A FAILURE OF IMAGINATION: Kwikset Smartkey® and Insecurity Engineering

ONE OF THE MOST SECURE and INSECURE LOCKS IN AMERICA
KWIKSET SMARTKEY
#1: IS SMARTKEY SECURE?
Brian: 06/25/2013 1105 A.M.
#2: IS SMARTKEY SECURE?
Satima: 06/24/2013 4:26 P.M.
#3: IS SMARTKEY SECURE?
Raymond: 06/25/2013 3:58 P.M.
KWIKSET LOCKS
A Spectrum Brands Company

♦ MILLIONS IN USE IN AMERICA AND CANADA
♦ HOMES, APARTMENTS, BUSINESSES
♦ INEXPENSIVE: COST: $20-$30
♦ MODELS:
  – Pin tumbler, 5 and 6 pin
  – Smartkey, 5 pin
  – Deadbolts
  – Electronic + override
ONE OF THE MOST POPULAR LOCKS IN U.S.

♦ MILLIONS SOLD EVERY YEAR
  – COMMON KEYWAY: WEISER, BALDWIN

♦ FOR MORE THAN FIFTY YEARS

♦ DIVERSE PRODUCT LINE
  – Deadbolts
  – Rim
  – Lever handle
  – Electronic
WIDE PRODUCT LINE
HOMES, APARTMENTS, BUSINESS, COMMERCIAL
KWIKSET, WEISER, BALDWIN: The Basics

- PIN TUMBLER AND SMARTKEY
- 5 or 6 PIN CONVENTIONAL CYLINDERS
  - Many configurations
- 5 PIN SMARTKEY PROGRAMMABLE
- COMMON KEYWAYS, NO SECURITY
- NO DUPLICATION PROTECTION
- NOT HIGH SECURITY
- MAINLY RESIDENTIAL AND APARTMENTS
KWIKSET HISTORY

♦ ORIGINAL PIN TUMBLER DESIGN
  – Rim cylinder
  – Deadbolt
  – Key-in-knob design

♦ EASILY COMPROMISED

♦ MOST POPULAR UNTIL 2008
  – Smartkey introduced to Canada and U.S.
PIN TUMBLER v. SMARTKEY
PIN TUMBLER DESIGN

- NOT SECURE
- Easy to pick
- Easy to bump
- Easy to impression
- Easy to mechanically bypass
- Can be master keyed
- Easy to determine the Top Level MK
- Limited number of combinations
PIN TUMBLER DESIGN: How it works
PIN STACKS = SECURITY:
Plug can turn: pins at shearline
LOCKED:
PINS NOT AT SHEARLINE
KWIKSET SMARTKEY: Not a pin tumbler lock
SMARTKEY ATTRIBUTES

- 5 PIN ONLY 6 DEPTH INCREMENTS
- SINGLE SIDEBAR SECURITY
- EXTREMELY PICK RESISTANT UL437
- CANNOT BE BUMPED
- CANNOT BE IMPRESSIONED
- INSTANT PROGRAMMABILITY TO ANY KEY
- CANNOT BE MASTER KEYED
MORE ATTRIBUTES

- ONE PRIMARY KEYWAY
- BHMA 156.5 GRADE 1 RATING
- UL 437 RATING
- SPECIAL “KEY CONTROL DEADBOLT” AS ALTERNATIVE TO MK SYSTEM
SMARTKEY DESIGN
PROGRAMMABLE SLIDERS
SIDEBAR = SMARTKEY SECURITY
MASTER KEY SYSTEMS: Pin Tumbler v. Smartkey

♦ CONVENTIONAL MK SYSTEMS
CONVENTIONAL MK SYSTEM ATTRIBUTES

✧ ONE KEY OPENS MANY LOCKS
  – Only bottom pin and master pin per chamber

✧ DIFFERENT LEVELS OF KEYING
  – Can reduce number of change keys

✧ EXPENSIVE TO REKEY OR ADD KEYS
  – Must disassemble cylinder to rekey

✧ CROSS KEYING BETWEEN LOCKS AND SYSTEMS
MK SYSTEM SECURITY

- INHERENT INSECURITY
- MUST HAVE AT LEAST TWO SECURITY LAYERS
- EASIER TO COMPROMISE ENTIRE SYSTEM
  - Multiple shear lines
  - Unintended key combinations will open lock
  - Easier to pick, bump, impression, decode
  - Extrapolation of TMK
KWIKSET KEY CONTROL: The Alternative to Master Keying

