COMP7370 Advanced Computer and Network Security

CloudAV: N-Version Antivirus in the Network Cloud (3)

Topics:

1. Motivations
2. Basic Ideas

Topic 1: Motivations (Limitations)

- Antivirus software
  - Malicious/unwanted software
  - $10 billion dollars (2008)
  - What Antivirus software are you using?
  - Methods:
    - Signature based detection
    - Heuristic-based detection, like malicious activity detection
    - Rootkit detection
- Vulnerability Window
  - threat appears to signature created
  - create signatures for all new threats <- one antivirus vendor? (Slides 1/2)
  - **Question:** How to measure Vulnerability Window?
    - Malware samples (Nov 11, 06 – 07)
  - **Discussions**:
    - Observations?
- Antivirus (AV) vulnerabilities
  - severe vulnerabilities in AV
  - see slide 3
  - **Question:** Observation?
  - **Future research:** Why some are more vulnerable than the others?
  - **Question:** What is the implication?

Topic 2: Basic Ideas

- From Host-Based to Server-based
  - How to implement? In-cloud detection
  - Pros of in-cloud detection**?**
    - No update.
    - Reduce cost.
    - Lightweight host
- N-Version protection
  - Multiple detection engines
  - N-version programming
  - Parallel computing
- Environment
  - Networks
    - Enterprise (good connectivities)

    - Government (highly controlled)
    - Mobile (lightweight)
- Problems:
    - Privacy
    - Network traffic