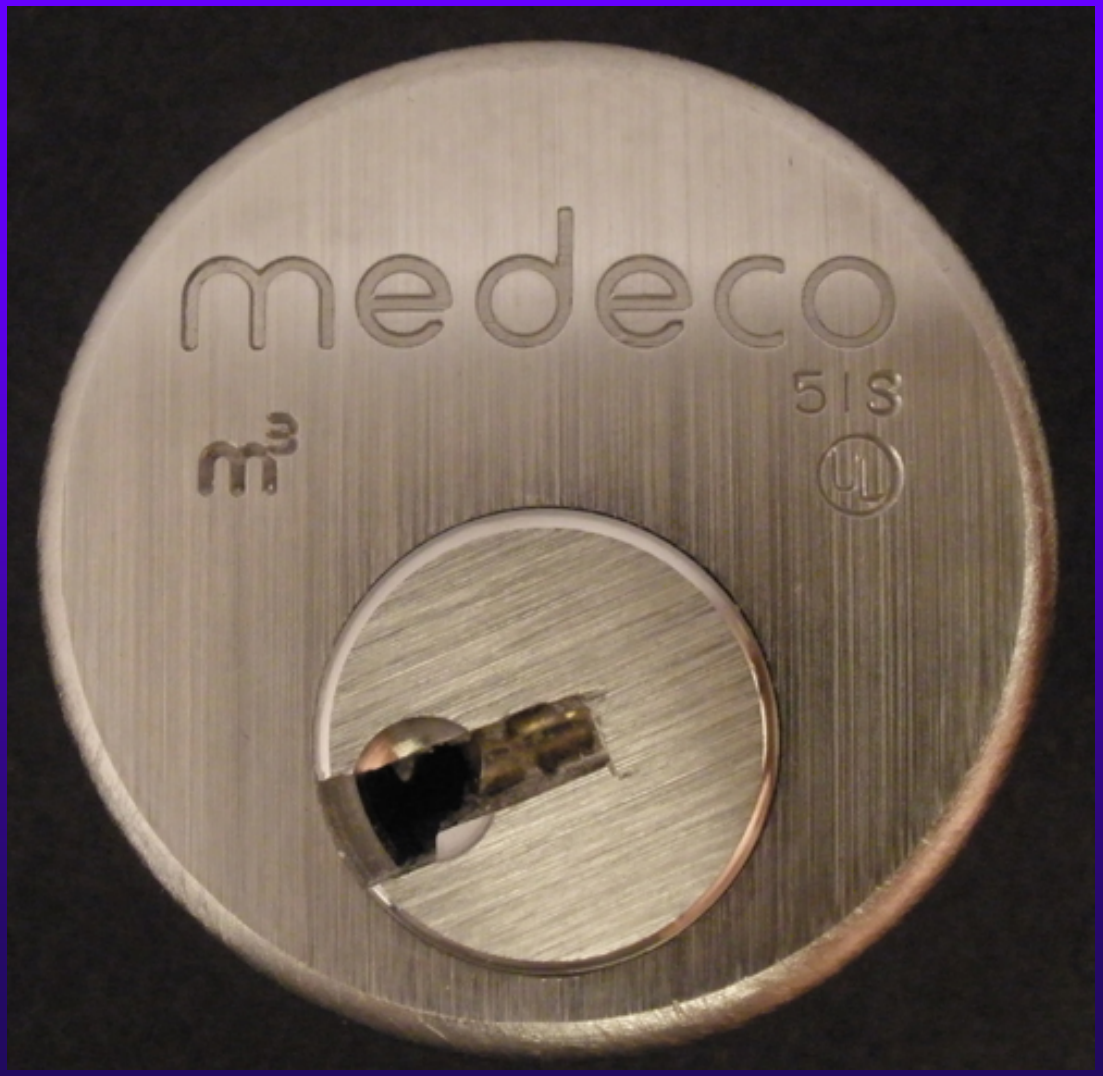
LSS+^{x} HIGH SECURITY SUPPLEMENT to LSS+

THE COMPROMISE OF MEDECO HIGH SECURITY LOCKS:

