SMART INDIA HACKATHON '18

Ministry Category: Ministry of Defence

Problem Statement: Prototype/application for whitelisting of USB devices in OFB which can be subsequently used on internet as well as on intranet.

Problem Code: #MOD7 **Team Name: X-GEN**

Team Leader Name: Akshata Jahagirdar **College Code**:1-3328028571

IDEA / SOLUTION / PROTOTYPE

- Creating a distributed database with encryption which consists of whitelisted MAC addresses.
- This can be implemented using Blockchain system which provides tamper-proof dataset e.g. – Hyperledger. We will implement encryption on top of blockchain infrastructure.
- When the storage device is connected to the computer a program will extract the MAC address, generate a hash and check if hash is present in the local database. A local probabilistic database (e.g. like bloom filter) will be used to check if the hash of the MAC address is whitelisted. If hash is not on the whitelist then the OS event will notify the admin regarding the same and block it. Use of Probabilistic database will protect the system working on internet/intranet and disconnected computers from the unauthorized storage devices. The program used, handles the connectivity of storage devices with the computer.
- Another level of security will be to create an encrypted file system on storage device and a decryption algorithm for the same on authorized computer. This prevents data transfer from authorized storage device to unauthorized computer. File system will get decrypted automatically when a whitelisted storage device is connected to an authorized computer. If decrypted correctly, only then data transfer or access between storage device and computer is possible.

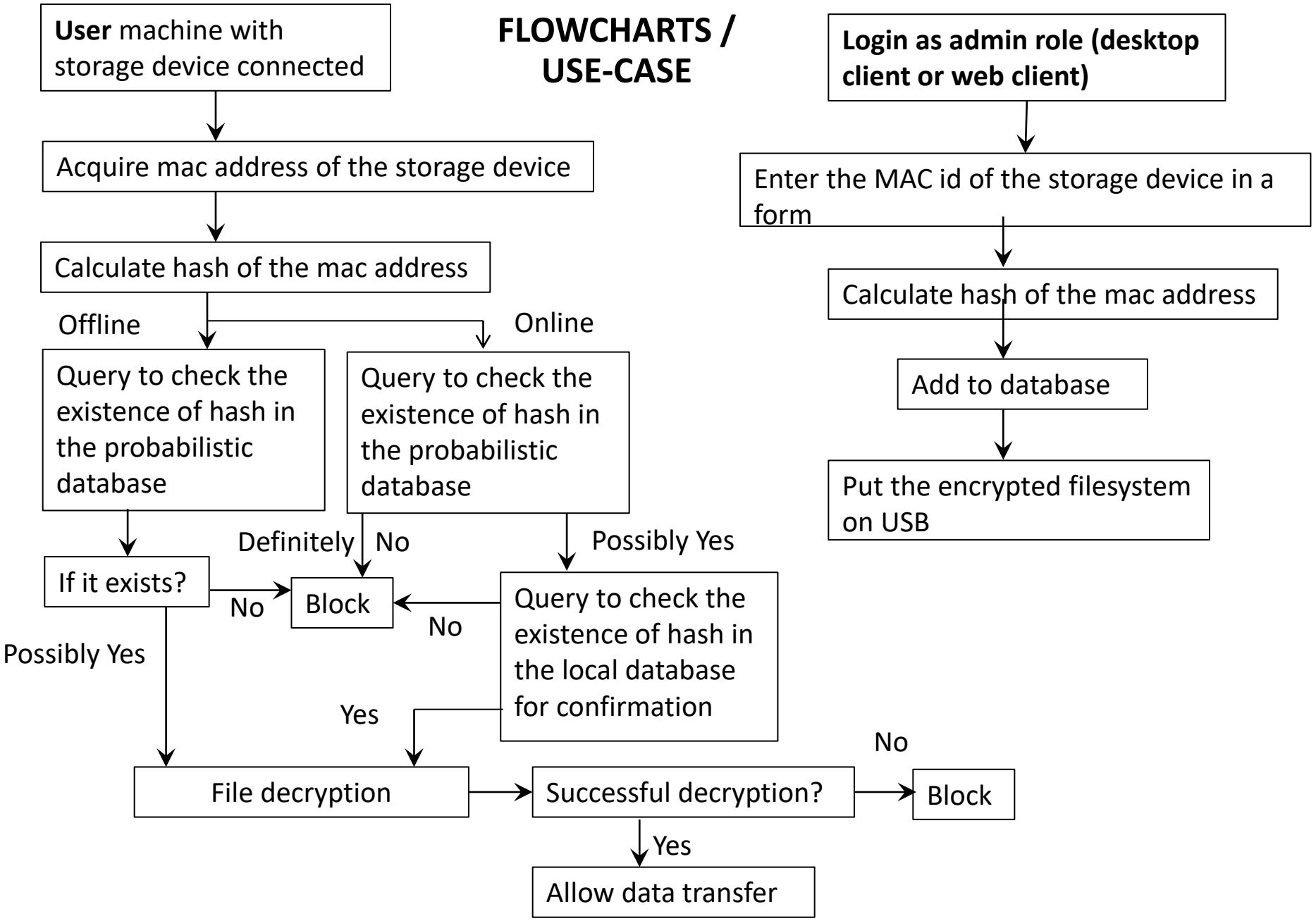
- The encrypted file system will be created on the storage device when it is connected to the blockchain system for the first time for registration on the database.
- The computers which are offline will also use a probabilistic database of authorized MAC addresses (e.g. like Bloom filter). The driver program on the computer will check the storage device against this probabilistic database. The driver program will block the devices which are not on the whitelist.
- The Bloom filter database will be updated when it is connected to the internet periodically. To update, the whole database is not replaced, instead the delta i.e. difference between the existing database on the Bloom filter and the local database is found and then added to the database of Bloom filter.

