Certes Secret
Resected and Secreted

Nitin Kuncham, Sharath S Chellappa & Chetan Purohit

nitin.kuncham@gmail.com
sharusrikanth@gmail.com
chetan.6108@gmail.com

Abstract

Internet has become an integral part of life and this dependence on web-based operations is leading to increasing Cyber-crime. This increasing cyber-crime has brought about a regular compromise of Passwords, secrets, privacy data etc. The solution presented in this paper meticulously addresses each vulnerability of storage and retrieval of secrets / information. The secure storage of information is ensured by having an agency to go about resection, distribution of each piece across multiple locations and then the destruction of the distribution index from the agency. Layers of security are added to the retrieval mechanism (each step being a NP hard problem) and each layer being administered by a different agent. Breaking the system would require successfully compromising at least two of these statistically independent agents. In simple words, the adversary would be able to break in only if two or more successful attacks on independent agents are carried out.The system has been implemented to mobile / internet banking.

Introduction

Safe storage and retrieval of secrets have always been a topic for discussion among many scholars and researchers. Many solutions have been created only to engender a counter. This constant war between countermeasures and counter-countermeasures keeps playing out in the world of computers incessantly.

In 2012, tech-giant LinkedIn faced a serious issue with a data breach from one of its centers leading to secrets of nearly 6.5 million registered users to be leaked. Adobe too had a data breach of a much lower magnitude though, in the product of Lastpass, their very own password manager.

In the Banking Sector last year alone, multiple breaches were witnessed. Payday lender Wonga had warned nearly a quarter of a million customers that they may have been affected by a data breach. Around 245,000 customers may have been affected by the cyber attack in the UK, and 25,000 in Poland. Another incident involves cyber thieves stealing 81 million USD from the central bank of Bangladesh.

Increasing dependence on IT has necessitated strengthening and hardening of security measures for transaction over the network. This becomes absolutely critical for defence establishments like the IAF where almost every operation either needs to be authenticated or secure or both. The Core Solution developed by us can be applied to many aspects of cybersecurity in the IAF. The rest of the paper gives a brief of our system and discusses the various opportunities that can be explored.

