Malware

CS 465

Malware

software intentionally designed or deployed to have effects contrary to the best interests of one or more users

— *Computer Security and the Internet*

Why study malware?

- helps us think like an attacker
- learn tricks that have worked in the past so we can avoid them in the future

Virus

a program that can infect other programs or files by modifying them to include a possibly evolved copy of itself

— Fred Cohen

(defined the term computer virus, invented defense techniques)

Brain Virus (1986)

- first PC virus
- replaces the boot sector of a floppy with a copy of itself — IBM PCs would load code from the boot sector prior to loading the OS
- slows down the floppy drive, but otherwise mostly stealthy
- written to prevent pirating of software distributed by brothers in Pakistan — it included their address and phone numbers

Chernobyl Virus (1998-2000)

- affected Windows 95/98/ME
- overwrites the partition map of hard drive, crashing OS, possibly causing loss of all files
- tries to rewrite BIOS firmware, causing machine to not boot
- places itself in unused bytes in files, splits across multiple files as needed, avoiding anti-virus programs that looked for changes in file lengths
- author claimed to write it as a challenge to bold claims by anti-virus companies

Melissa Virus (1999)

- mass-mailing virus
  - Subject: Important Message From <username>
  - Body: Here's that document you asked for. Don't show anyone else ;) — with a Word document attached
- virus embedded in Word document as a macro, mails itself to first 50 people in user’s contact list, disables some safeguard features of Word and Outlook
- estimated 1,000,000 emails, infected 100,000 computers
- author sentenced to 20 months in federal prison

Virus infection strategies

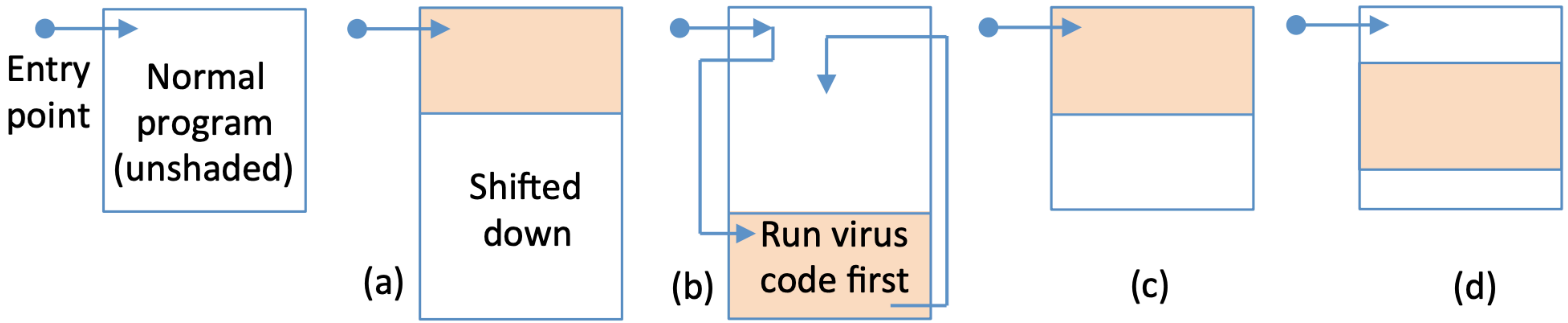


Figure 7.1: Virus strategies for code location. Virus code is shaded. (a) Shift and prepend. (b) Append. (c) Overwrite from top. (d) Overwrite at interior.

Virus detection strateges

- malware signatures — short byte sequences that are unique to the virus
    - anti-virus (AV) checks every program against a database of signatures prior to running the program
    - AV must be a part of the OS
- hashes of known good programs — AV checks programs against hash database
- behavioral signatures — actions known to be suspicious (disabling a program, deleting multiple files)
    - AV can pre-run a program in an emulated environment, allowing the virus to activate, then check behavioral signatures and using malware signatures

