Evan Smith

CIS 628 – Cryptography, Weissman

Exercise 6.01: Apple vs. FBI

My thoughts on this case are different now after a lot more experience in the computer science field than they were at the time. I wasn’t clear on what exactly the issue was for Apple to provide what was framed as some minor assistance that was certainly possible for them to do to potentially identify additional suspects or discover motives for a terrible attack. It was interesting to read about this again in the present and find myself surprised that the majority of Americans supported the FBI at the time. With the benefit of hindsight about the event itself, as well as a deeper understanding of the implications of this case, had the FBI succeeded, I definitely side with Apple.

Separate from any technological or cryptographical concerns, I found the arguments of the FBI for why they required access to the phone at all to be suspect at best. It seemed that this merely served as a wedge to get in the door of precedent for government backdoors, reviving the dreaded Clipper chip that was referenced in the Wikipedia article. Obviously, this issue does scale with the impact of the information on the device, and the surety that the information exists there at all. If, for example, the phone was the guaranteed location of the shutdown codes for a nuclear attack, the FBI’s position would be insurmountable. Even in that case it seems that there were options both potentially within the agency as well as with third parties that were already able to crack Apple’s encryption and would likely be the best option regardless of the use case. Any software made by the company would have to go through development prior to use, and an existing solution is obviously preferable.

While I certainly sympathize with the desire of law enforcement and the affected families to leave no stone unturned, the relative scales of impact in this case are wildly out of balance. There is a slight chance of a minor breakthrough in a single case versus the unlocking of a true Pandora’s box of security precedent that would reverberate across encryption technologies. If there is anything I am confident in, it’s that the best hackers do not work at Apple, and the creation of any backdoor into the system on purpose would be inevitably found and utilized by bad actors (which, in my opinion, likely includes FBI overreach). Heck, the macOS High Sierra bug showed that we don’t need to give these companies any more opportunities to create exploitable issues in some of the most widely used software in the world.

Exercise 6.02: Australia’s Assistance and Access Bill

I think that the questions posed in the lab drill right down into the issues with this bill. The fundamental issue seems to be very similar to the problems with almost all scientific issues that are legislated: legislators are just not educated on these questions, and it is not reasonable to expect them to be. It is inane, therefore, that they can make rules that make impossible expectations of technology and call it a win.

Another aspect of this bill that I found both interesting and frustrating is the ability of a single governmental body being able to create global restrictions on internet policy. While it seemed that some companies made threats of leaving Australia, I suspect those were idle, since the market is just too large. I remember similar things happening with Facebook and Twitter being regulated based on speech laws in other nations which drove shifts on the internet at large. While there are obviously technical parts of the infrastructure that must be regulated and standardized internationally (protocols, character standards, etc.), the fact that cultural or law enforcement standards of a single nation with sufficient clout can impress those standards onto everyone seems wrong to me.

Regarding the bill itself, some of the more frustrating aspects is that it was pretty clearly passed as a political win, and not even truly intended to trigger meaningful change in the area that it was ostensibly focused on, preventing crime. The clause that companies are not required to add any change that introduces a “systemic weakness” into their security. As pointed out in several of the articles, adding a way to break any arbitrary encryption is by definition a systemic weakness. It would seem that there is a legitimate argument to say that compliance with this bill beyond existing warrants for non-encrypted communications would be impossible.

This gets at the question posed in the lab: is it possible to set up a backdoor only for the “good guys”? Putting aside the question of whether there is sufficient legal controls on the requests for such information, and the definition of “good” in this case, encryption relies on the ability of only the sender and intended recipient being able to decrypt the message. Any middle-man, backdoor access immediately voids the entire concept, and decays privacy, security, and trust in one go.

While I made allowances to the FBI in the Apple case for extenuating circumstances (which were both hypothetical and wildly unlikely), this bill gets no such pity. By definition this is a broad-strokes requirement which does not establish a sufficient barrier of proof for the critical nature of the situation that would merit a request. The bill itself even lists harm to property alone as a sufficient use case for the law. This is clearly a gutting of long-term security for short-term possible benefit, and I can only hope it has and will be contested.

Exercise 6.03: To Serve Man

As a lover of the Twilight Zone, I was surprised that I had never seen this episode! While the cryptographic content was admittedly sprinkled in as buzzwords, I thought it was really funny that they were attempting to discover the meaning of a different language using decryption tactics rather than translation! That would imply that all languages are able to be manipulated into the same core language, which is an amusing miss by the Twilight Zone version.

From the sound of the summary about the original short story, the main character is a translator rather than a codebreaker, which makes a lot more sense. That being said, I guess the “ambassadors” to Earth know English and everything about our culture, so it isn’t unreasonable for them to be writing in some sort of transliterated English. This would make more sense given that the entire episode hinges on a double-entendre which very rarely make sense in multiple different languages when translated.

There is a bit of a deeper reading of the episode in the context of encryption, which I fully acknowledge is a stretch. The average user of services are neither very knowledgeable or critical of their security measures or business practices. This can lead to similar situations occurring where a panacea is presented with no apparent catch, but all too often the outcome is the same as the episode. As the saying goes, when the service is free, you are the product. While companies aren’t (necessarily) selling folks’ physical bodies for food, our information is harvested and sold while being strung along for the apparently altruistic benefits that are provided.

With my philosophizing out of the way, I enjoyed the break of pop culture references mixed in with the more serious and concrete articles.