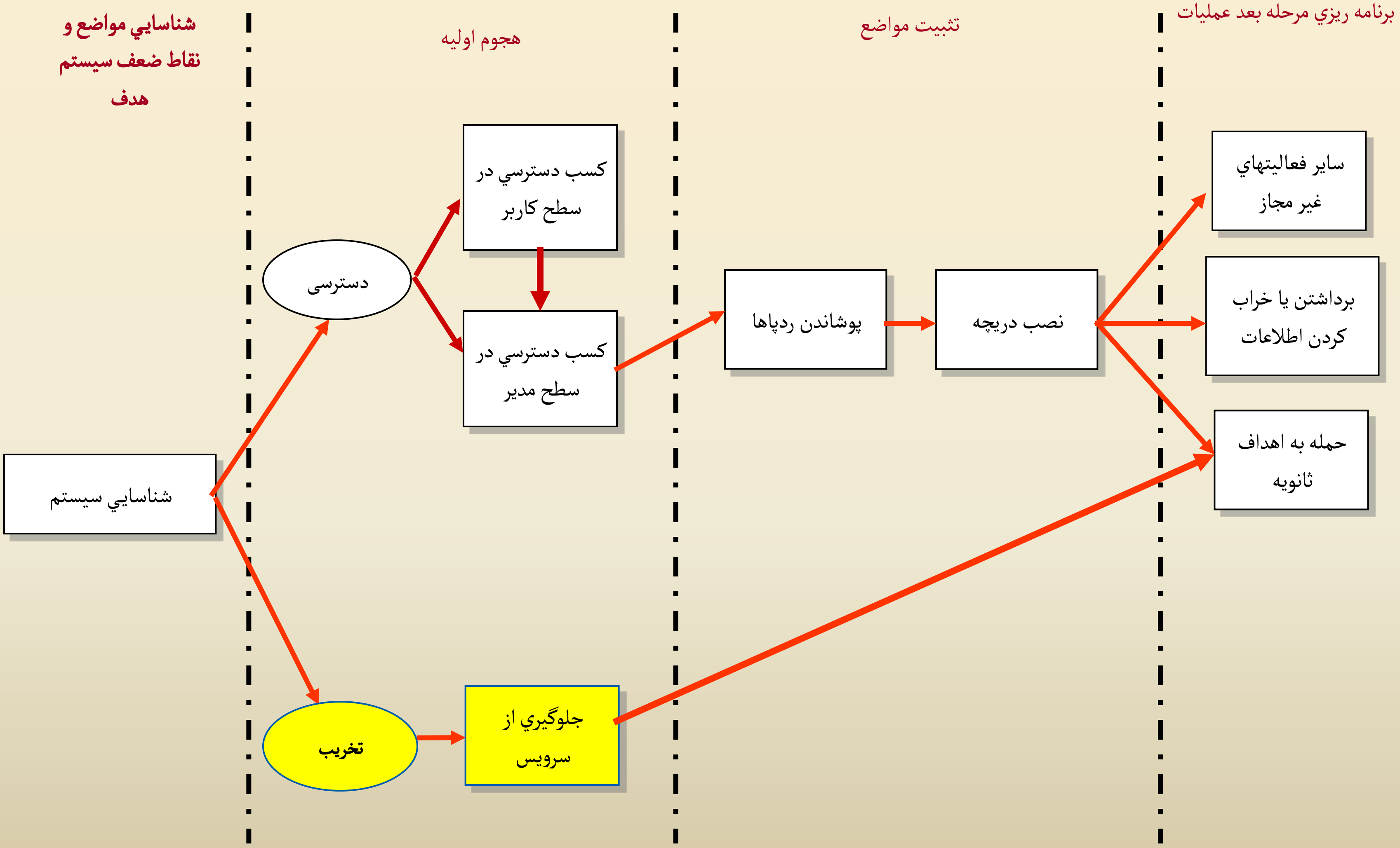
مروري بر نفوذگري و امنيت در سيستم‌هاي کامپيوتري

هجوم به قصد تخريب

روند نماي کلي انجام يک حملة کامپيوتري



شناسايي مواضع و نقاط ضعف سيستم هدف

هجوم اوليه

تثبيت مواضع

برنامه ريزي مرحله بعد عمليات

شناسايي سيستم

دسترسی

تخريب

کسب دسترسي در سطح کاربر

کسب دسترسي در سطح مدير

جلوگيري از سرويس

پوشاندن ردپاها

نصب دريچه

ساير فعاليتهاي غير مجاز

برداشتن يا خراب کردن اطلاعات

حمله به اهداف ثانويه

Contents

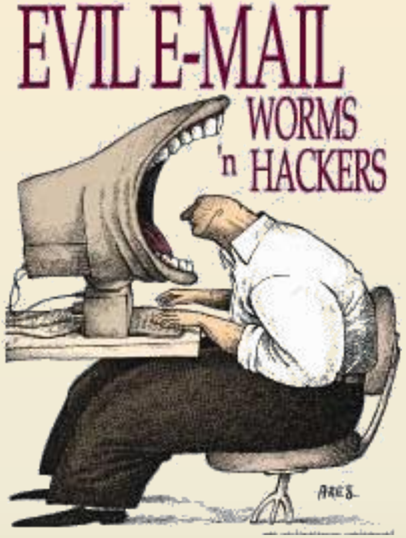
- Denial of Service attacks
  - Concepts
  - Samples of attacks
- Malicious Logic attacks
  - Concepts
  - Viruses

Denial of Service Attack

- “Attack in which the primary goal is to deny the victim(s) access to a particular resource.”
- Possible impacts: reboot your computer, Slows down computers- Certain sites, Applications become inaccessible

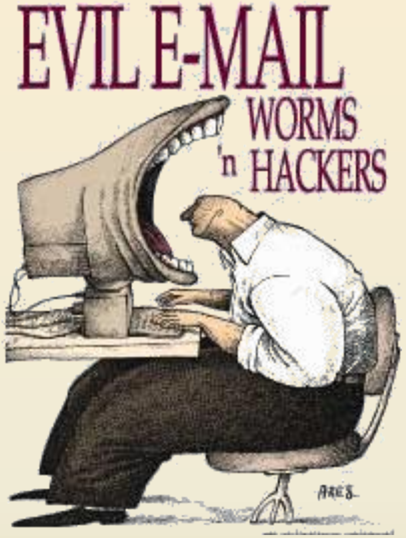
Results expected

- Denial-of-service attacks can essentially disable your computer or your network. Depending on the nature of your enterprise.

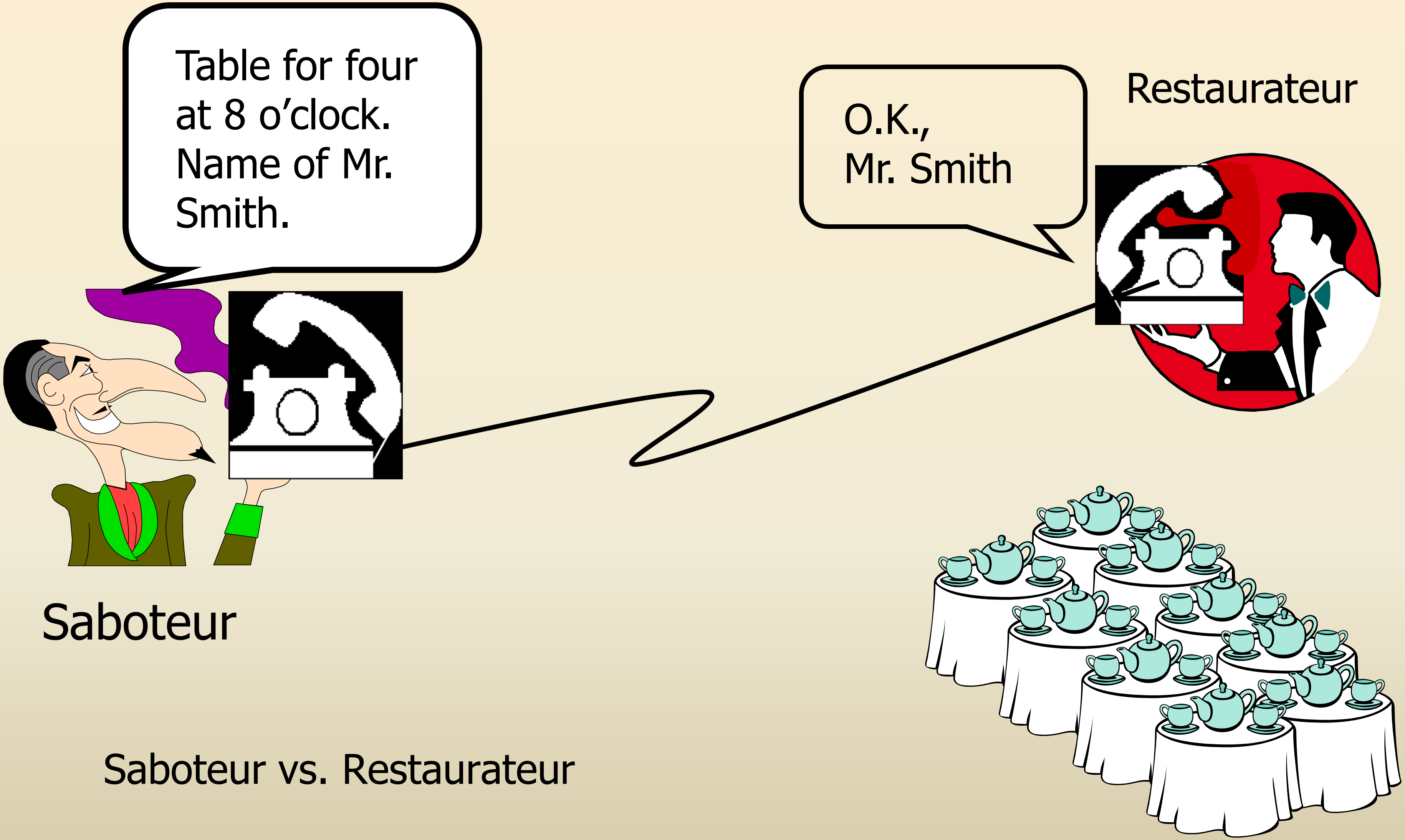


Results expected

- Some denial-of-service attacks can be executed with limited resources against a large, sophisticated site. This type of attack is sometimes called an "asymmetric attack“. For example, an attacker with an old PC and a slow modem may be able to disable much faster and more sophisticated machines or networks.



