

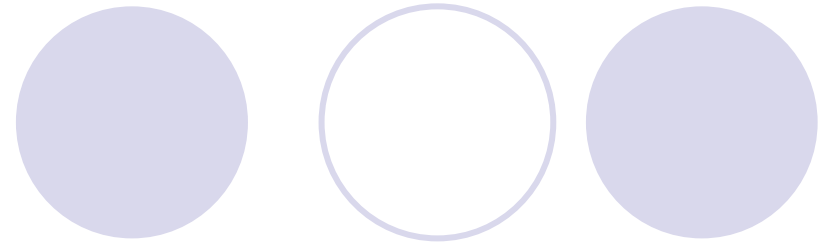
Things that go “BUMP” in the Night:

An analysis of current and emerging threats to Physical Security

Marc Weber Tobias

Matt Fiddler

Types of Locks

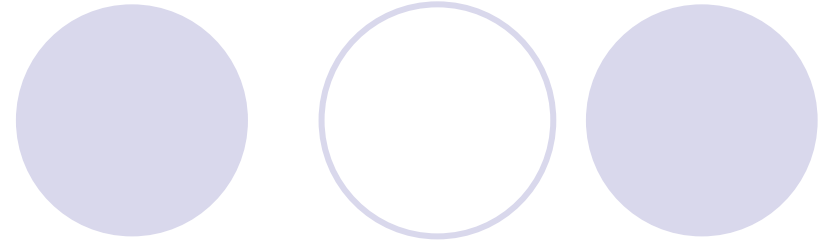


- Warded
- Lever
- Wafer and Disc Tumbler
- Pin Tumbler
- Hybrid: Combined Technologies
- Combination
- Most Often Utilized
 - LEVER (Europe)
 - PIN TUMBLER (US)

Pin Tumbler Locks

- 4000 year old Egyptian design
- Re-invented by Linus Yale in 1860
- Modern pin tumbler: split pins
- Comprises 95% of all locks
- Low to high security applications
- All based upon original Yale design
 - Billions of locks
 - Many different configurations

Security of Locks



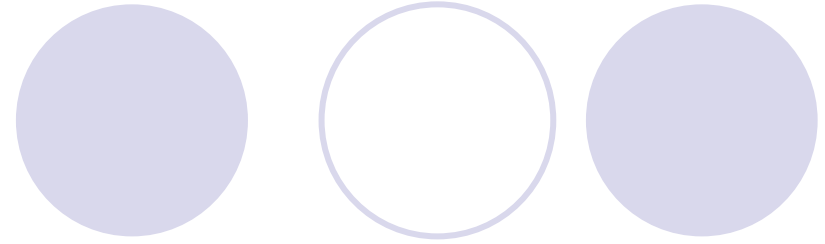
- The Perfect World:

- Locks cannot be opened without correct key or codes

- Reality:

- There are levels of difficulty or resistance to forced or covert methods of entry

Methods of Entry



- Destructive
- Non-Destructive
 - Covert
 - Surreptitious

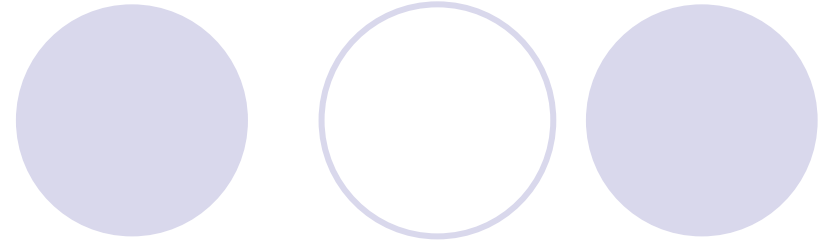
Covert Methods of Entry (CMOE)

- Picking
- Impressioning
- Decoding
- Extrapolation of TMK
- Bumping: “The New old threat”
 - ALL METHODS REQUIRE
 - Move all pins to shear line together or separately
 - Allow plug to turn without obstruction

What do we need to open a lock?

- Prior Intelligence?
 - Master Key Data
 - Sidebar codes
 - Keyway information
- Blanks or keys that can be modified
- Methods to Cut or produce a Key
 - Copy of Key
 - Simulate Key
 - Decode actions of Key and Tools
 - Impressioning
 - Manipulation of components

What is a Key?



- Keyway
- Bitting
- Secondary Locking Mechanism
- Check Pins
- Interactive components
- RF and Magnetics

“The Three T’s and Two R’s”

- Time

- Can bypass be achieved in under a minute?

