THE REVERSE ENGINEERING OF INSECURITY: How, Why and What

LOCKS ARE SECURITY PUZZLES

SECURITY LABS and Security Engineering Lab

SECURITY LABS:
What we do for our clients

- Team of security and legal professionals
- Analyze products and reverse engineer them
- Determine vulnerabilities and potential vulnerabilities in design
- Develop exploits and tools
- Work with design engineers to solve
- We find embedded or inherent defects or deficiencies in design of locks and hardware

FIND AND THEN EXPLOIT SECURITY VULNERABILITY

- We exploit them to compromise security
- We open locks that cannot be opened
- We have developed analysis protocols
- We open locks in seconds and have kids do it to demonstrate design defects and deficiencies

LOCKS ARE SECURITY PUZZLES

- Initially we do not know:
  - if they can be compromised in any way
  - if they can be opened
  - if there is a design flaw or vulnerability
  - if you don’t think they can be opened, they probably will not be opened
  - if there is one more step to open that was missed
-

OVERVIEW: THE PROBLEM

- Any mechanical or electro-mechanical lock has moving parts:
  - Alfred C. Hobbs: *"If you can feel one component against the other, you can derive information and open the lock."*

MOVING PARTS: A LOCK CAN BE COMPROMISED

- Decoding, measurement
  - Ikon MCS and Laser Beams to decode
  - Ultrasonic decoding
  - Wire decoders and feelers and special tools
- Impressioning
  - Optical access, Borescopes, Otoscopes
- Interacting elements
  - Springs
  - Access points
  - Mechanical bypass
  - Relationship between all components

ELECTRO-MECHANICAL AND ELECTRONIC LOCKS

ELECTRONIC LOCKS ARE VULNERABLE

- All electronic locks are mechanical because mechanics are required to move latching elements
- Permutation of options, unknown result
- Interaction of electronics and mechanics
- *Electrons do not open doors; mechanics do*

DESIGN FAILURES CAN LEAD TO INSECURITY

- Some are inherent, like pin tumbler lock bumping
- Lever lock impressioning techniques from friction
- Others are design failures

REAL CONSEQUENCES

- They often are unknown for many years

Countless examples that we have worked:

– Simplex 1000 magnetic attack

– Deadbolt designs

– Kryptonite bike lock and tubular designs

– Biometric locks

– Personal safes and gun safes

– Electromechanical locks and RFID based

MECHANICAL ENGINEERS

- Know how to make things work
- Do not know how to break things
- Different thought processes
- We use different tools and techniques

SEL

PITT | SECURITY ENGINEERING LAB

THE RESULT: INSECURE DESIGNS

- Facilities and critical infrastructure at risk
- Customers at risk
- Public can be at risk
- All security is about liability
- Legal and regulatory ramifications

FEW PROBLEMS ARE OBVIOUS OR EASILY FOUND

- The Japanese Puzzle box: A security analogy
  - Looks impossible to open
  - Looks and feels secure
  - Often no known methods of attack
  - No known specific tools or techniques
  - DefCon Kids example and our greatest fear
    - Puzzle box
    - E-Plex attack: 9 year old

OUR TOOLS AND TECHNIQUES

- OUR FOCUS: 3 PRIMARY ISSUES:
  - *Covert methods of entry*
  - Forced methods of entry
    - Hybrid attacks: forced and covert
  - Key control attack
- A key or code is the simplest way to open a lock
  - Simulate, duplicate, replicate

SECONDARY ANALYSIS

- WHAT REALLY OPENS THE LOCK
- Component Failure Analysis and Why: Case example
  - High security lock, 25 years secure
  - Had examined several times before
  - Non-critical component failure
  - Compromised entire security

MECHANICAL BYPASS AND OPTIONS ARE SUSPECT

- Any part or process that can open the lock is critical to security
  - Audit trails
  - Reprogramming functions
  - Mechanical bypass functions
  - Lock overrides
  - Remote open options
  - Reset functions and micro switches
  - Interaction of mechanical components

NON-TRADITIONAL METHODS OF BYPASS

- MANY NON-OBVIOUS METHODS
  - PX Lock example: wire and current
  - Iloq example
  - Reverse picking attack
- Physical design issues: not apparent, two examples:
  - Deadbolt attack
  - mortise cylinder attack

OUR TOOLS TO DEFEAT SECURITY

- Imagination and a matrix of options in unforeseen or unanticipated combinations
- Traditional Mechanical techniques
  - Picking
  - Impressioning
  - Theory
  - Traditional techniques
    - John Falle, lever locks
    - Kensington, BIC pen on tubular locks

MORE TOOLS

- Decoding
  - Must understand the interaction of components to determine decoding
  - Use of marking materials, plasticine
  - VingCard: carbon paper and wires
  - Use of optics, borescopes
  - Medeco Falle decoder
- Bumping, shock, vibration
- Extrapolation of TMK

MECHANICAL BYPASS

- SHOCK AND VIBRATION
  - S&G locks on WWII ships
  - Lock bumping, conventional and high security
  - HP computer lock
  - Safes
  - Winfield
  - Solenoids in safes

