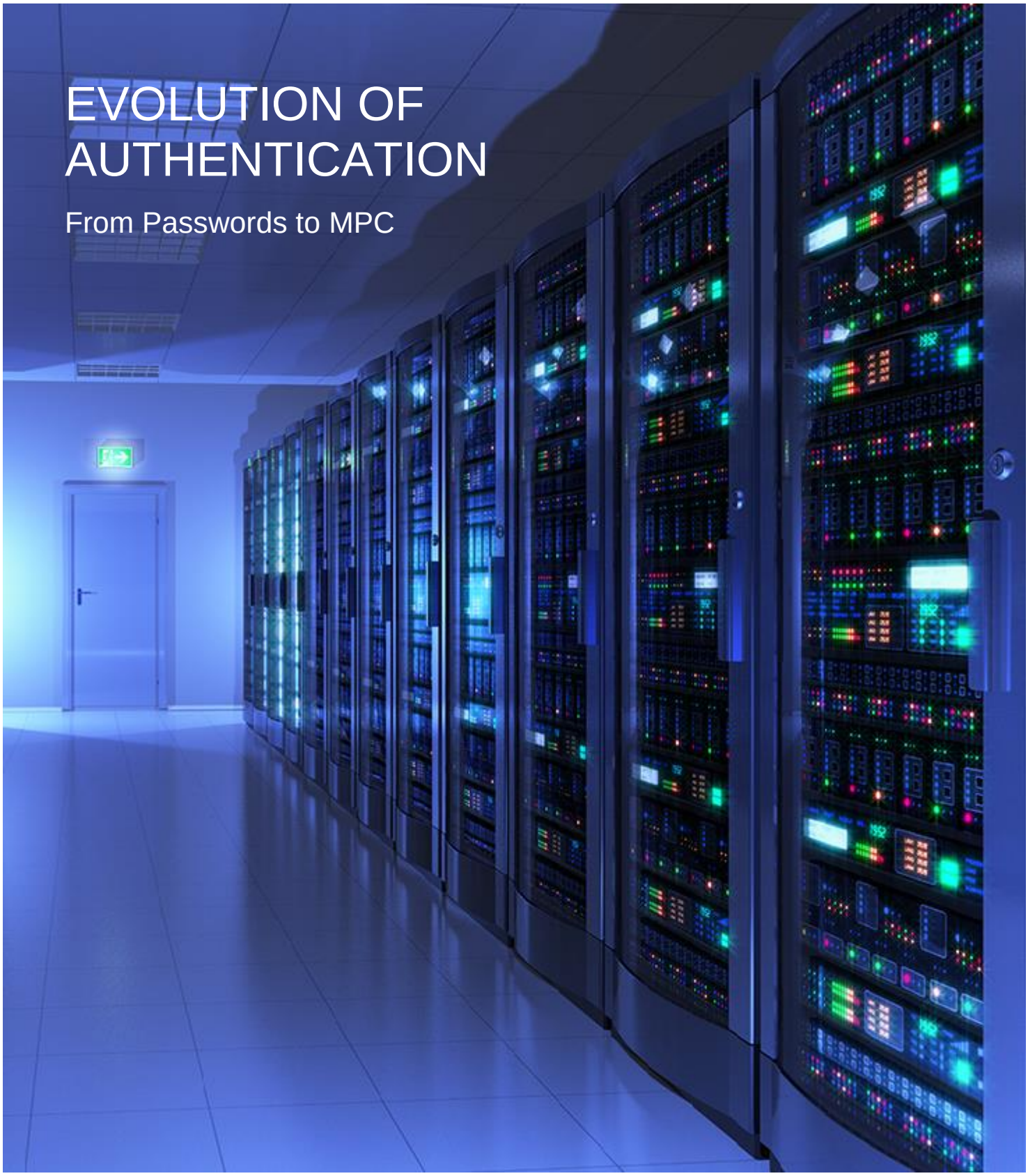
EVOLUTION OF AUTHENTICATION

From Passwords to MPC



RSM

WAR ROOM

Current Authentication Methods are not Secure Enough

Business assets have been physical for most of history. Protecting them has involved high fences, barbed wire and padlocks. With the emergence of the internet, the definition of business assets has expanded to include the mass collection and storage of digital data. As a result, digital data has become one of the most important resources a company can possess.

