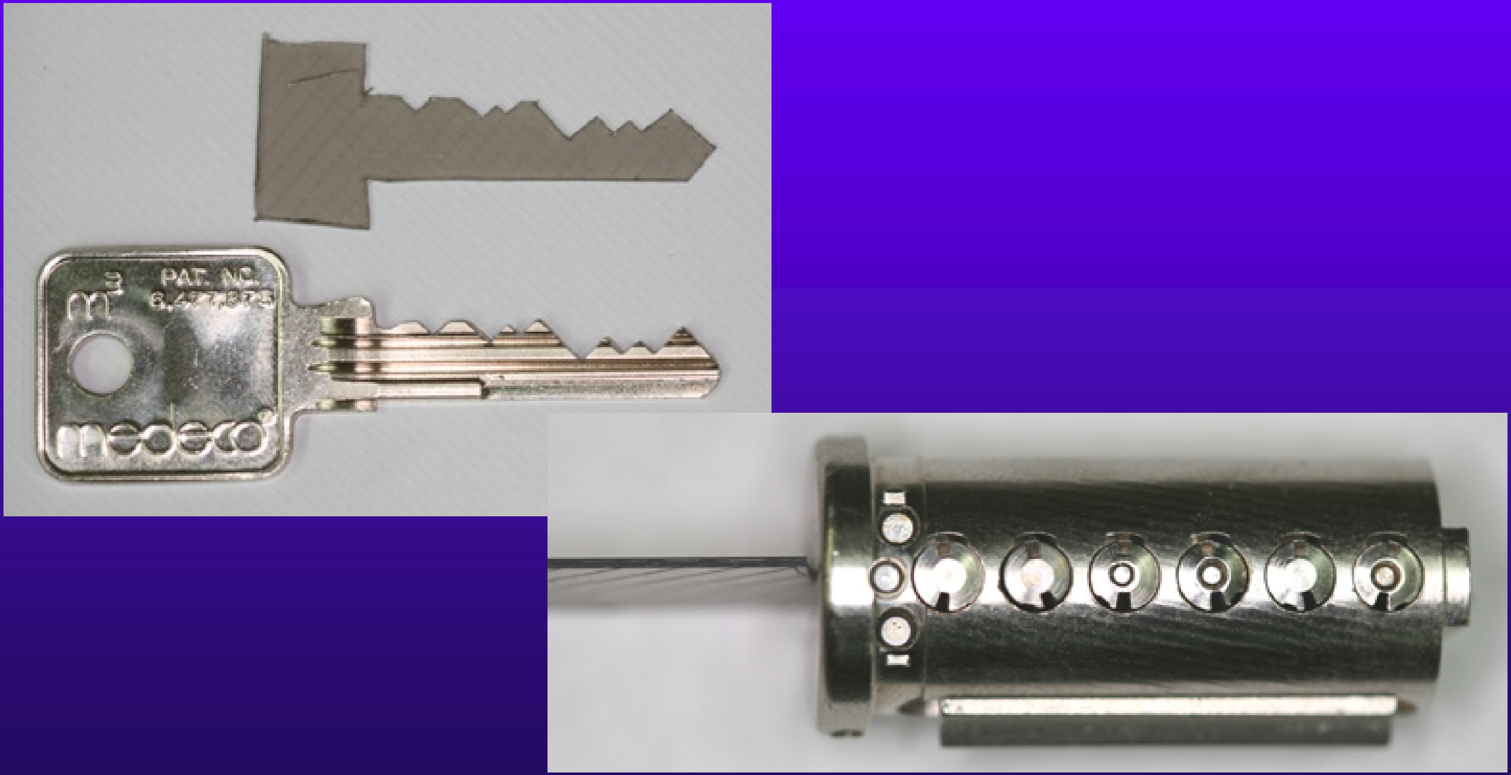
SET THE SHEAR LINE: OPEN THE LOCK



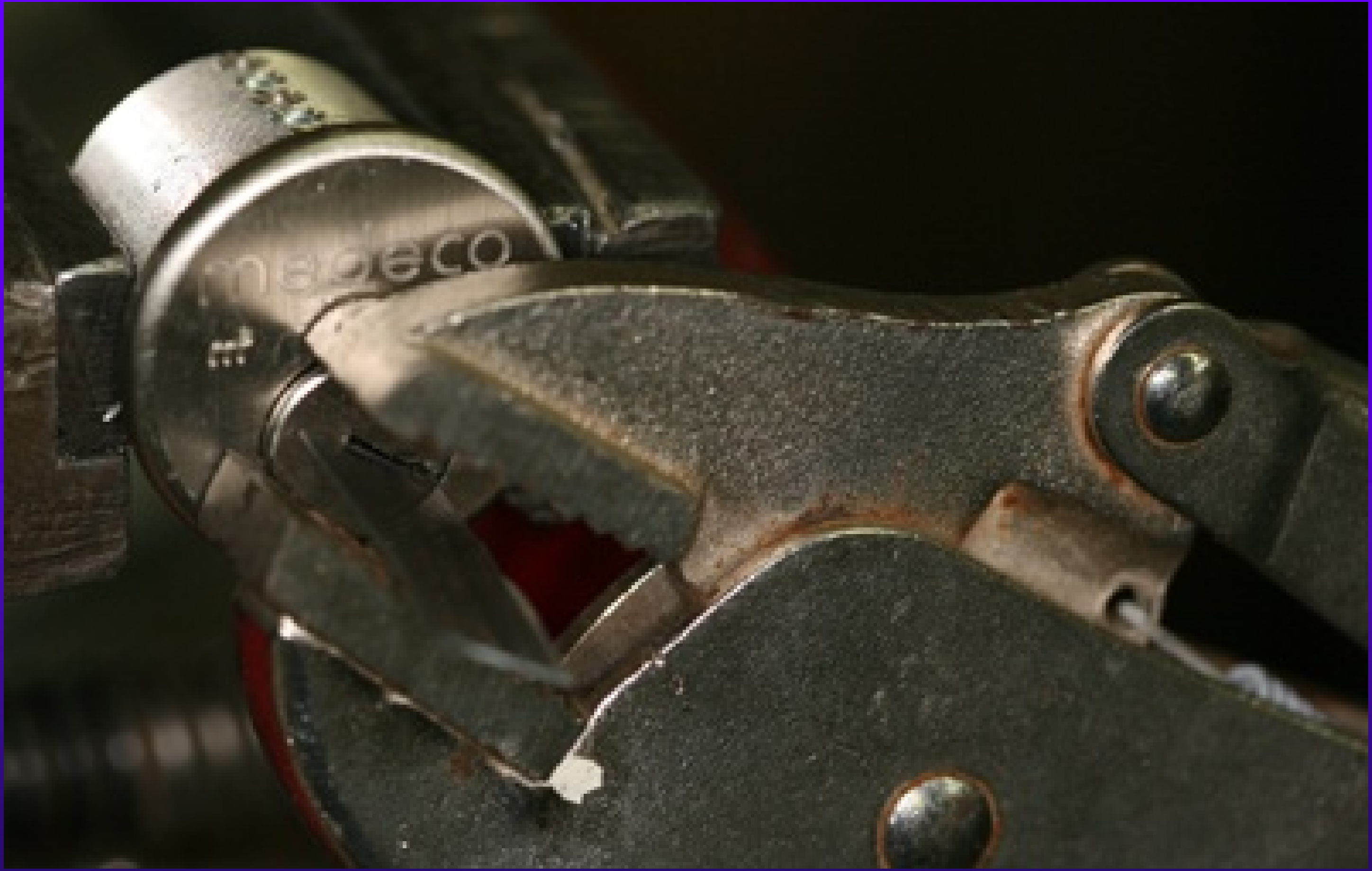


SET THE SHEAR LINE

- PLASTIC KEY SETS SHEAR LINE
- SIDEBAR IS IRRELEVANT

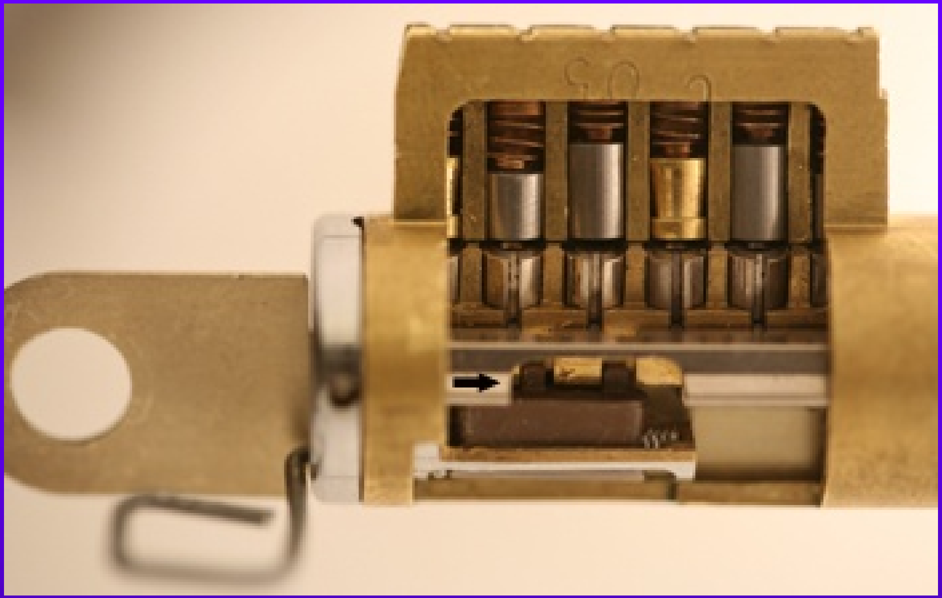