Anti detection strategies

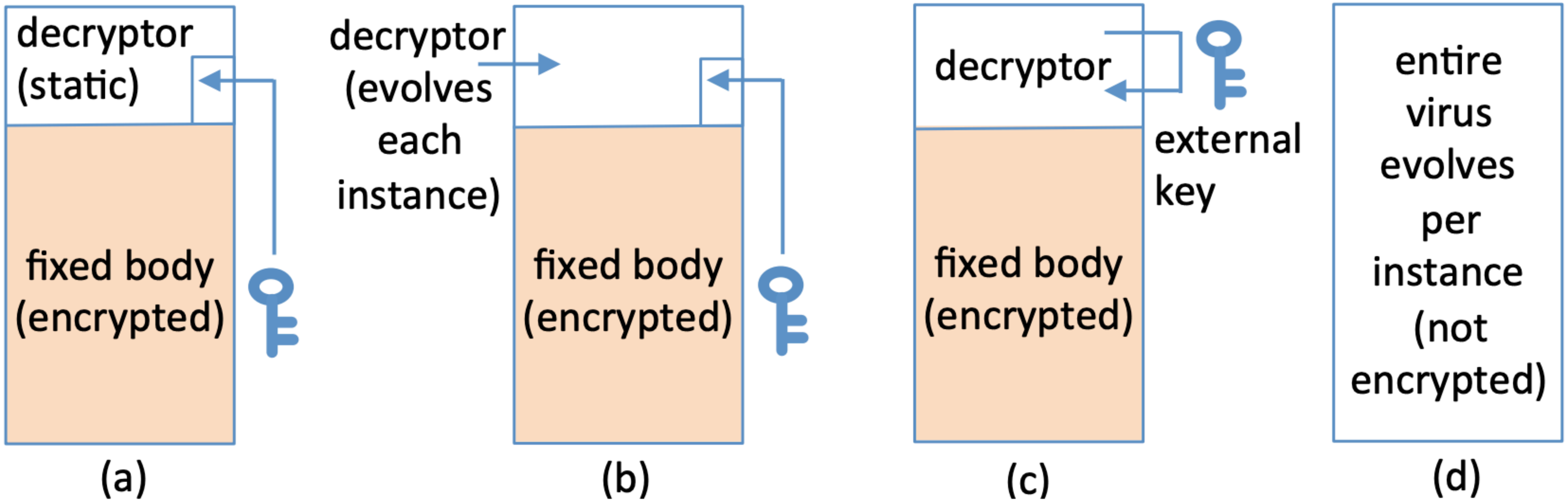


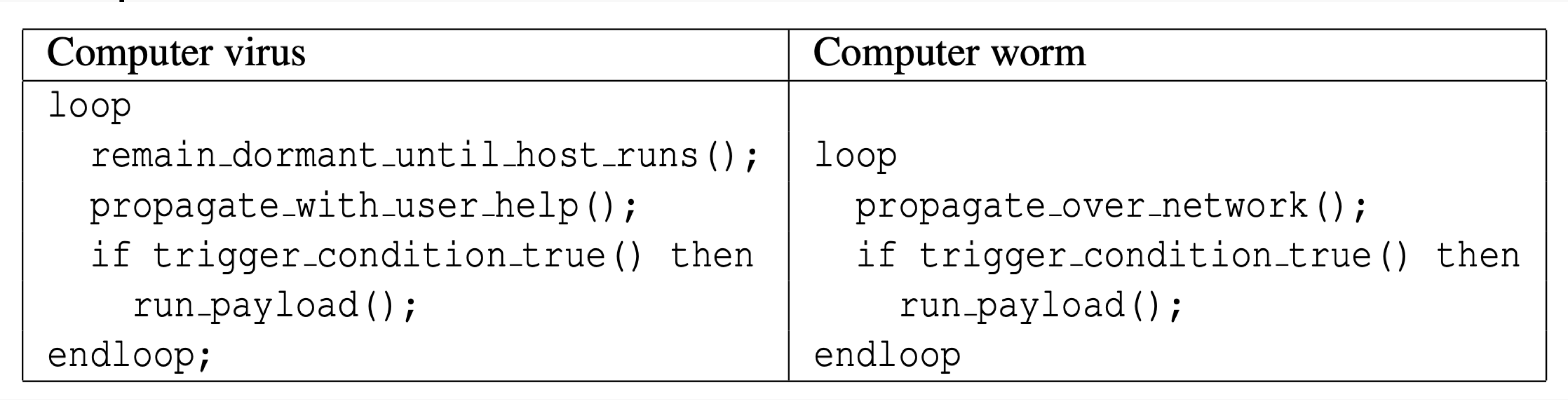
Figure 7.2: Virus anti-detection strategies. (a) Encrypted body. (b) Polymorphic virus, including self-mutation of decryptor. (c) External decryption key. (d) Metamorphic virus.

Worm

- actively spreads itself using the network

- no user interaction required (viruses spread via social engineering, such as clicking on a link in an email, inserting a portable drive, or some other social engineering)

- exploits software vulnerabilities



Computer virus	Computer worm
loop	
remain_dormant_until_host_runs();	loop
propagate_with_user_help();	propagate_over_network();
if trigger_condition_true() then	if trigger_condition_true() then
run_payload();	run_payload();
endloop;	endloop

Worm propagation

- *randomized scanning*, infecting those that are vulnerable
- *context-aware scanning*, prioritizing local machines over remote machines
- *hit-list scanning*, scan in advance to find vulnerable machines, add them to a hit list when ready to spread

  Zmap: With a ten gigabit connection, can complete a scan of entire Internet in under five minutes.

