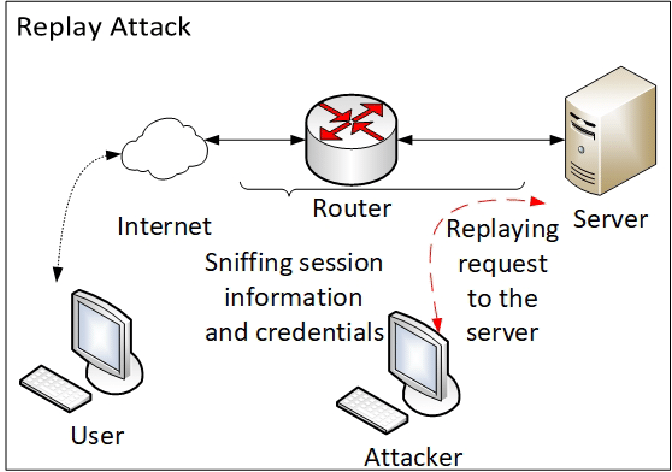
**Common Cyber Security Threats**

**Introduction**

For many organizations across the globe, susceptibility to online-criminal activities is a major concern. In recent years, the threat of cyber-attacks has not only increased but has also evolved in terms of scope, degree of sophistication, and purpose. Though financial theft remains the major motivation for the majority of attacks that many organizations encounter, denial of service, theft of sensitive information such as intellectual property, national secrets, and spread of misinformation are the other key incentives cybercriminals engage in cyber-attacks. To achieve their purpose of either knocking down of computer network system or steal sensitive information for financial or psychological gains, cybercriminals rely on several attack methods. While there are many methods cybercriminals employ to achieve their mission, replay attack, brute force attack, dictionary attack, rainbow table attack, birthday attack, social engineering attack, and fuzzing are most common.

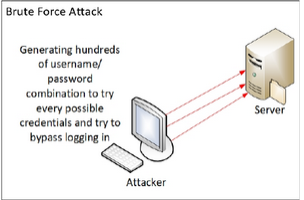
**Replay Attack**



**Source: Saleem, & Carter, 2019**

Replay attack can be described as an attack on security protocols by an intruder or malicious entity that intercepts encrypted network communication with the intention of delaying the message or misdirect the recipient of such communication (Jurcut, et al., 2014). Thus, a replay attack is an attack on a communication network by a cybercriminal or hacker that involves the interception of original content to misdirect and fool the recipient that the communication is authentic and is from an authorized user (Jurcut, et al., 2014). A replay attack is majorly caused by a flaw or weakness in the design and structure of a communication network such that an intruder can get access and take charge of the security protocol involved in the transmission of original content from authorized user to the recipient (Jurcut, et al., 2014). The danger of a replay attack is that an intruder or hacker does not have to decrypt the communication upon getting access to it. A common real-life example of a replay attack involves an attacker intercepting and resending encrypted financial transfer communication such that the recipient is deceived to wire funds to a wrong account controlled by a cyber-criminal. Just like other types of cyber-attacks, the replay attack is controlled by the Computer Fraud and Abuse Act (CFAA). The Act is the primary law that governs the prosecution of cyber-criminal activities in the country (McNicolas, & Angle, 2019). While a replay attack is often used to test the strength of a network's security protocol, it's one of the most common forms of cyber-criminals activities.

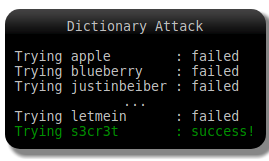
**Brute Force Attack**



**Source: Saleem, & Carter, 2019**

Brute force attack is a type of cyber-attack on a security protocol that entails the use of trial-and-error to guess access information to a computer or communication network (Bhandari, et al., 2017). The term brutal force is derived from a personal computer game that was released in 2000 (Dave, 2013). Depending on the speed of the computer being used to orchestrate a brute force attack, this process of guessing usernames and passwords often sees as high as a billion entries per second until a successful outcome is achieved (Dave, 2013). The effectiveness of a brute force attack on a communication network is largely dependent on the strength of the password used. For powerful computers just about two minutes to successfully crack username and password for 8-word authentication information, a 9-word password takes about 2 hours. On the same note, a 12-word password that employs unique characters may take tens of years to crack. Thus successful brute force attack on a computer or communication network is majorly facilitated by weaknesses in login credentials used (Bhandari, et al., 2017). Brutal force attack is illegal in most instances; however, the process is often used to ethically test the strength of security protocol. While brutal force attacks can be prevented successfully by the use of a complex encrypted password, the damage of a successful attack might be huge especially if the attackers managed to take control of the system.