How to take down a restaurant?



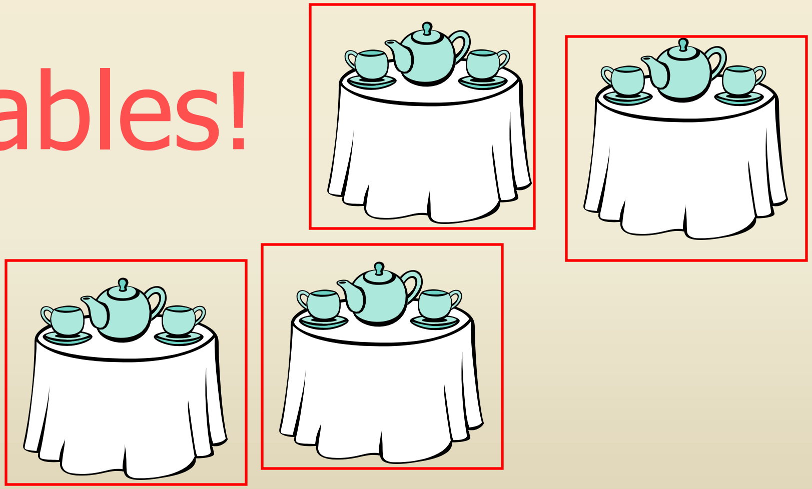
Saboteur vs. Restaurateur

How to take down a restaurant?

Restauranteur

Saboteur

No More Tables!



Categories of DoS attack

- Flood attack - This is when a system gets too much internet traffic (people trying to connect to it). The traffic uses bandwidth and the internet servers slow down and eventually stop.
- Logic and software attacks - Internet packets are sent that are supposed to use bugs in the software or system. These attacks are easier to defend against because firewall or software patches usually correct the problem.

Categories of DoS attack

- Distributed Denial-of-Service attack - This type of attack uses either flood attacks or logic attacks, but it uses many different computers under the attacker's control (see Botnet). This type of attack is one of the most often used, and usually against company websites. This type of attack is often the hardest to prevent, track, and stop.

Samples

- Ping of Death
- Smurf & Fraggle
- Land attack
- Synchronous Flooding

Ping of Death

- With a Ping of Death attack, an echo packet is sent that is larger than the maximum allowed size of 65,536 bytes. The packet is broken down into smaller segments, but when it is reassembled, it is discovered to be too large for the receiving buffer. Subsequently, systems that are unable to handle such abnormalities either crash or reboot.

- You can perform a Ping of Death from within Linux by typing

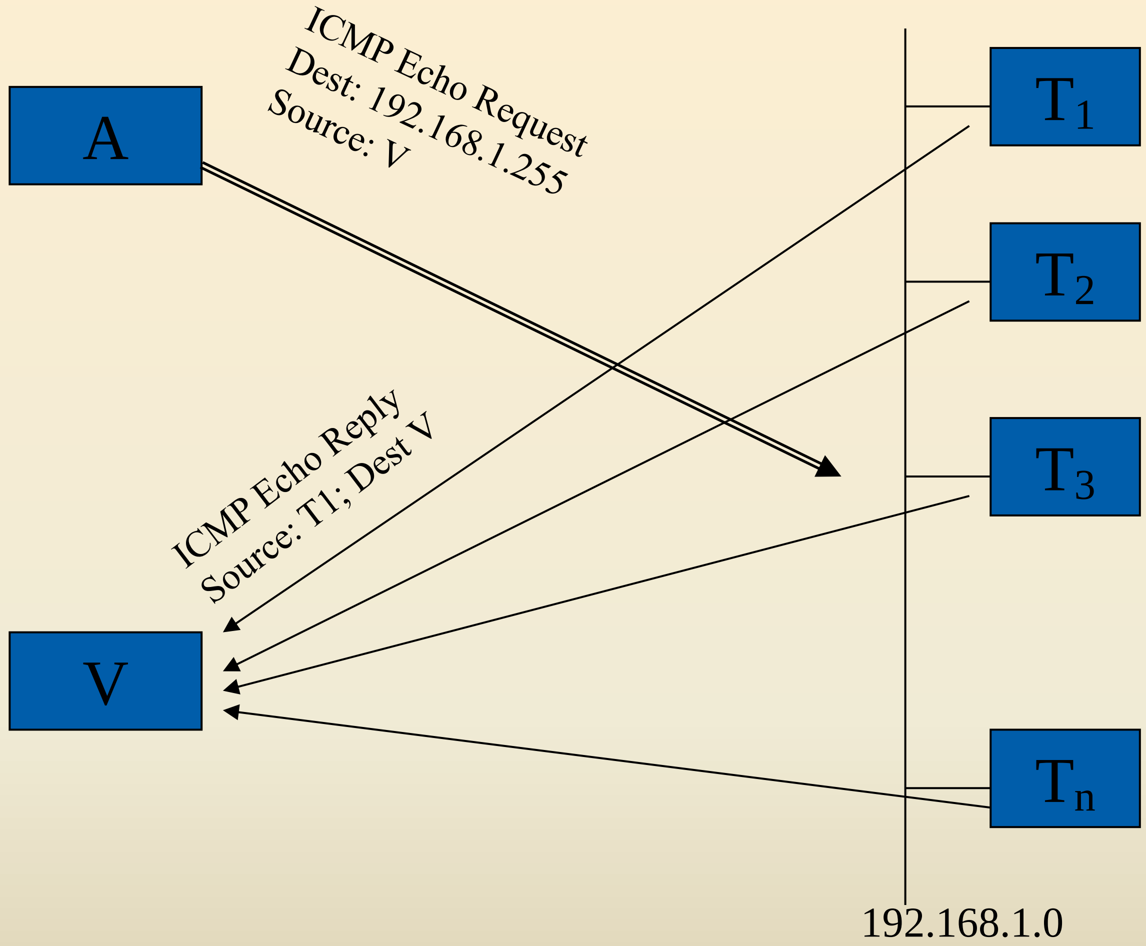
```
ping  –s 65537.
```

- Tools:
  - Jolt, Sping, ICMP Bug, IceNewk

Smurf

- A Smurf attack is another DoS attack that uses ICMP. Here, a request is sent to a network broadcast address with the target as the spoofed source. When hosts receive the echo request, they send an echo reply back to the target.
  - Sending multiple Smurf attacks directed at a single target in a distributed fashion might succeed in crashing it.

Smurf

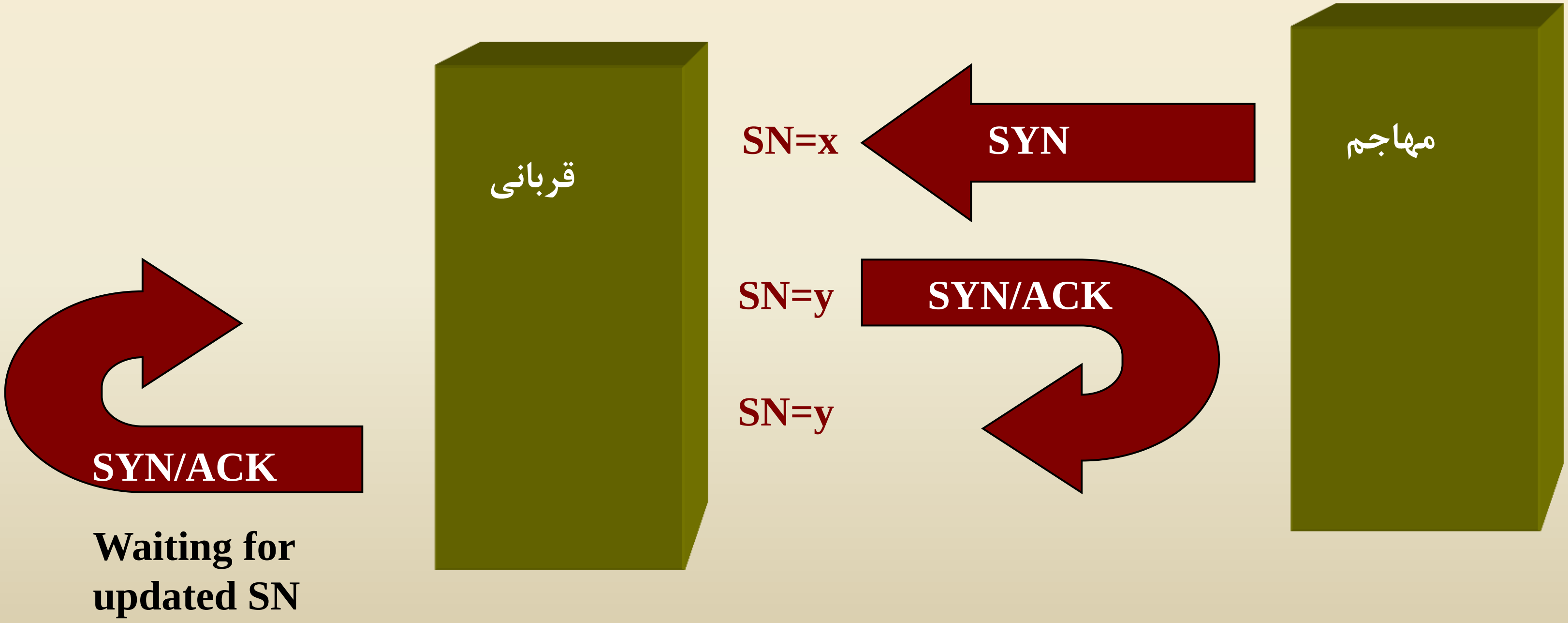

ICMP Echo Request
Dest: 192.168.1.255
Source: V
A
T$_1$
T$_2$
T$_3$
T$_n$
ICMP Echo Reply
Source: T1; Dest V
V
192.168.1.0

