Demo: Protecting User Data through Ephemeral Ownership of IoT Devices

Han Zhang
Carnegie Mellon University
hzhang3@cs.cmu.edu

Yuvraj Agarwal
Carnegie Mellon University
yuvraj@cs.cmu.edu

Matt Fredrikson
Carnegie Mellon University
mfredrik@cs.cmu.edu

ABSTRACT

This demonstration presents a working prototype of *TEO*, a new model of device ownership that divides traditional owners into "admin" and "ephemeral owners". TEO addresses the challenge that users have no say in how their data are managed when the device is controlled by third parties, such as in rental and shared spaces. We design a complete protocol suite to address several practical issues, including preserving data ownership after users stop using the device, minimizing trusts with untrusted storage providers, enabling access control and revocation, and supporting groups of owners. Our cross-platform prototype implementation enables us to demonstrate the operational flow for managing ephemeral ownership of TEO-enabled devices in a representative setup with mobile phones, embedded devices, and Linux servers.

CCS CONCEPTS

• **Security and privacy** → **Security services**; **Access control**; **Authorization**; Formal security models.

KEYWORDS

Internet of Things, ephemeral ownership, protocol verification, stakeholder privacy, access control

ACM Reference Format:
Han Zhang, Yuvraj Agarwal, and Matt Fredrikson. 2022. Demo: Protecting User Data through Ephemeral Ownership of IoT Devices. In *The 20th Annual International Conference on Mobile Systems, Applications and Services (MobiSys '22), June 25–July 1, 2022, Portland, OR, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3498361.3538664

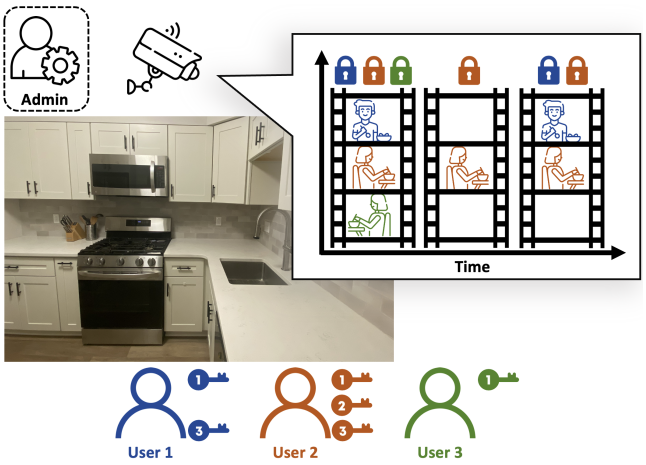

Figure 1: Motivating scenario of TEO deployment. Imagine a group of friends use this kitchen and dining area in a vacation rental. Users occupy the room at different times, sometimes with each other. The camera encrypts the recorded data with different session keys and distributes the keys accordingly. Meanwhile, the device admin has no access to any data to preserve users' privacy.

1 INTRODUCTION

Internet of Things (IoT) devices have gained tremendous popularity in recent years and have enjoyed growing ubiquity in both private and public settings. Given the breadth of sensitive data they can collect, IoT devices raise serious privacy concerns and need strong data protection built into their system designs. Unfortunately, many existing access management systems grant exclusive controls to whoever sets up the device (i.e., device administrators) and fail to consider more complicated scenarios where devices are used either exclusively or shared by people other than device administrators. In the latter cases, an ideal solution would empower the actual device users to have full control over their data captured by the IoT devices.

We present the design and a working demonstration of TEO — IoT Ephemeral Ownership — a new model of device ownership that splits the traditional fixed IoT owner roles into "admins" and "ephemeral owners", and a corresponding protocol that embodies this model. The admins handle logistic duties like device initialization and regular maintenance. More importantly, they can decide which users can *potentially* become ephemeral owners by issuing user-specific pre-auth tokens. Users can claim a device by presenting the pre-auth token directly to the device. Once claimed, the device starts to protect the corresponding owners' data. If someone in the future wants to access the data, they should reach out to all data owners and seek individual permissions. With the use of threshold encryption, the group of users can choose a fixed access policy a priori (e.g., requiring all approvals or a majority), and the data requester will not be able to decrypt the data unless such a threshold is met. One key aspect of TEO is that admins do not have any visibility into the operational data collected by the device to protect ephemeral owners. If admins want to access the data, they have to seek owner permissions as every other data requester.

TEO also leverages third-party storage service providers as untrusted entities to augment the limited storage space on IoT devices

MobiSys '22, June 25–July 1, 2022, Portland, OR, USA

ACM ISBN 978-1-4503-9185-6/22/06.
https://doi.org/10.1145/3498361.3538664

and users' agents (e.g., smartphones). Devices can directly upload encrypted data content to storage providers and distribute the keys asynchronously to data owners. To access the data, someone can download the encrypted data files and obtain decryption keys from the owners (by looking up the necessary information stored in plaintext metadata).