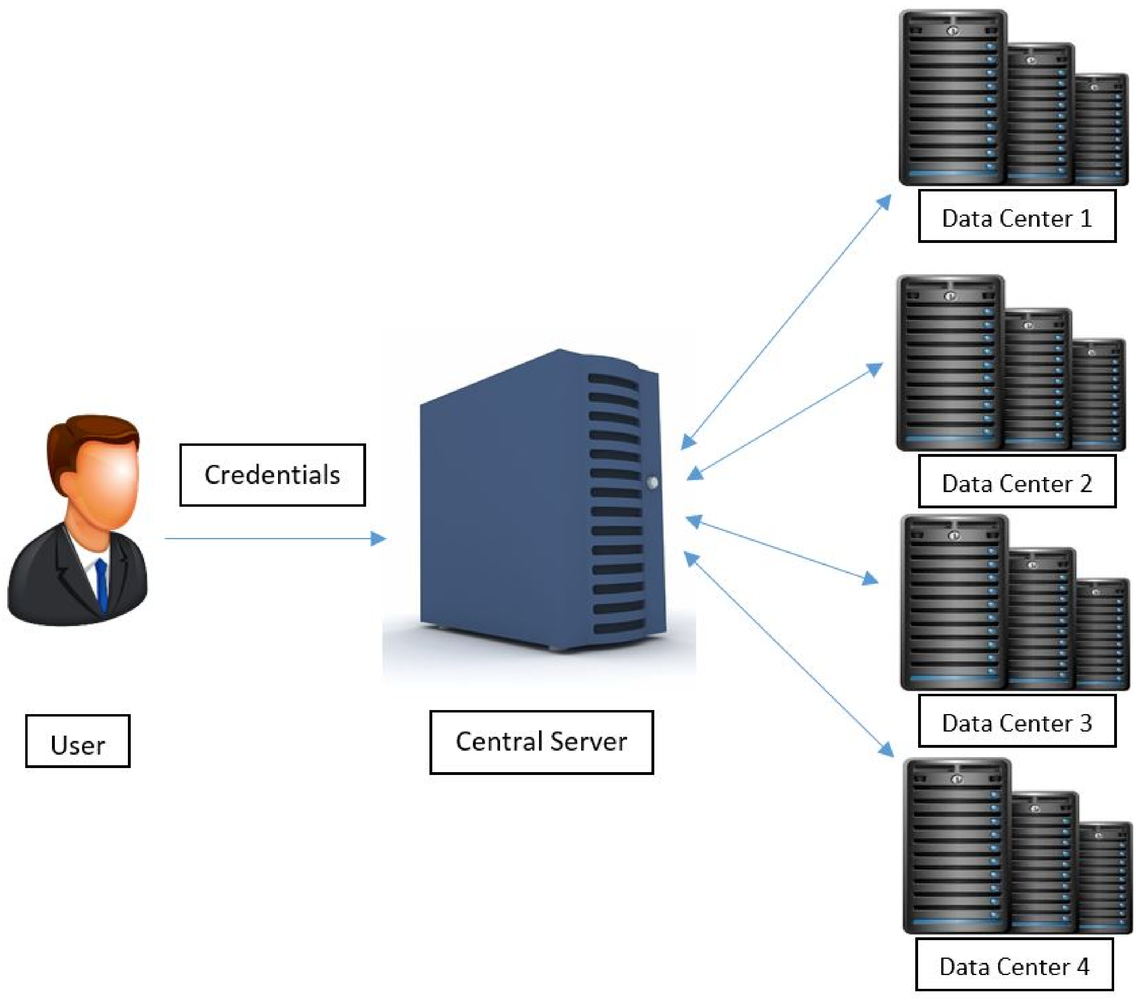
Objectives of the Core Solution

1. Design methodology ensures the following:
   - *Confidentiality*-Protect disclosure of secret by distributed storage by denying the adversary from stealing the secret with a single attack.
   - *Integrity*-Prevent modification of parts of independently secure secret; while ensuring the cryptosystem is resilient to modification of some parts.
   - *Availability*-Availability of information refers to ensuring that authorized parties are able to access the information when needed. Assuming an adversary blocks a data center, the property of integrity ensures availability.
2. Rigorous mathematical analysis of each subsystem to ensure compromise of any of them is computationally unfeasible. Compromise of each of the system components has been considered to ensure security of system over the entropy of the secret.
3. Device specificity can be added as an additional layer so that certain data can be accessed only through certain machines or specified devices.No other device can be used in lieu.
4. Avoidance of
   - Replay attack.
   - Denial of service.
   - Phishing/man in the middle attack.
   - Compromise of complete secret because of compromise of any system components.
5. Attacks by 'enemy within' is prevented by maintaining a memory-less central server.

Components of the Core Solution

The Core Solution can be adapted to meet various objectives.It has been demonstrated with a Proof of Concept for a representative banking system with a username and password.

The credentials entered by the User, during the first time, is taken and split into multiple parts called as "part secrets". These parts are then forwarded onto the Component Child Servers where these are securely stored in a tuple form. When the user enters his credentials subsequently, the pieces are securely retrieved from the Component Child Servers, and are combined to give a retrieved credentials. This retrieved credentials is compared with the user-entered password with access being granted if there is a successful complete match.



The Core Solution has 3 main system components which communicate through HTTPS are described below:

1. **User device**-The user enter his credentials into the cryptographic application to access the secret.The User device may be constrained to add an additional layer of security.
2. **Central Server**-The Central Server is a memoryless system which carries out the cryptographic operations.The Central Server is more of a processing unit than a storage unit. Once the operations are terminated, it contains no residue of the operations or the secret. It carries out 2 main functions:
   - Registration of user device to ensure device specificity by exchange of temporal and cryptographic information. Splits the secret and deposit the pieces in some of the multiple available servers and convey this information back to the registered device.
   - Operations-When the user enters his credentials through the registered device, it queries the set servers and matches the credentials and allows access the customer.
3. **Component Child Servers**- These are independently secured storage servers. They are maintained in data centers and hardened cryptographically. they return their part of the secret when queried by main server

Resilience

Traditional cryptosystems are well known and have many vulnerabilities as listed in appendix B. The proposed system has been designed to increase the resilience of every component of the system.

