High Insecurity: Locks, Lies, and Liability

Marc Weber Tobias

Matt Fiddler

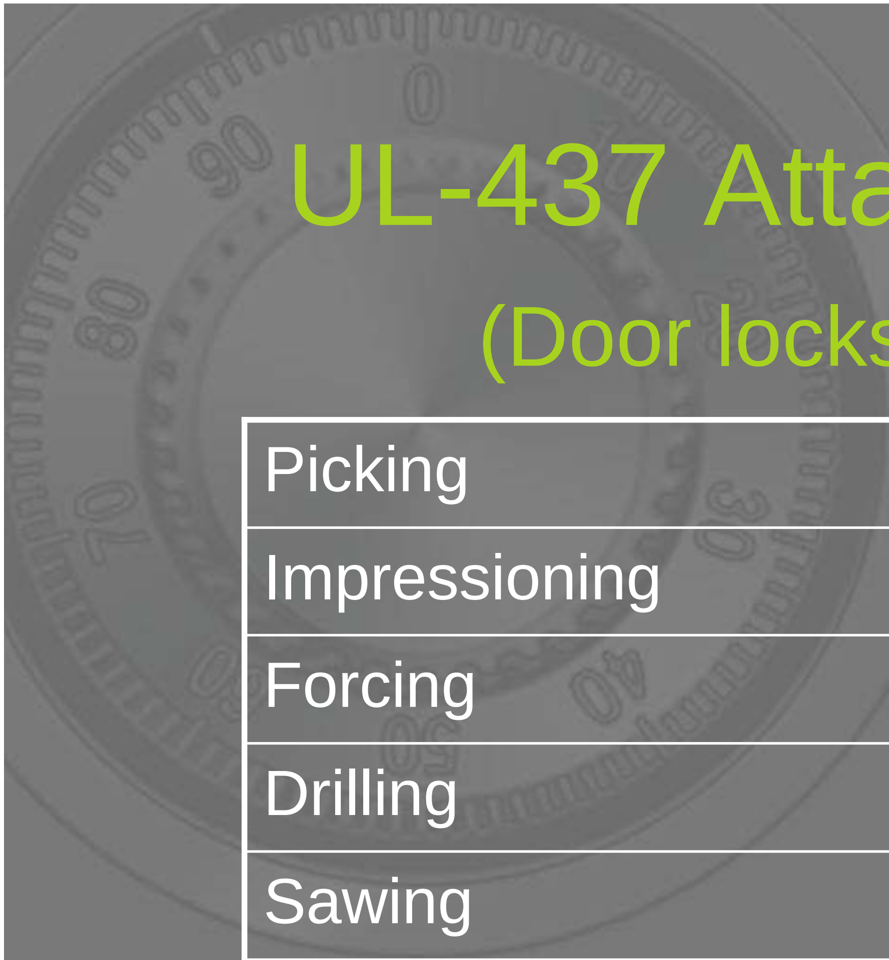
in.Security.Org

Agenda

- Security Standards
    - Conventional and High Security
    - UL-437
    - ANSI /BHMA (A156.5-2001)
    - ANSI (A156.30)
- LOCKS:
    - Bypass Methods
- LIES:
    - Representations
    - Design issues
- LIABILITY:
    - Legal issues

High Security Locks and Standards

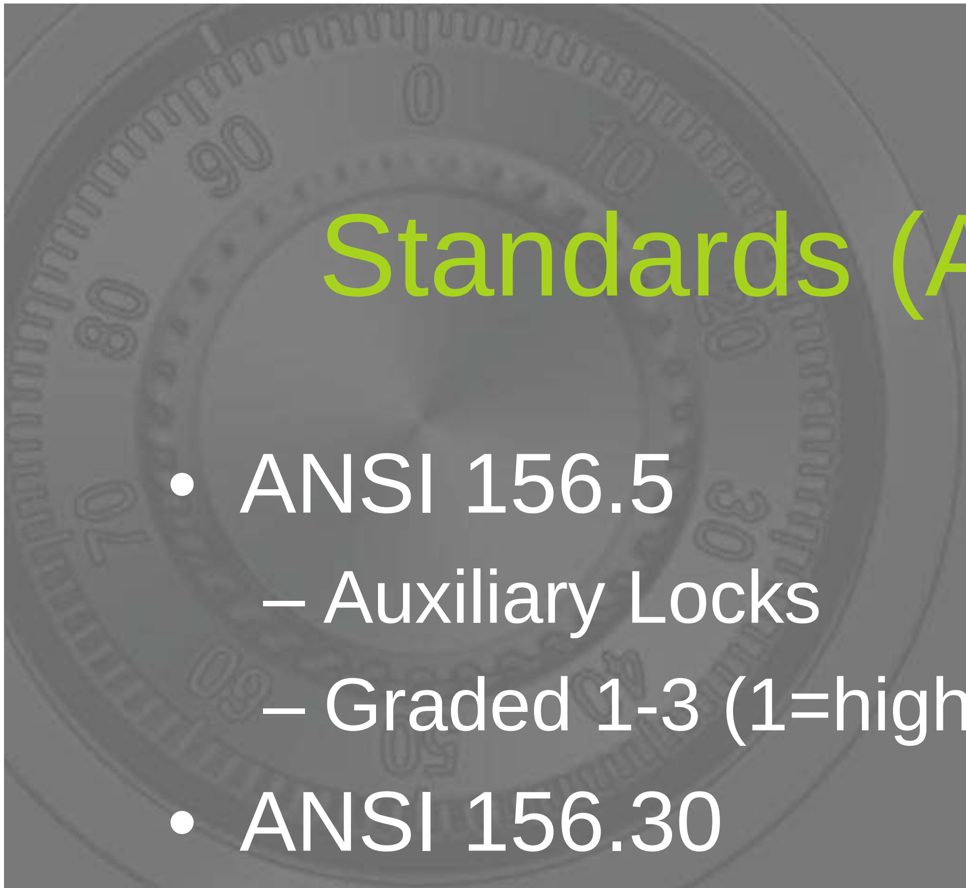
- Normal vs. High Security
- Facility specifications based on UL/ANSI
- Protection: Forced, Covert, Key control
- Protection of high value and critical targets



UL-437 Attack Resistance

(Door locks and Cylinders)

Picking	10 Minutes
Impressioning	10 Minutes
Forcing	5 Minutes
Drilling	5 Minutes
Sawing	5 Minutes
Prying	5 Minutes
Pulling	5 Minutes
Driving	5 Minutes



Standards (ANSI/BHMA)

- ANSI 156.5
  - Auxiliary Locks
  - Graded 1-3 (1=highest rating)
- ANSI 156.30
  - High Security Cylinders
  - Graded A-C (A=highest rating)

Standards (ANSI A156.5) Security Tests

- Impact
- Tension
- Torque
- Impact
- Sawing
- Pressure
- Tensile

In addition to the above requirements all cylinders must meet all DRILLING(5min) and PICKING(10min) requirements of UL-437

Standards (ANSI A156.30) High Security Cylinders

- Key Control (ratings are cumulative)
  - C - Manufacturer restricted blanks
  - B - Blanks protected by law
  - A - Authorization required
- Forced Entry Extensions (Above A156.5)

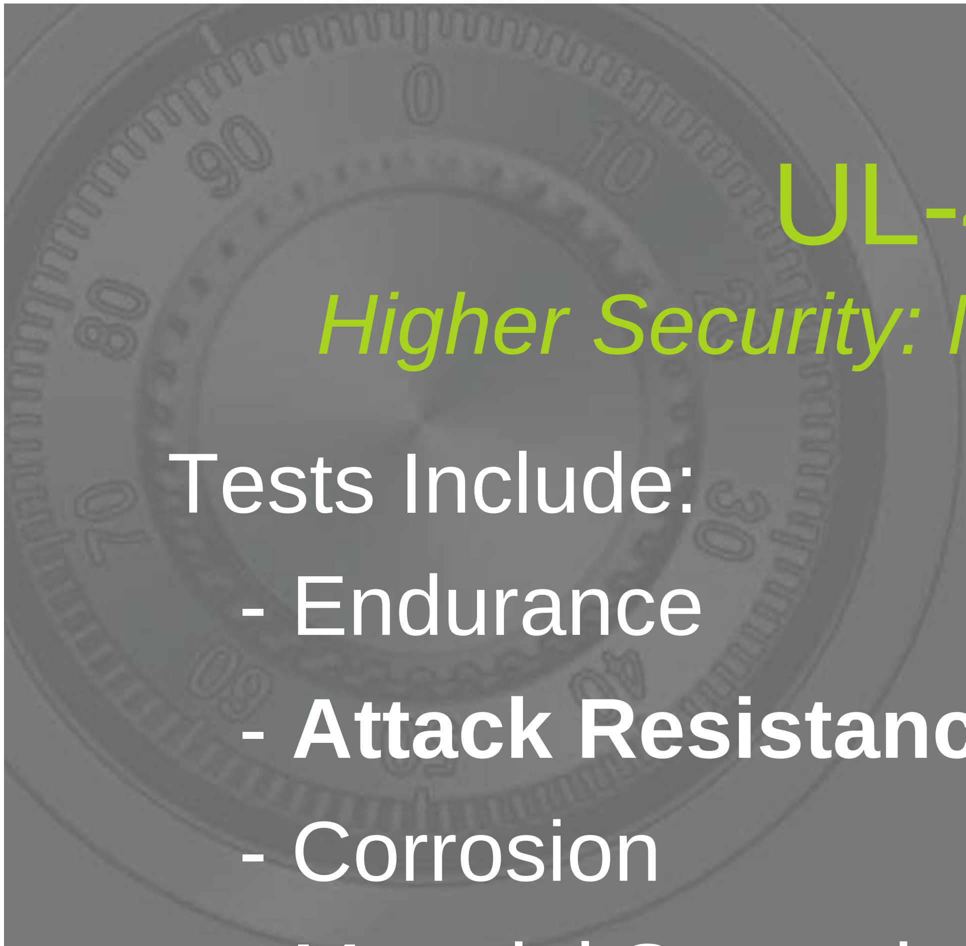
Standards (ANSI A156.30)

- Pick Resistance (Cumulative)
  - C: Minimum of 2 Security Pins
    - Paracentric Keyway
    - Minimum of one bore depth designed to prevent overlifting
  - B: Meets all levels of C plus UL-437 for pick resistance (10 min)
  - A: Resist picking for 15 min as tested by 5 “ALOA Certified” Locksmiths with “commercially” available tools

What is “High Security”?