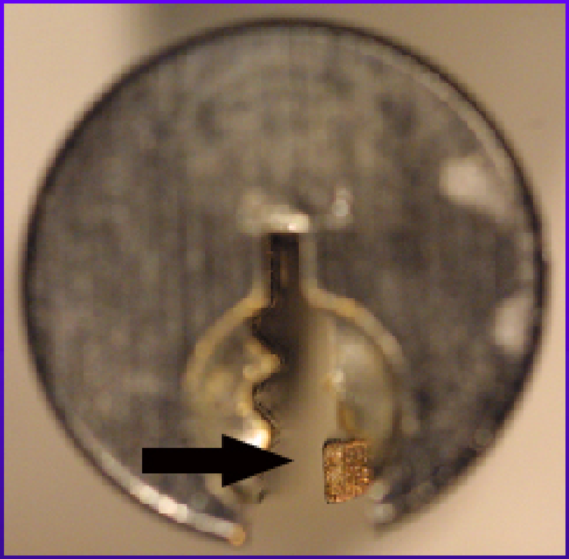
MORTISE ATTACK

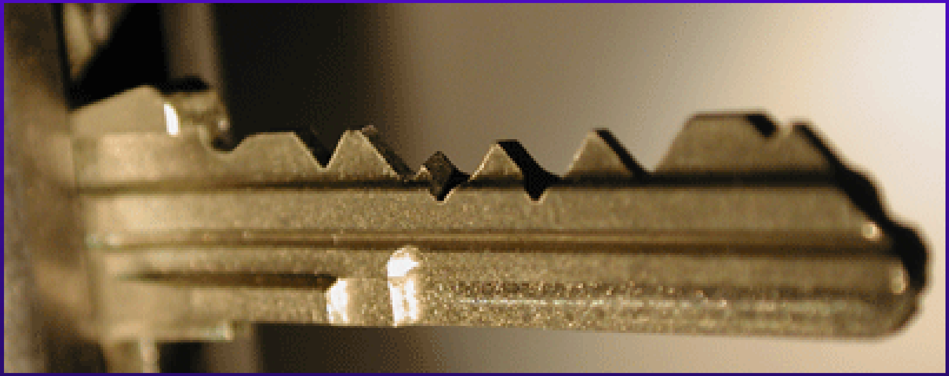


MEDECO MORTISE ATTACK: INSIDER KEY COMPROMISE

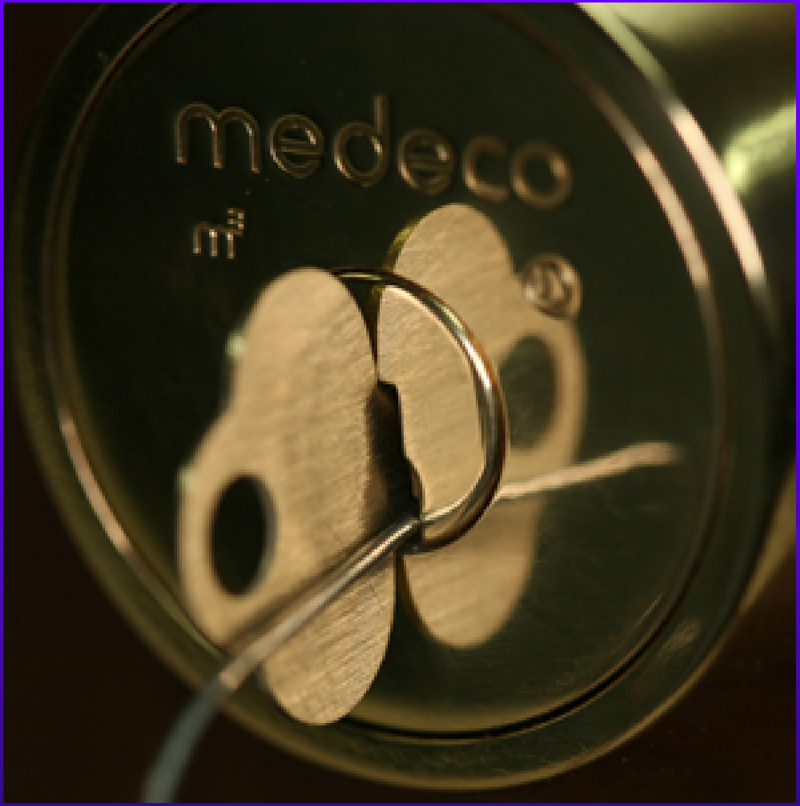
MEDECO m3: The Slider (2003)