1. **Compromise of the User Device** Online hacking would be extremely difficult due to single threading of the Communication Process(not described hither to). No other device can be used to access the associated secret. OIf the device gets compromised, the device is of no use without the users credentials.
2. **Compromise of the Central Server**-It would also be difficult to break through the underlying Firewall and IPS. However even if the adversary gets access to the central server, he would be unable to retrieve any data pertaining to any of the secrets.
3. **Compromise of the Child servers**- These servers are independently Secured through firewalls. The part secret is stored in these child servers. The barricades the adversary has to break through to break the system:
   - Adversary has to bypass the firewalls and IPS.
   - Adversary has to figure out location of storage of part secret.
   - Adversary has to decipher the encrypted part secret.
   - The adversary will obtain only a piece of the secret and it will not reveal any more information about the rest of the pieces or the complete secret. Hence the secret is not compromised.

The solution can be extended from a password or a key management system to one which can be used in a Secure Document Storage Scenario. The Algorithm being implemented has multiple use case scenarios and in its current implementation and can be extended to a scenario emulating that of a board of Directors. Here the absence of a Director or his key would not pose a hindrance to the functioning of the committee due to the presence of the rest of the pieces. Another use case of this system can be seen in the activation of a nuclear warhead where there can be a requirement of multiple pieces of the distributively split activation code.

Proposed Application

Looking at our base algorithm and the current implementation, we have identified a few areas where are solution could help secure the day to day functioning of the Air Force. Some of these applications are as follows:

1. **Access Control** : Access to all systems can be done using a single credential which will be secreted in the core solution. This will ensure that all applications can be accessed only by the individual and if required only through his device. The system will not have any record of any credentials, thereby making it unbreakable.
2. **Multiple Authorization** : Assuming a situation where access to the resource is critical with the absence of one of the access granting parties, the core solution could help solve the problem. The Core solution enables access to the critical resource by allowing access when the number of password pieces generated by the algorithm crosses a given threshold set. This solution is highly useful while dealing with resources like Nuclear Warheads which need multiple levels of authorization but have a constraint on time for enabling in the event of a war.
3. **Document Access and Retrieval** : The Core solution will be able to target collaborative timebound access and editing. No third entity will ever be able to break into this system since the credentials will not be offered to him.

   An example of this implementation can be seen taking the scenario of a secure communication channel which needs to be accessed by 2 parties. Now by using the base algorithm to create pieces, sharing the memory locations of these pieces with the involved parties would allow usage of the secure communication line for a limited period of time. Lapse of the time period would lead to the memory locations being wiped thereby leading to access being revoked.
4. **Multi Password Multi User Single Real Time Access** : Considering the case of work scheduling, our solution could be used to manufacture multiple pieces of the key which are distributed to the agencies.

Conclusions

By considering every possibility of attack and trying to deal with it in asystematic manner, we have truly attempted to create an virtually unbreakable key management scheme looking to protect the secret holistically.
The proposed system has been implemented as a Proof of Concept for a Bank. Here we have looked to implement a cryptosystem where any one successful attack on the cryptosystem would never lead to its compromise. By reducing the importance on the Bank/Central Server, we have looked to eliminate the possibility of internal compromise by now using the Bank/Central Server as a processing unit rather than as a storage unit. The layers of security added at every stage of communication making the compromise an NP Hard Problem, provides for additional security.
A secret is only as safe as the place it is kept in. In this approach to security, we have distributed the locations where the secret is stored and then made it difficult to individually break each location. Further, we have ensured that at least two components have to be compromised in order to break into the system.
We would like to implement the system as a Proof of Concept so that we can understand and explore ways of providing security solutions to the Indian Air Force.