Problem 1

Security Policy for Cameras

Solution

Objective

The following outlines a software-implemented security policy that may be implemented by camera manufacturers in order to add encryption to handheld digital cameras. The policy will detail principal roles of camera users and the privileges each principal may have. It will also give an overview of the technical implementation of such an encryption scheme.

User Roles

A camera may have multiple Authorized Users that know the alphanumeric password to access the data on the camera. Unauthorized Users should have no access to photos, settings, or any other data on the camera and do not know the password.

Authorized User

Any user may opt to set a password on the camera, leading to a distinction between authorized users and unauthorized users. Upon purchasing a camera, we recommend that new users set a password. If no password is set, anyone with physical access to the camera will have the privileges of an authorized user.

Authorized users have the ability to:

- Set/change/remove a password
- View photos on the camera
- Take photos on the camera
- Decrypt photos for exporting
- Change camera settings
- All other camera functions

Unauthorized User

If a password is set, a user who doesn't know the password is considered unauthorized and has almost no privileges on the camera. The camera will immediately ask the user for the password upon powering on. The only privilege unauthorized users have is the ability to take photos as they are encrypted with the public key.

Technical Implementation

If no password is set, decrypted images will be stored on the camera's SD card.

If a password is set, public key cryptopgraphy will be used to keep images secure. The public key $\textsc{Pk}$ will be stored on the SD card and used to encrypt new photos when they are written to disk. The secret key $\textsc{Sk}$ will be used to decrypt photos on the disk. But, we won't store the secret key on the SD card; given the secret key, hash function H, and password p, we compute the hidden key $\textsc{Hk}$:

$$\textsc{Hk} = \textsc{Sk} \cdot H(p)$$

In this way, an unauthorized user who does not know the password has no way of obtaining the secret key from the hidden key. However, given the password, we can compute the secret key simply by dividing $\textsc{Hk}$ by $H(p)$.

Upon powering up the device, the user will prompted for their password, which will be used to derive the secret key from the hidden key. Password correctness can be checked by seeing if the secret key derived from the hidden key matches the private key. If the secret key matches, it will be stored in voltaile memory on the camera to be used to decrypt images to be viewed on the camera.

If the user would like to decrypt photos on their SD card for exporting, they will be asked to enter their password which will be used to decrypt all photos on the SD card, effectively removing the password.

Security Analysis

The above security policy ensures confidentiality: a user without the password cannot access the photos on the camera or change any camera settings.

The policy also affects availability: not all services of the camera will be available immediately upon powering on. But, this is a tradeoff for ensuring confidentiality. It is notable that users can opt in to using a password.

The policy does not make any promises about photo integrity as this is a less important security goal for cameras. For example, confiscating an SD card or camera accomplishes the same goal as scrambling the SD card, so there is no need to ensure authenticity.