New Techniques of Forced, Covert, and Surreptitious Entry

MEDECO HIGH SECURITY



MEDECO HIGH SECURITY: What it means

- 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

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

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

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

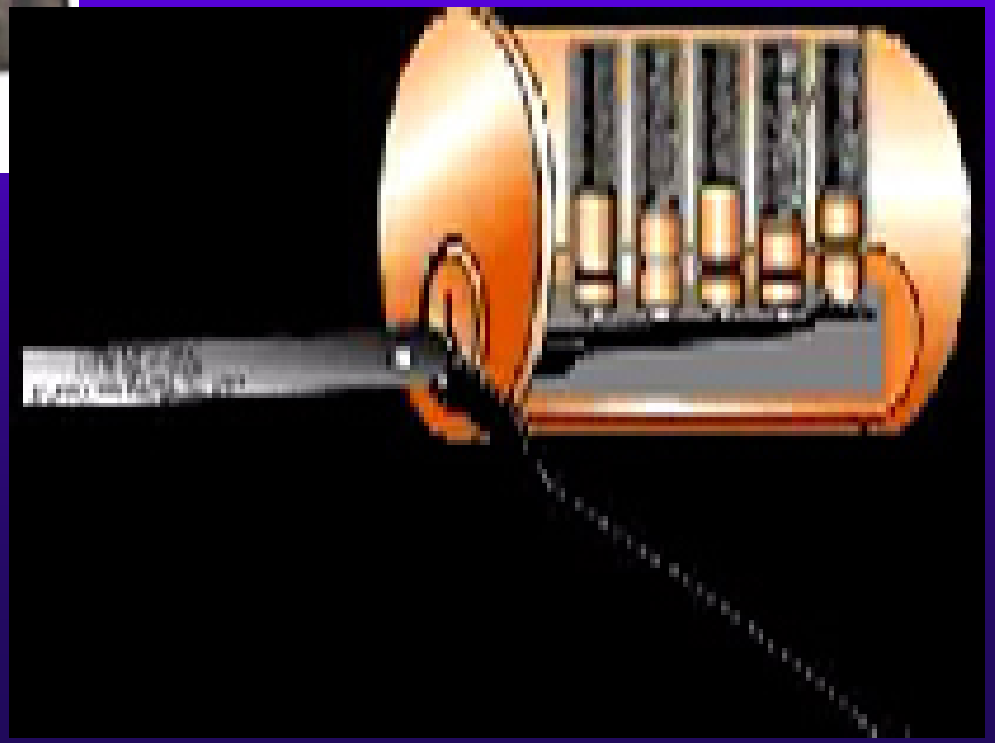
KEY CONTROL: Critical issues

- 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

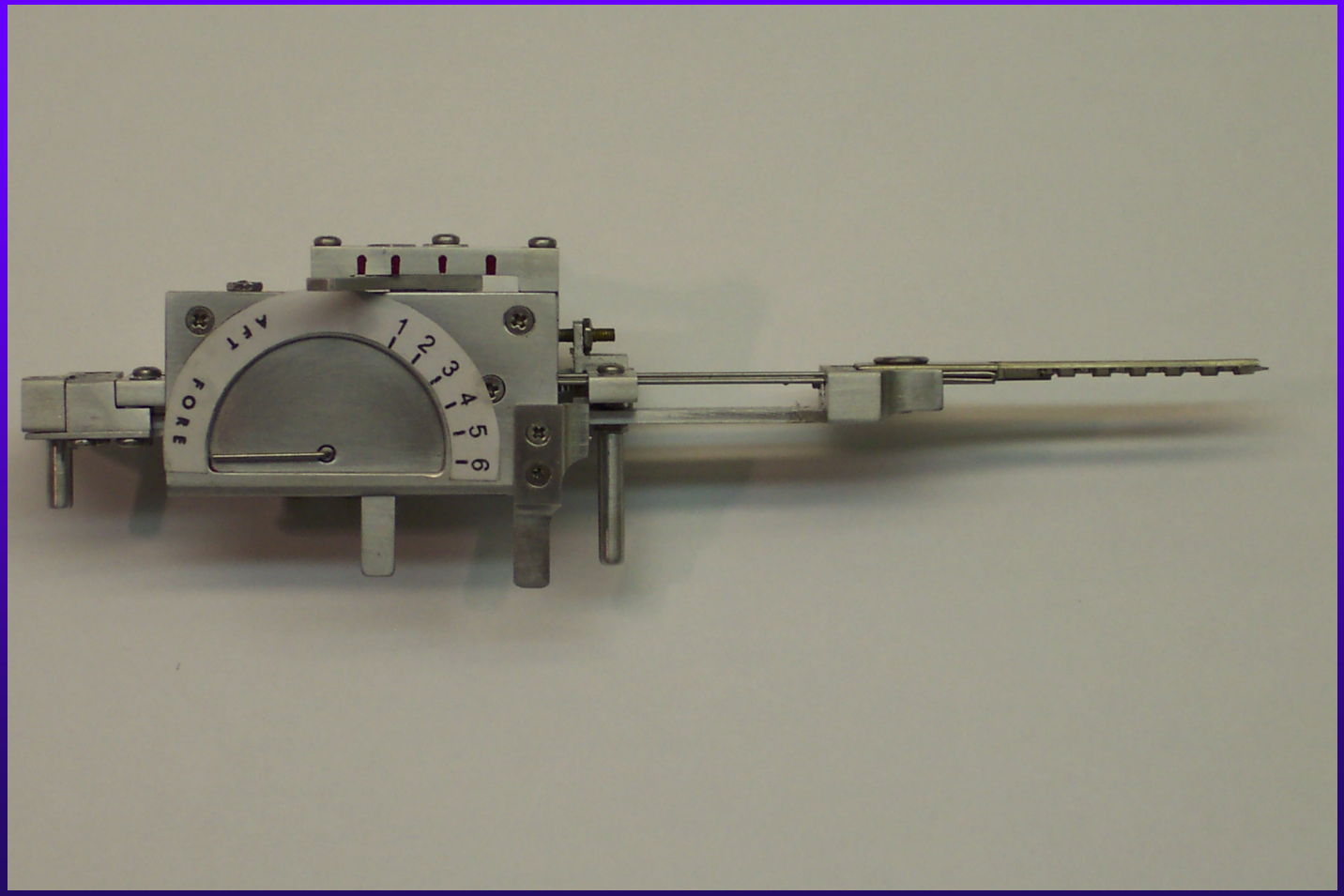
COVERT and FORCED ENTRY RESISTANCE

High security requirement

