INSECURITY ENGINEERING: Locks, Lies, and Videotape

LOCK DESIGN:

MECHANICAL v. SECURITY ENGINEERING

- PRIOR DefCon PRESENTATIONS
- Vulnerabilities in mechanical and electro-mechanical locks
- Resulted from Defective or Deficient engineering
- All-encompassing standards problem
- Failure to understand “why” locks can be opened, rather than “how”

INSECURITY ENGINEERING

- DEFICIENT OR DEFECTIVE PRODUCTS
  - Intersection of mechanical and security engineering
- FALSE SENSE OF SECURITY
  - What appears secure is not
  - How do you know the difference?
  - Undue reliance on standards
- MISREPRESENTATIONS BY MFG

SPECIFIC DESIGN FAILURES

- KWIKSET SMART KEY®
- KABA IN-SYNC
- AMSEC ELECTRONIC SAFE ES813
- ILOC ELECTRO-MECHANICAL LOCK
- BIOLOCK FINGERPRINT LOCK
  - Examine each lock for security vulnerability
  - Statements from the manufacturers about their security

LOCKS:
THE FIRST LINE OF DEFENSE

- LOCKS: FIRST SECURITY BARRIER
- OFTEN, THE ONLY SECURITY LAYER
- MEASURED BY STANDARDS
- WHAT IF NOT RATED BY UL or BHMA
- HOW DO YOU KNJOW THAT LOCKS ARE SECURE?
- WHAT DOES “SECURE” MEAN?

MANUFACTURER RESPONSIBILITIES

- UNIQUE RESPONSIBILITY FOR COMPETENCE
  - MECHANICAL ENGINEERING
  - SECURITY ENGINEERING
- IMPLIED REPRESENTATIONS
  - “WE ARE EXPERTS”
  - SECURITY OF THEIR PRODUCTS
  - REPRESENTATIONS
  - “WE MEET OR EXCEED STANDARDS”

EXPERTISE REQUIRED IN LOCK DESIGN

- MECHANICAL ENGINEERING
- SECURITY ENGINEERING
- MINIMUM INDUSTRY STANDARDS REQUIRE LEVEL OF KNOWLEDGE
- SECURITY ENGINEERING REQUIRES:
  - UNDERSTAND USE OF WIRES, MAGNETS, PAPERCLIPS, BALL POINT PENS, ALUMINUM FOIL
  - BYPASS TECHNIQUES

ENGINEERING FAILURES:
RESULTS AND CONSEQUENCES

- INSECURITY ENGINEERING
  - Insecure products
  - Often easily bypassed
  - Use standards as the measure when they do not address the relevant issues
  - Products look great but not secure
  - False sense of security

COST AND APPEARANCE v. QUALITY AND SECURITY

- DO YOU GET WHAT YOU PAY FOR?
- 2$ LOCKS ARE 2$ LOCKS!
- SHORTCUTS DO NOT EQUAL SECURITY
- CLEVER DESIGNS MAY REDUCE SECURITY
- PATENTS NOT GUARANTEE SECURITY

SECURITY GRADES v. SECURITY RATINGS

- UL 437 AND BHMA 156.30 SECURITY STANDARDS
- BHMA SECURITY GRADES
- DEADBOLT SECURITY
  - Lock cylinder v. locking hardware
  - Locks and hardware are different
  - “The key never unlocks the lock”

LOCK MFG OFTEN CANNOT OPEN THEIR OWN LOCKS

- MEET STANDARDS BUT NOT SECURE
- MISREPRESENTATIONS
- PRODUCE INSECURE PRODUCTS
- TODAY: FIVE EXAMPLES OF DEFICIENT OR OF INCOMPETENT SECURITY ENGINEERING

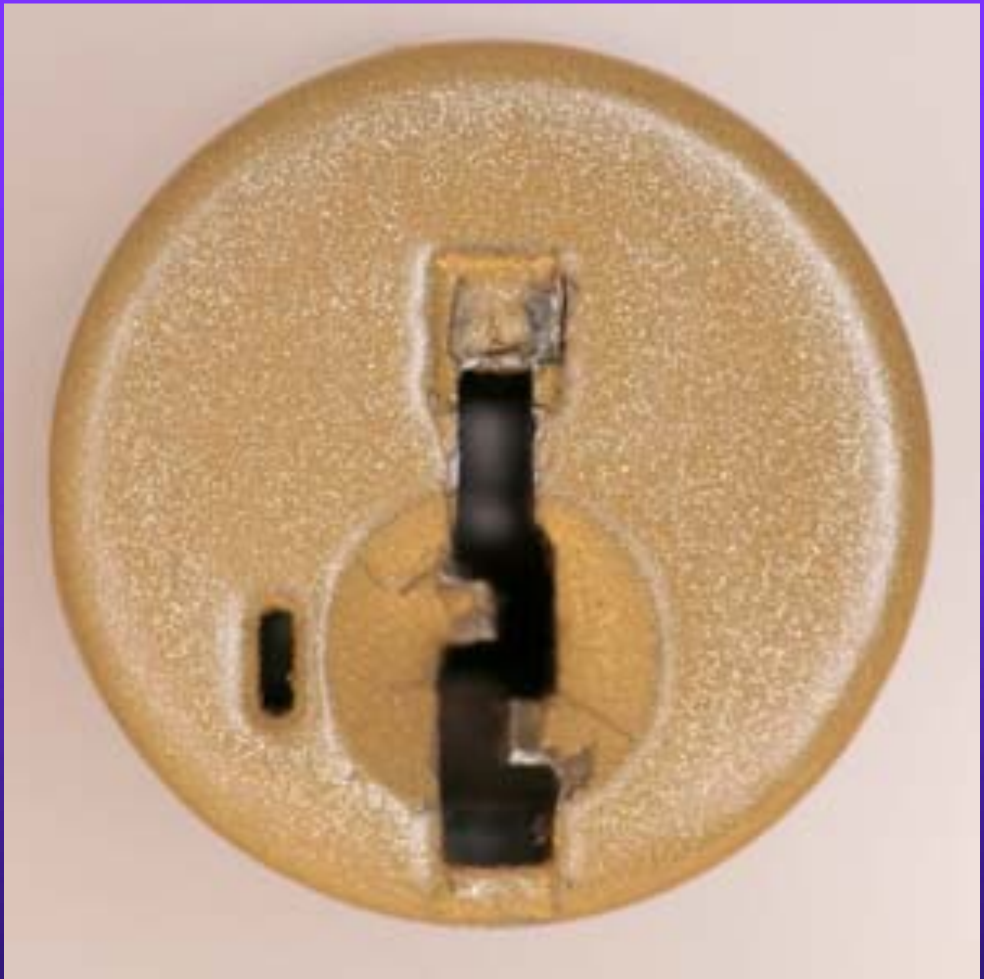
FIVE EXAMPLES: INSECURITY ENGINEERING

- CONVENTIONAL PIN TUMBLER LOCK
- ELECTRO-MECHANICAL LOCK
- BIOMETRIC FINGERPRINT LOCK
- ELECTRONIC RFID LOCK
- CONSUMER ELECTRONIC SAFE
  - All appear secure: None are!
  - This year, focus on wider problem
  - Representative sample
  - Hundreds of bypass tools based upon insecurity

