# INSECURITY ENGINEERING AND HIGH SECURITY LOCKS:

## Why cryptography is often irrelevant

# OUR WORLD OF SECURITY: An Overview

- HIGH SECURITY LOCKS AND INVESTIGATIONS
- ALL SECURITY IS ABOUT LIABILITY
- INCREASING INTEGRATION BETWEEN MECHANICAL AND ELECTRONIC LOCKS
- MORE CYER THREATS TO SYSTEMS
- COMPROMISE OF ACCESS
- WE FIGURE OUT HOW TO GET IN WHEN IT APPEARS IMPOSSIBLE

# BACKGROUND

- BEGAN PICKING LOCKS AT AGE 15
- LAWYER AND TECHNICIAN
  - Law offices, primary work is security
  - Security Labs within law office
- LAW ENFOREMENT BACKGROUND
- BOOKS
- PATENTS
- CLIENTS: Major lock companies

# VENUES FOR HIGH SECURITY LOCKS

- CRITICAL INFRASTRUCTURE
  - Airports, train stations, water, power
- GOVERNMENT FACILITIES
  - Military, White House, Royal Palaces
- BANKS AND FINANCIAL
- MEDICAL FACILITIES
- COURTHOUSES
- COMMERCIAL FACILITIES

# OUR TYPICAL CASE

- NEW LOCK TO ANALYZE
  - No intelligence
  - No engineering data
  - No input from manufacturer
- REVERSE ENGINEER EVERYTHING
  - Disassemble, Document and analyze
  - Develop theories to circumvent security
  - Test each theory
  - Develop bypass techniques
  - Report

# SECURITY LABS and INVESTIGATIVE LAW OFFICES

- ALL SECURITY IS ABOUT LIABILITY
- LAWYER CLIENT PRIVILEGE
- LOCKS AND SECURITY
  - Legal
  - Technical
  - Engineering
  - Security issues

# WE SOLVE PUZZLES

# OUR PUZZLES ARE REAL

- LOCKS THAT COST MILLIONS IN R&D WE OPEN IN SECONDS COVERTLY
- TEAM OF PHYSICAL AND CYBER SECURITY EXPERTS
- WORK FOR LOCK MANUFACTURERS
- WE TRAIN DESIGN ENGINEERS HOW TO THINK DIFFERENTLY
- TRAIN ENGINEERING STUDENTS

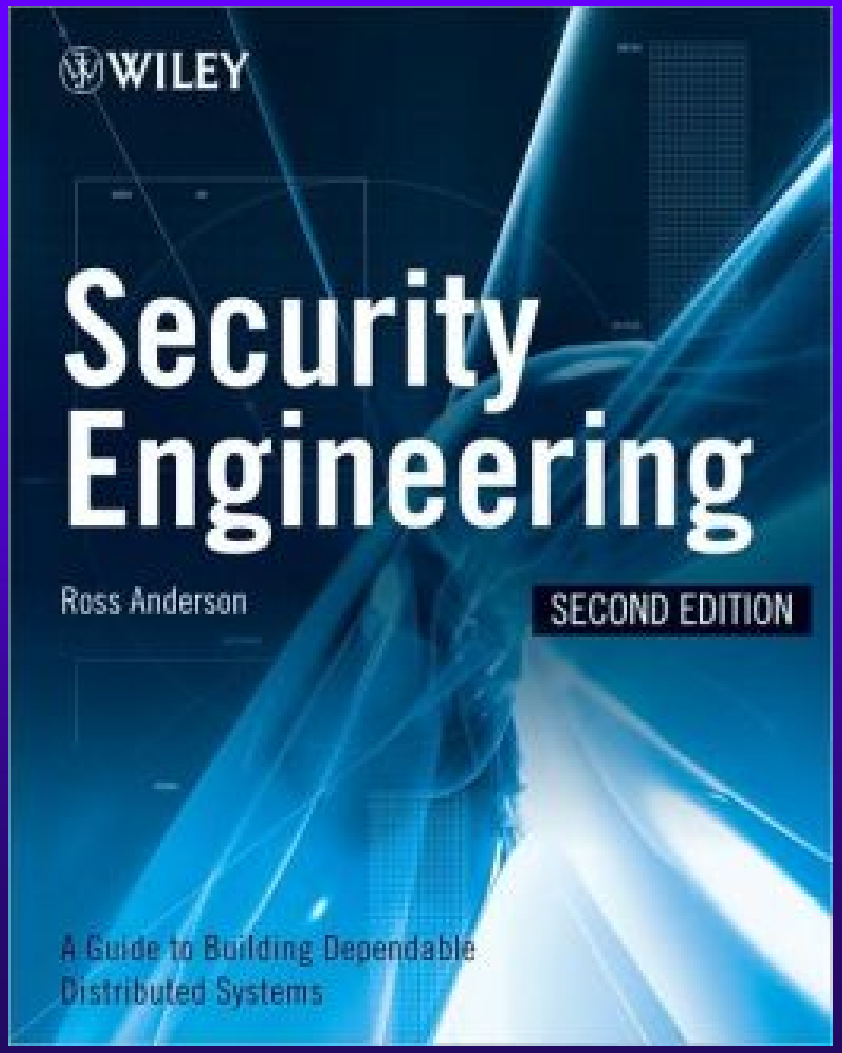
# OUR TEAM: WHAT WE DO

- INVOLVED IN NEW LOCK DESIGNS
- DISCOVER AND HELP FIX FLAWS
- MECHANICAL ENGINEERING AND PHYSICS PROBLEMS
- TOLERANCES OF .0015”