Standards (UL-437)

- Cabinet Locks
- Door Locks
- Locking Cylinder
- Security Containers
- Two-Key Locks



UL-437

Higher Security: Not High Security

Tests Include:

- Endurance
- **Attack Resistance**
- Corrosion
- Material Strength

UL-437 Attack Resistance

- “A product shall not open or be compromised as a result of application of the tools and methods described…”
  - Common hand tools
  - Hand or portable electronic tools
  - Saw blades
  - Puller mechanisms
  - Picking tools

UL-437 Tools (Hand or Electric)

Forced Entry

- Pry bars(up to 3ft)
- Chisels
- Screwdrivers (max 15in)
- Hammers (max 3lbs)
- Wrenches
- Pliers
- Drills
- Saw blades
- Pulling tools

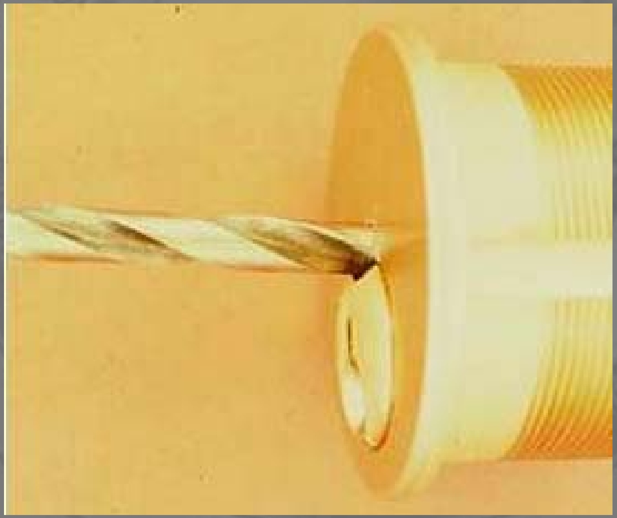
Covert Entry

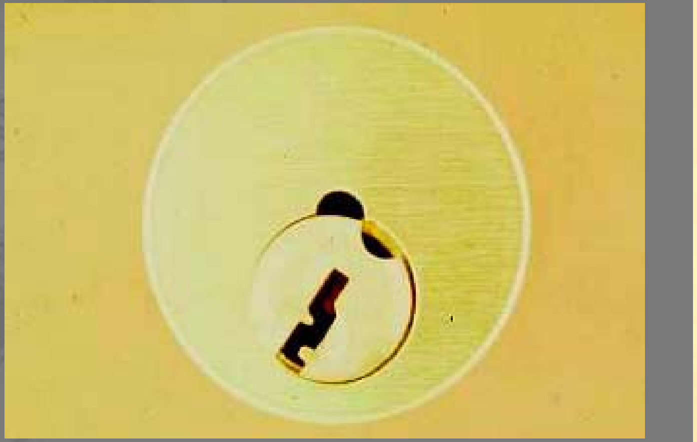
- Picking
- Impressioning

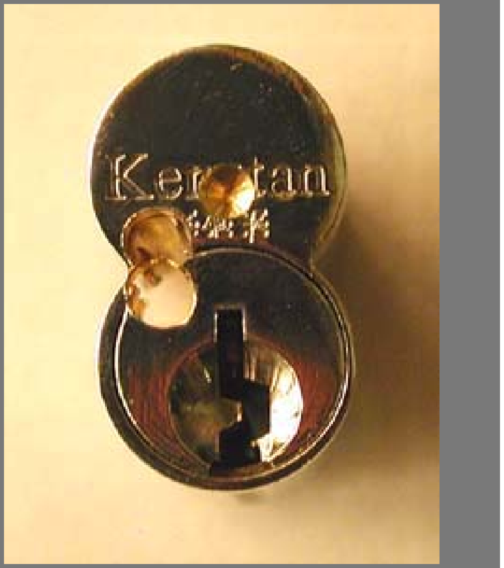
LOCKS

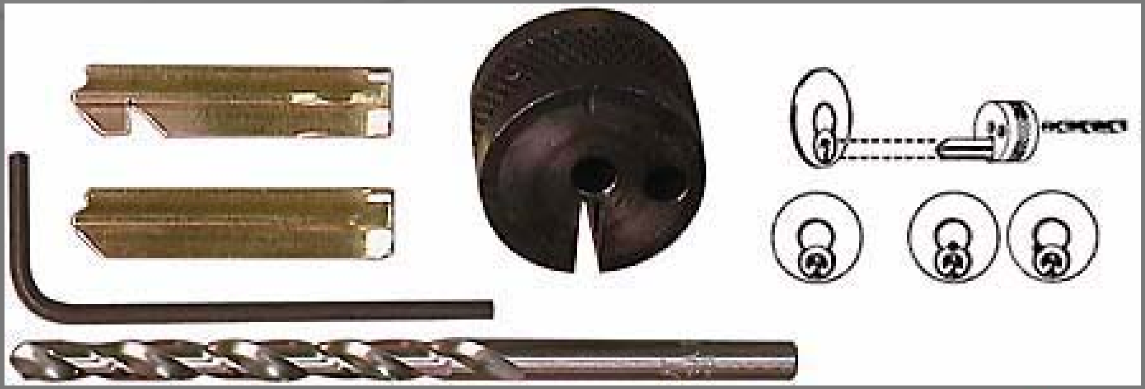
- Drilling
- Pulling
- Prying
- Sawing
- Picking
- Impressioning