MORE TOOLS

- Temperature extremes
- Wires, shims
- Magnetics: Examples
  - Read, decode, simulate: EVVA
  - Simplex 1000
  - Electric strikes
  - Videx solenoid-based locks

INDIRECT ACCESS TO LOCKING MECHANISMS

- MANY EXAMPLES OF BYPASS
- Iloq
- Deadbolt indirect access to tailpiece
- InSync USB port attack
- Simplex 1000
- E-Plex 5000

EXPLOIT DESIGN FAILURES

- Mechanical
- Closed but not locked scenarios
- VingCard: wire, carbon paper
- Electronic locks mechanical conponents
- Rotor control
- Access re-program buttons, microswitches
- Programming override

MORE EXPLOITS

- Key lock override of electronics
- Remote open options bypass
  - Electro-mechanical
  - Safes
  - Electronic locking systems
- Electronic techniques
  - Bypass electronic credentials mechanically
  - Magnetics
  - Electric fields
  - Direct motor control

INTERSECTION: SECURITY AND PHYSICS

- Much of what we do involves laws of physics
- As a lawyer, I cannot change them but can exploit them
- As engineers, you need to understand them
- Rules of physics apply to opening locks
- Exploit the laws of physics to open locks

LAWS OF PHYSICS and POTENTIAL ATTACKS

- Gravity
- Springs
- Moving elements
- Newton’s Laws of Motion
  - First Law: Objects at rest tend to stay at rest
  - Third Law: for every action there is an equal and opposite reaction
- Lock bumping

MORE LAWS OF PHYSICS

- NEWTON FIRST LAW OF MOTION
  - e-cylinder attack example
  - Acceleration and deceleration of components
- NEWTONS THIRD LAW OF MOTION
  - Springs and locking pins: PC Guardian
  - Rapping of safes to retract bolt
  - Wendt drill motor impact tool to open safes

TEMPERATURE

- Temperature: Expansion and contraction
- Temperature and fracture
- Thermal relockers
- Electric wires, cylinder design, open with hair dryer or hand-held torch

MORE PHYSICS

- X-Ray and lead balls in combination locks
- High speed spinning to open e-cylinders and lock components
- Air pressure
  - Use of tennis balls to open car locks, pneumatic system
- Pressure applied to internal components
  - VingcCard and decoding
- EMP attacks

MORE TECHNIQUES BASED UPON LAWS OF PHYSICS

- Induction and induced fields
- Audio resonance to measure components and move them
- Ultrasonic decoders with Piezo transducers
- Audio attacks: Medeco and metal center pin to prevent decoding of length

PURE PHYSICS ATTACKS

- Inertia (linear and rotational, moment of inertia tensor) Momentum - and Energy-Conservation (linear and rotational)
- Friction
  - Sticking and slide friction, rolling friction (No interaction without friction)
  - Influence of surface roughness
  - Influence of (normal) pressure

MAGNETICS AND COILS

- Magnetism and Curie Point
  - Induction and Lorentz force
  - Para, Dia- und Ferro-magnetisms
- Magnetic resonance, susceptibility, coercivity
  - Soft and hard magnetic materials
- Coils (difference of fair-core and iron-core coils)

MOTION

- Oscillation and waves
- Spring and mass
- Resonance and damping (how does the resonance depend on spring rate and mass)
- Thermal expansion (especially: examples for large and small thermal expansion)
- Special effects

SPECIAL APPLICATION OF ENERGY AND MOVEMENT

- Inertia and locks: using elements that normally do not move
- High RPM application to free-spinning cylinders

OUR PRIMARY RULES

- All security is about liability
- Always believe you can defeat a lock
- We look for simple solutions to solve what appear to be complex problems
- Look for exploiting a design or combination of designs
- Identify the problem and probable solutions
- Things are rarely what they appear to be

PRIMARY RULES

- **THE KEY NEVER UNLOCKS THE LOCK**
- ALL LOCKS ARE MECHANICAL
- JUST BECAUSE IT IS PATENTED DOES NOT MEAN IT IS SECURE
- DO NOT RELY ON STANDARDS
- EVERY LOCK CAN ULTIMATELY BE COMPROMISED; REMEMBER THE 3T2R RULE!

MORE PRIMARY RULES

- R&D costs money and a lot of companies take shortcuts
- Any opening creates vulnerability
- Look for the path of least resistance to unlock the lock
- You don’t know what you don’t know

MORE RULES

- Electrons don’t open doors, mechanisms do
- Credentials mean nothing
- Encryption means nothing
- e-cylinder defeats: bypass the credentials

MORE OF OUR RULES

- Never say never: what cannot be opened today will be opened tomorrow
- Small changes in patented design can mean big trouble: Open a can of worms

MORE RULES TO FOLLOW

- All secrets in a lock are self-contained
- We do not like plastic
- PATENTS DO NOT EQUAL SECURITY
  - Patents have nothing to do with security
  - Patented keys mean nothing
- Never know where we will end up with in an analysis of impenetrable locks
  - Medeco case study: bumping, picking, decoding, key control, hybrid attacks

