VULNERABILITIES

Bypass of Locks by exploiting design issues

HIGH SECURITY LOCKS: Why Important?

- Protect Critical Infrastructure, high value targets
- Stringent security requirements
- High security Standards
- Threat level is higher
- Protect against Forced, Covert entry
- Protect keys from compromise

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
  - Higher quality and tolerances
  - Resistance to Forced and Covert Entry
  - Key control

ATTACK METHODOLOGY FOR HIGH SECURITY LOCKS

- Assume and believe nothing
- Ignore the experts
- Think “out of the box”
- Consider prior methods of attack
- Always believe there is a vulnerability
- WORK THE PROBLEM
  - Consider all aspects and design parameters
  - Do not exclude any solution

HIGH SECURITY LOCKS: Critical Design Issues

- Multiple security layers
- More than one point of failure
- Each security layer is independent
- Security layers operate in parallel
- Difficult to derive intelligence about a layer

HIGH SECURITY: Three Critical Design Factors

- Resistance against forced entry
- Resistance against covert and surreptitious entry
- Key control and “key security”
- Vulnerabilities for each requirement

QUESTIONS: BYPASS AND REVERSE ENGINEERING

- Weakest link in lock to bypass (Medeco)
- What locks the lock?
- What locking elements lock and in what order. Is there a primary element to bypass?
- Result if one layer fails: Can others be compromised?
- What intelligence needed to open the lock?
- Can Intelligence be simulated?

SYSTEM BYPASS: More Questions

- How strong is the sidebar(s) against forced attack
- Is the sidebar the only locking system?
- What if defeat one of two sidebars or security layers?
- Bitting design: spring biased?
- Ability to manipulate each pin or slider to set its code?

SECONDARY SECURITY LAYERS: Techniques

- Telescoping pins
- Sliders and wafers
- Sliders to set sidebars: Medeco
- Pseudo-sidebars = virtual keyways
- Sidebars
  - Most popular
  - Originated in America with GM locks
  - Many locking techniques

LAYERS OF SECURITY AND BYPASS CAPABILITY

- How many
- Ability to exploit design feature?
- Integrated
- Separate
  - Primus = 2 levels, independent, complex locking of secondary finger pins
  - Assa = 2 levels, independent, simple locking, one level

EXPLOIT DESIGN FEATURES AND SYSTEM PARAMETERS

- Codes: design, progression
- Key bitting design
- Tolerances
- Keying rules
  - Medeco master and non-master key systems
- Interaction of critical components and locking systems
- Keyway and plug design

EXPLOIT TOLERANCES

- Sidebar locking: Medeco 10 v. 20 degree
- Relation to codes
- Simulation of codes: Medeco
- Reverse engineer code progression of system from one or more keys?
  - Master key conventional v. positional system
  - Difficulty = replication of keys
  - Medeco v. MCS as example

ATTACKS: Two Primary Rules

- "The Key never unlocks the lock"
  - Mechanical bypass
- Alfred C. Hobbs: "If you can feel one component against the other, you can derive information and open the lock."

METHODS OF ATTACK: High Security 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

ADDITIONAL METHODS OF ATTACK

- Split key, use sidebar portion to set code
- Simulate sidebar code
- Use of key to probe depths and extrapolate
- Rights amplification of key

KEY CONTROL

High security requirement

KEY CONTROL and "KEY SECURITY"

- Duplicate
- Replicate
- Simulate
- "Key control" and "Key Security" may not be synonymous!

KEY SECURITY: A Concept

- **Key control** = physical control of keys
- Prevent manufacture and access to blanks
- Control generation of keys by code
- Patent protection
- Key security = compromise of keys
  - Duplication
  - Replication
  - Simulation

KEYS: CRITICAL ELEMENTS

- Length = number of pins/sliders/disks
- Height of blade = depth increments = differs
- Thickness of blade = keyway design
- Paracentric design
- Keyway modification to accommodate other security elements
  - Finger pins
  - Sliders

KEY CONTROL: Critical issues

- Simulation of code or key components
- Security of locks = key control and key security
  - All bypass techniques simulate actions of key
  - Easiest way to open a lock is with the key