Forced Entry - Drilling

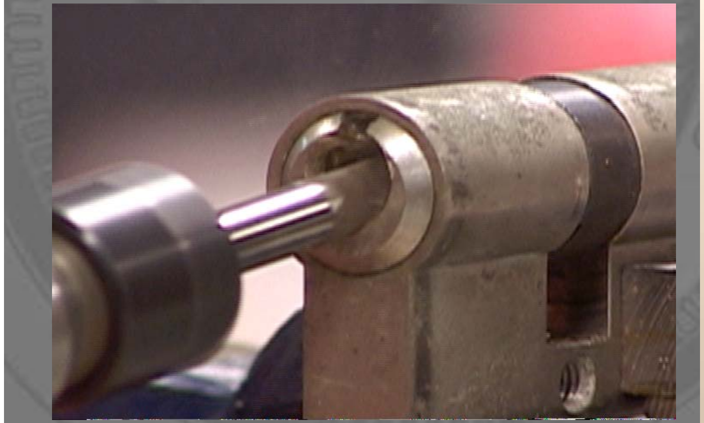


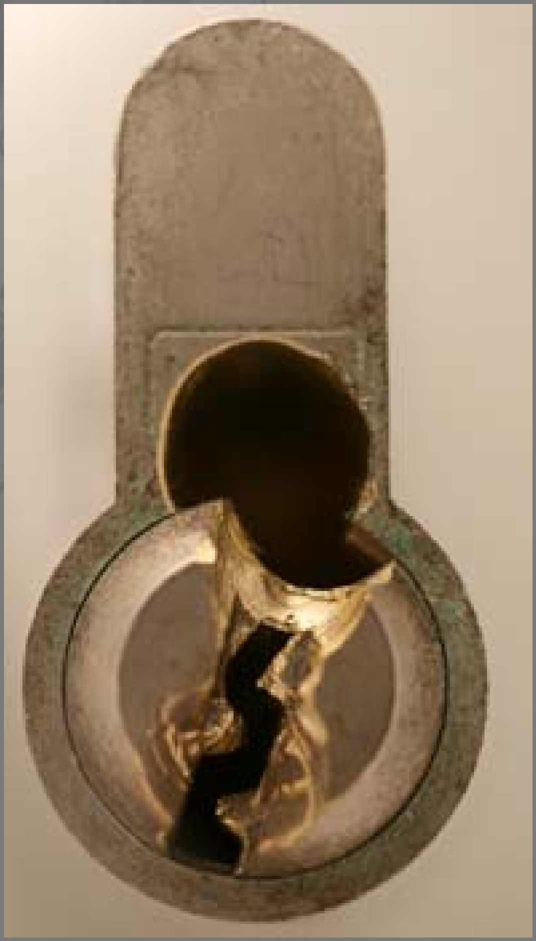


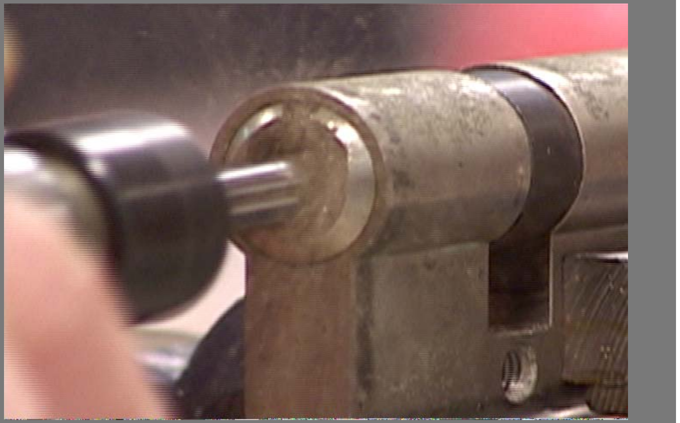


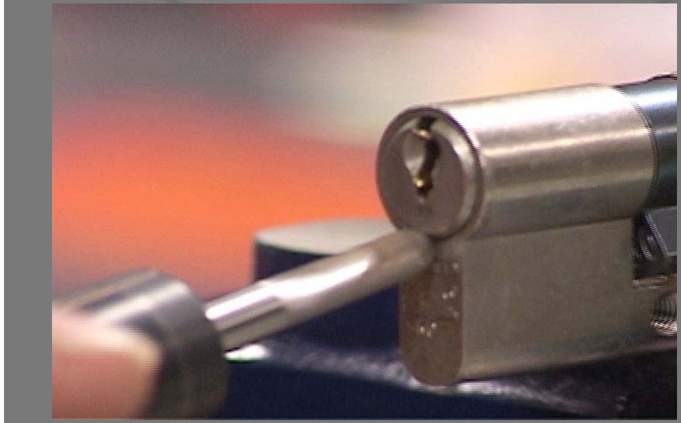


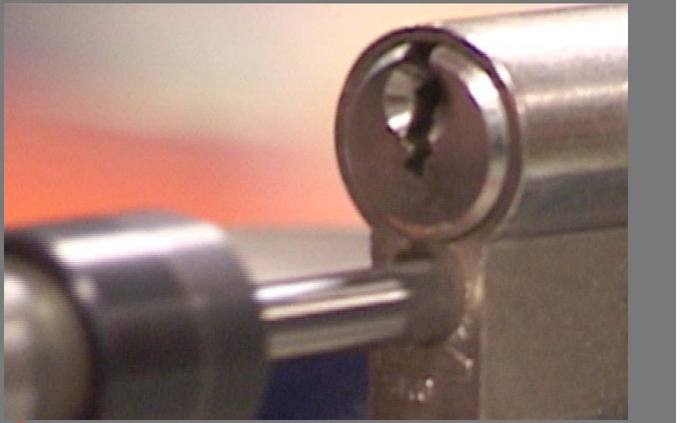
Drilling a standard cylinder and high security cylinder



