Group11: Yingxi Cao <yc2539@nyu.edu>, Nanako Sophia Chung <nsc309@nyu.edu>, Owen England <joe215@nyu.edu>, Zetong Wang <zetong@nyu.edu>, Wenxuan ruan <wr630@nyu.edu>

Exploiting camera vulnerability in DAHUA technology

A self-designed innovative five layer framework with Blockchain network.

ABSTRACT

The DAHUA camera is a commonly used device to record security footage. The footage is often downloaded and stored on to the device's respective database. This device is vulnerable due to a loophole in the device's database that allows an attacker to access and even "remotely download" users' private account information, such as their username and password (Tripwire, 2017). According to an independent researcher Bashis, this hack is extremely easy to perform, especially since the proof-of-concept code was published (Tripwire, 2017).

The main security problem we associated around the DAHUA camera device is that there is a largely unpatched vulnerability in the software that allows an attacker to easily hack and steal users' information, which poses an accessibility threat to its users and their data. Specifically, the vulnerability makes it easier for hackers to plant malware, such as BASHLITE, that targets Linux devices like Dahua cameras and turn them in to bots for use in DDoS attacks or for ransomware. Moreover, the Dahua software with the aforementioned vulnerability is also used by other, smaller companies which may not have sufficient resources to patch and address these security issues which raises even further concerns. The best way to patch up this loophole as best as possible would be to create and implement more security layers before reaching the database. This solution is described in detail below.

I. INTRODUCTION

A possible solution to cover up this loophole is implementing a five layer framework that is designed to secure the IoT network from unauthorized users. The layers consist of the application layer, the authorization layer, the network layer, the data encryption layer, and the physical layer. The application layer deals with "business logic," the way in which data is created, stored, or altered. The authorization layer involves sifting users to make sure that they are not malicious through a series of self-identification mechanisms before entering other layers. The network layer provides network access to the camera, where each IoT device is a node in the network. The data encryption layer encrypts the data that is safely passed and received from the camera to prevent any attackers from easily finding and reading data. Finally, the physical layer is the camera itself that sends data to be encrypted.

On top of this, blockchain technology can be integrated into each IoT node to better ensure the security and privacy of the network. The idea is to use a ledger in each node to safely keep track and prevent users from making any malicious transactions. The decentralized aspect of blockchain also makes it harder for attackers to steal large amounts of data at once.
Although this may fix a large portion of the loophole problem surrounding the DAHUA camera's database, there will still be more vulnerabilities found that we will need to account for in the future.

II. BACKGROUND

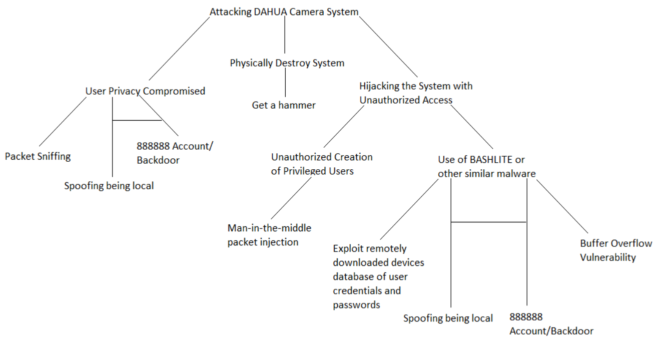
Lots of DAHUA camera's security issue surround authentication of who is accessing what resources, and what they are doing with that access to those resources. One major vulnerability allowed hackers to easily access a special '888888' account which is only supposed to work locally, but all validation to determine if a client is local to the camera is done by the client and not the recorder [3]. Further vulnerabilities such as transmission of cleartext passwords, as well as man-in-the-middle packet sniffing and packet injection attacks goes to show that DAHUA technology has lots of issues with the authentication and transmission of sensitive data [4][5]. We are suggesting the use of blockchain technology, specifically Hyperledger Fabric to address these security concerns.

Blockchain is essentially a decentralized ledger, a record of transactions made on a network stored across nodes, each of which have their own copy of the ledger. Updates to the ledger are added after being validated by a consensus protocol, where the nodes determine whether an update should be committed to the ledger. This means the decision of whether a transaction is valid is not just determined by a small authority but the system as a whole [5]. This allows for greater security of transactions as a nefarious actor(s) will not be able to easily inject code or modify the ledger in any way without the consensus of the rest of the nodes.