MORE RULES

- Locks are designed to be screwed with
- **Legal faulty logic:** all locks can be opened, so nobody should be liable does not work
- All exploits replicates what the key does
- Easiest way to open a lock is with a key

MORE RULES

- Programming access and audit capability can provide security vulnerabilities
  - E-Plex
- Clever does not mean secure
- Cannot get around the laws of physics
- You must examine both critical and non-critical components for a Component Failure analysis

FINAL RULE

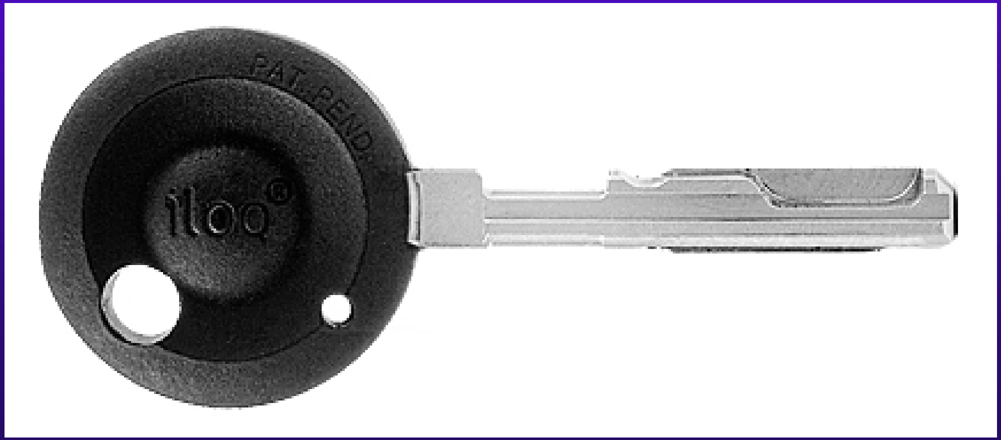
- EVERYTHING IS SUSPECT:
- movable parts, springs, motors, solenoids, ferrous materials, magnetic principles, inertia, coils, mechanical bypass circuits, mechanical override, micro-switches, drain holes, entry points, data ports

CASE EXAMPLE: ILOQ Electromechanical cylinder

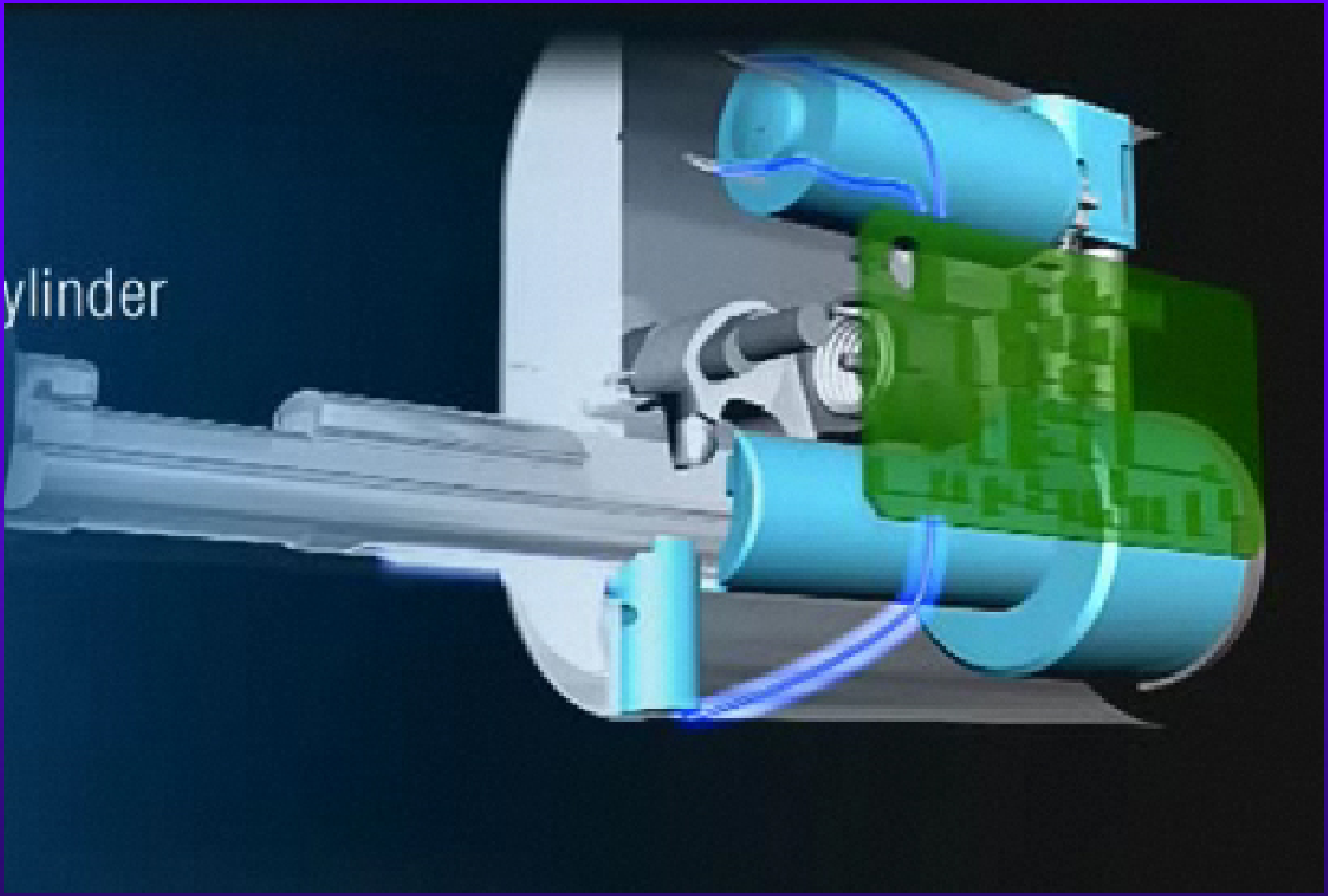
- MADE IN FINLAND
- VERY CLEVER DESIGN: PATENTS
- COST: $200+
- ELECTRO-MECANICAL DESIGN
- MECHANICAL KEY + CREDENTIALS
- NO BATTERIES: LIKE A CLOCK AND MAGNETO, GENERATES POWER
- WIND-UP CLOCK-LOCK