While data grew in importance, a new emphasis was placed on securing it. Traditionally, the most common way to protect an organization's data has been through the use of single-factor authentication, such as a unique password for login pages. Unfortunately, passwords have consistently proven to be a weak form of security. Data breaches occur on a regular basis, and often result in stolen passwords, personal information and even digital assets. To mitigate the risks of a data breach, organizations often employ two-factor authentication (2FA).

2FA requires a second piece of information, separate from a password, to be obtained before secured data is accessible. The most common form of 2FA involves the SMS text, which is sent once a user inputs their password, and usually contains a string of numbers. These numbers are then added to the login request, and verification is complete. The 2FA options available today (such as SMS texts) can still be points of weakness, and can provide an unwarranted sense of security to the user--if compromised, these factors can be used by a bad actor to lock an owner out of their account. Malicious actors have been known to remotely hijack phone numbers and obtain 2FA texts, rendering the whole system useless. This weakness, combined with the ever-present threat of a cyber-attack, has forced enterprise businesses to search for a more robust solution. One such solution is to use a Multi-Party Computation (MPC) protocol to help secure sensitive data.

Next Step in the Evolution of Authentication - Multi Party Computation

Since 1980, MPC has been extensively researched in the academic community, resulting in thousands of theoretical papers written on the topic. Due to recent advances in cryptographic research and computing technology, MPC has become practical to use in real-world applications.

MPC is a type of cryptographic protocol that distributes computation across multiple parties, where no individual party can see the other parties' data. MPC achieves this privacy through the use of secret sharing and homomorphic encryption, a type of encryption that allows individuals to perform calculations on encrypted data without decrypting it first. To prevent parties from cheating, an organization can enable zero knowledge proofs, which were created as a method for proving "correctness" without revealing underlying data. As such, zero knowledge proofs can be used by each participant in an MPC protocol to prove that they are behaving honestly and providing correct input, while keeping the input hidden from other participants. MPC protocols compute an output based on these inputs (which remain private to each party), which is then shared with all participants.

To illustrate how this works, let's discuss an example (Figure 1). John, Sarah and Jill want to know what their collective average salary is, yet none of them want to tell the others their salary for fear of having the lowest salary. Using MPC, each participant would input their salary without revealing what their salary was to the other participants, and the MPC protocol would tell the group what the average salary is. Each student would only know their own salary and the result of the computation (the average salary between the three individuals). In essence, MPC is a type of cryptographic protocol that allows multiple distinct parties or devices to collaborate without

revealing any unnecessary information. Most often, this occurs when parties do not trust each other due to fear of corruption or for fear that one of the parties could be breached. MPC would guarantee that any corrupted party would not be able to access or corrupt the information of another party.

