ELECTRONOTES

WEBNOTE 30 2/10/2016

ENWN-30

MISPLACED SECURITY

Passwords and Combinations

-by Bernie Hutchins, February 2016

Click if You Have Forgotten Your Password:

I wonder if most people's experience with passwords is the same as mine. The general concept is simple enough. But all of us likely disobey the recommendations and/or just mess things up. We are told to use "strong" passwords, different ones for different accounts, don't write them down where anyone can find your crib, and change them frequently. Good advice? Possibly also a recipe for locking yourself out. In fact, a lot of folks would probably prefer to never change passwords, use only one or two, something easy to remember (weak), and write them near our computers. We dread the instruction that forces us to change to a more secure password by making it longer; and/or using different cases, numbers, and symbols. We change it where we are forced to, and leave the rest alone. For the most part, this probably makes us reactive and short sighted.

About 6 months ago when I was sick with Lyme disease (a sometimes nasty bacteria vectored by an equally nasty "deer tick" transported by deer, chipmunks, white-footed mice, etc.) and was in the hospital, my daughter was kind enough to watch over my online accounts. I told her the user names and passwords I could remember. Some of them I misremembered. She got into all the accounts, and everyone here probably knows how. She simply pretended to be me and checked the "Forgot Your Password" box. The instructions for resetting the password came to the email address on file, and she entered

the reset code provided and answered “security questions” (like dog’s name!) and set a new password. In fact, I had done the same thing myself, as myself, at least several times. That box seems very handy; virtually essential.

A couple of things pop to mind. In modifying a “weak” password to make it stronger (a process that often indirectly gets us into trouble) we make it more probable we lock ourselves out. And the reset procedure is less than the original strength (even your dog knows his own name!). The kid riding by on his bike knows the dogs name as he hears him being called. Perhaps you should lie to the secure site and say your dog “Spot” is named “Stravinsky”. But then you have to remember that false information. Likewise, it would seem possible that someone could guess or research the other security answers.

All and all it seems unlikely that this reset is, prima fascia at least, a serious vulnerability. It’s a good enough system.

How Secure is a Lock?

Drop back 47 years or so and I was in an Army classroom being caught “counter-intelligence”. I somehow ended up enlisted as a trainable “Special Agent” in Army Intelligence. It was mostly very boring. I got there in large part by chance – you needed a college degree and to be able to pass the security clearance. The class work was very easy (after Cornell engineering – I suppose) and the reward for being in the top 10% or so was two promotion grades (E3 to E5, or PFC to 3-stripe “buck” Sergeant). The school was a good assignment and a lot more enjoyable than Basic Training.

In the instance, there was an instructor (E6 or 4-stripe Staff Sergeant) who was teaching a unit as part of the Physical Security part of our training. He had wheeled in a Tea-Cart which had on it a collection of I guess 100 padlocks. These he told us offered very little security, and as he lectured, he opened the locks one by one in sequence. No keys, nothing that even looked like lock picks, or even anything that resembled lock picking (as most people understand it). His sophisticated “tools” looked like bent paper clips or slivers of band-metal. Some locks took him two full seconds – most he barely touched. By the time he finished the last one, he was saying that all these locks amounted to were invitations for the honest person to stay out – at best a delay of an intruder. All of us had these sorts of locks on our lockers in the barracks.

This was interesting. As a recent engineering student, I was perhaps expecting a detailed set of instructions and likely a “lab”. But this was the lesson in total. Soon thereafter I did learn how to pick locks (many of them at least). My instructor was a fellow student (and friend named Rich), who happened to be a U.S. Marine PFC. Our class was

mainly U.S. Army types, but the training was cross-branch enough that we also had some Marines (reservists who also had degrees).

I knew that the Staff-Sergeant had “bypassed” any picking of the lock tumblers; basically he had reached in through the key slot and triggered the “dog” to snap and release the shackle. Each padlock is different. I guess you learn each type by experiment, or definitively by taking each type apart. But it was a one-second operation if you knew your stuff. I had no such ambitions.