TECHNOLOGY STACK

- Open Source Blockchain distributed database like Hyperledger
- Browser/desktop based front-end for admin
- Windows service for detecting/blocking connected USB storage device
- E-mail / SMS notification service
- Language used: Go / Rust, Python

DEPENDENCIES / SHOW STOPPER

- Probabilistic data structures are not 100% accurate. In extremely rare case authorized device may get blocked if computer is offline
- The offline devices have to be connected to the internet or intranet for updating it periodically. This can give access to the devices which have been removed from the whitelist and won't give access to the newly added devices.


FLOWCHARTS / USE-CASE
User machine with storage device connected
Acquire mac address of the storage device
Calculate hash of the mac address
Offline
Online
Query to check the existence of hash in the probabilistic database
Query to check the existence of hash in the probabilistic database
If it exists?
Definitely No
Possibly Yes
No
Block
No
Query to check the existence of hash in the local database for confirmation
Possibly Yes
Yes
File decryption
Successful decryption?
No
Block
Yes
Allow data transfer
Login as admin role (desktop client or web client)
Enter the MAC id of the storage device in a form
Calculate hash of the mac address
Add to database
Put the encrypted filesystem on USB

NOVELTY

- Use of *blockchain* based systems to provide tamper-proof, distributed database of registered devices.
- The local probabilistic data base is space-efficient and provides high accuracy for 'offline' access.

e.g. A bloom filter with 1 million items in the filter with error of 0.001% (1 in ten thousand) requires about 3 MB memory.

SECURITY

- Our solution provides a facility to protect an authorized computer from an unauthorized USB storage devices in online/offline mode efficiently using combination of both, probabilistic database and blockchain.
- Block chain system keeps a track of the USB devices connected to a machine, and the devices added and removed from the whitelist. It also records the timestamp of the above mentioned activities, MAC address of the respective machines and the user IDs. Blockchain 'audit trail' is tamper-proof. Therefore, suspicious activities can be traced back.
- Even if the probabilistic database is stolen, the MAC address of registered devices cannot be retrieved.
- The encrypted file system in the storage device protects the authorized storage device from connecting to an unauthorized machine.
- Use of compiled languages like Rust/Go which avoid security issues like buffer overflow.