Encryption Always Leads to Character Substitution

ir. Emile M. Hobo — 16 June 2022
E-mail: e.m.hobo@hotmail.nl

"All Your Data 'Are' Belong to Us"

"No, Your Honor, you are not allowed to rape, murder, or steal." How often have we heard this from a criminal's mouth? Here's another one, "You have to be smart to get away with it." I'm smart. I get away with everything, because I refuse to break the law. Criminals are stupid and so are most engineers, because that's what they are: criminals.

These criminals, hackers, have familiar phrases and quite honestly, they represent their culture adequately. For instance, "All your base are belong to us" is a classic from an old Japanese videogame: Zero Wing. The broken English is an honest representation of their character: they are broken, want everything else to be broken, and will break everything when they can.

We employ these hackers to find weaknesses in our systems, but they aren't honest when you study them. They gather data by diving in your dumpster, stealing your trash, hoping to find your password. They install backdoors into systems, so they may later make use of them to break in. The people building in the backdoor are now hired to manage our system safety.

They cheat, lie, steal, and manipulate: that's what their manuals state. They call it "social engineering," a term coined by Kevin Mitnick. It's what fascists label "neutral language," so they told me on Twitter, in this case replacing the word "manipulation."

We have allowed the world to turn into an outlaw Walhalla. The system is thus corrupt globally, that all faults are now considered to be virtues by the powers that be. The people that can actually handle security get excluded and the perpetrators now get to decide who's guilty or not. These are also the people that come up with encryption mechanisms.

"Our encryption mechanisms are smart. We are the best at this. Trust us," we hear. I've also heard differently. These very same hackers, whose culture I was partially forcefully submerged in when I studied Computer Science, are very specific and do say it, as do all criminals when they commit a crime, "There is no privacy on the Internet."

If you want to be able to get away with it, you need to say it. Only when the righteous say what's going on, that's considered to be bad, because we don't join in on the "everyone is doing it"-culture we have today. If there is no privacy on the Internet, then what does this mean for encryption? Why is finding the next biggest prime number horse shit?

Why do you need a prime number? What does encryption really do?

The Internet always sends characters separately.

A stronger kind of encryption would probably be that senders and receivers have a book with code numbers, with a character representing words and commands. You could essentially map all words in a dictionary to numbers, but with natural language this will be a problem due to preserving typos and creative interpretations.

With general use Internet-portals of any kind, like stores, everyone would still have the dictionary on their computer to make use of, so then it doesn't add to the security. Still, why do we need prime numbers?

Prime numbers make sure that the same character or character string (that includes numbers) doesn't get mapped onto a character or character string that another character or

character string has also been mapped onto. It makes sure that it's an *isomorphic* relationship, a one on one mapping.

This means that all encryption really just makes use of character substitution. How big is this problem? If you want to break the code, all you need is raw computing.

Think back to 1997, Deep Blue, a supercomputer dedicated to chess. It beat Gary Kasparov, but Gary Kasparov was also able to beat it. That means it had a human ELO rating equivalent of around 2800. My 2015 laptop can reach a computer ELO-rating of 3200.

Computer ELO-rating means that a human would need an equivalent ELO-rating to solve a problem of that human ELO-rating even just occasionally. The computer solves those problems without fault. Everyone has a supercomputer. Anyone can do this.

Our problem is either faith or a lack of options.

You trust the system to work, which it doesn't, or you find yourself within a system that you've realized doesn't work, working that very same system to try and induce change, even though you know the system has become fully corrupted globally. Sticking to the faulty system isn't the answer. Using your voice and calling out all misdeeds is.

When they tell you to shut up, use your voice, make sure people know. Don't ever shut up. Open up. Unhinge whatever is already in the open, but they try to make look like a coverup. Make sure people keep seeing it and can't deny it. Spotting the problem once isn't enough. We need to spot problems continuously for them to be solved.