LAND Attack

- In a LAND attack, a TCP SYN packet is sent with the same source and destination address and port number. When a host receives this abnormal traffic, it often either slows down or comes to a complete halt as it tries to initiate communication with itself in an infinite loop.
- Although this is an old attack (first reportedly discovered in 1997), both Windows XP with service pack 2 and Windows Server 2003 are vulnerable to this attack.
- HPing can be used to craft packets with the same spoofed source and destination address.

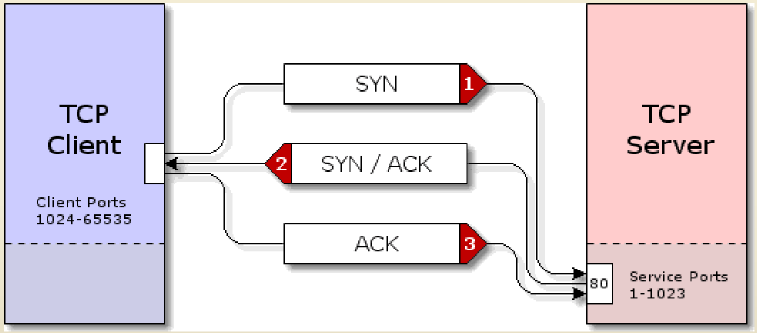
LAND Attack

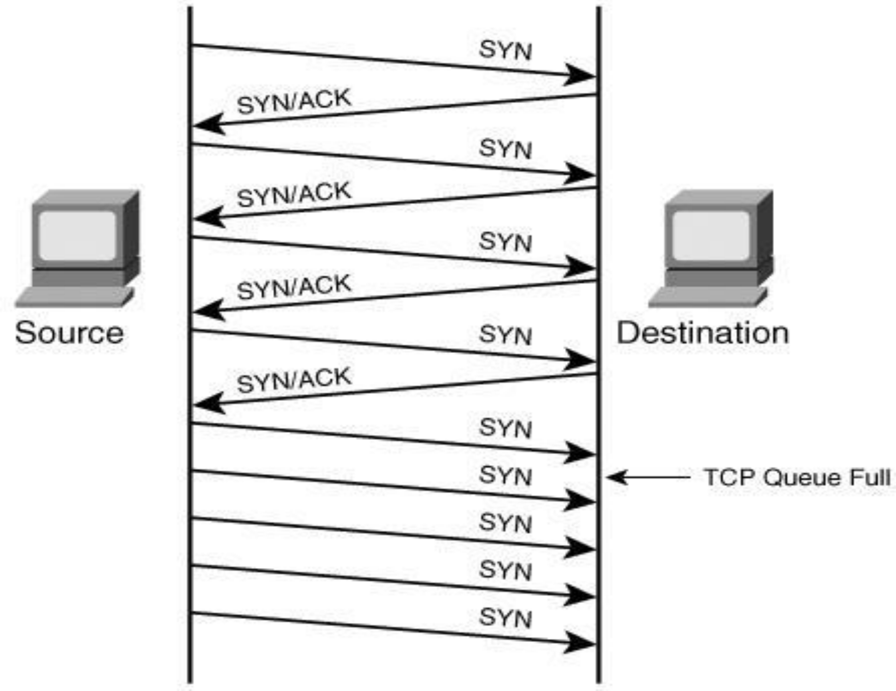
- هنگامی که قربانی SYN را دریافت می کند، شماره ترتیب را به روز کرده، ACK می فرستد، سپس بسته ای با شماره ترتیب مشابه دریافت می کند و آن را با همان شماره ترتیب برای فرستنده می فرستد تا توسط او اصلاح شود
- چون شماره ترتیب هرگز به روز نمی شود، قربانی دچار حلقه بی نهایت می شود!



Synchronous flood

- Attacker will send a flood of syn packet but will not respond with an ACK packet. The TCP/IP stack will wait a certain amount of time before dropping the connection, a syn flooding attack will therefore keep the syn_received connection queue of the target machine filled.



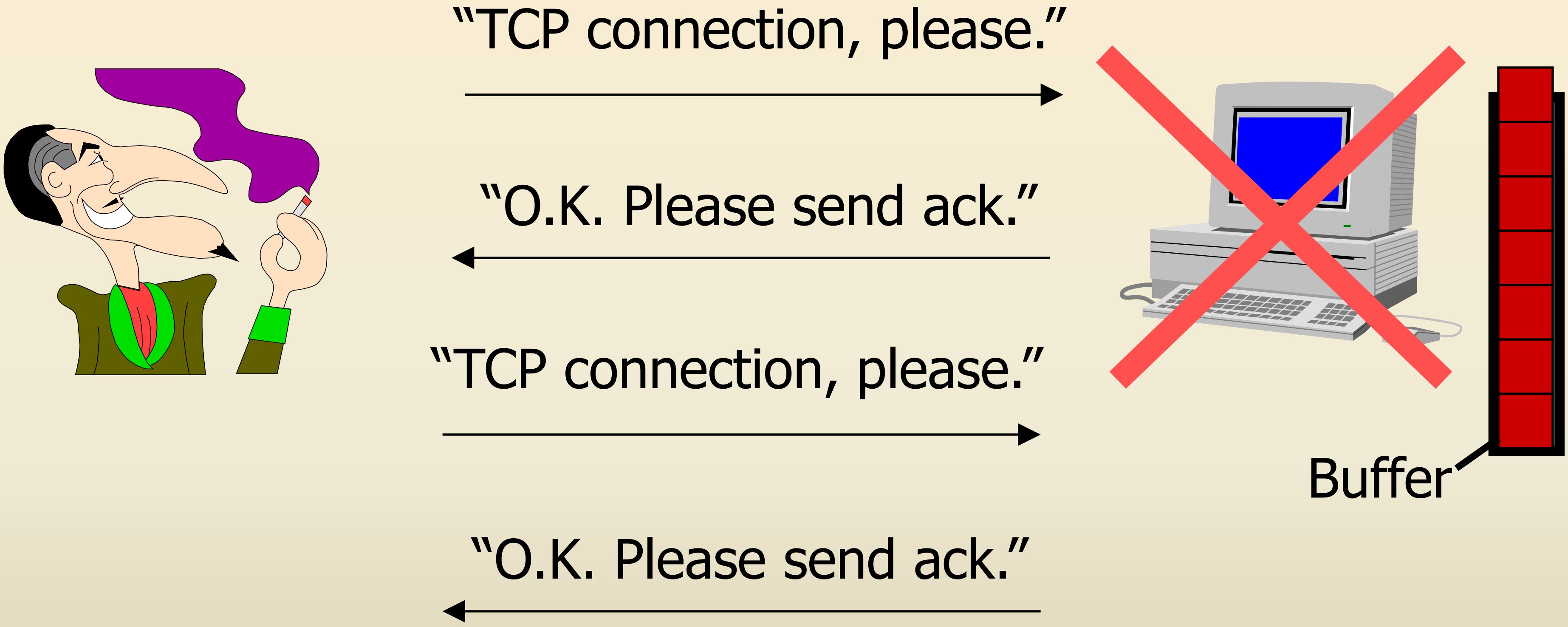


Synchronous flood

- SYN floods are still successful today for three reasons:

1) SYN packets are part of normal, everyday traffic, so it is difficult for devices to filter this type of attack.
2) SYN packets do not require a lot of bandwidth to launch an attack because they are relatively small.
3) SYN packets can be spoofed because no response needs to be given back to the target. As a result, you can choose random IP addresses to launch the attack, making filtering difficult for security administrators.

Return to our Restaurant



"TCP connection, please."

"O.K. Please send ack."