ANALYSIS OF EACH LOCK

- HOW IT WORKS
- WHY DEFICIENT OR DEFECTIVE
- BYPASS VULNERABILITIES
- STATEMENTS BY MANUFACTURERS
- MUST UNDERSTAND THE METHODOLOGY
- REMEMBER FIRST RULE: “THE KEY NEVER UNLOCKS THE LOCK”

EXAMPLE #1: KWIKSET SMART KEY®



KWIKSET SMART KEY®

- $2 TO MANUFACTURER
- CLEVER DESIGN: OUR OPINION: POOR SECURITY
- NOT JUST OURS: READ MANY COMMENTS ON WEB
- MANY SECURITY VULNERABILTIES
- MILLIONS SOLD EVERY YEAR
- EXTREMELY POPULAR LOCK

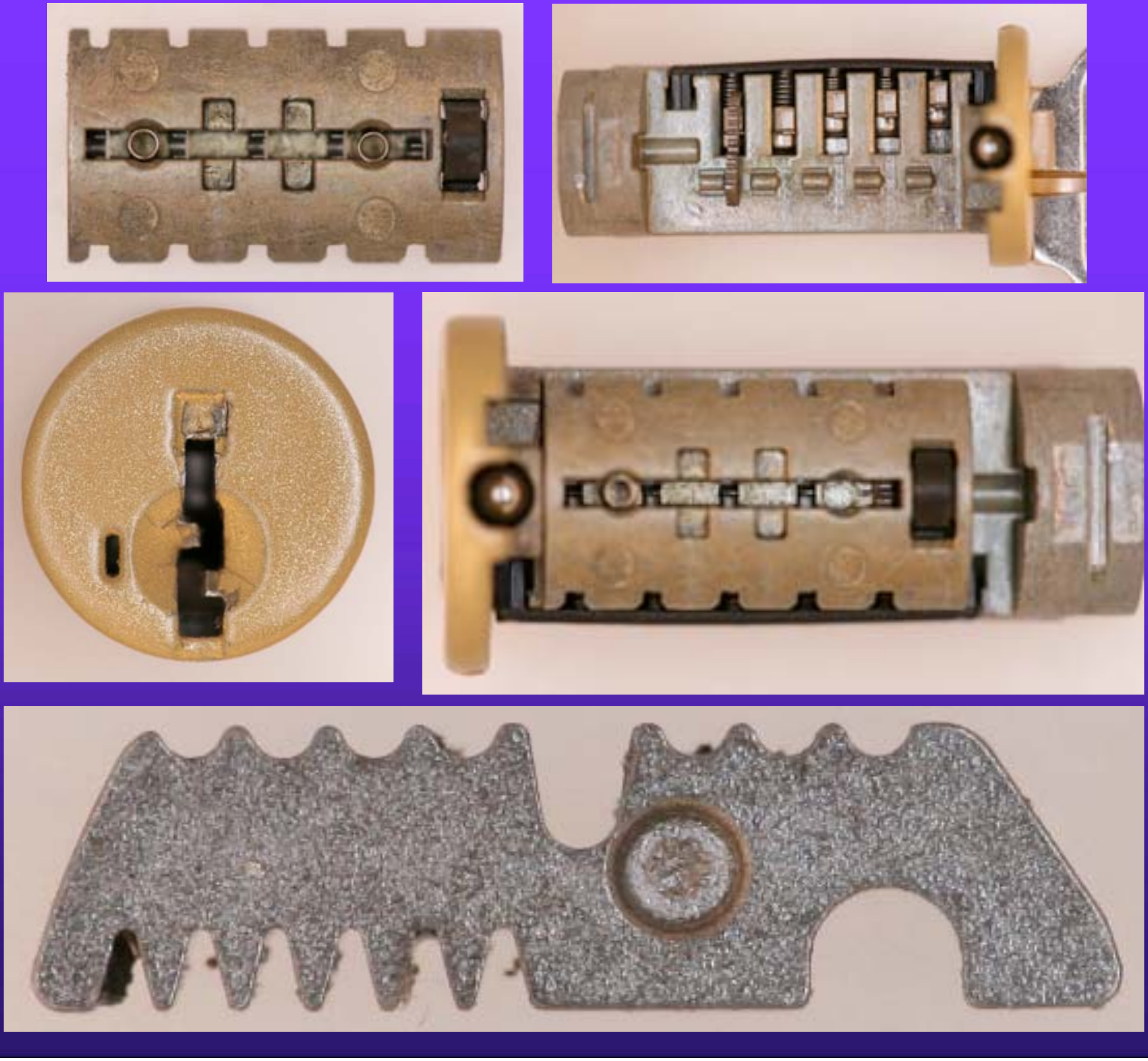
KWIKSET ATTRIBUTES

- CLEVER DESIGN
- PROGRAMMABLE
- COPIED AND MODIFIED EARLIER DESIGNS
- CANNOT BUMP
- DIFFICULT TO PICK
- RATINGS

KWIKSET REPRESENTATIONS

- “ANSI Grade 1 deadbolt for the ultimate in security. Secure your home in seconds with SmartKey.”
- INCREASED SECURITY
- BUMP RESISTANT
- PICK RESISTANT

HOW SMART KEY WORKS



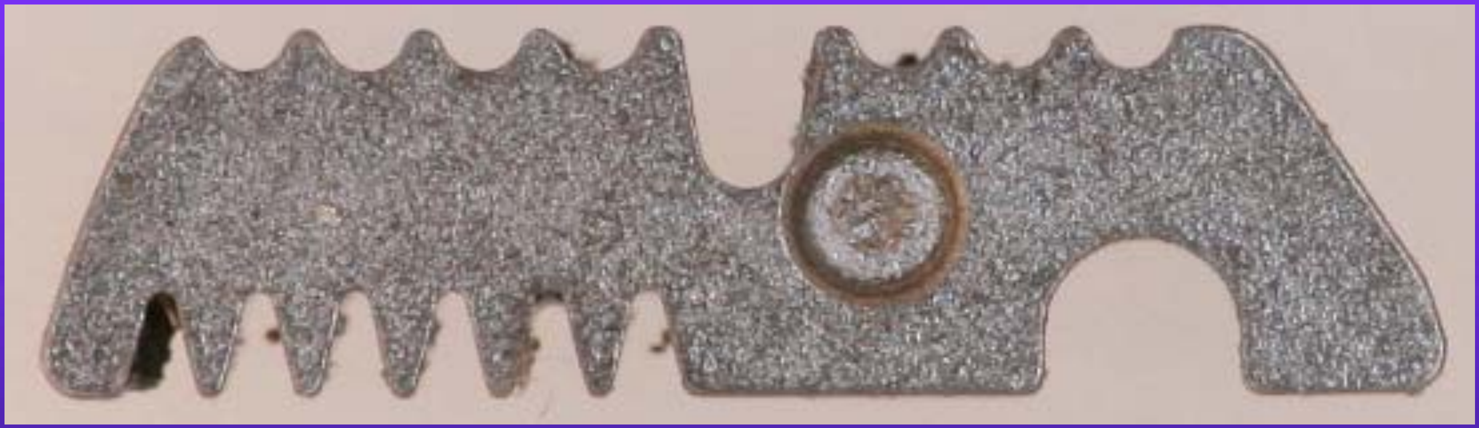
VULNERABILITIES

- COMMERCIAL TOOLS AVAILABILE
- EASY TO COMPROMISE WITH SIMPLE IMPLEMENTS, RAPID ENTRY
  - COVERT ENTRY
  - FORCED ENTRY
  - KEY SECURITY

