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

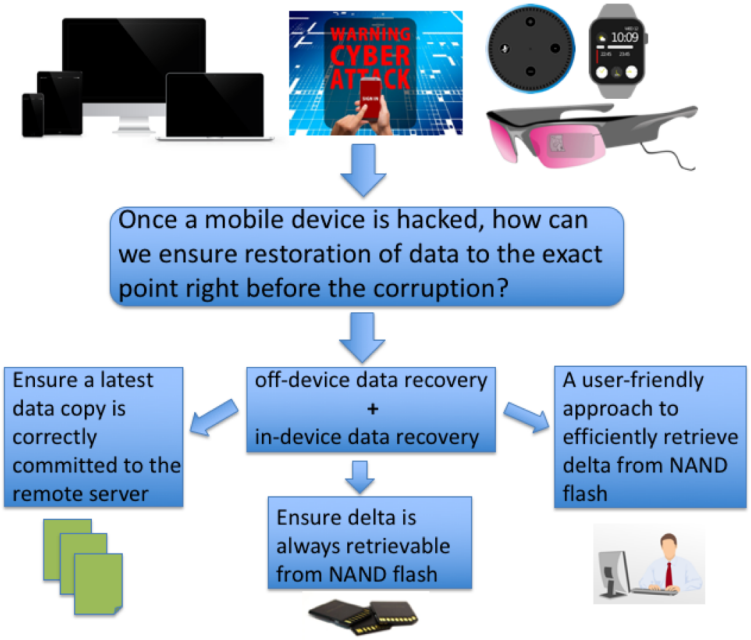
Michigan Tech

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:

- Propose a novel data recovery framework combining both the traditional off-device data recovery and a new in-device data recovery
- Ensure recoverability of data by hiding them in the flash memory using special hardware features of flash



Scientific Impact:

- Challenge defects of the broadly used 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:

- Data recovery upon malicious attacks benefits individuals, enterprises, federal agencies, government sectors
- Incorporate research results into 3 graduate courses and 2 undergraduate courses in MTU
- Disseminate project knowledge to K-12 students and teachers in UP of Michigan

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