# INSECURITY ENGINEERING

- IDENTIFICATION, ANALYSIS, AND EXPLOIT OF DESIGN FLAWS
- INTERACTION OF MECHANICAL ENGINEERING AND SECURITY
  - Both are equally important

# SECURITY IS OFTEN AN ILLUSION



# SECURITY THEATER 3000: By Argonne Laboratories

# OUR METHODOLOGY

- LOCKS HAVE MULTIPLE SECURITY LAYERS
- NEUTRALIZE EACH LAYER
  - Each layer is identified
  - Bypass techniques developed for each layer
    - Mechanical layers, like pin tumblers and sidebars
    - Credentials
  - Electronic credentials are one layer
    - They ultimately rely on mechanical designs

# STANDARDS ARE LARGELY IRRELEVANT TO WHAT WE DO

- THE PROBLEM WITH STANDARDS
- Define security for locks and safes
  - UL and BHMA
  - UL 437 and BHMA 156.30
    - UL 437 COMMERCIAL PICKING STANDARD
    - BHMA 156.30 HIGH SECURITY STANDARD

# STANDARDS AND LOCKS

- HIGH SECURITY LOCKS
  - FORCED ENTRY
  - COVERT ENTRY
  - KEY CONTROL
- NOT ENCOMPASS MANY METHODS OF BYPASS
  - Mechanical bypass
  - Credentials bypass
  - Key control bypass

# WHY STANDARDS DON'T MATTER IN OUR WORLD

- NON-TRADITIONAL MEANS
- CANNOT DEVIATE IN TESTING
- OUT OF DATE AND DELAYED REVIEW PROCESS TO UPDATE

# STANDARDS AND 3T2R RULE

- ALL STANDARDS ARE ABOUT OUR 3T2R RULE:
  - TIME
  - TOOLS
  - TRAINING
    - REPEATABILITY OF EXPLOIT
    - RELIABILITY OF EXPLOIT

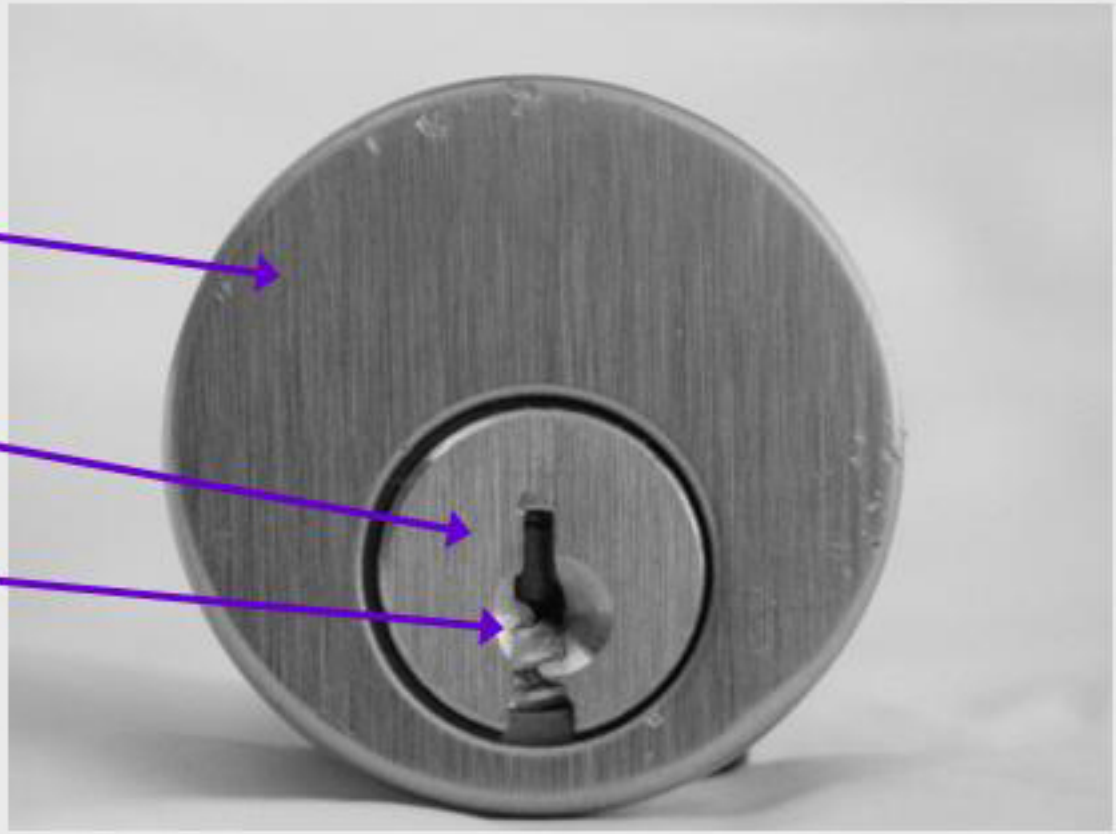
# WHAT HAPPENS WHEN THINGS GO WRONG?