EXAMPLE #2: ILOQ:

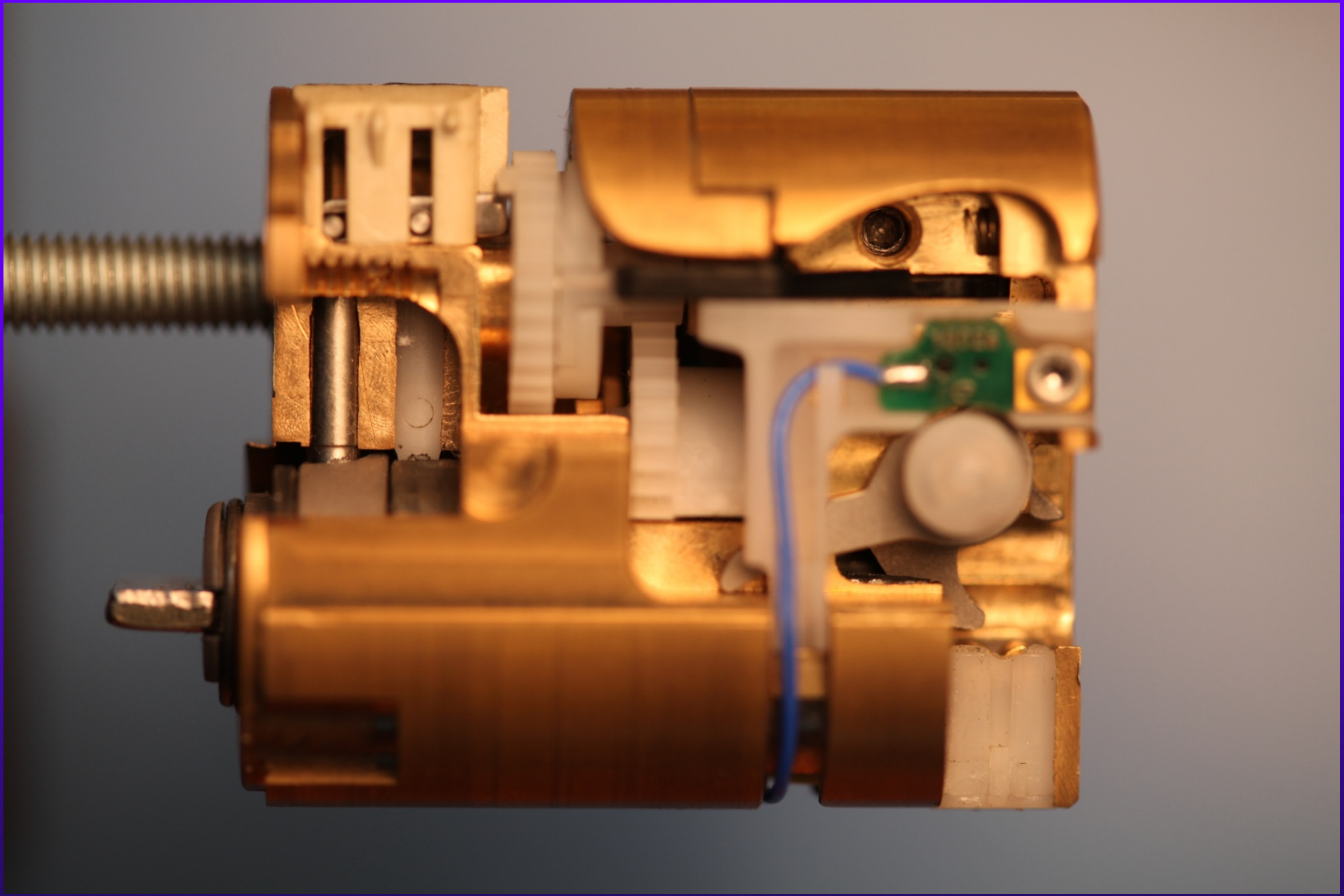
TAKING SECURITY TO A NEW LEVEL



ALL KEYS IDENTICAL



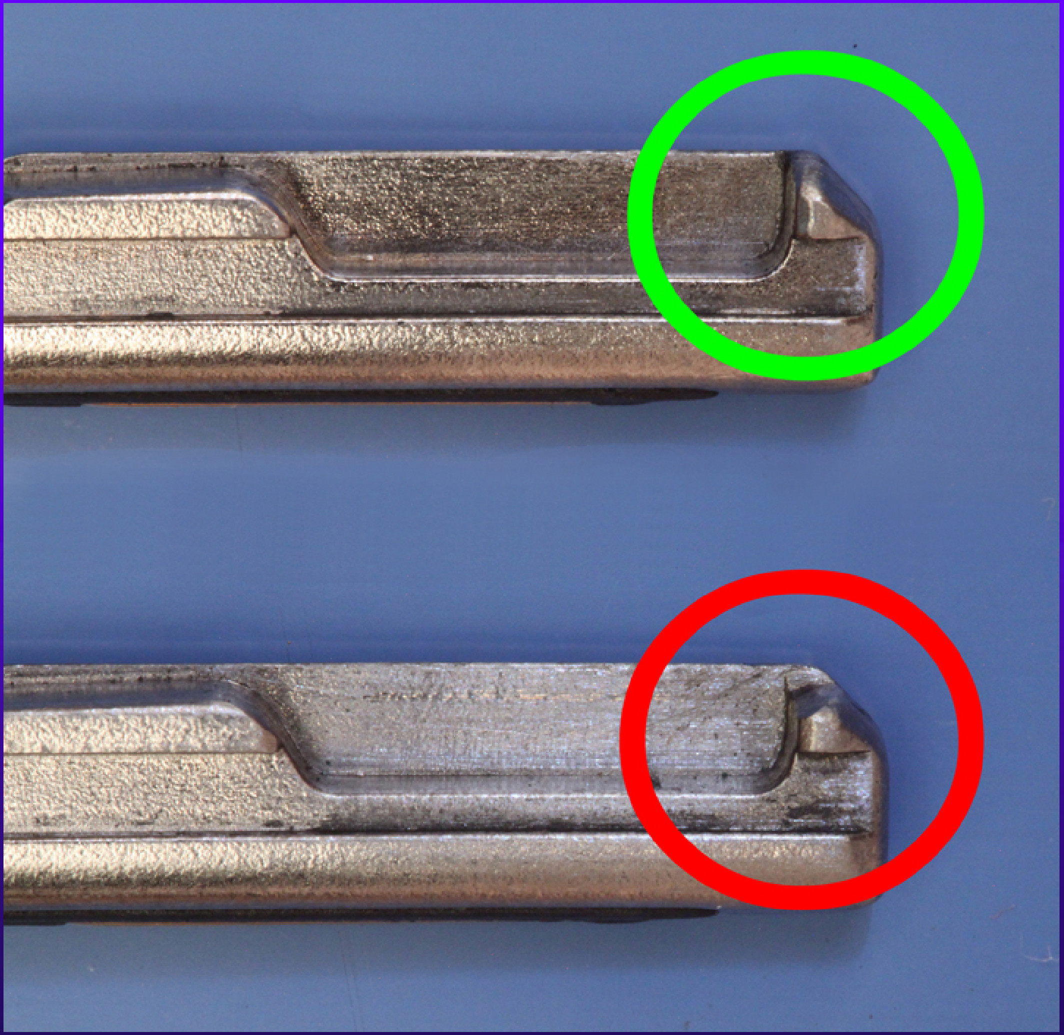