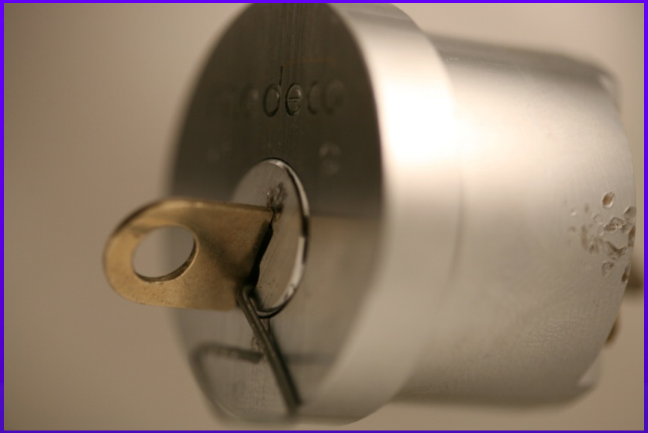






M3 SLIDER: (Not secure) Bypass with a Paper clip





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

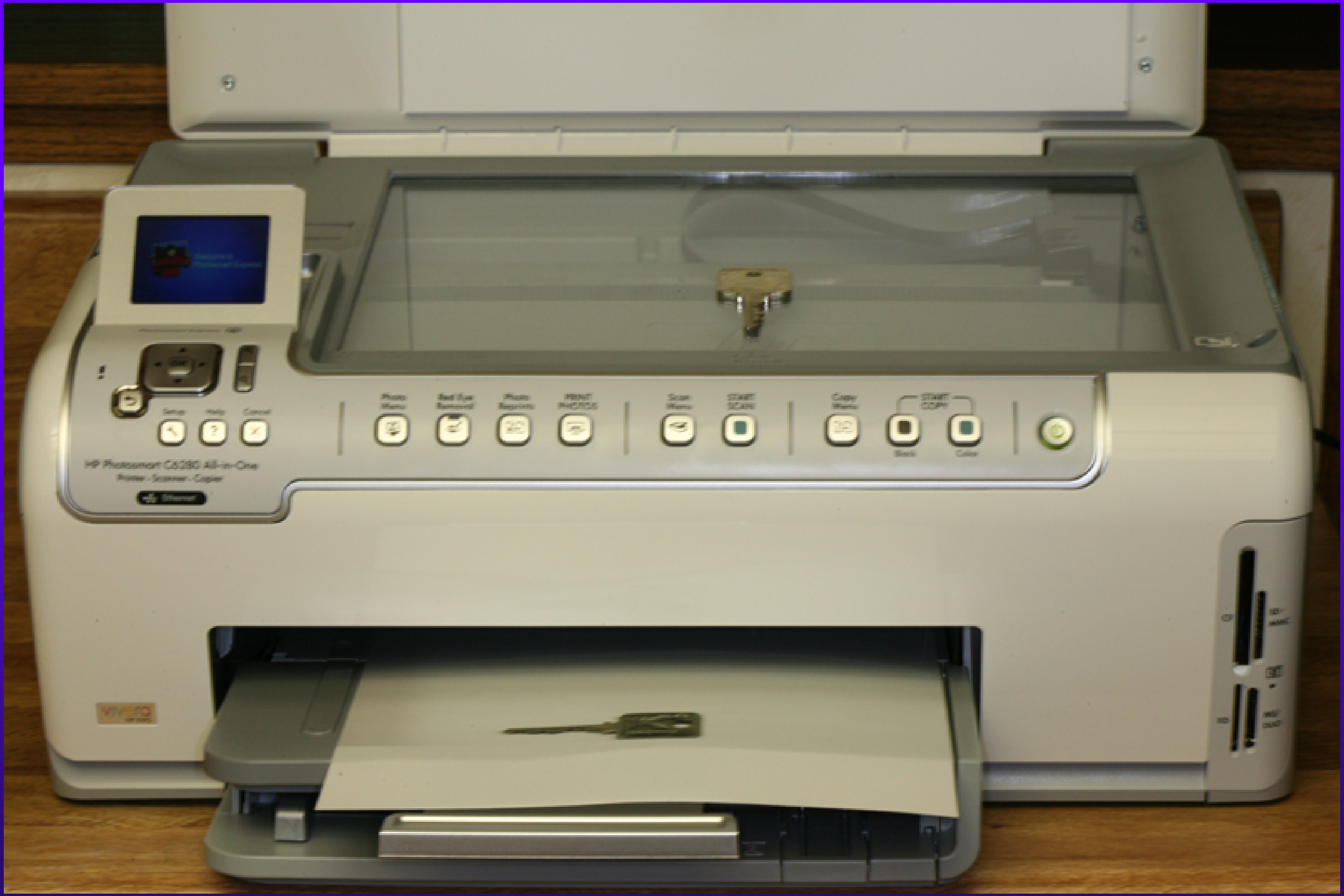
KEYS and KEY CONTROL

- KEYS ARE THE EASIEST WAY TO OPEN LOCKS
  - Change key or master key
  - Duplicate correct bitting
  - Bump keys
  - Rights amplification: modify keys