**Dictionary Attack**



**Source: Stack Exchange, n.d**

A dictionary attack is unauthorized access into a password-secured computer or network system that involves trying every possible word stored in a dictionary as a password (Bhandari, et al., 2017). The main cause of the dictionary attack is related to the fact that the majority of computer and communication network users do use simple phrases that are easy to remember like those in a dictionary (Bhandari, et al., 2017). The fact that many users often reuse passwords, vary them slightly, or don't even bother to change the password used after detection of attempted breach makes dictionary attack one of the most popular. Therefore, a dictionary attack is usually initiated on a system when there is high confidence that the password used consists of specific characters or letter combinations. A possible dictionary attack list could contain names of people, cities, local teams, organizations, and so on. Unlike brute force attack which tries every combination of words and special characters to guess a password to a system, dictionary attack only rely on pre-selected words (Bhandari, et al., 2017). Because of this, a dictionary attack is mostly designed for specific target organizations or individuals. Good examples of word combinations that qualify as dictionary attack include words such as 'CityOfLondon2020', DemocraticParty@2020, QWERTY, or even 12345. The Computer Fraud and Abuse Act is the principal federal effort to deal with cyber-related crimes targeted at government and bank computers (McNicolas, & Angle, 2019). The law does also covers unauthorized access to a computer system to commit espionage.

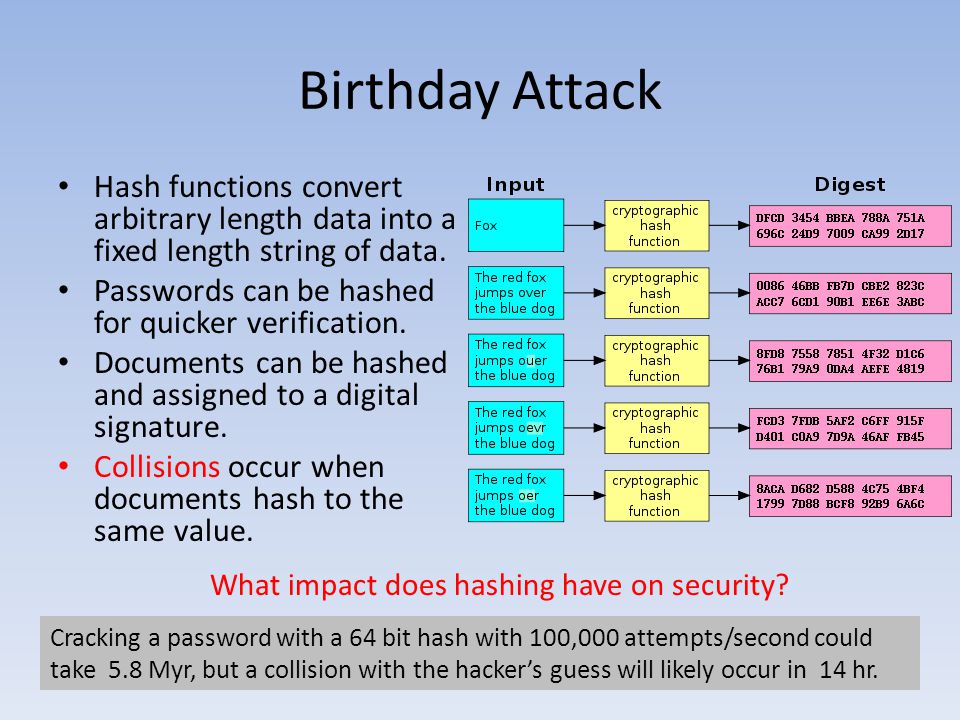
**Rainbow Table Attack**



**Source: The Security Blogger, 2015**

Rainbow table attack is a cyber-attack strategy that entails the use of rainbow hash or trail left or stored in a rainbow table every time a password is keyed to discover the actual password (Bhandari, et al., 2017). Unlike dictionary and brute force attack that seek to use common words stored in a dictionary or guessing the password by trying a combination of characters to unlock a system, rainbow table attack matches several hashes with those stored in a computer system to begin the hacking process (Bhandari, et al., 2017). In other words, a rainbow table attack simply entails matching a hash of original password with those stored in a rainbow table. The process of hacking a system using a rainbow table attack is completed once a perfect match between the hashes is found. Because of this, a rainbow table attack is more effective since a hacker only needs to discover whether the hashed text or password actually exists within a computer database to begin the hashing process. The rainbow attack is usually prevented using a salt mechanism where unique characters are added into the hash generated every time a password is entered to prevent a hacker from successfully discovering the hash trail stored in the system (Bhandari, et al., 2017). While rainbow table attack is usually used for password retrieval, the creation of stronger and more secure passwords, they are often utilized in hacking computer systems and communication networks. Like other types of attacks, rainbow table attacks can be dealt with by long passwords that encompass special characters.

