The New York Times

Many Locks All Too Easy To Get Past

By John Schwartz

Jan. 23, 2003

A security researcher has revealed a little-known vulnerability in many locks that lets a person create a copy of the master key for an entire building by starting with any key from that building.

The researcher, Matt Blaze of AT&T Labs-Research, found the vulnerability by applying his area of expertise -- the security flaws that allow hackers to break into computer networks -- to the real-world locks and keys that have been used for more than a century in office buildings, college campuses and some residential complexes.

The attack described by Mr. Blaze, which is known by some locksmiths, leaves no evidence of tampering. It can be used without resorting to removing the lock and taking it apart or other suspicious behavior that can give away ordinary lock pickers.

All that is needed, Mr. Blaze wrote, is access to a key and to the lock that it opens, as well as a small number of uncut key blanks and a tool to cut them to the proper shape. No special skills or tools are required; key-cutting machines costing hundreds of dollars apiece make the task easier, but the same results can be achieved with a simple metal file.

After testing the technique repeatedly against the hardware from major lock companies, Mr. Blaze wrote, ''it required only a few minutes to carry out, even when using a file to cut the keys.''

AT&T decided that the risk of abuse of the information was great, so it has taken the unusual step of posting an alert to law enforcement agencies nationwide. The alert describes the technique and the possible defenses against it, though the company warns that no simple solution exists.

The paper, which Mr. Blaze has submitted for publication in a computer security journal, has troubled security experts who have seen it. Marc Weber Tobias, a locks expert who works as a security consultant to law enforcement agencies, said he was rewriting his police guide to locks and lock-picking because of the paper. He said the technique could open doors worldwide for criminals and terrorists. ''I view the problem as pretty serious,'' he said, adding that the technique was so simple, ''an idiot could do it.''

The technique is not news to locksmiths, said Lloyd Seliber, the head instructor of master-key classes for Schlage, a lock company that is part of Ingersoll-Rand. He said he even taught the technique, which he calls decoding, in his training program for locksmiths.

''This has been true for 150 years,'' Mr. Seliber said.

Variations on the decoding technique have also been mentioned in passing in locksmith trade journals, but usually as a way for locksmiths to replace a lost master key and not as a security risk.

When told that Mr. Seliber taught the technique to his students, Mr. Tobias said: ''He may teach it, but it's new in the security industry. Security managers don't know about it.''

In the paper, Mr. Blaze applies the principles of cryptanalysis, ordinarily used to break secret codes, to the analysis of mechanical lock designs. He describes a logical, deductive approach to learning the shape of a master key by building on clues provided by the key in hand -- an approach that cryptanalysts call an oracle attack. The technique narrows the number of tries that would be necessary to discover a master-key configuration to only dozens of attempts, not the thousands of blind tries that would otherwise be necessary.

The research paper might seem an odd choice of topics for a computer scientist, but Mr. Blaze noted that in his role as a security researcher for AT&T Labs, he examined issues that went to the heart of business security wherever they arose, whether in the digital world or the world of steel and brass.

Since publishing Mr. Blaze's technique could lead to an increase in thefts and other crimes, it presented an ethical quandary for him and for AT&T Labs -- the kind of quandary that must also be confronted whenever new security holes are discovered in computing.

''There's no way to warn the good guys without also alerting the bad guys,'' Mr. Blaze said. ''If there were, then it would be much simpler -- we would just tell the good guys.''

Publishing a paper about vulnerable locks, however, presented greater challenges than a paper on computer flaws.

The Internet makes getting the word out to those who manage computer networks easy, and fixing a computer vulnerability is often as simple as downloading a software patch. Getting word out to the larger, more amorphous world of security officers and locksmiths is a more daunting task, and for the most part, locks must be changed mechanically, one by one.

But Mr. Blaze said the issue of whether to release information about a serious vulnerability almost inevitably came down to a decision in favor of publication.

''The real problem is there's no way of knowing whether the bad guys know about an attack,'' he said, so publication ''puts the good guys and the bad guys on equal footing.''

In this case, the information appears to have made its way already to the computer underground. The AT&T alert to law enforcement officials said that a prepublication version of the paper distributed privately by Mr. Blaze for review last fall had been leaked onto the Internet, though it has not been widely circulated.

''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,'' the company wrote.

There is evidence that others have chanced upon other versions of the technique over the years. Though it does not appear in resources like ''The M.I.T. Guide to Lockpicking,'' a popular text available on the Internet, Mr. Blaze said, ''several of the people I've described this to over the past few months brightened up and said they had come on part of this to make a master key to their college dorm.''

Mr. Blaze acknowledged that he was only the first to publish a detailed look at the security flaw and the technique for exploiting it.

''I don't think I'm the first person to discover this attack, but I do think I'm the first person to work out all the details and write it down,'' he said. ''Burglars are interested in committing burglary, not in publishing results or warning people.''

Mr. Tobias, the author of ''Locks, Safes and Security: An International Police Reference,'' said that the technique was most likely to be used by an insider -- someone with ready access to a key and a lock. But it could also be used, he said, by an outsider who simply went into a building and borrowed the key to a restroom.

He said he had tested Mr. Blaze's technique the way that he tests many of the techniques described in his book: he gave instructions and materials to a 15-year-old in his South Dakota town to try out. The teenager successfully made a master key.

In the alert, AT&T warned, ''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 nonmastered one.''

The letter added, ''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 new vulnerability.''

Other defenses could make it harder to create master keys.

Mr. Blaze said that owners of master-key systems could move to the less popular master-ring system, which allows a master key to operate the tumblers in a way that is not related to the individual keys. But that system has problems of its own, security experts say.

Mr. Blaze suggested that creating a fake master key could also be made more difficult by using locks for which key blanks are difficult to get, though even those blanks can be bought in many hardware stores and through the Internet.

But few institutions want to spend the money for robust security, said Mr. Seliber of Schlage. His company recommends to architects and builders that they take steps like those recommended by Mr. Blaze, measures that make it more difficult to cut extra keys -- like using systems that are protected by patents because their key blanks are somewhat harder to buy, Mr. Seliber said. Even though such measures would add only 1 to 2 percent to the cost of each door, builders were often told to take a cheaper route. He said that they were told, '' 'We're not worried about ninjas rappelling in from the roof stuff -- take it easy.' ''

That is not news to Mr. Blaze, who said it was also a familiar refrain in the world of computer security. ''As any computer security person knows,'' he said, ''in a battle between convenience and security, convenience has a way of winning.''