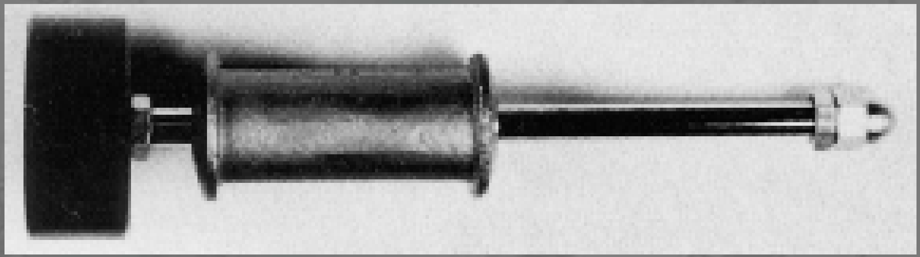


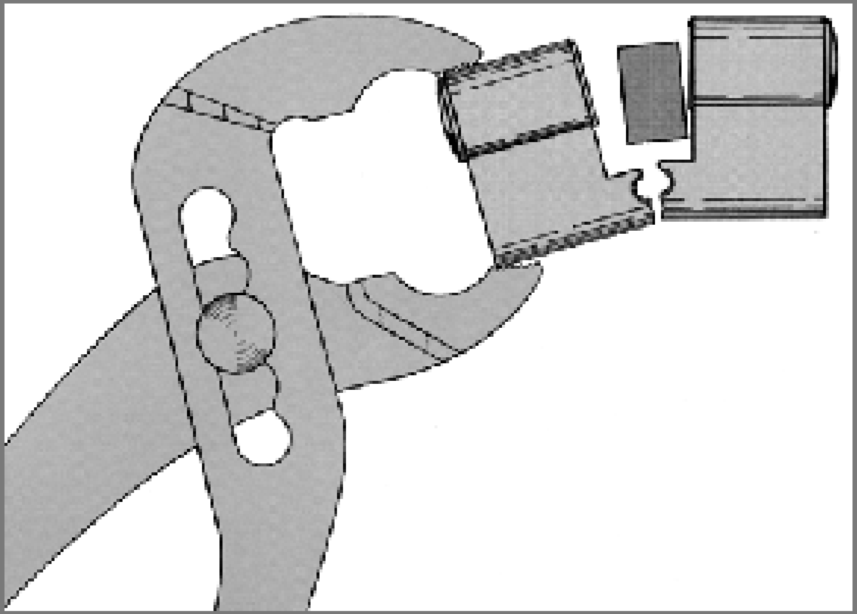






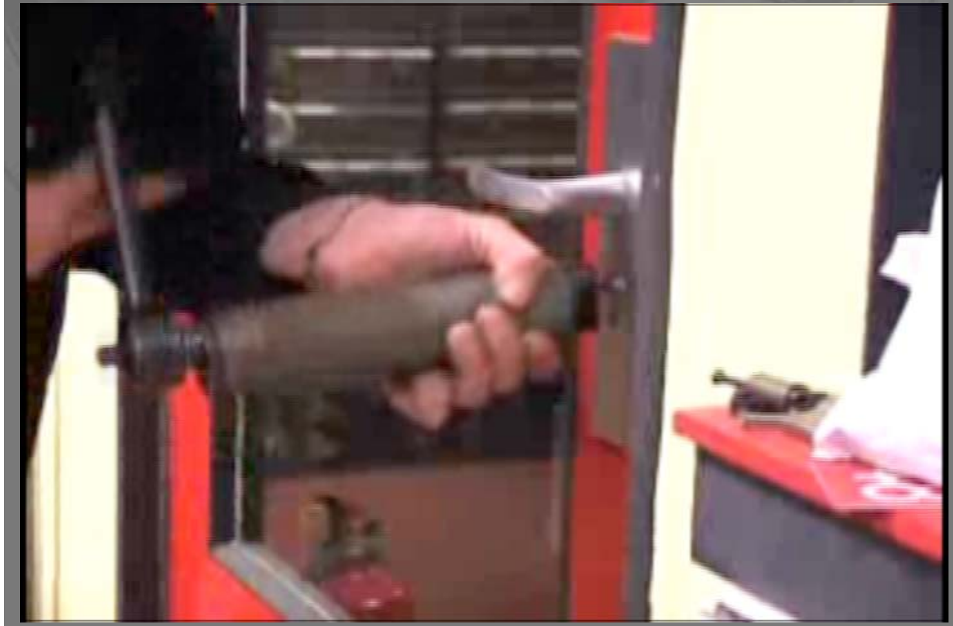
Forced Entry - Pulling



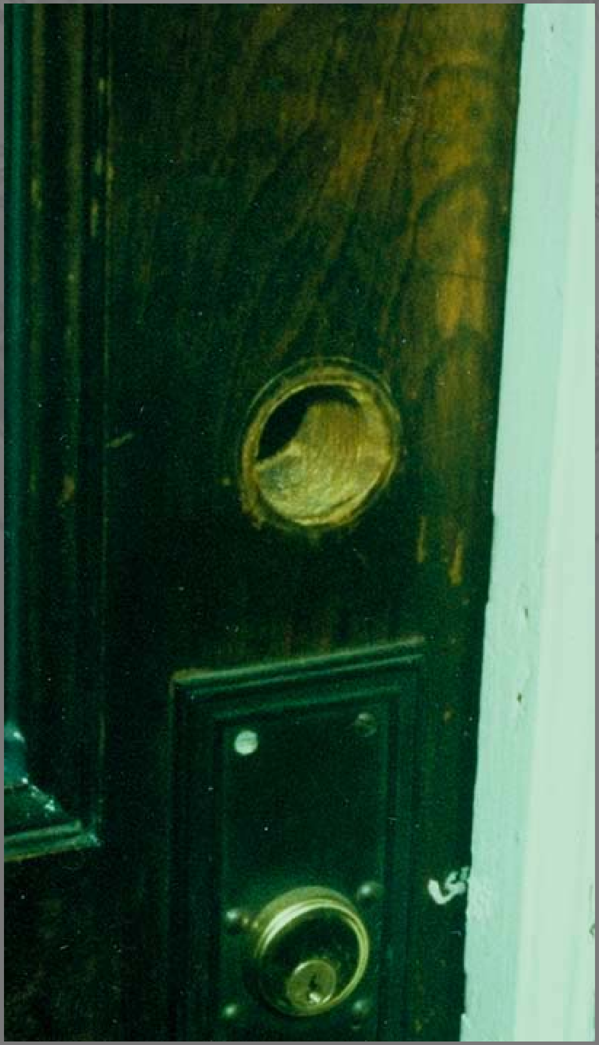


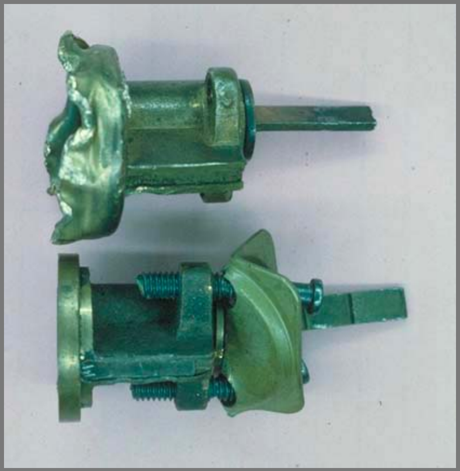
PULLING A MUL-T-LOCK

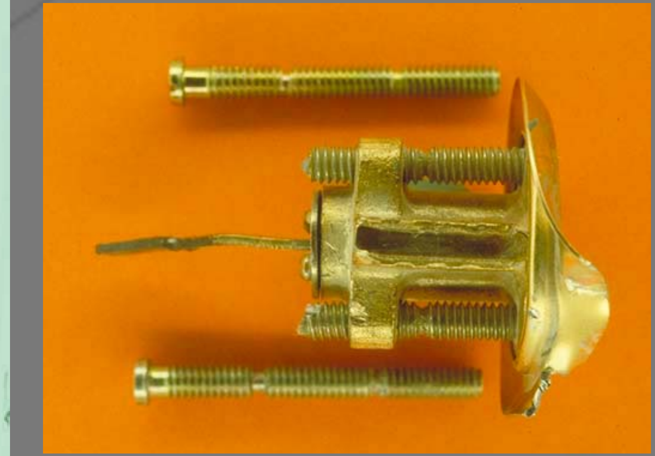
- Use of a puller on the plug



Forced Entry - Prying

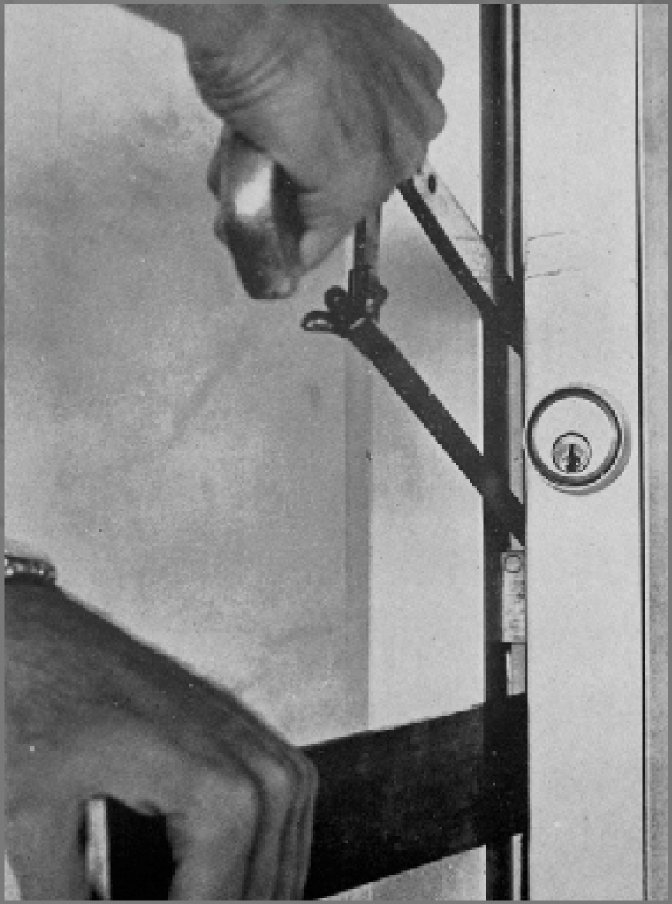


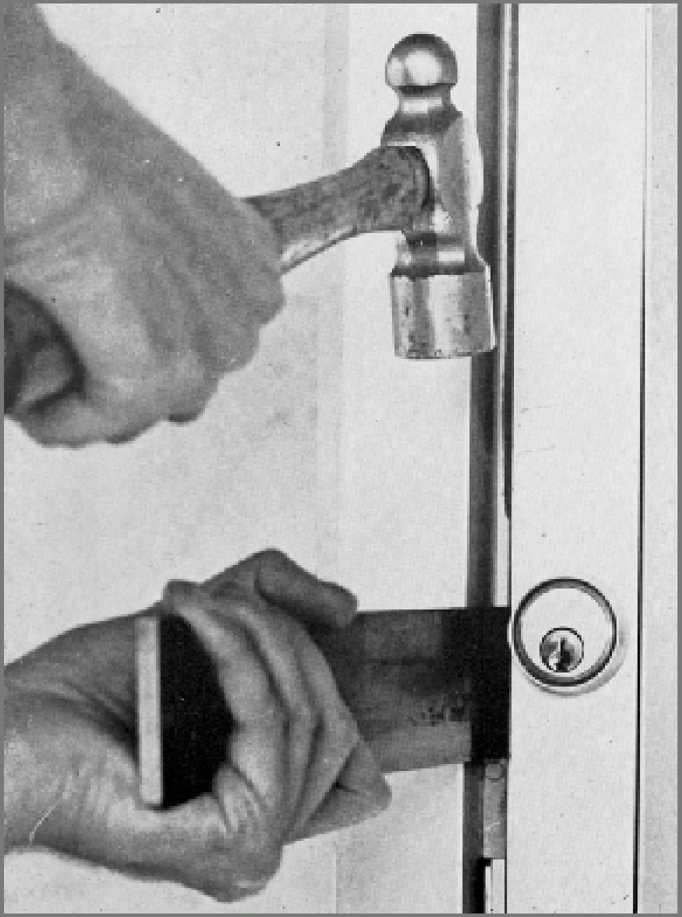




in.Security.Org

Forced Entry - Sawing



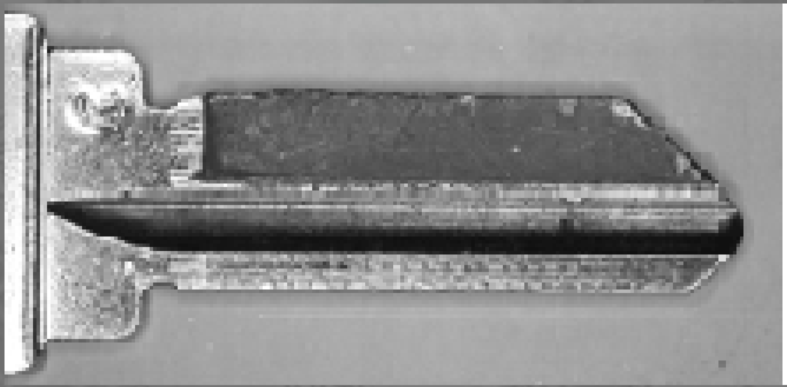


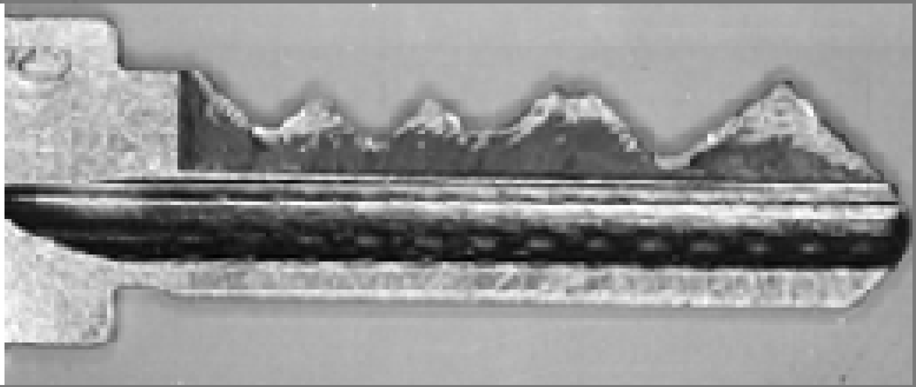
in.Security.Org

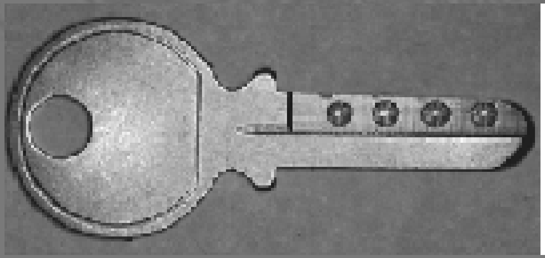
Covert Entry - Picking

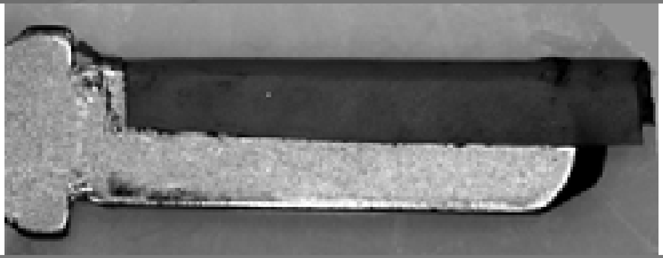
in.Security.Org

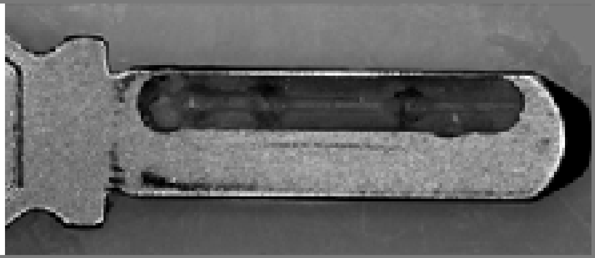
Covert Entry - Impressioning



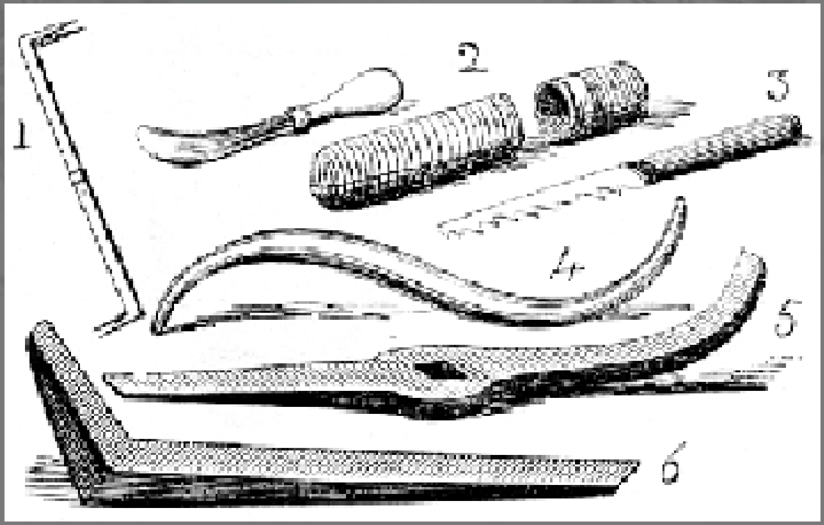


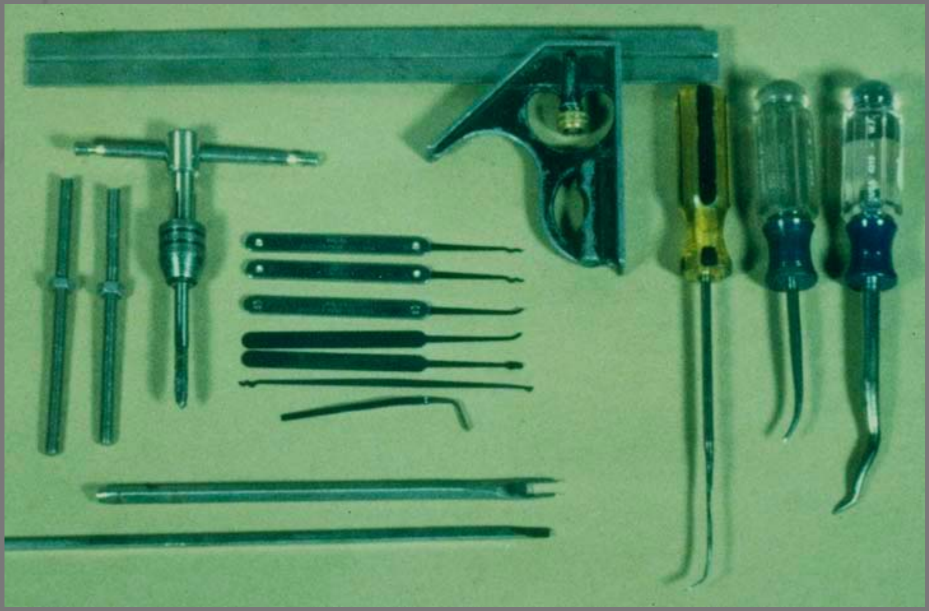




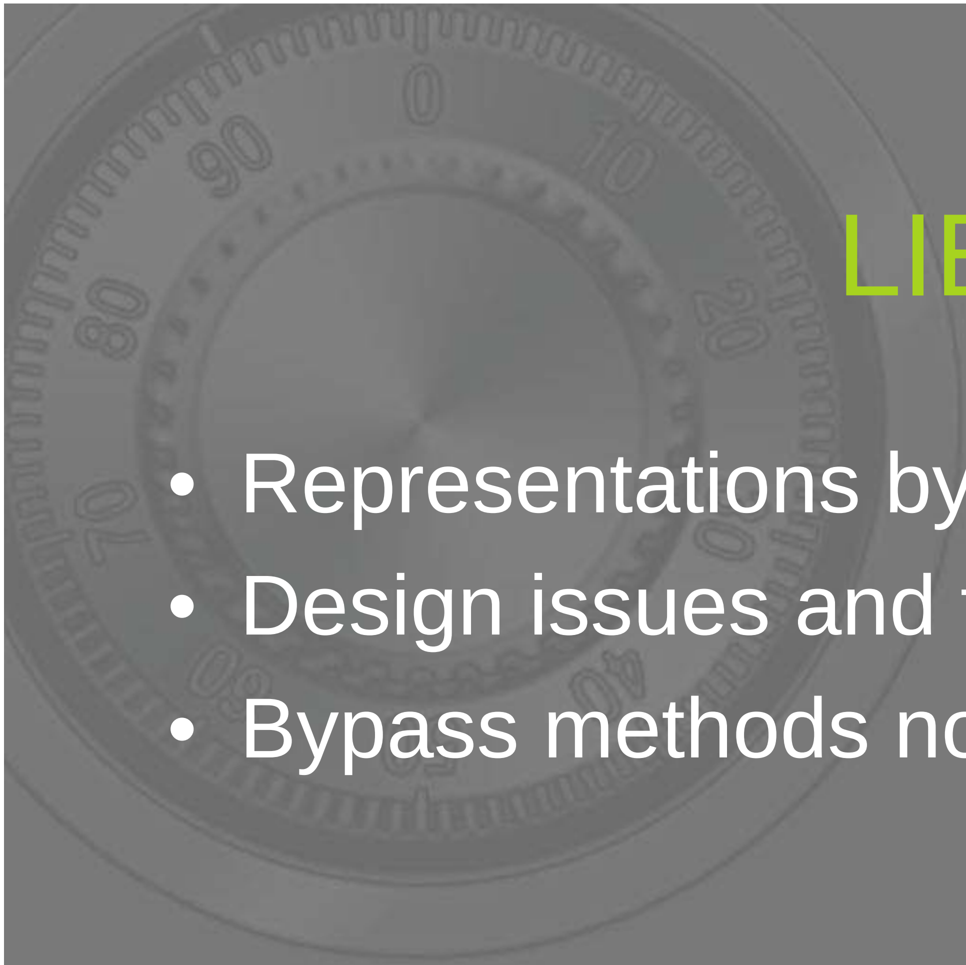


Common Hand Tools





LIES



- Representations by lock manufacturers
- Design issues and failures
- Bypass methods not contemplated

Representations by Manufacturers

- Locks are secure
- High security v. standard locks
- Implied representations
- Know or should have known of problems
- Meet specifications?
- Need truth in packaging and advertising

Design Issues

- Failure of imagination
- Design engineer problem
- Key never unlocks the lock
- Moshe Dyan problem

Mechanical Bypass

- Defeating locks in less than a minute
- Not included in standards
  - Not forced or covert entry
- Many certified locks can be compromised
- Public is misled

Mechanical Bypass: Another Method of Entry

- Wires and shims
- Vibration, shock, bumping
- Air pressure
- Magnetics
- Breaking of internal components
- Radio Frequency energy
- Temperature

Failure of Imagination

- Mechanical bypass
- Forced entry techniques
- Covert entry techniques
- Key control compromise
  - – Manufacturers cannot find the vulnerabilities