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

“KEYMAIL”: Security Threat from Within



KEYMAIL: How It Works

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

→ 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

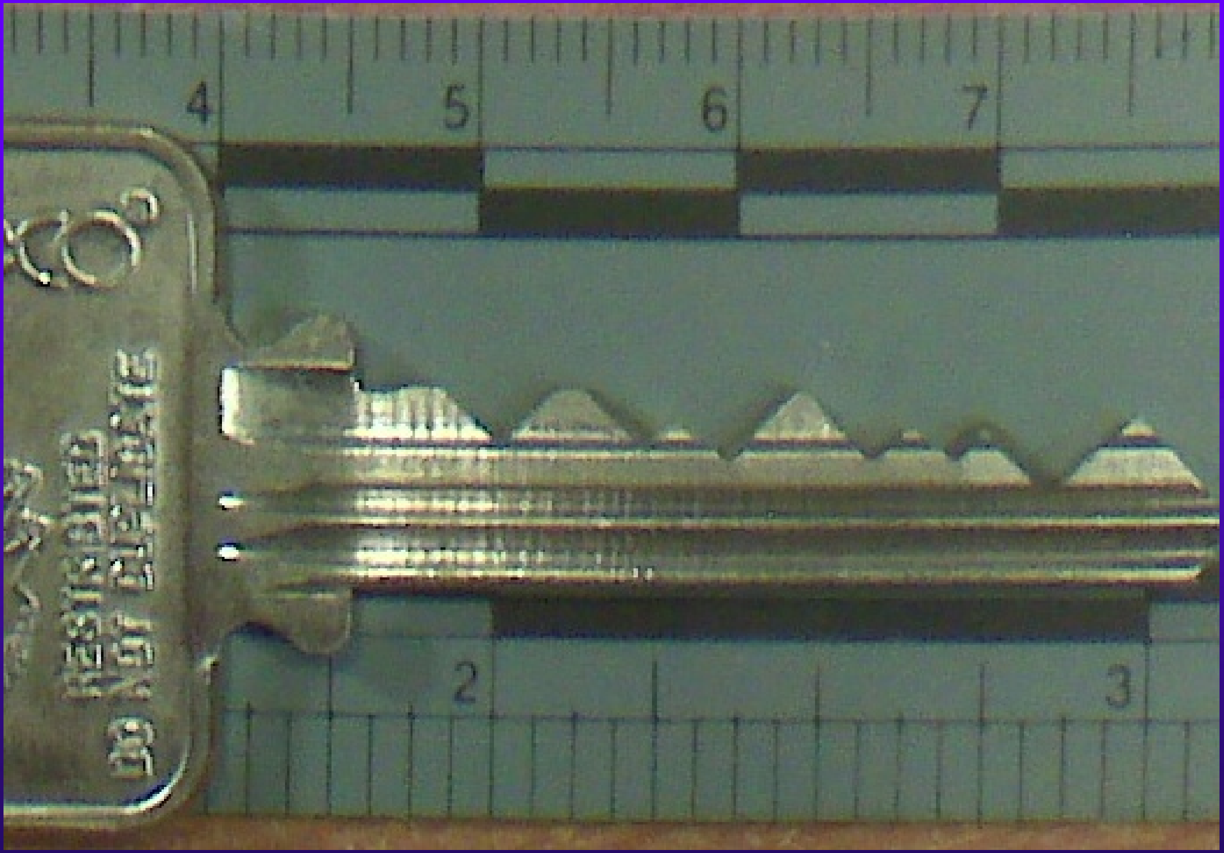
→ OBTAIN DATA: COPIER OR SCANNER

OBTAIN DATA

- CELL PHONE

OBTAIN DATA: BLACKBERRY CAMERA

- CAPTURED IMAGE

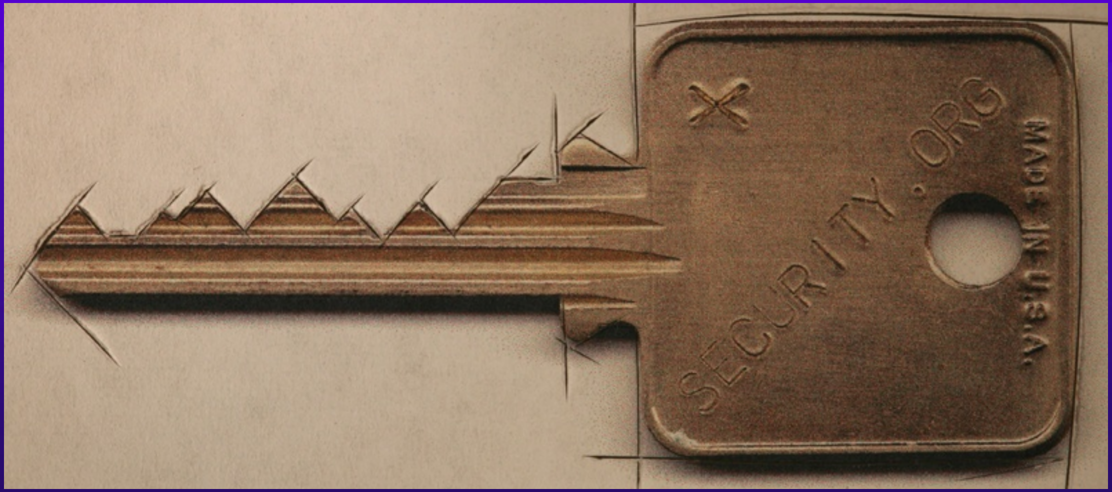


→ RESULTING IMAGE

- 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

→ CUT A FACSIMILE OF KEY

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

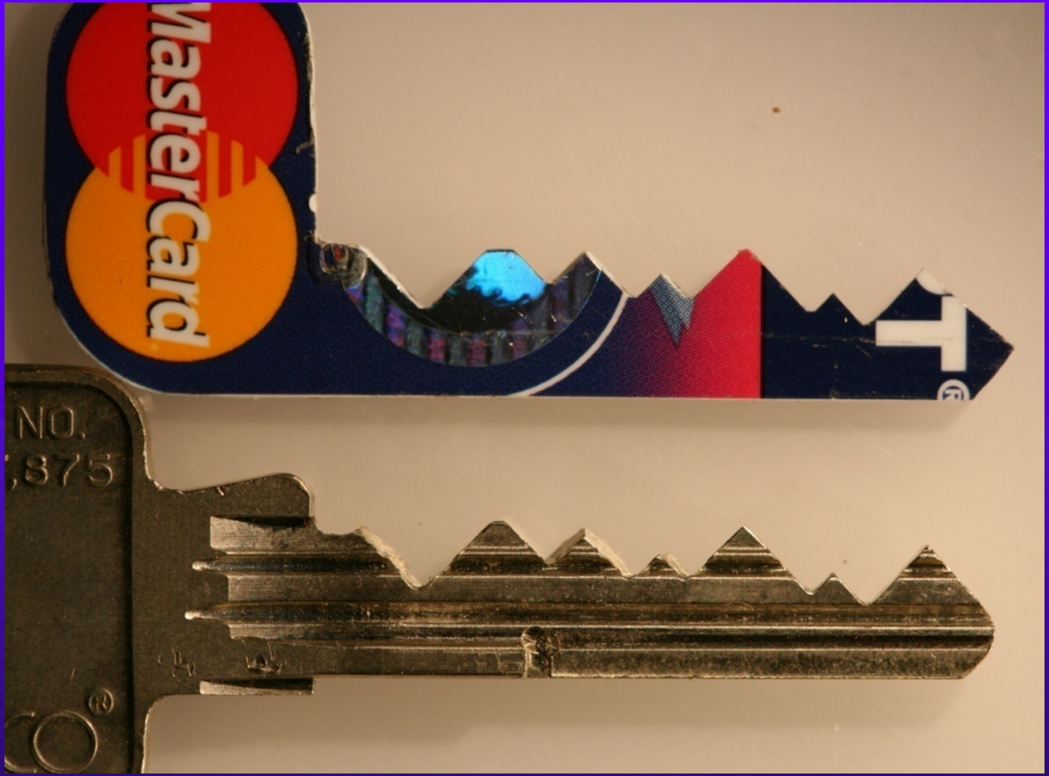


HIGH SECURITY FACILITIES: CONVENTIONAL LOCKS

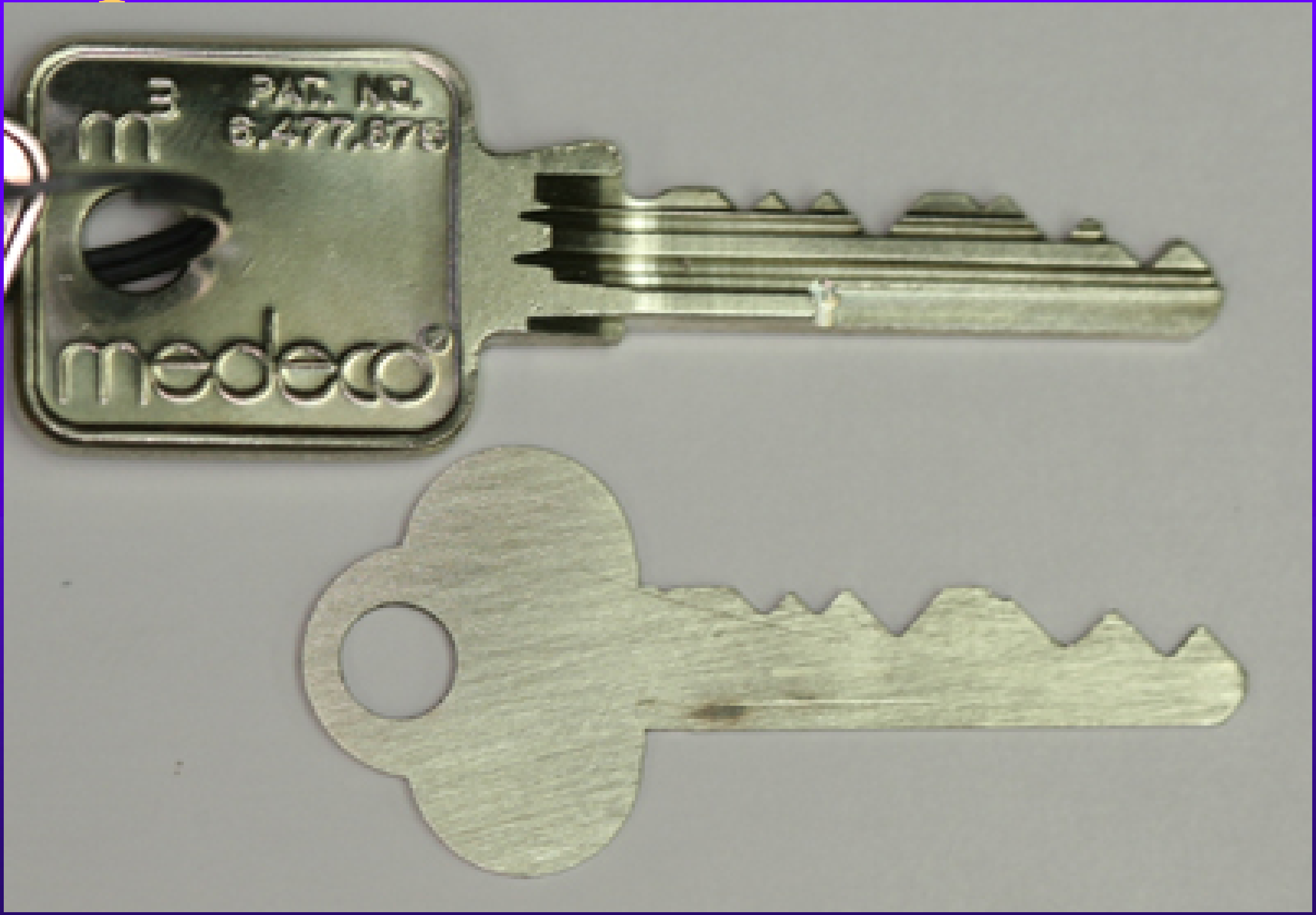
- CONVENTIONAL MECHANICAL LOCKS ARE NOT SUFFICIENT