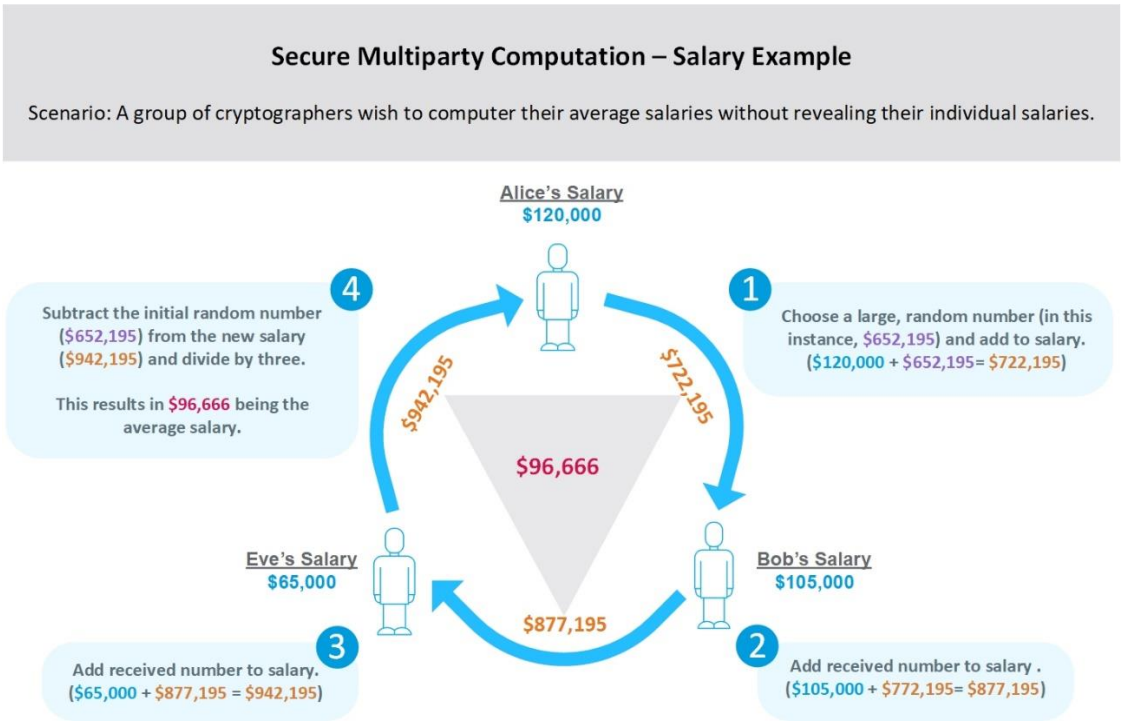


Figure 1: MPC example scenario

MPC Usage for Cyber Security

Using MPC protocols to distribute an authorization mechanism amongst multiple parties would vastly improve data security. A multi-party approval structure enhances security by creating a digital key, which is used to "sign," or authorize, a transaction that is distributed from its onset. This means that there is never a full key, either at generation or usage. The protocol accomplishes this by generating the key in a distributed manner and dividing the key-shares between approving parties. It is important to emphasize that there is no single key at any stage of the computation. Whenever an event needs to be authorized, the participants will submit an encrypted approval while running the MPC protocol. The protocol will use everyone's key-share to compute a signature, without needing the shares to exist in a single location. Distributed generation of the private key-shares effectively eliminates vulnerabilities that are associated with shares existing in one centralized location.

This can be illustrated using the following example. Suppose that a digital key spelled out the phrase, "MPC is powerful." This phrase would never be assembled or re-assembled in a single location (on a single server). Instead, when the phrase is created, each party would receive one encrypted word (or letter, depending on how many parties) of the phrase as their share of the total. Whenever an authorizing or signing event needs to occur, such as authorization to access a bank account or send a digital asset, each party will use their share ("MPC" or "Powerful") to submit an encrypted approval to the protocol for computation. The encrypted share approvals are the computational inputs. Once all encrypted approvals have been submitted, the protocol will compute the approval function and produce an authorization signature if the inputs are valid. Each party is never exposed to the other inputs (the other encrypted words). Therefore, no participant is able to see that the full key is "MPC is powerful"; the participants only know their part of the phrase, and as long as the protocol proves it, the inputs from all other participants are valid.

MPC, how does it work?

For those readers with a background in cryptography, this cryptographic protocol might seem similar to another cryptographic protocol called Shamir's Secret Sharing Scheme (SSS). Although SSS and MPC are both ways to cryptographically distribute the shares of a key, they are different in how each system distributes the shares. When using SSS, the key has to be created in its full format, which results in a single point of failure. Only after it is created in its unencrypted form will the key be distributed. Whenever an event requires an authorization or signature, the SSS key-shares will be reassembled into the full unencrypted key, again creating that single point of failure. With MPC, the private key is never assembled unencrypted in a single location, even when shares are being used to authorize the event.