CONVENTIONAL PICKING

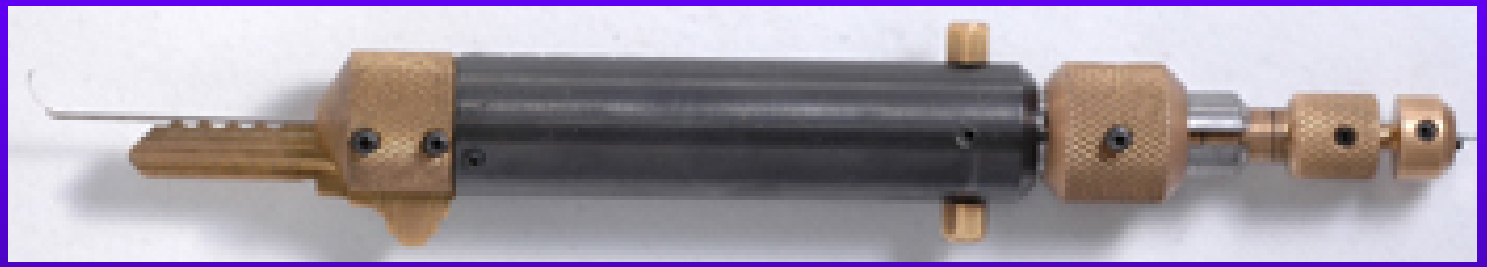


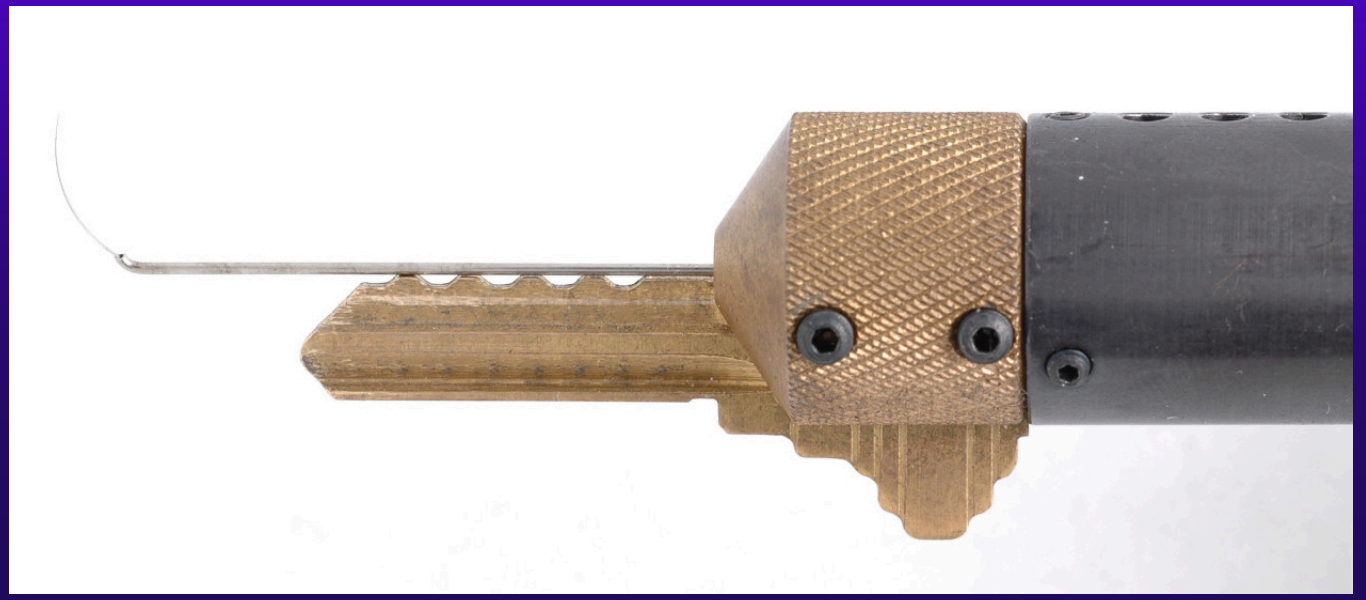
TOBIAS DECODER:
Medeco decoder: by “Crackpot!”



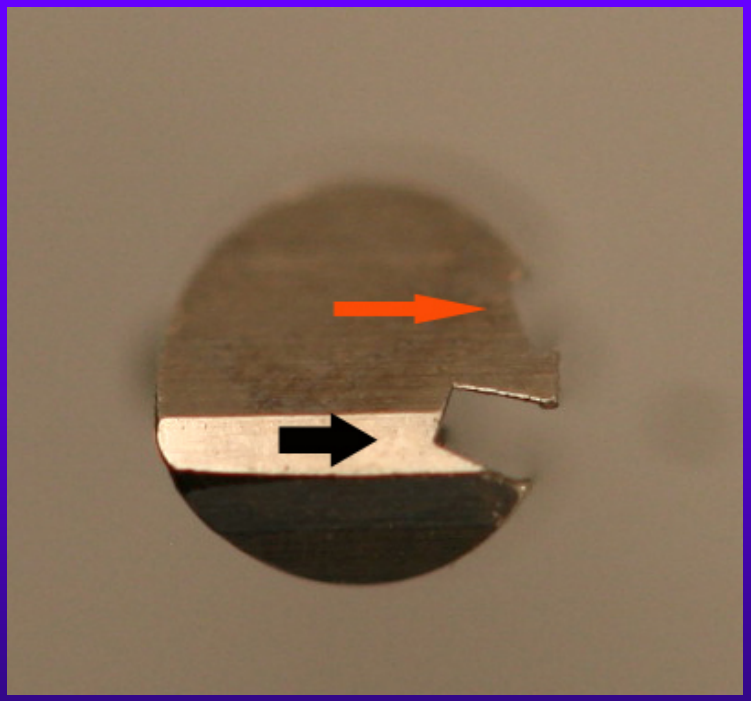
SOPHISTICATED DECODERS

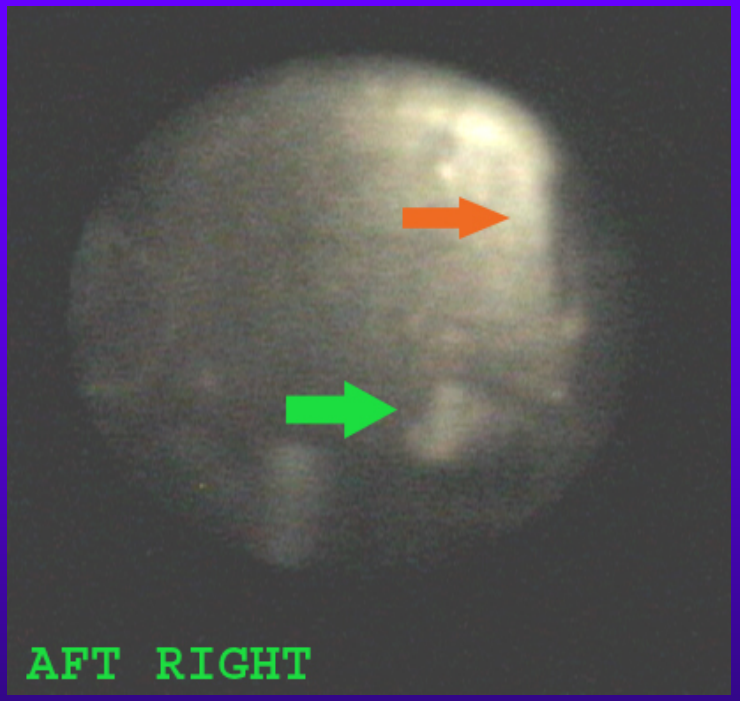
- John Falle: Wire Shim Decoder





DECODE PIN ANGLES





FORCED ENTRY RESISTANCE

High security requirement

FORCED ATTACK METHODS

- Original deadbolt design
- Interim deadbolt design
- Final deadbolt version
  - Reverse picking attack
- Mortise, Rim, and IC
  - Simulated key in plastic
  - Set shear line
  - Turn the plug