ILOQ: INSECURITY ENGINEERING



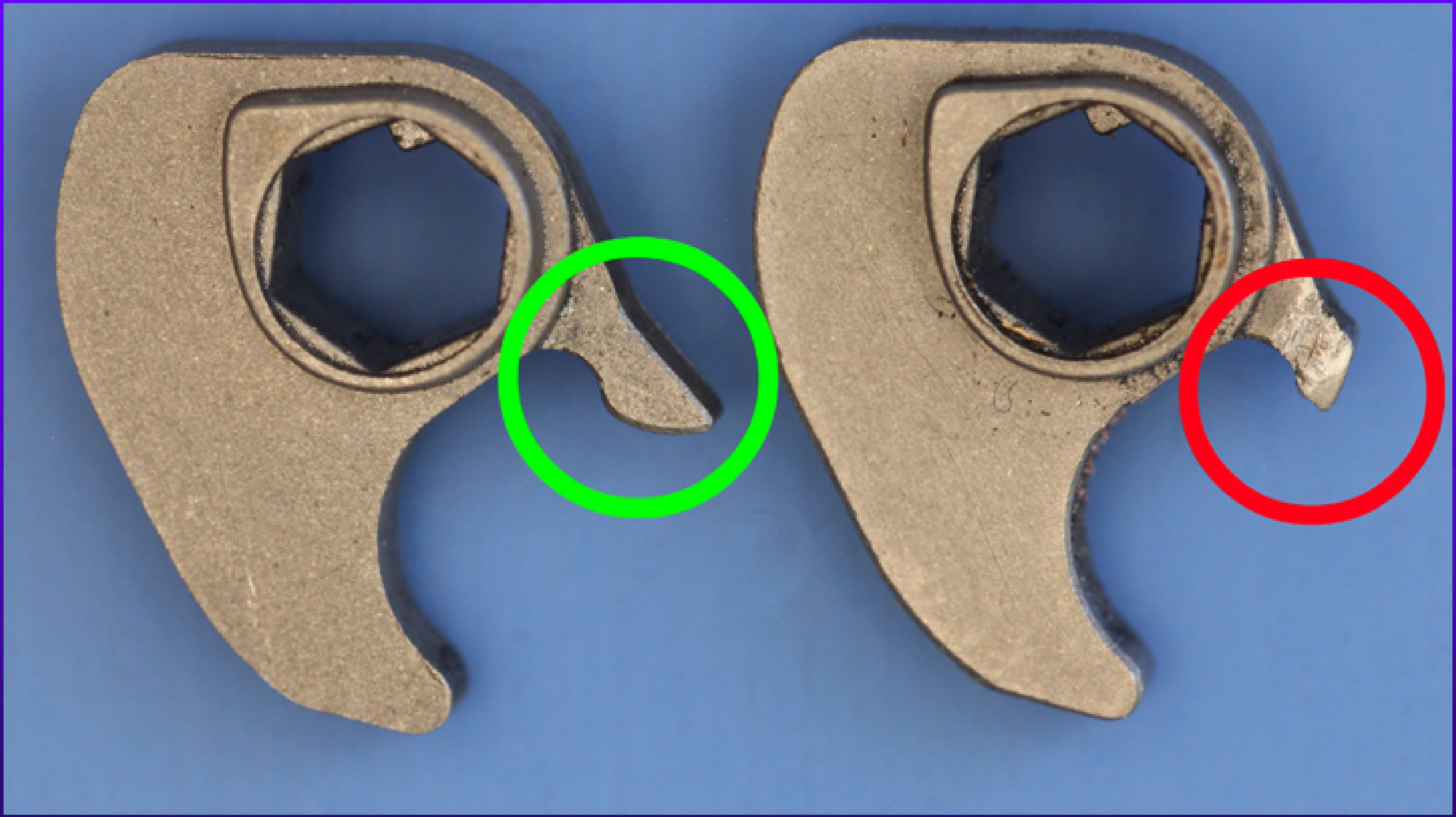
ILOQ VULNERABILITIES

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

