EAGER: Enabling Secure Data Recovery for Mobile Devices against Malicious Attacks

Michigan Tech

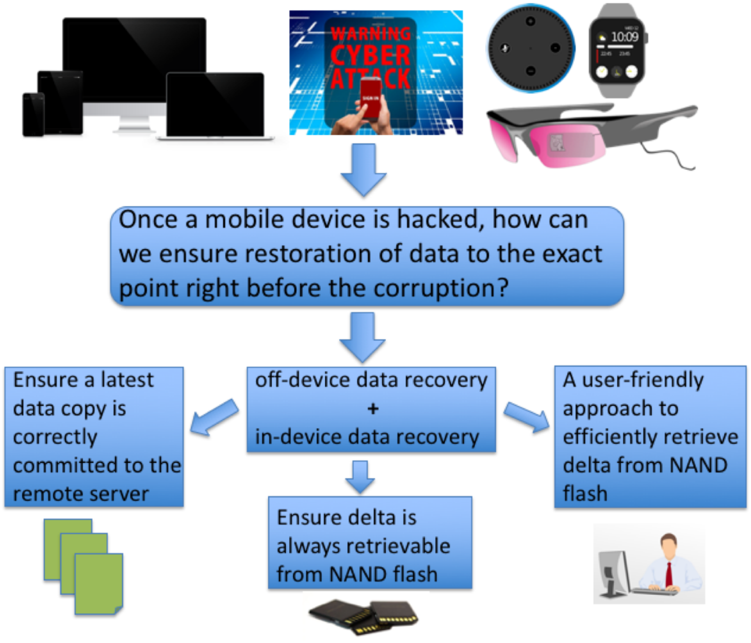
Challenge:

- Mobile computing devices usually rely on off-device data recovery: periodically back up data remotely and restore them upon failures
- Cannot ensure restoration of data to the *exact* point of time right before the malware hacks (i.e., the corruption point)

Solution:

- Proposed a novel data recovery framework combining both the traditional off-device and the new in-device data recovery
- Ensured recoverability of data by hiding them in the flash memory using special hardware features of flash
- Designed a novel malware detection algorithm which can detect OS-level malware in the flash translation layer

NSF EAGER grant CNS-1938130,
Michigan Technological University,
Bo Chen (bchen@mtu.edu)



Once a mobile device is hacked, how can we ensure restoration of data to the exact point right before the corruption?

off-device data recovery + in-device data recovery

Ensure a latest data copy is correctly committed to the remote server

Ensure delta is always retrievable from NAND flash

A user-friendly approach to efficiently retrieve delta from NAND flash

Scientific Impact:

- Address synchronization gap present in traditional off-device data recovery
- Allow restoration of data to the corruption point
- Establish a novel in-device data recovery concept, and enable it in computing devices using flash memory

Broader Impact and Broader Participation:

- Data recovery upon malicious attacks benefits individuals, enterprises, federal agencies, government sectors
- Involved 5 graduate students into the project
- Incorporated research results into 2 graduate and 1 undergraduate courses
- Disseminated project knowledge to K-12 female students