VICEROY: GDPR-/CCPA-compliant
Verifiable Accountless Consumer Requests
Scott Jordan\textsuperscript{1}, Yoshimichi Nakatsuka\textsuperscript{1}, Ercan Ozturk\textsuperscript{1}, Andrew Paverd\textsuperscript{2}, Gene Tsudik\textsuperscript{1}
\textsuperscript{1}University of California, Irvine, and \textsuperscript{2}Microsoft Research

Data Protection Regulations
- GDPR and CCPA grant consumers rights to \textit{Access}, \textit{Correct}, and \textit{Delete} their data
- To exercise this right, consumers must submit \textit{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
- \textbf{Ad-hoc}: No proposed standards
- \textbf{Insecure}: Attacked and broken in literature
- \textbf{Privacy-invasive}: Provide more info

Symmetric solution: Cookies

\textbf{Pros:}
- Unforgeable
- Privacy-preserving

\textbf{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

\begin{itemize}
  \item Trusted device
  \item Client device
  \item Server
  \item \textbf{A: Device public key issuance}
  \begin{itemize}
    \item \textit{initial interaction (e.g., GET request)}
    \item \textit{cookie} \text{, pk(1/f), pk(1/f)}
    \item \textbf{cookie} = \text{sign}_{\text{public}}(h(\text{cookie}, pk(1/f)));
  \end{itemize}
  \item \textbf{B: Wrapper issuance}
  \begin{itemize}
    \item \textbf{wrapper} = \text{sign}_{\text{public}}(h(\text{cookie}, pk(1/f)));
    \item \textbf{data exchange using cookie}.
    \item \textbf{cookie}, \text{request}, \text{pk(1/f)}, \text{wrapper}, \text{sign}.
  \end{itemize}
  \item \textbf{C: VCR issuance}
  \begin{itemize}
    \item \text{sign}_\text{public}(\text{request}, \text{cookie})
    \item \text{access}_{\text{IRC}}.
  \end{itemize}
\end{itemize}

Challenges & Solutions
\begin{itemize}
  \item \textbf{Key Explosion}: Generate per-session public key using BIP32
  \item \textbf{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
  \item \textbf{Long-Term Storage}: Allow consumers to use untrusted, third-party services to store cookie wrappers
  \item \textbf{Multiple Device Support}: Use BIP32 to generate per-device public key
  \item \textbf{Server-side storage modification}: Cookie wrappers prevent this
\end{itemize}

Evaluation
\begin{itemize}
  \item \textbf{Evaluated security using Tamarin Prover}
  \item \textbf{Latency}
    \begin{itemize}
      \item Cookie wrapper flow: \textbf{50.3 ms}
      \item VCR flow: \textbf{1357.4 ms (generation)} + \textbf{1.5 ms (verification)}
    \end{itemize}
  \item \textbf{Data transfer}
    \begin{itemize}
      \item Cookie wrapper: \textbf{1.10 kB}
      \item VCR: \textbf{1.27 kB}
    \end{itemize}
  \item \textbf{Cookie wrapper storage (annual)}: \textbf{22.61 MB}
\end{itemize}

Future directions
\begin{itemize}
  \item Support broader communication protocols
  \item Adapt VICEROY for 3rd party cookies
  \item Improve privacy via TEES and PIR
  \item Support for account-holding consumers & client re-auth
\end{itemize}