Morris Worm (1988)

- infected 10% of Internet devices
- traffic overloaded the network, causing denial of service
- four vulnerabilities exploited
  - stack overflow in finger daemon
  - backdoor in sendmail daemon
  - password guessing attack on /etc/passwd
  - trusted remote login in /etc/hosts.equiv

Happy 99 Worm (1999)

- first worm to propagate via email and Usenet
- runs a Happy New Year program with fireworks
- modifies a Windows library to spread itself
- attaches automatically to all outgoing emails and Usenet posts
- automatically starts itself when the computer is booted
- written by a French programmer who was inspired by the Brain virus

Stealth techniques

- trojan horse — hide malicious code in a seemingly good program
- backdoor — hide remote access to a program
- rootkit — set of software that is installed in secret, hides itself, controls or manipulates the host, facilitates long-term malicious activity
- keylogger — record user keystrokes and send to attacker
- surveillance — logging user activity (microphone, webcam, GPS sensor)

Stuxnet Worm (2010-)

- attacks SCADA systems that control programmable logic controllers (PLCs) in manufacturing plants
- uses a rootkit to prevent detection
- initial contact is through a USB drive (helpful for systems that are not connected to the Internet), and then it spreads through the networked control system
- originally targeted uranium enrichment facilities in Iran, causing centrifuges to burn themselves out
- later adapted to attack water, power facilities, chemical plants