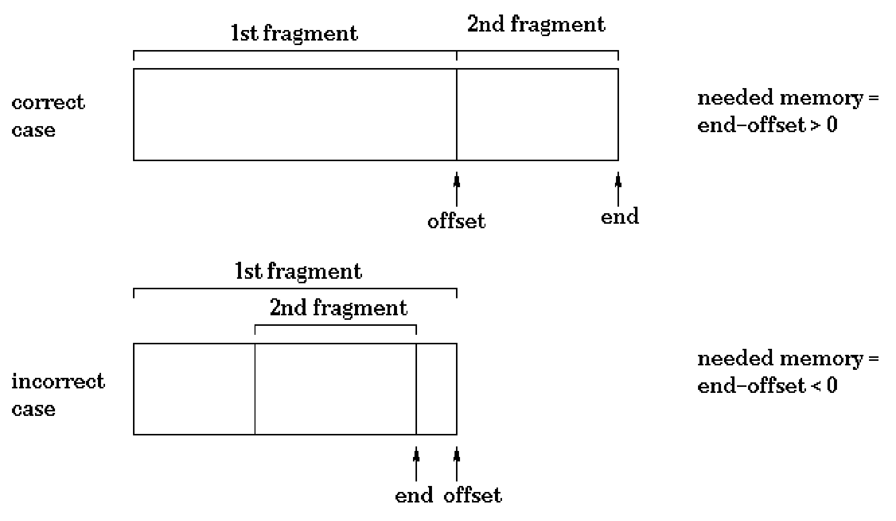
"TCP connection, please."

"O.K. Please send ack."

IP related attacks

- **IP Packet options**
  - در این روش برخی از فیلد های انتخابی بسته به صورت تصادفی تغییر داده می شوند و بسته حاصل برای قربانی ارسال می شود مثلاً بیت های مربوط به کیفیت خدمات یک می شوند و لذا باعث بالا رفتن زمان پردازش **CPU** می شود

- **Tear drop**
  - در این حمله بسته ی **IP** در اثر یک افراز غلط، به قطعه هایی تقسیم می شود که همپوشانی دارند لذا قربانی نمی تواند این بسته را دوباره از قطعه هایش بسازد. این کار باعث می شود سیستم **Crash** کند.



Tiny Fragment Attack

- uses small fragments to force some of the TCP header information into the next fragment.
- TCP flags field is forced into the second fragment and filters will be unable to test these flags in the first octet thereby ignoring them in subsequent fragments.
- can be prevented at the router by enforcing rules, which govern the minimum size of the first fragment, large enough to ensure it contains all the necessary header information

Overlapping Fragment Attack

- not a denial of service attack but used to bypass firewalls to gain access to the victim host
- can be used to overwrite part of the TCP header information of the first fragment, which contained data that was allowed to pass through the firewall, with malicious data in subsequent fragments.
  - overwriting destination port number to change from port 80 (HTTP) to port 23 (Telnet) which would not be allowed to pass the router in normal circumstances

The Unnamed Attack

- attempts to cause a denial of service to the victim host, there is a gap created in the fragments.
- done by manipulating the offset values to ensure there are parts of the fragment, which have been skipped.

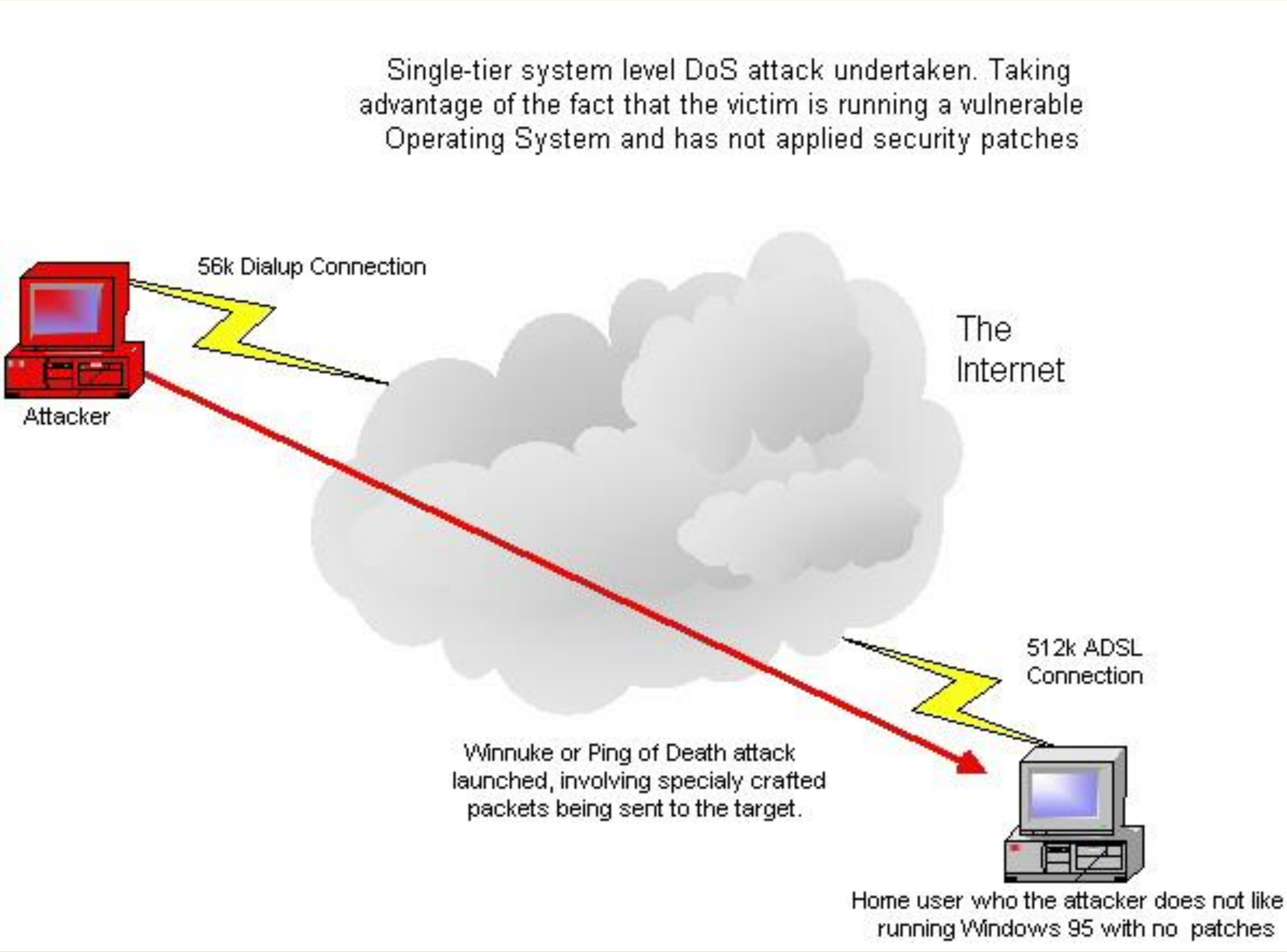
X-tire Dos Attacks

- Single-tier DoS Attacks
  - Straightforward 'point-to-point' attack, that means we have 2 actors: hacker and victim.
    - Examples: Ping of Death, SYN floods, Other malformed packet attacks
- Dual-tier DoS Attacks
  - A more complex attack model
  - Difficult for victim to trace and identify attacker
    - Examples: Smurf
- Triple-tier DDoS Attacks
  - Highly complex attack model, known as Distributed Denial of Service (DDoS).
  - DDoS exploits vulnerabilities in the Internet, making it virtually impossible to protect networks against this level of attack.
    - Examples: TFN2K, Stacheldraht, Mstream

