SaTC: CORE: Small: Collaborative: Hardware-assisted Plausibly Deniable System for Mobile Devices

Submitted by Bo Chen on Mon, 07/06/2020 - 11:51am

Project Details

Lead PI

Bo Chen

Performance Period

Oct 01, 2019 - Sep 30, 2022

Institution(s)

Michigan Technological University

Sponsor(s)

National Science Foundation

Award Number

1928349

Ranked 577 out of 2290 Group Projects.
88 related hits.

Mobile computing devices typically use encryption to protect sensitive information. However, traditional encryption systems used in mobile devices cannot defend against an active attacker who can force the mobile device owner to disclose the key used for decrypting the sensitive information. This is particularly of concern to dissident users who are targets of nation states. An example of this would be a human rights worker collecting evidence of untoward activities in a region of oppression or conflict and storing the same in an encrypted form on the mobile device, and then being coerced to disclose the decryption key by an official. Plausibly Deniable Encryption (PDE) has been proposed to defend against such adversaries who can coerce users into revealing the encrypted sensitive content. However, existing techniques suffer from several problems when used in flash-memory-based mobile devices, such as weak deniability because of the way read/write/erase operations are handled at the operating systems level and at the flash translation layer, various types of side channel attacks, and computation and power limitations of mobile devices. This project investigates a unique opportunity to develop an efficient (low-overhead) and effective (high-deniability) hardware-assisted PDE scheme on mainstream mobile devices that is robust against a multi snapshot adversary. The project includes significant curriculum development activities and outreach activities to K-12 students.

This project fundamentally advances the mobile PDE systems by leveraging existing hardware features such as flash translation layer (FTL) firmware and TrustZone to achieve a high deniability with a low overhead. Specifically, this project develops a PDE system with capabilities to: 1) defend against snapshot attacks using raw flash memory on mobile devices; and 2) eliminate side-channel attacks that compromise deniability; 3) be scalable to deploy on mainstream mobile devices; and 4) efficiently provide usable functions like fast mode switching. This project also develops novel teaching material on PDE and cybersecurity for K-12 students and the Regional Cybersecurity Education Collaboration (RCEC), a new educational partnership on cybersecurity in Michigan.

Bo Chen

Related Artifacts

No related artifacts found.

CORE Small Collaborative Division of Computer and Network Systems (CNS)