**“Cryptography: The World of Encryption”**

***Table of Contents: Pages***

*Introduction………………………………………………………………….........(1)*

*Understanding Cryptographic Attacks…………………………………………(1)*

* *Birthday Attack………………………………………………….(2)*
* *Mathematical Attack…………………………………………....(2-3)*

1. *Ciphertext only Attack…………………………………(2)*
2. *Known Plaintext Attack……………………………….(3)*
3. *Chosen Plaintext Attack……………………………….(3)*
4. *Chosen Ciphertext Attack……………………………..(3)*

* *Brute Force Attack……………………………………………...(3)*
* *SSL/TLS Downgrade Attack…………………………………..(4)*
* *Dictionary Attack………………………………………………(4)*
* *Replay Attack…………………………………………………...(5)*

*Citations………………………………………...………………………………..(6)*

Daniel Rao

Apr 13th, 2021

Vince Skinner

**Cryptography: The world of Encryption**

**Introduction**

Encryption is used everywhere in modern computer systems. It plays a crucial part in security by providing confidentiality, integrity and authenticity. While on the other hand no matter how secure a system is there is always a possibility of a cryptographic attack. This may come in different ways. As one said that, “No system is secure, given enough time and resources anything can be cracked.” In this paper I am going to discuss some of the most common type of cryptographic attacks.

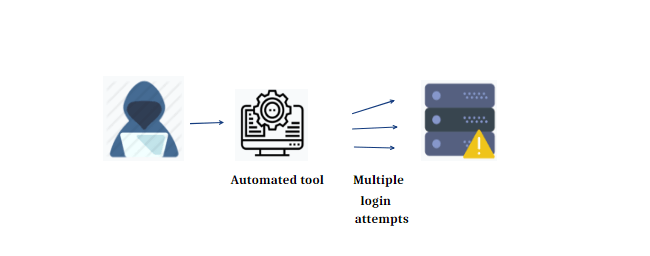
**Understanding Cryptographic attack**

To such as tcpdump and Wireshark considered passive attacking tools because the attacker is only collecting data sent to and from a cryptosystem. activate attack attempt to determine the secret key used to encrypt plain text by actively sending input to a cryptosystem . Generally the public usually knows the algorithm because companies developing encryption algorithms realize that the public might discover vulnerabilities that the companies program might have missed in their developing process. because they release the source code to the public, Public can give positive feedback and modify or add to the programming code. making source code available can contribute to making a better product. agencies such as NSA and CIA do not release their encryption algorithms. below are some of the most common active attacks:

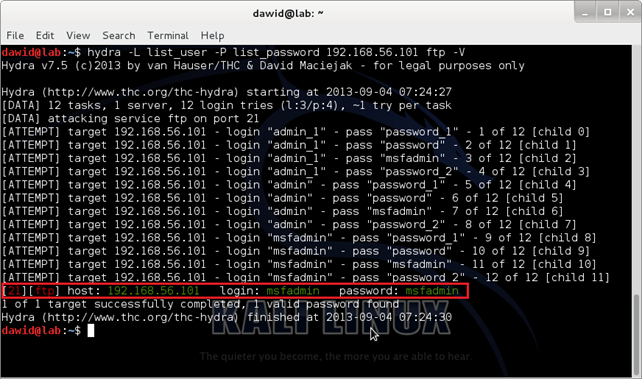
1. **Birthday attack**: We might have probably heard that if there are 23 people in a room, the probability of sharing the same birthday is about 50%. This kind of attack is pretty similar as in birthday attack the attacker uses the same hash value for the two different inputs and reveals any mathematical weakness in the hashing algorithm. for example if an attacker has 1 hash value and wants to find another message that creates the same hash value, one can easily do so in a couple of hours if the hashing algorithm is not very strong. SHA-1 uses a 160 bit Digest. theoretically, signing a collision for a different message would require , computations which may be possible in the near future.
2. **Mathematical attack:** In this type of attack, properties of the algorithms are attacked by using mathematical computation. attackers perform this type of attack in many different ways and it all depends on what information they have access to. there are about five main categories for this type of attack which are as follows:

* **Ciphertext only attack:**  attackers have deciphered text off several messages encrypted with the same encryption algorithm but has no access to the plain text so they must try to figure out the key used to encrypt the data. Getting a copy of side protects is usually easy with a sniffer such as tcpdump or Wireshark, but this type of attack is the most difficult to perform because little or no information is known about the encryption algorithm used.
* **known plaintext attack:** Attackers has access to boat message which is encrypted and decrypted form. this attack is easier than this I protected on the attack because patterns in the plain text can be examined.
* **chosen plaintext attack:** Attackers has access to both plaintext and ciphertext and can choose which message to encrypt. because the whole plain text message and Ciphertext message are available, determining the key is much easier. this type of attack is mostly carried out by spoofing an email to someone, claiming to be someone else.
* **Chosen ciphertext attack:** In this type of attack the attacker has access to the ciphertext to be decrypted resulting plaintext. Apart from this they also have access to the cryptosystem to perform this type of attack.

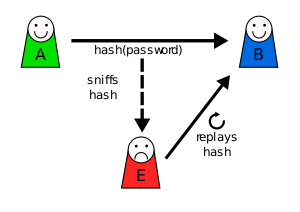
1. **Brute Force attack:** A Brute Force attack tries all possible keys in a key space.One example in using a password cracking program would be to attempt every possible combination of characters in an effort to break the password hash. Brute Force attack can be launched on any kind of message Digest, set as a Certificate request.



1. **SSL/TLS Downgrade Attack:** This type of attack who intercepts the initial communication between a web server and a web browser can force a vulnerable server to insecurities renegotiate the encryption being used down to a weak Cipher. This works because of a web server and a web browser must negotiate with Cipher and will be used to communicate before they begin. if a client tells the server it can only communicate over weak protocols and the server agrees to use that weak protocol the communication would be at risk.
2. **Dictionary Attack:** In a dictionary attack, The attackers have access to a password file they can run a password cracking program that uses a dictionary of known words or passwords as an input file. Most of these input files are available on the internet and can be downloaded for free.



1. **Replay attack:** In this type of attack, did Tiger capture data and attempt to resubmit the captured data so that the device which can be a computer or router things and legitimate connection is in effect. if the captured data is login information then the attacker could gain access to a system and can be authenticated. Many systems have countermeasures to prevent these attacks from occurring such as packets using sequence numbers that detect when the packet is out of order or not.



Citations:

<https://www.crypteron.com/blog/the-real-problem-with-encryption/>

Hands On Ethical And Network Defence