- Tools

- Are special tools needed

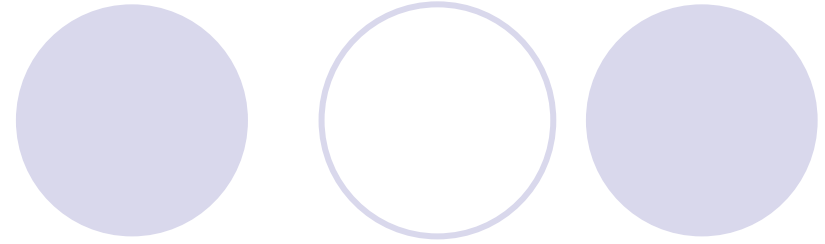
- Training

- Are special skills or training required

- Repeatability

- Reliability

Bumping Locks



- The Threat from Bumping
- What is a Bump Key?
- 999 key and cylinder
- Training
- Difficulties Making Keys
- Covert Entry via Bumping?
- Is it Easy to Learn?
- Variables that affect Bumping
- Misinformation
- Case Examples



The Threat from bumping

- Quick
- Easy
- Repeatable
- Applies to most locks
- Virtually anyone can open a lock
- Often no trace or damage

Reinvigorated by Toool;

<http://www.toool.nl/bumping.pdf>

What is a Bump Key

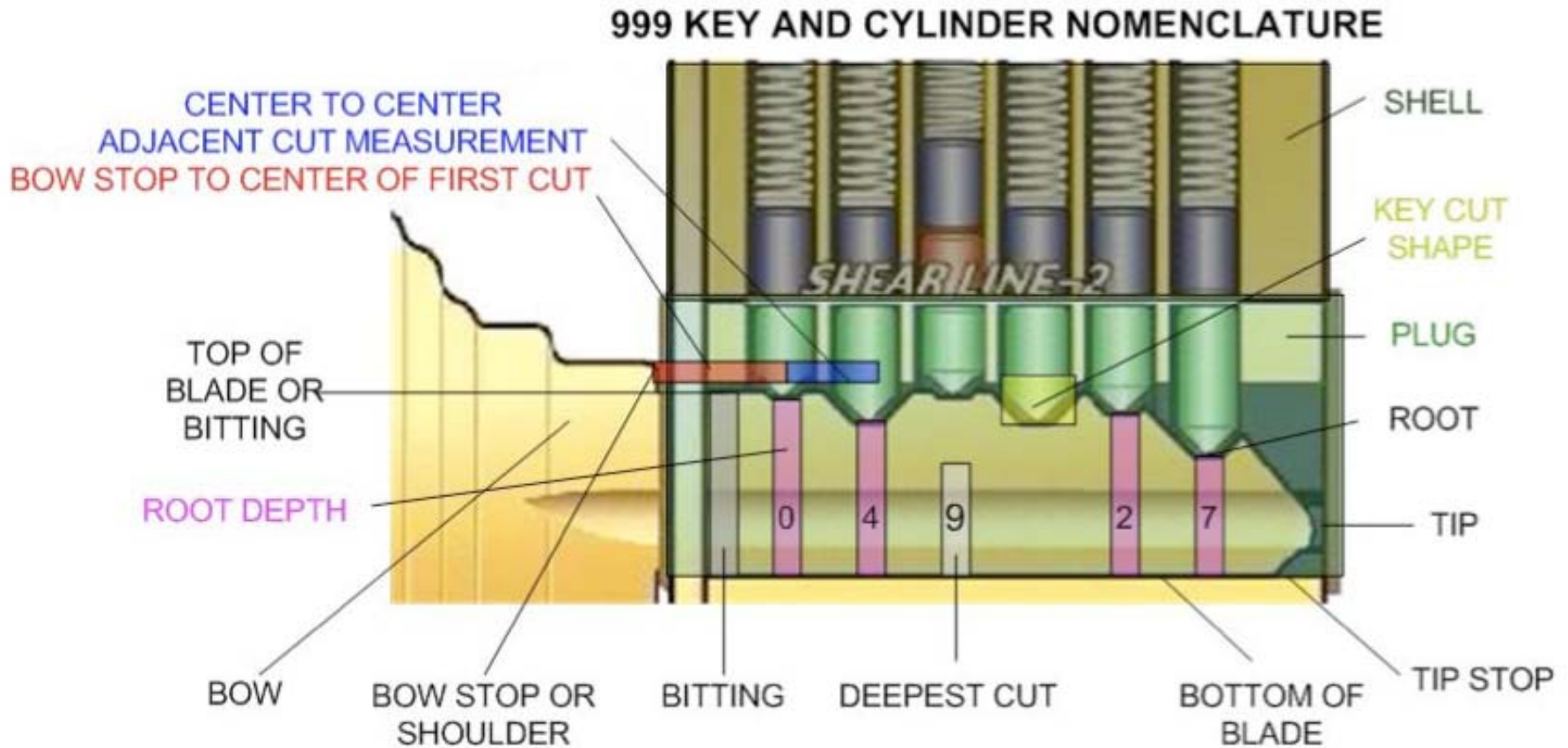
- Any key that fits the lock
- All cuts made to the deepest allowable position



Why 999?