- Reputation
- Liability and damages
- Certifications
- Statutory requirements
- Contract compliance
- Public relations and media
- YouTube and Social Media and Internet
  - The Internet is forever
  - Can influence current and potential customers

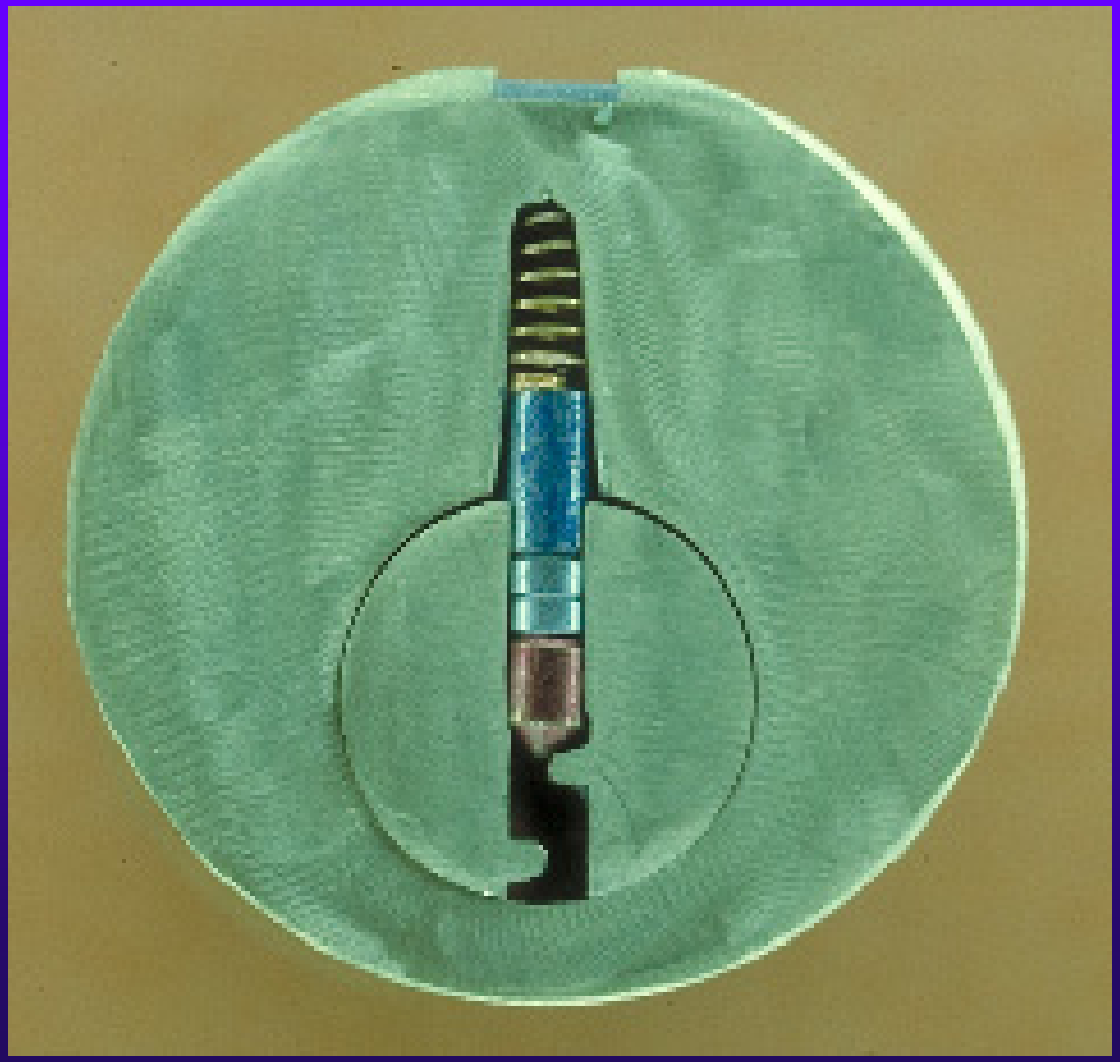
