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

Bo Chen, Michigan Technological University

http://snp.cs.mtu.edu/research/drm2.html


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

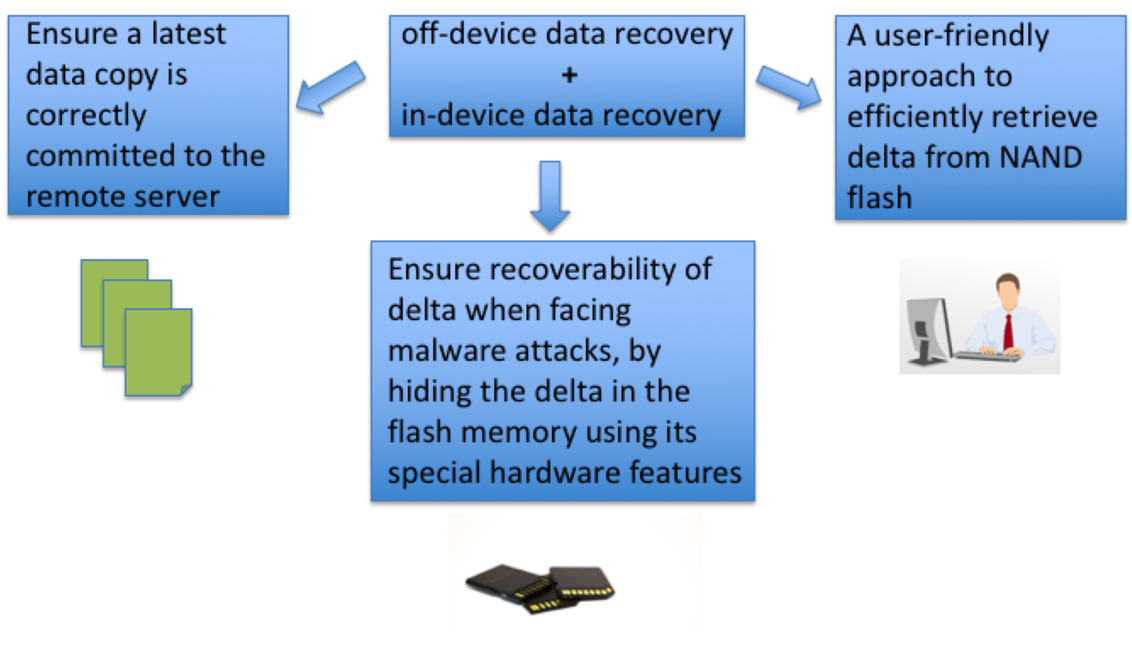
## Challenge

- Mobile computing devices usually rely on off-device data recovery: periodically back up data remotely and restore them upon failures.
- This suffers from a fundamental limitation: the backup in the remote server is usually not synchronized with data stored locally; when a mobile device suffers from malware attacks, it can only be restored to a historical state, rather than the exact state right before the failure.
- How to allow restoration of data to the exact point of time right before the malware starts to perform corruption (i.e., corruption point)?

## Scientific Impact

- Significantly advance data recovery research by challenging defects of the broadly used traditional off-device data recovery, and establishing a new data recovery framework allowing data restoration to the corruption point.
- Enable data recovery against the malware which can compromise the entire OS.
- Initiate a novel *in-device data recovery* concept and enable it in computing devices using flash memory.

## Solution




## Broader Impact – Society

- Individual/enterprise mobile users: can recover data from ransomware attacks without paying the ransom.
- Federal agencies, government sectors: can ensure recoverability of mission critical data even if the malware can compromise the OS of the victim mobile devices.

## Broader Impact – Education & Outreach

- Project results will be incorporated into 3 graduate cybersecurity courses (CS5471, CS5472, CS5740) and 2 undergraduate cybersecurity courses (CS4471, CS4740) in MTU.
- Disseminate project knowledge to K-12 students and teachers in the Upper Peninsula (UP) of Michigan, through GenCyber summer cybersecurity camps.
- Train female students from UP and Northern Wisconsin with cybersecurity knowledge.