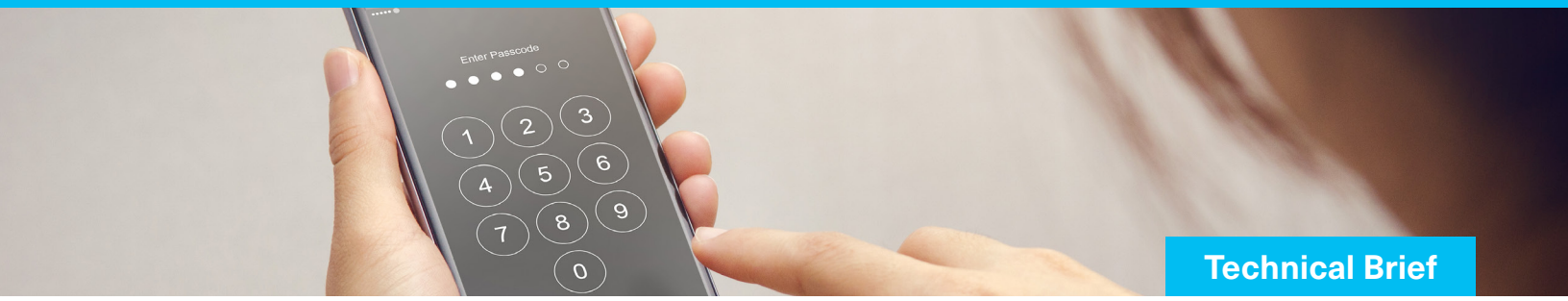
KIOXIA



Technical Brief

Introducing Replay Protected Memory Block (RPMB) within the e-MMC and UFS Specifications

Protects Against Replay Attacks / Pre-Programmable to Address a Variety of Preventative Smartphone Use Cases

Overview

Smartphones have become our lifeblood. There are billions of smartphone users globally and that number is expected to grow. Of today's smartphone users, most will probably say that they cannot live without them. They store confidential and important user information, and it's where sentimental content, transactions, contacts, schedules and a host of personalized information and applications reside. Protecting user content from being accessed by unauthorized personnel remains a priority to manufacturers of smartphones and other devices that store user data.

Typical smartphone access is by way of password or fingerprint authentication, while more advanced unlocking options include table sequence pattern authentication and biometric authentication such as facial and voice recognition, and iris scanning. The future looks promising as artificial intelligence and machine learning technologies will deliver smarter algorithms and sensors to help reduce false entries by unauthorized users and block spoofing attempts.

In the interim, the embedded Multi-Media Controller (e-MMC) specification[1] supported by NAND flash memory provides a high level of smartphone access protection that not many system and storage architects are familiar with. First introduced in the e-MMC v4.4 specification, with continued support up to version 5.1, the 'Replay Protected Memory Block' (RPMB) feature enables smartphone users to store and access private, important data in a small, specific **partition** area within the device. This area requires authenticated access and is designed to protect against replay attacks (discussed later). It acts similarly to a digital safe and uses an advanced authentication process to prevent unauthorized device access. The RPMB partition is also supported by the Universal Flash Storage (UFS)™ specification[2] and available within the majority of the Android™ OS-based smartphones used today.

Though the RPMB feature protects against replay attacks, it can solve many other problems and create innovative smartphone use cases as it has its own security protocol - and set of commands and instructions that can be programmed. This enables smartphone manufacturers to customize the 'RPMB partition' before a device ships. Understanding how the RPMB feature works and how it is currently used can provide smartphone development teams (architects, developers, engineers, product managers, etc.) with a jump start in pre-programmable ideas on how RPMB can be utilized to create even more compelling smartphone use cases.

What is a Replay Attack?

A replay attack occurs when a cybercriminal eavesdrops on a valid data transmission between two parties, intercepts the transmitted message, and is now in a position of resending it in the future for malicious, fraudulent or personal gain. Since the intercepted message is authenticated between the two parties (with sender and destination identifiers and encryption established), it looks like a legitimate correspondence that the attacker can re-use without suspicion.