# LOCKS: CURRENT TECHNOLOGY

- MECHANICAL LOCKS
- ELECTRO-MECHANICAL LOCKS
- E-CYLINDERS
- ELECTRONIC ACCESS CONTROL

# CONVENTIONAL MECHANICAL LOCKS

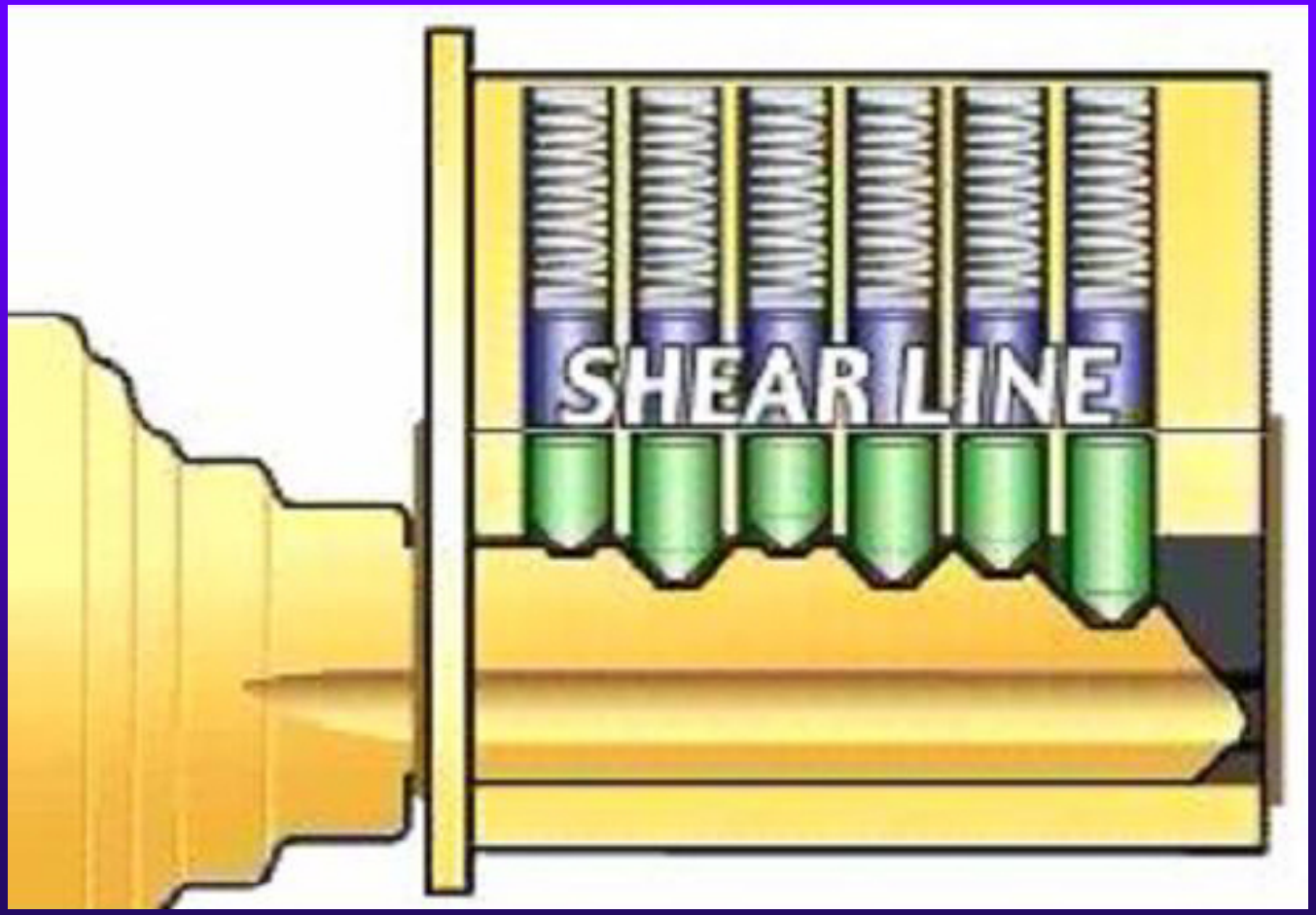


# PIN TUMBLER DESIGN



# PIN STACKS = SECURITY:

## Plug can turn: pins at shearline

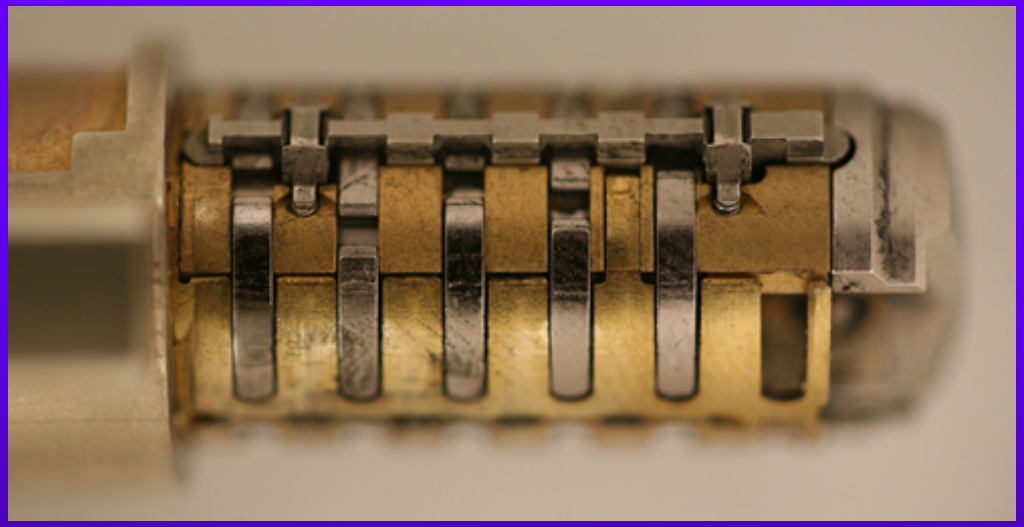