In the event of a security incident, such as hacking, strong MPC protocols create an additional layer of security. Unlike standard SSS, in which each piece of the authorization mechanism is static and unchanging, it is possible with MPC to periodically change (refresh) the share, and the weight of the share compared to the remaining shares, so that it is not static. This is important, as it prevents an attacker from slowly obtaining shares one at a time. In particular, because the shares change periodically, an attacker would have to simultaneously steal all shares in order to obtain any information.

For example, if SSS was used to distribute a cryptographic key between three parties, each party would control 33.33% of the whole key. Using this kind of infrastructure leaves keys vulnerable to "slow breach" attacks, in which malicious actors slowly accumulate access to each of the key parts until full control is obtained. A slow breach attack is only possible because any compromised piece is under control of the malicious actor, which provides them with additional time. Using an MPC protocol, each key-share becomes refreshed after a fixed interval of time (e.g. every hour) or after an operation takes place. After the time interval has elapsed, the protocol will regenerate shares with a slightly different weight or value (going from 33.33% to 35.77%). The time interval refresh, as well as the encryption of all shares from their creation, means that a malicious actor would need to hack all shares within the time interval to gain access to sensitive information. Encryption, distribution and refreshing shares make MPC an incredibly secure protocol. It is important to note that MPC can be implemented without the share refresh function. If a company were to do this, they would only eliminate the single point of failure threat present with SSS. If there is no refresh function, a malicious actor could still slowly collect key shares over time.

Apart from its distributed design and the constantly changing share value, MPC has the advantage of flexible implementation. Every business is different, and segregation of duties is a cornerstone of physical and virtual security. MPC allows businesses to distribute the duties associated with an authorization approval across multiple parties within a variety of organizations. MPC shares can be held by any party, either in a virtual or physical hardware security module (HSM). HSMs are physical computing devices that safeguard and manage keys, and perform encryption and decryption functions for digital signatures. These devices traditionally come in the form of an external device that can be plugged into a computer or network server.

MPC protocols also allow for almost anyone to assume a party within the ecosystem. Parties can be people within the organization or a software bot that approves or declines a transaction based on an automated algorithm or artificial intelligence. A party could also be an external, trusted third party. Furthermore, the approval process can be done in one phase or in multiple and sequenced phases, requiring certain parties' approval before others. Sufficient data security practices call for the segregation of duties between the approval initiator and the approver. This process can seem cumbersome, but for certain less complex steps such as a KYC or AML check, the approval process can be automated. This automation assists in smoothing the approval process, and improving efficiency.

Therefore, it is easy to establish a secure, multi-party, cryptographically validated and compliance-ready approval process with MPC. For example, a policy of multiple approving parties could consist of three groups, a total of nine possible signers and a policy of five of nine signers for each transaction. The signers could either be humans or artificial intelligence, and external or internal signers.

Finally, it's important for any business to make sure that shares can be recovered in a disaster or significant loss. In the event that one party is corrupted, having access to a backup share is critical to an organization. Backup shares can be stored in offline servers, or with trusted third parties, and be accessed whenever necessary. Recovery would require a strong policy, designed to prevent the key recovery process from becoming a point of weakness. It is recommended that recovery keys are stored in an encrypted offsite backup storage facility. This way, the recovery will be insulated from both cyber and physical attacks. MPC share backup is an essential feature of any good MPC protocol.

Use Cases

MPC is often associated with digital asset security and secure transactions, but there are other uses for this protocol. These uses include secured authentication, phone-as-a-keychain, virtual HSM (vHSM) and password-less authentication.

Secured Authentication

One specific use case for MPC technology is that it enables the most secure form of authentication. Secured authentication is the cornerstone of data security and relies on the two-factor password and SMS text structure. This system depends on authentication from "something you know" (SYK) and "something you have" (SYH).

