Slik Photos Encryption Overview

Technical White Paper

Version 1 Published Oct 18, 2021

Contents

Introduction

Slik Photos is an end-to-end-encrypted photo collaboration platform. It allows users to collaborate on photos while the photos remain end-to-end-encrypted. Slik Photos also provides an end-to-end-encrypted and geo-replicated photo storage service to ensure that the users can always access their photos. We also enable users to search their photos locally without sharing any data with anybody. We start by describing our threat model and then describe components of our security and privacy system.

Threat Model

We consider a powerful adversary that can eavesdrop and corrupt all network communication between the clients and between the client and Slik servers. Such an adversary would be able to control local networks (e.g., owners of wireless networks or administrators of enterprise networks) as well as large segments of the Internet (e.g., a nation state). Our threat model also treats Slik Photos and its service providers as adversaries to ensure that they are unable to see any plaintext client data.

Security by Simplicity

"*The worst enemy of security is complexity. This has been true since the beginning of computers, and it's likely to the true for the foreseeable future"*

- A Plea for Simplicity: You can't secure what you don't understand.
Bruce Schneier, 1999

Slik Photos core innovation is a set of simple cryptographic protocols that exclusively use symmetric encryption. We worked hard to simplify our protocols so that they are easy to understand, analyze, and implement. Our simplified protocols were designed to achieve privacy at scale, which along with our meticulously designed distributed system, enable Slik Photos to scale to virtually any number of users.

Cloud Storage

We store all photos end-to-end-encrypted in the cloud with keys that only exist on your devices, therefore, nobody other than you, and people you share your photos with, can

access the decrypted photos. We store the encrypted photos on the cloud in a geographically replicated fashion to ensure your photos are safe and always accessible. We describe our cloud storage protocol below:

Protocol 1: Cloud Storage Protocol

We use `orange` for keys, `red` for plaintexts, and `green` for ciphertexts. All keys are 256-bits.

User Key Generation

1. The client generates a uniform random `User Key`.

Album Upload

1. The client generates a uniform random `Album Key`.
2. The client encrypts the `Album` with `Album Key` using symmetric encryption to obtain `Encrypted Album`.
3. The client encrypts `Album Key` with `User Key` using symmetric encryption to obtain `Encrypted Album Key`.
4. The client uploads `Encrypted Album` and `Encrypted Album Key` to the Slik server.

Album Download

1. The client downloads `Encrypted Album` and `Encrypted Album Key` from the Slik server.
2. The client decrypts the `Encrypted Album Key` with `User Key` to get `Album Key`.
3. The client decrypts the `Encrypted Album` with `Album Key` to get `Album`.

Photo Collaboration

We allow users to share albums of photos with other users and allow them to view and edit the photos in the shared albums. Every album is encrypted with an `Album Key` that only exists on the user device(s). To share an album with another user, the user needs to share the `Album Key` and the `Encrypted Album`. The `Encrypted Album` is shared directly through the Slik server. However, the `Album Key` only exists on the user's device(s). We encode the `Album Key` as a QR code and share the QR code physically or using an end-to-end-encrypted messaging service, such as, WhatsApp or Signal. We describe our photo collaboration protocol below:

Protocol 2: Photo Collaboration Protocol

Suppose a user Alice wants to share an album with another user Bob. They will proceed as follows:

1. Alice shares `Encrypted Album` with Bob using the Slik server. The album is encrypted with `Album Key`.

2. Alice will generate a one-time `Sharing Key` and encrypts the `Album Key` with `Sharing Key` using symmetric encryption. Alice shares the `Encrypted Album Key` with Bob using the Slik server.

3. Alice encodes the `Sharing Key` as a QR code and shares it with Bob either physically or using an end-to-end encrypted messaging service, such as WhatsApp or Signal.

4. Bob decodes the QR code and obtains the `Sharing Key` and uses it to decrypt the `Encrypted Album Key` to obtain `Album Key`.

5. Bob decrypts the `Encrypted Album` with `Album Key` to retrieve the plaintext `Album`.

Multi-Device Support

Slik Photos seamlessly supports multiple user devices without compromising security and user experience. We allow users to securely enroll multiple devices and our system securely synchronizes the photos across all user devices. We describe our multi-device synchronization protocol below:

Protocol 3: Multi-Device Synchronization Protocol

Device Enrollment

1. To enroll the first device, a user, say Alice, will sign up for Slik and create an account. During this process, the Slik app will perform User Key Generation, described in Protocol 1, on this device to generate `User Key`.

2. To enroll all subsequent devices:

    2.1. Alice uses any of her already enrolled device(s) to generate a one-time `Enroll Key`, encrypts the `User Key` with `Enroll Key` using symmetric encryption, and shares this `Encrypted User Key` with the new device using the Slik server.

    2.2. Alice encodes the `Enroll Key` as a QR code and physically shares it with her new device.

    2.3. Alice's new device retrieves the `Encrypted User Key` from the Slik server, decodes the QR code and obtains the `Enroll Key`, and uses it to decrypt the `Encrypted User Key` to obtain `User Key`.

State Synchronization

1. Alice's device with a newly created or shared album, encrypts `Album Key` with `User Key` using symmetric encryption and obtains `Encrypted Album Key.` This device shares the `Encrypted Album Key` and the `Encrypted Album` with all of the Alice's devices using the Slik server.

2. The Slik server sends the `Encrypted Album Key` to all of the Alice's devices.

3. All Alice's devices will decrypt the `Encrypted Album Key` using the `User Key` to obtain `Album Key`.

4. All Alice's devices decrypts the `Encrypted Album` with `Album Key` to retrieve the plaintext `Album`.

Key Recovery

As the encryption keys are only present on the user's device(s), Slik provides a recovery mechanism if the user loses a device. If the user still has access to at least one of their devices that was enrolled to use Slik, they can use that device to enroll a new device. If the user do not have access to any of their devices enrolled in Slik, we provide a seed phrase at the install time, which could be used to recover the encryption keys.

Personalized Search

Slik allows users to search photos using date, time, location, and type of photos (family, food, beach, etc.). Our search system exclusively uses photos that you own or that are shared with you to generate personalized search experience. All the data and indices remain on the client and no information from the client is shared with anybody.

Encryption Algorithms

Slik employs authenticated symmetric encryption. We use AES block cipher in Galois Counter Mode (GCM) with 256-bit key for all of our encryption operations.

Quantum Safe Cryptography

Photos have a long life and are passed on to future generations. Slik uses Quantum safe cryptography to ensure that your photos will be secure even against a future adversary with quantum computing capabilities.

Conclusion

In this white paper, we present a technical overview of security and privacy system that Slik Photos have developed. Our system allow users to store their photos in the cloud and share them with other people, while their photos remain end-to-end encrypted. Our system supports multiple devices per user and is quantum-safe. We provide a personalized search experience without sharing your data with anybody else. Our cryptographic protocols are designed with “security by simplicity” mindset, which makes our protocols easy to understand, analyze, and implement.