THE KEY TO ILOQ INSECURITY

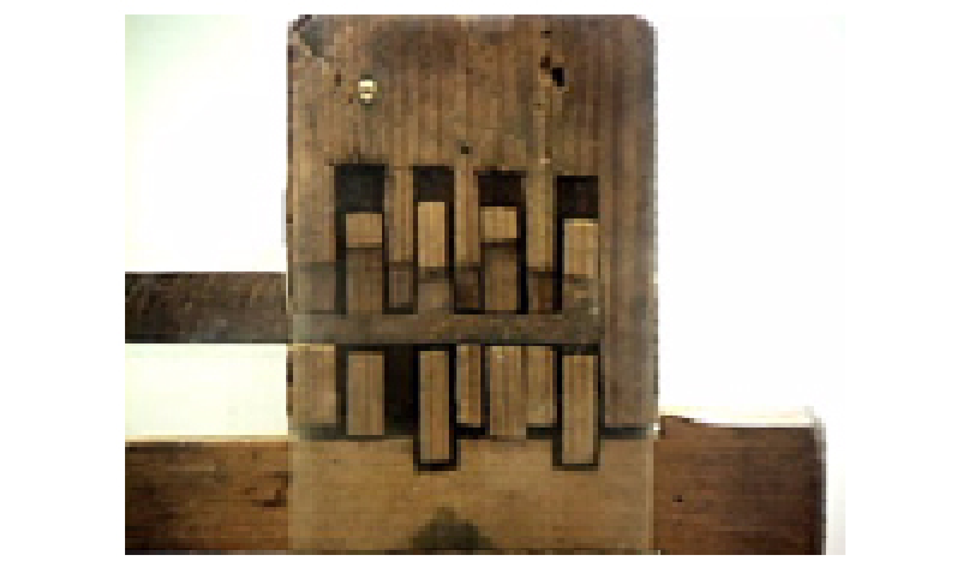


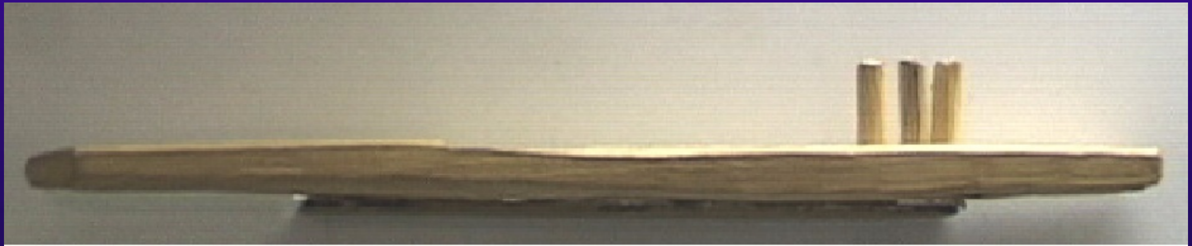
INSECURITY ENGINEERING 101