SYK is a password that only the individual knows, and SYH is the phone that receives the SMS text. SYK is less secure than SYH, because SYK can be replicated multiple times and accessed in multiple ways. Consider the many places in which passwords are stored. Unlike SYH, SYK is stored in a central location, such as a company's server, which significantly decreases its level of security. SYH is stored only with the individual—because the physical nature of something one owns is difficult to compromise, SYH is therefore more secure (though still vulnerable to theft and hacks).

The most secure form of authentication is using "something you are" (SYA), such as a fingerprint or a retina scan. These types of authentication mechanisms cannot be stolen or accessed remotely by a third party. The highest level of secure authentication would involve using an MPC protocol combined with multi-factor-authorization, leveraging SYH as the first factor and SYA as the second factor. Each key share created through MPC would be protected on any device by SYH and SYA.

A MPC multifactor structure designed in this way would provide what the National Institute of Standards and Technology would describe as "hard" cryptographic authentication, which offers impersonation resistance verification. MPC is extremely secure and fully adheres to the SYH requirement.

Phone as a Key Chain

With the emergence of smartphones, these mobile devices have become an integral part of our daily lives. As such, they have become the default hardware that sensitive, valuable information is stored on. Phones are often a point of entry for bad actors. If a phone is stolen, any password stored on it can easily be accessed and used wherever the password is accepted. Companies have gone so far as to prevent employees from using phones because of their associated security risks.

Using a MPC protocol allows parties to store a share of the private key on their phone without the fear of an account being compromised if the phone were to be stolen. This is because the information an MPC share protects cannot be used in isolation.

Storing one of the key shares on a phone also allows the party to approve an authorization from anywhere the phone is. The phone serves as an additional factor of authentication, replacing the old hardware token and enabling a multi-factor authentication and approval process that relies on biometrics and the key share (MPC).

One example of this would be granting access to a door. The door lock could host (via a micro-server) a key share and a person could hold another key share on a mobile device. Both pieces of information would need to be provided to unlock the door. Key shares could refresh and update the means by which a party accesses the share, such as switching between a finger print and face ID. As with all MPC models, this creates a heightened level of security while giving people the flexibility to be anywhere and approve an authorization.

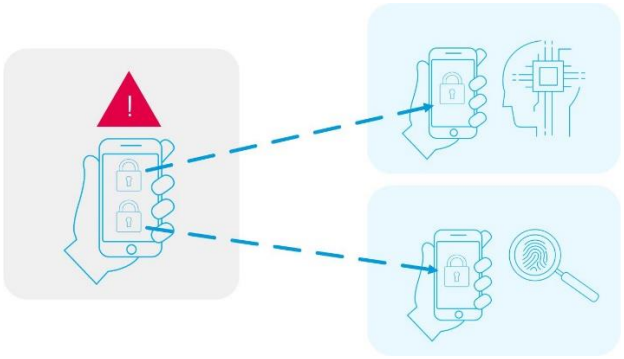


Figure 2: Multi-factor authentication with both SYA and SYH

vHSM

Another significant use case for MPC technology focuses on replacing our reliance on hardware as a hard-cryptographic identifier. In current enterprise applications for public or private key management, most companies utilize a physical HSM. These HSMs are physical computing devices that safeguard and manage digital keys, perform encryption and decryption functions for digital signatures, and provide strong authentication and other cryptographic functionalities. In physical HSMs, there remains limitations related to the following:

1. Reliance on physical hardware as a cryptographic identifier.
2. High capital and operational expenditures associated with the shipping, deployment and maintenance of hardware-based modules.
3. Lack of availability to use biometric identifiers as an inherit part of the solution.
4. The underlying encrypted key stored within the physical HSM still constitutes a single point of failure.
5. The secure element is hardware based only.
6. The confidentiality of the key is protected but its usage isn't. With use cases such as digital assets, the usage is enough to steal all assets, therefore making this single point of failure very significant.

