

SaTC: CORE: Small: Preventing Web Side-channel Attacks via Atomic Determinism



Challenge:

- The existence of Timing side channels that can leak out browser private information

Solution:

- Decomposition of a browser into several atomic units
- Separation of clocks and observers



Side Channel

Determinism



Scientific Impact:

- Securing private user information
- Providing secure and privacy-preserving browser to common users
- Publications at CCS and USENIX

Broader Impact:

- Websites are running in a more secure browser.
- Possible transition to Tor browser
- A new course: Web Security

1854001, Johns Hopkins University, Yinzhi Cao (yzcao@cs.jhu.edu)