“Picking” a pin-tumbler lock (the usual kind) is more generic, and takes longer. Perhaps as little as 5 seconds, typically 20 seconds, and perhaps forever to complete. [Some better quality locks (at least $40), particularly those with two-sided keys (identical profiles or not) are much more difficult.] To pick a lock, you need two tools: a “tension-bar” and a so-called pick or rake. These can be made (but avoid carrying them as they may be considered burglar tools!) or in a pinch, a small screwdriver and a unbent paper clip may do. A serviceable tension bar can be made from band-metal (the black metal bands that secures wooden packing crates). A width of 3/8 inches to 1/2 inch and perhaps 1.5 inches long will work. This you cut down the centerline stopping perhaps 1/8 inch from the end, and then cut that portion free leaving an L. The width should be slightly larger than the width of a typical key slot. You need to be able to hold the lock in one hand with the tab of the tension bar in the key slot exerting a slight tension. Then you insert your rake in the slot and lightly run it over the tops of the tumblers. This is a bit random, but you will generally cause tumblers to pass up or down and occasionally get stuck on the edge of their slot. Often the whole cylinder just smoothly releases, and the tension bar then acts to rotate it much as a key would. You need to practice, and not be afraid to release the tension (hearing the tumblers all click back!) and start over. Sometime you just miss.

Have I given Lesson 1 in becoming a burglar? Hardly. For one thing, there are many videos on the web that tell you all this and much more. For another, picking is useful when you want to save the lock – if you just want in, use a bolt cutter – buy a new padlock. If it’s a door lock, you have more incentive to avoid destruction such as drilling (a burglar would not hesitate to break a window or use a hammer or pry-bar). The Good Sumerian is helping a neighbor who foolishly locked himself out.

Rich taught me how to pick the simple types of padlocks we all had, and I practiced. Soon it became widely known that Rich or I could pick these locks. Were we considered suspect. We were not. Why? Picture the scenario where it’s morning wake-up and a poor guy has just returned from the shower and found his locker locked and that he has forgotten his key (usually you put it on the chain with your dog tags). You are the proud possessor or a towel, and 10 minutes time before muster. You scream for Rich or Bernie. We probably had one or two customers every week.

Misplaced Security

In this note, the phrase “Misplaced Security” has two meanings. There was first the notion that a password (or combination, or key) has been lost – thus misplaced. In the second sense, there is the view that an ordinary padlock is easy to get through (likewise the relatively easy recovery of a password). That is – what we would usually term a “false sense of security”. This is not new, nor at all restricted to the examples already given. For example, a thief might come to your front door and contemplate trying to pick the entry lock, or perhaps to look under the doormat for the spare key. Or perhaps he might just pick up a rock and smash one of the window “sidelights” by the door and reach through and twist the knob.

Locks are in many ways different from passwords. With regard to improving the security of passwords, one thing that unnerves us is the issue discussed above that, as we improve the password strength, (over which we have this uneasy control), we may be inconveniencing ourselves into being locked out. Another adjacent issue is that the account user has very little knowledge of or control over the cyber-security. On the other hand, we usually can think of several or many ways to improve physical security. We can buy better locks, use alarms, install thick Plexiglas over entry door sidelights, or get a ferocious dog. And as they say in the commercials, you just need to add something to get the criminal to move on to your easier neighbor!

Document Security

A good part of what I was involved with in Army Counterintelligence was “document security.” That is, certain documents (most of our own) were “classified” (such as Confidential, Secret, and Top Secret, among others). Most everything we generated was assumed to be Secret, although eventually stamped as Confidential. [I never handled a Top Secret document myself. The only single item of Top Secret information I ever “had” was whispered directly into my ear!] Being the security experts or “spooks” we of course had <u>mostly</u> sensitive papers, and we wrote most of them. In contrast, a more typical Army unit had less classified material overall and generated very little themselves. They might write occasional routine reports, but their usual classified items were more like manuals, encryption keys, or instructions. That is, the individual units were generally <u>consumers</u>.

