Antivirus Techniques and IBM's Digital Immune System

The Antivirus Problem

5 Definition 1: Virus

- A computer program that spreads or is spreaded over computer systems.
- It invokes unwanted operations or compromise security on the infected system.

5 Definition 2: The Antivirus Problem

- Distinguish between virus-free and virus-infected programs or systems.
- Stop any mal-functioning caused by the infection
- Remove the viral codes, and, if possible, restore the programs or systems back into normal state.
Goal of Antivirus Systems

1. Reliably detect and distinguish viral codes from non-viral codes.
2. Block abnormal behaviors caused by the virus.
3. Remove virus from the protected system.
4. Restore or maintain the usefulness of the protected system.

Virus Hiding Techniques

1. Compressed
   - Virus stored in compressed form.
2. Stealth
   - Virus intercept system interrupts to fool antivirus softwares, thus avoid being detected.
3. Polymorphic
   - Virus encrypt itself using different encryption keys each time it spreads.
Antivirus Categorizations

5 Order of Play:
5 Play First
   • Behavior blocking
   • Integrity checking
   • Access control
5 Play Second
   • Scanning methods
   • Virtual machine analysis

5 Time of Play:
5 On-Access
   • Virus are checked automatically upon program execution or data access.
5 On-Demand
   • Virus are checked upon user's request.

Technique 1: Scanners

5 Good Points
5 Very few false alarms
5 ‘Play second’ (some can also partially "Play first")
5 Can be very fast
5 Can usually disinfect infected files

5 Bad Points
5 Need updating
5 May have problems with polymorphic viruses
Technique 2: Integrity Checkers

5 **Good Points**
5  Shouldn’t need updating

5 **Bad Points**
5  "Play first" (and not very well)
5  Cannot find viruses, only changes
5  Many false alarms, and some false negative
5  Ineffective against macro viruses

Technique 3: Behavior Blockers

5 **Good Points**
5  Shouldn’t need updating

5 **Bad Points**
5  Many false alarms, and some false negative
5  Needs very high level of technical support
5  Ineffective against macro viruses
5  No disinfection capability
Technique 4: Heuristics

5 **Good Points**
5  No updates needed
5  Detect unknown or even polymorphic viruses

5 **Bad Points**
5  Tendency for false alarms
5  May miss a number of viruses

Technique 5: Virtual Machine

5 **Good Points**
5  Catch also Trojan horses or Worms
5  Complete virus behavioral analysis
5  No updates required

5 **Bad Points**
5  Resource demanding
5  Not practical for high-level language (C, Fortran, Delphi, etc.) written viruses
Technique 6: Access Control

5 Good Points
5 Limits possible virus entry points
5 No updates required

5 Bad Points
5 No virus discrimination
5 Ineffective against viruses spread via email and the Internet
5 No disinfection capability

The Digital Immune System

5 Innate Immune System
5 Detection
5 Adaptive Immune System
5 Prescription
5 Dissemination
5 Cure (hopefully)
The Innate Immune System

- Reside on each client machine
- Traditional Scanners
- Heuristics for file infectors
- Neural networks for boot infectors
- Disinfect whenever sure and possible
- Forward difficult ones to the Adaptive Immune System

The Adaptive Immune System

- Centralized Virtual Machines
- Behavioral Analysis
- Decoy and Replication
- Autosequencing
  - Determine viral portion and their location
- Automatic signature extraction
  - Extract reliable signature for detection and disinfection
Delivery and Dissemination

5 Hierachical Active Network
5 Distribute prescription efficiently
5 Reduce average load

5 Administrator System to control and audit virus/prescription transmission
5 Quarantine: address epidemics, reduce peak load
5 Encryption: maintain security and safety
5 Automation: decrease overload possibility

Virus Epidemics Nature

![Graph showing the incidence of various viruses over time](image-url)
Conclusion

1. Antivirus: theoretically a loser
   - Exist no algorithm that can detect all viruses
   - Exist virus which is undetectable

2. Practical solutions:
   - Fastly evolving
   - New tools / systems to fight new threats, such as integration of torjan horse, worms, and viruses
   - Intersection with IDS when computer programs become "smarter" and more powerful