Security Advice That Can Be Followed

My youngest child entered college this fall. During orientation, parents were advised by the school’s medical director that prescription medications should be kept locked in the student’s room. As a security person, this seemed straightforward, so I set out to help my daughter comply.

First, I asked the medical director for recommendations for secure storage—and was surprised that she had no recommendations, despite this being part of the normal parent presentation. So I asked about the threat model: Should we be concerned about theft by a roommate, someone down the hall, someone from the college but not nearby, or someone from outside the college? How much time and expertise might they have? What might their goals be in stealing medication? In each case, I basically came up blank. Had I not been a security engineer, I would have given up at this point and told my daughter to hide her medications in her sock drawer (that is, security through obscurity)—which was in fact her doctor’s recommendation.

So I made up a threat model: someone outside her dorm community who could get access to her room unobserved, but probably not for an extended period of time, and with some level of experience, but not anything approaching a safecracker. I assumed that the goal of the attacker was theft, not tampering, and that ex post facto detection wasn’t a major concern to the attacker. And I hoped that walking away with the storage unit was too obvious, so I assumed that the thief would prefer to get into the storage without stealing it intact—but I was less confident of this assumption.

Next came the goal of finding a suitable container. I looked online at safes (Amazon as well as safe companies) and found that although plenty of safes are being sold, and many are rated for how long they will withstand fire, there doesn’t seem to be any rating for home-level safes against an adversary (or what sort of adversary). Some advertisements brag about the number of digits in the door code while, at the same time, advertising emergency override mechanisms. According to customer reviews, many can be trivially opened with a screwdriver, or by dropping them or hitting them with a hammer. Sad to say, Consumer Reports doesn’t rate safes the way they rate cars or dishwashers. I consulted with colleagues, including a couple who are cybersecurity experts who play with locks, and concluded that a keypad was probably better than a keylock (because all keys from a safe vendor are likely to be the same), although determining the quality of the lock was seemingly impossible if I relied on vague vendor claims. I found nothing about resistance of any of the locks to electronic manipulation. I read many online reviews, and looked at pistol cases, thinking that those might be more regulated because they’re used to protect firearms. (Spoiler alert: they’re not. And the thought of having something in her dorm room that looked like it might be used for firearms made my daughter nervous—both because the school housing office would certainly not approve a weapon, even if it wasn’t there, and because it might increase the risk to her if someone thought it did contain a weapon.) The more I read, the less I believed anything I saw, so I consulted with a professional safe company that installs safes for companies. It had nothing at the home level to offer—its cheapest model was about $500—but it suggested two companies that were “less bad.”

Returning to Amazon to examine those two companies’ products in more depth, I found that the reviews suggested that home safes might only be reasonably useful to protect against theft if they’re bolted to a wall or floor—not exactly something colleges encourage in dorms where putting a thumbtack in the wall is a violation of the housing

Jeremy Epstein
Associate Editor in Chief
contract. I finally selected one and ordered it, only to find that, as an override in case the owner forgets the keypad combination, it can be opened with a key, which is most probably the same for every safe of that model. My threat model assumed someone having to break into the safe while in the room (as opposed to stealing the safe and having the time to manipulate it in a workshop). As a countermeasure, I thought of using a steel cable to connect the safe to a water pipe in the dorm room, but this was foiled by both the lack of such a pipe and the fact that the safe didn’t have holes designed to thread a cable for such a connection.

Having concluded that there was no good solution, I kept the safe I had purchased. Perhaps it doesn’t need to be secure, only more secure than the protection for medication in the next dorm room. Or is having a safe itself a signal to a potential thief, and therefore increasing the risk? Would putting a sign on the safe “contains only medication” be an incentive or a disincentive to a thief? What would the tradeoffs be of having a camera that would take a picture of a thief? (Almost certainly negative, given the privacy concerns of having a camera in a dorm room!) Should she keep some small backup amount of medication hidden in her sock drawer, in case the safe is compromised (or the lock fails)?