One of the ways to most effectively leverage MPC in order to assure best in class security, is the use of an MPC-based vHSM solution. vHSM's are virtual hardware security modules, which come in the form of digital suites. Companies can then leverage these suites to securely store their passwords or digital keys. An MPC-based vHSM can provide the same level of security as an HSM, with the added ability to scale with an organization and easily authorize or revoke HSM ownership rights.

MPC-based vHSM technology solves for the traditional HSM limitations in the following manner:

1. MPC technology places reliance on mathematical proofs instead of hardware as an identifier. In addition, it allows for identity binding on any device by allowing for any participant to "Bring Your Own Device," with no hardware required.
2. Biometrics are an available option for identification as part of a multi-factor, software based authentication.
3. The private key never exists in a single assembled form using MPC technology, with the key inherently decentralized.
4. The secure element is software-based, allowing for greater flexibility and lower operational and capital expenditures.

Although MPC does solve for many of the above limitations of physical HSMs, it is important to note that there are added considerations related to software storage and maintenance. The servers in use should be wholly owned by the underlying company implementing MPC, since reliance on cloud-based servers can present other vulnerabilities that are not present in physical HSMs.

Go Password-less

The next significant use case for MPC technology is focused on providing the ability for entities to secure and simplify the process of using passwords. Password based authentication can be cumbersome and

frustrating to users due to the necessity of memorizing passwords, as well as the procedure for resetting passwords when they have been forgotten. The process of resetting passwords is what exposes many individuals and entities to malicious hacks. Passwords can also be stolen from individuals if their underlying platform is hacked or if key-logging malware is in use on their device.

MPC technology solves these issues by providing a robust, user-friendly experience without compromising security. MPC technology never requires the password to be created or used in its full form, and instead creates two separate, random shares. One of these shares is held on the user's mobile or desktop device, and the second share is contained within a secure server. As in every MPC implementation, these shares are completely isolated from each other and never combined at any time (as with SSS). MPC hides the password from the end-user, while still using it to authenticate to the application server behind the scenes. The password never appears in plain text, even when in use, and it is also never cached by the platform it is used for. This means that malicious actors that hack a platform for user information, or deploy malware on individual's computers can never obtain the password.

In addition, the solution is implemented directly on a mobile application with no changes to the backend of the application, which renders its implementation simple with a short time-to-market. MPC-based password management also allows for the use of any choice of authentication, PIN, Swipe, FaceID and other biometric options.

Signing a Transaction

Finally, the MPC protocol can allow a party to sign a transaction without having to reassemble the private key. To do so, each party uses their encrypted key-shares to authorize any particular transaction. The authorization process contributes key material from each share individually to compute and decrypt the full authorizing signature. Each share must contribute their encrypted key-share to approve a transaction when using an MPC protocol. The protocol allows for signatures to be obtained without revealing the key shares to other parties or assembling them in a single location. Companies using digital assets would find this especially appealing, because they are able to send digital assets without compromising the private key.

Advantages of Enterprise grade MPC

MPC is the next advancement in secure key management and transaction authentication and approval processes. MPC protocols eliminate single points of failure, offer improved enterprise grade, mathematically guarantee security and drastically enhances scalability.

Enterprises will continue to adopt digital assets, which will begin to not only represent newer forms of value, but also serve as more efficient ways to track and exchange traditional forms of value, such as real estate. In order for enterprises to scale the diversity of digital assets that will exist on various blockchains, they will need a security platform that is adaptive and platform agnostic.

MPC protocols have the unique ability to provide a multi-party cryptographically validated approval engine. Traditionally, there has not been a means by which to achieve a distributed validation of a rules engine, only a centralized authority to validate rules. Using enterprise grade MPC, there is a requirement to use a multi-party cryptographic validation rather than a centralized validation process. Therefore, there is no longer the need to rely on a centralized application rules engine. Enterprise-grade, MPC based solutions assure that multiple parties, each holding a key share, submit approval without relying on any centralized authority to validate the event.