Rootkits: hijacking system calls

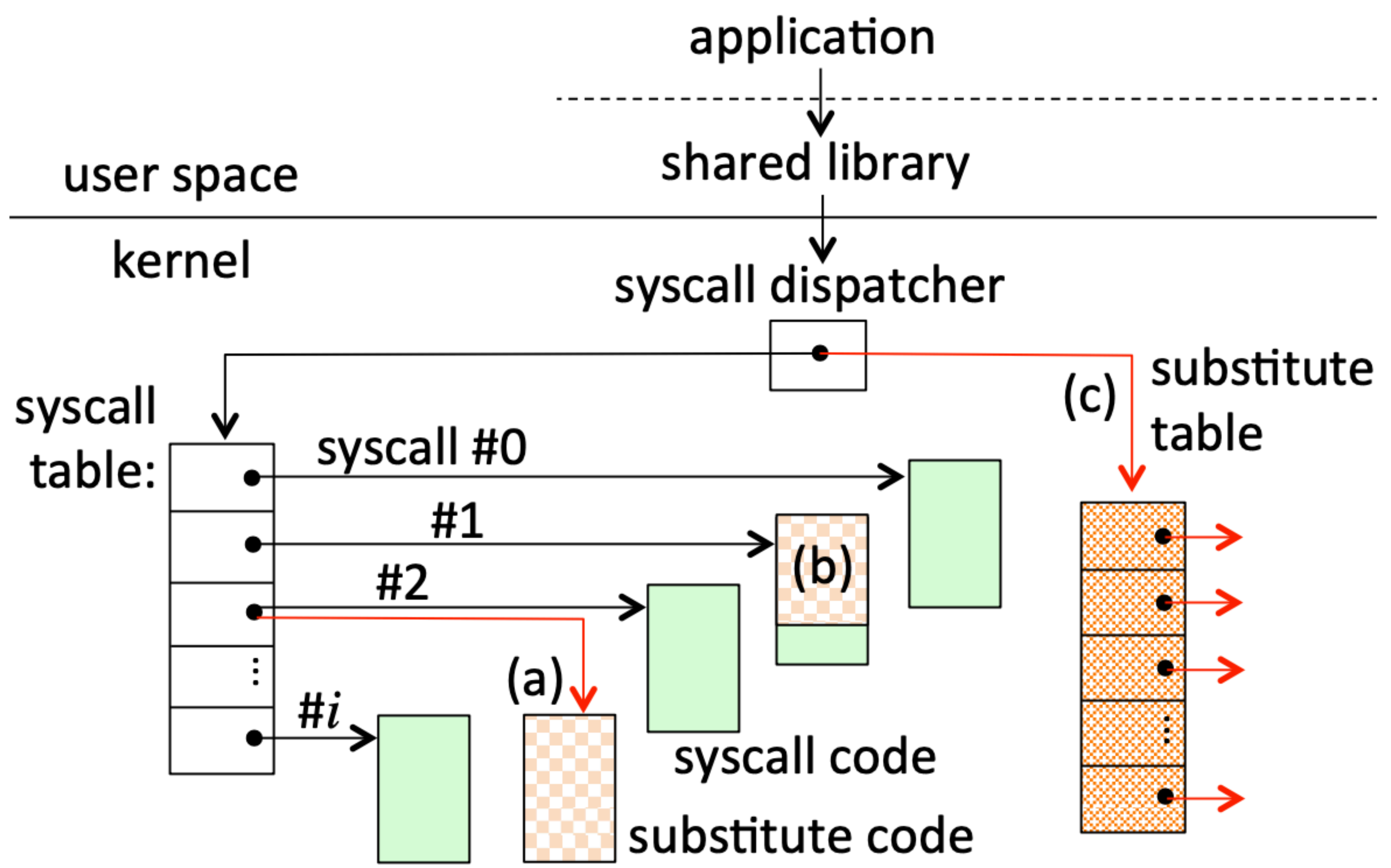


Figure 7.4: System call hijacking. (a) Hooking an individual system call; the substitute code (hook function) may do preprocessing, call the original syscall code (which returns to the substitute), and finish with postprocessing. (b) Overwriting individual system call. (c) Hooking the entire syscall table by using a substitute table.

Rootkits: hijacking system calls

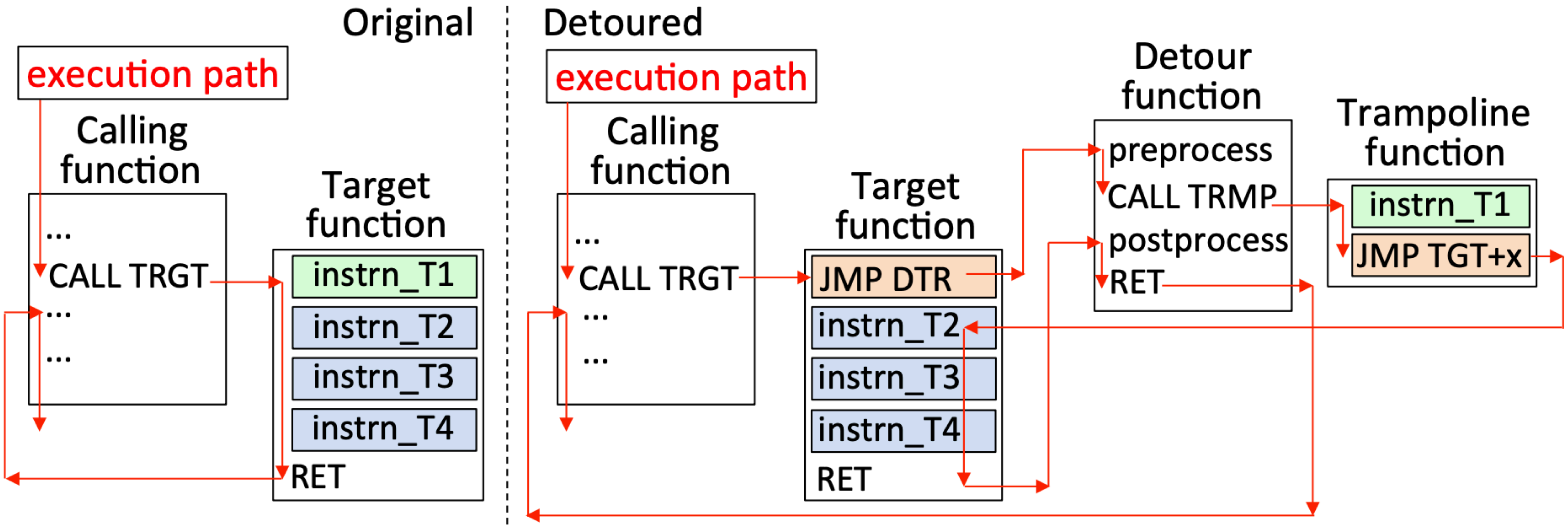


Figure 7.5: Inline hooking, detour and trampoline. A trampoline replaces the overwritten instruction, and enables the target function's return to the detour for postprocessing.

