NoPrying – Level 5 — Design Specification

Overview

This protocol builds on Level 4, which in turn builds on Level 2 and provides end-to-end encrypted messaging between two parties (Alice and Bob) using an offline uncrackable one-time pad (OTP). This level of security provides diplomat level messaging ability where it is to be expected every data transfer is intercepted and any online device is compromised, even the persons main phone is rooted by an adversary.

The primary encryption layer is a one-time pad (OTP) generated with CSPRNG random data, which is fed into a purely symmetric — AES-256-GCM keyed by an HKDF ratchet chain, exactly as specified in Level 2. Layered on top Lavel 4 which has is per-message randomness into the key hierarchy on every message sent and canary detection system.

Group chats and multi-device support are out of scope for this version.

---

1. Initial Setup

1.1 One-Time Pad

The design relies, not on mathematical unbreakable locks, rather on random data to encrypt with the same at either end. This in itself creates challenges, to move large amounts of data, out of band without interception and to be used where even a compromised connected device would not break the messaging encryption.

The design relies upon an online application and offline application, the idea is an offline is very difficult to compromise, offline in this instance means no sim card, no network connections. This offline device would handle the encryption, whilst such encrypted packets are passed to their everyday phone for sending and receiving.

Alice would buy two new phones, the storage abilities of said phone is the main important factor, 256GB would allow 200GB of random data, a significant store to be used going forward. The devices would be registered, updated and the offline application installed on both phones. At this point the phones are told to forget all network connections, they are isolated from the outside world.

Each phone would then be told to generate the CSPRNG random data and synchronize half and half from each other device, through airdrop. The end result is two phones with the same random data. One half is used by one phone for sending, the other half is used for

receiving, during the airdrop and blending process, this was determined. One device is decided as Entity1 (Alice) the other Entity2 (Bob), during the data loading process, for the purposes of Level 3 encryption. In addition, during the initial setup the AES keys are passed from one offline device to the other, private asymmetrical keys are generated and kept private, the public keys are shared to the other device.

The devices are ready to be given to their respective users, the device should be put in airplane mode with all forms of communication disabled (Bluetooth, airdrop, WIFI, etc)

One phone is then given to Bob, the security of the physical transfer is down to the individuals involved, a company for high level executives would have an inhouse courier and transport the device secured in a locked container.

1.2 Link to outside world

On Bob and Alices normal everyday use phones they would install a lightweight transmission application. This application would key with the offline phone through an visual animated QR code process.

1.3 Initial Key Generation

Whilst random data held on the offline device, one must not be complacent about the OTP encryption, by introducing Level 3 security as well in the offline sending application is prudent, so that even if the OTP was fully duplicated, standard encryption would still have to be defeated, including self-healing abilities, post compromise as baked into Level 3.

2. Message Encryption (inside the offline device)

2.1 Algorithm

The initial method of encryption is to use the Send OTP, byte for byte, the message is XORed with the OTP, upon use the OTP is blanked, at the other end the Receive OTP is used to undo the XORed data.

This is then passed to Level 4 / 2 for processing under that protocol.

---

3. Security Design Philosophy

3.1 The Case for a Tripple Lock Design

OTP is unbreakable by any supercomputer, any quantum computer, as long as the CSPRNG random data is random.

AES-256-GCM and HKDF (built on HMAC-SHA-256) have been subjected to decades of intense public scrutiny. No meaningful attack exists against either. They are the primitives considered most resistant to quantum computing attacks. The symmetric ratchet provides forward secrecy, message integrity, and message key uniqueness with zero transmitted key material and zero synchronisation requirements.

The entropy added to keys addresses a specific gap. If an attacker exfiltrates all key material at time T and then loses device access, the symmetric ratchet alone cannot recover — the salters are deterministic, so the attacker can compute all future keys. The asymmetric ratchet breaks this determinism by introducing fresh, unpredictable entropy on every message sent. One message is sufficient to close the attacker's window.

---

10. Real-World Attack Scenarios

Scenario 1: Active malware or spyware

Spyware would have to somehow get onto the offline device, cannot be done without taking physical control of the device.

Scenario 2: Physical device seizure

An adversary with physical access to an unlocked device can access key material in secure storage if they can bypass OS protections. Future messages are exposed until re-key on a clean device. Past messages are protected by forward secrecy — advanced keys are gone.

This level of compromise the channel would be abandoned and new devices created.

Scenario 3: Server compromise

An attacker gains access to the message server.

This protocol: Strong. It cannot decrypt any content.

Scenario 4: Man-in-the-middle at session establishment

This protocol: Strong. A MITM would need to intercept the initial transfer of the physical devices, such an intercept would likely be spotted.

Scenario 5: Quantum adversary

This protocol: Strong. OTP with random data, there is no mathematic puzzle to solve, such as Elliptic Curves.

Scenario 6: Catastrophic break in asymmetric/symmetric primitives

A previously unknown vulnerability is found in X448, ML-KEM-1024, or AES, or all.

This protocol: Falls back to a one time password as the root encryption method.

---

11. Known Limitations

Single device per identity. Multi-device support is not supported.

Group chat. Out of scope.

No long-term identity. There are no persistent identity keys. Session continuity is provided by the out-of-band relationship, not the protocol.

Run out of Encryption OTP whilst no one would send 100GB of text messages, it is possible that images could use the OTP, during use a % remaining can be shown, when low new devices should be delivered, it is good security practice to build this into a fixed time period.