Hyperledger Fabric is an open source blockchain technology established under the Linux foundation. It is permissioned, meaning that participants are known to each other, instead of anonymous and untrusted [2]. This is beneficial, as it means networks can operate with some level of trust of users, as well as aiding in establishing who performs what actions on what resources. If an individual were to introduce malicious code, by nature of the system and blockchain, the transaction will be logged and the user who performed such an action will be known. This may raise some concerns about user privacy, and confidentiality but these are also addressed through a channel architecture. The network can be deployed such that there is a trusted channel, whose members are given permission to view transactions. Hyperledger Fabric is also designed to have a modular architecture so that it can be used in a variety of environments [2]. As such in the case of an IoT device like DAHUA cameras, it would be advisable to use consensus protocols and other modular components that ensure transaction validity and promote greater security.

III. THREAT MODEL

Based on what we have analyzed from last report, we updated the attack tree.

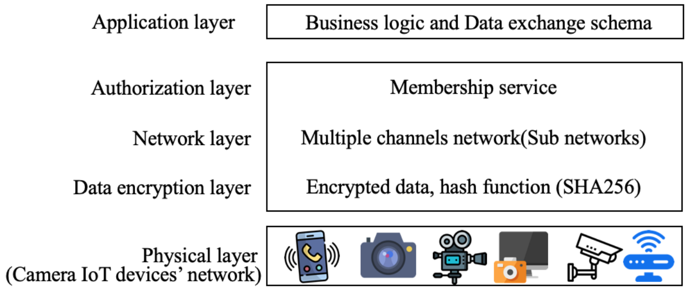

Attacking DAHUA Camera System
User Privacy Compromised
Physically Destroy System
Get a hammer
Hijacking the System with Unauthorized Access
Packet Sniffing
888888 Account/ Backdoor
Spoofing being local
Unauthorized Creation of Privileged Users
Use of BASHLITE or other similar malware
Man-in-the-middle packet injection
Exploit remotely downloaded devices database of user credentials and passwords
Buffer Overflow Vulnerability
Spoofing being local
888888 Account/Backdoor

THREAT ANALYSIS TABLE

Threat	Proposed Solution
Man-in-the-middle packet injection	Packet injection is difficult in a blockchain system, as an individual or group must achieve consensus for a change to be applied. This is particularly difficult in systems that use Byzantine Fault Tolerance. [6]
Backdoor '888888' account and spoofing being local	Part of any secure design should be not using a backdoor. This is not necessarily something that would be resolved just by applying hyperledger but must also be addressed by DAHUA themselves if it is in fact a backdoor.
Downloading and exploiting database of authorized credentials, packet sniffing	This issue is addressed in a few ways. Data encryption using SHA-256 is part of the proposed solution and is done at a low level making sniffing ineffective, and user data will only be accessible to members of a specific trusted channel. Access to this channel is heavily restricted, primarily DAHUA employees, and users who have been given consent by DAHUA.
Buffer Overflow Vulnerability [7]	In our framework, it is possible to restrict users not in the trusted channel such that they are unable to write data into the buffer. Moreover it is difficult for hacker to get access to the code, as they would need to crack several layers of our model.

IV. DESIGN AND METHODOLOGY

Knowing the camera's vulnerability in DAHUA technology, it is noticed that such IoT devices should be protected from diverse perspectives. It is not only needed to be improved from identification aspect, but also needed to be issued certain right so that it will be accessible or non-accessible by different type of users. Hence, learn from DAHUA's technical vulnerability and inspired by previous experiments [1], a five layer framework is designed in order to prevent malicious attacks.


Application layer
Business logic and Data exchange schema
Authorization layer
Membership service
Network layer
Multiple channels network(Sub networks)
Data encryption layer
Encrypted data, hash function (SHA256)
Physical layer
(Camera IoT devices' network)

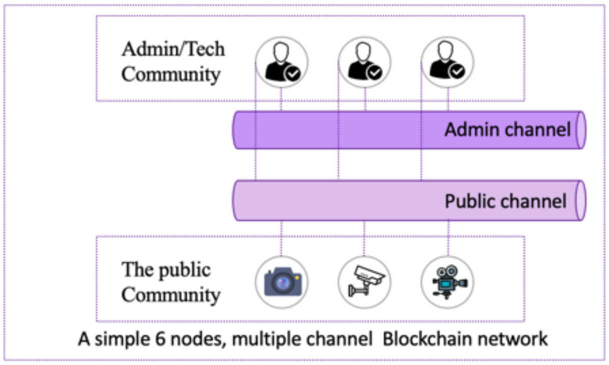
Five layer framework

It can be seen from the above figure that the bottom layer is physical layer. Data is generated in this layer. Each of device may has a small database to store user and device information. After creating user information, users may want to connect themselves to the network. So an identification mechanism is designed, user need to create a password with length more than 8 that contains both alphabet, numeric and special characters. Then the password is sent to data encryption layer, in this layer, password is stored in Hashcode, specifically in SHA256 format. The next layer is network layer, each IoT device (camera) is a node in the network. Subnetworks are also designed in order to provide private communication channel for different parties. Also, there is authentication layer where the membership service is designed. Each user is belong to one community. For example, software development engineer staff may belong to the DAHUA's staff community while a normal user may belong to the public community. By default, new user will be registered in the public community with the most standard permission level. If they want to promote their level, they need to get the consent of DAHUA's authorization department. At the top layer, business logic is designed, where we can give users permission in details. Such as, users cannot query data more than 10 times per minute.

