Incognoto Security Policy

Take control of your personal data with Incognoto, your secure incognito notes.

May 2018

Contents

1 Introduction **2**
- 1.1 Application Information . . . 2
- 1.2 Terms of Service . . . 2
- 1.3 Contribute . . . 3

2 Basic Measures **4**
- 2.1 Authentication . . . 4
- 2.2 Default Notes . . . 4

3 Setting Up Advanced Authentication **7**
- 3.1 Overview of YubiKey . . . 7
- 3.2 YubiKey Usage Instructions . . . 7

4 Application Security **9**
- 4.1 AES-256 . . . 9
- 4.2 Screenshot Blocking . . . 9
- 4.3 Blocking Application Screen Content . . . 9
- 4.4 Secure Storage . . . 10
- 4.5 Responsible Disclosure . . . 10
- 4.6 Further Reading . . . 10

5 Threat Model **12**
- 5.1 Evaluation Information . . . 12
- 5.2 Disclosure Objective . . . 12
- 5.3 Accepted Risks . . . 12
  - 5.3.1 User Created Password . . . 12
  - 5.3.2 Importing . . . 13
  - 5.3.3 YubiKey NEO . . . 13
- 5.4 Mitigated Risks . . . 13
  - 5.4.1 Harvest (Guessing) Passwords . . . 13
  - 5.4.2 Timing Attack . . . 13

5.4.3 Potential Zero-Day Vulnerabilities 13

6 Glossary **15**
6.1 Terms to Know 15

Chapter 1

Introduction

1.1 Application Information

Corporations are constantly collecting your private, personal information. Many companies track your behavior and collect your data as part of their business model. User privacy continues to be a concern, but individuals do not have the right tools to take complete control of their data.

Welcome to Incognoto version 1.0. A free and open source application for Android in which you can securely store your personal notes, passwords, and task lists. This application is free of trackers, ads, and intrusive device permissions. Incognoto is a stand alone application that does not have access to your data; ensuring that your content will never be sold, traded, or shared. Take the first steps to regaining control of your privacy by encrypting your notes in a single file for exporting and easily storing backups of your data locally or on any cloud storage. Incognoto uses 256-bit encryption and offers the option of using a YubiKey for fast and secure authentication. We cannot, nor can your cloud storage provider or any other application installed on your device access or view the contents of your notes.

1.2 Terms of Service

These terms of service govern your use of Incognoto, its website and services. Unless required by law or expressly agreed to in documented communication, this software is distributed under Public License and is distributed on an ”AS IS” basis, without warranties or conditions or guarantees, either express or implied. In no event shall the authors or copyright holders be liable for any claim, damages or other liability, whether in an action or contract, arising from, out of, or in connection with the software or the use of other dealings in the software. See the GNU General Public License V2.0 for the specific language governing permissions and limitations (https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html). By using Incognoto you agree to adhere to these terms and conditions.

1.3 Contribute

If you love security as much as we do then please don't hesitate to find us at https://github.com/Incognoto/incognoto and join in on making a free and open source security minded notes application even better.

Chapter 2

Basic Measures

2.1 Authentication

In order to use Incognoto a user must first create a password. The user will be asked to retype their password in order to verify the input and after selecting enter a message will be shown at the bottom of the screen confirming that the input was accepted and that password has been saved. The user will be provided with an opportunity to change this password later from the setting menu. In order to change the password the user will be required to be logged into the application in an active session. This is to ensure that a valid user is accessing the content. Should a user forget their password while logged out of the application their data will now unaccessible until such a time that they remember or again have access to your password.

The importance of an effective password policy cannot be stressed enough. Incognoto decided to take a new approach to this philosophy by designing a password policy were there is not a minimal password length or complexity requirement, and the passwords never expire. We are encouraging users to challenge themselves to practice good security standards by creating a product that holds them accountable for protecting their data when it comes to password creation.

2.2 Default Notes

Default notes are displayed in order to allow a user to familiarize themselves with the outline of the privacy and security policy and the secure storage feature. This is intended as a way for a user to immediately become familiar with the most basic policies governing the design and implementation of Incognoto.

- **Security**
  All notes are encrypted and data never leaves your device without your permission.