in.Security.Org

Design Defects

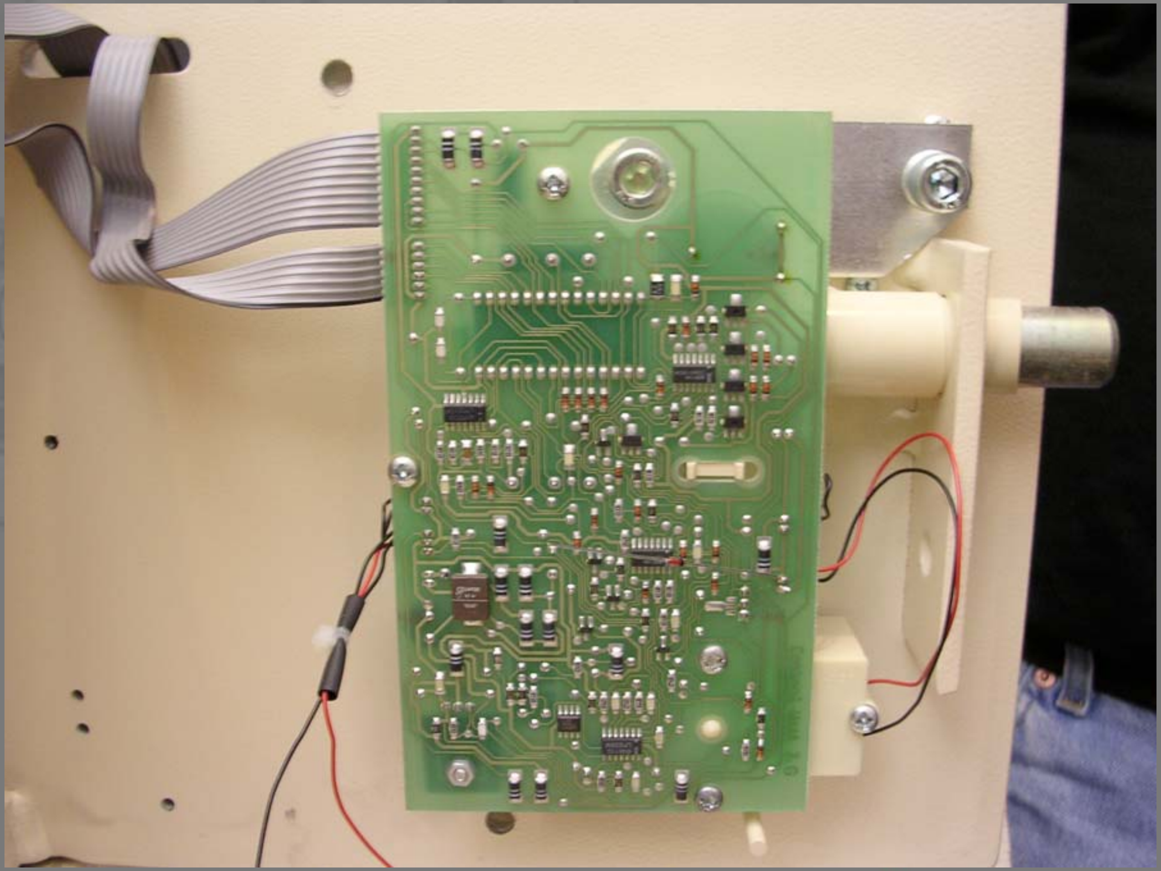
- Failure to understand laws of physics
- Failure to understand methods of entry
- Failure to imagine
  - Generally simple design failures
  - Directly affect the security of the lock
  - Affect any security ratings
  - Mislead the consumer

Case Examples

- El Safe (UnSafe) hotel safe
- File cabinet locks
- Targus Defcon CL
- Padlocks: Master and Corbin Sesamee
- Codelock electronic lock
- Kwikset
- Medeco

El Safe in room hotel safe

- Security = gear drive in back of door

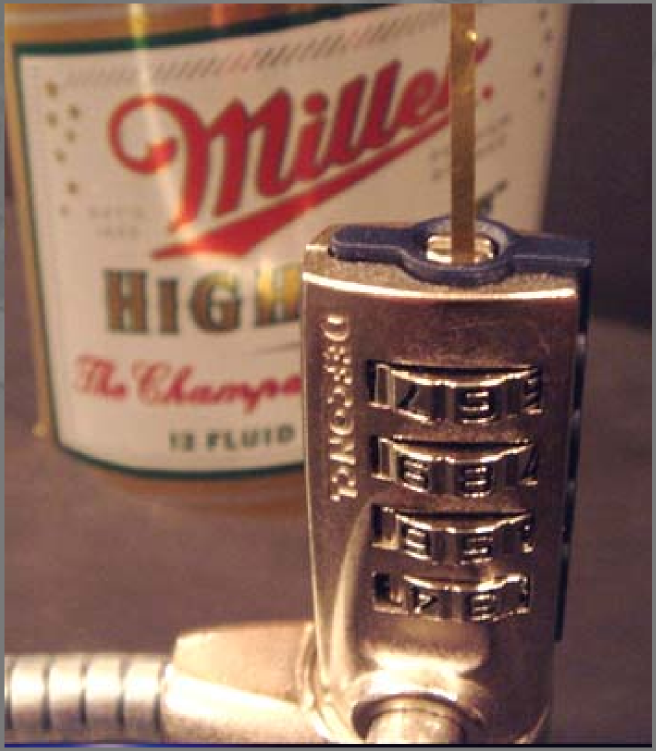


File Cabinet Locks

- Security = spring loaded locking dog

Targus Defcon CL

- Piece of plastic to decode gate position



Padlocks

- Master combination
- Corbin Sesamee

Codelocks CL1000

- Security = spring loaded blocking tab

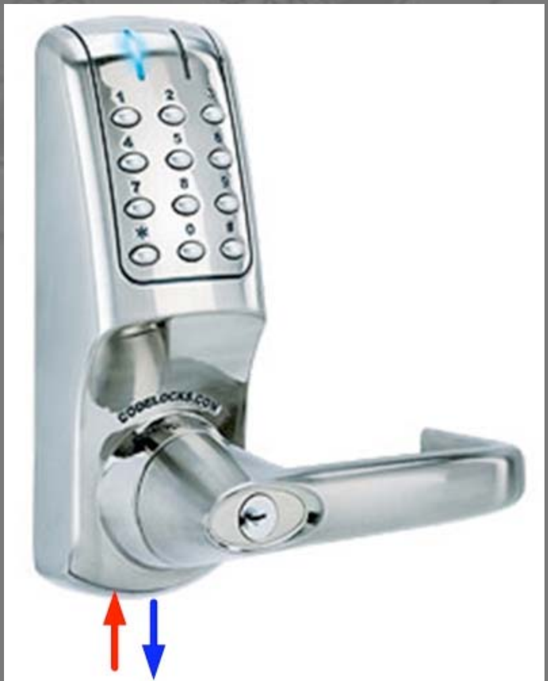
in.Security.Org

Codelocks 5000

Moshe Dyan Problem

“The road from Damascus to Tel Aviv also runs from Tel Aviv to Damascus”

- Drain hole out: wire in



Kwikset Maximum Security

- Defective design
- No real security
- Open in under 30 seconds
- No apparent evidence of entry

in.Security.Org

Kwikset Ultra Max

- No real security
- Defective design

in.Security.Org

Common Myths

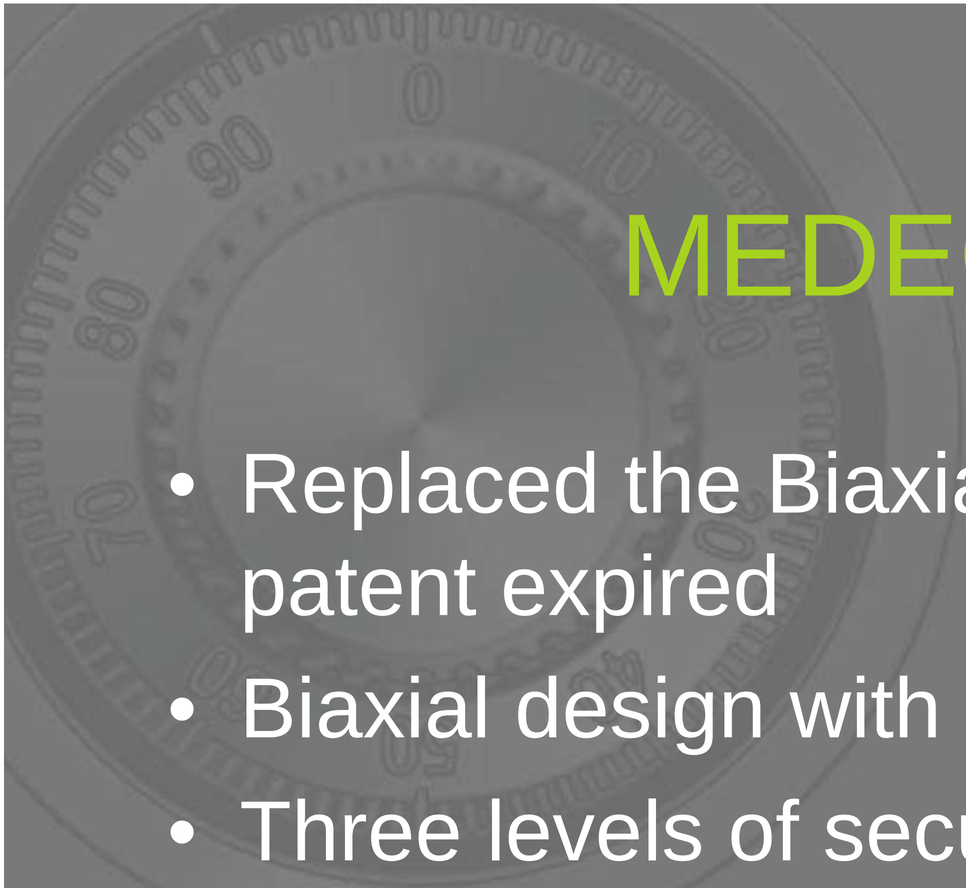
- Key Control
- Bumping
- Picking
- Mechanical Bypass

MEDECO:
The High Security Cylinder

- Protects high value and critical targets
- For 35 years: THE lock to attack
- UL437 and ANSI 156.30 rated
- Advertising Statements: Consider in context
  - “bump proof”
  - Highly pick resistant
  - Key control
  - Secure

MEDECO “CAVEATS”

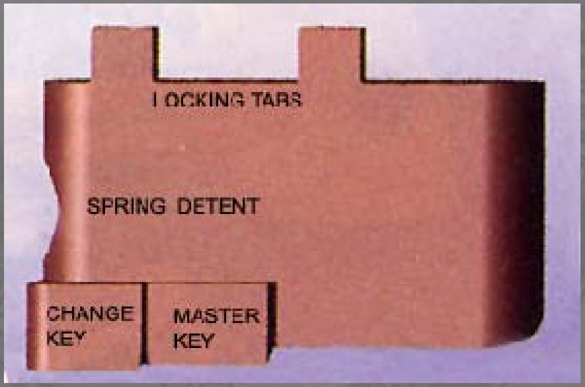
- High quality locks and hardware
- Secure for most locations and uses
- May be vulnerable for high value targets
- User needs to assess security
- Security depends upon many factors
  - Location and value of target
  - Expected sophistication of attack
  - Master key or non-master key system