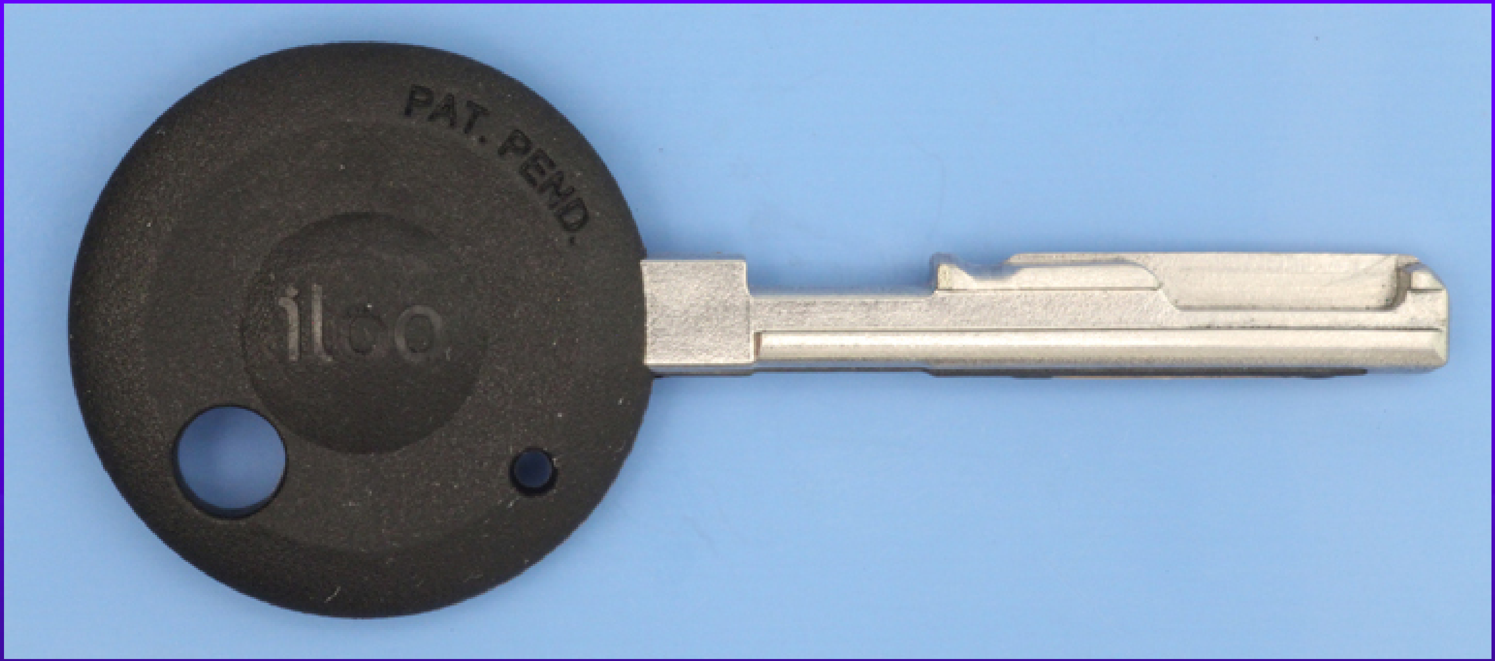
EGYPTIAN PIN TUMBLER v. ILOQ C10S

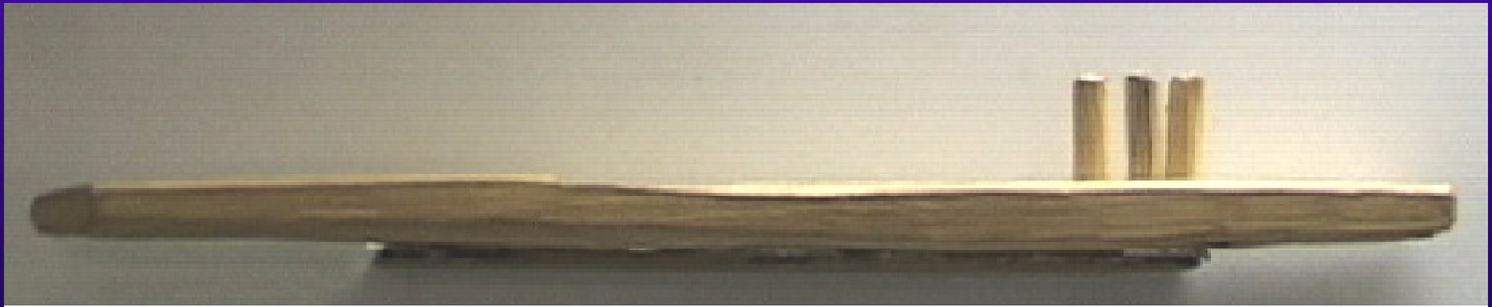
- BYPASS ELECTRONIC CREDENTIALS
  - EGYPTIAN LOCK WINS