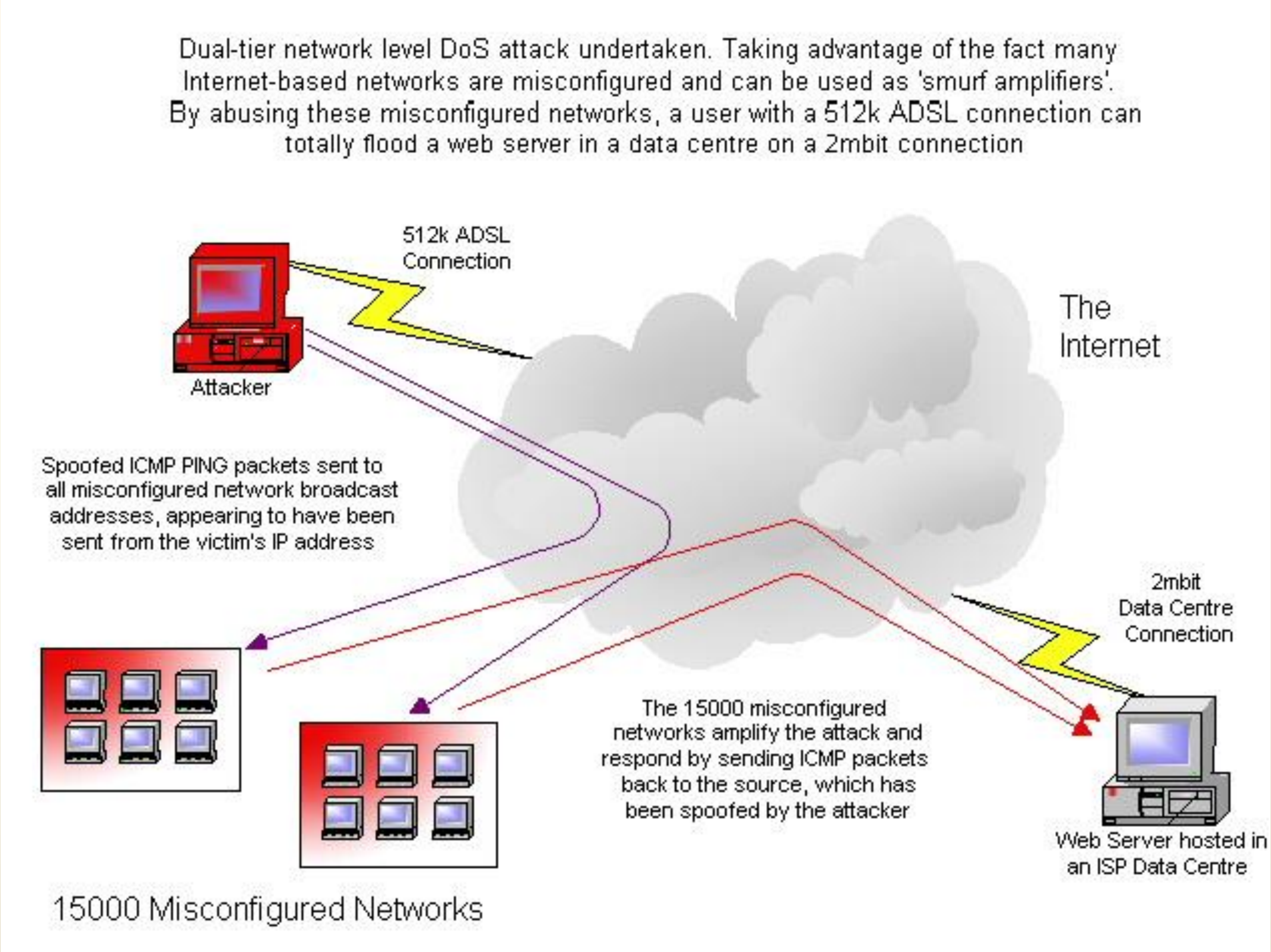
Components of a DDoS Flood Network

- Attacker
  - Often a hacker with good networking and routing knowledge.
- Master servers
  - Handful of back-doored machines running DDoS master software, controlling and keeping track of available zombie hosts.
- Zombie hosts
  - Thousands of back-doored hosts over the world

Single-tier DoS Attacks


Single-tier system level DoS attack undertaken. Taking advantage of the fact that the victim is running a vulnerable Operating System and has not applied security patches
56k Dialup Connection
Attacker
The Internet
512k ADSL Connection
Winnuke or Ping of Death attack launched, involving specialy crafted packets being sent to the target.
Home user who the attacker does not like running Windows 95 with no patches

Dual-tier DoS Attacks



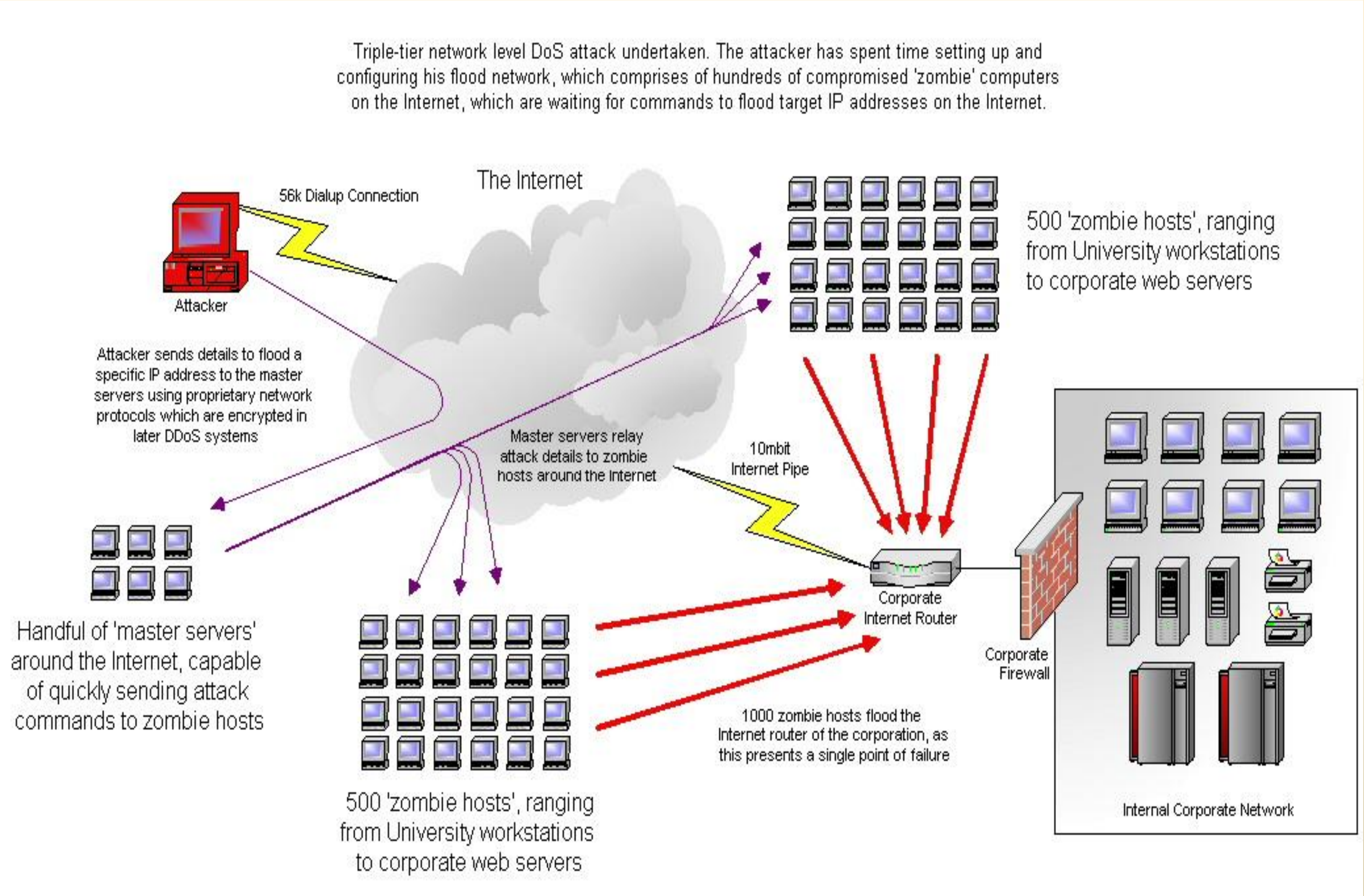
Dual-tier network level DoS attack undertaken. Taking advantage of the fact many Internet-based networks are misconfigured and can be used as 'smurf amplifiers'. By abusing these misconfigured networks, a user with a 512k ADSL connection can totally flood a web server in a data centre on a 2mbit connection

Spoofed ICMP PING packets sent to all misconfigured network broadcast addresses, appearing to have been sent from the victim's IP address

The 15000 misconfigured networks amplify the attack and respond by sending ICMP packets back to the source, which has been spoofed by the attacker

512k ADSL Connection
Attacker
The Internet
2mbit Data Centre Connection
Web Server hosted in an ISP Data Centre
15000 Misconfigured Networks

Triple-tier DDoS Attacks


Triple-tier network level DoS attack undertaken. The attacker has spent time setting up and configuring his flood network, which comprises of hundreds of compromised 'zombie' computers on the Internet, which are waiting for commands to flood target IP addresses on the Internet.
56k Dialup Connection
The Internet
Attacker
500 'zombie hosts', ranging from University workstations to corporate web servers
Attacker sends details to flood a specific IP address to the master servers using proprietary network protocols which are encrypted in later DDoS systems
Master servers relay attack details to zombie hosts around the Internet
10mbit Internet Pipe
Handful of 'master servers' around the Internet, capable of quickly sending attack commands to zombie hosts
Corporate Internet Router
Corporate Firewall
1000 zombie hosts flood the Internet router of the corporation, as this presents a single point of failure
500 'zombie hosts', ranging from University workstations to corporate web servers
Internal Corporate Network

Contents

- Denial of Service attacks
  - Concepts
  - Samples of attacks
- Malicious Logic attacks
  - Concepts
  - Viruses

Program Security

- Secure Programs: behave as expected
  - Unexpected behavior is a “program security flaw”
  - Happens because of an existing “vulnerability”

- IEEE Terminology

  Human error →

  Fault (incorrect code) →

  Failure (incorrect system behavior; external)

Patching

- One way of addressing faults: test, discover faults, patch them

- Problems:
  - No guarantee all faults are found
  - No guarantee the patch does not add another fault
    - Pressure leads to hurried patches
  - Because the entire system cannot be redesigned, there’s a limit to how much a single patch can fix because it is constrained not to affect the rest of the system (for example, a definition of a variable that is passed on to several different modules, but creates a fault only in one)

Faults will always exist

- Human error
- Complexity of system
  - The study of security finds more possibilities for flaws while software engineering proceeds to find new software techniques
- Non-malicious and malicious faults

Malicious Logic

- Pfleeger definition: "*Hardware, software, or firmware capable of performing an unauthorized function on an information system.*"
- Bishop definition: "*a set of instructions that cause a site's policy to be violated*"
- Also known as malicious code or malware
- Unintentionally faulty code can cause the same/similar effects

Types of malicious logic

Trojan Horses

- Bishop definition: “a program with an overt effect (documented or known) and a covert effect (undocumented or unexpected)
- Propagating/replicating Trojan Horse: one that creates a copy of itself
  - Might modify compiler to insert itself into programs, including future version of compiler

Types of malicious logic

Virus

- Bishop definition: “a program that inserts itself into one or more files and then performs some (possibly null) action”
- Self replicating code, parasitic (attaches to “good” code)
- Can be
  - “resident” (attaches itself to memory and can execute after its host program is done) or
  - “transient” (active only while its host is executing)

Types of malicious logic – contd.

