COMP7370 Advanced Computer and Network Security

Cold Boot Attacks on Encryption Keys

A memory remanence attack aims to obtain memory images and recover cryptographic keys from DRAM after a reset or moving the DRAM to another system.

1. Motivation: How to attack encrypted disks?
   - Obtain memory images (step 0)
   - Identifying keys in memory (step 1, but we need step 0)
   - Attack encrypted disks using reconstructed keys (step 3)

2. Overview
   - Characterizing Remanence Effects
   - Imaging Residual Memory
   - Key Reconstruction
   - Identifying Keys in Memory
   - Attacking Encrypted Disks

3. DRAM Remanence Effects
   - Computer's memory is erased almost immediately when it loses power. Is this true?
   - Ordinary DRAMs typically lose their contents gradually over a period of seconds
   - Why do DRAMs lose their contents?
     - DRAM cell is essentially a capacitor.
     - Over time charge will leak and cell will lose its state
     - To forestall this, cell must be refreshed
     - Standard refresh time is order of ms
   - Data will persist for minutes or even hours if the chips are kept at low temperatures

4. **Discussions:** How will you study the remanence effect (decay if not refreshed) of DRAMs?
   - Factors: (1) time; (2) types of chips; (3) types of machines; (4) temperature
   - Metrics: % of decayed memory = error rate
   - How to measure? read back these memory regions after varying periods of time without refresh and under different temperature conditions, and measured the error rate of each sample.
   - How to present results:
     - x-axis is time; y-axis is % decay.
     - Under different machines/DRAM chips
     - Under different temperatures

5. Decay at operating temperature
    - See Figs 1-3
    - Question: Observations?
        - Similar shape
        - Fast data loss 2.5; slow data loss
    - Question: Indication? – the above results are the evidence for what?
        - Decay times (even the shorter times) are long enough to facilitate most of DRAM attacks.
    - Suggestions for your research:
        - Any claim must be supported by evidence.
        - e.g., If you claim that you can attack DRAM, you need to show evidence.

6. Decay at reduced temperature
    - Question: how to reduce temperature for DRAMs?
        - “canned air” duster products
        - dry ice
    - See Table 2
    - Question: Observations?
        - Very low decay rate under low temperature
    - Question: Indication?
        - Data in DRAMs may be recoverable for hours or days with sufficient cooling.
        - Evidence?: cut power for 60 seconds would recover 99.9% of bits correctly.
    - See Fig. 4 (slide 8-11 in coldboot.ppt)
    - Decay patterns and predictability
        - A few always decayed to the opposite value
        - Order in which different cells decayed is highly predictable.

7.