



Your locks are lame and easily picked: notes on the first layer of your physical security

By: Dave Chappelle

October 27, 2010 |  [What's this](#)



[SecTor](#) attendees were treated to lock-picking lessons, and given the opportunity to try their hands at the part of physical security that many IT managers seldom consider.

At first thought, you might think locks are the physical counterpart of passwords. Both protect access to something. Both come in different strength levels.

Security analyst and member of TOOOL [Deviant Ollam](#) says locks are not like passwords.

Making locks like passwords doesn't work in the physical world. Making them longer only makes locks bigger. The door has to be thicker, and the key will be like a sword hanging around your neck.

You can attack a lock one pin, or aspect of the password, at a time. With gentle turning pressure using a turning tool, you can get a pin to bind in the up position while you "attack" the rest.

Lock manufacturing practices determine lock quality. Imperfections in pins and plugs result in misalignments that while never intended, are unique. Lock-pickers exploit those misalignments.

Often the more a lock is rated for ruggedized performance, and weather, the easier it is to pick. For example Master tests well in overuse cycle tests and brute force resistance. Perhaps you remember the old commercial in which a rifle bullet penetrates a Master padlock, and it remains locked.

Other methods include key bumping... in which you use the principals best visualized as croquet or billiard balls to slam the pins out of the way and turn the lock cylinder. Or the use of shims to open combination padlocks.

Deviant's Four Types of Locks:

1. Basic "anybody pickable" locks.

2. Pick-resistant locks slow down skilled persons
3. High security locks require lots of time by very skilled attackers.
4. So-called un-pickable locks not many can get into. Locksmiths are the best place to get good high security locks.

Dollar and convenience stores are the best places to get crummy locks. But you don't want those.

Amongst lousy locks, Deviant feels wafer locks are the worst.

“Desk drawers are “protected” with wafer locks... every power panel is a wafer lock. How is your UPS protected? It doesn't take a lot of skill to wreck a company's day.”

Electrical rooms are notorious for lousy locks, because all of the panels inside have them, so the contractor often feels a secure lock to the room door isn't required. Two layers of bad security is still bad security.

Why do these bad locks exist? Why do we use them? Standards don't replicate real world attacks.

“A bump attack is either going to work or it's not. A manufacturer can claim its lock is 15-minutes bump resistant, but really the only 15-minute bump attack is the one in which you left your bump key in the car.”

A lock with a crooked keyway indicates tighter milling and machining tolerances. Spool pins and mushroom pins take more time to pick. They're still pick-able with more time and finesse.

Secure level three locks need different tools and techniques. You're not going to be able to pick one with a couple of tools and a weekend course. It slows conventional tools and techniques.

Deviant's fourth category is any lock with no known pick. Abloy Protec... Milwa... Evva MCS that use magnets instead of pins. “That's possibly the most duplication-resistant lock. I can issue this key to anyone, and ask for it back months later, without worrying that an employee has copied it. Why?

Because there is only one machine in Vienna that makes those keys.

Safes are rated much better than locks. They can be compromised via cutting or mechanical bypass – robot dialers that try every combination. Good safes are protected against electronic safe dialers. If you dial it 16,17,18,19 it'll jump or slow, so if someone is looking over your shoulder or through a spycam, it changes to another number. Some will shut down when the dial is rotated more than a full turn, because a human hand can't do that without stopping. The safe lock “knows” a robotic dialer is at work.

Deviant is a colorful character. Among his numerous memorable quotes:

“Nobody wants to pick a lock to get into your house. There’s lots of glass in your windows that’s much easier to break. Me, I have a dog and a shotgun for that. “

“What good is a hundred dollar lock on a ten dollar door?”

“I’ve never worked for any of the companies I praise, nor have I been fired by those I slam.”

“If I were a crazy policy guy, I’d say there are three types of access in your facility—Internal, External, and Sensitive.

Internal is for anybody inside. Internal doors require security level 2 locks.

External is for who goes where. External doors require high security, level 3 locks.

Sensitive is termination-worth data. Put un-pickable locks on your sensitive data.

“Get a policy of ‘no basic locks’. The most basic locks you can find aren’t going to protect you. Bumping, shimmying, zero-skill attack level locks are no good. Your security is worth a \$70 locks. Take wafer locks out of people’s desks. Shitty locks create a false sense of security. There is a cross contamination effect. “

“For example, on one audit we found a padlock holding a chain across the entrance to an empty parking lot. I understand why. Somebody told Jim from Plant Ops to go buy a lock. Jim doesn’t buy the lock, because he buys packs of cheap locks. As long as there’s no policy of ‘no crappy locks’ then Jim keeps putting locks from the multiple purchase everywhere. I’ve seen a seven dollar lock used to secure a truck worth tens of thousands of dollars. Get them out of your company.”

Manufacturers:

Unpickable: Abloy, Evva, Mul-T-Lock, Kabamas (electronic safe dials)

High security: Abus, Assa, Evva, Schlage

Resistant: American, Best

How to social engineer your way into any facility:

You and friends/co-conspirators call the company every day for a week. Act like angry customers “I’ll never buy your stuff again...” “You people have done this for the last...” and always hang up the phone mid-sentence.

After a week of this, walk in wearing a 20-year-old AT&T ID badge, and ask “Have you been having trouble with your phone lines?” They’ll let you right in.

How to motivate your staff to prevent social engineering attacks:

Tell them about Stop-Challenge-Authenticate and follow it up with a reward. They’re going to ignore it unless you reward. They won’t want to act nasty towards strangers. So tell your staff... “In the next six months someone is going to be here who isn’t supposed to be. You find that person, you get steak dinner on us.”

For more info see <http://Deviating.net/lockpicking> and TOOOL