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

MEDECO CASE HISTORY

- Exploited vulnerabilities
- Reverse engineer sidebar codes
- Analyze what constitutes security
- Analyze critical tolerances
- Analyze key control issues
- Analyze design enhancements for new generations of locks: Biaxial and m3 and Bilevel

DESIGN = VULNERABILITIES

- Basic design: sidebar legs + gates
  - How they work: leg + gate interface
  - Tolerance of gates
- Biaxial code designation
- Biaxial pin design: aft position decoding
- M3 slider: geometry
- M3 keyway design
- Deadbolt design

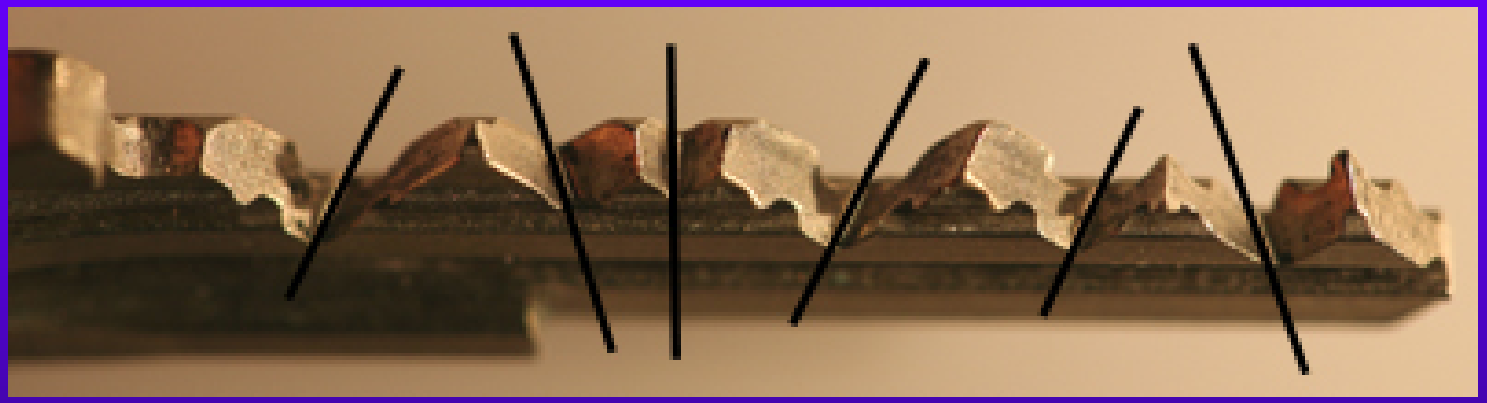
MEDECO DESIGN: Exploit design vulnerabilities

- EXPLOIT BEST DESIGN FEATURES
- Sidebar leg – true gate channel
- Code assignment: Biaxial 1985
- Gate – sidebar leg tolerance
- M3 design 2003
  - Widen keyway .007”
  - Slider geometry, .040” offset

