|  |  |  |
| --- | --- | --- |
| **Attack Type** | **RFID System** | **Dynamic & Encrypted QR System** |
| Brute Force | Vulnerable after 248 attempts  ≈ 22623 years (using 1 RFID Reader) | Resistant (2256 complexity) |
| Sniffing Attack | Dangerous vulnerable | Resistant with encryption, difficult to intercept |
| Counterfeiting Attack | Can counterfeit the identity of the reader or tag | Difficult to counterfeit due to dynamic encryption |
| Physical Attack | Hijacking, clonning or destruction of RFID devices | Impossible because of non-physical nature |
| Replay Attack | |  | | --- | | Vulnerable to replay attacks without anti-replay mechanisms | | Resistant with dynamic encryption |
| Data Manipulation Attack | Possible to manipulate data stored on the tag | |  | | --- | | Resistant with encrypted data storage | |
| Deactivation of Transponder Attack | Can deactivate RFID transponders to hide objects | Impossible because of the non-physical nature |
| Middleware Attacks | Vulnerable to malware injection, SQL injection, or manipulation of data | Resistant with encrypted backend communication |
| Denial of Service - DoS | Possible jamming or frequency interference to disrupt communication | Protected against jamming with frequency-hopping |

TABLE 3

Encryption Strength Comparison.