Network Security

Asim Rasheed

Where we are …

- Introduction to network security
- Vulnerabilities in IP
- I. CRYPTOGRAPHY
  - Symmetric Encryption and Message Confidentiality
  - Public-Key Cryptography and Message Authentication
- **II. NETWORK SECURITY APPLICATIONS**
  - Authentication Applications (Kerberos, X.509)
  - Electronic Mail Security (PGP, S/MIME)
  - IP Security (IPSec, AH, ESP, IKE)
  - Web Security (SSL, TLS, SET)
- **III. SYSTEM SECURITY**
  - Intruders and intrusion detection
  - **Malicious Software (viruses)**
  - Firewalls and trusted systems

Malicious Software

On War, Carl Von Clausewitz

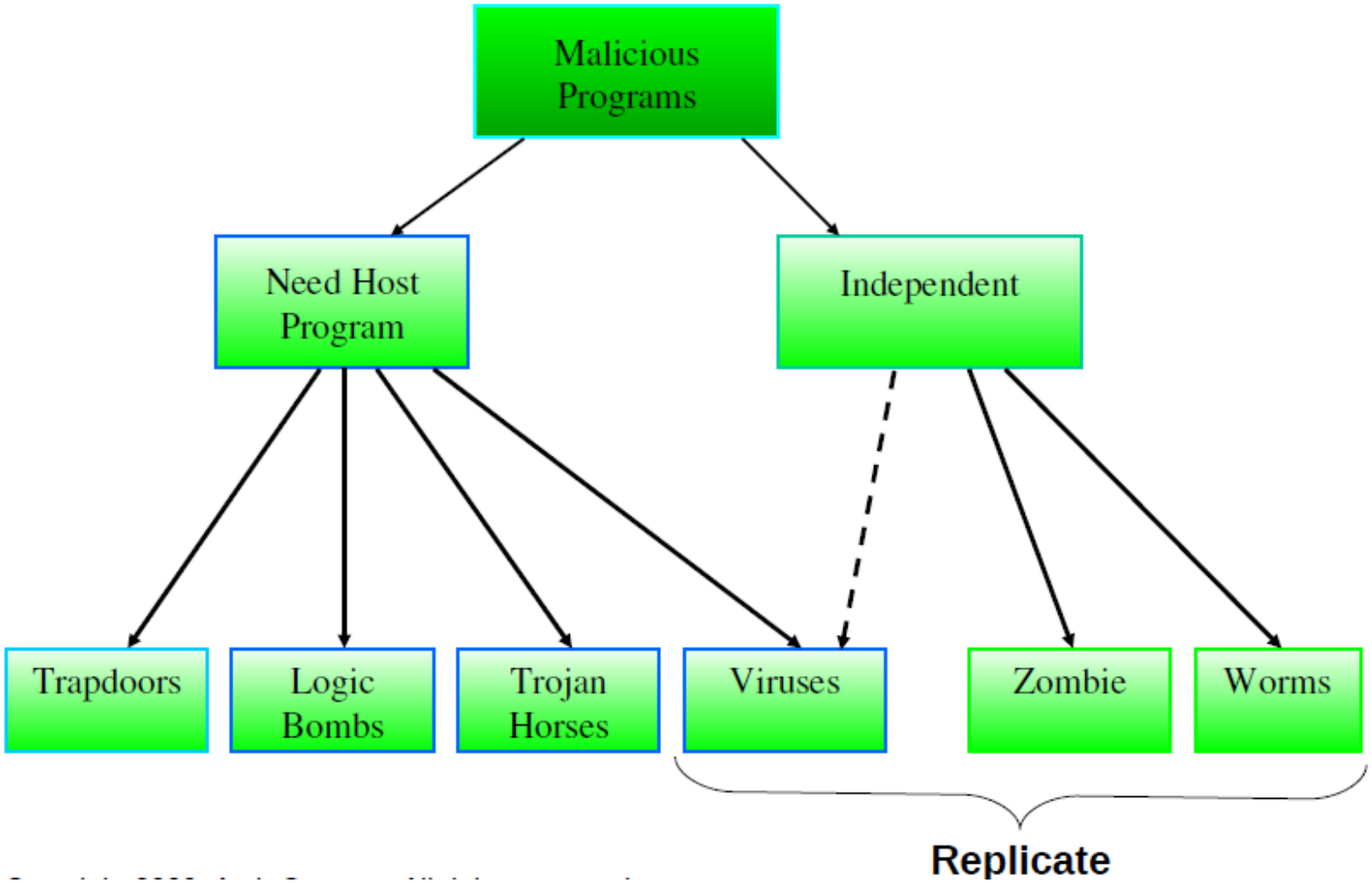
What is the concept of defense: The parrying of a blow.