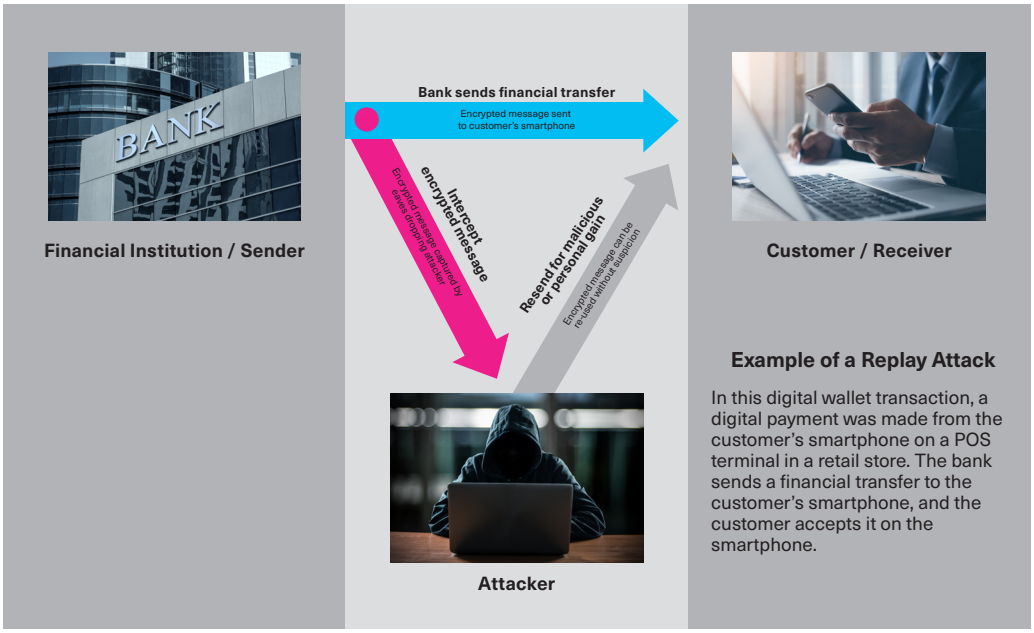


Figure 1: Example of a replay attack involving a financial transfer

A good example of a replay attack is a digital wallet transaction where a customer makes a digital payment from their smartphone. In this example, it could be on a POS terminal at a retail store. The bank sends an encrypted financial transfer to the customer's smartphone, where the transaction is accepted. During this transfer, an attacker intervenes by hacking into the communication channel between the bank and customer. As the bank sends the transaction to the customer's smartphone, the attacker captures the transmitted authenticated message. Capturing this message enables the attacker to transmit it to another phone for personal gain, in which case, could be re-used to send money to the attacker's bank account or to maliciously invoke a virus that could hack the financial system (Figure 1).

Protecting Smartphones from Replay Attacks

The RPMB feature within smartphones can withstand replay attacks by requiring a key (password authentication) in order to gain access. The password is used to generate a message authentication code (MAC) that resides in both the host and in the e-MMC or UFS devices. The password is pre-programmed in a secure environment (such as in the smartphone manufacturer's production line). Both the host and the e-MMC or UFS device **MUST** have the same key programmed, which essentially creates a pairing between the two devices. An example of a write to the RPMB partition by the host now follows (Figure 2):

Step 1:
The host reads the authentication key and write counter, and generates a MAC to the e-MMC or UFS controller.

Step 2:
The e-MMC or UFS controller reads the authentication key and write counter, generates the same MAC, and then compares the two MACs to see if they are identical.

Step 3:
The host-generated MAC is compared to the e-MMC or UFS controller-generated MAC, and if the two keys match, write access to the RPMB partition is granted.

Step 4:
A write counter appends after each RPMB write to keep track of the current write number to the RPMB partition. This means that if a hacker gains access to the MAC, they cannot use the same MAC in a replay attack because the write counter has incremented and the MAC that was based on an older write count will no longer match.

RPMB Authenticated Write Access Process

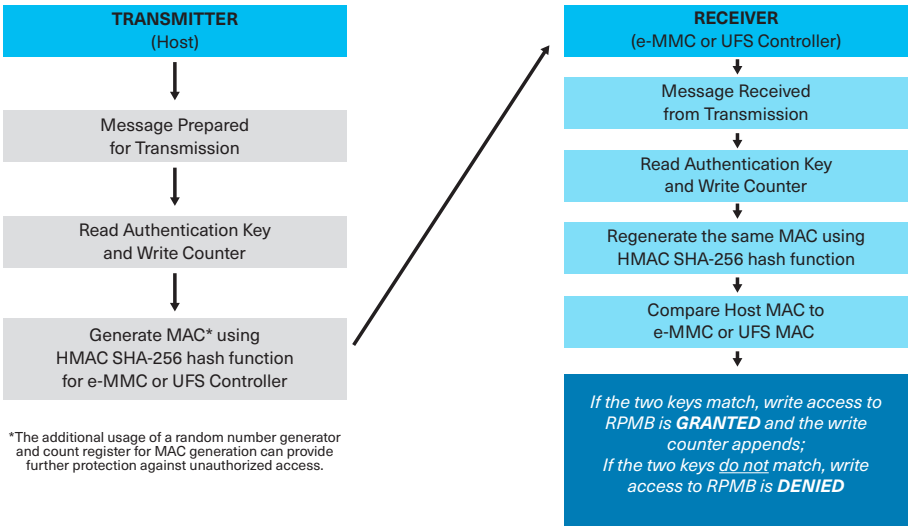


Figure 2: The RPMB Process

This authentication process enables important and confidential smartphone content to be securely stored in the RPMB partition, blocking 'replay attackers' from intercepting encrypted messages, and then resending them for malicious, fraudulent or personal gain.