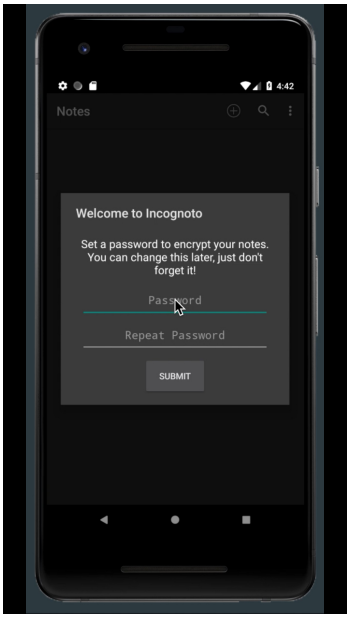

Figure 2.1: Password Prompt

- **Privacy**
  There are no trackers, no ads, no Internet connections, and no intrusive device permissions. We do not collect, sell, or share your information since Incognoto is entirely free and open source.

- **Backups**
  For when life's accidents happen, you can rest assured that your data is available only to you. Store encrypted backups on any cloud while keeping your data locked behind your password.

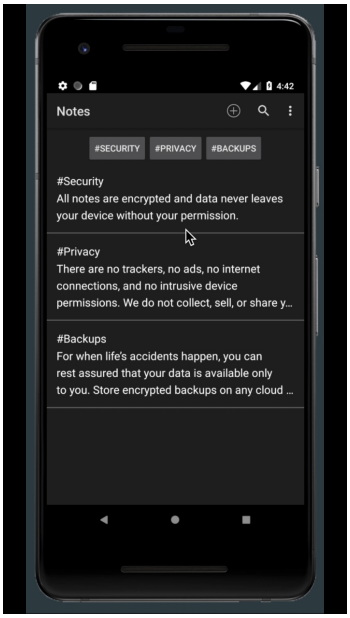

Figure 2.2: Default Notes

Chapter 3

Setting Up Advanced Authentication

3.1 Overview of YubiKey

The YubiKey is a hardware authentication device manufactured by Yubico that supports one-time passwords, public key encryption and authentication, and the Universal 2nd Factor (U2F) protocol. It allows a user to securely log into their accounts by emitting one-time passwords or using a FIDO-based public/private key pair generated by the device. YubiKey also allows for storing static passwords for use at sites and with applications that do not support one-time passwords. YubiKey strengthens the security of your Incognoto application by allowing you to create and use a very strong static password for encryption.

3.2 YubiKey Usage Instructions

Incognoto supports the use of YubiKey NEO as an authentication method. The YubiKey NEO contains a secure element (SE) that is accessible over both UBS and NFC. The SE offers a JavaCard 3.0/JCOP 2.4.2-compatible execution environment, an ISO14443A NFC interface, Mifare Classic emulation and an NDEF applet for interaction with Yubikey functionality.

Using a YubiKey NEO to unlock Incognoto requires that your device can authenticate using an NFC tag. This functionality is not supported by stock Android but is generally implemented in proprietary versions of the software. You may need to install and configure a RemoteAuthenticator application. Once installed, the application needs to be initialized with the same key and account name as the OATH applet on the YubiKey Neo.

Ensure that NFC is enabled before beginning configuration. To begin configuration for authentication of your Android device using the YubiKey NEO open the Android settings to the Location and Security screen, and configure your lock screen to be Secured with password. When asked to type it in, plug in the Yubikey with adapter, touch the disc, and the pre-configured static password

spits out into the password field that is currently in focus on the device. Android has a limit of 17 characters for its disk encryption and screen unlock password so you will want to configure your static password with this in mind before beginning the configuration process. Once the YubiKey NEO has been configured to your Android device you can follow the same step to set up and store a static password specifically for Incognoto authentication.

Chapter 4

Application Security

4.1 AES-256

Incognoto implements AES-256 for encryption of your data. The security of this algorithm has been tested over many years of use in hundreds of different applications and ensures that your content will remain secure. Advanced Encryption Standard (AES) is one of the most frequently used and most secure encryption algorithms available. It is publicly accessible, and it is the cipher that the NSA uses for securing documents with the classification ”top secret”. The algorithm is based on several substitutions, permutations and linear transformations, each executed on data blocks of 16 bytes, hence the term blockcipher. These operations are repeated over several times rounds and during each round, a unique roundkey is calculated out of the encryption key, and incorporated in the calculations. Based on the block structure of AES, the change of a single bit, either in the key, or in the plaintext block, results in a completely different ciphertext block. Currently, a time efficient and reproducible attack against AES does not exists. Therefore, AES remains the preferred encryption standard for governments, banking institutions, and security applications.

4.2 Screenshot Blocking

Screenshot blocking is a default security feature of Incognoto that disables the ability of your phone to take screen grabs of the content of the application. Should an unauthorized user gain access to an active session of Incognoto on your device they will be unable to take screenshots of your content. This security feature cannot be disabled within the application.