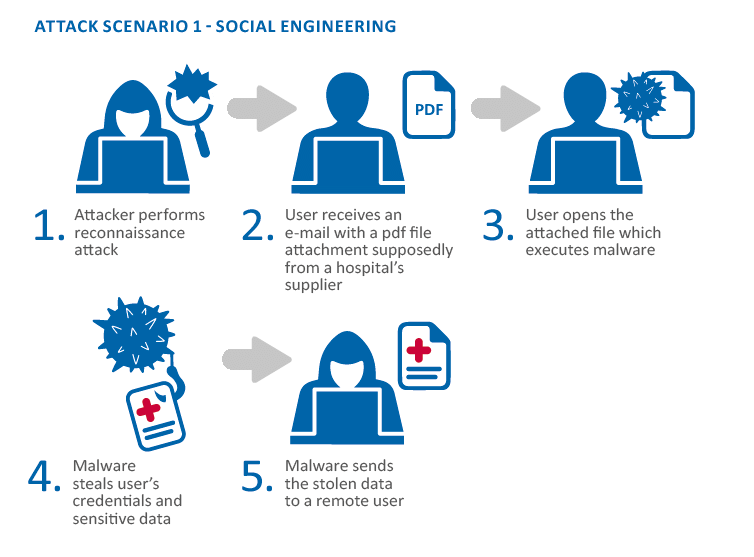
**Birthday Attack**

****

**Source: Bond, n.d.**

A birthday attack is a type of attack on a computer system or communication network that uses the mathematical probability theory. Based on the mathematical probability theory, the birthday paradox expects that in any unselective or random group of 23 persons, there is a 50% probability that two of the individuals in the group share birthday. Thus, a birthday attack works by comparing any input that results in a matching of the hash generated every time a password is keyed into a system (Bhandari, et al., 2017). Hash collision or matching ensues when the hash process generates an identical hash for other passwords. While the problem is undesirable, it does occur often, thereby leaving room for birthday attacks by cyber-criminals. A birthday attack is usually often employed by cybercriminals to trick users of digital signatures to sign fake contracts that resemble the actual contracts (Bhandari, et al., 2017). An actual example of birthday may involve an individual tricking another into signing a fraudulent contract as opposed to the actual one by altering specific characters such as replacing a full stop with a comma, inserting commas, using one instead of three spaces at the beginning of a sentence and so on. Numerous variations to the actual contract can then be generated to find one whose hash matches the hash of the actual contract. Once a perfect hash match is found, the real contract is presented for signing but this signature is fraudulently attached to the fake contract.

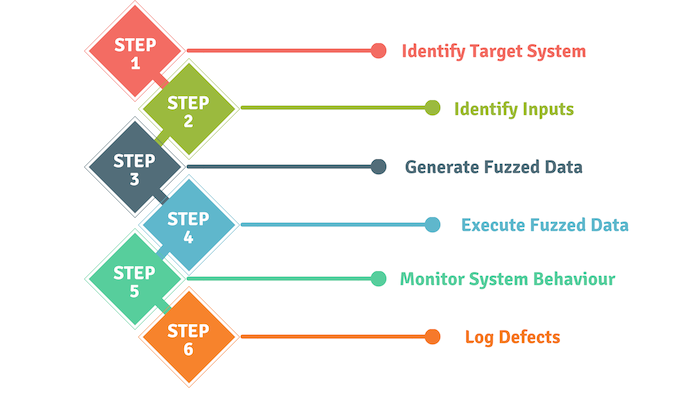
**Social Engineering Attack**



**Source: Mayol et al., 2016**

Mayol, et al., (2016), describes social engineering attack as the human side of hacking. Social engineering attacks are a type of attack that uses all manner of tricks to manipulate entities or individuals into releasing valuable and often sensitive information to intruders (Salahdine, & Kaabouch, 2019). Unlike other types of attacks that can be prevented using computer firewall and software systems, social engineering attack is difficult to prevent as humans tend to trust other humans once given enough reasons to do so (Mayol, et al., 2016). The U.S. Department of Justice views social engineering attacks as having the biggest threat to the world today (Salahdine, & Kaabouch, 2019). Social engineering attacks such as the 2018 attack on the Equifax company database that resulted in access to personal information of about 146 million individuals in the country was achieved by sending thousands of emails that appeared to originate from large financial institutions (Salahdine, & Kaabouch, 2019). The attack is said to have resulted in a loss of more than $2.3 billion (Salahdine, & Kaabouch, 2019). Since social engineering is the most common and perhaps the most successful, several laws have been enacted to deter and prosecute social engineering attacks. The Computer Fraud and Abuse Act is the principal law that is designed against cyber-attacks on government computers, financial institutions in the country, and interstate or foreign commerce (McNicolas, & Angle, 2019). This law tasks the Federal Bureau of Investigation (FBI) with the responsibility of arresting, providing evidence, and prosecuting against persons who commit cyber-criminal activities that are targeted against the U.S. government, enterprises, or even individuals.

