Natnael Kebede

**Inventing a Cryptanalytic Attack**

There are a wide variety of mechanisms to break into cryptographic systems. Some of the common cryptanalytic attack vectors include attacking the cryptographic key, attacking the cipher or algorithm itself, analyzing the cipher’s implementation to find weaknesses, manipulating the encrypted and decrypted data to find clues about the keys used, and attacking the people themselves. Nevertheless, these attack vectors rely on humans to implement and perform to some extent. As a result, the easiest way to execute a cryptanalytic attack is through social engineering, which involves tricking users into giving confidential information. To illustrate how this can be done, I will describe a possible plan that relies on social engineering for key discovery and breaking into a cryptographic system.

Consider the following scenario: I have been targeting an organization that is close by a Dunkin' Donuts coffee shop and observing how employees behave during work hours several times from the parking lot. One day at 8 a.m. on a typical Monday morning, I show up with my suit as any other regular employee. Many people are getting into the office to start their workday, and one must swipe their ID badge to enter the building. So, I wait for someone to go ahead of me while I get my hands full with boxes of donuts and different coffee beverages. I smile and ask the employee to hold the door so that I can get in. As soon as the person replies with “sure, no problem” and holds the door open, I tell them that the Dunkin' Donuts nearby is marketing some new products and that I am a representative sent from corporate to deliver the products so that everyone in the office can try them. Before the person responds, I request to walk with them to their desk or direct me to the kitchen so I can put the boxes I brought over there. While the individual taught I was a fellow employee at first and gets surprised that they are getting free donuts the next, I pull out a card for the worker to fill out so that Dunkin' has a representative from the office to reach out to the next time someone else from corporate visits to deliver new products. The card would ask them to fill out their full name, date of birth (claiming that they would get free donuts on their birthday), and employee ID number and email address stressing that Dunkin' would want them as business customers from here on for any of the office’s needs. While the person fills out the card, I ask them where the restroom is and get directions. However, instead of going to the restroom, I look around for open offices, unsecured workstations, plug-in keyloggers that will send live captured keystroke data back to me, take photos of sensitive information left on desks, and names of staff members placed on desks. With all the information I gathered, including the card and maybe when I was on my way back from the kitchen, I leave the office.

Next, I would utilize LinkedIn, Facebook, etc. to gather more data about the individual. The possible username and passwords I collected using the keylogger would also come in handy to log into systems and see who encrypted a specific document/s with a unique key. Once I have an aggregated information about the unique document I am interested in, I would then call the person who encrypted the document (in this case, the employee I had interactions with). Pretending to work for the organization’s Information security office, I would ask them for the key stressing the fact that a problem has occurred with the network, computers, servers, and so on. To avoid any trust issues, I would also confirm the employee’s identity with what the information I acquired about them and what they have given me before. At this point, the employee is very unlikely to hesitate in providing the key. So just like that while another attacker could have spent tremendous hours attempting to decipher an encrypted message, I would have easily tricked a person into providing me that information by exploiting them psychologically.