4.3 Blocking Application Screen Content

When switching between applications Incognoto will automatically hide the screen content with a plain gray screen. A header will still be available at the top of the application identifying it as Incognoto, but the current activity will be hidden and will not be viewable until the application

is actively open. This default security feature cannot be disabled within the application and is intended to supply an extra layer of protection to the user and their content.

4.4 Secure Storage

Incognoto offers users the ability to store your data in a single encrypted file locally or with any cloud storage provider. 256-bit encryption is a data/file encryption technique that uses a 256-bit key to encrypt and decrypt data or files and is used in most modern encryption algorithms, protocols and technologies. This affords you the ability to securely backup your content which ensures that you will always have access to your data without ever having to compromise the security of your application or system.

4.5 Responsible Disclosure

If you encounter a bug or a security vulnerability while using or researching Incognoto we ask that you kindly report it at https://github.com/Incognoto/incognoto. The source code for Incognoto is fully available and auditable on our GitHub repository and we encourage all users of the software to explore this as an option to understanding the improving Incognoto.

Please include in your report:

- Your device information
- A vulnerability description
- Reproduction steps

4.6 Further Reading

Even the best security measures can fail if they are not used in combination with good security minded habits. Because there are not any limitations on password requirements you have the power to make the best possible password for keeping your information secure. This means when creating your password it is important to not make a weak password or reuse an existing password that you use for authentication for another application. The use of a password manager of a YubiKey can help ensure that you create and use the strongest possible password.

When you are finished using the application you should always close it. This will require you to reenter your password to decrypt the application upon restart and will prevent any unauthorized users from accessing your content.

Be mindful of the source that you import content from and only import from a known and trusted source. This ensures the vulnerability protection and security of not only your application but your entire system.

Chapter 5

Threat Model

5.1 Evaluation Information

Application Version:	1.0
Description:	Incognoto is a notes application designed to provide a secure text storage environment.
Document Owner:	Incognoto
Participants:	@jxDenney
Reviewer:	@collinux

5.2 Disclosure Objective

The objective of risk management is to reduce the impact that the exploitation of a threat can have to the application. The following threats have been either accepted or mitigated through the implementation of design and development features. Through full disclosure of these risks Incognoto hopes to further mitigate the threats associated with each potential exploit by raising user awareness.

5.3 Accepted Risks

5.3.1 User Created Password

User created passwords present a vulnerability to the system by presenting attack surfaces in the form of users reusing passwords, creating weak passwords, and creating passwords that are easy to break through the investigation of an individual or through social engineering.

5.3.2 Importing

Importing is an important user feature that is not negotiable in terms of inclusion in the final product. It saves time and offers an important usability feature to users that aids in creating a fully functioning and robust application. Importing creates a threat in terms of exposing a closed system to threats and exploits.

5.3.3 YubiKey NEO

YubiKey presents a risk in the form of a third party authentication method that requires users to make the following assumptions.

First to trust that YubiKey's hardware producer, Yubico, to have uploaded firmware known to them to have no vulnerabilities in the OpenPGP implementation. Next a user must trust that no malicious agent messes with the firmware while the key is in transit between Yubico and the user. And finally a user must takes steps to ensure that once the key is flashed with the user's own trusted copy of the firmware that they never let the key physically fall into the hands of a malicious agent that could reflash the key.

5.4 Mitigated Risks

5.4.1 Harvest (Guessing) Passwords

Incognoto's password policy does not require a minimal password length or complexity requirement, and the passwords never expire. This actually helps to mitigate the risk of a guessing attack because this policy does not present to any potential attackers parameters to use during a attack. The threat of harvested passwords is further mitigated through the default security features of screenshot blocking and blocking screen content when switching between applications on the device. The use of a YubiKey can further prevent this type of attack by allowing a user to create and easily use a extremely long and complicated password on a daily basis.

5.4.2 Timing Attack

A timing attack is a side channel attack in which the attacker attempts to compromise a cryptosystem by analyzing the time taken to execute cryptographic algorithms. Incognoto buffers the decryption when users are entering passwords in order to lower the chances of an attacker narrowing down the length of the password.

5.4.3 Potential Zero-Day Vulnerabilities

With an a total application size of approximately 400kB Incognoto presents a small attack surface. This is accomplished by its stand alone application feature combined using only native Android libraries, a NoSQL database, and not implementing APIs. A small application ensures transparency

in that it is easy to review the source code, should you be interested in doing so, and allows you to verify for yourself that Incognoto is not using any third party trackers, ads, and does not require intrusive device permissions.