What is its characteristic feature: Awaiting the blow.

Malicious Software

- Software threats or malicious code can be divided into two categories
  - That needs a host program
    - Fragments of program that cannot exist independently
  - That are independent
    - Self contained programs that can be scheduled and run by the OS
- Software threats can be differentiated as:-
  - Those replicate e.g., viruses, worms, etc.
  - Those do not replicate e.g., trap doors, logic bombs, etc.

Malicious Software



Trapdoors

- Secret entry point into a program
- Allows those who are aware of trap door to access
  - Bypassing usual security procedures
- Have been commonly used by developers
- A threat when left in production programs
  - Allowing exploitation by attackers
- Very hard to block in O/S
- Requires good SW development & update

Logic Bomb

- One of oldest types of malicious software
- Code embedded in legitimate program
- Activates when specified conditions are met
  - e.g., presence/absence of some file
  - particular date/time
  - particular user
- When triggered, typically damages system
  - modify/delete files/disks

Trojan Horse

- Program with hidden side-effects
- Which is usually superficially attractive
  - e.g., game, s/w upgrade etc
- When run, performs some additional tasks
  - Allows attacker to indirectly gain access they do not have access directly
- Often used to propagate a virus/worm or install a backdoor
- Or simply to destroy data

Zombie

- Program which secretly takes over another networked computer
- Then uses it to indirectly launch attacks
- Often used to launch Distributed Denial of Service (DDoS) attacks
- Exploits known flaws in network systems

Viruses

- Set of instructions that can infect other programs by modifying them
- A piece of self-replicating code attached to some other code
  - Like a biological virus
- Both propagates itself & carries a payload
  - Carries code to make copies of itself as well as code to perform some covert task