Smartphone Use Cases for RPMB

In addition to replay attacks, there are a number of use cases for which the RPMB partition can be pre-programmed to meet a variety of smartphone challenges. A few that are in practice today include:

Preventing Stolen Phone Access

The RPMB feature is used to store a sequence of locks through the Hardware Abstraction Layer[3] (HAL) that provides Android-based smartphone manufacturers with further device protection in cases when the smartphone is unlocked, locked or unlockable. In this scenario, the smartphone uses HAL to pass commands to the boot loader, which in turn analyzes the commands the next time that the smartphone is booted and determines if changes to the locks are required. Since the lock sequence is securely stored in the RPMB partition, if the smartphone is stolen, this safeguard prevents the device from being accessed or reset, keeping user content secure.

Preventing Unauthorized Biometric Access

A smartphone user records PIN codes, fingerprint authentication and swipe sequences as access methods to unlock their device. Some phones feature facial recognition. For fingerprint authentication as an example, the fingerprint database template and the user's fingerprint data are stored in the device's RPMB partition using AES-256 encryption to prevent the leak of the fingerprint encryption key and the users' fingerprint data. Unless the hacker physically has the user's fingerprint data, unlocking the device becomes almost impossible since they cannot override the tracking of unlock attempts (or the physical number of attempts) because that data is also securely stored in the RPMB partition.

Whenever someone attempts to unlock the smartphone, the actual time of each attempt is recorded in the RPMB partition. If too many attempts are made within a specified period of time, the software that controls the lock will prevent further attempts to unlock the device for a set period of time.

Preventing Software Anti-Rollback

The RPMB feature is used in two preventative areas of software anti-rollback (also known as software downgrade prevention). Software anti-rollback is usually part of the verifications that are performed during a secure boot and a mechanism to prevent an older software component that contains a security bug in a smartphone from being reinstalled and executed when a newer software component version that fixes the security bug has been installed. In this scenario, a security revision number is increased for each security-sensitive bug that is corrected.

One way to address the increase in security revision numbers is to keep a table that contains the highest security revision for each protected software component that has been installed on the smartphone. This 'anti-rollback table' can be securely stored in the RPMB partition where the integrity of the table cannot be compromised. Integrity-protected reads and writes to the RPMB partition require a key that is shared between the e-MMC or UFS specification and the trusted computing base (TCB), guaranteeing that non-trusted software cannot tamper with the content in the RPMB partition.

The second preventative area of software anti-rollback is when software updates are pushed to a smartphone. The new software release uses the RPMB partition to protect itself from a downgrade attack by checking for a new, updated version number during the upgrade procedure. If the new version number is lower than the one that is already present in RPMB partition, the installer would reject the update, preventing the previous update from being installed. Due to the nature of the RPMB partition design, there is no way for an attacker to change the software version information that is stored in the RPMB partition, as that requires a password authentication key in order to gain access.

Summary

The Replay Protected Memory Block feature within the e-MMC and UFS specifications enables smartphone users to store and access personal and important content in a partition within the device that requires authenticated access. Though designed primarily to protect smartphones against replay attacks, it also prevents access to stolen phones, unauthorized biometric access, software anti-rollbacks, and downgraded software from being installed.

Future use cases could include storing personal and confidential medical and financial information onto your smartphone's RPMB partition, not only for heightened data protection, but also for scanning, reading and/or accessing the information in real-time, whether you are in the doctor's office, at a bank or some other location. For many of us who have an untold amount of passwords and logins for subscribed services relating to work and personal activities such as video streaming, social media, online shopping, internet, travel and entertainment, and more, storing these keys in the RPMB partition would provide an additional layer of security. Though smartphones are somewhat protected by login authentication using a password, thumbprint, facial recognition, etc., once access is hacked, the login passwords are unprotected and available.

With its own security protocol, and set of commands and instructions, the RPMB feature can be pre-programmed in secure manufacturing facilities before a new device ships, enabling many other potential applications covering personal computers, automotive, healthcare, financial and IoT / IIoT markets.

NOTES:

1 The embedded Multi-Media Controller (e-MMC) v4.5 specification is the current release by the Joint Electron Device Engineering Council (JEDEC®) and published in June 2011.

2 The Universal Flash Storage (UFS) v3.1 specification is the current release by JEDEC and published in January 2020.

3 The hardware abstraction layer (HAL) is an interface and layer of programming that allows a computer operating system (such as the Android OS) to interact with a hardware device (such as a smartphone) at a general or abstract level versus at a detailed hardware level.