- Worms
  - Self replicating, spread through networks
  - Stand-alone, not attached to another piece of logic
- Logic Bombs
  - Bishop definition: “a program that performs an action that violates the security policy when some external event occurs”
  - Waits for a trigger condition
  - Time bomb!

Types of malicious logic – contd.

- Trapdoors
  - Alternative means of executing code
    - Intentional – legitimate and malicious purposes
- ActiveX, Java code
  - Execution of malicious code via Java applets, ActiveX scripts
  - Malicious mobile code

Types of malicious logic – contd.

- Bacteria
  - Virus or worm that “absorbs all of some class of resource”
  - For example: self-replicating piece of code fills up disk

- Hybrids
  - Usually a mixture of above

What we talk about now

- Virus (used as a generic term for malicious code)
  - Types of viruses
  - Means of attaching
  - Anatomy of a simple virus
  - More sophisticated virus
  - Virus detection methods
  - Antivirus mechanisms

Types of virus

- Classification by where they attach
  - Boot sector viruses
  - Parasitic viruses

- Classification by type of code
  - Binary viruses: usually written in assembly language then assembled to form executable image (binary file); attaches to other binary files or boot sector.
  - Macro viruses: written in high-level macro language then interpreted (possibly after pre-processing); attaches to other files that support same macro language

Types of viruses – contd.

A general classification

- Boot sector viruses
  - Modify and reside in boot sector
  - Bishop definition: “a virus that inserts itself into the boot sector of a disk”
- Parasitic viruses
  - Attach itself to files
  - Infect executable programs
- Multipartite
  - Can infect either boot sectors or applications

Types of viruses – contd.

- Polymorphic viruses
  - Mutate like biological viruses
- Stealth Viruses
  - Hard to detect
- TSRs (Terminate Stay Resident)
  - Memory resident viruses
  - Stay active in memory after application has terminated
- LKMs (Loadable Kernel Modules)
  - Future of Unix based viruses
- Encrypted viruses
  - Encrypts all virus code except a small decryption routine

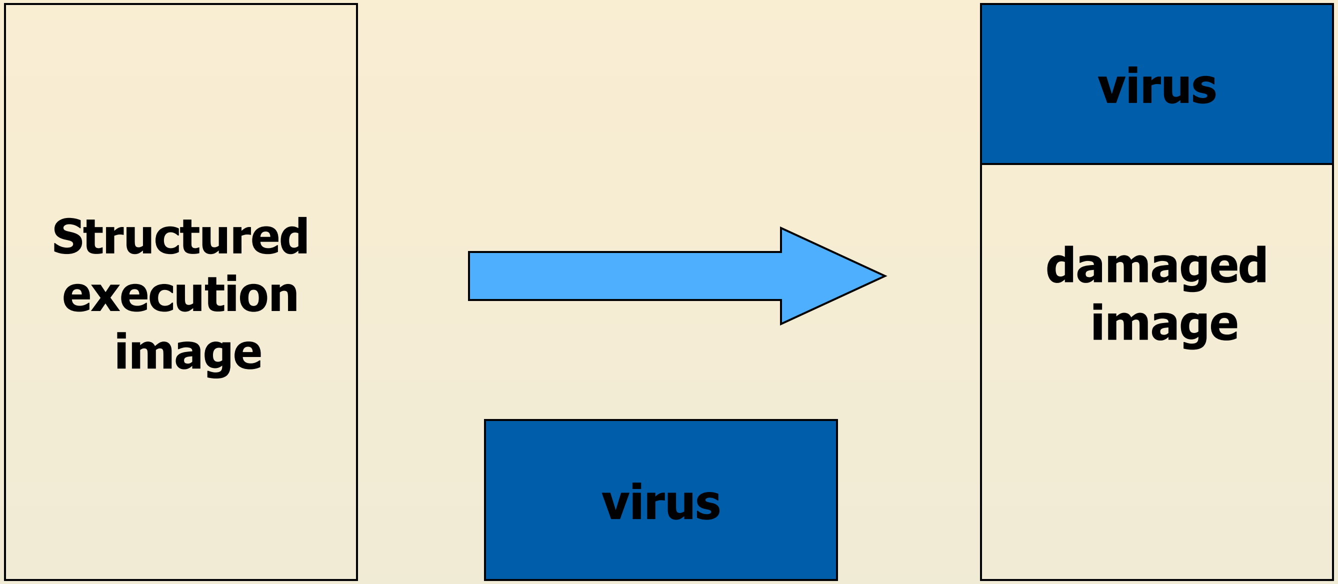
Example: Boot sector virus

- Computer starts with firmware testing all hardware and then initializing a specified OS and transferring control to it.
- Code copies the OS from disk to memory; starts with bootstrap loader, which is a small set of instructions that then copies the rest of the OS. Initial part of bootstrap loader is contained in boot sector
- Because OS length is not pre-determined, and to allow flexibility, the bootstrap loader consists of non-contiguous blocks on disk chained together with pointers.
- Virus can easily insert itself in the chain, on disk.
- Very effective, as difficult to detect

Virus logic

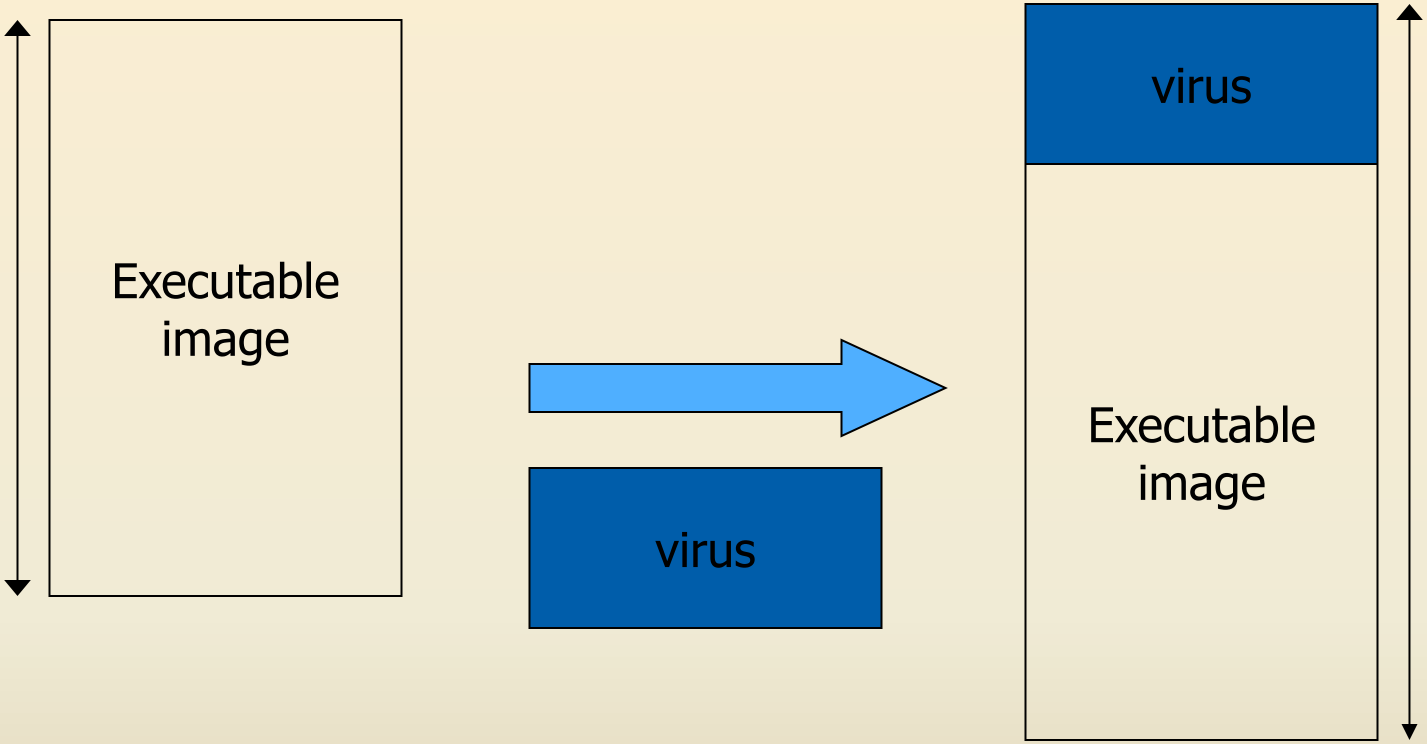
- Virus includes code to
  - Search for files to infect
  - Replicate
    - Make copy of self
    - Attach to file/boot sector
  - Reduce evidences of detection
    - Ideally, should execute quickly then pass control to infected program’s normal code
    - Intercept system calls
    - Fool antiviral tools

Means of attaching: overwriting (virus *replaces* part of program)