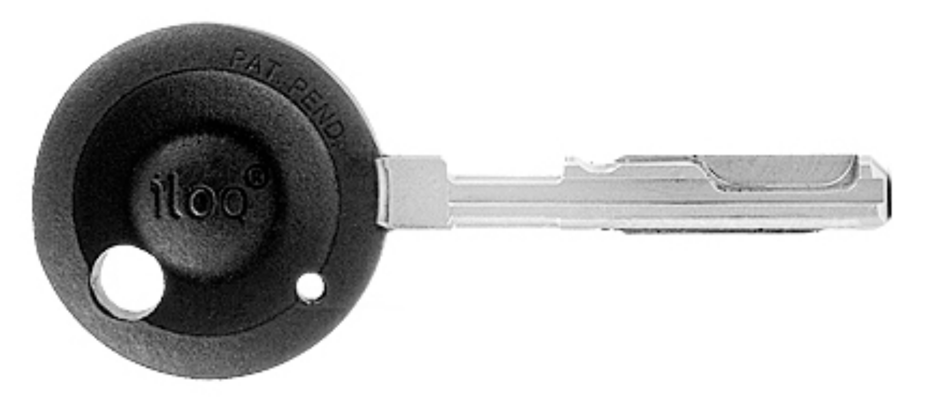
KWIKSET SECURITY

- TINY SLIDERS
- THIN METAL COVER AT END OF KEYWAY
- OPEN RELATIVELY EASILY AND QUICKLY
  - Wires
  - Small screwdriver
  - $.05 piece of metal

