High Insecurity Locks: What you Need to Know about Locks, Lies, and Liability

Marc Weber Tobias
Agenda

• Conventional v. High Security Locks
• 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
Conventional Pin Tumbler Locks

- Minimal security against covert methods of entry and forced entry
- Bump open easily
- No standards for security, some grades of strength and endurance
- Not used for high security locations
- No secondary locking systems as in high security cylinders
High Security Locks: Critical Elements?

• What are they?
• When are they used and why?
• Standards and what they mean?
• What you need to know!
• Manufacturer knowledge: representations and the truth
• Misrepresentations by lock makers
• Medeco® case study
What is a High Security Lock

- High tolerance
- Quality materials and workmanship
- Expensive: a form of insurance
- Extended testing for security
- Special distribution channels
- Many security enhancements
- Two or three separate parallel systems
- More difficult to compromise than conventional cylinders
Use of High Security Locks: When you need to be sure!

- High value targets
- Critical infrastructure
  - I-T, Command and Control Centers
  - High value business: banks, gems, drugs
  - Government Installations
  - White House, Pentagon, Nuclear security
  - Embassies, Critical Missions
Why We Need High Security Locks

Protect Against Special security vulnerabilities:
  – Bumping
  – Picking
  – Replication of keys and key control
  – Extrapolation of Top Level Master Keys
Standards: What they Mean

• High security lock standards:
  – Benchmarks for everyone to rely upon because most cannot test locks themselves
  – Facility specifications based on standards:
    • In U.S. UL/ANSI
    • In Germany: Vd.S

• How are locks tested and by whom
• Standards are inadequate for real world
• Case Example: Medeco® High Security Locks
High Security Locks: Primary Protection Criteria

• Forced Entry
• Covert Entry
• Key Control
• What is not covered: Common exploits
  – Bumping
  – Special forms of picking
  – Mechanical bypass
  – “Real World” Techniques
  – Bypass of key control
## UL-437 Attack Resistance

(Door locks and Cylinders)

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Time Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Picking</td>
<td>10 Minutes</td>
</tr>
<tr>
<td>Impressioning</td>
<td>10 Minutes</td>
</tr>
<tr>
<td>Forcing</td>
<td>5 Minutes</td>
</tr>
<tr>
<td>Drilling</td>
<td>5 Minutes</td>
</tr>
<tr>
<td>Sawing</td>
<td>5 Minutes</td>
</tr>
<tr>
<td>Prying</td>
<td>5 Minutes</td>
</tr>
<tr>
<td>Pulling</td>
<td>5 Minutes</td>
</tr>
<tr>
<td>Driving</td>
<td>5 Minutes</td>
</tr>
</tbody>
</table>
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
Security Against Forced Entry
Drills and End-Mills: A common attack
Forced Entry: Drilling Conventional Cylinders
UL-437 Tools used for Testing (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
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
  – Test for different methods of attack
Standards (ANSI A156.30): Covert Methods of Entry

- Pick Resistance (Cumulative)
  
  C: Minimum of 2 Security Pins
  Paracentric Keyway
  Minimum of one bore depth designed to prevent over-lifting
  
  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
Covert Entry - Picking
Mechanical Bypass

• Defeating locks in less than a minute
• Often not included in standards
  – May be forced or covert entry
• Many certified locks can be compromised
• Public is misled into a false sense of security
Mechanical Bypass: Another Method of Entry

- Wires and shims
- Vibration, shock, bumping
- Air pressure
- Magnetism
- Breaking of internal components
- Radio Frequency energy
- Temperature
Manufacturers: What they Know and will Disclose

- Great R&D
- Some have a poor understanding of methods of bypass
- Cannot Make secure if don’t know how to break
- Failure of Imagination
- Misrepresentations of security:
  - Know and will not disclose
  - Don’t know, negligent misrepresentation
What You Need to Know about High Security Locks

- Manufacturer may not know or tell you
- Manufacturer may not fix: It's about $
- Criminals may know and exploit problems
- Mechanical bypass often simple
- Medeco® deadbolt: Secure for 20 years
- Tobias attack: Secure for 40 years
Representations by Manufacturers

- Locks are secure
- Implied representations
- Know or should have known of problems
- Meet specifications?
- Need truth in packaging and advertising
- Design issues and failures
- Bypass methods not contemplated
Failure of Imagination

- Mechanical bypass
- Forced entry techniques
- Covert entry techniques
- Key control compromise
  - Manufacturers cannot find the vulnerabilities
  - Why we need White Hat hackers
Design Issues

- Failure of imagination
- Design engineer problem
- Key never unlocks the lock
- Moshe Dyan problem: Design issues can create a two-way path
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
Medeco® Security: A Classic Case Example

- Do they know or are they incompetent?
- They continue to represent:
  - Locks cannot be bumped
    - Even after JennaLynn, the 12 year old bumped open their lock at Defcon 15
  - Locks cannot be picked
  - Key control cannot be compromised
MEDECO®: The High Security Cylinder

- Protects high value and critical targets
- Leading U.S. High Security manufacturer
- For 35 years: THE lock to attack
- UL-437 and ANSI 156.30 rated and VdS
- Everyone trusts their security
- Best engineering in industry
More Medeco® Security

- Many attacks during past 35 years: difficult, complex, high skill level, not consistent results
- Global presence of company, owned by Assa-Abloy
- Two or three separate security levels, all of which must be compromised
Medeco®: Ultimate Security?

• Invented the modern sidebar
• Almost every lock has copied
• Revolutionary design in 1968
• Three generations:
  – Original
  – Biaxial
  – M3 and Bilevel
The Medeco® Problem: Forty years of success!

