The purpose of this Analysis report in my cybersecurity career was to deepen my understanding and analytical skills in cybersecurity through both theoretical exploration and practical application.

It began with an examination of Side Channel Attacks, teaching me about vulnerabilities stemming from the physical operations of systems. I then delved into evaluating security protocols using Physically Unclonable Functions (PUFs) in RFID systems, helping me to assess their strengths and weaknesses critically.

Finally, it culminated in a hands-on password auditing exercise using L0phtCrack, which illustrated the real-world implications of social engineering on password security. This comprehensive approach not only broadened my grasp of complex security concepts but also prepared me to tackle real-world cybersecurity challenges effectively.

Side channel is a type of attack where the attackers exploit indirect information which is gained from the physical computer operations implementations to gather sensitive information rather than exploiting software vulnerabilities. They take in analyse indirect datas like power consumptions, electromagnetic leaks, or even sounds to extract sensitive datas. The three different types of information which can enable hardware-based side channel attacks are.

1. Electromagnetic Emissions: Devices can emit electromagnetic signals during operations which varies with their processed data, which can be analysed to work out sensitive information.
2. Power Consumption: Different data processing and operations can consume different amounts of power. This is done by monitoring devices power usage that an attacker can use to deduce information about operation being able to be performed and data to be processed.
3. Timing of Execution: Even the time it takes fro an operation to be completed can show information about the processes that occur within the system. Such as speculative execution vulnerabilities to exploit timing differences to extract very sensitive data.

Side channel attack are usually passive as they rely on observing and analysing the byproducts of a system's operations without actually actively intersecting or altering the system's behavior. It is important to be undetected while gathering data which can used to workout sensitive information. The nature of this attack suggests passive approaches in gathering information indirectly rather than active manipulation of the system.

Even though the protocol might be resistant to eavesdropping due to its ability to generate unique responses by PUFs for each of the challenges without having to reuse challenge-response pairs, there are still drawbacks that we have to consider that would discourage their recommendation.

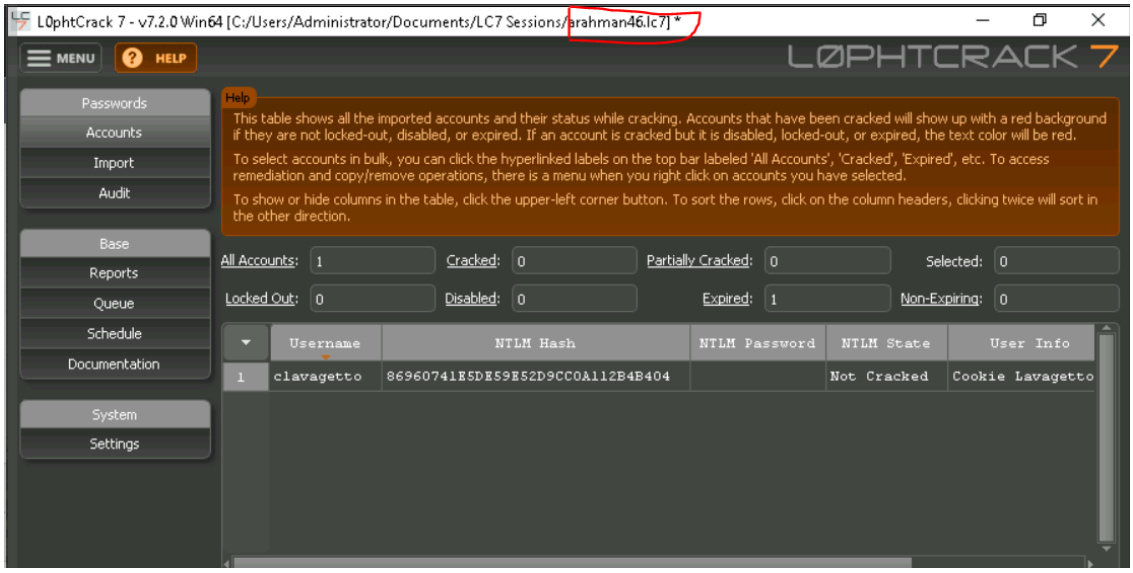
While the PUF can provide robust mechanism against cloning, PUFs assumed to be unclonable will bever be entirely accurate. Physical attacks that are advanced might be able to very closely approximate and/or deduce the PUF structure which may lead to possible breaches. Therefore those assumptions can cause complacency in security practices and overreliances on PUFs's unclonability can be a significant failure point.