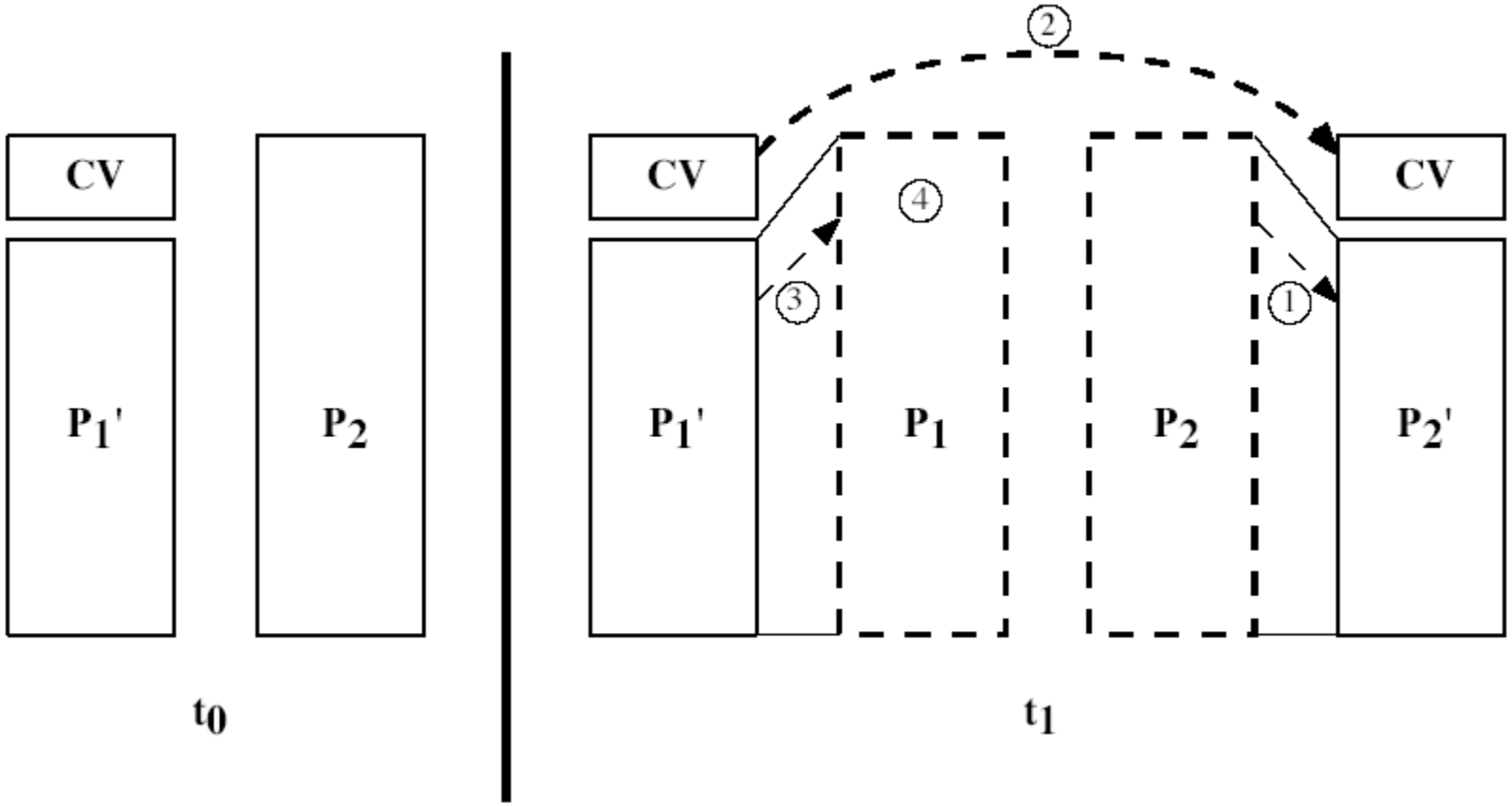
Virus Operation

- Virus phases:
  - Dormant – waiting on trigger event
  - Propagation – replicating to programs/disks
  - Triggering – by event to execute payload
  - Execution – function is performed
- Details of functionality
  - Usually machine/OS specific
- Exploiting features/weaknesses of that machine or OS
- Virus can be pre-pended or post-pended to an executable program

Virus Operation

- When infected program is invoked, it first executes the virus code
- Viruses can be detected by program length
  - Length of infected program is greater than the original program
- To avoid this the virus compresses the infected program equal to its original length

Compression Virus



Types of Viruses

- Can classify on basis of how they attack
- Parasitic virus
  - Attaches itself to executable files, and replicates when infected program executes
- Memory-resident virus
  - Lodges in main memory as part of resident program
  - Then effects every program that executes
- Boot sector virus
  - Infect master boot record and spreads when a system is booted from the disk containing virus

Types of Viruses

- Stealth virus
  - Explicitly designed to hide itself from detection
- Polymorphic virus
  - Mutates with every infection, making detection by the signature of the virus impossible

Macro Virus

- **Macro code attached to some data file**
- Interpreted by program using file
  - e.g., Word/Excel macros
  - especially using auto command & command macros
- Is a major source of new viral infections
- Blurs distinction between data and program files making task of detection much harder
- Classic trade-off: "ease of use" vs "security"

Reasons for Threat

- Macro virus is platform independent
  - All macro viruses infect MS Word documents
  - Any hardware or platform supporting Word can be infected
- Infects documents not executable portions of code
  - Most of the information in computer system is in form of a document
- Macro viruses can easily spread
  - Through emails

Email Virus

- Spreads using email with attachments containing a macro virus
  - like Melissa
- Triggered when user opens attachment
- Or worse even when mail viewed by using scripting features in mail agent
- Usually targeted at Microsoft Outlook mail agent & Word/Excel documents