**Fuzzing Attack**

****

**Source: Levale, 2020**

Fuzzing attack or fuzz testing involves deliberately sending invalid data to a system to jam or cause an error in the system. The basic principle behind fuzzing is, you generate and send invalid, distorted, unforeseen, or troublesome input to a target system with the see whether it will crash (Li, et al., 2018; Levale, 2020). Fuzzing was discovered accidentally by Barton Miller when his attempt to accomplish the normal command process of more than 1,200 data input during a storm at his office at the University of Wisconsin resulted in system failure (Li et al., 2018). Follow up studies on the phenomenon made Miller conclude that the software failure was caused by unexpected and highly deformed input. While fuzzing is not as serious as other types of cyber-attacks, it's traditionally employed to test the strength of computers and other communication network systems to withstand cyber-attack (Li et al., 2018). Since the discovery, fuzzing has become one of the most popular strategies that information cyber-security experts use to protect detect vulnerabilities in a system and fixing it (Levale, 2020). However, the challenge of using fuzzing is that it requires knowledge and understanding of the target system for the attack to be successful.

**Conclusion**

As discussed, cyber-attack on a computer or communication network can take many forms. The choice of method of attack is majorly influenced by the aim of the attack which can be to destroy a network system or steal important data. When the aim is to destroy a system, fuzzing may be preferred as it is usually designed for a specific computer system. Social engineering is preferred where the key purpose is to trick users to release sensitive data which might then be applied to achieve a broad objective such as financial theft. Given the many motives for cyber-criminal activities, the heavy financial losses related to some of these thefts, and the misdirection that is often generated when sensitive information is captured, organizations have no room to let their guard down.

References

Bhandari, A., Bhuiyan, M., & Prasad, P. (2017). Enhancement of MD5 Algorithm for Secured

Web Development. *Journal of Software*, *10*(14), 240-252. <https://doi.org/10.17706/jsw.12.4.240-25>

Bond, L. (n.d.). *Monte Carlo simulations*. SlidePlayer - Upload and Share your PowerPoint

presentations. https://slideplayer.com/slide/4547555/

Dave, K. T. (2013). Brute-force Attack “Seeking but Distressing”. *International Journal of Innovations in Engineering and Technology (IJIET*, *2*(3), 75-78. [International Journal of Innovations in Engineering and Technology (IJIET](file:///C:\Users\HP\AppData\Roaming\Microsoft\Word\International%20Journal%20of%20Innovations%20in%20Engineering%20and%20Technology%20(IJIET)

Levale, Y. (2020, March 10). *Fuzzing ICS Protocols*. Dreamlab Technologies. <https://dreamlab.net/en/blog/post/fuzzing-ics-protocols/>

Li, J., Zhao, B., & Zhang, C. (2018). Fuzzing: A survey. *Cybersecurity*, *1*(1).

<https://doi.org/10.1186/s42400-018-0002-y>

Mayol, et al., (2016). *Smart Hospitals: Security and Resilience for Smart Health Service and*

*Infrastructures*. European Union Agency For Network And Information Security. file:///C:/Users/HP/AppData/Local/Temp/Smart%20Hospitals.pdf

McNicholas, E., & Angle, K. (2019, October 22). *Cybersecurity 2020 | Laws and regulations |*

*USA | ICLG*. International Comparative Legal Guides International Business Reports. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*,

*11*(4), 89. <https://doi.org/10.3390/fi11040089>

Saleem, D. & Carter, C. (2019). Certification Procedures for Data and Communications

Security of Distributed Energy Resources. National Renewable Energy Laboratory 10.13140/RG.2.2.15474.04803.

Stack Exchange. (n.d.). *How does the attacker know what algorithm and salt to use in a*

*dictionary attack?* Information Security Stack Exchange. <https://security.stackexchange.com/questions/180535/how-does-the-attacker-know-what-algorithm-and-salt-to-use-in-a-dictionary-attack>

The Security Blogger. (2015, November 25). *Understanding rainbow tables*. The Security

Blogger – Security news, notes, and ramblings. <https://www.thesecurityblogger.com/understanding-rainbow-tables/>