Phillip Johnson

ESOC 488 – Final Project Proposal

10/4/2017

False Decryption

One issue that civilians or military can encounter is an immediate need to ‘unlock’ a device, or present a document, for fear of either physical harm, or legal issues. This can take the form of having to unlock a phone, or present a requested document that has been encrypted. It appears to be an all or nothing event with the only options currently being to comply, fail to comply, or destroy the items in question. What if there was another option, which constitutes complying, but does not jeopardize all of what the individual is attempting to keep restricted? Having the option to decrypt documents two separate ways would prove invaluable in situations like this. Specifically, where one decryption, a ‘false’ or ‘partial’ decryption could provide enough information that the viewpoint is that the document was entirely decrypted. Current or old technologies that a could compare to this, without destroying the device or information would be a metadata hidden information, or source hidden. This would be where you have a full document, or image, which is a full piece on its own, but when manipulated in a specific way, reveals a second layer. The top layer would constitute complying with handing over information, but the more important information would still be secure.

The reason for choosing this technology is due to the ever-growing intrusion of privacy by law enforcement, where if the individual does not have a lock on their phone, the officers have, at times, simply opened the phone and used the information in their investigation. When they cannot do that we encounter issues like the Apple Vs FBI in the case of the Iphone and wanting to force the company to crack the phone or build a backdoor specifically for law enforcement activities. This new technology could help fill the gap. By having a double decryptable format the persons could comply with all legal requests of the law, while still maintaining privacy over sensitive items.

The strongest arguments against this form of technology would be that it does not constitute complying with legal directives when encountering a subpoena or something of the likes. It could be said however, that any subpoena would simply be asking for information, or access to a device, and not the assurance of 100% accessibility to all forms of all items, as most people have aspects of their phones that only the provider can access.

Comparing this to non-computational technologies is difficult, as this requires having a protected document that can be viewed multiple ways. The best analogy would be of a puzzle box, when it is implemented to the form of a desk or drawer, etc. A puzzle box when implemented to a desk would have the normal functionality of a desk with multiple hidden compartments that require a specific set of circumstances to open, whether that be a combination of knob pulls, drawers pulled out a certain distance, or by requiring a specific amount of weight on a spot on the desk. This analogy falls apart when you look at the realization that if the desk was broken or disassembled, then all the hidden compartments could be found, while in the multiple decryption format, this would yield no additional information.