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

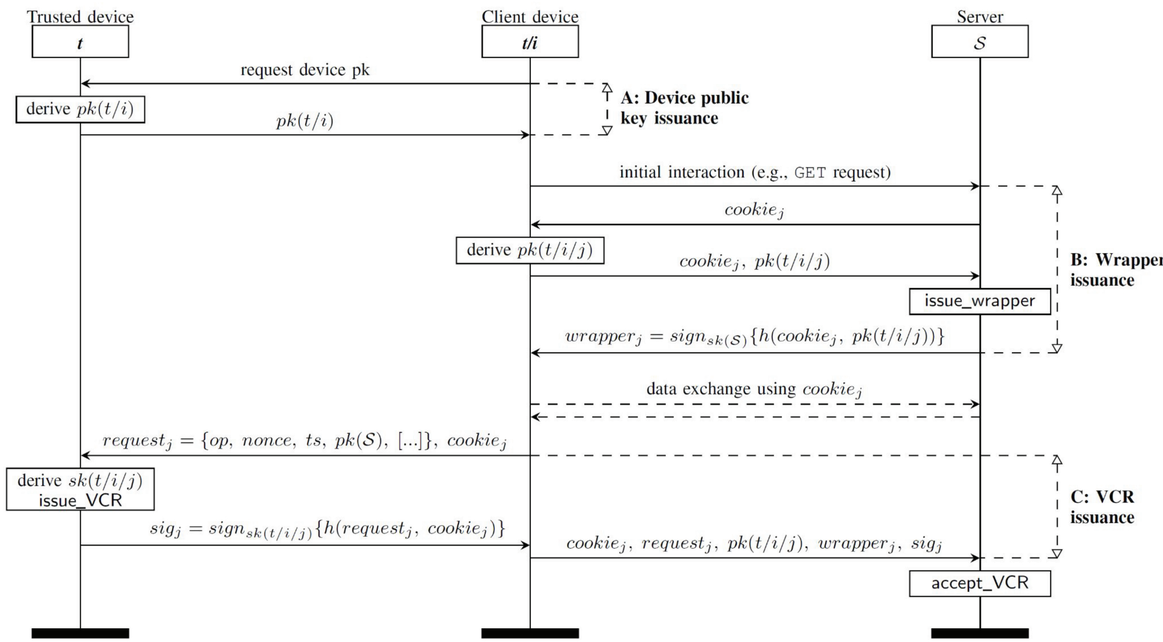
Pros:
- Unforgeable
- Privacy-preserving

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 for 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]