- Originated in Denmark 25 years ago
- Keys could be duplicated by code
- 0 = Shallowest
- 9 = Deepest
- Thus “999” Key

999 Key and Cylinder



Training

- How to position the key
- Amount of force needed
- Correct amount of torque
- Timing between “Bump” and “Torque”
- How to repeat the process

Difficulties Making Keys

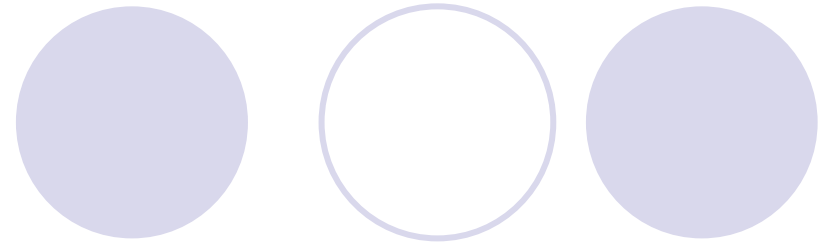
- Availability of key that fits the target
- Virtually any key can be modified
- File to deepest depth
- “Most” are easily obtainable

Covert Entry via Bumping

- There can be significant noise
- Depends on the condition of the lock
- Sometimes only one strike is required



Is it Easy to Learn?



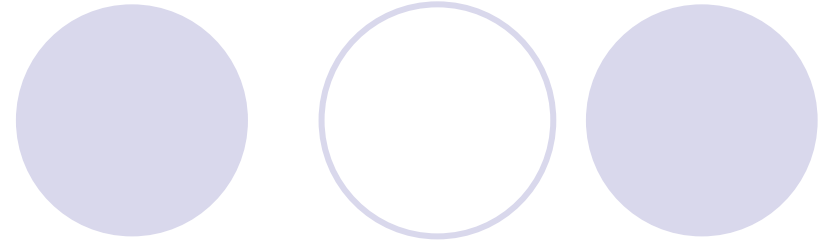
- Can be learned in less than an hour
- Requires virtually no skill



Variables that affect Bumping

- Availability of Blanks
- Secondary locking mechanisms
- Noise tolerances while bumping
- Spring conditions / biases
- Lubrication and ease of movement of pins
- Concerns with forensic marks or indications
- Depth and spacing info and availability
- Shoulder and Tip modifications
- Solid cams at end to stop blanks
- Anti-Bump Locks

Misinformation



- Not all locks are affected!
- Protection against bumping methods
- Complexities
- Ability to create keys

Millions and Millions Vulnerable

- Apartments
- Office Buildings
- Hotels
- Elevators
- Colleges
- Mailboxes...

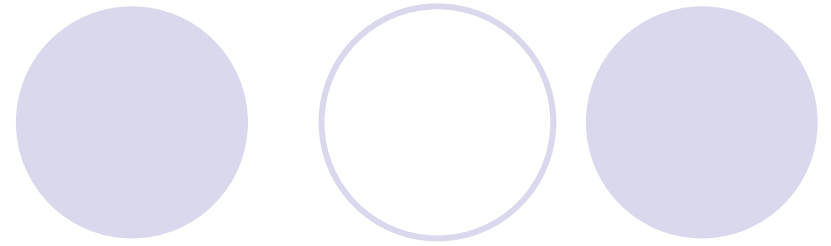
Is it really a threat to physical security?

Case Examples

- The UPS Store
 - Mail Boxes Etc.
- USPS



The Real World



- Post Office and UPS / MBE Boxes Worldwide
- Millions of users at risk of:
 - Identity Theft
 - Surveillance of mail
 - Unlawful Interception
 - Injection of explosives / Bio-Hazzards

38,000 Locations
5+ Million Mailboxes



Legal Issues of Bumping

- Current Statutes
- Trafficking in precut Bump-Keys and Tools
- Manufacturers Liability
- What if I suffer a loss?

