Mail Order Cores that Defeat Matt Blaze

Victor Aguilar **www.commercial-locksmith.com/blaze.php**

Matt Blaze is a professional cryptographer who published a paper, Rights Amplification in Master-Keyed Mechanical Locks. (He is also the author of Safecracking for Dummies, which teaches illicit safecracking.) Facilities that use SFIC locks are vulnerable to rights amplification, which allows a low-level employee who is issued a key only to his own office to obtain a master key for the entire facility. This attack requires only a key machine or, if one is persistent, a hand file. The attack is carried out entirely by trial and error in the employee's own office using no more than eight key blanks; the lock is neither disassembled nor damaged. The key machine need not be present; though conducting one trial per day is time consuming. The trials are conclusive, so when the thief finally works up the nerve to approach the cash office or server room, he already knows that he has a master key that will open it. Imagine losing your server! Thousands of identities could be stolen and your business bankrupted.

My Anti-Blaze Masterkey System precludes a Blaze attack; the thief would have to approach the cash office or server room *hundreds* of times, trying one potential master key after another. Also, the cores defy the Peterson lock pick and include spool pins to make them pick resistant. The keys are nickel silver because brass keys wear out, become blunt and damage the cores.

Beware of lazy locksmiths who use color-coded pins! Some locksmiths are not very bright and/or they work with interchangeable cores so rarely that it seems complicated to them. But making each size of pin a different color is a weakness; anybody with an otoscope can look in the keyway and see what color the pins are. With your naked eye you can see the outer pin; if it is colored, then you *need* to replace your cores! Also, colored pins are soft brass and wear out quickly. In a few months the locksmith will charge you to fix a problem that he created!

My masterkey system is also designed to foil someone using a bench grinder to disassemble a lock and decode it for the control key, which can then be used to pull the cylinders from important locks. Padlocks that are left hanging loose on their chain and mysteriously disappear are probably the subject of this type of attack. If a core is brought to me, I ask the person what company he works for and then I call to get a manager to vouch for him. He may be legitimate; companies sometimes lose their control key, or their previous locksmith was trying to lock them in as customers by not giving them their control key. But there are many disreputable locksmiths who will decode any lock that is brought to them. My system will stymie a decoder.

There are two types of grand-masterkey systems:

1) **A district manager** has a grand master key that operates every lock in hundreds of stores. Each store has only two keys; the exterior doors and the cash office. The store manager's master key operates both locks while his assistant can only open the store.

2) **A few big buildings** with hundreds of offices each. There is a grand master key that opens everything; a master key for each building; and every tenant has a key only to his own office or workspace.

In the former case, what is wrong with each store manager carrying two keys, one for his cash office and one for the exterior of his store? The district manager will still have a master key that fits everything, which is necessary if he fires a manager or must find a substitute when one is ill or on vacation, but the store managers are only slightly inconvenienced by having two, not one, keys on their rings. In the latter case, who really needs a key that fits every lock? Upper management has authority over everybody in all those buildings; but the CEO is not walking around opening doors; if he wants to see someone, he calls that employee to his own office.

In point of fact, security is weakened by the presence of a grand master key, so I hope the rationale in the preceding paragraph is convincing, because I will not supply a grand master key. I will, however, partition your system into low-, medium- and high-level locks. It is difficult to the point of impossible for an employee assigned the key to a low- or medium-level lock to employ the Blaze attack against a high-level lock, like the cash office or server room. Also, it is difficult for an employee assigned the key to a low-level lock to employ the Blaze attack against a medium-level lock, like his supervisor's office. Thus, in a way, my system is similar to a grand-masterkey system, in that there are low-, medium-, and high-level employees.

Facilities do not get to specify the cuts on their master key or control key. The Anti-Blaze Masterkey System cannot be implemented by replacing only certain locks, like the cash office. Because rights amplification means a low-level employee obtaining a master key by trial and error on his own lock, *all* the cores in the facility must be replaced, high and low. Since you are purchasing a complete set of cores, there is no reason not to change the keyway; doing so prevents bump keys from being made out of the old keys. And you do not get to choose; you are getting L because it is compatible with Cormax and it defies the Peterson lock pick.

The price is $20 for SFIC cores (minimum ten cores), $20 to masterkey and $3.50 for keys. I can also do Corbin-Russwin System 70 and Schlage Everest for the same labor charge, plus the list price of cores. ASSA cylinders with my sidebar are $95 and keys are $8; the labor is the same.