Master-Keyed Lock Vulnerability

Matt Blaze AT&T Labs -- Research

16 January 2003, Revised 27 January 2003

The threat

In a recent research paper, we describe weaknesses in most master-keyed lock systems, such as those used by offices, schools, and businesses as well as by some residential facilities (particularly apartment complexes, dormitories, and condominiums). These weaknesses allow anyone with access to the key to a single lock to create easily the "master" key that opens every lock in the entire system. Creating such a key requires little skill, leaves behind no evidence, and does not entail engaging in recognizably suspicious behavior. The only materials required are a metal file and a small number of blank keys, which for many locks are readily available.

Needless to say, the ability for any keyholder to obtain system-wide access represents a serious potential threat to the security of master keyed installations. Individuals and institutions that depend on such locks to protect their safety and property should be aware of these risks and consider alternatives to eliminate or reduce their exposure to this threat.

Who is vulnerable?

A master keyed lock system is one in which locks are designed not only to be opened by their individual keys, but also by special "master" keys that open some or all other locks in the system. They are commonly found in commercial, industrial, educational and government facilities as well as in some centrally managed residences. Master keying is used because it allows those who must have access to many locks (maintenance workers,

managers, etc.) to carry only a few keys. (Note that master keying is unrelated to whether the locks are sold under the "Master ®" brand name.) It is not usually possible to tell by inspecting a key or a lock from the outside whether it is part of a master system. Individuals should ask their locksmith, building management, or maintenance office whether their locks are master keyed.

This research demonstrates that virtually all master keyed mechanical lock systems are at least theoretically vulnerable; the practical seriousness of the threat to any particular system depends on a number of factors:

- Only master keyed locks are vulnerable to this threat. These techniques are not effective against locks that are not part of a master system.
- In order to make a master key, the attacker must have access to one of the locks in the system and possess or have previously examined its associated key. Any lock and key in the system is sufficient for this purpose, and so any individual who has ever been given access to any key has the potential to carry out the attack. The technique involves a series of simple "probes" of a lock (typically less than fifty) which reveal successively more information about the master key. This can be done in several sessions; continuous access to the lock for an extended period of time is not required.
- The procedure consumes a small number (less than ten) of "blank" keys of the kind that fit the locks. Blank keys for most commonly-used locks are available in small quantities from a wide range of commercial sources. The keys are "cut" using hand-held machines or a small metal file.

Alternatives and countermeasures

Unfortunately, at this time there is no simple or completely effective

countermeasure that prevents exploitation of this vulnerability short of replacing a master keyed system with a non-mastered one. Residential facilities and safety-critical or high-value environments are strongly urged to consider whether the risks of master keying outweigh the convenience benefits in light of this vulnerability. Lock users should evaluate these risks before purchasing or installing new master keyed systems.

Depending on individual circumstances, a range of defenses may be appropriate:

- Eliminate the use of master keying entirely. This is the safest option in most cases. Simple mechanisms such as locked key control cabinets can provide a workable alternative to master keying, especially in smaller-scale environments.
- Use a lock design that is not vulnerable. There are lock designs (including those that use "master rings," those that employ multiple cylinders, and those based on electronic controls) that permit master keying without this vulnerability, but they are not widely used commercially and may not be available for some lock applications.
- Use a lock system for which it is difficult to procure keys. Some locks, particularly those marketed for larger-scale commercial installations, use "restricted" keys, which may make it more difficult for a potential attacker to obtain the correct blanks. However, in practice this may offer only the appearance of protection; many "restricted" blanks are in fact readily available from aftermarket and offshore sources, and even when they are not it is often not difficult to fabricate a working blank directly.
- If master keying must be used, limit the scope of a successful attack by separating different functions into different master systems. For example, instead of having a single master system for an entire organization, use separate master systems for different work groups, floors, etc.

Why is this information being made available?

Since this research was completed last Fall, we have been quietly circulating details of the vulnerability to the lock, law enforcement, and security communities. However, there is some evidence that the details are now circulating in the underground world. At this point we believe that it is no longer possible to keep the vulnerability secret and that more good than harm would now be done by warning the wider community. Several correspondents have noted that this attack, and similar techniques, have been passed down as folklore in both the locksmithing and underground communities.

Click here for an interesting historical viewpoint on the disclosure of security vulnerabilites. For a brief essay on the reaction to this particular vulnerability, click here.

Technical details and resources

The vulnerability was discovered by applying the techniques of cryptanalysis, ordinarily used to break secret codes, to the analysis of mechanical lock design. The research paper describing this analysis and the discovered vulnerability can be found (in PDF format) on the world wide web at http://www.crypto.com/papers/mk.pdf. (Note -- this file is rather large, about 4MB and is not suitable for download over dialup or slow connections). A version of the paper will appear in the IEEE journal *Security and Privacy*.

The author strongly suggests that facility managers and concerned individuals consult with a competent security professional or locksmith to discuss the vulnerability of their particular installations.

Neither the author nor AT&T endorses or recommends specific lock products or security services. However, the following resources and organizations may be helpful for locating an appropriate security

specialist or as a source of technical information:

- Investigative Law Offices, http://www.security.org, has extensive information on the evaluation of physical security systems generally and has a video demonstration of the attack available to qualified security professionals.
- The Associated Locksmiths of America, http://www.aloa.org, is the main trade association for locksmiths and can help locate a locksmith in your area.
- The American Society for Industrial Security, http://www.asisonline.org, is the professional society for industrial security specialists.

This fact sheet will be available on the world wide web at http://www.crypto.com/masterkey.html.