KWIKSET SLIDERS:
The Critical Component



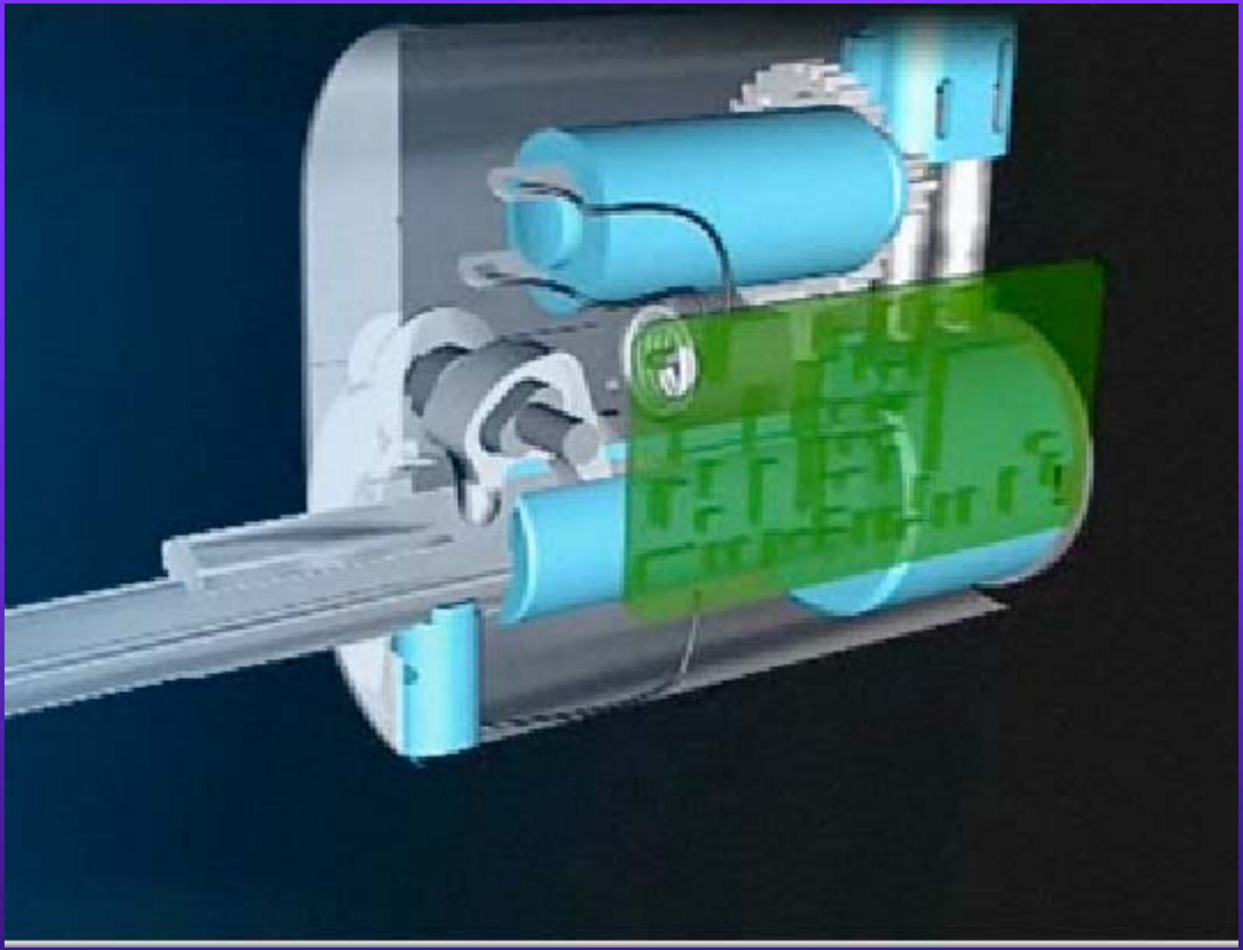
EXAMPLE #2: ILOQ



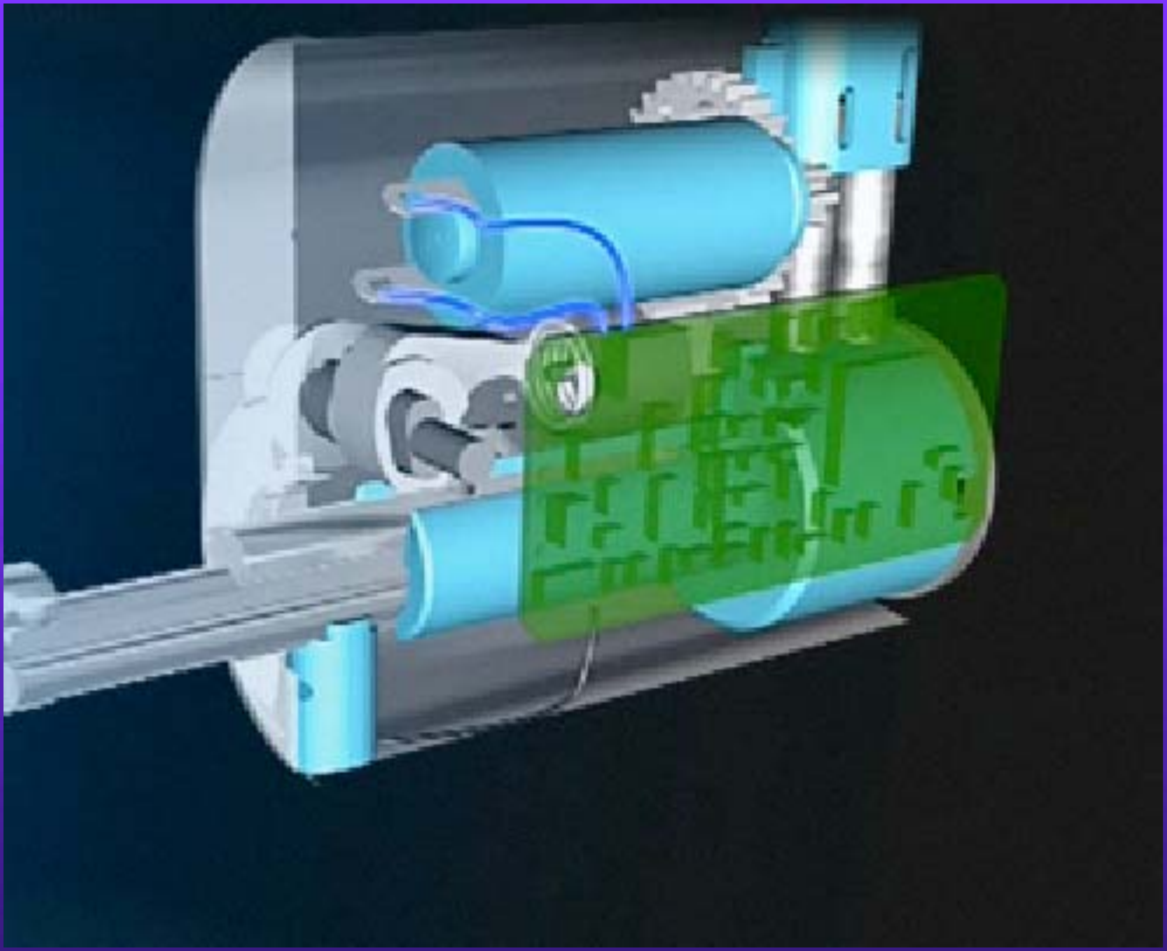
EXAMPLE #2: ILOQ

- MADE IN FINLAND
- VERY CLEVER DESIGN
- COST: $200+
- ELECTRO-MECANICAL DESIGN
- MECHANICAL KEY + CREDENTIALS
- NO BATTERIES: LIKE A CLOCK AND MAGNETO, GENERATES POWER