In order to even glance at a classified document or item you needed two things. Obviously, you needed a “security clearance.” This meant that some folks (meaning – Army Counterintelligence) went around looking for dirt. With the “subjects” permission, we went around checking all the items you filled in on an application, and the references (persons) who you provided. As you would expect, the friends whose names you gave us generally thought you were above reproach. So we had to keep going – digging up our

own sources. Clearly not a perfect system. Then, suppose you are cleared for Secret. Do you then run down to the safe and rummage through all the Secret documents. Of course you don't. In addition to a clearance, you had to have a "need to know" which is a self-explanatory term. This was more restrictive than a clearance. But it did rely on some one person refusing to grant access to a second person, not unusually refusing the access to a superior in the hierarchy, making for some interesting and courageous incidents.

What is the danger in having a classified document go "wild." It varies immensely. There are many different circumstances, but central to evaluating any loss is the information that can no longer be assumed to be restricted. (Almost always, there is no monetary issue at all – in fact it is a violation to keep valuable property such as cash in a safe intended for secure materials – so as not to temp ordinary thieves). There are cases where the loss of a document (like plans for an A-bomb!) would be a disaster. At other times, disclosure of yesterday's password challenge and responses would not be as serious an issue. In all cases, however, it is important to know that the information has leaked. In such an instance, at least partial corrective measures can be made. This means that the material needs to be in a secure facility, and that a broach of that protection leaves lasting evidence (for example, a padlock with a broken shackle).

Feynman

The idea to write up this note was proximally caused by rereading a favorite chapter of a favorite book: "Safecracker Meets Safecracker" in ***Surely You're Joking, Mr. Feynman***, (Norton 1997 – written about 1985). The name Richard P. Feynman likely needs no introduction to readers of these notes. He is hero to many (most) of us. In this chapter Feynman took us on a tour of a "zoo" of the unusual security-related things he encountered during his Los Alamos days. He always saw through and beyond all conventional wisdom. Further, he was curious and relished a challenge. His stories are always entertaining, so the usual reader might not single out this chapter as exceptional. Because of my Army experiences, the narrative rang particularly true.

Feynman was thus neither a conventional-wisdom nor a rule-based thinker. Thus he noted that some workers had cut a hole in a perimeter fence in order to avoid for themselves, the trouble of walking to the main gate. Rather than following channels, he went out the gate, around thorough the hole and back in, and likewise until someone noticed. He immediately noticed that even when a side cabinet of certain desks was locked in front, it was possible to reach in and pull out papers from the back. Part of his reputation for safecracking was a matter of trying factory-set original combinations, which often no one could be bothered to properly change. Further, he noted that nearly everyone had a crib somewhere. Combinations were written down nearby, were birthdays, or perhaps mathematical constants (such as 31 41 59). This, plus his inherent inventiveness.

BETTER COMBINATION LOCKS

As I said, there was no issue getting through an ordinary padlock without destruction; or most any lock if you had the right brute-force tools. That's a given. The trick would be to cut a lock, remove and photograph the documents, putting them all back (possible) and then putting the lock back. Suppose it is a non-trivial padlock and you just cut it. Just switch out a lock of the same type? Looks the same at first glance. But how would you get the same key or the same (unknown) combination? [If you knew the combination, why would you have cut it!]

So you want a lock that keeps others out as a routine, and that must be destroyed to get through it otherwise. These existed as changeable combination drawer locks and very commonly as combination padlocks securing more ordinary cabinets (through modifications with rebar rods through multiple handles). Once your locks were set, the combinations were recorded and sent to the next higher headquarters. If you forgot the combination, you could contact them and ask (suitably verified) for the combination. They could even give you the combination over the phone, since your first act after opening the safe would be to change to a new combination. (Like getting a change code sent to your email for resetting a password.) This worked fine, and the locks (Sargent and Greenleaf, S&G) were excellent. Most units probably had a dozen or more of them.