KEY CONTROL and "KEY SECURITY" ISSUES

- Most keys are passive: align = open
- Simulate components of key
- Replicate critical components
- Duplicate critical components
- Require interactive element for security
  - MUL-T-LOCK element
  - MCS magnets

KEY CONTROL: Design Issues

- Bitting design
- Bitting and sidebar issues and conflicts and limitations in differs
- Ability to decode one or more keys to break system
- Consider critical elements of the key: require to insure cannot be replicated
- Hybrid attacks using keys
  - Medeco mortise cylinder example

DUPLICATION AND REPLICATION OF KEYS

- Key machine
- Milling machine: Easy Entrie
- Clay and Silicone casting
- Key simulation: Medeco
- Rights amplification
- Alter similar keys

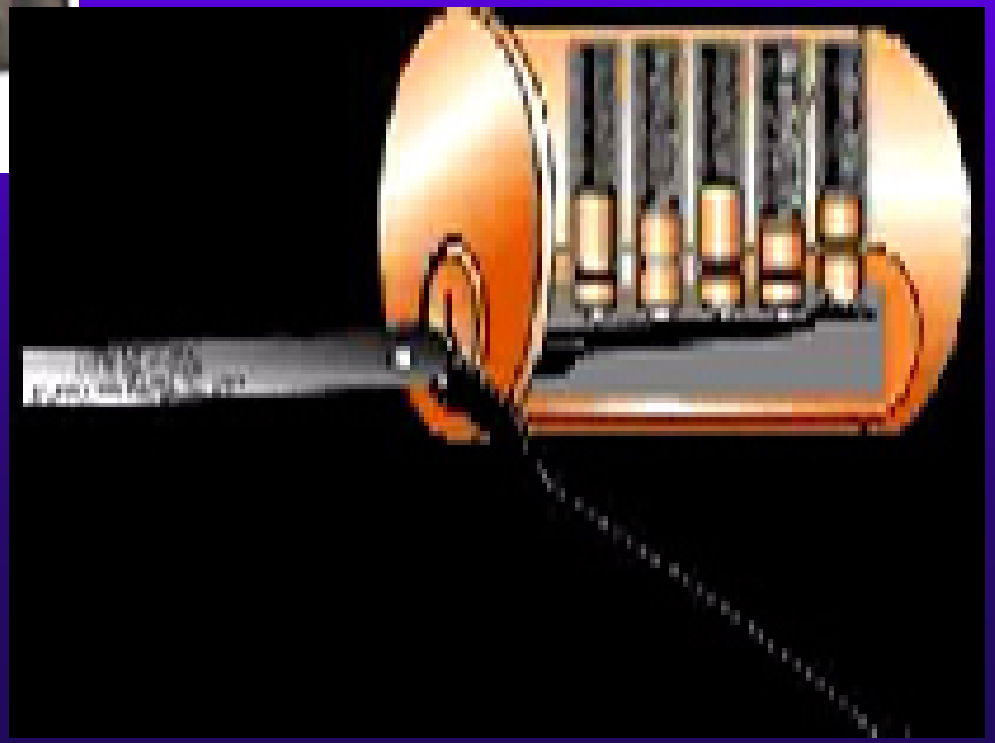
COVERT and FORCED ENTRY RESISTANCE

High security requirement

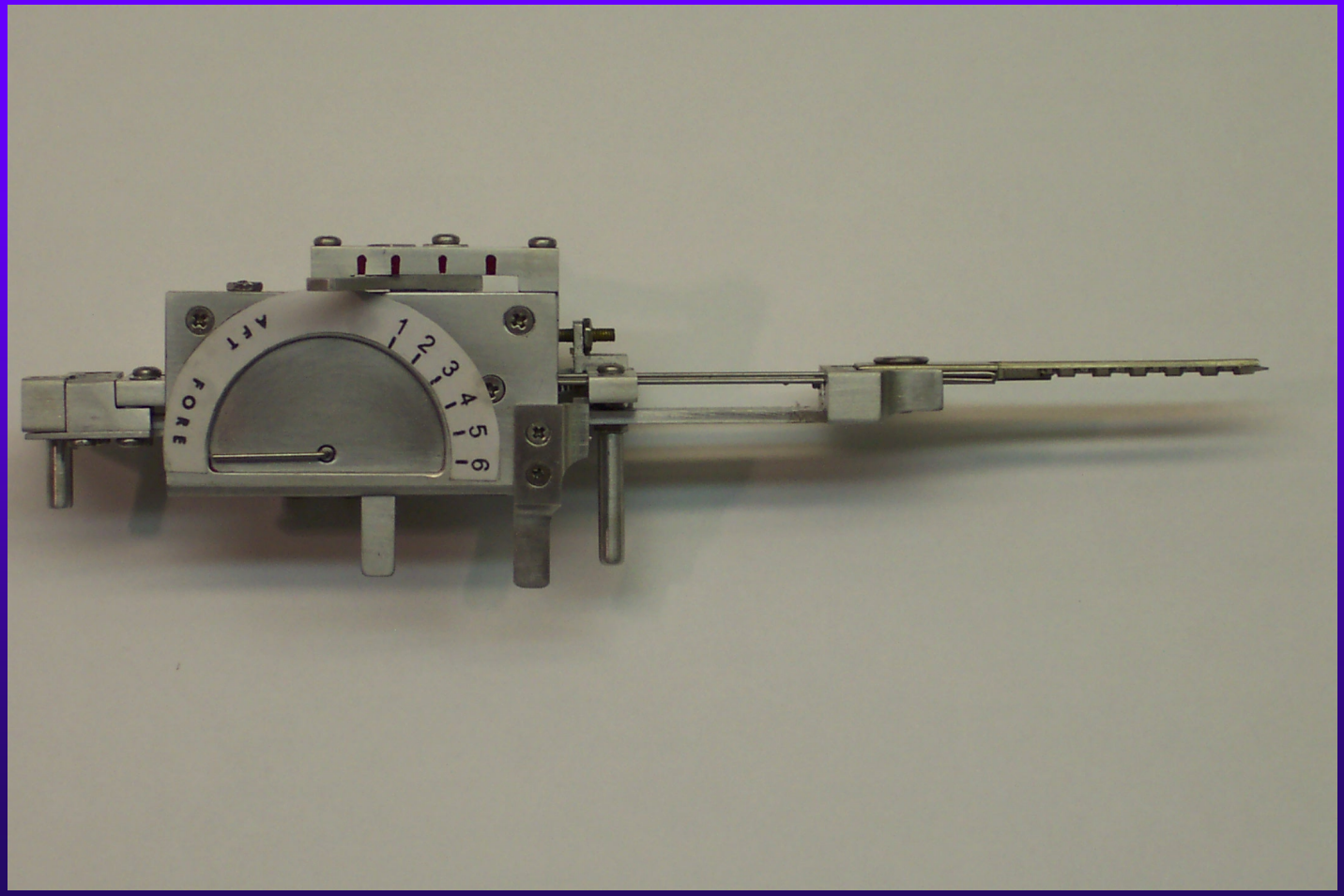
STANDARDS REQUIREMENTS

- UL and BHMA/ANSI STANDARDS
- TIME is critical factor
  - Ten or fifteen minutes
  - Depends on security rating
- Type of tools that can be used
- Must resist picking and manipulation
- Standards do not contemplate more sophisticated methods