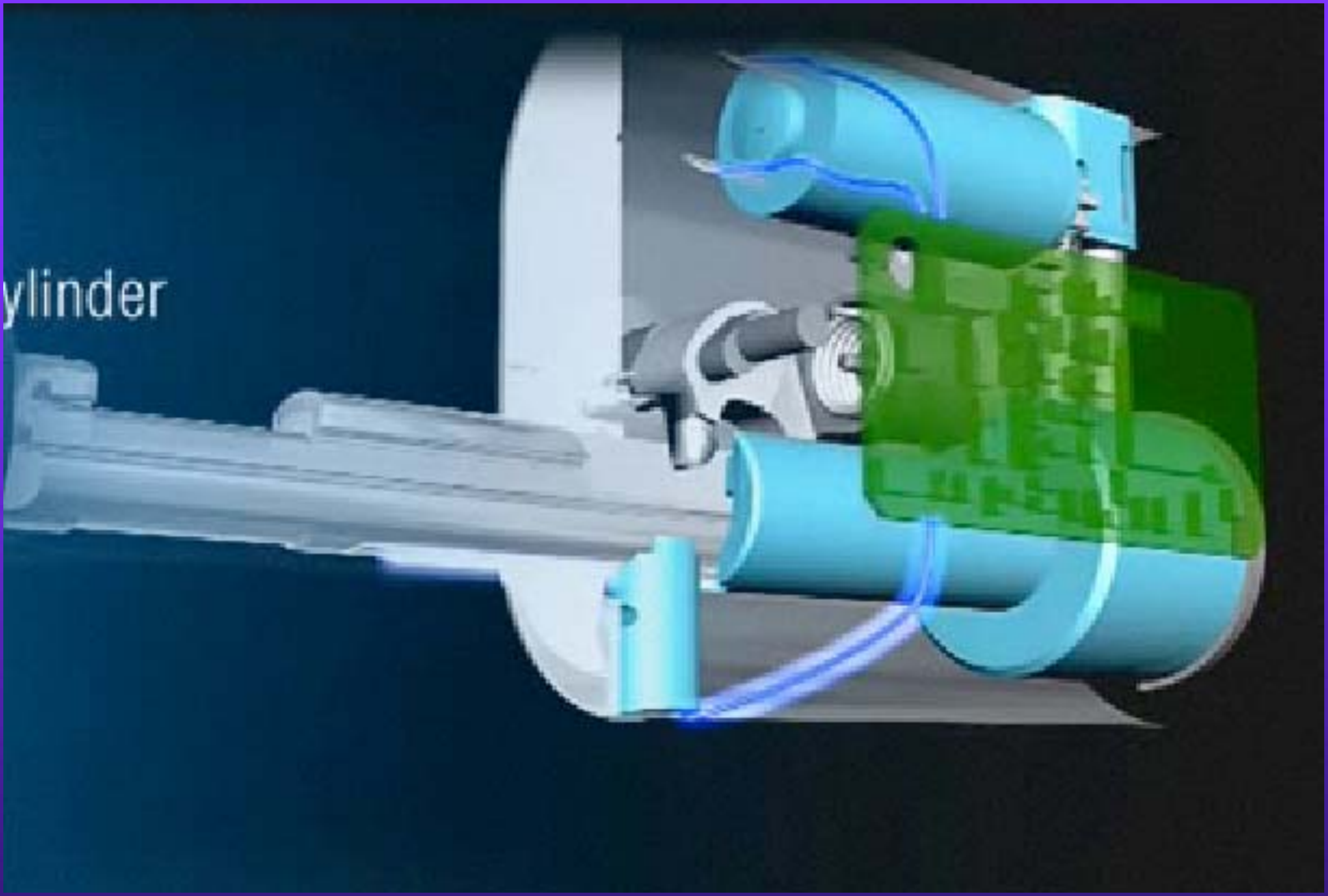
ILOQ: OUR SECURITY



ILOC MECHANISM



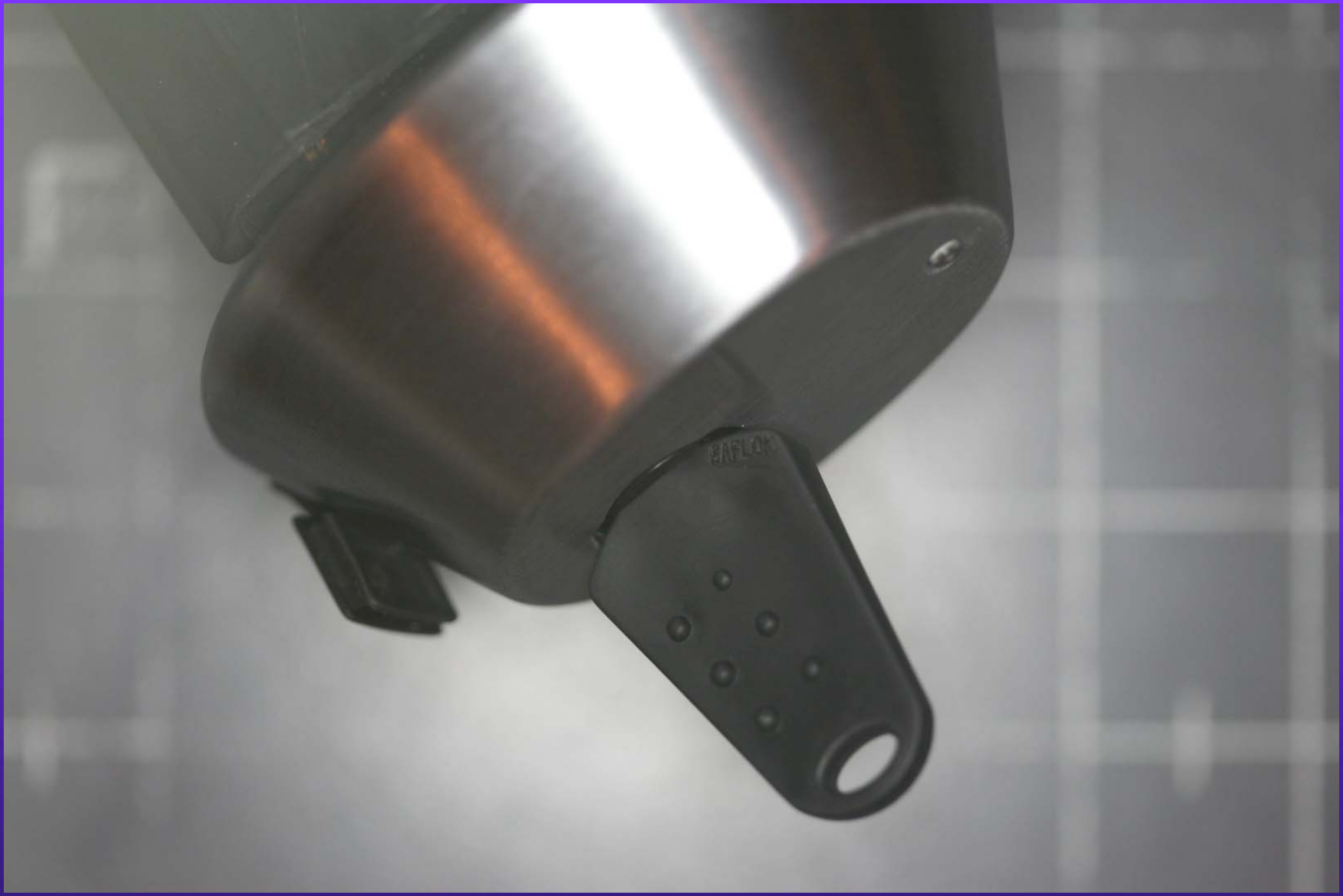
ALL KEYS IDENTICAL



ILOQ VULNERABILITIES

- SET THE LOCK ONCE
- ANY KEY WILL OPEN
- NO NEED FOR CREDENTIALS
- VIRTUALLY NO SECURITY
- DIFFICULT TO DETECT
- LOCK OPERATES NORMALLY ONCE SET

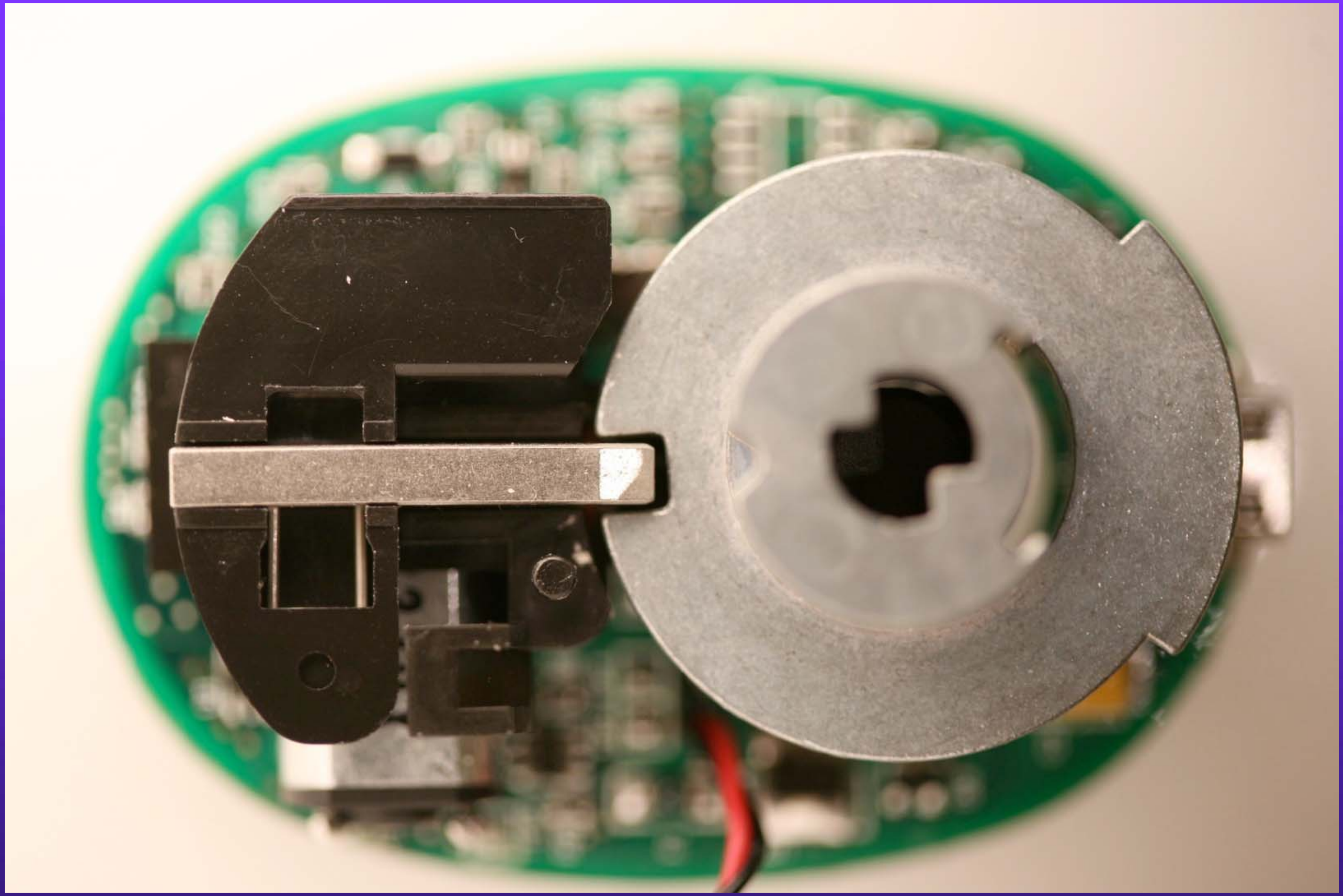
EXAMPLE #3: KABA IN-SYNC RFID-BASED LOCK