• Caught up in their own arrogance
• Smarter than anyone else regarding their products
• Nobody could know as much as they do!
• Inability to properly test for “real world” vulnerabilities
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
- All Medeco® locks cannot be compromised
- Security depends upon many factors
  - Location and value of target
  - Expected sophistication of attack
  - Master key or non-master key system
It all Began with Bumping:  
A chronology of Events

• Marc Tobias and Matt Fiddler: Defcon 14, Las Vegas: Bumping, August 2006
• JennaLynn, 11 year old, bumps Kwikset
• August 4, 2006, Medeco® press release: “Our locks are bump proof”
Can Medeco® Locks be Bumped: A research project

• Marc Tobias + Tobias Bluzmanis begin year-long research project re Medeco®
• Originally: Can the locks be bumped? Medeco® said no!
• Resulted in wider inquiry:
  – Reliable method of picking
  – Method to bypass high level key control
  – Hardware bypass: deadbolt disaster
Medeco® 2006: “Our Locks Cannot be bumped”

- October meeting at Medeco®
  - Early research stages
  - Tryout keys not perfected
  - Bumped some but not all locks
    - 24 hours later, opened the test locks from factory
  - Medeco® was not impressed because of early demonstration; They did not believe it.
Miami Vice: Detailed Demonstration for Medeco®!

• Detailed demonstration on video, submitted to Medeco® in December, 2006, showing:
  – Bumping
  – Picking
  – Bypass of key control
  – Simulation of bump keys
December 2006-Present: Bypass of Medeco® security

- Perfected ability to bump open locks with four keys
  - Non-master keyed cylinders
  - Must have correct keyway
  - Not all locks can be bumped open, but many
  - Very reliable process
Four Keys to the Kingdom!

• Four tryout keys to theoretically open all Medeco® non-master keyed cylinders
Bumping to Picking to Bypass of Key Control

• Bumping expanded our research and method of attack
  – Developed a method to reliably pick virtually all Medeco® Biaxial and m3
  – Developed a technique to determine sidebar coding
Medeco® Security Compromise: A Year of Research

- Medeco® Security: 3 levels + key control
  - Conventional pin tumblers
  - Sidebar: a combination of angles
  - M3 slider blocks sidebar
  - Restricted keyways and blanks
  - Each security level has been compromised
Medeco® Methodology: Five Steps to Insecurity

- Compromise key control
- Determine or simulate sidebar code
- Bypass the m3 slider with a paper clip
- Determine how to make a bump key
- Develop a reliable means of picking
Bypass of Key Control

- Analyzed Key control of m3: wider keyway: needed a way to produce blanks
- Simulated restricted keyways
- Made regular keys to open locks
- Made bump keys from simulated blanks with known sidebar code
- Made a bump key with simulated code
Sidebar Codes: Learn or Simulate

• Obtain correct sidebar code to produce a bump key or simulated bump key
• Simulate sidebar codes to open locks
• Two levels of security:
  – First Level: known sidebar code
  – Second level: unknown code, must simulate
The Steps to Insecurity: How we Began

- Bump one lock with known sidebar code
- Simulate a blank to bypass restricted keyways
- Analyze all Medeco® codes
- Analyze lock tolerances
- Synthesize all codes to four keys
- Leverage use of keys for picking
Result: Compromise of all levels of Medeco® security

- Open locks by bumping
- Open locks by picking
- Compromise m3 key control
- Pick and bump one level of ARX pin
Latest Technology: The MEDECO m³

• 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® Security: Sidebar Codes

• Group of angles
• If not known, cannot open the lock
• If the sidebar code is known or can be simulated, then can bypass security
• Each lock or system has unique code
  – First level of compromise: know the code
  – Second level: unknown code
Sidebar Codes: A Combination of Angles
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® Security: Key Control

- Restricted blanks
- Inability to replicate means cannot make keys
  - Key simulation
  - Bypass virtually all key control
  - Make regular and bump keys to open lock
Medeco m³ Meets the Paper Clip

“Michaud M3 Degrade Attack”
Bypassing m3 Key Control

- Circumventing m3 key control with a paper clip
Common Myth #2: Bumping

- Some High security locks can be bumped open
- Medeco®, Assa®, Mul-t-Lock®
- 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!”
  - Our locks are “virtually resistant”

Virtually bump proof = virtual reality
Medeco® Virtual Reality

• “Virtually Resistant”
JennaLynn: Bumps a Medeco® at age 12

- Bumping Medeco® Locks

JennaLynn One Year after opening the Kwikset at Defcon 14
Bumping High Security ARX pins

- ARX pins are the most secure
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 disclosed in patent filing
• High percentage of these locks can be picked
Picking the Medeco® m3

- A reliable means of picking has been developed
Common Myth #4: Hardware Bypass

• Medeco® hardware security: Is it really secure?
• Example: Deadbolts - A failure of imagination

“The key never unlocks the lock!”
Medeco® Deadbolt: The Final Straw

- 20 year design history
- The best design in the industry?
- Bypass in 30 seconds with a 2$ screwdriver
- Bypass of all internal security
- UL, ANSI rated for minimum of five minutes
- No security
Bypass Internal Mechanisms:
Medeco® Deadbolt
Simplicity Itself: Opening the Medeco® Deadbolt

- Opened in 30 seconds
- Incompetent engineering
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
Thank You

Marc Weber Tobias
mwtobias@security.org

Web: http://security.org
Blog: http://in.security.org

© 2007 Marc Weber Tobias

MEDECO®: is a registered trademark of Medeco High Security Locks