POSTER: VICEROY: GDPR-/CCPA-compliant Enforcement of Verifiable Accountless Consumer Requests

Scott Jordan
UC Irvine
sjordan@uci.edu

Yoshimichi Nakatsuka*
UC Irvine
nakatsuy@uci.edu

Ercan Ozturk*
UC Irvine
ercano@uci.edu

Andrew Paverd
Microsoft Research
andrew.paverd@microsoft.com

Gene Tsudik
UC Irvine
gene.tsudik@uci.edu

Abstract

Recent data protection regulations (notably, GDPR and CCPA) grant consumers various rights, including the right to *access*, *modify* or *delete* any personal information collected about them (and retained) by a service provider. To exercise these rights, one must submit a *verifiable consumer request* proving that the collected data indeed pertains to them. This action is straightforward for consumers with active accounts with a service provider at the time of data collection, since they can use standard (e.g., password-based) means of authentication to validate their requests.

However, a major conundrum arises from the need to support consumers *without accounts* to exercise their rights. To this end, some service providers began requiring such *accountless* consumers to reveal and prove their identities (e.g., using government-issued documents, utility bills, or credit card numbers) as part of issuing a verifiable consumer request. While understandable and reasonable as a short-term fix, this approach is cumbersome and expensive for service providers as well as privacy-invasive for consumers.

Consequently, there is a strong need to provide better means of authenticating requests from accountless consumers. To achieve this, we propose VICEROY, a privacy-preserving and scalable framework for producing *proofs of data ownership*, which form a basis for verifiable consumer requests. Building upon existing web techniques and features, VICEROY allows accountless consumers to interact with service providers, and later prove that they are the same person in a privacy-preserving manner, while requiring minimal changes for both parties. We design and implement VICEROY with emphasis on security/privacy, deployability, and usability. We also assess its practicality via extensive experiments.

I. Full bibliographic reference to paper

Title: VICEROY: GDPR-/CCPA-compliant Enforcement of Verifiable Accountless Consumer Requests

Authors: Scott Jordan, Yoshimichi Nakatsuka, Ercan Ozturk, Andrew Paverd, and Gene Tsudik

Date: 27 February - 3 March 2023

Venue: Network and Distributed System Security (NDSS) Symposium 2023

DOI: https://dx.doi.org/10.14722/ndss.2023.23074

* Corresponding authors. Authors ordered alphabetically.

VICEROY: GDPR-/CCPA-compliant Verifiable Accountless Consumer Requests

Scott Jordan[1], Yoshimichi Nakatsuka[1], Ercan Ozturk[1], Andrew Paverd[2], Gene Tsudik[1]
[1]University of California, Irvine, and [2]Microsoft Research

Scan QR code for link to implementation↑

Data Protection Regulations

- GDPR and CCPA grant consumers rights to **Access**, **Correct**, and **Delete** their data
- To exercise this right, consumers must submit **Verifiable Consumer Requests (VCRs)** to prove that they own the data
- Straightforward and secure for consumers with accounts
  → What about **accountless consumers**?

Accountless Consumer Request

- **Ad-hoc**: No proposed standards
- **Insecure**: Attacked and broken in literature
- **Privacy-invasive**: Provide more info

Symmetric solution: Cookies

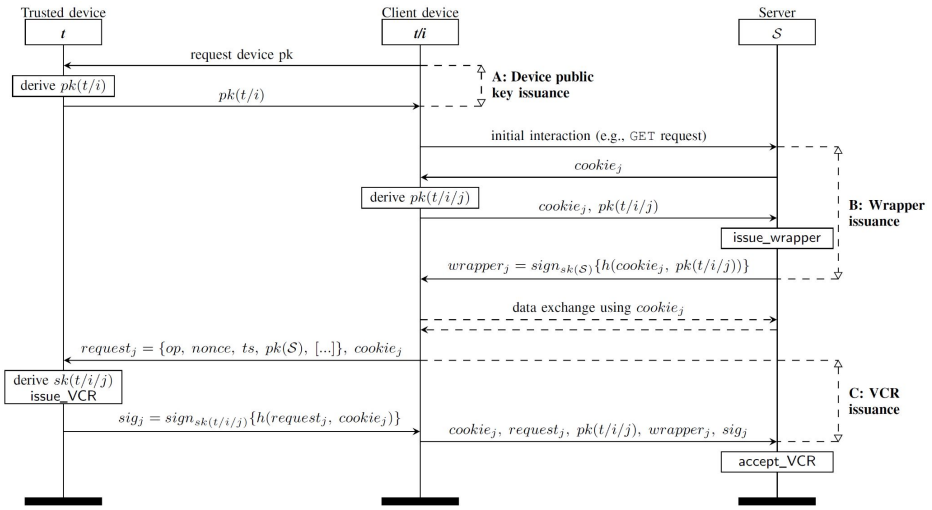
Pros:
- Unforgeable
- Privacy-preserving

Cons:
- Secure transmission & storage
- No binding between VCR & Cookie

Asymmetric Solution

- Consumer generates key pair for each session and sends public key to server
- Server associates all data collected for session to public key
- Digital signature used as VCR

VICEROY Protocol



Challenges & Solutions

- **Key Explosion**: Generate per-session public key using BIP32
- **Secure Key Management:** Store BIP32 master private key in Trusted Consumer Device, which is only used during VCR issuance and will not leave the device
- **Long-Term Storage:** Allow consumers to use untrusted, third-party services to store cookie wrappers
- **Multiple Device Support**: Use BIP32 to generate per-device public key
- **Server-side storage modification:** Cookie wrappers prevent this

Implementation

Evaluation

- Evaluated security using **Tamarin Prover**
- Latency
  - Cookie wrapper flow: **50.3** ms
  - VCR flow: **1357.4** ms (generation) + **1.5** ms (verification)
- Data transfer
  - Cookie wrapper: **1.10** kB
  - VCR: **1.27** kB
- Cookie wrapper storage (annual): **22.61** MB

Future directions

- Support broader communication protocols
- Adapt VICEROY for 3rd party cookies
- Improve privacy via TEEs and PIR
- Support account-holding consumers & client re-auth

SaTC Frontiers: Collaborative: *1956393* [1], *1955227* [2], *2103439* [3], *1956435* [4]
Institutions: UC Irvine [1], Northeastern Univ. [2], UC Davis [3], USC [4]
Lead PIs: A. Markopoulou [1], D. Choffnes [2], Z. Shafiq [3], K. Psounis [4]