Some locks got orphaned, which was unfortunate because they were expensive. Once they were out of use (or just set aside for a period of time) it was not uncommon that no person remembered the latest combination or even its history. Further, it was necessary to change the combination every time someone who knew it was permanently transferred from the unit. It was not unreasonable that instead of changing the combination on a lock in place you set a new combination on a spare lock and tested it carefully. Then you swapped out the lock with full intentions of resetting the first to the factory 10-20-30. But you never did, and no one could remember it a month later. Orphan. What happens to orphans? They end up in an old box with companions. In Korea (where I ended up), at that time, they could just as easily end up "on the economy", which meant you could buy one at a hole-in-the-wall store that sold all sorts of surplus items. They were sold for a couple of bucks (MPC, green, or equivalent in Won) as ordinary combination locks with the combination (now considered fixed) on a paper tag (more expensive than the Master locks). So someone sold them on the "black market" and no one really worried about their being out there. I bought a couple. It was clear enough that they had been drilled and/or the back had been taken off. It was not much of a problem to get the back off again. Inside - pretty much what it had to be. Now, anyone could have bought and opened these junked items. No hard secrets here.

Normally, one changed the combination by dialing in the current combination and opening the lock. Then you could flick open the change window (a spring-loaded round cover over a hole) on the back, insert the special tool (called a “change key” that looked a lot like an Allen wrench), twist it to unlock the three locking wheels that set the outer ring of the wheels relative to the shaft, dial the new combination, twist the key to re-lock, and pull out the change key. Messing this up was another excellent way of generating an orphan.

We went around making unannounced inspections. With very few exceptions, things were in excellent order (this was the army after all). Document were in the containers and/or properly signed out for work. Minor deficiencies could often be corrected on the spot. We weren’t into “Gotcha” mode. We wanted a call when there was a problem so we made friends. [Incidentally we were generally E5 enlisted with civilian cover and clothing. This was so we could inspect a unit usually commanded by a Captain or Major. This worked. If things got tight at any time, our boss told us to point out the “all personnel are ENJOINED to cooperate with this Special Agent”. On a couple of occasions, I simply said I really hated to have to begin a report by saying that the commanding officer was unfamiliar with the services provided by Army Intelligence.]

So we often chatted and BS’ed. Then I usually offered to see if they had any orphaned padlocks that needed to be opened. They usually had several to a half dozen. If the lock was open or even if it was closed and had the change window open (as was advised when out of service) I could open them (perhaps 2/3 of cases). If the lock was closed and the window not flipped open prior to closing, I couldn’t open it (That’s the Idea!) “in the field”. [There was a way to do this and get it back into service, but I’m saying no more except you would be quite disappointed if I did. No gamma rays! No ESP!]

Now this was fun of course. I spread the locks I intended to open on a desk and announced it would take me about 20 minutes. To my surprise (the first time I did this) everyone got up and left! They assumed they weren’t supposed to watch. Only one guy (a SP4) said “Can I watch.” He said it with no emphasis on any of the three words. No expression of a preference – just an inquiry. “Sure”, I said. Then I took out my tools from my key case. What the Specialists saw was what looked like an ordinary change key (it was slightly modified) and what looked like (and was) a bent <u>finishing</u> nail (again looking like an Allen wrench). The <u>head</u> of the nail had been filed square just like the cross section of the change key. Fancy, sophisticated stuff!

I showed him that we needed the change window open, but could then feel through it with the nail head as the wheel was rotated. In this way, you could put the head through the first locking wheel, and indeed, unlock it. Now unlocked, you could turn the rotor (which would have otherwise been immovable) and find the second locking wheel, and unlocked it. Likewise for the third wheel. Then set the dial to OPEN, pull out the nail, and insert my

change key. My change key had been modified by filing off a tab, the purpose of which was to prevent you from pulling out the change key with the wheel locks loose. So the modified change key went in through all three locking wheels. [Because it went through several locking wheels in general, unlocking one wheel individually without locking others was not possible – hence the need for the nail with its squared-off head (pg 11) and smaller round shaft.] Now, at this point, I had a perfectly serviceable change key in a lock just as though I had dialed the correct combination. Dial on a new (actually factory 10-20-30) combination and lock the change. All this I learned by taking apart the lock I got downtown.