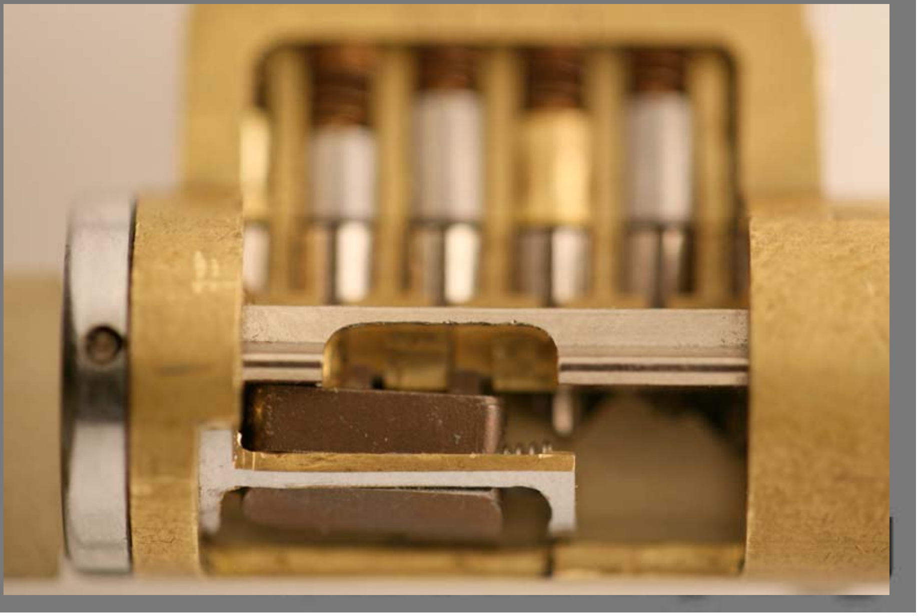


MEDECO m^3

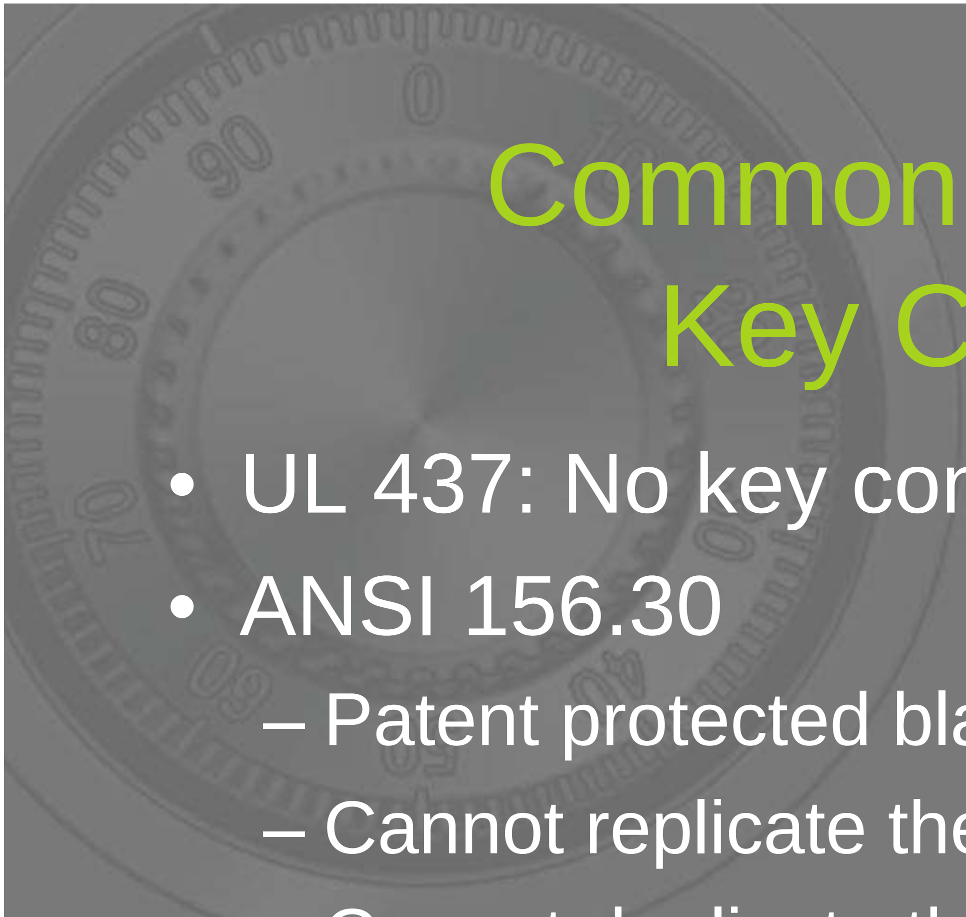
- Replaced the Biaxial in 2005 when patent expired
- Biaxial design with slider
- Three levels of security:
  - Pin tumblers elevated to shear line
  - Pin tumblers rotated to correct angles
  - Slider moved to correct position

Medeco m^3 Design





Common Myth #1: Key Control



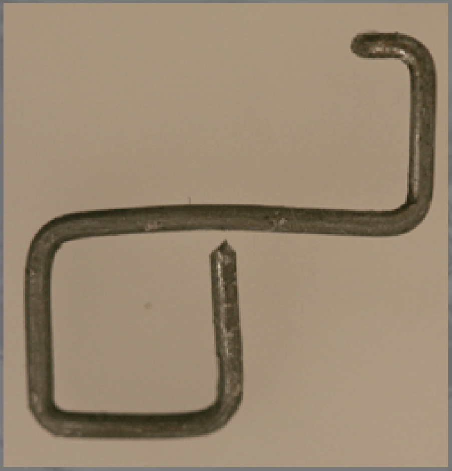
- UL 437: No key control criteria
- ANSI 156.30
  - – Patent protected blanks
  - – Cannot replicate the blanks
  - – Cannot duplicate the keys
  - – Factory control of keys produced by code

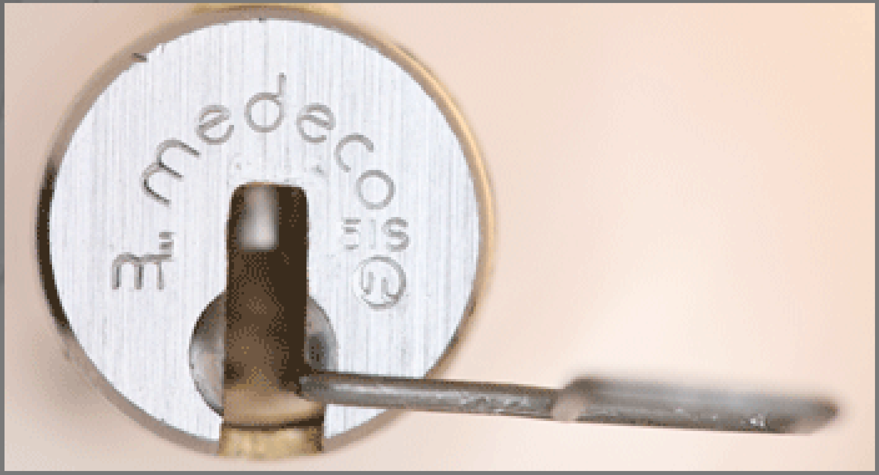
Medeco Key Control

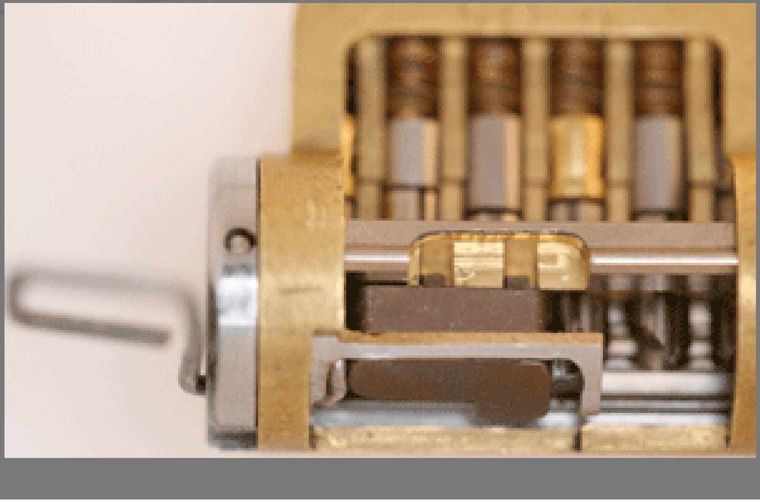
- Biaxial patent expired in 2005
- Replaced with m^3
- m^3 is protected but can be simulated
- Restricted keyways can be bypassed
- Security feature of m^3 can be bypassed which does not infringe on patent