CONVENTIONAL PICKING

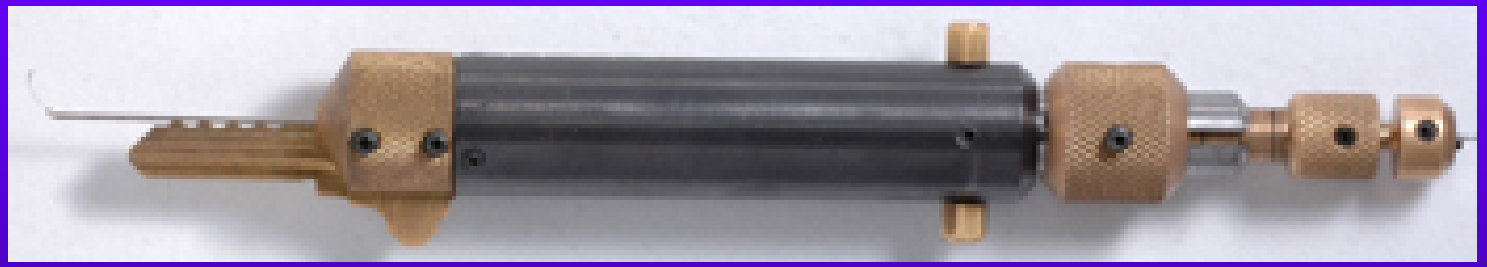


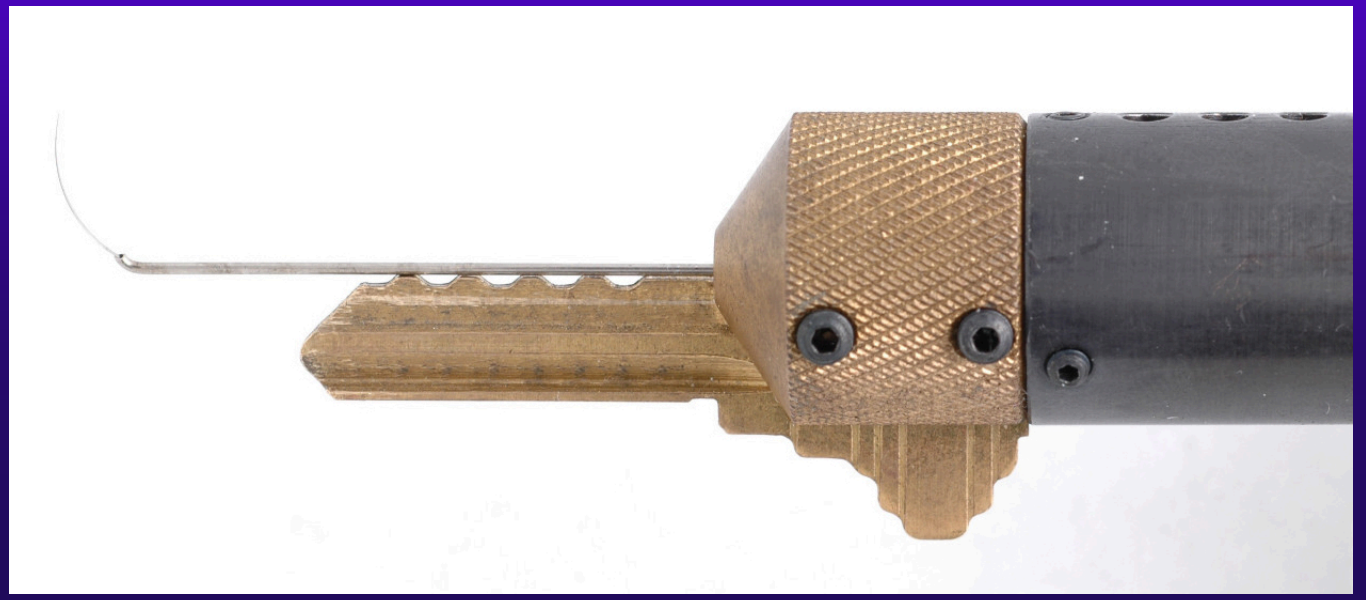
TOBIAS DECODER:
Medeco decoder: by “Crackpot!”