→ OPEN THE LOCK: Replicate the Key in Plastic

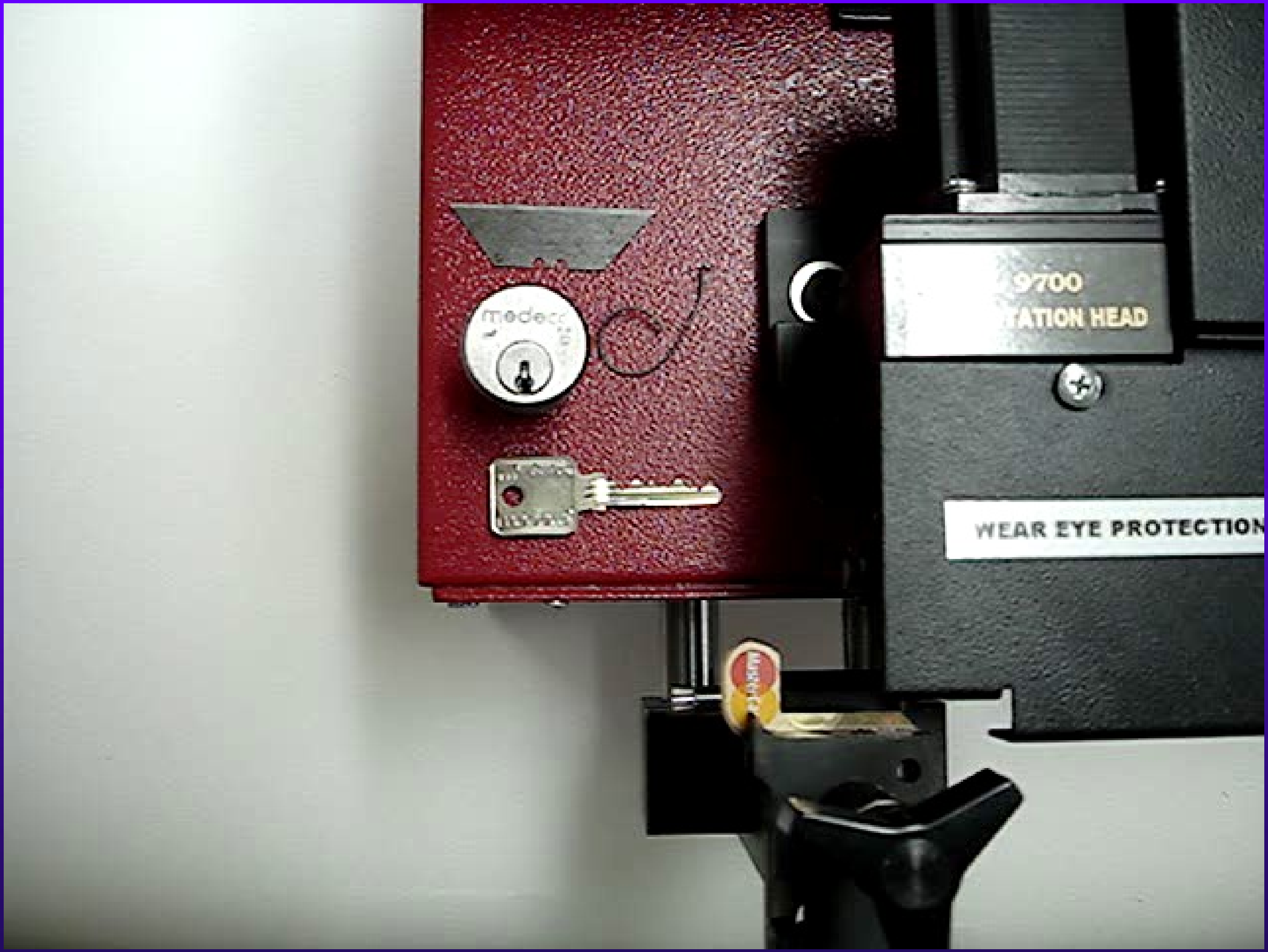
- ♦ MEDECO TAKES PLASTIC!



MEDECO SIMULATED KEYS: Replicate in metal



FAILURE OF KEY CONTROL: MEDECO TAKES PLASTIC



MECHANICAL LOCKS: NOT ENOUGH PROTECTION

- LIMITATIONS
  - 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: HIGHER SECURITY SOLUTION?

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

MUL-T-LOCK CLIQ ADVERTISING

STAND-ALONE EAC: ASSA ABLOY CLIQ TECHNOLOGY

- MUL-T-LOCK, IKON, ASSA, MEDECO LOGIC = SAME TECHNOLOGY
- SYSTEM DESIGN
- ELECTROMECHANICAL STAND-ALONE CYLINDERS
- MECHANICAL LOCKING + AUDIT
- ENHANCED CONTROL OPTIONS
- USED THROUGHOUT THE WORLD

LOGIC AND CLIQ LOCKS: DESIGN ATTRIBUTES

- PROGRAM PERMISSIONS
- AUTHORIZED KEYS
- AUDIT TRAIL EVENTS
- MECHANICAL+ ELECTRONIC SECURITY
- NO WIRING OR ADDED HARDWARE

CLIQ AND LOGIC HARDWARE: STATED ADVANTAGES?

- KEY POWERS THE LOCK
- MECHANICAL BITTING + CREDENTIALS
- EASY RETROFIT TO EXISTING LOCKS
- ADD-DELETE KEYS
- WIDE RANGE OF ACCESS CONTROLS: TIME, DATE, DOOR CONTROL

LOGIC AND CLIQ KEYS: STATED ADVANTAGES?

- MECHANICAL AND ELECTRONIC KEYS
- PATENTED KEY CONTROL
- REVERSIBLE KEY
- 1000 AUDIT EVENTS

ASSA ABLOY EAC: SECURITY AND REALITY

- KEY CONTROL
  - SIMULATION OF KEYS
  - LOST, STOLEN, DELETED KEYS
  - ENTIRE SYSTEM AT RISK
  - CANNOT RE-KEY CYLINDERS
- SIMULATE CREDENTIALS
- BYPASS ALL AUDIT FUNCTIONS