Secondly, the protocol don't consider security risks that are associated with the TAG id transmissions in plaintext. Even if the tag privacy being searched is not the main concern, transmitting those ID in plaintexts can allow attackers to even track the tag movements or even inventory., which may lead to privacy violations or even cause further targeted attacks.

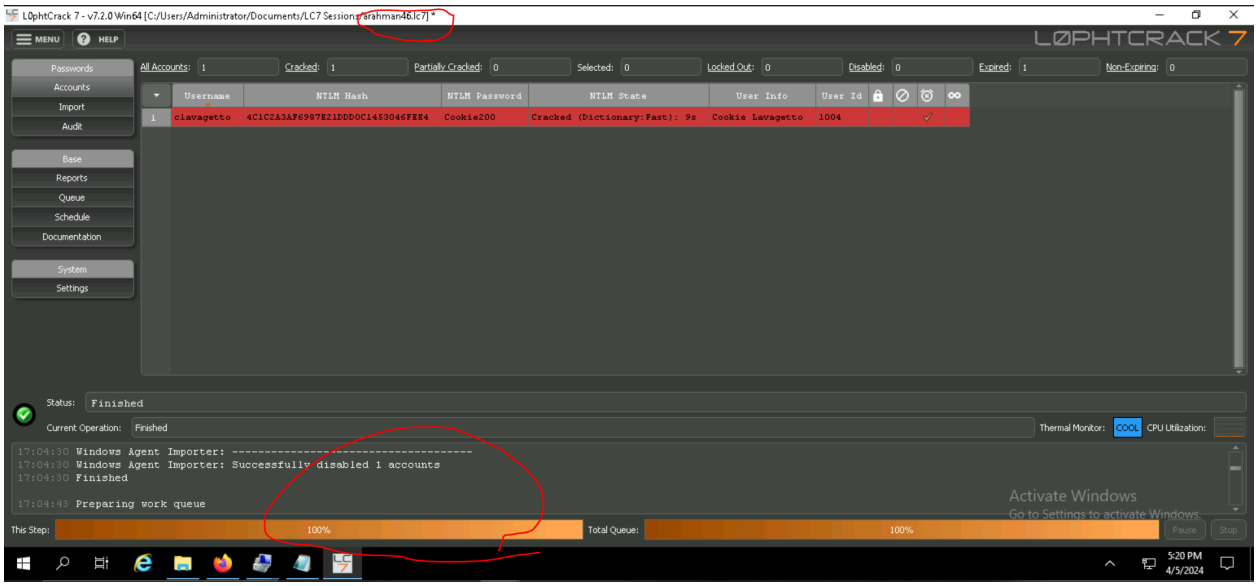
Another issue has to do with scalability and management, such as if a large number of RFID tags are used then managing the unique challenge response pairs could become unwieldy for each tag, as the system would therefore require a very robust database and a very secure method of challenges and responses synchronization. This in turn could result in very complex infrastructure to even maintain.

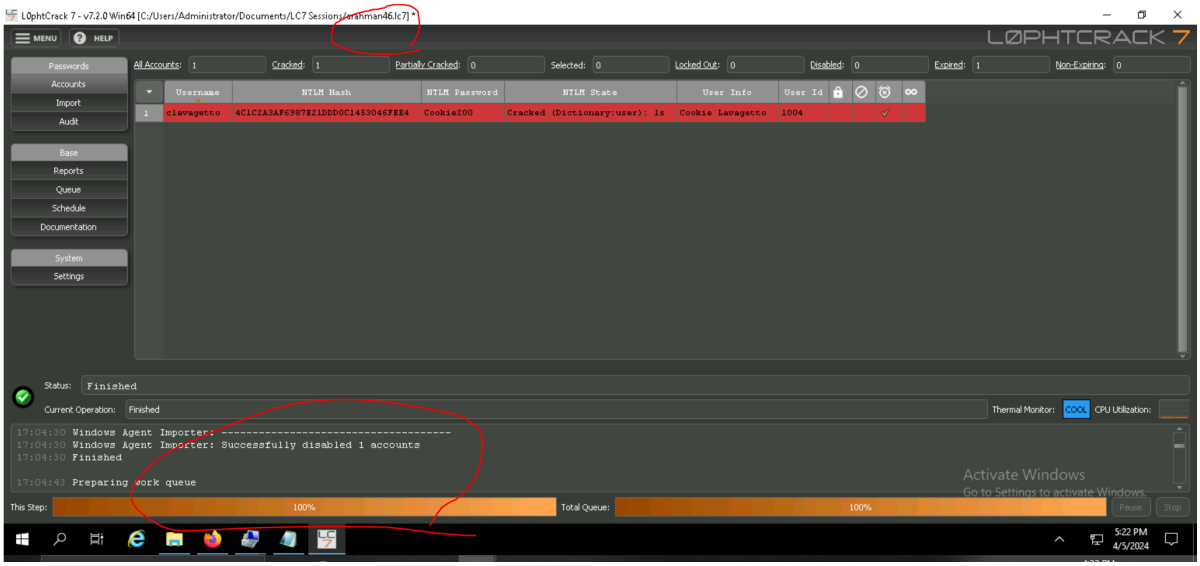
Even though this is not mentioned in protocol, it is worthy to point out that even the lack of mutual authentication (such as the the reader providing tag authentication) could be problematic because without mutual authentication, a reader that is unauthorized could initiate several communication with a tag and even though it may not be able to clone the tag, it can still potentially engage in other activities that are malicious such as denial of services attacks. These issues demonstrate that even though the protocol uses PUfs strength for security, it won't fully account for other security and practical challenges that might arise in a real-worl implementation.