MPC, while being complicated mathematically, is easy to use. With enterprise grade, MPC-based solutions that are platform agonistic and client agnostic, the approving user does not need to hold any hardware token, remember any password or enter any one-time-password (OTP). The usage of the key-share is seamless to the end user, and is as easy as clicking a button (that triggers the usage of the key share).

Drawbacks of MPC

As with any newer technology, while the benefits may take the spotlight, there are always drawbacks and limitations that must be considered. MPC technology is a novel solution that obfuscates a lot of complexity on the backend to achieve a scalable, secure and

private key management solution. One of the inherent issues of this is the complexity itself—while it may provide a robust solution, it can be difficult to understand and comprehend. This effectively limits some of its ability to move quickly to market.

There are also strict limitations in regulatory requirements when implementing MPC technology at large enterprises. Many of the largest banks in the U.S are required to maintain level 4 HSM security, which specifically requires that the HSM be physical, not virtual or software-based. While it is possible to implement MPC using physical HSMs, much of the value proposition on speed of use is based on transitioning away from hardware-based HSM and pivoting towards vHSM.

Most importantly, one of the most significant limitations of MPC technology is that it requires online connectivity by all participants to execute a digital signature or password. Since all participants are always required to be online and every piece of action using MPC requires computationally heavy zero knowledge proofs and random number generation schemas, this results in a higher computational cost compared to plain text computation. This challenge can be addressed during deployment with the structuring of offline parties in parallel to online parties, but still the challenge is still valid.

While these limitations are important to understand, the potential of MPC and its ability to greatly enhance data security make it a powerful tool. Now that an MPC protocol has become practical, multiple companies have begun to provide services both implementing MPC infrastructures and providing custody services utilizing the technology.

Unbound Technology

Given the nascent nature of MPC technology, there are few competitors in the space that are offering these solutions on a commercial scale. One of the premier companies that specialize in deploying MPC solutions is Unbound Technology. Unbound is founded on the premise that key orchestration security and operational efficiency are paramount. Unbound's MPC technology, developed by leading academic cryptographic researchers in the field of MPC, bridges the security-usability gap, while streamlining processes for businesses across the globe by providing enterprise-ready solutions that protect an organization's most critical asset: information, identity, and financials.

Unbound is primarily focused on selling licenses of their MPC technology, including capabilities to assist with integration and deployment alongside a network of premier enterprise partners. Unbound has integrated their MPC solution with some of the most successful Fortune 500 enterprises, counts investors such as Goldman Sachs, Citi Ventures, and Innovation Endeavors, and are partnered with firms such as IBM, AWS, Microsoft, Oracle, Salesforce, VMWare, and more. While Unbound has numerous large enterprise clients, their technology is equally designed and priced to fit any sized business ranging from small to large-cap.

As more middle market clients begin to explore the benefits of cutting edge security and operational solutions such as MPC, RSM is well equipped to assist clients with the necessary education, design and deployment of MPC solutions leveraging Unbound's software.

Conclusion

Whether you're a company who is interested in improving your data security or an emerging technology company wanting to more securely store your digital assets, implementing an MPC protocol serves as a means for accomplishing that goal. MPC protocols leverage distribution, cryptography, and share refreshing to increase security. It is easy to use and flexible allowing for almost anyone, regardless of technical ability, to interact with it. As businesses grow and expand into new areas, they will need to have a security infrastructure that can keep up with rapidly growing technology expectations. MPC scales with any business and eliminates a significant amount of friction involved in the current data security practices. RSM makes sure our clients have access to the best possible data security solutions. In leveraging relationships with companies like Unbound, RSM can provide best in class data security services and help clients stay ahead of potential data breaches.

Sam Auch (sam.auch@rsmus.com)
Bennett Moore (bennett.moore@rsmus.com)

RSM US, National Blockchain and Digital Assets Team