Worms

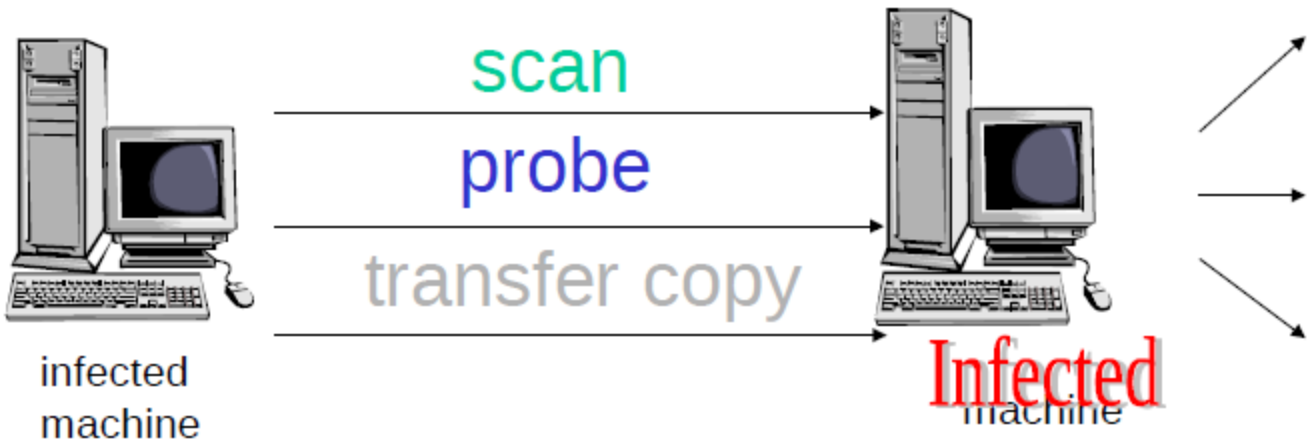
- Typically spreads over a network
  - like Morris Internet Worm in 1988
  - led to creation of CERTs
- Using users distributed privileges or by exploiting system vulnerabilities
- Widely used by hackers to create **zombie PC's**
  - subsequently used for further attacks, especially DoS
- Major issue is lack of security of permanently connected systems, especially PC‘s

Worms

- Characteristics similar to email virus
- Worm actively seeks out machine to infect
- Network worm propagates using network connections
- Once active it can behave as:
  - A virus
  - Can implant a Trojan horse program
  - Perform any number disruptive or destructive actions

How an Active Worm Spreads

- Autonomous
- No need of human interaction



Worm Replication Techniques

- Electronic mail facility
  - Mails a copy of itself to other systems
- Remote execution capability
  - Worm executes a copy of itself on another system
- Remote login capability
  - Worm logs onto a remote system as a user and then uses commands to copy itself

Worm Operation

- Worm phases like those of viruses:
  - Dormant
  - Propagation
    - Searches for other systems to infect
    - Establishes connection to target remote system
- Replicates itself onto remote system
  - Triggering
  - Execution

Morris Worm

- Best known classic worm
- Released by Robert Morris in 1988
- Targeted Unix systems
- Using several propagation techniques
  - Simple password cracking of local password file
  - Exploit bug in finger daemon
  - Exploit debug trapdoor in sendmail daemon
- If any attack succeeds then replicated self