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

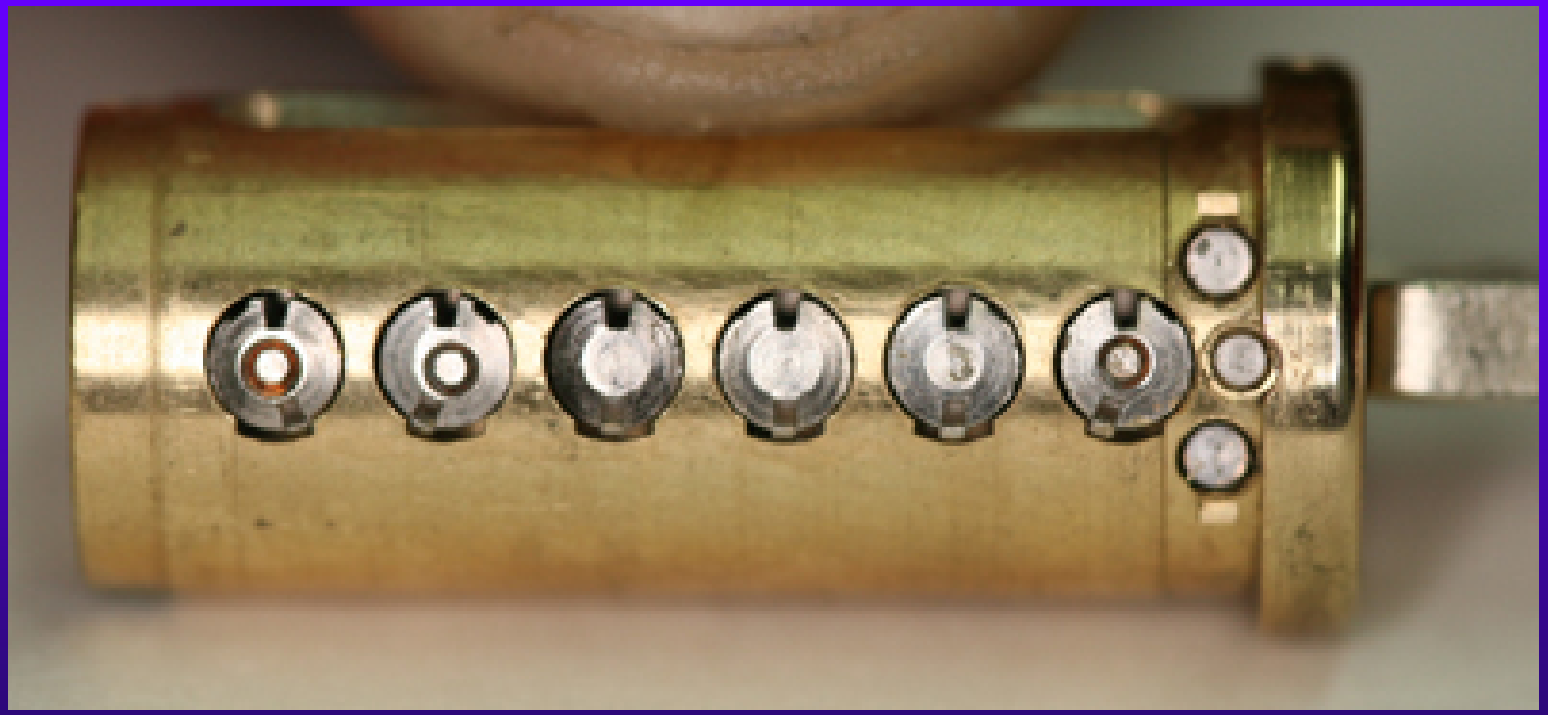


SECURITY CONCEPTS: Sidebar IS Medeco Security

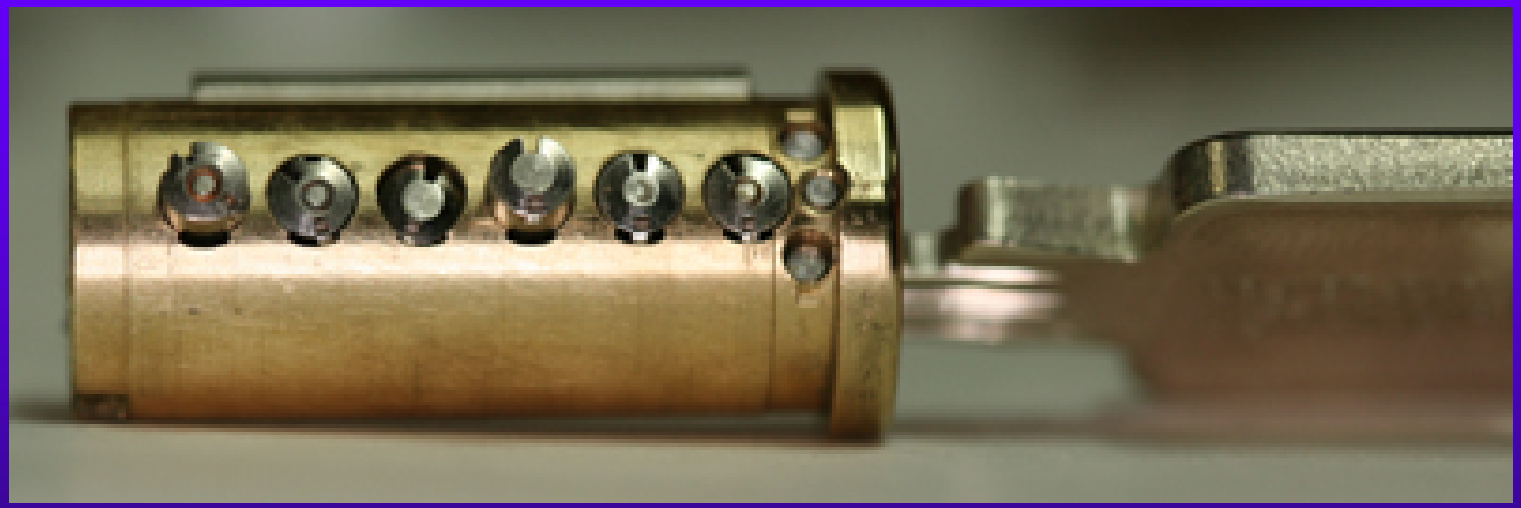
- GM locks, 1935, Medeco re-invented
- Heart of Medeco security and patents
- Independent and parallel security layer
- Integrated pin: lift and rotate to align
- Sidebar blocks plug rotation
- Pins block manipulation of pins for rotation to set angles

PLUG AND SIDEBAR: All pins aligned

SIDEBAR RETRACTED



PLUG AND SIDEBAR: Locked



MEDECO CODEBOOK: At the heart of security

- All locksmiths worldwide must use
- All non-master keyed systems
- New codes developed for Biaxial in 1983
- Chinese firewall: MK and Non-MK
- Codebook defines all sidebar codes