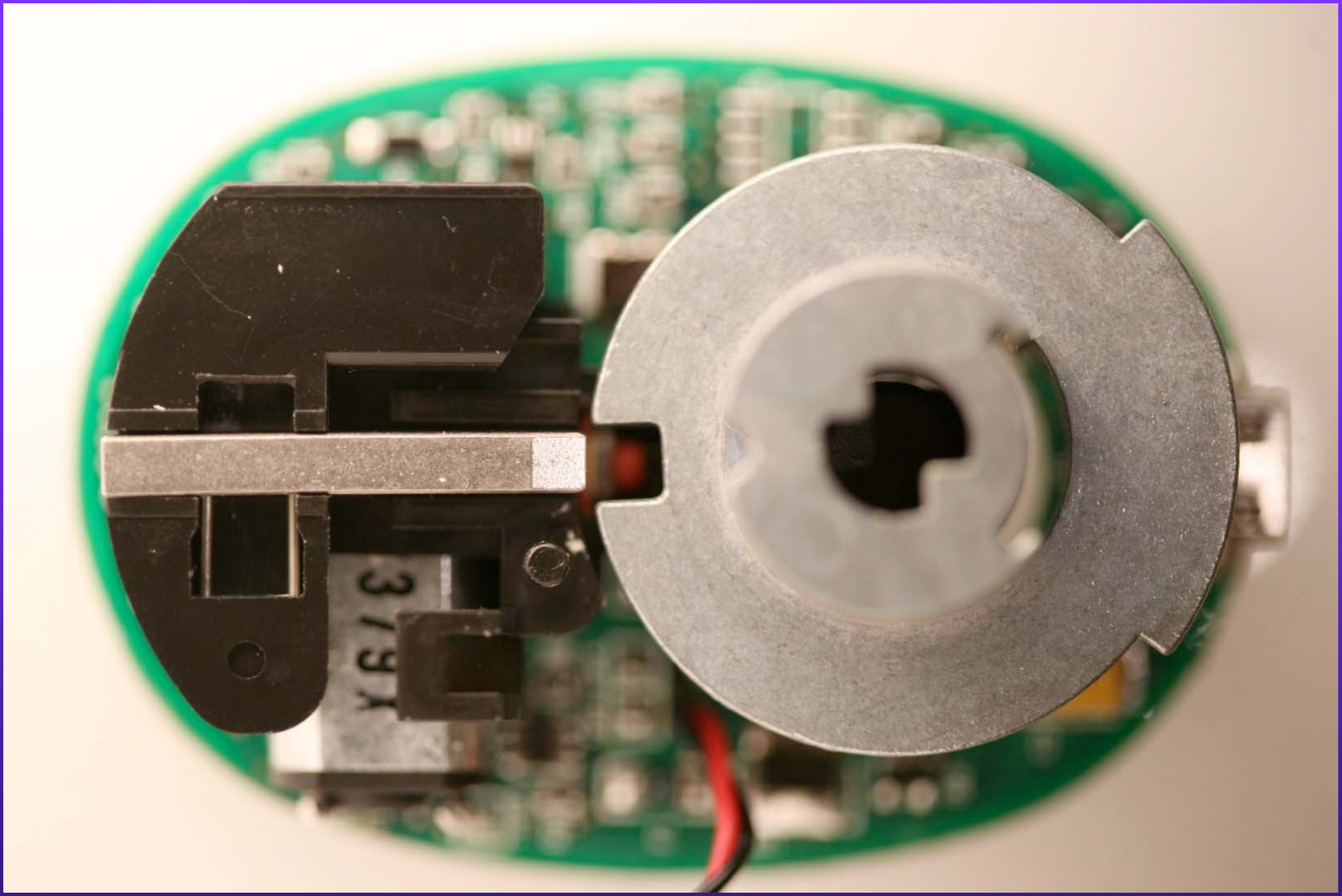
KABA IN-SYNC ATTRIBUTES

- WIDE APPLICATOIN
- AVAILABLE FOR SEVERAL YEARS
- MILITARY AND CIVILIAN APPLICATIONS
- USE SIMULATED PLASTIC KEY WITH RFID
- AUDIT TRAIL