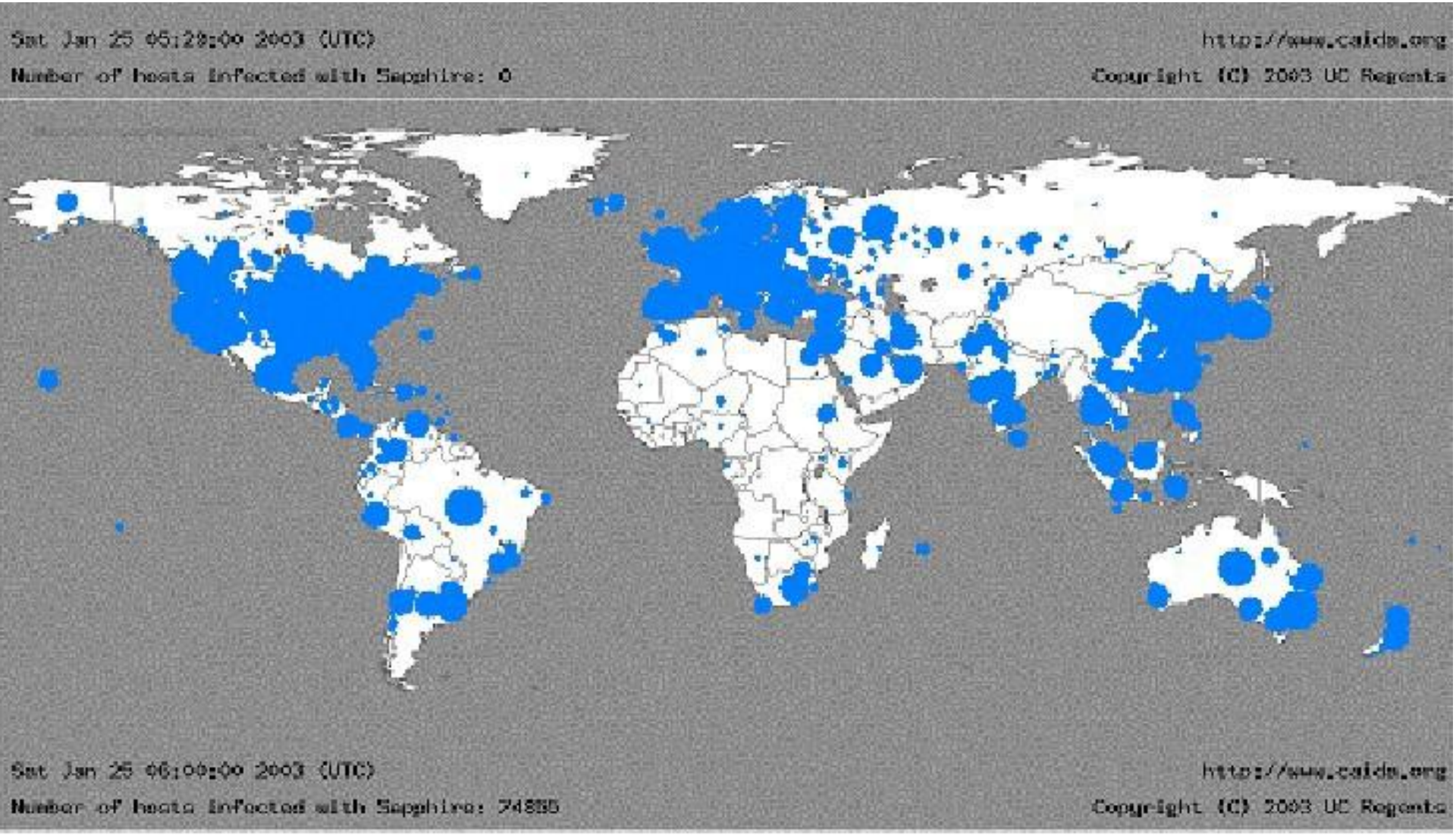
Famous Worm Attacks from mid-01

- Code Red
  - Exploited bug in MS IIS to penetrate & spread
  - Probes random IPs for systems running IIS
  - Had trigger time for denial-of-service attack
  - 2nd wave infected 360,000 servers in 14 hours
- Code Red 2
  - Had backdoor installed to allow remote control

Famous Worm Attacks from mid-01

- Nimda
  - Used multiple infection mechanisms
    - email, shares, web client, IIS, Code Red 2 backdoor
- Slammer
  - Infected nearly 75,000 Microsoft SQL servers. Attack
  - finished in less than one hour

Spread of the Slammer in 30 Mins



Virus Countermeasures

- Viral attacks exploit lack of integrity control on systems
- To defend need to add such controls
- Ideal solution is **Prevention - block virus** infection mechanism.
- Next best thing is:
  - Detection - of viruses in infected system
  - Identification - restoring system to clean state
  - Removal – remove all traces of the virus and restore the program to its original state

Anti-Virus Software

- First-generation
  - Scanner uses virus signature to identify virus
  - Or change in length of programs
- Second-generation
  - Uses heuristic rules to spot viral infection
  - Or uses program checksums to spot changes
- Third-generation
  - Memory resident prog identify virus by actions
- Fourth-generation
  - Packages with a variety of antivirus techniques
  - e.g., scanning & activity traps, access-controls

Advanced Anti-Virus Techniques

- Generic decryption
  - Use CPU simulator to check program signature & behavior before actually running it
- Digital immune system (IBM)
  - General purpose emulation & virus detection

Generic Decryption

- Enables the antivirus program to detect easily the most complex polymorphic viruses
- Fast scanning speed
- Executable files are run through GD scanner, which contains
  - CPU emulator
    - Virtual computer that interprets instructions in an executable file
    - Emulator includes software versions of all registers and other processor hardware, so that underlying processor is unaffected