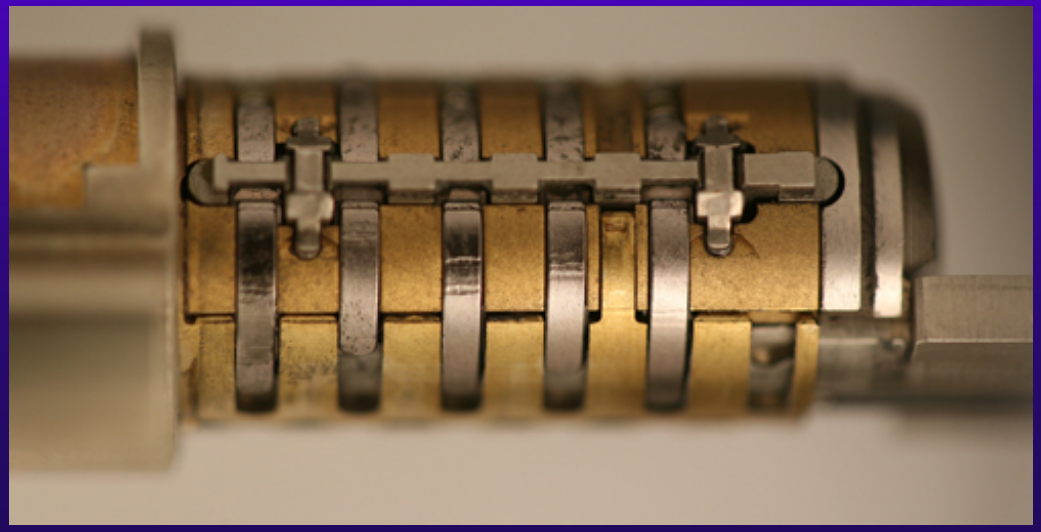
# MECHANICAL LOCKS: ATTRIBUTES

- 4000 YEAR OLD DESIGN
- LINUS YALE: 1860
- NO INTELLIGENCE
- LOW TO HIGH SECURITY
- MANY WAYS TO COMPROMISE
  - Picking, impressioning, decoding, bumping
  - Mechanical bypass
- NO AUDIT TRAIL, NO OPTIONS
- LIMITED WAYS TO MAKE SECURE