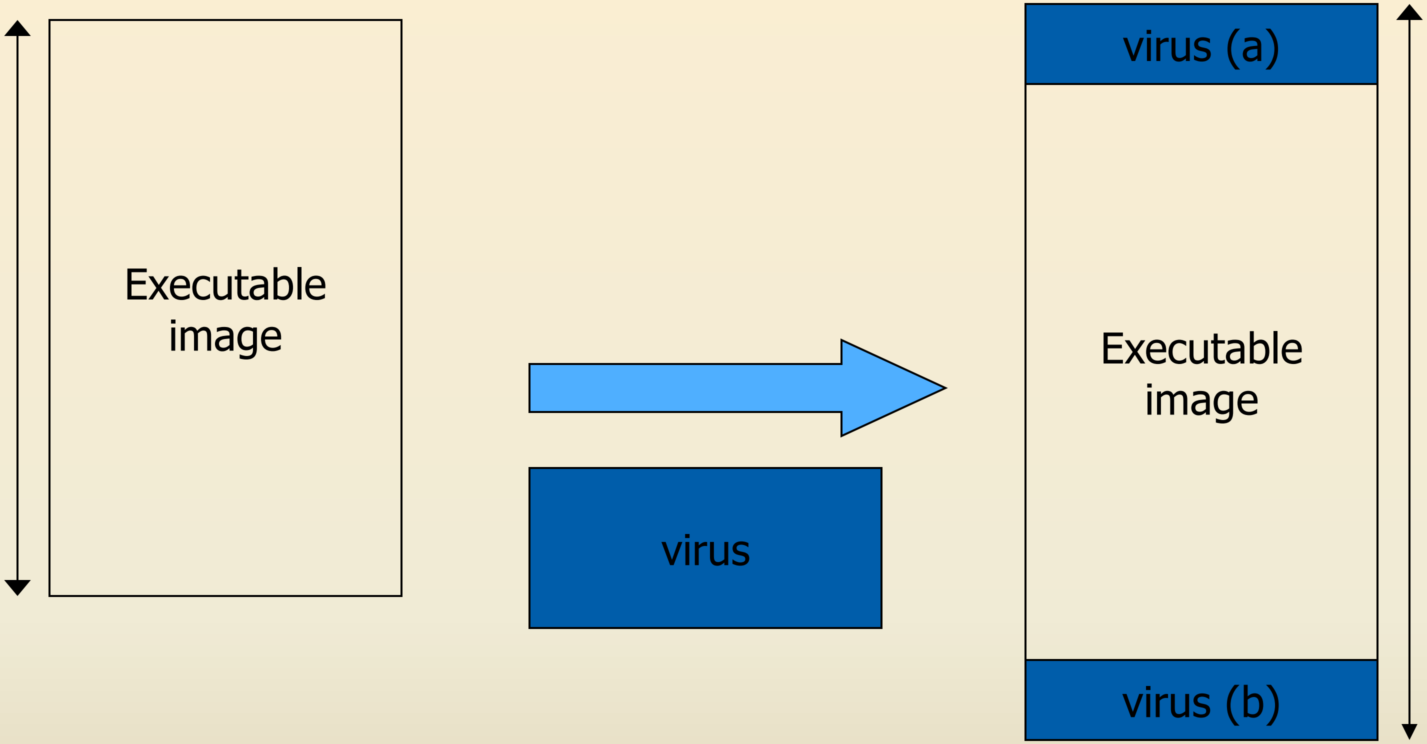
- Virus overwrites an executable file
- Easiest mechanism
- Since original program is damaged easily detected

Means of attaching: at the beginning (virus is *appended* to program)



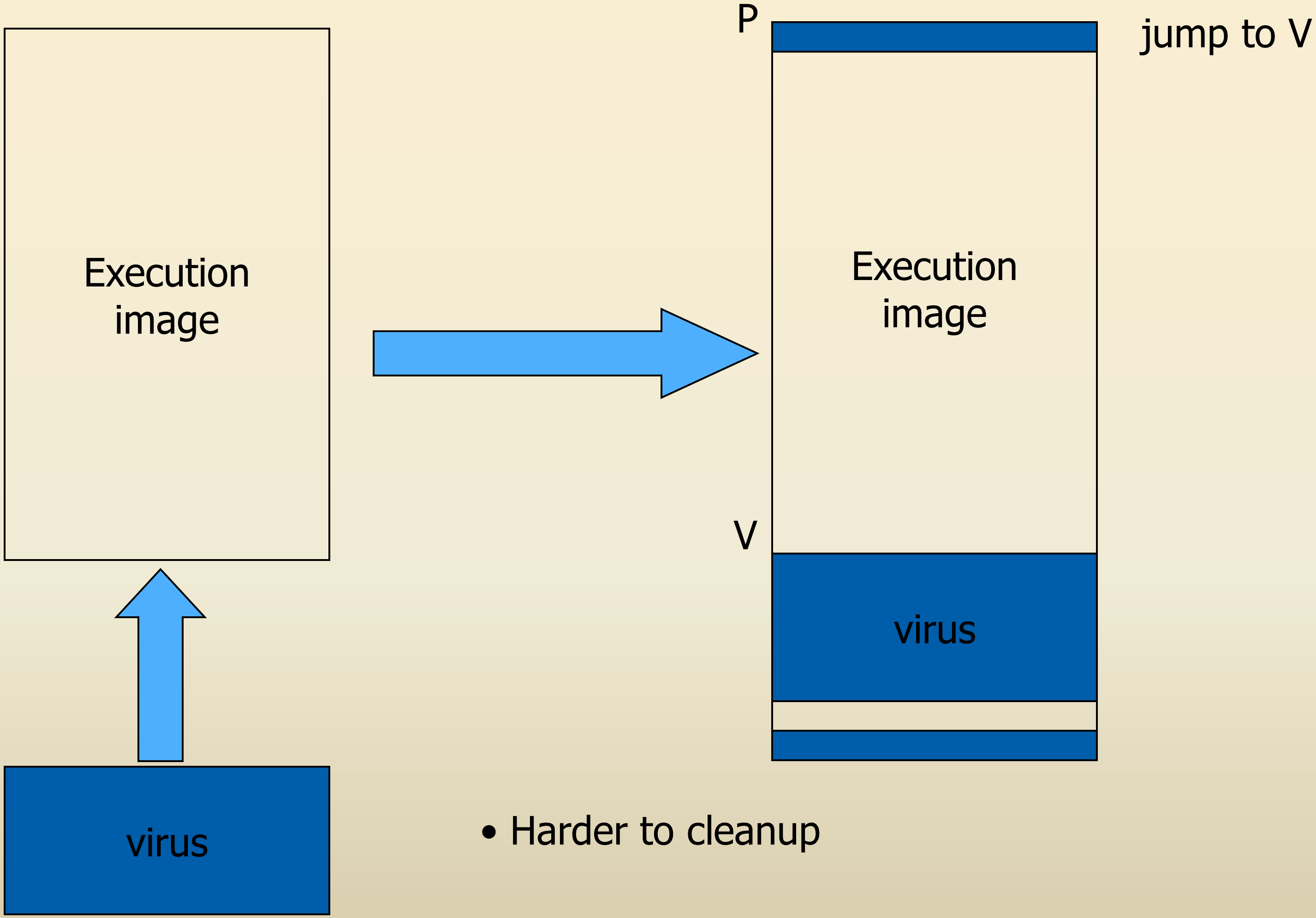
- Improved stealth because original program is intact
  - ✓ If original program is large, copying it may be slow
  - ✓ File size grows if multiple infections occur

Means of attaching: beginning and end (virus *surrounds* program)



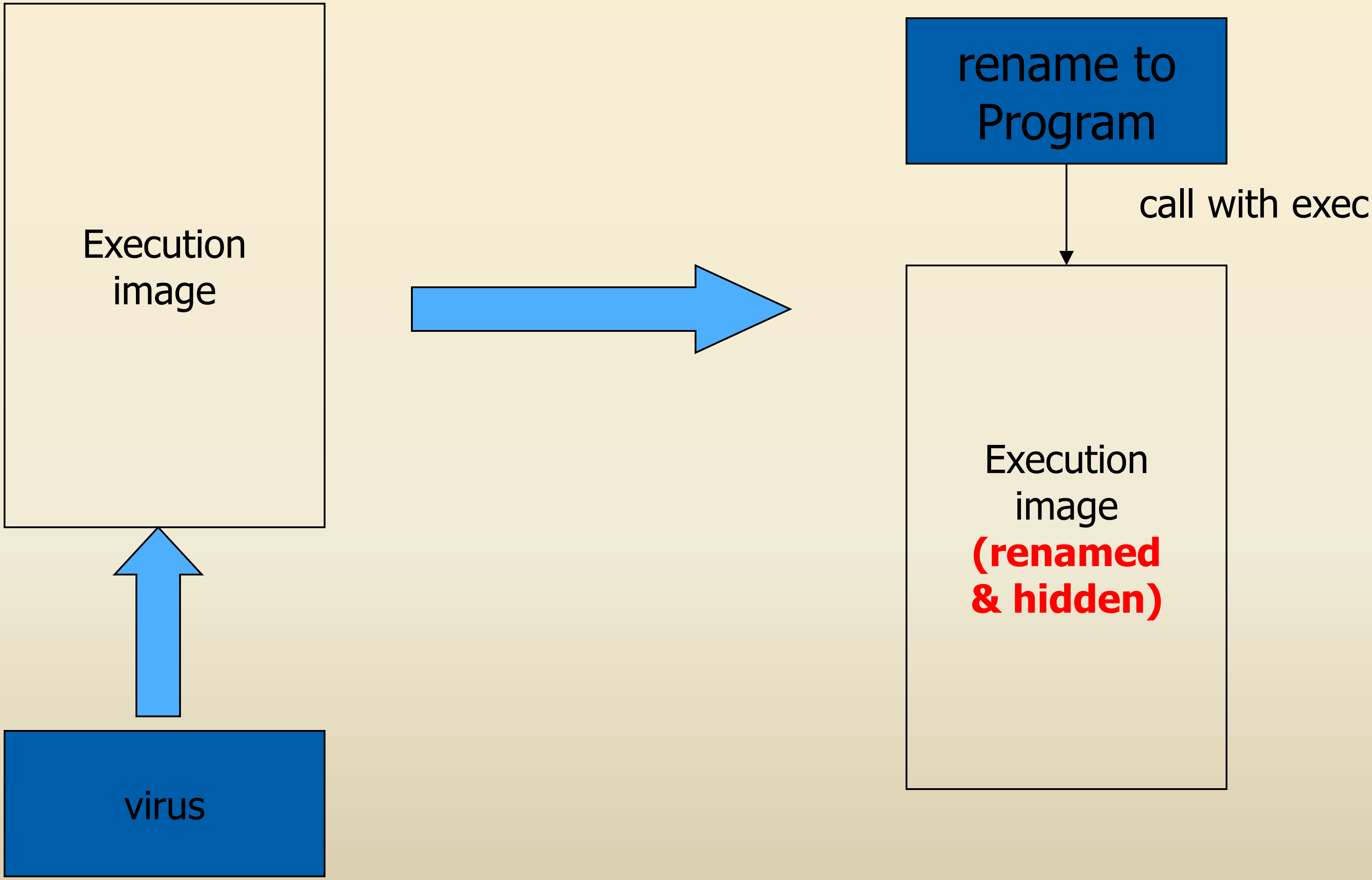
- Properties of appended virus
  - ✓Ability to clean up and avoid detection

