

Viewpoint Paper

The Hobbyist Phenomenon in Physical Security*

Eric C. Michaud
Vulnerability Assessment Team
Argonne National Laboratory
emichaud@anl.gov

Pro-Ams (professional amateurs) are groups of people who work on a problem as amateurs or unpaid persons in a given field at professional levels of competence. Astronomy is a good example of Pro-Am activity. At Galaxy Zoo [1], Pro-Ams evaluate data generated by professional observatories and are able to evaluate the millions of galaxies that have been observed but not classified, and report their findings at professional levels for fun. To allow the archiving of millions of galaxies that have been observed but not classified, the website has been engineered so that the public can view and classify galaxies even if they are not professional astronomers. In this endeavor, it has been found that amateurs can easily outperform automated vision systems.

Today in the world of physical security, Pro-Ams are playing an ever-increasing role. Traditionally, locksmiths, corporations, and government organizations have been largely responsible for developing standards, uncovering vulnerabilities, and devising best security practices. Increasingly, however, non-profit sporting organizations and clubs are doing this. They can be found all over the world, from Europe to the US and now South East Asia. Examples include TOOOL (The Open Organization of Lockpickers), the Longhorn Lockpicking Club, Sportsfreunde der Sperrtechnik – Deutschland e.V., though there are many others. Members of these groups have been getting together weekly to discuss many elements of security, with some groups specializing in specific areas of security. When members are asked why they participate in these hobbyist groups, they usually reply (with gusto) that they do it for fun, and that they view defeating locks and other security devices as an interesting and entertaining puzzle.

A lot of what happens at these clubs would not be possible if it weren't for "Super Abundance", the ability to easily acquire (at little or no cost) the products, security tools, technologies, and intellectual resources traditionally limited to corporations, government organizations, or wealthy individuals. With this new access comes new discoveries. For example, hobbyist sport lockpicking groups discovered—and publicized—a number of new vulnerabilities between 2004 and 2009 that resulted in the majority of high-security lock manufacturers having to make changes and improvements to their products. A decade ago, amateur physical security discoveries were rare, at least those discussed publicly. In the interim, Internet sites such as lockpicking.org, lockpicking101.com and others have provided an online meeting place for people to trade tips, find friends with similar interests, and develop tools.

*Editor's Note: This paper was not peer reviewed.

The open, public discussion of software vulnerabilities, in contrast, has been going on for a long time. These two industries, physical security and software, have very different upgrade mechanisms. With software, a patch can typically be deployed quickly to fix a serious vulnerability, whereas a hardware fix for a physical security device or system can take upwards of months to implement in the field, especially if (as is often the case) hardware integrators are involved.

Even when responding to publicly announced security vulnerabilities, manufacturers of physical security devices such as locks, intrusion detectors, or access control devices rarely view hobbyists as a positive resource. This is most unfortunate.

In the field of software, it is common to speak of Open Source versus Closed Source. An Open Source software company may choose to distribute their software with a particular license, and give it away openly, with full details and all the lines of source code made available. Linux is a very popular example of this. A Close Source company, in contrast, chooses not to reveal its source code and will license its software products in a restrictive manor. Slowly, the idea of Open Source is now coming to the world of physical security. In the case of locks, it provides an alternative to the traditional Closed Source world of locksmiths.

Now locks are physical objects, and can therefore be disassembled. As such, they have always been Open Source in a limited sense. Secrecy, in fact, is very difficult to maintain for a lock that is widely distributed. Having direct access to the lock design provides the hobbyist with a very open environment for finding security flaws, even if the lock manufacturer attempts to follow a Close Source model.

It is clear that the field of physical security is going the digital route with companies such as Medeco, Mul-T-Lock, and Abloy manufacturing electromechanical locks. Various companies have already begun to add microcontrollers, cryptographic chip sets, solid-state sensors, and a number of other high-tech improvements to their product lineup in an effort to thwart people from defeating their security products. In my view, this is a somewhat dangerous development because many physical security companies are not holding themselves to the same standards and sophistication as companies in, for example, the software or casino industries. It is irresponsible, in my view, for a manufacturer or vendor to label a product is “secure” solely because there are billions of possible digital combinations, particularly when there are examples of software being used by an adversary to try all possible combinations.[2]

I would like to see manufacturers of physical security products and Pro-Ams groups come to some agreed upon mechanism for the latter to disclose security vulnerabilities to the former. Essential in any such mechanism is the need to avoid shooting the messenger, threatening researchers or hobbyists, or suing anybody when vulnerabilities are discovered. It is essential for manufacturers to take the vulnerabilities seriously, and fix the issues that can be readily mitigated. Manufacturers and Pro-Ams should not be at odds with each other, but should instead work together to improve security.

Considering that there is surprisingly little extensive research and development in the physical security field, even less imaginative testing, and a lack of effective vulnerability assessments for physical security products, the industry leaders need to take a proactive step forward. Manufacturers need to stop ignoring security experts (Pro-Ams or otherwise) when designing new products and

evaluating current ones. Critical, knowledgeable input is especially important when physical security products are in their infancy, and crucial changes can be easily implemented. Effective use of Pro-Ams will prove to be essential in the upcoming years as cutting edge technologies continue to be implemented in new security products while also becoming more and more accessible to the general public. Indeed, a good first step can be seen in the open letter Peter Fields of Medeco wrote to the locksmith community magazine Non-Destructive Entry.[3]

References

1. “Galaxy Zoo”, http://en.wikipedia.org/wiki/Galaxy_Zoo
2. Richard Clayton, “Brute Force Attacks on Cryptographic Keys”, <http://www.cl.cam.ac.uk/users/rnc1/brute.html>
3. Peter Field, “An Open Letter to the Sport Lock-Picking Community”, Non-Destructive Entry, <http://ndemag.com/nde3.html>