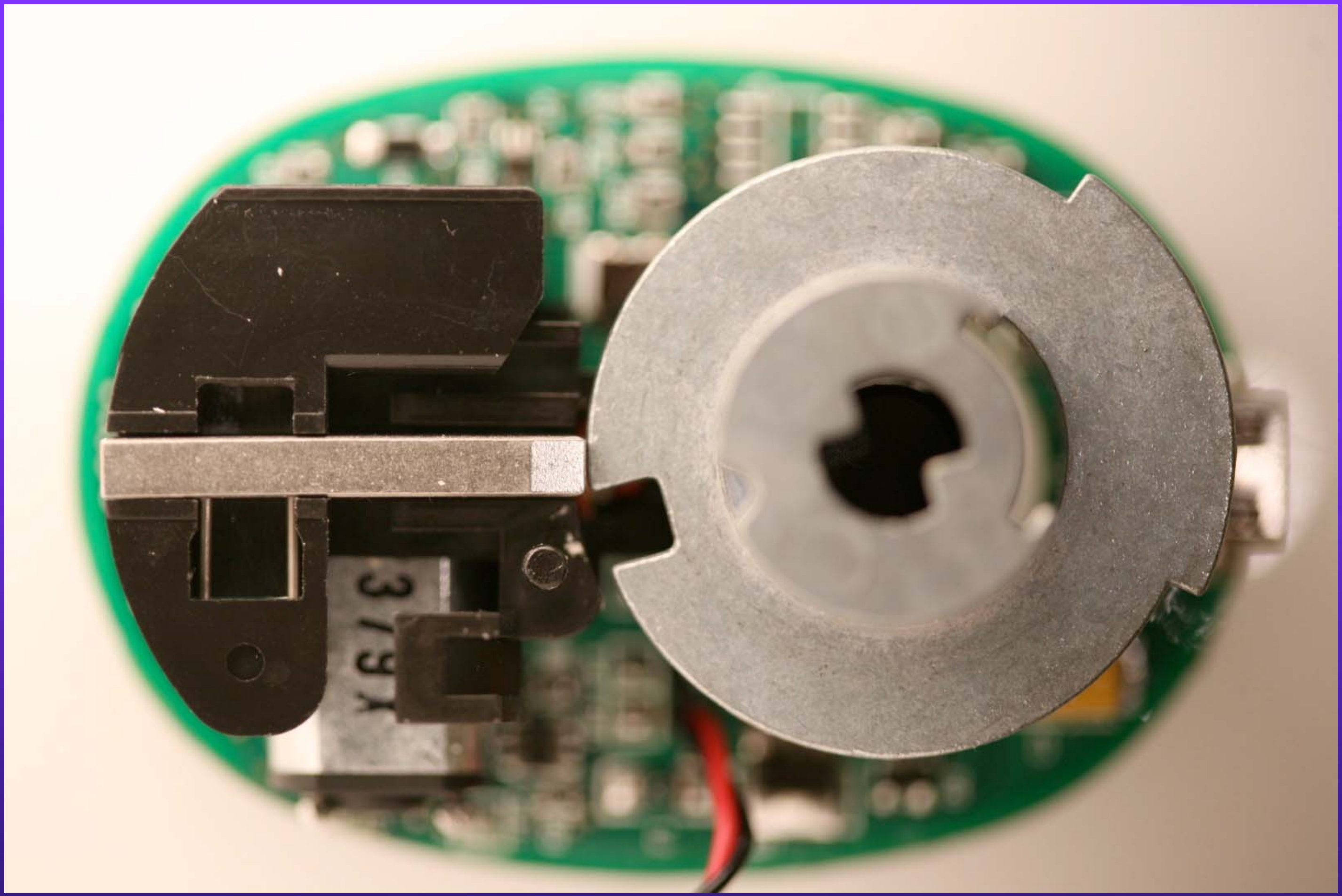
IN-SYNC INTERNAL MECHANISM: LOCKING



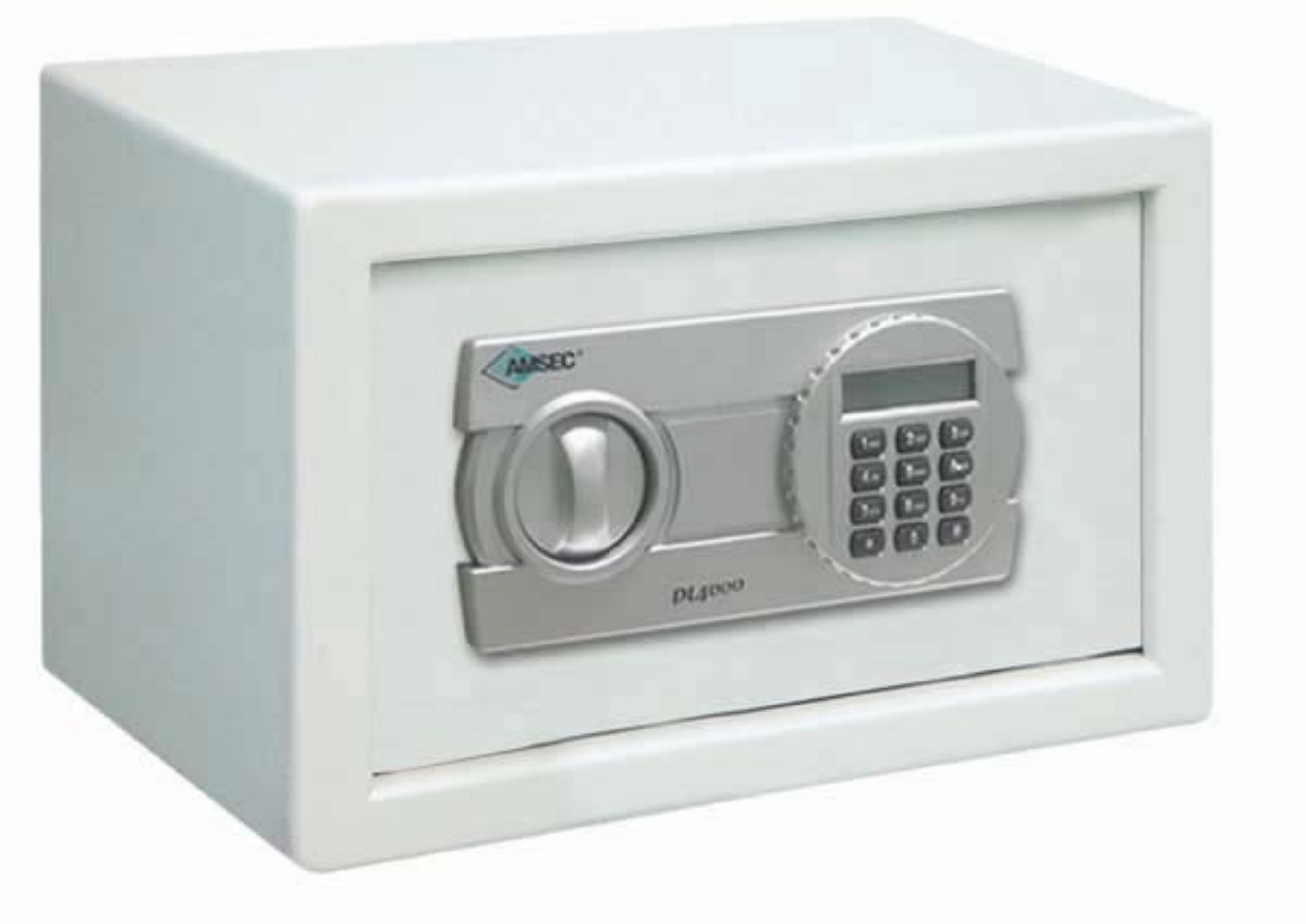
BOLT RETRACTS



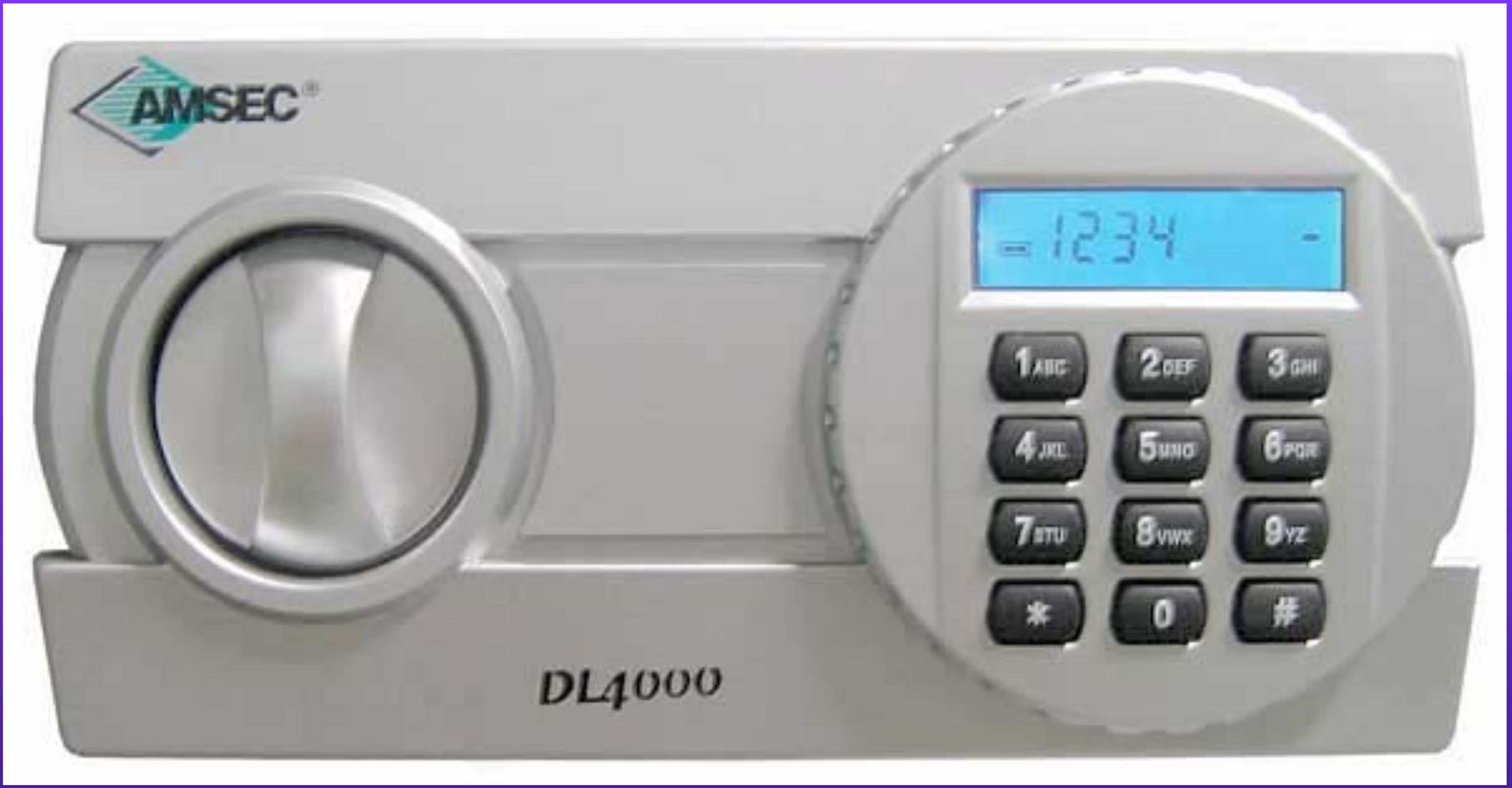
TURN TO OPEN



EXAMPLE #4: AMSEC ES813 CONSUMER “SAFE”



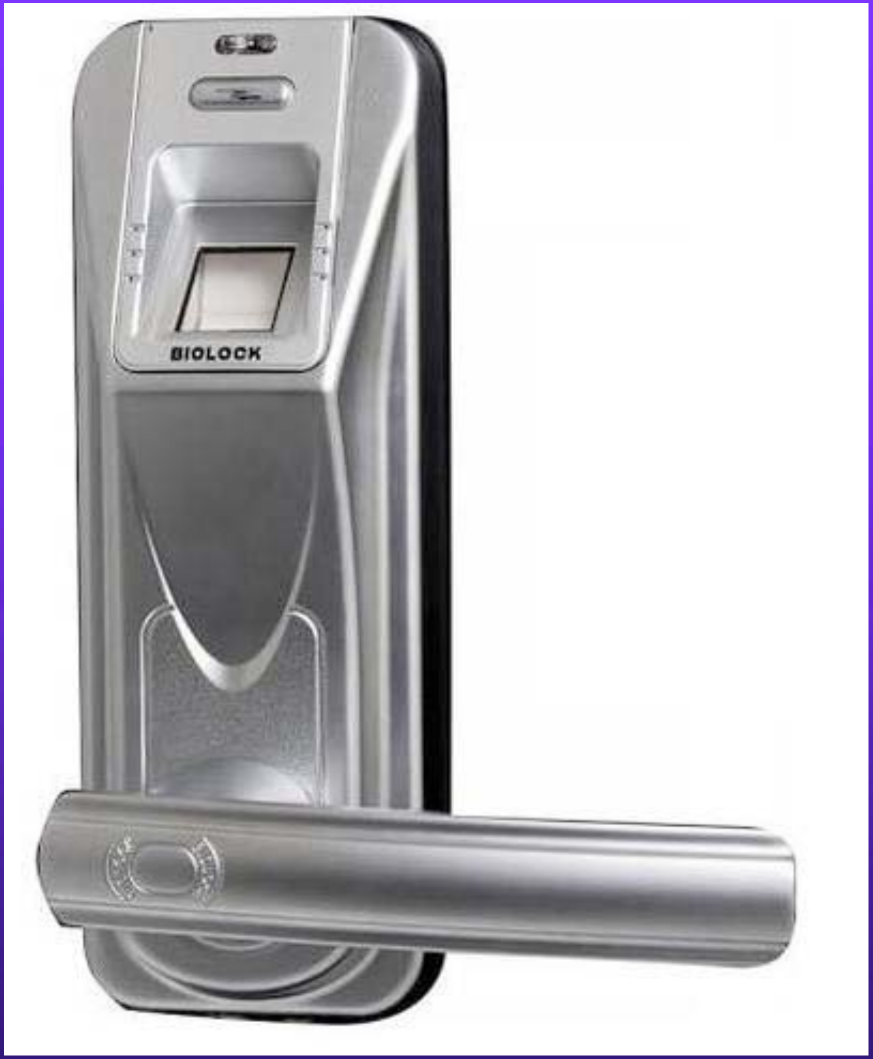
ELECTRONIC KEYPAD



AMSEC SAFE ES813 AND OTHERS

- CONSUMER LEVEL SAFE
- $100 FOR SMALLEST UNIT
- ELECTRONIC KEYPAD
- HOW MUCH SECURITY EXPECTED?
- INCOMPETENT DESIGN
- FOUND IN MANY OTHER SAFES

EXAMPLE #5: BIOLOCK



BIOMETRIC LOCK

- FINGERPRINT + BYPASS CYLINDER
- LOOKS SECURE
- $200 OR MORE
- INSECURITY ENGINEERING AT ITS BEST

LESSONS LEARNED

- CLEVER ≠ SECURITY
- LOCKS REQUIRE BOTH MECHANICAL AND SECURITY ENGINEERING
- PATENTS DON’T GUARANTEE SECURITY
- STANDARDS DO NOT MEAN SECURITY

INDUSTRY UPDATE

- STANDARDS
  - BUMPING
  - PROPOSED BHMA CHANGES