Means of attaching: intersperse (virus is *integrated* into program)



- Harder to cleanup

Means of attaching: companions



Invoking a virus

- Virus invoked because:
  - It has replaced part of a program code within the file structure
  - It has appended itself to the code within a file
  - It has overwritten the file in storage
  - It has changed the pointer in the file table, so that it is located instead of a particular file
  - It has changed the table of pointers to typical operating system parts (such as interrupt handler)

Memory residents or TSRs (*Terminate and Stay Resident*)

- Infect memory-resident code (e.g. frequently used parts of the OS), which remains in memory while the computer is running
- Resident code usually activated many times, giving virus many opportunities to spread
- Example: attach to interrupt-handler and check whether any new flash memory have been inserted; if so, infect the flash memory.
- Also many other homes for viruses: libraries, application program startup macros, compilers, virus detection software!

Five major detection methods

- Integrity checking
  - Look for modified files by comparing old and new checksum
  - No software updates required
  - Requires maintenance of virus free checksums
  - Unable to detect stealth viruses
- Interrupt monitoring
  - Attempts to locate and prevent a viruses’ interrupt calls
  - Poor system utilization
  - Obstructive, because of false positives
- Memory detection
  - Depends on recognition of known viruses’ location and code in memory

Five major detection methods

- Signature scanning
  - Recognizes viruses’ unique “signature”: a pre-identified hex
  - Need to maintain current signature files and scanning engine refinements
  - False positives
- Heuristics/Rule based
  - Faster than traditional scanners
  - Uses a set of rules to effectively parse through files and identify code
  - Uses expert systems or neural networks
  - Depends on current rule-set

(Detection can be performed on-access or on-demand)

Properties of a good signature

- Should always appear in the virus, so there won’t be any false negatives
- Should not appear in (m)any other files, so there won’t be (m)any false positives
- Should be reasonably short, for efficient scanning
- For simple viruses, it’s easy to find good signatures but for complicated ones …!

Polymorphic Viruses

- Polymorphic = “many forms”
- Goal: Foil virus scanners by changing virus code each time virus replicates, so that it will be difficult to find a good signature
- Approaches:
  - Encrypt virus with random key
    - Note: Goals and techniques are different than in the encryption techniques we studied earlier. XOR with stored key is sufficient.
  - “Mutate” virus by making small changes that don’t affect the semantics of the code
  - Nearly 2 billion similar codes can be evolved from a single code
  - Requires algorithm based matching instead of simple string based matching

Replication of encrypted virus

- Copy decryption engine to infected file
- Select new key and copy it to the infected file
- For each byte of the encrypted portion of the virus:
  - take decrypted byte
  - encrypt it with the new key
  - copy it to the infected file
- Result: different replicas of virus have different byte patterns, so difficult to find signature

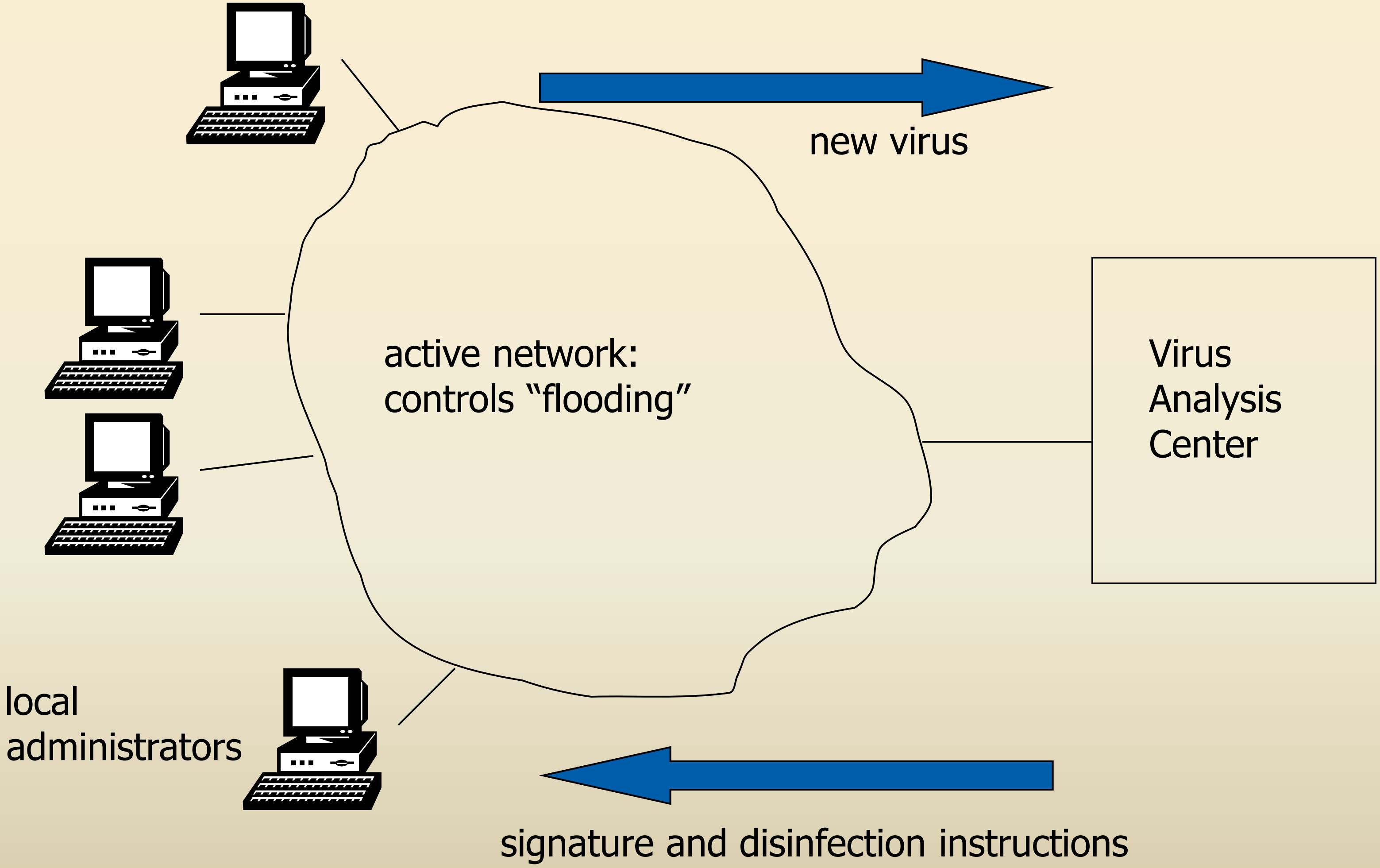
Anti-virus tools’ answer to encryption

- Select the signature from the unencrypted portion of the code, i.e. the decryption engine
- Problems:
  - Anti-virus tools usually want to determine which virus is present, not just determine that some virus is present (in order to “disinfect”).
    - Can emulate the decryption then further analyze the decrypted code.
  - virus writers have responded by obscuring the encryption engine through mutations
- It’s a game of cat and mouse!

Virus Analysis

- Analysis of virus by human expert
  - slow: by the time signature has been extracted, posted to AV tool database, downloaded to users, virus may have spread widely.
    - pre-1995: 6 months to a year for virus to spread world-wide
    - now: days or hours
  - labor-intensive: too many new viruses
    - currently, 8-10 new viruses per day
  - can't handle epidemics:
    - queue of viruses to be analyzed overflows
- Automated analysis, e.g. "Immune System"
    - developed at IBM Research
    - licensed to Symantec

Immune System Architecture



Signature Extraction at VAC

- Virus allowed (encouraged) to replicate in controlled environment in immune center
- This yields collection of infected files
- In addition, a collection of “clean” files is available
- Machine learning techniques used to find strings that appear in most infected files and in few clean files (e.g. award/punishment learning):
  - search files for candidate strings
    - add points if found in infected file
    - subtract points if found in clean file

Macro-viruses

- Written in macro-language
- Infect documents (as opposed to programs), such as word-processor docs, etc.
- "Attach" by modifying commonly used macros, or start-up macros
  - popular target is Normal.dot, which is opened when MS Office applications are executed
- Spread when documents are transmitted, via disks, file transfer, e-mail attachments, ...
- Macro virus dependencies:
  - Application popularity
  - Macro language depth
  - Macro implementation