from *SIAM News*, Volume 36, Number 2, March 2003

Master-Keyed Mechanical Locks Fall to Cryptographic Attack

By Sara Robinson

Getting through a locked door isn't hard; locks can be picked or forced, and glass windows can be broken. But the sophisticated burglar might prefer a more subtle approach: deducing a master key mathematically.

Last month Matt Blaze, a cryptologist at AT&T Labs–Research, showed that anyone with access to a single lock and key in a typical master-keyed system of locks can easily determine the master key. Requiring no more than a file and a small number of blank keys, the attack appeals to the thrifty burglar.

Blaze started to ponder the cryptography of locks after thinking about a more general question: Might the theory of cryptography provide interesting insights into systems outside computers and electronics?

"Locks are among the very few surviving examples of a truly mechanical computational security device," Blaze says, "yet we tend to think of them not as computers, but rather simply as physical objects."

Once he began thinking of locks abstractly, he immediately saw a problem: A design flaw in the standard master locking system enables an attacker to guess and verify the secret description of the master key one bit at a time.

To those steeped in mathematical training, the flaw seems absurdly obvious. Yet few people think of locks mathematically, Blaze observes.

"I think this is an example of how useful abstractions are," he says. "If you think about locks in computational terms, this sort of question [i.e., whether key bits can be tested one by one] comes quite naturally. But if you're thinking about them in strictly mechanical terms, that's just not something you'd think to ask. I've known about the physical design of locks for years, but it wasn't until I thought to consider them more abstractly that this attack presented itself, and then it did so almost immediately."

How a Lock Locks

Blaze's attack applies to "pin tumbler" locks, the kind of lock you probably have on your front door. The basic mechanism has existed for thousands of years, Blaze says; it was used to lock tombs in ancient Egypt. The modern version seems to date from the late 19th century (judging by an 1889 patent).

In a pin tumbler lock, the key fits into a rotatable tube, called a "plug," that sits within a fixed cylinder known as the "shell." Rotating the plug within the shell operates the locking mechanism. When the lock is locked, the plug is prevented from rotating by little sticks of metal under spring pressure that protrude from the plug into the shell. Each stick, known as a "pin stack," is cut into two (or more) pieces ("pins") at one or more of a standard, discrete set of positions.

When the lock is empty, the cuts in the pin stacks sit inside the plug and the ends of the outermost pins protrude into the shell. When a correct key is inserted, it lifts each pin stack to a height where the cut is precisely aligned with the boundary between plug and shell. This enables the plug to turn and operate the mechanism.

The height of a key under each pin stack position (the "bitting") is the cryptographic equivalent of the secret that decodes an encrypted message and can be thought of as a series of digits. For a five-pin lock, for instance, the bitting could be described as 13264, meaning that a key for the lock would be cut to depth 1 nearest the grip and to depths 3, 2, 6, and 4 moving toward the tip.

Typically, a pin tumbler lock has between four and seven pins and anywhere from four to ten depth ranges; the number of possible keys for such a lock thus ranges from 4^4 to 10^7. By computer standards, where a candidate key can be tested in a fraction of a second, this is a tiny number. But for the physical world, where testing a key is a slow procedure, this key space is large enough to thwart a brute-force attack.

Master Keying

In institutional settings, it's often convenient for janitors or building supervisors to have a single key, a master, that opens some or all of the locks in the building.

The standard way to create a master-keyed tumbler lock system is to cut some or all of the pin stacks for each lock in two places: one standard set of cuts corresponding to the master key, plus a separate specific set of cuts for an individual key (called the "change key").

Imagine, for example, cutting one lock at 11111 and 22222, then cutting another at 11111 and 33333; 11111 is then a master key for this two-lock system. Notice that 12222 and 11222 and 22111 all yield functioning keys for the first lock.

Herein lies the weakness of the system.

Deducing a Master Key

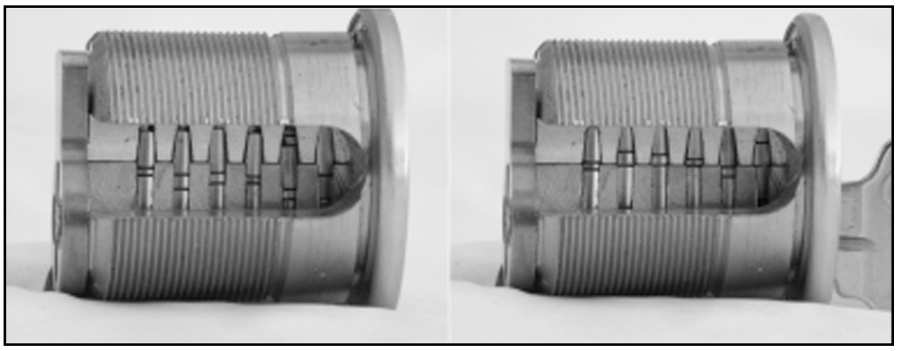
Blaze's master-key crack goes like this: Assume you have access to a single change key and lock, and suppose the system has pin stacks 1 through P and potential bittings 1 through N (a key space of size N^P).