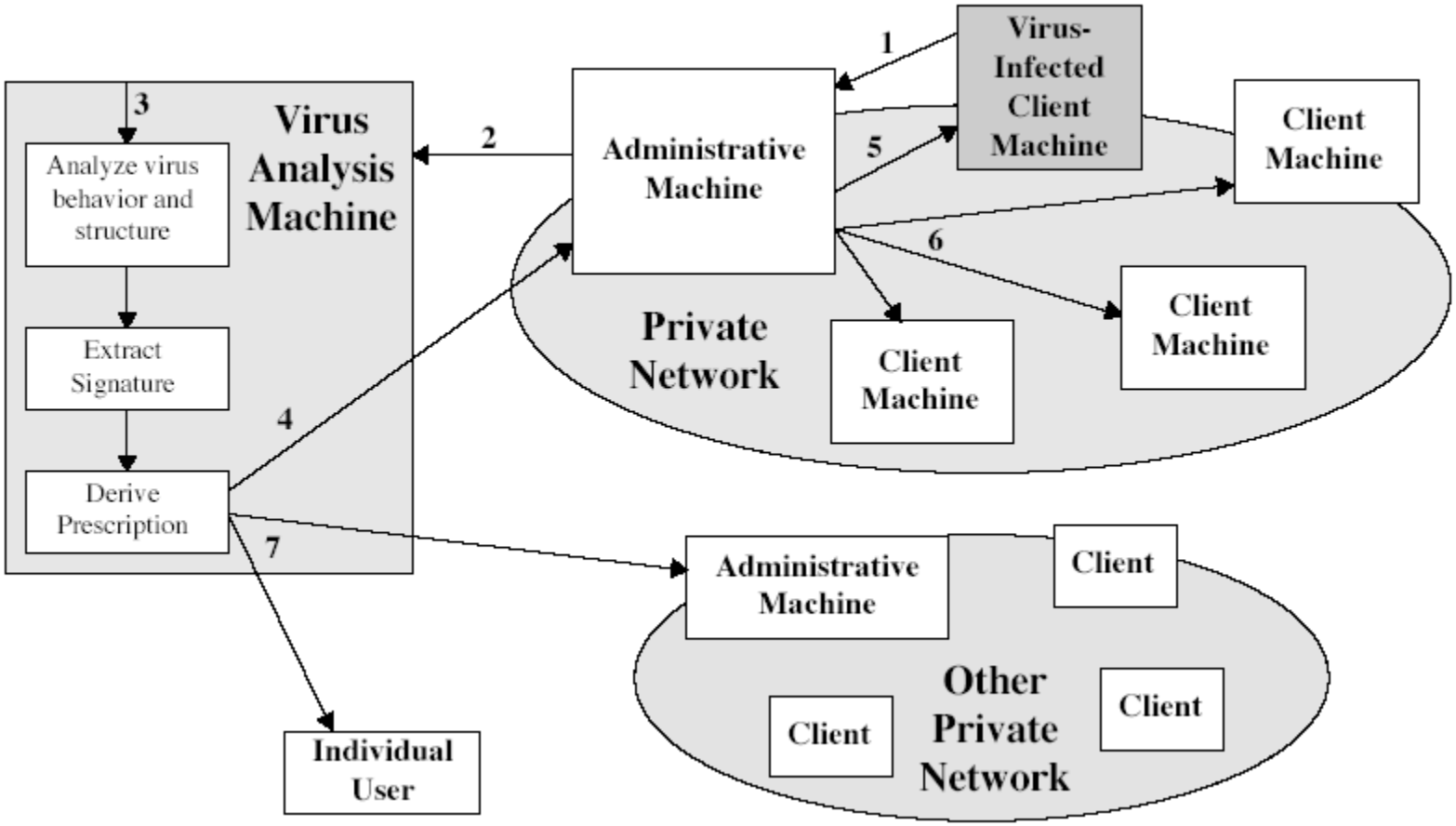
Generic Decryption

- Virus signature scanner
  - Module that scans the target code looking for known virus signatures
- Emulation control module
  - Controls the execution of the target code
- During interpretation target code can cause no damage

Digital Immune System

- Motivation for its development has been rising threat of Internet based virus propagation
- Increase in virus propagation has been due to:
  - Integrated mail systems:
    - Systems such as Microsoft Outlook makes it very simple to send anything to anyone
  - Mobile program codes:
    - Java and ActiveX allow programs to move on their own from one system to another

Digital Immune System



Digital Immune System Operation

- Expands on Generic Decryption
- Monitoring program uses a variety of heuristics to infer that virus may be present
  - Forwards a copy of infected program to an administrative machine
- Administrative machine encrypts the sample and sends it to a central virus analysis machine
- This machine creates an environment to analyze the infected program and generates a prescription

Digital Immune System Operation

- Prescription is sent to administrative machine
- Administrative machine forwards it to infected machine
- Other clients are also sent this prescription
- Subscribers receive regular antivirus updates

Behavior-Blocking Software

- Integrated with host O/S
- Monitors program behavior in real-time for possibly malicious actions
  - e.g., file access, disk format, executables, system setting changes, network access
  - If detected can block, terminate, or seek ok
- Has advantage over scanners
- But malicious code runs before detection

Any question ?