Identifying Threats to Privacy

Cryptoparty in Boston

December 28, 2016

Metaphor

How many possible ways could a stranger get into your house or apartment? Just some examples off the top of my head:

Steal your key when you're not looking
Pick your lock
Use a crowbar
Copy your key at a hardware store; then replace it
Make a wax/clay impression of your key, as in *The Day of the Jackal*
Trick someone with a key into unlocking the door
Get in through an unlocked window
Take the key by force/threat (including legal)
Try the knob and find it unlocked

Your author is not a security professional or lawyer. Comments or corrections are encouraged!

Can you think of other ways someone could get in without permission? From the would-be burglar's perspective, what are some advantages/disadvantages of any of these methods? Which ones do you think someone is most likely to ever try against your apartment in real life? Which ones are most likely to *succeed* in real life? How would that change if you were a bank or electronics store?

Brief assessment of threats to my own privacy

Now take the thought process we just applied to the physical security of your apartment, and try to apply it to privacy.[1] So, what if the intruders were after information, rather than access to your place?[2]

Ways in which my privacy could be compromised: *Tracking by servers* including my home internet company, any relaying server, or destination server. If they keep a big pot of data on what I connect to, what times of day, contents of communications, etc., then this could later be accessed inappropriately from within, breached, or used as circumstantial evidence. *Breach of single password* because of: loss or confiscation of a written password, someone tricking me into disclosing a password, or data breach directly at a server. This can compromise the privacy of that account and any accounts that used the same password. *Guessing a password.* This can happen to a weak random password,[3] an extremely common password,[4] or to passwords based on significant people's names, dates, etc. *Flaw in software* that implements a given algorithm.

[1] For our purposes, *privacy* means *keeping yourself or information about you secluded, or free from observation or intrusion.*

[2] Think: credit card numbers, photos of you, Watergate style snooping, etc. And again, can you think of ways someone's privacy could be compromised, other than the ways I list? I've left some items off for space, and I don't intend this list to be a complete "answer sheet."

[3] For example, a password of six lowercase letters, like `nkpukf` or `orfpvv`.

[4] For example, `iloveyou1`, `dragons1`, `michael1`, or `princess1`. A nice discussion of common passwords is at wpengine.com/unmasked/.

Why/who? It can also be useful to think about which one(s) of the following scenarios is/are likely. Are the bad guys after *you specifically* (trying to break into your e-mail because of who you are and information that only you have)? Or do they profit from *anyone's* data/resources (trying to steal any financial details, collect data about everyone's movements, or remotely control anyone's computer)? Or are they just malicious?[5] Are they going to try entering passwords in the same web form where you log on, or can they try passwords offline, or are they going to go for the data directly on the server? Are they people you have ever interacted with in real life or online? Or are they perfect strangers to you?

What harm is likely to occur if someone accesses or discloses information about you? Would people stalk/harass you? Would you get fired? End up with a drained bank account or ruined credit score? Would you be under suspicion (e.g. for searching "how to steal an identity")?[6]

My current approach to these threats

I use Tor Browser for plenty of things (such as all the research I did for this write-up). I purchased a subscription to a non-Gmail e-mail account. I *never* reuse passwords used to secure sensitive data. My passwords are completely random. To encourage myself to use strong passwords, I write them down and keep this list very safe. I memorize many but not all. I avoid pseudorandom numbers and use `random.org` or literally a box of dice to generate passwords.[7] I can carry some randomly pre-selected words as "entropy in my pocket," so it's easy to change passwords.[8] Keep your software updated. Consider whether it's safer just to talk in person rather than assuming technology is the solution.

Conclusion

To decide on my approach to privacy, I first think *how* someone may try to compromise my privacy, *why* they may do so, *who* they may be, and *what harm* may occur if they succeed. Keeping a written vs. a memorized password is a prime example of a choice that can trade off the likelihood of different threats.

[5] "He said the hack was simply a grab for my three-character Twitter handle. That's all they wanted. They just wanted to take it, and fuck shit up, and watch it burn. It wasn't personal." Mat Honan, How Apple and Amazon Security Flaws Led to My Epic Hacking. *Wired* 2012-08-06.

[6] What if there was no identity theft or public embarrassment? If a stranger knew about your messages, receipts, income, movements, or how you probably vote, would that fact alone bother you? I'm not saying it's *supposed* to.

[7] world.std.com/~reinhold/diceware.html

[8] I'm sure that we will discuss more password practices beyond this short list.