Medeco m^3 Meets the Paper Clip

“Michaud M3 Degrade Attack”







in.Security.Org

Common Myth #2: Bumping

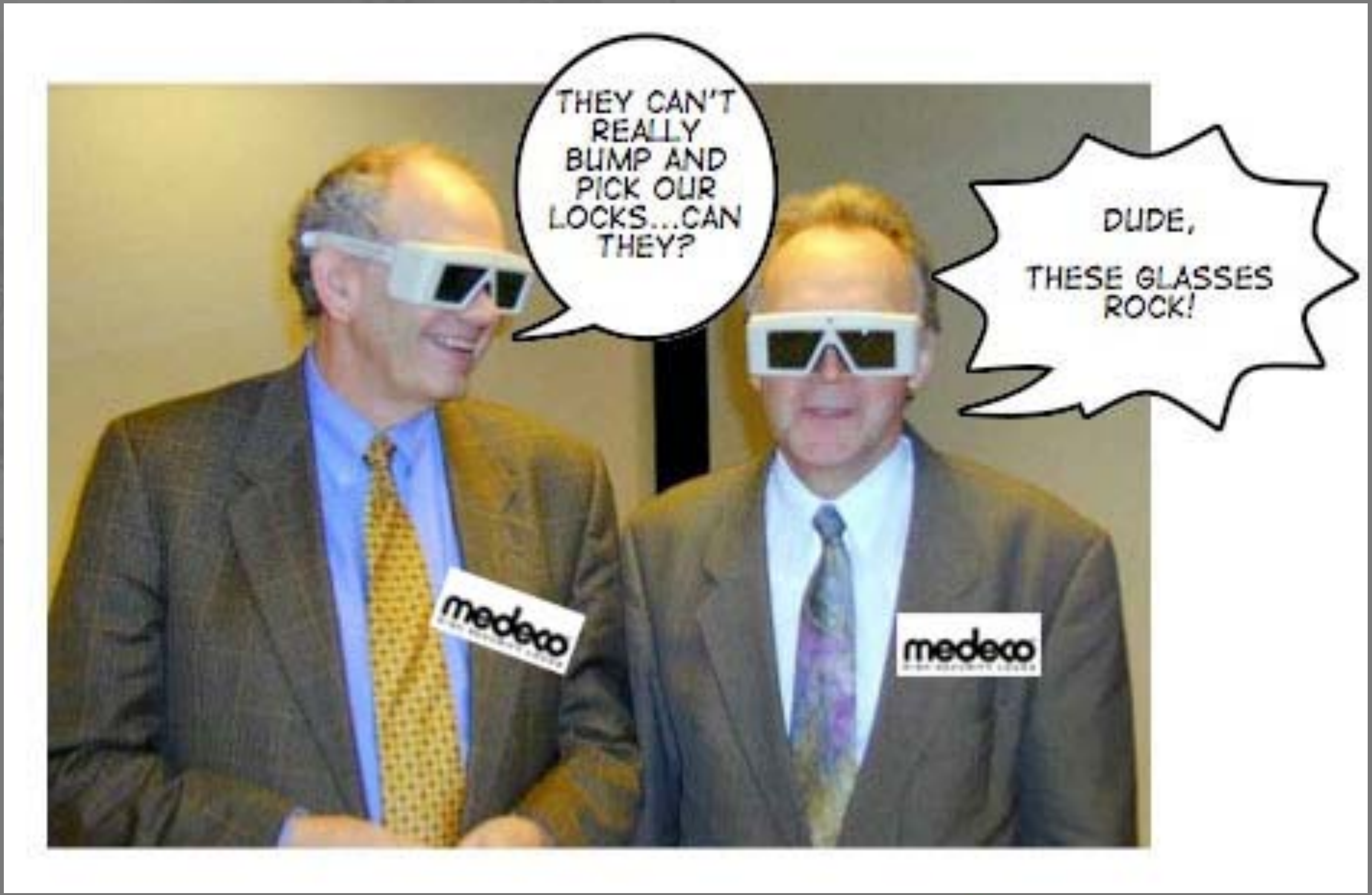
- Some High security locks can be bumped open
  - Locks can be bumped: Not all but many
  - Depends on many factors
  - Sidebar codes must be known or simulated
  - Patent filing for technique to bump

Medeco Not Bump-proof

- Medeco:
  - – “Our locks are bump proof!”
  - – “Our locks are virtually bump proof!”

Virtually bump proof = virtual reality

Virtual Reality


THEY CAN'T REALLY BUMP AND PICK OUR LOCKS...CAN THEY?
DUDE, THESE GLASSES ROCK!
medeco
medeco

Common Myth #3: Picking

- Special pick and decoder tools developed
- Medeco locks can be extremely difficult to pick because of pin rotation
- A target for 35 years
- Attempts largely unsuccessful
- Caveats

Picking Medeco Locks

- Medeco locks can be picked with conventional tools with a special technique in patent filing
- High percentage of these locks can be picked

Common Myth #4: Hardware Bypass

- Kwikset UltraMax and others
- Medeco hardware security: Is it really secure?
- Example: Deadbolts - A failure of imagination
- The entire security is based upon two small components

“The key never unlocks the lock!”

Medeco Security: Two Screws Loose!

Medeco Security: Two Screws Loose!

- Medeco Deadbolt Lock
  - – Security is based upon two tiny screws
  - – Can be compromised in under 30 seconds
  - – Will not meet high security standards
    - UL and ANSI does not address this issue
    - Bypass of deadbolt mechanism
    - Design incompetence

LIABILITY

- Defective or deficient products
- Negligent designs
- Misrepresentations in packaging
- Manufacturers are experts
- Federal statutes
- Fiduciary duty to customers
  - DCR v. PEAK

NEEDED: Real World Testing

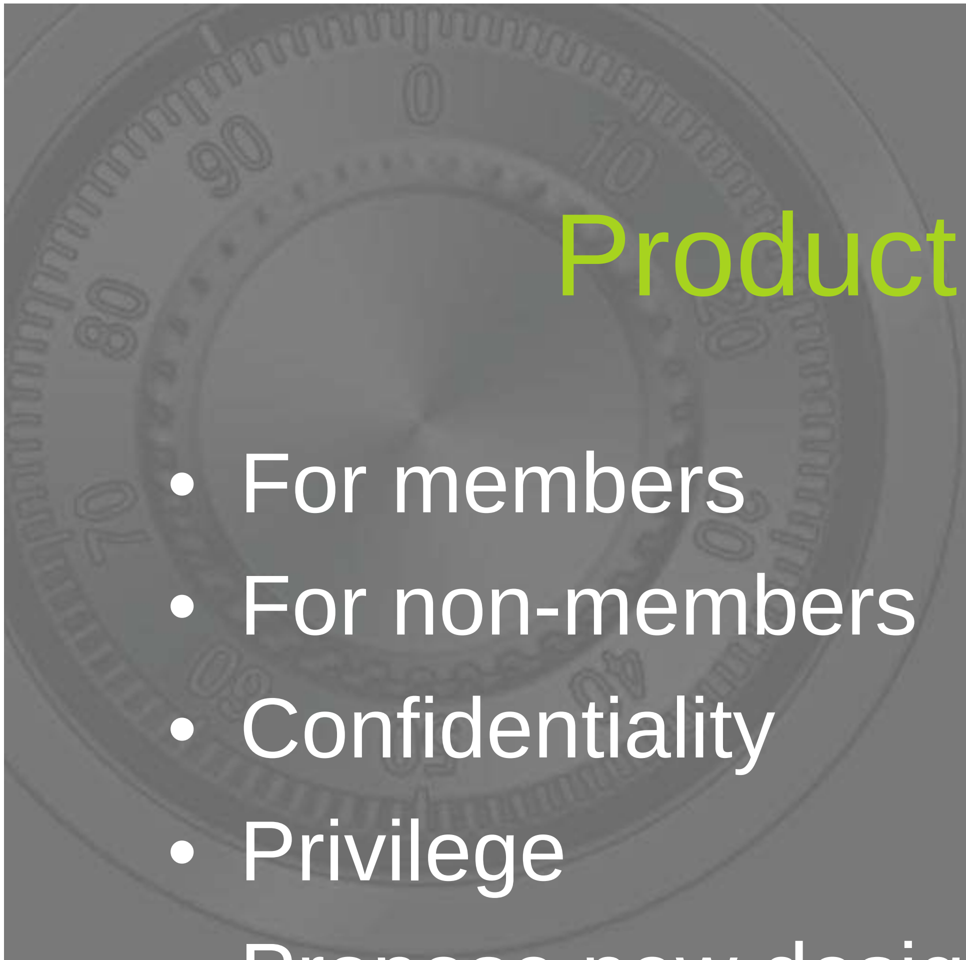
- Propose Security Laboratories
  - – Security professionals
  - – Manufacturers
  - – Law enforcement
  - – Locksmiths
  - – Hackers: Vulnerability Geeks
    - Why we need Physical Security Hackers

SECURITY LABORATORIES

- Disclosure Policy
  - Product beta v. introduced
  - Can the problem be fixed
  - Who’s at risk
  - Notify manufacturer: recall or replace
  - How many locks are affected
  - Level of risk
  - National security issues?

DISCLOSURE CRITERIA

- Public or private disclosure
- Level of threat
- Likelihood of exploit
- Market penetration
- Level of disclosure
  - Security issues only
  - Detail the vulnerability
  - Demonstrate the vulnerability



Product Testing

- For members
- For non-members
- Confidentiality
- Privilege
- Propose new designs

Feedback

- Idea of joint cooperation
- Structure of Security Laboratories
- Disclosure policy
- Use of hackers

Thank You

Marc Weber Tobias

mwtobias@security.org

Matt Fiddler

mjfiddler@gmail.com

Web: http://security.org

Blog: http://in.security.org

in.Security.Org