Given this 5 layer architecture, it is suitable to apply Blockchain technology to the network. Blockchain is a decentralized system without a central authority which made the system even more secure. Hyperledger Fabric [2] system is chosen for its high availability, efficiency, and flexibility.

Each node in the network is a IoT device, they have different database with same information (ledger) stored in chain. So if one user want to request information, the user need to get the consent of all other users. If a small group of people created their backdoor account in their database, while other majority groups of people did not have the certain information, the user from small group will not get the consent of the majority user. Thus, their requests will be rejected. It is hard and time consuming to hack all the nodes from Blockchain network. So the possibility that user may successfully get information with a backdoor account is nearly zero.

The figure below shows the simple network architecture. There are two communities and two channels, users of the admin community can get the access to the whole network, where users belong to the public community can only get access to the public channel. Channel can also be interpreted as subnetwork. Moreover, The network is scalable. There can be multiple IoT devices and admins connect to the network. Before connection, user will need to be registered into the community, so he or she could have the pre-issued key to entry the network.

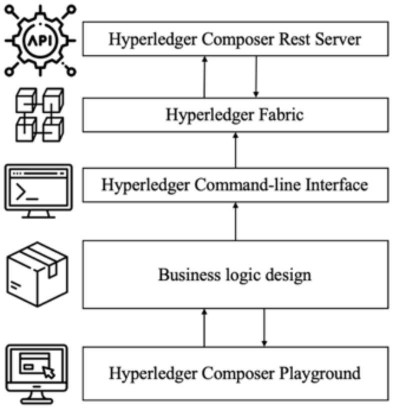


The Blockchain network

With the mentioned five layer framework, all the security vulnerability will be conquered. Detailed evaluation will be illustrated in evaluation section.

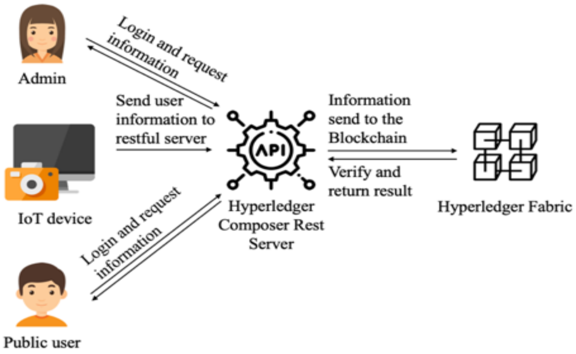
V. IMPLEMENTATION

The five layer framework is implemented through Hyperledger platform.
The figure below shows the major components used in the system.


API
Hyperledger Composer Rest Server
Hyperledger Fabric
Hyperledger Command-line Interface
Business logic design
Hyperledger Composer Playground

Major components used in network

Hyperledger Fabric is the main Blockchain system, each node has a database, in our case, each IoT device has a small database that store user's identifications and device information. The command line interface can be used to create sub network (Channel), add new node and users. The Hyperledger Composer rest server will connect with user directly to help retrieve corresponding and a key value pair will be generated and store in the system distributary. Each user will have to get a valid key to access to the network. The business logic is designed through a javascript liked language and stores in the top layer of the system . For example, the query limitation per user (10 query per minute) is designed here. All the interactions can be visualized with Hyperledger composer playground that installed on our localhost.


Admin
Login and request information
Send user information to restful server
Information send to the Blockchain
Verify and return result
API
IoT device
Hyperledger Composer Rest Server
Hyperledger Fabric
Login and request information
Public user

Data Flow

The data flow of our system is implemented as follow:

1. User register and send information to rest server.
2. Rest server receive the information and send it to Blockchain.
3. Blockchain check the user's membership information and verify its key.
4. If the key is correct and all nodes reach consensus, then return consent. Otherwise return refuse.
5. Every database in Blockchain will be updated, new log is appended to the ledger.
6. Rest server send corresponding result to the user.

In this way, user will have their information stored in the IoT network securely and privately.