(As I wrote this column, I learned that Underwriters Laboratories [UL] provides some level of home safe testing, and their standard was revised in 2016 to offer a three-tiered Residential Security Container certification. However, finding products that meet this standard isn’t easy, and I’m unconvinced that it’s adequate for the threat model. One critique notes “The [older, single-tier] RSC certification requires that [the safe] block access for five minutes using a pry bar less than 18 inches long and a hammer weighing less than three pounds,” which is a fairly minimal level of protection, although perhaps adequate for a dorm room. It was unclear to me from the UL website or other sites whether the certification includes an examination of locks and keys. I was unable to find a safe that complied with even that standard for less than about $1,000, nor one small enough for a dorm room.)

Mapping the above description to the information security world is easy. We tell consumers and businesses to use many types of security software but give them minimal guidance regarding what to pick. We don’t help them understand threat models (which will differ for an individual versus a company, and might include or exclude insider threats such as the roommate). Although some ratings are available for some classes of security software, those ratings aren’t meaningfully understandable by consumers. There’s certainly no clear correlation between price and protection. We don’t have a way to rate how usable the security is (is a key easier or harder than a keycode?) — and how hard it is to bypass. It’s impossible for a buyer to determine if there’s a master key, as appears to be the case for the safe I bought, that subverts the controls.

Most home computer users therefore throw up their hands—the equivalent of putting the medications in the sock drawer. They might install an antivirus program, but have no understanding that such programs are woefully ineffective against modern threats.

We routinely tell users not to write down their passwords, but we know that leads to weak (and reused) passwords—using a password manager is in some respects the equivalent of keeping a small amount of medication outside the safe in case the safe is compromised, or keeping a backup key to the safe.

Small businesses are perhaps most at risk, because they have assets that are valuable to an adversary, but minimal skills or funds to figure out what’s really needed.

Perhaps most relevant for the discussion of safes that opened this column, the Internet of Things introduces dramatically greater risks to individuals from information security threats. Flaws in door locks and home cameras have increased risks to individuals, rather than reducing the risks as was intended by the security devices. Would I have been more comfortable with a safe with remote monitoring capabilities, or would that have increased the risks in other ways?

This is, of course, not a new problem. Security engineers and scientists have been trying to measure security for decades. Government efforts in the 1980s such as the US “Orange Book” (Trusted Computer Systems Evaluation Criteria) and European and international successors were explicitly trying to measure security. Documents offered government users ways to determine what level of security is needed for various broadly drawn classes of systems, but such controls need constant updating to account for the changing threat landscape. NIST 800 series publications aim to provide guidelines,
but require too much expertise to be usable by individuals or small businesses. Private sector companies have tried ratings (for instance, Verizon’s ICSA Labs), but these haven’t been widely recognized.

The situation isn’t entirely dire, however. Over the past few years, Consumer Reports has put significant energy into educating the general public about computer security technology (although not home safes, as noted above). UL offers security testing services, although consumers (and businesses) haven’t yet come to rely on the UL logo as a meaningful assurance for software-based systems.

For now, my daughter’s medication is locked up in her room—and I’m hoping that the security by obscurity of having the safe in her closet, coupled with some level of protection provided by the lock, and perhaps an overly pessimistic threat model, is sufficient to keep her medications safe from theft.

Acknowledgments
Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

IEEE Software seeks practical, readable articles that will appeal to experts and nonexperts alike. The magazine aims to deliver reliable, useful, leading-edge information to software developers, engineers, and managers to help them stay on top of rapid technology change. Topics include requirements, design, construction, tools, project management, process improvement, maintenance, testing, education and training, quality, standards, and more. Submissions must be original and no more than 4,700 words, including 200 words for each table and figure.

Author guidelines: www.computer.org/software/author.htm
Further details: software@computer.org
www.computer.org/software