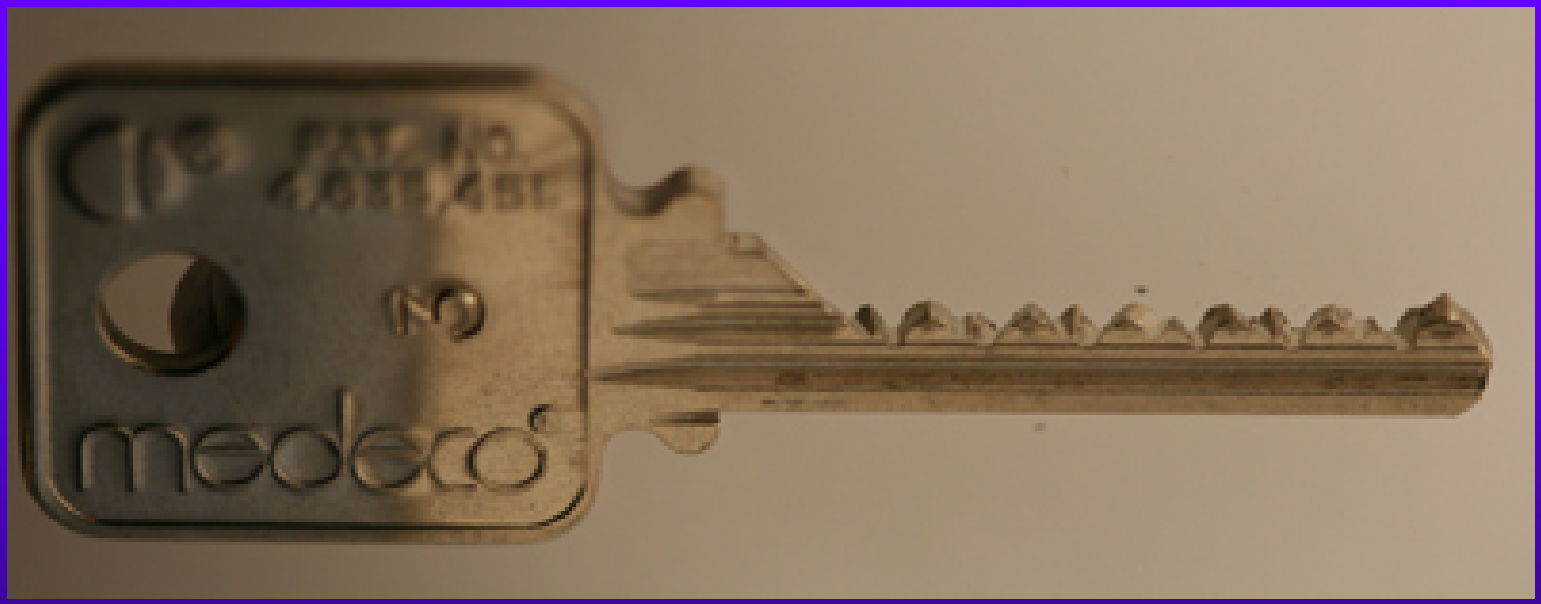
MEDECO RESEARCH: Results of Project

- Covert and surreptitious entry in as little as 30 seconds: standard requires 10-15 minutes
- Forced entry: four techniques, 30 seconds, affect millions of locks
- Complete compromise of key control
  - Duplication, replication, simulation of keys
  - Creation of bump keys and code setting keys
  - Creation of top level master keys

RESULTS OF PROJECT: Bumping

- Reliably bump open Biaxial and m3 locks
- Produce bump keys on Medeco blanks and simulated blanks
- Known sidebar code
- Unknown sidebar code

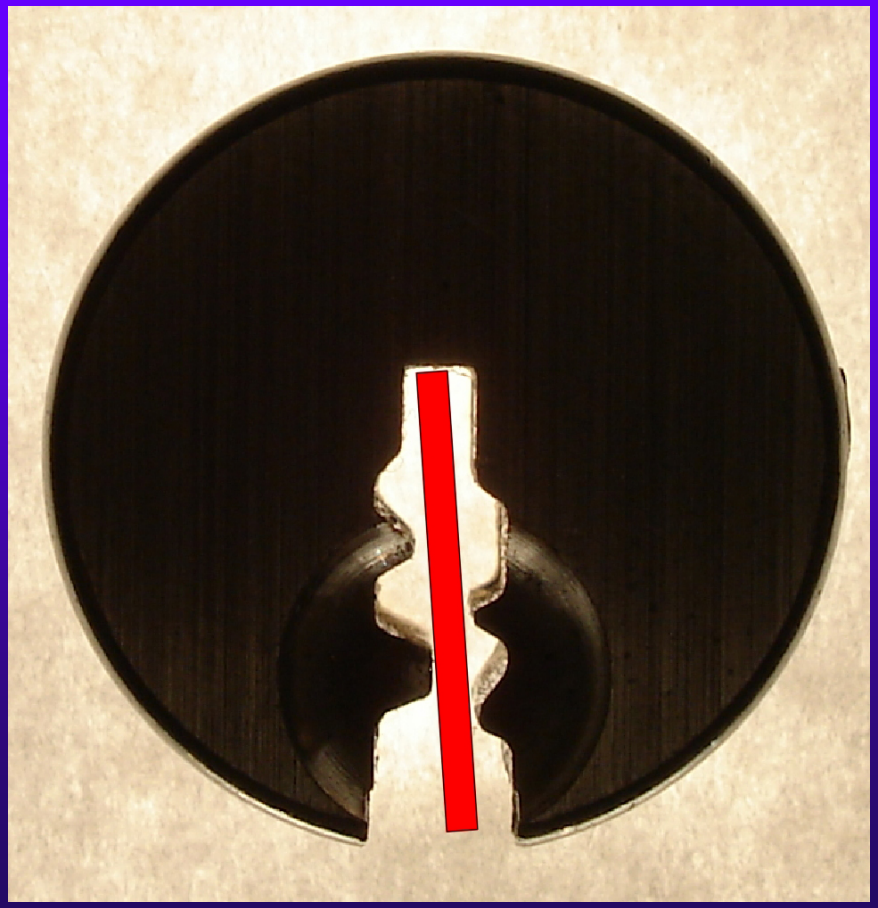
MEDECO BUMP KEY



RESULTS OF PROJECT: Key Control and Key Security

- Total compromise of key control and key security, vital to high security locks
  - Duplicate, replicate, simulate keys for all m3 and some Biaxial keyways
    - Restricted keyways, proprietary keyways
    - Government and large facilities affected
  - Attack master key systems
  - Produce bump keys
  - Produce code setting keys

