COMP7370 Advanced Computer and Network Security

Announcement: midterm exam – March 3rd, 2011.

CloudAV: N-Version Antivirus in the Network Cloud (4)

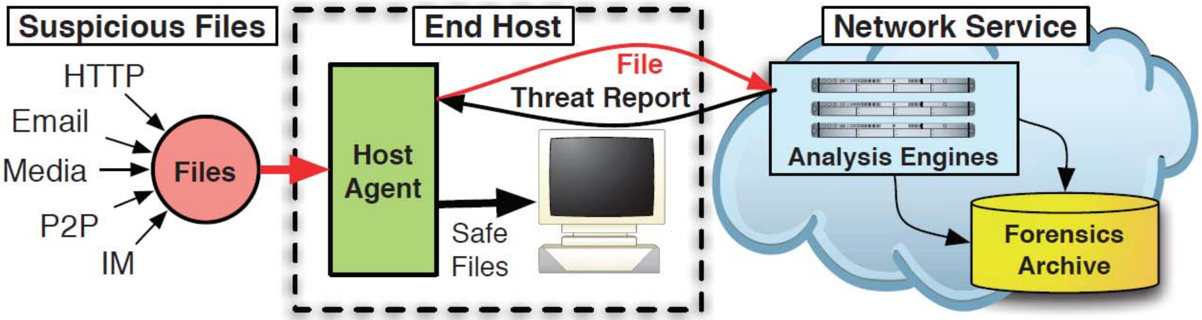
Topics:

1. Architecture and Design Issues
2. Evaluation (not covered, next time)

Topic 1: Architecture

- Basic ideas:
    - N-Version protection
    - host-based to server-based: what benefits?
        - host agent may be disabled by attackers.
        - Good performance; multiple agents
    - cloud computing

- Three components.
    - Client software
    - Network service
    - Archival/forensics service
    - Can you outline architecture of CloudAV?
        - Individual exercise (5 min)
        - Group discussion



- Client software
    - File unique identifier.
        - many files, which one has been analyzed?
        - MD5 or SHA-1
    - User interface
        - Transparent mode
        - Warning mode
        - Blocking mode

- Network service
  - Detection engines
    - A cluster of servers
    - Update signatures at a central source
  - Aggregation
    - Problems:
      a) Detector may fail.
      b) Detector may be very slow
      c) Solution?: use subset
    - How to determine a file is malicious? (threshold)
      a) e.g. strict police: single engine
      b) send a report to client/host
  - cache: (improve performance)
    - what should be cached? reports
    - Where to cache? Client and server

Topic 2: Evaluation

- Malware Dataset
  - Arbor Malware Library
  - X-axis is time; y-axis is detection rate
    - Use different datasets
- Results
  - Compare cumulative executable launches with unique executable launches
    - what do you observe ?
    - what is the indication?