- **TWO INDEPENDENT CORES**
- **TWO SEPARATE AND DISTINCT KEYS**
  - Supposed to maintain security of key blanks
  - Control key only from factory
- **INSTANTLY REPROGRAMMABLE**
- **NO CROSS KEYING OR INCIDENTAL MASTER KEYS**
- **NOT A REAL MK SYSTEM**
- **ONLY ONE LEVEL OF KEYING**
KWIKSET “KEY CONTROL”
Positive Attributes

- NO LOCKSMITH REQUIRED
- 46,656 THEORETICAL COMBINATIONS
- GOOD FOR FACILITIES THAT NEED ONE MK LEVEL ONLY
- GREAT FOR CONSTRUCTION MK
- NO DISASSEMBLY OF CYLINDERS
- TWO INDEPENDENT SHEAR LINES WITH NO INTERACTION LIKE CONVENTIONAL SYSTEMS
KWIKSET “KEY CONTROL”
More positive attributes

- INSTANT ABILITY TO REPROGRAM
- TWO SEPARATE KEYWAYS
- CANNOT DERIVE CONTROL KEY FROM CHANGE KEY
- LIKE CORBIN “MASTER SLEEVE” SYSTEM 75 YEARS AGO, INHERENTLY MORE SECURE
- LITTLE CHANCE OF ONE SYSTEM OPENING ANOTHER
KWIKSET “CONTROL KEY”

The Bad

- NO WARRANTY FOR COMMERCIAL
- NOT FOR COMPLEX OR COMMERCIAL SYSTEMS
- CAN BE COMPROMISED IN 15 SECONDS
- EASY TO DECODE CONTROL KEY
- EASY TO REPLICATE CONTROL KEY
- NO PATENT PROTECTION ON KEYS
SECURITY: YOU GET WHAT YOU PAY FOR

- DO YOU EXPECT A $20-$30 LOCK TO PROVIDE ANY SECURITY?
  - Some buyers cannot afford higher security
  - What is the minimum they are entitled to?
- KWIKSET KNOWS THESE LOCKS HAVE SERIOUS VULNERABILITIES
- DOES THE PUBLIC HAVE A RIGHT TO KNOW HOW EASY TO OPEN?
  - Should there be warnings on packaging?
KWIKSET SMARTKEY: INSECURITY ENGINEERING

- MILLIONS OF PEOPLE AND FACILITIES AT POTENTIAL RISK
  - COVERT ENTRY
  - FORCED ENTRY

KWIKSET “Highest grade of residential security available.”
  - True but misleading
  - Open in less than thirty seconds
FALSE SENSE OF SECURITY

- BHMA GRADE 1 RATING
- “Highest grade of residential security”
- UL 437 PICKING RATING
- VIRTUALLY BUMP PROOF
- USERS ARE NOT AWARE OF RISKS
- LOCKS CAN BE OPENED IN SECONDS
- FAILURE TO DISCLOSE VULNERABILITIES
KWIKSET ADVERTISING and MISREPRESENTATIONS

- FALSE OR MISLEADING STATEMENTS BY TECH SUPPORT AND SALES

- 8 SEPARATE INTERVIEWS:
  - “Cannot be opened except by drilling”
  - “No maintenance problems”
  - “Video on YouTube not true: lock was tampered with”
  - “No way can be opened with a screwdriver”
  - “The problem has been dealt with”
SMARTKEY DESIGN ISSUES

- SIDEBAR SHOULD PROVIDE MORE SECURITY THAN PIN TUMBLER LOCK
- ONLY ONE LAYER OF SECURITY
- SMALL FRAGILE SLIDERS
- PROGRAMMING PROBLEMS
- LOW TOLERANCE, LIMITED DIFFERS
  - 243 Key combinations
  - All the same blank
- CAST METAL EASILY COMPROMISED
MORE DESIGN ISSUES