No one would have made the mistake of not recognizing that a lock on the downtown market had been opened (file marks on the back) so there was no chance of a tampered locking coming back in. Nor was my method of opening an orphaned lock a threat to a properly used lock (change window closed when locked). Further, I suspect that S&G knew perfectly well the same techniques with regard to their locks.

Other Army Matters

My Army experiences were not so bad – much better for me than for so many. As I said, I more or less accidently ended up in intelligence. Why not the famous Army Corps of Engineers? Timing basically. We had batteries of tests to see what we could do, and having a degree in Engineering Physics, I scored well technically, but was not so much good at things like language. So of course, I ended up with 47 weeks of language training among other schooling. Very little use of any electronic skills, but we were a small office on a small Army compound in a medium sized city in Korea, so we enjoyed a certain amount of autonomy and self reliance. And engineers like to fix problems.

When they provided us with a mobile commo trailer with an external generator, we soon found that the generator worked in standby (receive), but when we keyed the transmitter TTY, the breaker blew. I rigged two discarded 12 volt jeep batteries in series across the generator output (24 volts) as a buffer against the keying surge. Worked like a charm. That sort of thing. Phones and all that were worth doing ourselves. Reasonably nice army-built buildings and houses. Far from the “flagpole”.

In addition to our intelligence office, the compound had an EOD (Explosive Ordnance Disposal) unit (HQ and housed away from any explosives!), and a more extensive Signal Corps facility. Most of us were friends. I got along with the Signal Corps folks, some of whom were degreed engineers, and all of whom knew which end of the soldering iron was hot. More interestingly, the Signal Corp had (just cross the yard from our office) a phone switchboard “manned” by female Korean civilian employees. I have been married to one of them for 45 years.

Cornell 9999

At Cornell, I had little uses for “safecracking” skills. No classified materials. No combination locks. With a few exceptions. No keyed padlocks. Just S&G “institutional” (“Do Not Duplicate”) door locks (very hard to pick) and desks with key locks with keys long since lost. A few keyed file cabinets for storing upcoming exams.

On occasion we had a need for combination padlocks. These were for doors to instructional labs where perhaps a dozen or more TAs needed to be able to open up lab sessions, many during the evenings. Too many individual keys would have been needed. These doors had a hasp and a four wheel (0…9) combination padlock. Usually the combination was a course number. At some point, I had an evening session and the combination had just been reset and given to me (so I thought). Arriving an hour or two early, the combination did not work. The “Safety Division” had keys to all buildings/doors but no combinations. No big deal to cancel a lab session and make it up later – but what if….? I tried a few variations on what I had been given. No luck. It struck me that I probably had time enough to try half the 10,000 possible combinations. For some reason, I decided to start at the top (9999), clicking downward (9998, 9997,9996….). So I started with 9999. **CLICK! IT WAS OPEN!** The combination was 9999.

My guess is that the person sent by the building manager had changed to the new combination, tested it, and written it down correctly. Then he returned the setting to ground (0000), our standard practice, and thinking that it was not good to leave it there, rotated to 9999 and only then removed the change key. But I don’t know. And of course, I had no real notion that I could stumble on the right combination – let alone on the first try.

Feynman (in the reference above) had a similar accident of good luck. An open combination lock is inherently more vulnerable than a closed one. [For this reason, you are not supposed to leave a lock open and available even with the cabinet open and in use – either put it through the hasp and lock it (requiring redialing the combo to relock the cabinet) or put the open lock inside the cabinet and out of sight.] Feynman had discovered a simple way of getting the last two numbers off a combination lock if it is open. He was showing how it could be done to some skeptical watchers. By accident, he had also dialed in the correct first number (within tolerances which were as large as 5 numbers!). CLICK. He had apparently opened it “cold”. Good for his reputation.

At Cornell we were protecting mostly property – not secrets (but see below). Also in the old days we were a lot freer (with care) to “accuse” or at least wonder about misdeeds. (Today we would be fired or sued, I suspect.)