# ELECTRO-MECHANICAL LOCKS

# CLIQ TECHNOLOGY

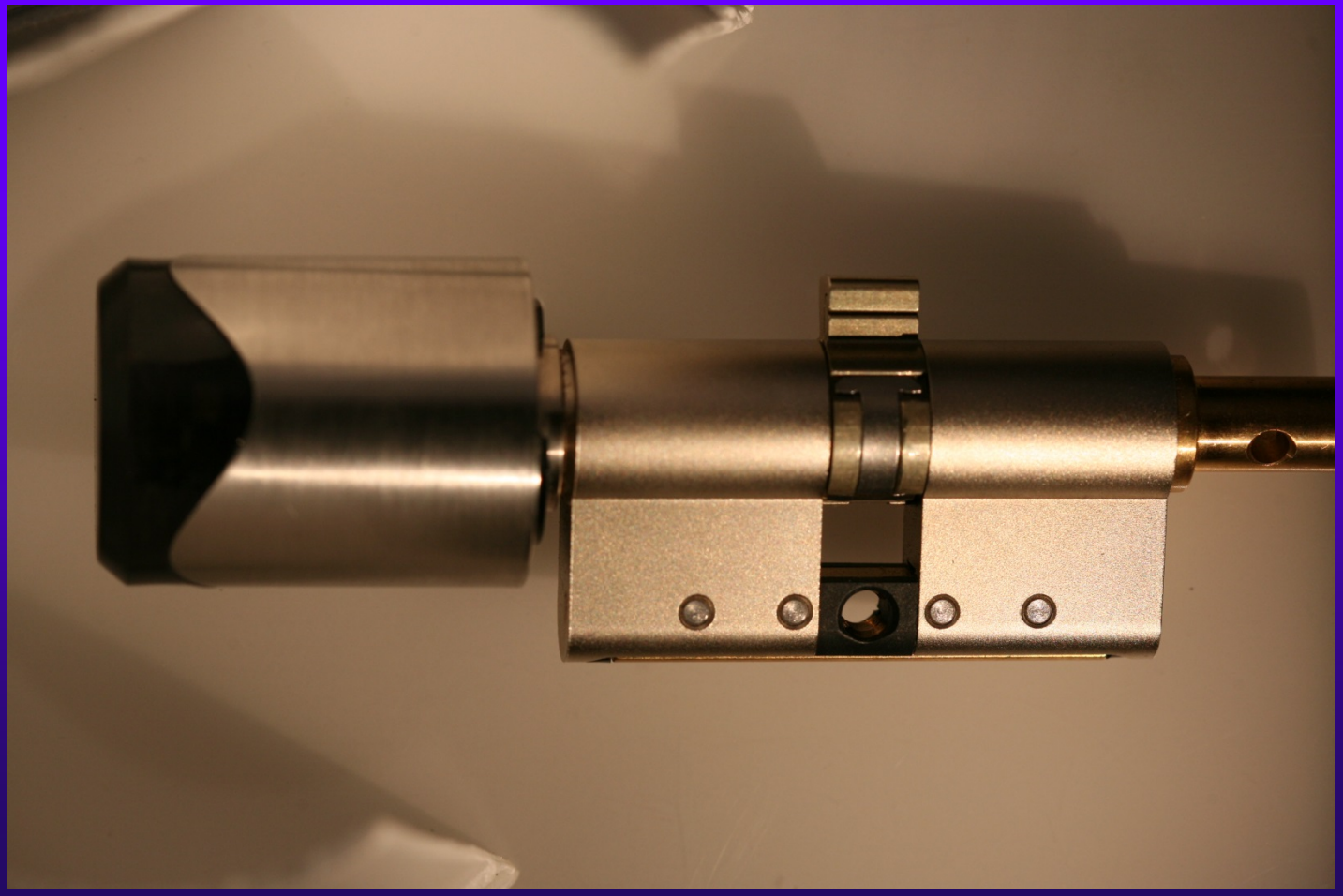




# ATTRIBUTES FOR ELECTRO-MECHANICAL LOCKS

- MECHANICAL SECURITY AND ELECTRONIC CREDENTIALS
- COMPROMISE IN DESIGN
- TWO INDEPENDENT LAYERS
- KEYS WITH CREDENTIALS
- AUDIT TRAIL
- POWER OR NO POWER
- BYPASS CREDENTIALS
- CREDENTIALS MUST TRANSLATD TO MECHANICS TO CONTROL THE BOLT

# E-CYLINDER AND ACCESS CONTROL SYSTEMS



# E-CYLINDER ATTRIBUTES

- NO KEYWAYS
- FULLY ELECTRONIC CREDENTIALS ARE ENTIRE SECURITY
- HOTELS, RESIDENCES, OFFICES
- STAND-ALONE, NETWORKED, WIRELESS, DATA-ON-CARD
  - RFID, SMART CARDS, NFC
  - WIRELESS AUTHENTICATION SERVERS
  - NOT HIGH SECURITY

# E-CYLINDERS

- POPULAR IN EUROPE, WILL BE IN NORTH AMERICA
- HOTELS, OFFICES
- ONE SECURITY LAYER, NO KEYS
- CAN BE DEFEATED
- RELY ON CRYPTOGRAPHY FOR SECRITY

# SOME OF OUR TOOLS

- LOCK MANIPULATION TOOLS FOR MECHANICAL BYPASS
- COVERT ENTRY TECHNIQUES
  - Picking, Decoding, Impressioning, Bumping
- LAWS OF PHYSICS
- MECHANICAL ENGINEERING PRINCIPLES

# MORE TOOLS

- TEMPERATURE EXTREMES
- WIRES, SHIMS
- MAGNETICS
- NEWTONS LAWS OF MOTION
- GRAVITY, SPRINGS, MOVING ELEMENTS
- SHOCK AND VIBRATION
- INERTIA, FRICTION

# INSECRITY ENGINEERING RULES

- THE KEY NEVER UNLOCKS THE LOCK
- ELECTRONS DO NOT OPEN DOORS
- WHATEVER IS SECURE TODAY WILL NOT BE TOMORROW
- YOU DON’T KNOW WHAT YOU DON’T KNOW
- ENGINEERS ONLY KNOW HOW TO MAKE THINGS WORK
- PATENTS DO NOT MEAN SECURITY

# MORE RULES

- IT MAY TAKE EXPERTISE TO DEVELOP AN ATTACK BUT NOT TO LEARN IT
- THERE ARE NO MORE SECRETS
- OFTEN A MANUFACTURER DOES NOT KNOW ABOUT VULNERABILITIES
- ANY OPENING CREATES VULNERABILITY
- THINGS ARE RARELY AS THEY APPEAR

# CRYPTO AND LOCK DESIGN

- LOCKS THAT EMPLOY ELECTRONIC-BASED CREDENTIALS
  - Electro-mechanical, e-cylinders and Electronic Access Control
  - Credentials must be secure especially as only security layer
  - Interface must also be secure
  - It is not just about credentials
  - How crypto fits into lock design