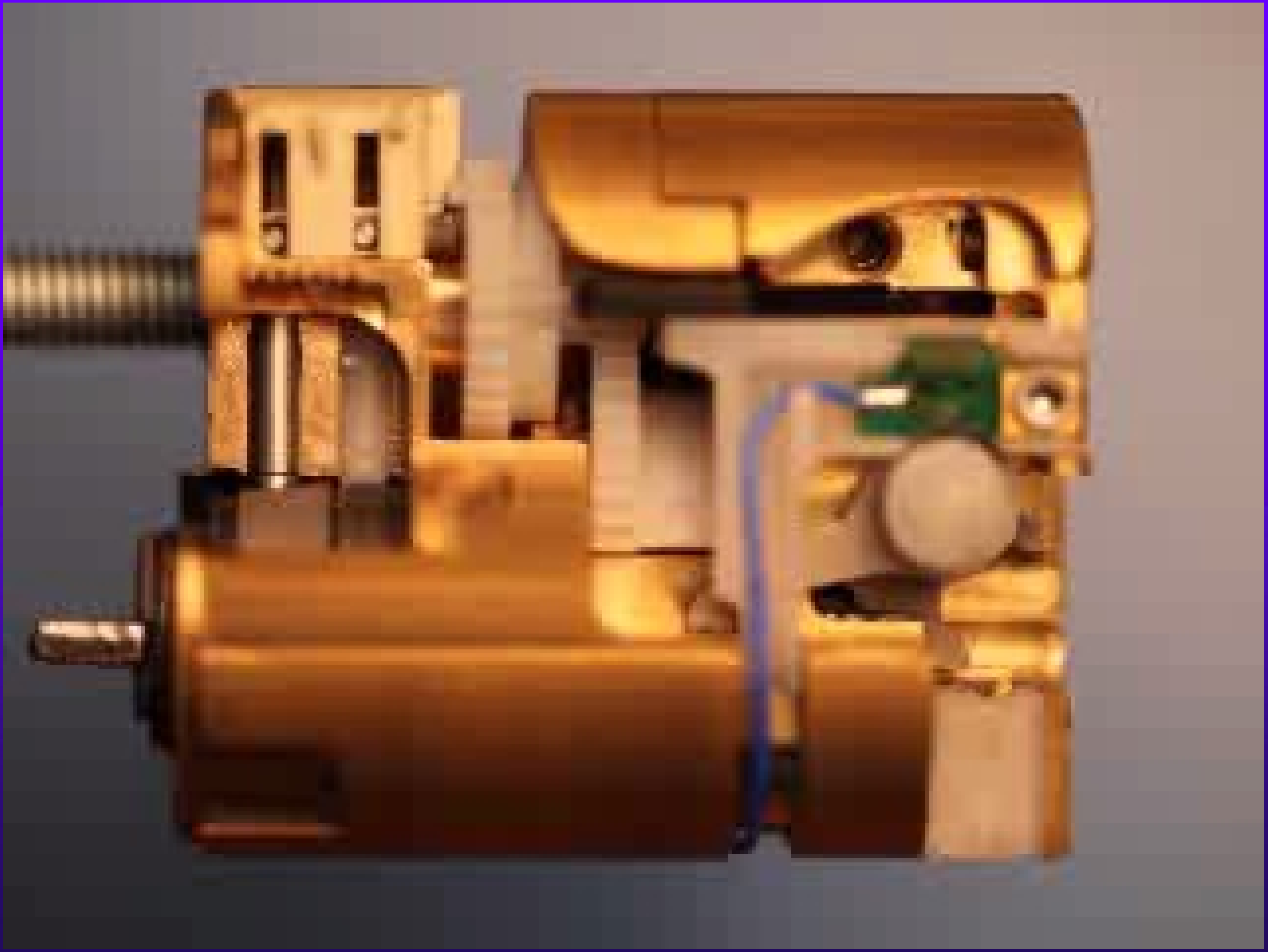


EGYPTIAN: 4000 YEARS AGO v. ILOQ KEYS





ILOQ INSECURITY



REVERSE ENGINEERING OF INSECURITY

- Marc Weber Tobias and Tobias Bluzmanis
- mwtobias@security.org
- tbluzmanis@aol.com
- 1.605.334.1155