Current Statutes

- **83 USC 1704**, makes it a federal crime to improperly utilize, sell or traffic in keys that will open post office locks
- **39 USC 3002(a)** prohibits sending lock picking and bypass tools by mail
- **18 USC 1716A** makes it a crime to send any materials defined in **39 USC 3002(a)** through the mail or interstate commerce by common carrier such as Federal Express or UPS

Trafficking in Bump Keys and Tools

- **39 USC 3002** is not applicable to bump keys and only applies to tryout keys for motor vehicles and related issues, and bypass tools
- Should Bump Keys and Tools be **RESTRICTED?**



SINCE
1997



Product Categories

LOCK ENTRY TOOLS

- Pick Guns (Electrics)
- Pick Sets
- Tubular Lock Picks
- Lock By-Pass Tools
- Pick Set Parts
- Special Tension Tools
- Plug Spinners
- Destructive Entry

AUTOMOTIVE

- Auto Opening Kits
- Individual Auto Tools
- Auto Pick Tools
- Try-Out Keys

LOCKSMITH TOOLS

- Locksmith Tools
- Broken Key Tools
- Impression Tools
- Files

PIN KITS & REKEYING TOOLS

- Rekeying Tools & Pins
- I-Core Tools

KEY MACHINES & PUNCHES

- Key Machines
- Key Machine Parts

KEY BLANKS



Email this to a friend

KE-Bump Kinetic Energy Bumping Starter Kit KEH-1-SK-A

KE-Bump Kinetic Energy Bumping Starter Kit

In Stock	Normally	Your Price	Qty	
Y	US\$29.50	US\$26.00	1	BUY

Detailed Description

This new method of lock manipulation is becoming popular among locksmiths worldwide.

We are happy to bring to you the KE-Bump Lock Bumping Starter Kit. The kit includes the KE-Bump Tool, (2) sample packs of Lock Saver Lock Lubricant (increases bumping successfulness), (1) M1 (padlock) bump key, and a key turning tool to get you started. Locksmiths should use this kit to see how bumping locks works and then easily make their own bump keys as needed. Locksmiths will find the KE-Bump Tool itself a great addition to their tool collection.

We do have 3 additional bump keys available to qualified professionals including government, military personnel, repossessors, etc. who do not have access to a code machine or key punch. Keys available include KW1 (Kwikset), SC1 (Schlage), and WR5 (Weiser Lock). More to come in the near future. Please contact us to purchase these additional bump keys.

Your Basket

Your Cart Is Empty



HACKER SAFE
TESTED DAILY 29-JUN

Legal Matters

Terms Of Sale
Privacy Statment



[Sign In](#)

[Can I buy from Hawley Lock Supply?](#)

[Antique Auto Locks, Keys, etc](#)

[AutoSmart Books](#)

[Baxter Books/Code Books](#)

[Baxter Guide/Depth Key Sets](#)

[Books](#)

[Blackhawk Products](#)

[Baxter Tryout Sets](#)

[Curtis #15 Clippers](#)

[Determinator Tools](#)

[Framon Key Machines/Tools](#)

[Good Stuff](#)

[Hinge Doctor](#)

[Knockers Bump Keys](#)

[High Security Guide Keys from National Auto Lock](#)

[Precuts](#)

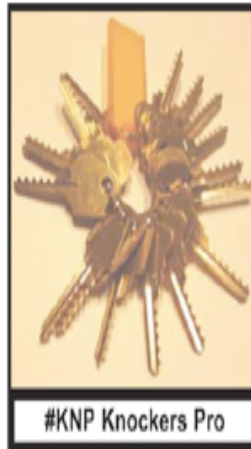
[Peterson Manufacturing](#)

[Rytan Key Machines and Tools](#)

[Tools, Tryouts and Equipment](#)

[Wedqeco Extractors & Tools](#)

Knockers Pro Bump Key Set



Quantity in Basket: 3

Price: **\$44.95**

Quantity:

Includes: Arrow (5 and 6 pin), Dexter, Ilco, Kwikset, Master (M1), National, Schlage (5 & 6 pin, 3 keys), Weiser (5 pin), Weslock, Titan and Yale (5 & 6 pin)

Manufacturer Liability?

- If a lock can be opened in two seconds by simply applying torque to the plug and rapping on a key, should such a problem give rise to a claim for defective product or false advertising?

What if I Suffer a Loss?

- If proof of entry must be evident...
 - Theft may not be recoverable
- In some cases...
 - Forensic evidence may be difficult to prove

Questions?



Marc Weber Tobias (mwtobias@security.org)
Matt Fiddler (langly@redteam.org)

<http://www.security.org>