VI. EVALUATION

Security and privacy

In the DAHUA vulnerabilities reports, hackers turned off the camera feed to the four channels and locked out access to turn them back on. There were changes made to color setting, general network, and channel name. For the system we designed, when an attacker wants to change information in one node, the attacker needs to ask for permission from all users. Once one of users finds this behavior is suspicious, the request will be rejected. Even if a group of users want to create a backdoor, they still need consent of users in other groups. All users need to pre-register and a valid key to enter the network.

In the DAHUA's records, some data was changed that caused the screen to go black, and the camera names were changed to Hacked 1, Hacked 2, Hacked 3 and Hacked 4. But for our system, all transactions will be stored in chain for every device, so if hacker want to modify one database, he has to modify all the database in order to reach consensus. Which is nearly impossible.

For the DDos attack, our self designed system will not allow more than 10 information query in a minute.

Time and performance:

By using the Hyperledger, we need less number of verifications and less layers of trust to across node types. It makes transactions happen faster without any effects.

Network Latency: Around 0.045s latency per transaction. Depend on the distance between different node and device used.

Transaction Validation time: Around 0.05s latency per transaction.

Scalability and Robustness

For higher performance, we can increase the population of endorsing peers and distribute load of endorsing proposals during the large set. We can use separate endorsing peers for different channels, which makes multiple channels executing concurrently.

VII. RELATED SOLUTIONS

1. A decentralizing IoT networks that established on Blockchain infrastructure is introduced in a blog [8].
   The decentralized platform overcomes the vulnerabilities and threats a traditional IoT

solutions may has. In an IoT network, the blockchain keeps an immutable record of the history and all transactions of smart devices. This feature allows the autonomous functioning of IoT devices without the need for centralized authority. Moreover, all the malicious behaviors will be recorded and rejected by the network.

2. Blockchain to protect video integrity [9] Blockchain is also the solution for preventing anonymous photos uploading and protect photo and video's integrity. Instead of Hyperledger, Bitcoin Blockchain Ethereum platform can also be used. Hyperledger is private platform which is good for a specific company like "DAHUA" while Ethereum is popular for its public features. The authors of the paper declare that "any subsequent attempt to manipulate the video is futile, because the hash of the manipulated footage will not match the hash that was secured in the blockchain. Using this approach, the integrity of video evidence cannot be contested."

VIII. CONCLUSIONS AND FUTURE WORKS

Our five layer framework of blockchain technology can definitely help to guarantee the security and privacy issue of Dahua. By utilizing the Hyperledger, we can easily manipulate our platform. Our data is guaranteed and we have provide private communication channel for different parties and make sure each user is identified as one community. We also have specific rules for the users. Therefore, It make sense to apply blockchain technology into our system because blockchain is a decentralized system without a central authority which made the system much more secure.

Though our five layer framework is good enough to satisfy the security issue of Dahua technology, we think of applying more layer in the system. We can also extend our network and setup more sub network. Also, there's no single blockchain that will solve every problem: Different types of blockchains are better suited to different needs and circumstances. We could also apply different type of blockchain into the system.

REFERENCES

[1] Blockchain: A Safe, Efficient Solution for Driver Privacy and Connected Vehicle Transportation Data Sharing by Yingxi Cao , Abdullah Kurkcu, Kaan Ozbay https://www.researchgate.net/publication/328202629_Blockchain_A_Safe_Efficient_Solution_for_Driver_Privacy_and_Connected_Vehicle_Transportation_Data_Sharing

[2]Hyperledger Fabric: https://hyperledger-fabric.readthedocs.io/en/release-1.3/

[3] Description of attacks/vulnerabilities: https://ipvm.com/reports/hack-dahua-recorders

[4] Cleartext passwords: https://www.cvedetails.com/cve/CVE-2017-6341/

[5] Blockchain and Decentralization https://lisk.io/academy/blockchain-basics/benefits-of-blockchain/what-is-decentralization

[6] Hyperledger Fabric-Byzantine Fault Tolerance https://medium.com/kokster/understanding-hyperledger-fabric-byzantine-fault-tolerance-cf106146ef43

[7] Buffer Overflow https://www.theregister.co.uk/2017/07/20/dahua_cameras_stung_by_web_interface_bug/

[8] How to Secure the Internet of Things (IoT) with Blockchain https://datafloq.com/read/securing-internet-of-things-iot-with-blockchain/2228

[9] SECURING VIDEO INTEGRITY USING DECENTRALIZED TRUSTED TIMESTAMPING ON THE BITCOIN BLOCKCHAIN http://www.sciplore.org/wp-content/papercite-data/pdf/gipp2016a.pdf