We will be testing a password auditing and recovery application called L0phtCrack for this question. L0phtCrack version 7.2.0 is open-source, and you will download and install it on the Windows VM (Virtual Machine).


L0phtCrack 7 - v7.2.0 Win64 [C:/Users/Administrator/Documents/LC7 Sessions/arahman46.lc7] *
MENU
HELP
LØPHTCRACK 7
Passwords
Accounts
Import
Audit
Base
Reports
Queue
Schedule
Documentation
System
Settings
Help
This table shows all the imported accounts and their status while cracking. Accounts that have been cracked will show up with a red background if they are not locked-out, disabled, or expired. If an account is cracked but it is disabled, locked-out, or expired, the text color will be red.
To select accounts in bulk, you can click the hyperlinked labels on the top bar labeled 'All Accounts', 'Cracked', 'Expired', etc. To access remediation and copy/remove operations, there is a menu when you right click on accounts you have selected.
To show or hide columns in the table, click the upper-left corner button. To sort the rows, click on the column headers, clicking twice will sort in the other direction.
All Accounts: 1
Cracked: 0
Partially Cracked: 0
Selected: 0
Locked Out: 0
Disabled: 0
Expired: 1
Non-Expiring: 0
Username
NTLM Hash
NTLM Password
NTLM State
User Info
1
clavagetto
86960741E5DE59E52D9CC0A112B4B404
Not Cracked
Cookie Lavagetto

(next page)


L0phtCrack 7 - v7.2.0 Win64 [C:/Users/Administrator/Documents/LC7 Sessions/arahman46.lc7] *
MENU
HELP
LØPHTCRACK 7
All Accounts: 1
Cracked: 1
Partially Cracked: 0
Selected: 0
Locked Out: 0
Disabled: 0
Expired: 1
Non-Expiring: 0
Username
NTLM Hash
NTLM Password
NTLM State
User Info
User Id
1
clavagetto
4C1C2A3AF6987E21DDD0C1453046FEE4
Cookie200
Cracked (Dictionary:Fast): 9s
Cookie Lavagetto
1004
Status: Finished
Current Operation: Finished
Thermal Monitor:
CPU Utilization:
17:04:30 Windows Agent Importer: ----------
17:04:30 Windows Agent Importer: Successfully disabled 1 accounts
17:04:30 Finished
17:04:43 Preparing work queue
This Step:
100%
Total Queue:
100%
Pause
Stop
Activate Windows
Go to Settings to activate Windows.
5:20 PM
4/5/2024


LØPHTCRACK 7
MENU
HELP
Passwords
Accounts
Import
Audit
Base
Reports
Queue
Schedule
Documentation
System
Settings
All Accounts: 1
Cracked: 1
Partially Cracked: 0
Selected: 0
Locked Out: 0
Disabled: 0
Expired: 1
Non-Expiring: 0
Username
NTLM Hash
NTLM Password
NTLM State
User Info
User Id
1
clavagetto
4C1C2A3AF6987E21DDD0C1453046FEE4
Cookie200
Cracked (Dictionary:user): ls
Cookie Lavagetto
1004
Status: Finished
Current Operation: Finished
Thermal Monitor: COOL
CPU Utilization:
17:04:30 Windows Agent Importer: ----------
17:04:30 Windows Agent Importer: Successfully disabled 1 accounts
17:04:30 Finished
17:04:43 Preparing work queue
This Step: 100%
Total Queue: 100%
Pause
Stop
Activate Windows
Go to Settings to activate Windows.
5:22 PM
4/5/2024