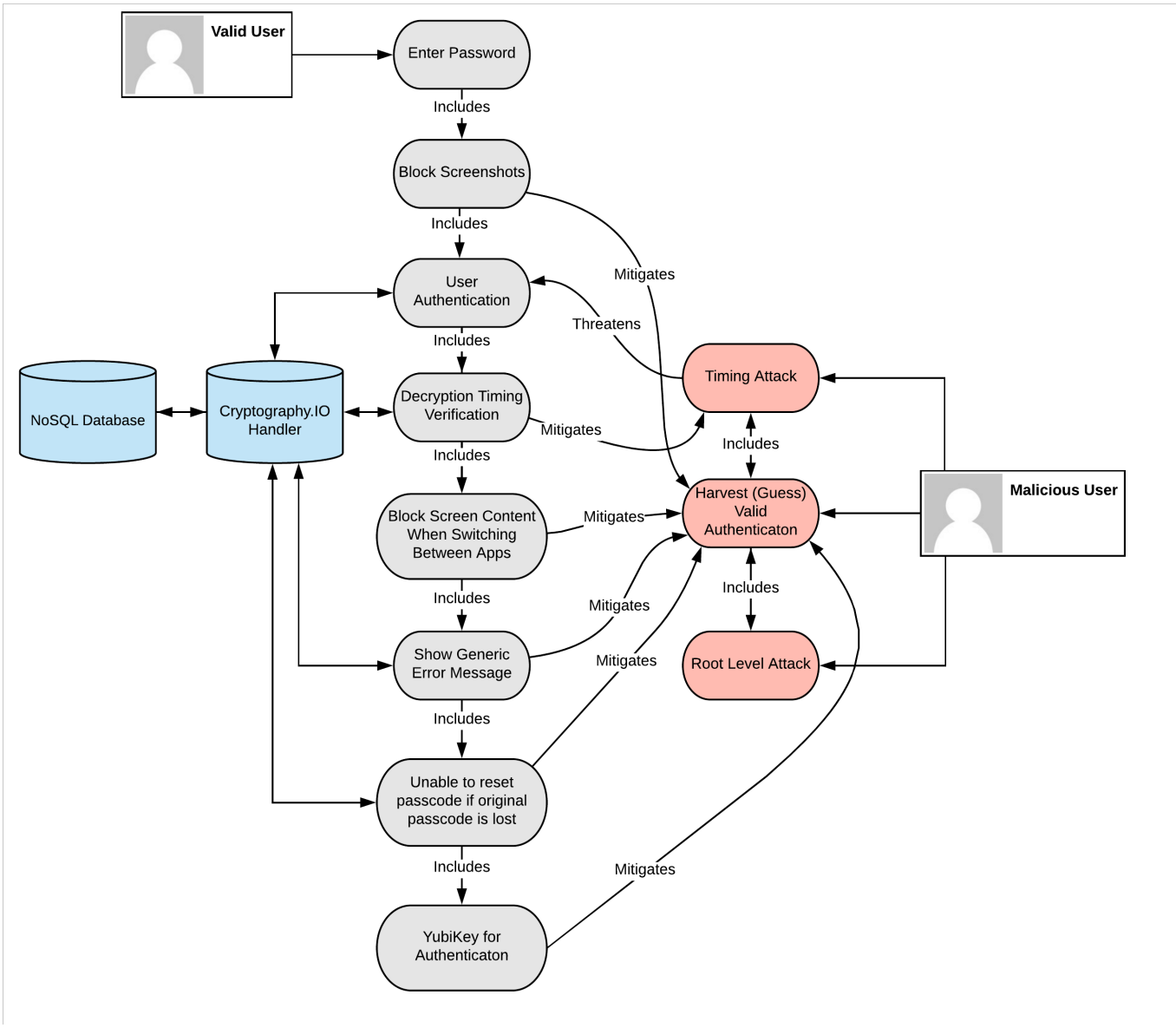

Figure 5.1: Use and Misuse Case Graph for Authentication

Chapter 6

Glossary

6.1 Terms to Know

- **AES-256**
  The advanced encryption standard. An algorithm used for encryption.
- **Cloud Storage**
  Saving content to remote storage servers.
- **Exporting**
  To send data from one program to another.
- **File Manager**
  A program that provides a user interface to manage files and folders.
- **Hashtag**
  A word of phrase preceded by the pound symbol that is used to categorize content and track topics.
- **Importing**
  To receive data into one program from another.
- **Local Storage**
  Saving content directly to a device.
- **Password Protection**
  A security process that allows only those with an authorization to gain access to certain information. Saving content directly to a device.
- **YubiKey**
  A hardware authentication device manufactured that supports public key encryption and authentication.