

The Rise of the Analog Hacker: A New Physical Security Concern

By Leonard Gallion

A New Kind Of Hacker

You have been working night and day securing your network. Multiple electronic layers of defense, including firewalls, antivirus software, application gateways and intrusion detection systems stand ready to meet any computer-based attack. However, what if a malicious hacker was able to walk into your server room anytime they wanted? Would you still be so confident your network is secure?

While electronic defense is a critical part of any I.T. infrastructure, the foundation of all security starts in the physical realm. Without the ability to control access to your hardware, your information can be stolen, corrupted or even destroyed despite any number of electronic countermeasures. Of course, most I.T. security managers realize this danger and place their hardware behind locked doors and their offline data in vaults.

What most security experts are not aware of, however, is the emergence of a new kind of hacker. Like traditional computer hackers, this hacking community strives to learn everything they can about complex devices and then devise ways to exploit weaknesses in these systems. The machines they hack are not digital, however, but analog devices such as locks and safes. These Analog Hackers are driven by the thrill of solving the mechanical puzzle that secured enclosures represent.

The New Reality

For centuries the locksmithing community had closely guarded all information about locks and the techniques to open them. Traditionally the only way to obtain this knowledge was to spend years as a journeyman working under a master locksmith. The arrival of the Internet, however, changed everything. Once information about a lock or an opening technique was leaked to the Net, it instantly became accessible to anyone with access to a search engine. This data was then gathered and distilled by the Analog Hacker community until, within just a few years, it had effectively demolished hundreds of years of "security by obscurity" in the locksmithing industry. Now, long-hidden techniques such as lock picking, latch slipping, bypass techniques, impressioning, bumping, and safe manipulation are documented on the Internet for anyone to access.

The Analog Hacking Community

Like their digital cousins, Analog Hackers need to be able to easily gain basic knowledge about their kind of hacking, access the proper tools to perform it, and communicate with other, like-minded people in order to build their collective knowledge. All of these elements are in place in the Analog Hacking community today.

Many Analog Hackers start their journey by discovering the free, online document—"The MIT Guide To Lock Picking." This thorough tutorial (complete with illustrations) covers all of the basics a beginning lock picker needs to get started. In addition, various books on lock picking are also available from any major retailer, including the *Visual Guide To Lock Picking* by Mark McCloud, *Secrets of Lock Picking* by Steven Hampton, and *Steel Bolt Hacking* by Douglas Chick.

Contrary to popular belief, lock picking tools are generally not illegal to own and are readily available from dozens of firms selling over the Internet. In fact, you can probably find them at your local 'spy shop' in a nearby strip mall. Purchasing picks is also not the only option for the more mechanically inclined. Picking tools are easy to make using a wheel grinder and some basic raw materials, such as hacksaw blades, windshield wiper parts, or street sweeper bristles. As usual, written instructions and hands-on videos are available on the Internet to help the do-it-yourself pick maker.

Finally Analog Hackers need a place to meet so they can swap ideas and information. One of the largest places on the Internet to do this is LockPicking101.com. Boasting over 10,000 members, it is the definitive place for beginning (and more experienced) lock pickers to share their knowledge. In fact, some of the members of LockPicking101 are practicing locksmiths who, despite the ire from others in their profession, guide aspiring pickers into the sport of lock picking, and sometimes the profession itself.

Lock Picking Is A Sport?

Although not widely known, lock picking is considered both a hobby and a sport by thousands of non-locksmiths around the world. Organizations such as TOOOL (Netherlands), Sportsfreunde der Sperrtechnik (Germany) and LockSports International (Canada) have hundreds of dues paying members who attend regular meetings, hold membership cards, and participate in lock picking competitions. Aware of the public concern amateur lock picking could cause, all of these organizations have a strong, written code of conduct that limits their members to only picking locks they have permission to open.

Manned by active hobbyists, these organizations explore how locks work, devise improved opening techniques, and regularly see which members can open the most difficult locks in the shortest period of time. To further show off their lock opening abilities, some members not only pick at local competitions, but also participate in various international events. Two of the more popular of these are LPCon and The Dutch Open.

LPCon, now in its third year, is held annually at Defcon in Las Vegas. This year's event featured sixty-seven contestants participating in a two-day

tournament. The winner this time around was 'Gandolf,' who managed to open his final lock in just six seconds. At the same time across the Atlantic, the Dutch Open was being held. Sponsored by TOOOL, this four-year-old event was held at the What-The-Hack conference in Liempde Netherlands. As usual, the Dutch Open featured its normal contingent of extremely strong Dutch and German pickers, who are generally considered the best amateurs in the world. This year's Open champion was Dr. Torsten Quast, a research scientist from Berlin. In 2004 he also won a prestigious lock opening competition in Germany.