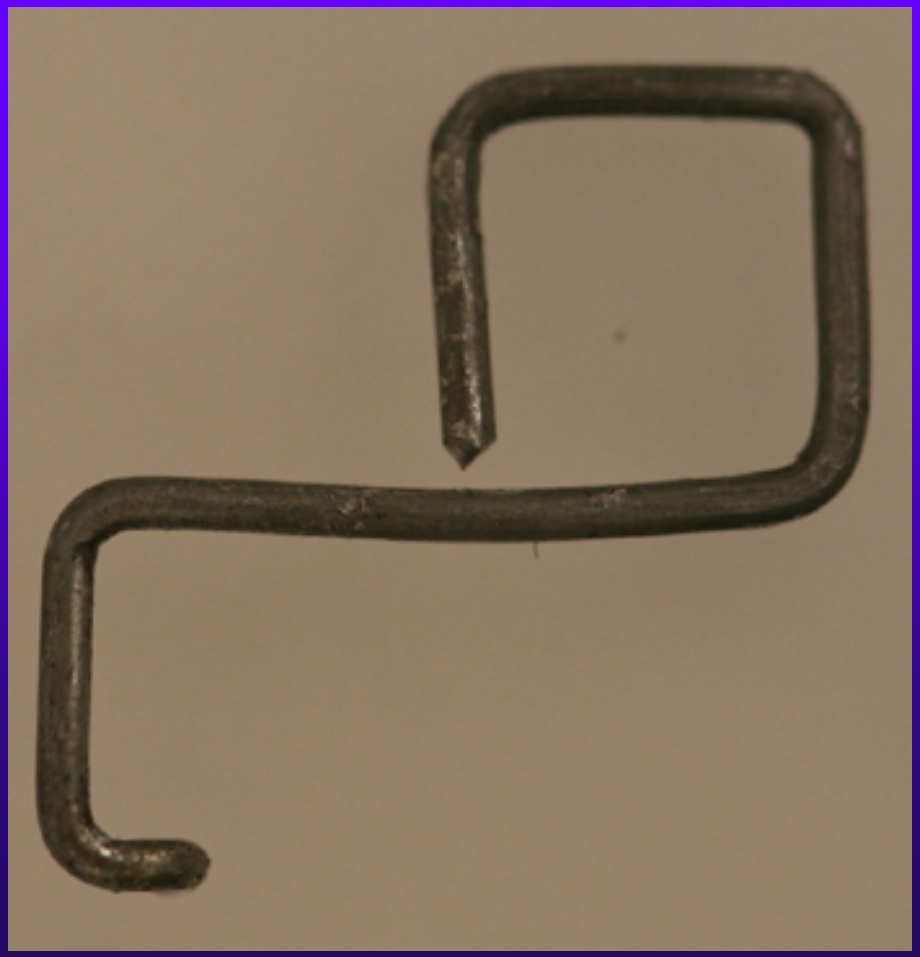
SIMULATED BLANKS: Any m3 and Many Biaxial Locks



SIMULATED BLANKS

M3 SLIDER:
Bypass with a Paper clip

SECURITY OF m3: High Tech Wire!



RESULTS OF PROJECT: Picking

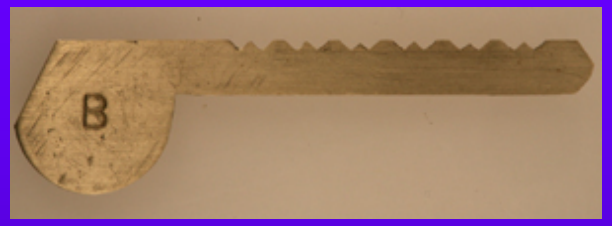
- Pick the locks in as little as 30 seconds
- Standard picks, not high tech tools
- Use of another key in the system to set the sidebar code
- Pick all pins or individual pins
- Neutralize the sidebar as security layer

