# FSD – File System Defender

## As part of project in ransomware, Spring 2018

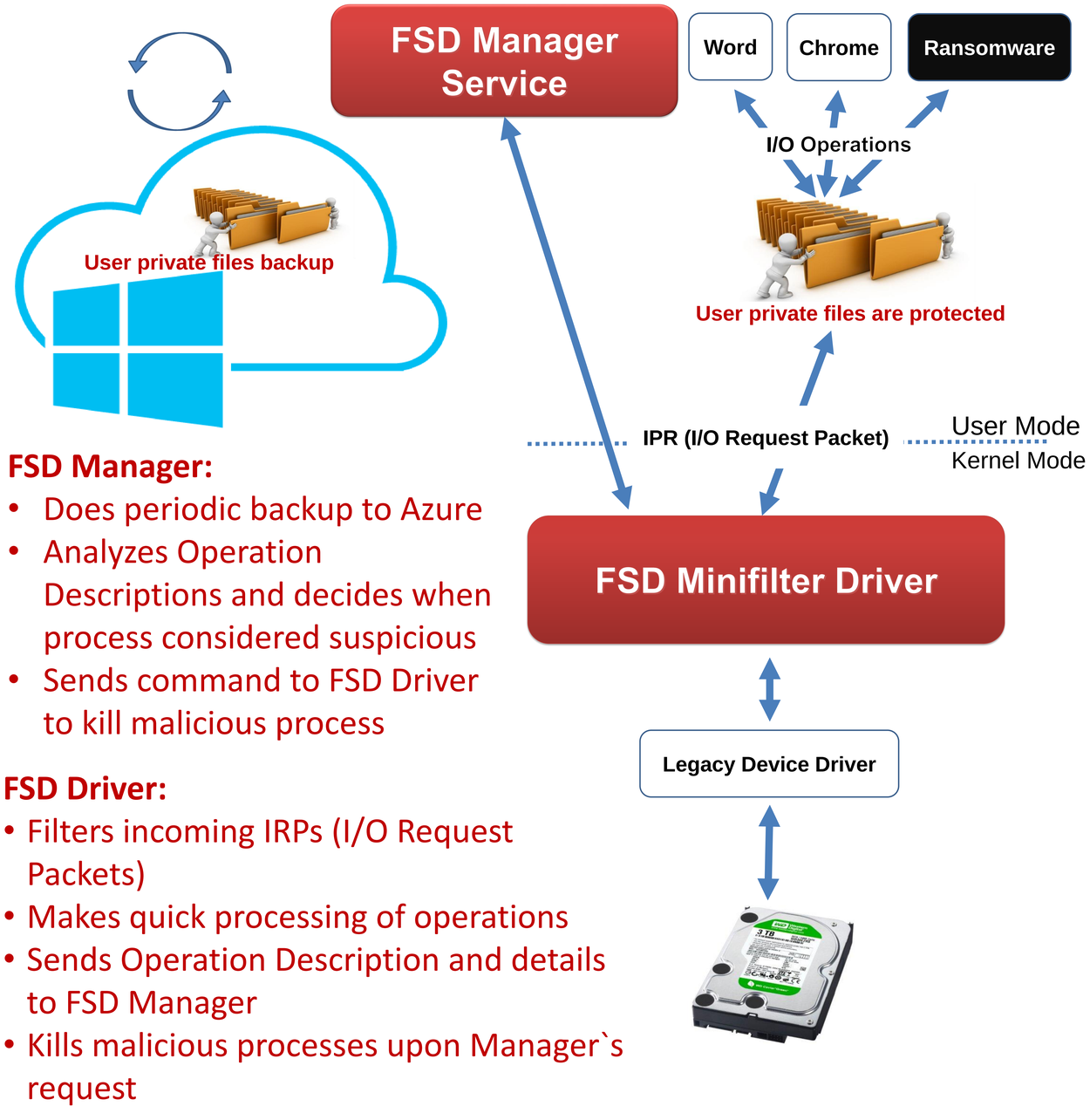
Alexander Gurevich and Denys Svyshchov

Prof. Eli Biham, Assaf Rosenbaum, Dr. Nir Levy

**FSD protects your PC against ransomware and guaranties zero file loss even in case of successful Ransomware attack.**

**We protect your private files and backup them to Azure Cloud Storage.**

**FSD uses kernel module to filter filesystem activities and uses heuristics to detect Ransomware like behavior.**




**FSD Manager:**

- Does periodic backup to Azure
- Analyzes Operation Descriptions and decides when process considered suspicious
- Sends command to FSD Driver to kill malicious process

**FSD Driver:**

- Filters incoming IRPs (I/O Request Packets)
- Makes quick processing of operations
- Sends Operation Description and details to FSD Manager
- Kills malicious processes upon Manager`s request

**Detection techniques:**

- ✓ **Measurement of writes entropy (Shannon`s entropy)**
  - Ransomware used to write encrypted data => high entropy writes
- ✓ **Comparison of file modification**
  - After ransomware finishes encryption of file, the data changes significantly
  - Bulk modifications of user data should considered suspicious
- ✓ **File type changes**
  - Ransomware usually changes file types when it does the encryption
- ✓ **Statistics of file access types**
  - Multiple deletion of user files may indicate malicious activity

**Only triggering of multiple indicators will be considered malicious activity.**

CYBER LAB
Cyber, Cryptology and Computer Security lab

Microsoft