Is Analog Hacking Just Lock Picking?

Although lock picking is by far the most popular form of Analog Hacking, a growing number of people are becoming interested in defeating other areas of physical security, including biometric devices and safe locks. One of the most important works released in this area has been Matt Blaze's paper entitled, "Safecracking for the Computer Scientist." This document, available from his Web site at www.crypto.com, disclosed many of the secrets of safe manipulation. Manipulation, once known to only a handful of safe technicians, allows you to determine the combination of a safe by using the dial to chart small variations within the lock mechanism. Although a difficult skill to master, many amateur manipulators have already started purchasing surplus locks from eBay™ in order to start learning the technique.

The Changing Security Landscape

Historically, physical security vendors have not always responded quickly when flaws in their products have been discovered. For instance, for years a popular brand of home door lock was sold in America with a serious security flaw. The entire lock could easily be pulled out of the door just by using a special key and a wooden stick as a lever. Of course, locksmiths knew about this flaw and regularly used this technique when called out to people's homes. However, the public was rarely told about the security problems of these locks and today millions are still on doors across the country.

While "security by obscurity" had served lock manufacturers and the locksmithing industry well for many years, it also left the end users of their products vulnerable if persons with less than honorable motives discover this information. Today's security managers need to realize it is generally just a matter of time before these sorts of vulnerabilities are discovered by Analog Hackers and released to the Internet. One recent example of this was the publication of the "minimal movement bumping technique" by Barry Wels and Rop Gonggrijp of the TOOOL locksports group. Release of this vulnerability caused a significant public outcry when a Dutch TV station did an expose on the subject. In the program it was demonstrated that a specially cut key could, when inserted in the lock and stuck by a small hammer, open almost any door lock sold in the Netherlands. Once publicized, several lock manufacturers in Europe responded by releasing new, bump-resistant locks. In addition, many firms asked the TOOOL group to test the changes they made in order to make certain the new locks were really secure. Unfortunately for the rest of the world, this major vulnerability has gone unrecognized by other lock manufacturers, even though their products are also vulnerable.

The Danger of Non-Destructive Entry

Although groups such as TOOOL, Sportsfreunde der Sperrtechnik and Locksports International stress ethical conduct by their members, it can't be ignored that many non-destructive opening techniques (such as bumping, lock picking and safe manipulation) are no longer strictly held in the

domain of the security industry. This is a particularly dangerous situation, since non-destructive entry leaves no sign of attack, and thus, defeats one of the critical features of any lock—intrusion detection.


Common burglars, only interested in obtaining hard merchandise they can resell, have little use for non-destructive techniques. For them, it is pointless to try to hide the method of entry when the loss of physical goods is often immediately detectable by the owner. However, when data is the target, non-destructive entry can be of great value to the thief. Since there are no obvious signs of intrusion, data can often be subverted, copied or removed with the victim being completely ignorant of this fact. For example, if the door to your server room has been kicked in and a backup tape is missing, it is immediately apparent you have had data stolen and remediation steps can begin. However, if the break-in is not detected for weeks (or months) because everyone assumes the tape was simply misplaced, then critical evidence may be destroyed and any chance to limit the damage from the theft (such as canceling stolen credit card numbers) may be lost forever.

Physical Security For The Computer Scientist

Having a good physical security plan is just as critical as electronic countermeasures for maintaining the safety and integrity of your data. Because of this, I.T. security professionals need to work closely with their physical security counterparts in order to make certain that I.T. assets are properly secured.

As with I.T. security, a layered defense is a must for any successful physical security plan. Never rely on a single point of failure, such as an isolated lock, to defend a critical asset or its data. Instead, deploy multiple resources, such as video surveillance cameras, guards and alarms, to reduce the chances an attacker will be able to reach a valuable target undetected. Physical security practitioners may also not realize where critical I.T. resources are located. For instance, sometimes gaining access to a wiring closet is just as effective as entering the actual server room from a data theft standpoint. Therefore, it is vital that you view your physical infrastructure from an attacker's standpoint and defend it accordingly.

Conclusion

The potential threat posed by rouge members of the Analog Hacking community should not be ignored. It is also important to recognize that there is a heavy overlap between the computer and analog hacking communities. This means that your adversary may be well versed in both physical and electronic security countermeasures. This makes it even more critical that Analog Hackers and their techniques are factored into your overall security plan. 

Leonard Gallion, CISSP, is the Vice President of Information Services for a Dallas-based company. He is also a security consultant.