- MANUFACTURERS ARE PAYING ATTENTION AND MAKING CHANGES
- CORRECT PROBLEMS AT PRIOR DEFCON PRESENTATIONS
- WORKING WITH MANUFACTURERS TO TEST LOCKS “REAL WORLD”

SECURITY LABS: REAL WORLD TESTING

- MISSION OF SECURITY LABS
  - TEST LOCKS FOR MAJOR COMPANIES AND VENDORS
  - LEVEL ABOVE UL, BHMA, AND OTHERS
  - DETERMINE AND EXPOSE VULNERABILITIES
  - WORK WITH CLIENTS IN NEW PRODUCT DESIGN
  - PURSUE ACTIONS FOR DEFECTIVE PRODUCTS

CONCLUSIONS

- MISREPRESENTATIONS BY MANY MANUFACTURERS
- HIGH-TECH DESIGNS ≠ SECURITY
- BYPASS TOOLS FOR MANY LOCKS, RELY ON INSECURITY
- MANY MFG DON’T KNOW OF VULNERABILITIES
- INSECURITY = LIABILITY
- CAVEAT EMPTOR

INSECURITY ENGINEERING: Locks, Lies, and Videotape

© 2010 MarcWeber Tobias, Tobias Bluzmanis, Matthew Fiddler

mwtobias@security.org

tbluzmanis@security.org

mjfiddler@security.org