# WHY CRYPTOGRAPHY CAN BE IRRELEVANT

- Credentials are only one security layer
- If not designed properly, credentials are meaningless
- Cryptography has its place if all else is designed securely
- Mechanical designs can be circumvented
- Crypto failures and OS failures
- Recent Onity Lock failures worldwide

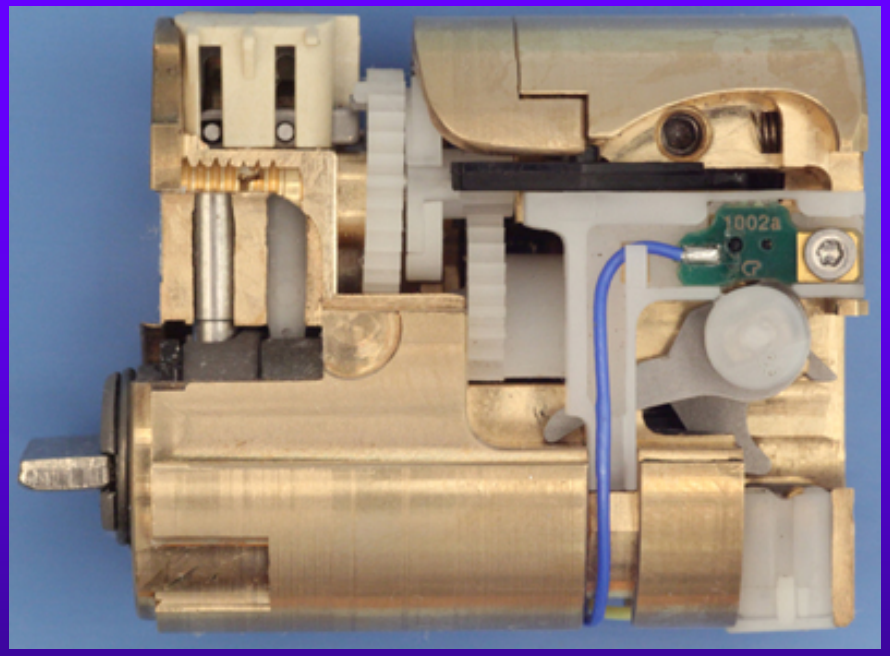
# FUTURE OF LOCK DESIGNS

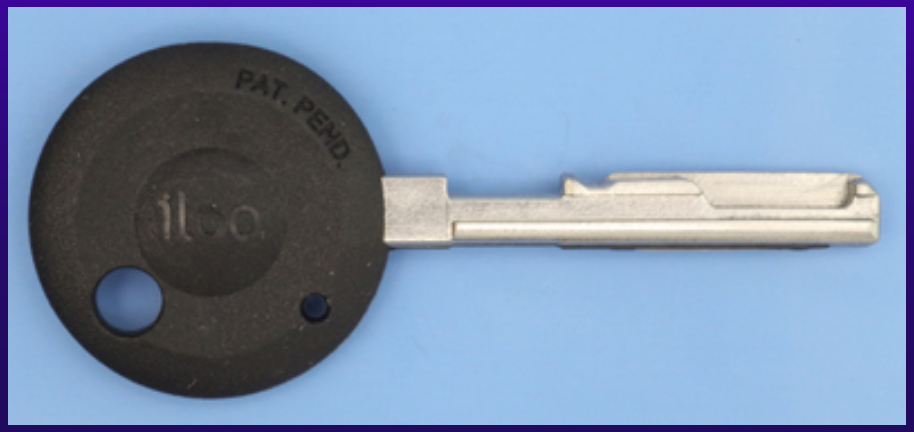
- Electronic access control systems
- Wireless integration: Assa Abloy Aperio
- Mobile keys: remote management
- Data-on-Card systems: Salto
- NFC, Bluetooth and Smartphones
- More e-cylinders
- Merging of mechanical and electronic
- Public communications systems use

# CASE EXAMPLES

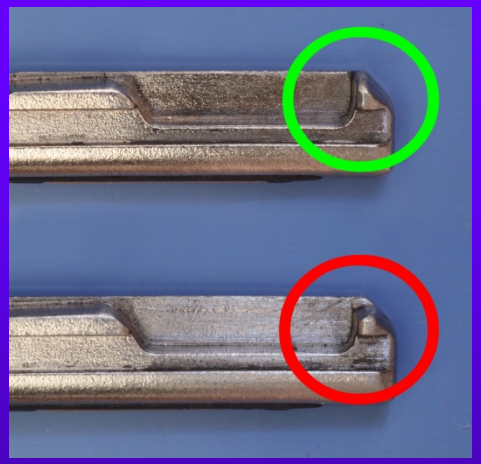
- ILOQ ELECTRO-MECHANICAL
- BIOLOCK FINGERPRINT LOCK
- IN-SYNC RFID CYLINDER
- E-CYLINDER DEFEAT
- STACK-ON BIOMETRIC SAFE