- Plug design can be warped
- Slider design
- Able to decode the sliders
- Sliders easily jammed
- Tailpiece design and access
- No key detent for programming
SMARTKEY: METHODS OF DEFEAT

- TRYOUT KEYS
- TAILPIECE, WIRE THROUGH KEYWAY
- VISUALLY READ SLIDER POSITION
- TORQUE THE PLUG AND OPEN
- REPLICATING CONTROL KEY
- DECODING OF THE MASTER KEY
TRYOUT KEYS

- BITTING = 6 DEPTHS @ .023”
- 5 SLIDERS
- UNIVERSE OF KEYS = 3 to 5<sup>th</sup> = 243
- #1.5 = DEPTHS 1-2
- #3.5 = DEPTHS 3-4
- #5.5 = DEPTHS 5-6
DEPTH INCREMENTS AND TOLERANCE

DEPTHs 1-2-3-4-5-6
DEPTH INCREMENTS 1-2

DEPTH 1-2 = 1.5
DEPTH INCREMENTS 3-4

DEPTHS 3-4 = 3.5
DEPTH INCREMENTS 5-6

DEPTHS 5-6 = 5.5
TAILPIECE DESIGN

♦ SAME DESIGN FOR PIN TUMBLER AND SMARTKEY
♦ HOLLOW AND SOLID TELESCOPING
♦ PLUG CAP NOT SUFFICIENT
♦ ZIG ZAG WIRE THROUGH KEYWAY
  – No trace
  – No damage
  – Less than 30 seconds
KEY-IN-KNOB ATTACK: Tailpiece access
KEY-IN-KNOB ATTACK
TAILPIECE AND WIRE
VISUAL DECODING SLIDERS

- SLIDER TO TUMBLER INTERFACE
- CAN DETERMINE POSITION OF SLIDER AND KEY CODE
- INSERT BORESCOPE OR MIRROR TO VIEW POSITION
TORQUE THE PLUG

♦ BELIEVE VIOLATES THE BHMA 156.5
♦ Formal complaint filed
♦ HOW THE LOCK CAN BE COMPROMISED: DESIGN ISSUES
  – Warp sliders or keyway
  – Application of 110 pound force inches
  – Set sliders to specific position
  – Apply torque with 4” screwdriver and wrench
  – OPEN IN ABOUT FIFTEEN SECONDS
SLIDER DESIGN AND TORQUE ATTACK
TORQUE AND BHMA 156.5

REQUIREMENT = 300 lbf-in
OPEN in 112 lbf-in
112 Pounds Force Inches = OPEN
KEY CONTROL: NONE
DECODING THE LOCK OR CONTROL KEY

- KEY CONTROL BLANK ONLY AVAILABLE FROM FACTORY
- NOT THE SAME AS CHANG KEY
- SPECIAL DECODER TO READ THE SLIDERS
MAKING THE CONTROL KEY

- SEPARATE KEYWAYS ARE NOT SUPPOSED TO BE INTERCHANGEABLE
- THE REPRESENTATION: CONTROL KEYS ARE SECURE
CHANGE KEYS AND CONTROL KEYS
SUMMARY: SMARTKEY INSECURITY

♦ ONE OF MOST POPULAR AND INEXPENSIVE LOCKS IN US. AND CANADA
♦ CONSUMER FRIENDLY
♦ FILLS CERTAIN NEEDS
♦ SECURE AGAINST CERTAIN ATTACKS
  – Picking
  – Bumping
BURGLARS:
THEY DON’T PICK LOCKS

- PICK RESISTANT
- BUMP PROOF
- ALL OF THE SECURITY IS MEANINGLESS IF THE LOCK CAN BE OPENED IN 15 SECONDS
- PATENTS MEAN NOTHING
- BHMA RATINGS MEAN NOTHING
- COULD BE MADE SECURE
- YOU GET WHAT YOU PAY FOR