Workgroup: Network Working Group
Internet-Draft:
draft-coolidge-enhanced-data-protection-00
Published: 3 April 2023
Intended Status: Informational
Expires: 5 October 2023
Authors: M. Coolidge
CoolTech Inc.

# Enhanced Data Protection via Cryptographic Signing and Permission-based Labeling

## Abstract

This document proposes an enhanced approach to data protection for computer applications by requiring them to cryptographically sign or label data generated using granted permissions. This would allow the host system to manage the storage and transport of generated data, ensuring a granular level of control and ultimately protecting user data more effectively.

## Status of This Memo

## Copyright Notice

## Table of Contents

## 1. Introduction

This document proposes an enhanced approach to data protection for computer applications by requiring them to cryptographically sign or label data generated using granted permissions. This would allow the host system to manage the storage and transport of generated data, ensuring a granular level of control and ultimately protecting user data more effectively.

## 2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

## 3. Detailed Mechanism

The proposed data protection mechanism can be further explained through the following components:

### 3.1. Permission Request and Granting

Computer applications MUST explicitly request permissions from the host system to access certain resources (e.g., microphone, camera, location). The host system SHALL evaluate the request based on predefined criteria and grant the necessary permissions if deemed appropriate.

### 3.2. Cryptographic Signing and Labeling

For each granted permission, the computer application MUST sign or label the data it generates accordingly. The host system SHALL provide a unique identifier for each permission, which can be used by the application to sign or label the data.

### 3.3. Data Storage and Transport Management

The host system SHALL manage the storage and transport of the generated data based on the application's permissions and the cryptographic signature or label. This includes determining whether the data can be stored locally, transferred over a network, or shared with other applications.

### 3.4. User Control

Users SHOULD have the ability to review and modify the permissions granted to applications and the corresponding rules for data storage and transport. This gives users more control over their data and helps prevent unauthorized access or misuse.

## 4. Use Cases

The enhanced mechanism can be applied to various scenarios:

### 4.1. Audio Recording

When an application uses the microphone permission to generate a file or data stream, the host operating system may allow the application to store this data locally but deny the application when attempting to upload the data. The default setting could be to deny the transfer of unsigned or unlabeled data, thus protecting user data by default.

### 4.2. Device Information

When data is generated with permissions that allow for obtaining device information, the host system may choose to allow the data to be stored or transported, as it is considered less sensitive.

### 4.3. Cloud Storage and Synchronization

When an application attempts to store data on a cloud storage service or synchronize data across multiple devices, the host system can use the cryptographic signature or label to determine whether the data is allowed to be uploaded or synced.

### 4.4. Third-Party Application Integration

When an application shares data with another application or third-party service, the host system can verify the cryptographic signature or label to ensure that the data is being shared with an authorized entity and in compliance with the granted permissions.

### 4.5. Data Deletion and Archiving

The host system can use the cryptographic signature or label to determine when and how data should be deleted or archived, ensuring that sensitive data is not retained longer than necessary and in accordance with the user's preferences.

## 5. Implementation Considerations

Implementing the proposed mechanism requires changes to both the host system and the computer applications. Host systems need to be updated to support permission-based cryptographic signing and labeling, as well as enhanced data storage and transport management. Computer applications must be modified to request permissions, sign or label data accordingly, and adhere to the host system's data storage and transport rules.

## 6. Security Considerations

The enhanced approach provides an additional layer of security by ensuring that data generated by applications is properly signed or labeled based on the granted permissions. This allows for more granular control over the storage, transfer, and processing of sensitive user data, reducing the risk of unauthorized access or misuse. However, it is crucial to ensure that the cryptographic signing and labeling process is secure and cannot be tampered with by malicious applications or external actors.

## 7. IANA Considerations

This document does not require any IANA actions.

## 8. References

### 8.1. Normative References

**[RFC2119]** Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

### 8.2. Informative References

**[RFC4949]** Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <https://www.rfc-editor.org/info/rfc4949>.

**[RFC6973]** Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/info/rfc6973>.

## Author's Address

Max Coolidge
CoolTech Inc.

38 Innovation Way
Silicon Valley, CA 94025
United States of America