At one time (many years ago as I say) an oscilloscope turned up missing from a student lab. Everyone knew it was gone, and there were no good clues. It was clear that a storeroom from an open access area had a common wall with the lab. AND, the wall between the back of the storeroom and the lab was "short" being 8 feet while the ceiling was 10 feet. (I don't know why, but this was not an uncommon construction.) But no evidence of climbing. Seemed unlikely. "Inside job" was our guess. Oh well.

Shortly thereafter I got a call from the lady in accounting about one of my project students. We had limited funding for projects (perhaps $50/student total) and a couple of credit cards which students could use (when authorized, and receipt presented). She asked me if I had authorized this student to spend a larger amount, and if he needed a new multi-meter (she recognized that we had these already available) and a radar detector! No he wasn't. I called him up and he was evasive but eventually allowed that the Radio Shack clerk must have confused the department card with his personal card. Possible. So he and I agreed that he would settle up with accounting ASAP, and he was in front of the clerk's door, cash in hand, when she came in the next morning.

Shortly pieces of a likely puzzle conglomerated. First, I was quite sure the guy had deliberately used the department card for personal items. Multi-meter ? He's equipping his own lab. Radar Detector? He's interested in breaking laws. Then I remembered that he was sometimes absent Fridays – traveling with an athletic team – Gymnastics. Perfect physique for climbing a wall I would suppose. No – nothing could be proven nor was an attempt to do so made by me.

Very little got stolen. At times of the year, labs were open 24 hours. My office was always open when I was on campus. Books turned up missing, but really only because I lent them out and all involved (including me) forgot. Sometimes they reappeared courtesy of the librarians who found them in the "night return" with a bunch of actual library books. I am still to this day not finding some old books I remembered and now needed; not found among the boxes I packed when I retired. Thanks to the Internet, you can usually find a replacement copy for a small fee and postage.

At Cornell, we weren't protecting secrets – much. There were of course students who would not have minded getting an advanced copy of an exam for the next day. We were very careful about this. Not so careful about protecting the exams during grading! What could go wrong?

Well, one exam had a very difficult final problem. I did not write it, nor did I have much of an idea how to solve it. I think it was for holding down the average. The professor who wrote the problem wrote the solution the next day after the exam. Now we could grade it.

Grading is never much fun unless we all sat around a table with pizza and made jokes. [We were never laughing at a student's poor performance. We cheered (Yesssssss!!!!) when someone got a hard problem right.] But scheduling grading was not automatic, and exams were often on a table in a lab or office waiting for ambition or a deadline to appear.

With this particular exam, one student was waiting to see me (or a TA or whatever) and was relentlessly "bugging" the one grad student who was there to the point where the grad student left. When we got to grading the last problem, only one student (of like 100 total) got it completely right. Few got very far at all. Further, his solution was identical to the professor's. Further still, his "correct" solution was overwritten – a previous two pages had been completely erased (well, you could see the smears). Can you say blatant?

The grad student who was chased away related how a student had been left alone in the lab, but he did not know the student's name. We knew for certain who the modified exam belonged to, and that the problem had been copied rather exactly from a solution produced a day after the exam. I took the grad student to the next class session and asked him to discretely point out the annoying lab-invader. Of course, it was the same guy.

Again, this was many years ago when we could take reasonable actions and offend no one that mattered. So I call the student up and say, "Is there anything you want to tell me about the last problem on the exam"? "Like what?" "Well, If I though you didn't know exactly – I wouldn't be calling." Long pause. "Don't count it," he suggests. "We'll see."

Now I had in mind that he was not a dedicated cheater because he did such an inane job of it in this case. Later I ruminated on the fact that he had, after all, "annoyed out" the grad student from the lab – an intentional act. Another grad student told me that in certain parts of the world, cheating is considered good-sport as long as you don't get caught. Perhaps. I don't know what eventually happened. Not my decision. Just the messenger.

But – all and all, I would guess that 99.99% of the students were a joy. A few bad apples probe the rule.