Figure 1 illustrates a motivating example of TEO deployment in the home rental scenario. As TEO admin, the rental host installs and sets up a TEO-enabled smart camera at this place. A group of friends rent this place for their trip and use TEO to protect their data by becoming the camera's ephemeral owners. During their stay, the camera continuously encrypts all video footage with unique session keys and distributes these keys to its active ephemeral owners (through threshold encryption and key shares). As illustrated in the timeline, all three users are present on the first day, so they all should be co-owners of the device. On the second day, Users 1 and 3 leave, so User 2 should obtain exclusive control of the camera, and anyone looking to decrypt the data must have her approval. When User 1 returns on day 3, the device should adjust its owner list accordingly and give Users 1 and 2 equal shares in managing access control of their co-owned data in the future.

2 TEO DESIGN

To address device users' privacy concerns, we design TEO to fulfill the following high-level goals:

- Flexible Association of Device and Users: devices can handle frequent changes in their current owners and groups in a dynamic environment.
- Preserving Data Ownership: users should retain control over their data, even if they no longer use the device in the future;.
- Decentralized Trust: users should be able to make access control decisions without requiring trusts in any external third-parties.
- Formally Verified Security: we want to design a streamlined TEO protocol suite to provide assurances of security and correctness.

Figure 2 illustrates TEO's workflow involving multiple entities. Throughout the design, we addressed several technical challenges to facilitate ownership management and access control. First, we separate the holistic "owner" role into "admin" and "users", with complementary capabilities. Admins can set up new devices (①) and decide who are eligible to become ephemeral owners (②). Second, we group the data into smaller time segments and use unique session keys to enable frequent and quick changes in device ownership. By encrypting the data, we can utilize untrusted storage services to mitigate the limited space on local devices (③). Third, we support groups of co-owners and configurable data access policies by leveraging threshold encryption (Shamir Secret Sharing). The group of owners can decide how many approvals a data requester needs to obtain to decrypt the data collectively owned by the group. Finally, to support data access revocation with low communication overhead, we incorporate a special encryption scheme to enable the storage provider to re-encrypt data contents on user's behalf without being able to decrypt it into plaintext (⑥).

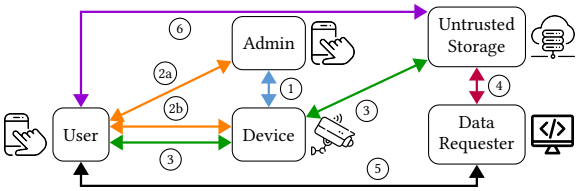

Figure 2: TEO workflow. An admin initializes the device (①). Next, the user claim device ownership with the admin's pre-approval (②a and ②b). During normal operation (③), the device encrypts users' data and uploads it to storage. A requester can download the data (④), but needs to seek individual owner's permission to decrypt it (⑤). To revoke access, the user directly issue a request to the storage provider (⑥).

TEO leverages a number of cryptography primitives in its design. We combine key homomorphic encryption with threshold encryption into the data storage process to enable data owners maintain direct control over their data, while utilizing untrusted third-party providers to store encrypted user data for scalability. Please refer to the full paper [1] for the details of TEO. In addition, we conducted a formal verification of TEO's protocol design to ensure that it satisfies various security goals related to secrecy, authenticity, resilience to data spoofing, and correctness of the revocation.

3 DEMONSTRATION

We demonstrate the technical contribution of TEO's protocol design by showcasing a complete TEO workflow in a setup resembling real-world use cases. Both the TEO user and the admin programs are packaged as Android phone apps. We will use a Raspberry Pi 4 as the demo device, although we also have a prototype for the Raspberry Pi Zero. For untrusted third-party storage, we will use a Linux server in the cloud to represent arbitrary service providers. Finally, we provide a command line interface for programmatic requests for access to user's private data.

The demonstration consists of working examples of (a) initializing new devices by the admin, (b) claiming new devices for users to become ephemeral owners, (c) storing private data for current owners during normal operation, (d) managing data access requests for data owners, including approval and revocation, and (e) extending ownership into group modes by requiring all owners' approval to grant access.

The source code of the TEO project as well as the prototype used for the demonstration is publicly available at https://github.com/synergylabs/TEO-release.

REFERENCES

[1] Han Zhang, Yuvraj Agarwal, and Matt Fredrikson. 2022. TEO: Ephemeral Ownership for IoT Devices to Provide Granular Data Control (conditionally accepted). In *Proceedings of the 20th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '22).*