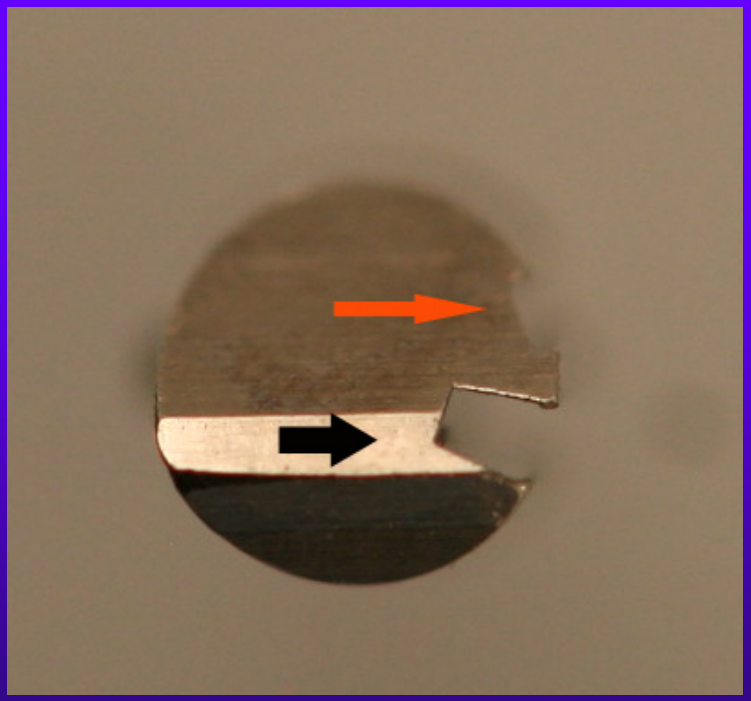
SOPHISTICATED DECODERS

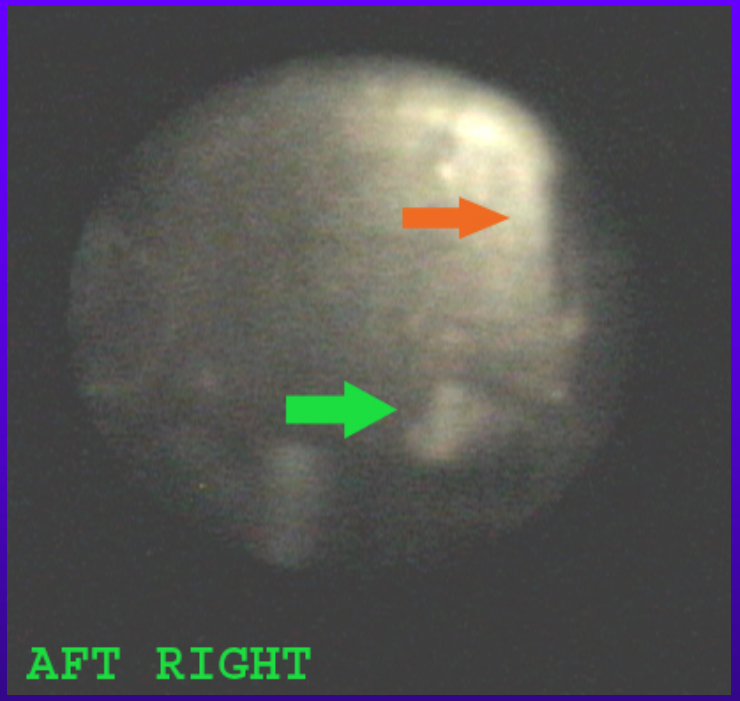
- John Falle: Wire Shim Decoder





DECODE PIN ANGLES





FORCED ENTRY RESISTANCE

High security requirement

FORCED ENTRY ATTACKS: Deficiencies in standards

- Many types of attacks defined
- Do not contemplate mechanical bypass
- Must examine weakest linkis
- Do not cover “hybrid attacks”
  - Medeco deadbolt attacks
  - Medeco mortise attack

SIDEBAR: Bypass and Circumvention

- Direct Access
  - Decoding attacks
  - Manipulation
  - Simulate the sidebar code (Medeco)
  - Use of a key (Primus and Assa
- Indirect access
  - Medeco borescope and otoscope decode issues

SIDEBAR ATTACK: Physical Strength

- Independent protection
- Integrated with pin tumblers or other critical locking components
- Compress plug
- Defeat of sidebar as one security layer: result and failures
- Anti-drill protection

FORCED ENTRY ATTACKS

- Direct compromise of critical components
  - Medeco deadbolt 1 and 2 manipulate tailpiece
- Hybrid attack: two different modes
  - Medeco reverse picking
- Defeat of one security layer: result
  - Medeco Mortise and rim cylinders, defeat shear line