SOME EAC LOCKS: SERIOUS SECURITY ISSUES

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

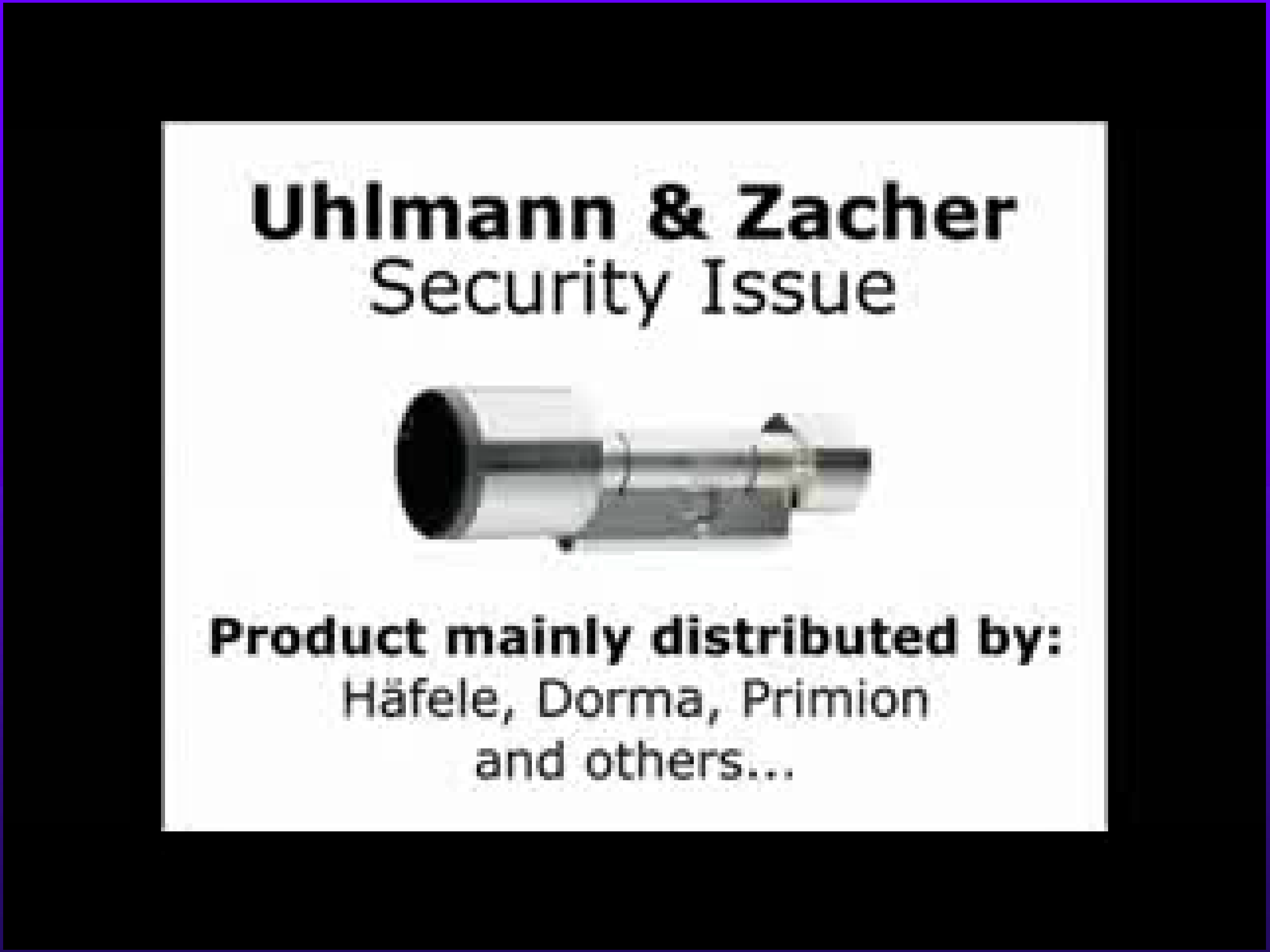
POTENTIAL SECURITY VULNERABILITIES?

- BYPASS OF MECHANICAL OR ELECTRONIC SYSTEM
- AUDIT TRAIL DEPENDS ON READING THE KEY
- WHAT IF ONE LAYER IS BYPASSED
- RF-BASED SYSTEMS: DoS ATTACKS
- LOSS OF KEYS
- LEGAL ISSUES: AUDIT TRAILS

ELECTRO-MECHANICAL EAC LOCKS

- MECHANICAL LOCKS +ELECTRONIC CREDENTIALS
- STILL MECHANICAL LOCKS
- BYPASS TECHNIQUES AVAILABLE

MAGNETIC ATTACK: UHLMANN and ZACHER



Uhlmann & Zacher

Security Issue

Product mainly distributed by:

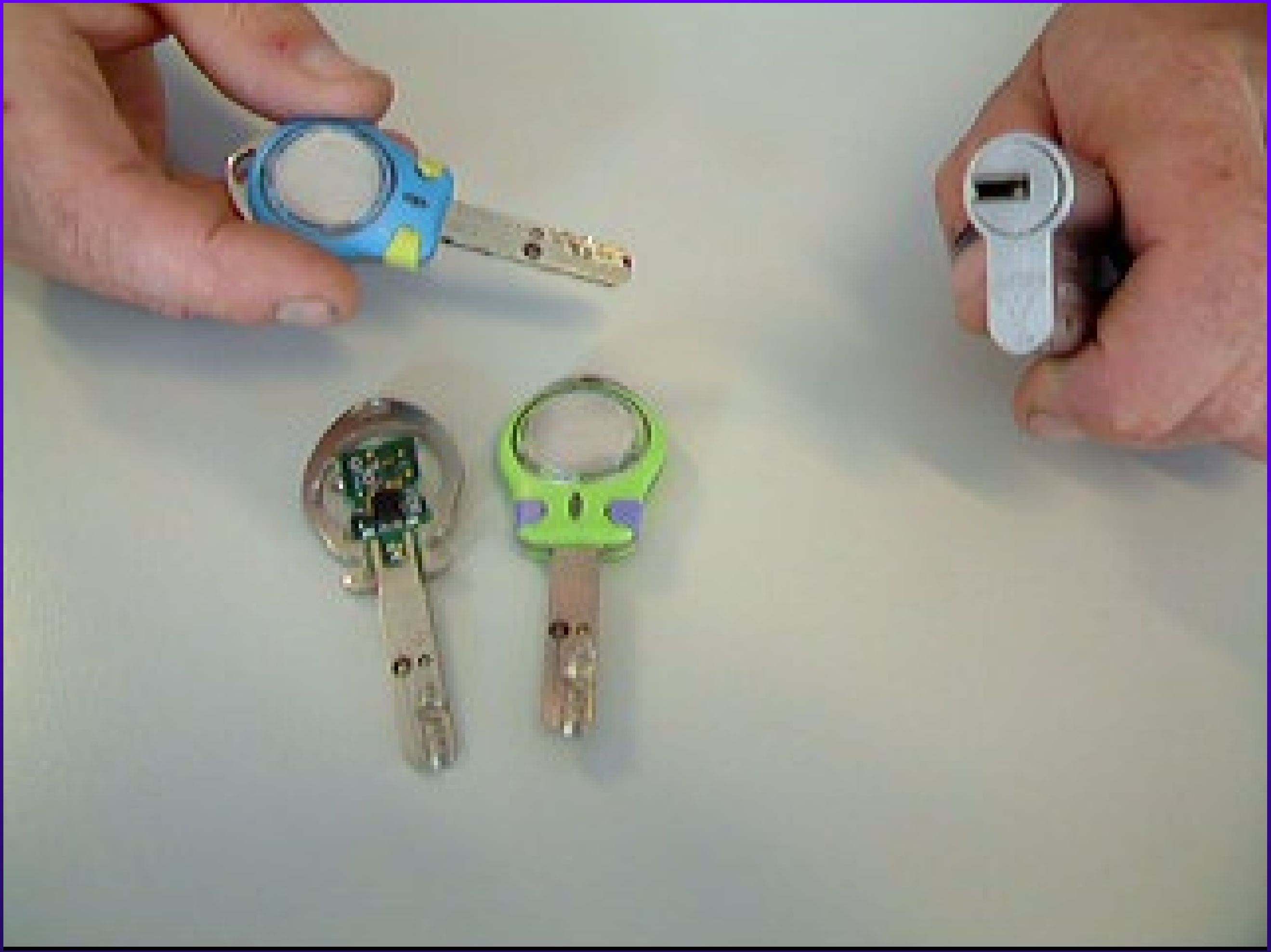
Häfele, Dorma, Primion

and others...