Ransomware

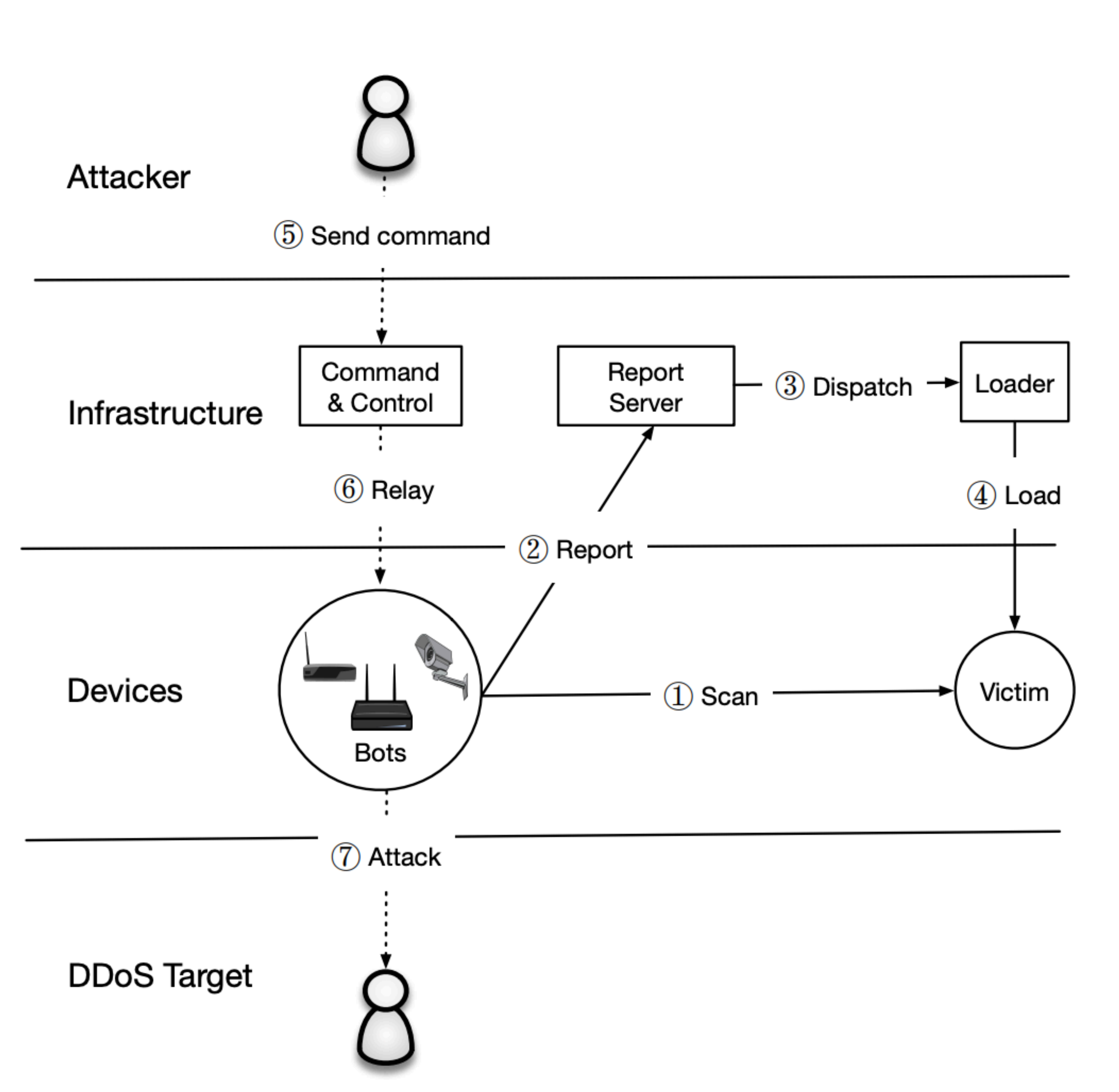
- malware that encrypts files in a computer system, attacker demands a ransom to decrypt them
- attacker keeps the decryption key offsite
- we will return to cryptography details once we cover cryptographic primitives

Botnets

- a large collection (e.g. 100,000) of hacked computers controlled by an attacker
- attacker uses a command-and-control infrastructure to send commands to the botnet machines
- often used to send spam, phishing attacks, have also been used for denial-of-service attacks (which we will cover later)

Mirai Botnet (2016)

- infected 65,000 IoT devices (DVRs, IP cameras, routers, printers) in first 20 hours, steady state of 200K-300K devices



Understanding the Mirai Botnet, USENIX Security 2017

Social Engineering

- psychological manipulation of people to trick them into performing actions or divulging information
  - clicking on an email or downloading a malicious program
  - impersonating someone on a phone call or an in-person visit
  - can include obtaining physical access to systems
- see The Art of Deception, Kevin Mitnick, Social Engineering, Christopher Hadnagy