CODE SETTING KEYS

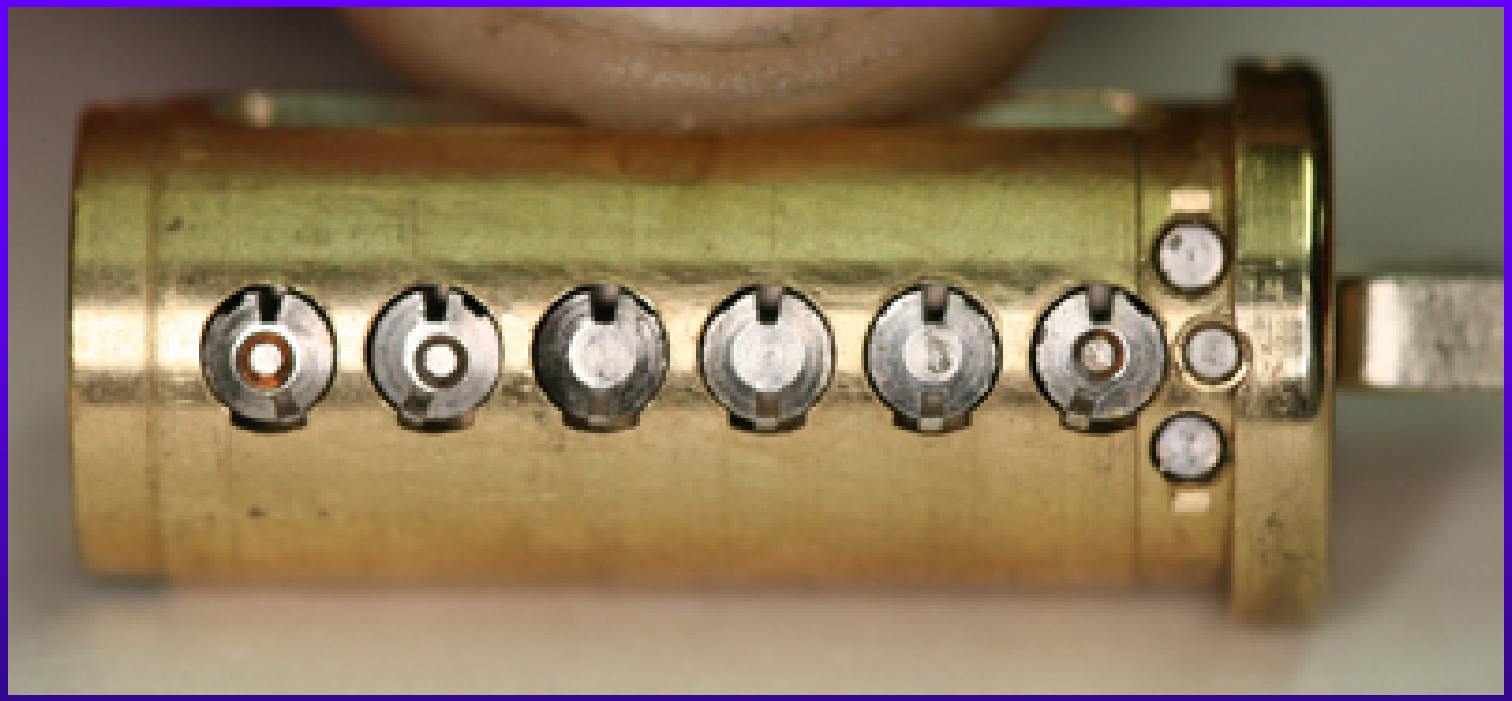
CODE SETTING KEYS

- FACTORY BLANKS
- SIMULATED BLANKS FOR ANY m3 and MANY BIAXIAL KEYWAYS
- USE A CHANGE KEY TO SET CODE

CODE SETTING KEYS: SIMULATED BLANKS



SET THE SIDEBAR CODE

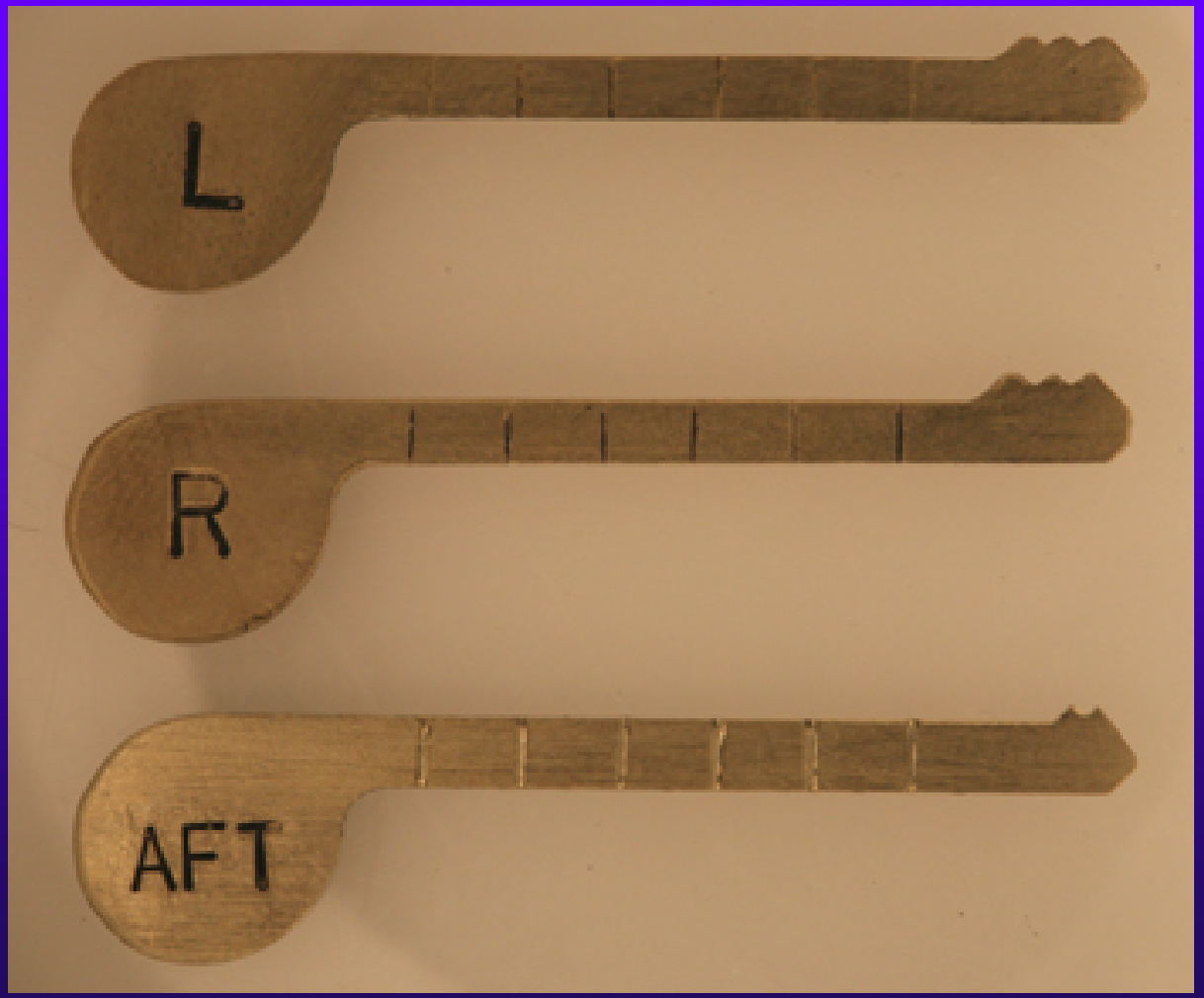


CONVENTIONAL PICKING

- Setting the Sidebar Code
- Conventional pick tools

PICKING A MEDECO LOCK

SET INDIVIDUAL ANGLES



RESULTS OF PROJECT: Decode Top Level Master Key

- Determine the sidebar code in special system where multiple sidebar codes are employed to protect one or more locks
- Decode the TMK
- OWN the system

RESULTS OF PROJECT: Forced Entry Techniques

- Deadbolt attacks on all three versions
  - Deadbolt 1 and 2: 30 seconds
  - Deadbolt 3: New hybrid technique of reverse picking
- Mortise and rim cylinders
  - Prior intelligence + simulated key
- Interchangeable core locks

DEADBOLT ATTACK

DEADBOLT BYPASS: 2$
Screwdriver + $.25 materials

MORTISE CYLINDER

MORTISE ATTACK

REAL WORLD ATTACK: Bumping a Medeco Lock

OPEN IN THIRTY SECONDS

- Setting the Sidebar Code
- Conventional pick tools

THE COMPROMISE OF MEDECO HIGH SECURITY LOCKS: New Techniques of Forced, Covert, and Surreptitious Entry

© 2008 Marc Weber Tobias and Tobias Bluzmanis

www.security.org

mwtobias@security.org