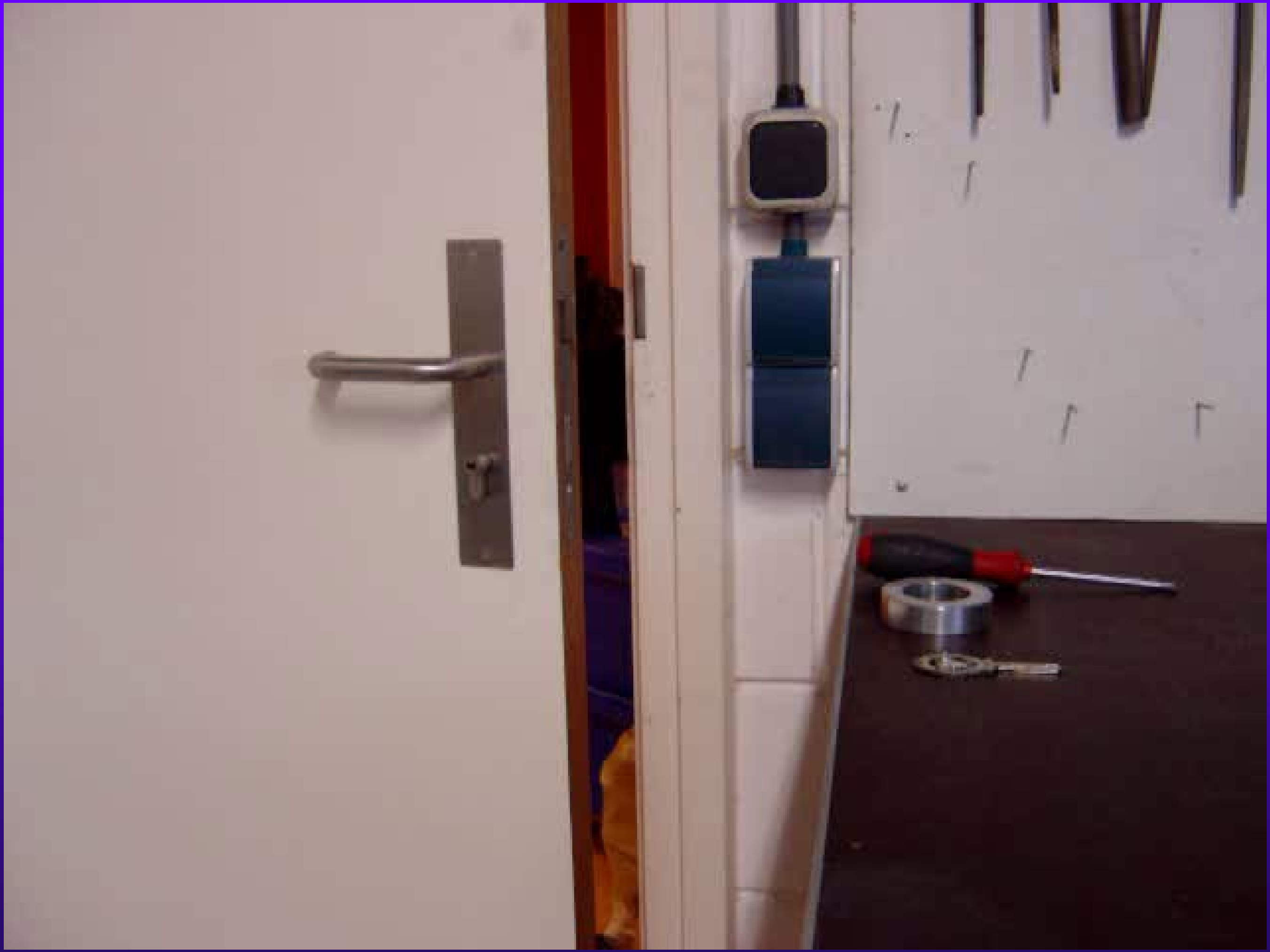
CLIQ AND LOGIC SECURITY ISSUES: KEYS

- MECHANICAL KEYS
- WAFER OR PIN TUMBLER SYSTEM
- OFTEN KEYED ALIKE SYSTEMS
  - KEYS ONLY CUT AT FACTORY
  - ELECTRONIC TECHNOLOGY IN KEY
- RESULTS IF KEYED ALIKE OR CAN DUPLICATE KEYS (MUL-T-LOCK)

MUL-T-LOCK CLIQ AND MAGNETS



CLIQ AND MAGNETIC RING



CLIQ AND LOGIC SECURITY: SIMULATE CREDENTIALS

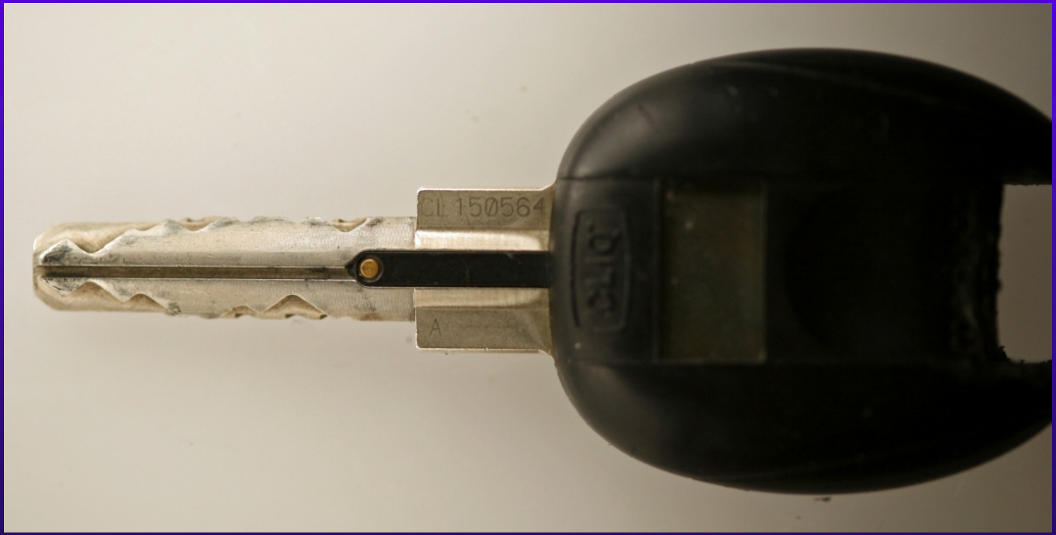
- SECURITY OF SYSTEM: MECHANICAL KEYS + ELECTRONIC CREDENTIALS
- QUESTION: POSSESS KEY AND SIMULATE OR BYPASS CREDENTIALS
- ONE LOST KEY: COMPROMISE ENTIRE SYSTEM

SECURITY AND AUDIT TRAILS

- BYPASS AUDIT TRAIL: AUDIT TRAIL IS DEPENDENT UPON READING THE KEY OR LOCK
- IF THERE IS NO AUDIT TRAIL:
- FALSE BLAME
- FALSE SENSE OF SECURITY
- UNKNOWN COMPROMISE
- NO EVIDENCE OF ENTRY

CLIQ AND LOGIC SECURITY

- MEDECO: “UNAUTHORIZED KEY COPYING IS REMOVED FROM THE EQUATION” “SUPERIOR PROTECTION AGAINST UNAUTHORIZED KEY COPYING”