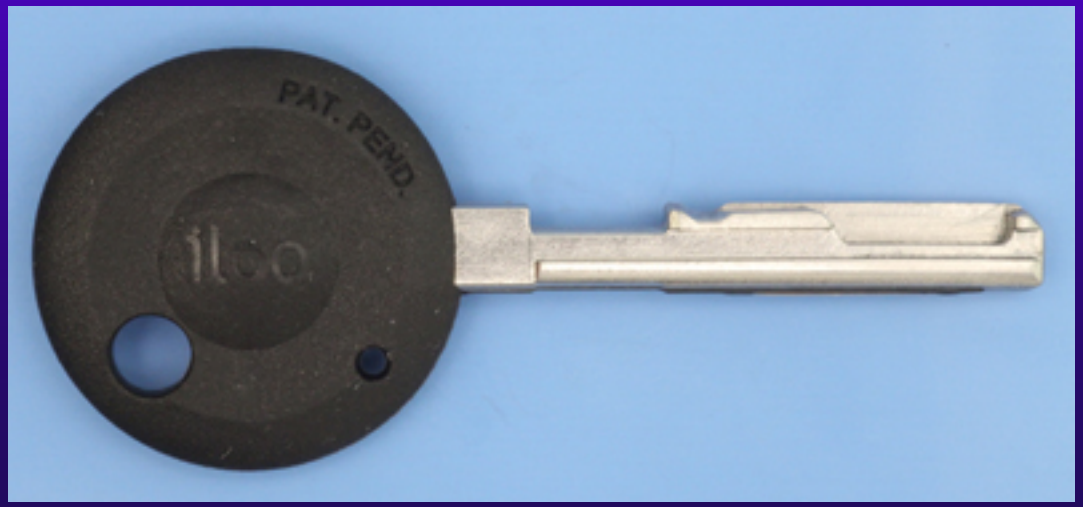
# ILOQ E-MECHANICAL



# DEFEAT OF CREDENTIALS



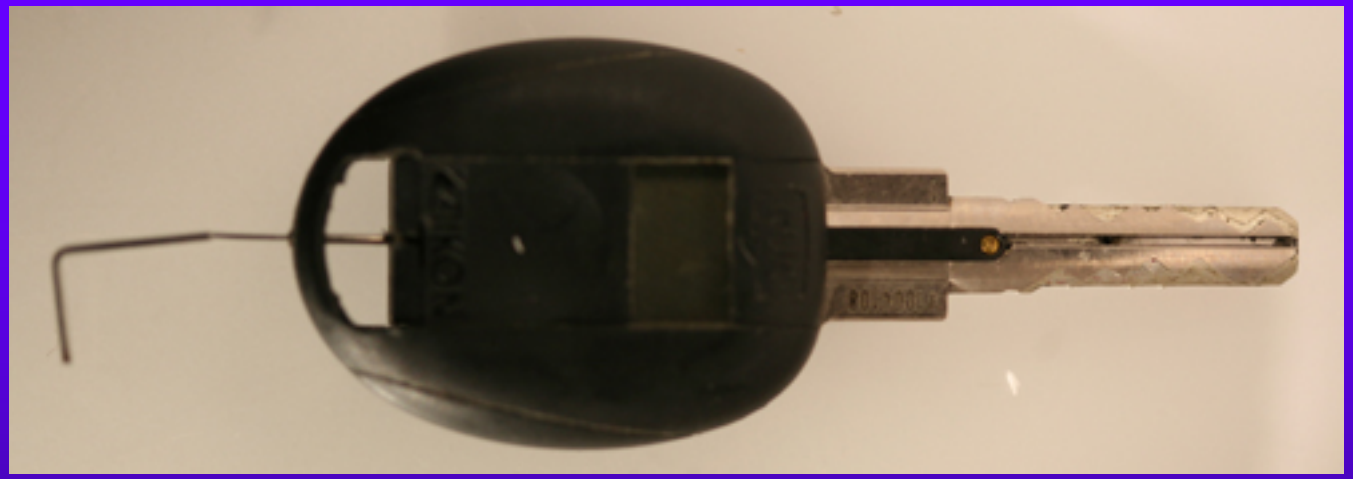


# ILOQ BYPASS

# BIOLOCK FINGERPRINT

# RFID-BASED CYLINDER

# E-CYLINDER DEFEATS



# MAGNETIC ATTACK

**Uhlmann & Zacher**
Security Issue

**Product mainly distributed by:**
Häfele, Dorma, Primion
and others...

# BIOMETRIC GUN SAFE

# INSECURITY ENGINEERING HAS REAL CONSEQUENCES

# CRYPTOGRAPHY AND LOCK DESIGN: EQUAL FACTORS

- MECHANICAL DESIGNS AND ELECTRONIC CREDENTIALS ARE EQUAL IN IMPORTANCE
- SECURITY ENGINEERING MUST RELY ON MULTIPLE SECURITY LAYERS
- EACH LAYER MUST BE SECURE

# CRYPTOGRAPHY AND LOCK DESIGN


- © 2013 Marc Weber Tobias and Security Laboratories


- mwtobias@security.org