Exercise – 4

Abdurrehman Syed
2308546

Task – 1

Side-Channel Attack: Power Analysis

Side-channel: Power consumption

In such an attack, the power consumed by a device while performing some cryptographic operation is measured. Different cryptographic operations result in different power consumptions. Therefore, an attacker may deduce important information from such patterns of power consumption, even the secret key.

Systems affected: Any system that performs cryptographic operations, including microcontrollers, smart cards, etc.

Information leaked: Secret keys, encryption algorithms, and other sensitive data.

Real-life case: Power analysis attacks have been used in various real-world scenarios, including attacks on smart cards, cryptocurrencies, and other embedded systems.

Fix: There are several techniques to aid in power analysis attacks:

- **Hardware countermeasures:** These include techniques like masking, shuffling, and dynamic voltage scaling.
- **Software countermeasures:** These include techniques like blinding and randomizing data.
- **Protocol-level countermeasures:** These include techniques like using secure cryptographic protocols and algorithms that are resistant to side-channel attacks.

Task – 2

Slow Loris Denial-of-Service Attack

Slow Loris is a low-bandwidth DoS attack where an attacker sends a series of incomplete HTTP requests to a target server and keeps the connections open for an extended period which can then make server resources unavailable to others.

Uniqueness: Unlike other high-bandwidth DDoS attacks, which overwhelm the servers by flooding them with traffic, Slow Loris attacks use a very low bandwidth approach to make its detection and mitigation by traditional DDoS protection measures quite challenging.

Effects: Slow Loris can significantly degrade the performance of a web server, which may make it unresponsive to legitimate traffic. This, in turn, can hold business operations, disrupt finance, and negatively affect the site's reputation.

Mitigation/prevention:

- **Limiting Rate:** Limit the number of concurrent connections per IP address.
- **Timeout:** Have appropriate timeouts for idle connections
- **Web application firewall (WAF):** Use a WAF to find and block malicious HTTP requests.

Notable instances: Slow Loris has been used in various attacks, including targeting popular websites, online gaming platforms, and government servers. It has been notably used in an attack in 2015 against the website of the French government.