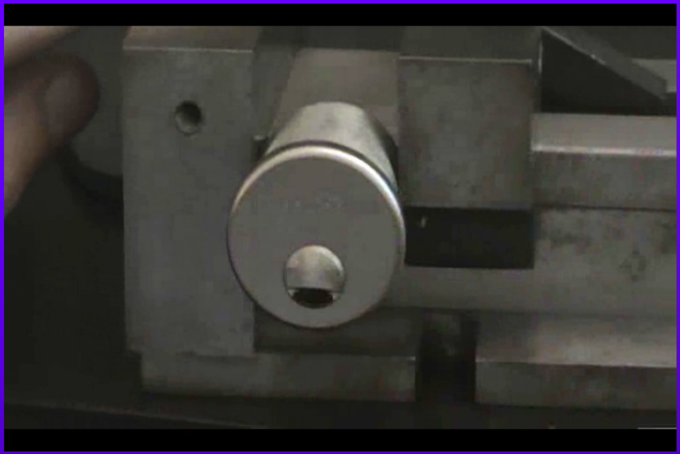


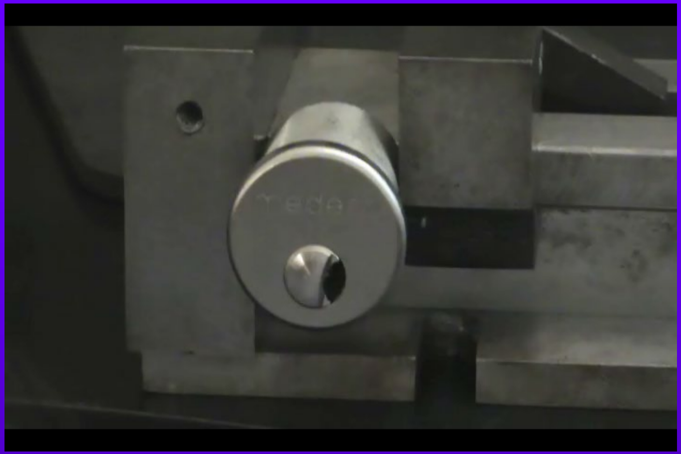
CLIQ, LOGIC, NEXGEN POTENTIAL ISSUES

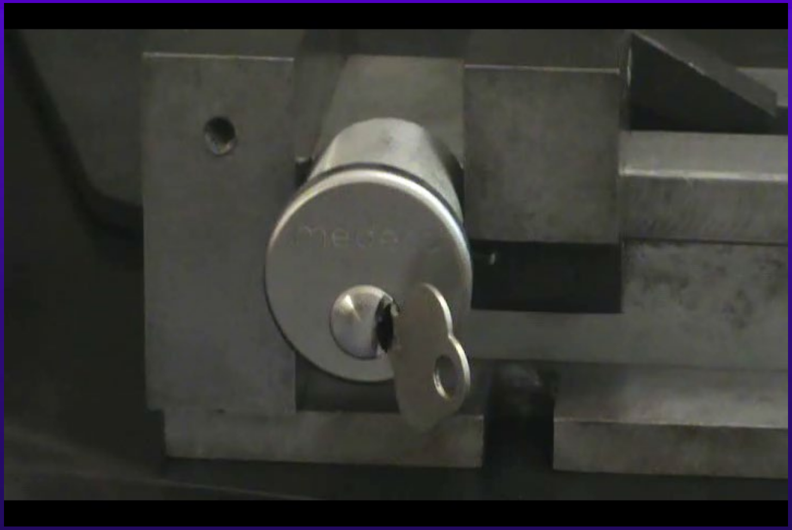
- PRELIMINARY RESEARCH
  - ONE KEY LOST, STOLEN, DELETED MAY COMPRIMSE ENTIRE SYSTEM
  - SIMULATE CREDENTIALS
  - OPEN IN 30 SECONDS OR LESS
  - NO AUDIT TRAIL
  - SIMULATION OF KEYS

MEDECO LOGIC BYPASS

LOGIC INSECURITY: SIMULATED KEYS



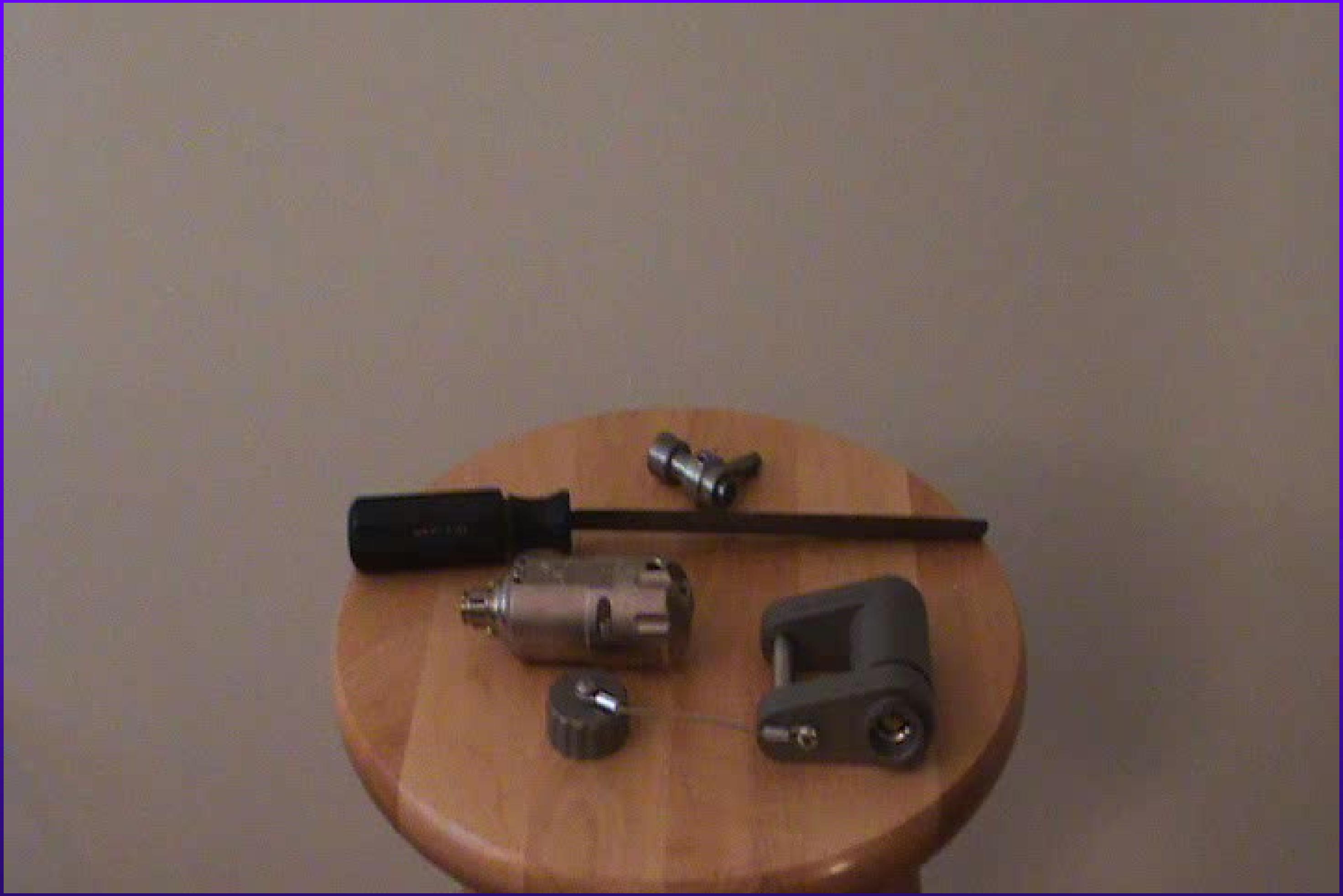




LOGIC COMPROMISE: SIMULATE ELECTRONICS

CLIQ COMPROMISE

MEDECO NEXGEN



in.Security.Org

ALL EAC SYSTEMS: CRITICAL ASSESSMENT

- MECHANICAL LOCKING SYSTEM
- MECHANICAL BYPASS
- KEYING SCHEMES
- BYPASS OF ELECTRONICS
- SIMULATE CREDENTIALS
- CLONE CREDENTIALS

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

© 2009 Marc Weber Tobias and

Tobias Bluzmanis

www.security.org

mwtobias@security.org