For each pin stack q, create N keys (labeled $1 \ldots N$) so that the keys look identical to the change key at pin stack $p \neq q$, and the key has height N at pin stack q.

Now, for each pin stack place, try each of the N keys in turn. If one of the keys works, mark down that bitting height and pin stack

position. For each position, two of the bitting heights will work, that of the master key and that of the change key. (They may be the same.) Because the change-key heights are known, the remaining list of working bittings is a description of the master key.

The number of steps required for the attack is at most $P \cdot N$, a great improvement over a brute-force approach, which requires up to N^P steps. The only materials required are a file and $N \cdot P$ blank keys. Practically speaking, P blank keys will also suffice, since a single blank key can be cut repeatedly to progressively greater depths.



A master-keyed pin tumbler lock. Two cuts can be seen in each of the six pin stacks (left). With the correct change key inserted (right), one of the cuts on each pin stack is aligned at the shear line. The other cut is sometimes above and sometimes below the shear line. Courtesy of Matt Blaze.

After discovering the attack, Blaze tested it (with permission, of course!) against a variety of medium- and large-scale institutional master-keyed systems, installed in both educational and commercial environments. He tested both new and old systems, from half a dozen different manufacturers.

The attack was complicated by some practical considerations, such as variations in the standard bitting depths. Still, in every case, Blaze was able to obtain the master-key bitting after only a few minutes of effort.

One design in commercial use does avoid the vulnerability, by using two concentric plugs so that there are two separate points where the pin stack cuts can align to open the lock. (That design, Blaze explains, was developed to allow a richer hierarchy of possible master keys rather than to thwart an attack.) Systems of this type are somewhat more expensive than standard systems, however, and are rarely used in practice. Blaze says that he never encountered locks of this type in his field research.

An Ethical Dilemma

It was immediately clear to Blaze that the vulnerability he had discovered affects a very large number of locks. He thus found himself facing an ethical dilemma: Should he publicize the problem, possibly providing thieves and other mischief makers with a means for causing trouble? Or should he keep the vulnerability secret, despite a significant possibility that it was already being exploited?

The issue has been the subject of a longstanding debate. Many companies prefer to keep the design of their security schemes under wraps, arguing that making the inner workings of a system public just gives a leg up to hackers. Cryptographers, however, tend to deride this notion of "security through obscurity," contending that real security comes only with transparency. The best way to devise a secure system, they argue, is to make the details of the security scheme public and allow the experts to attack it.

In practice, the uneasy compromise has been for security researchers to follow a standard procedure on finding vulnerabilities in commercial software. First, the researcher contacts the company that makes the product and gives it time to produce a patch. Only after the patch is released do the researchers speak freely or publish results on the vulnerability.

In this case, with the security flaw being in a mechanical system, the standard approach didn't make sense. A piece of computer software typically comes from one company; thousands of manufacturers make lock systems, however, so it wasn't clear who should be told. Installing a patch, moreover, takes only a short time, while installing new locks on hundreds of doors is time-consuming and expensive.

"We can't think about disclosing security vulnerabilities in crypto in the same way as for physical systems," Blaze says. "I substantially finished this back in September and thought: Okay, what do I do now?"

He began by preparing a fact sheet, which he sent to law enforcement agencies but wasn't sure where else to send it. Meanwhile, he circulated his findings among his colleagues. As the circle of people in the know inevitably grew larger, John Schwartz, a *New York Times* reporter, eventually got wind of it and Blaze decided to go ahead and publicize the issue.

The master-keyed systems he investigated are "what's done by default and that has to change," Blaze says. "If we had a way of telling only those pure of heart we would do it; the problem is to be able to reach those people we have to tell everybody."

After January 23, when Schwartz's story ran in *The New York Times,* Blaze received dozens of angry phone calls and letters from locksmiths. The letters made the same two points, he said, almost without exception: This is something that all locksmiths are aware of, and it's too dangerous to talk about it.

Beyond the angry locksmiths, however, Blaze says he's gotten a very positive response. Many facility managers told him that they would change the system in their buildings, either to one without master keys or to one in which a single master key gives access to only a few doors.

Most interesting of all was the response of academic computer scientists: "Every time I talked to a group of them," Blaze says, "one person would say that this is how they got a master key to their college dorm."

Overall, Blaze thinks that informing the world about the problem was the right decision. He tells of doing a search on Google after the *Times* story appeared, and finding a news story about a jewel thief who had made a master key to some safe deposit boxes.

"I don't know that he used this exact method, but certainly master keys have been a target of thieves for a long time," he says. "I don't think I'm telling the smart criminals anything they haven't figured out."

Sara Robinson is a freelance writer based in Berkeley, California.