Packet Sniffing and Spoofing

Lecture 01

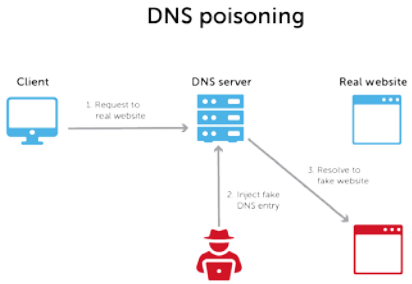
Instructor: Dr. Cong Pu, Ph.D.

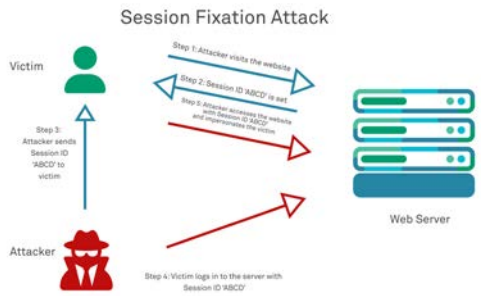
cong.pu@okstate.edu

Acknowledgment: Adapted partially from course materials from Dr. Wenliang Du at Syracuse University, Dr. Fengwei Zhang at Southern University of Science and Technology, and Dr. Steven M. Bellovin at Columbia University.

Introduction

- Two *common attacks* on *networks*:
  - ***sniffing attack***
    - eavesdropping on and capturing packets over networks
  - ***spoofing attack***
    - sending out invalid packets with false identification
- *sniffing* and *spoofing* are the *basis* for other network attacks
  - e.g., DNS cache poisoning and TCP session hijacking attacks





- *tools for conducting sniffing* and *spoofing*
  - *Wireshark* *Netwox* *Scapy*

How Packets Are Received?

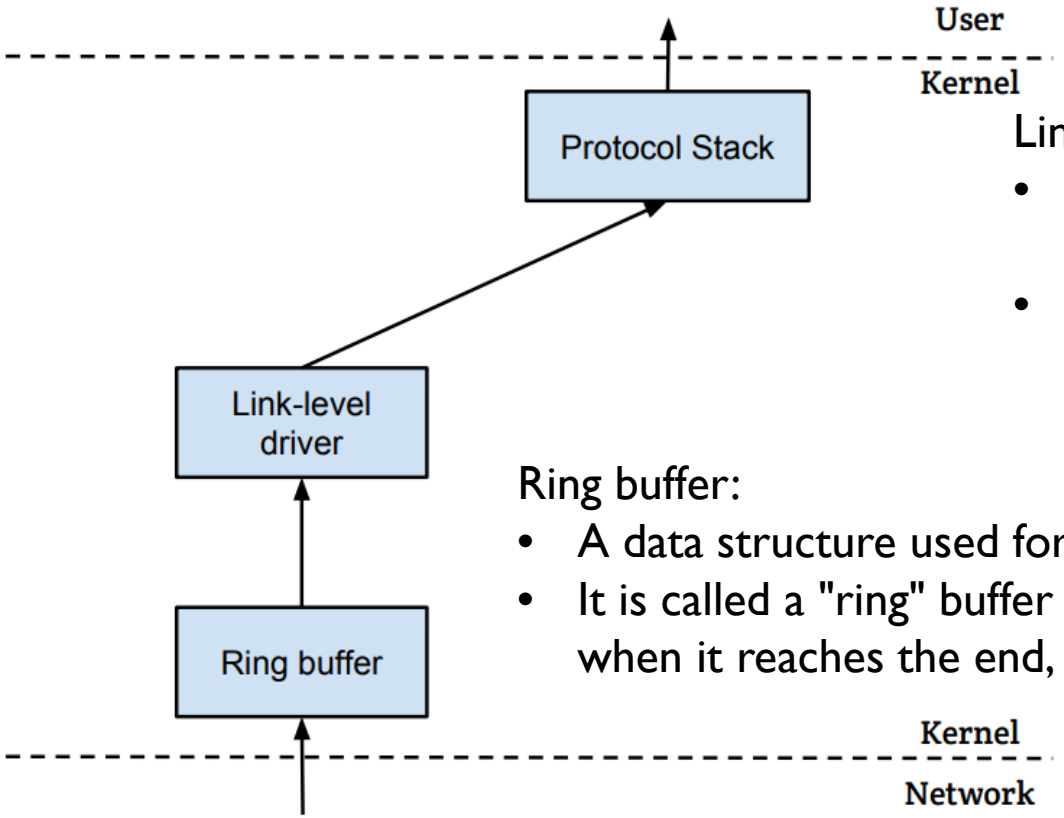


- Network Interface Card (NIC)
  - a *link* (physical or logical) between machine and network
  - NIC has a *hardware address*: ***MAC address***
- Common local comm. techniques: Ethernet and WiFi
  - *broadcast medium* by nature (or *single shared medium*)
  - as data (frame) flow in the medium, **every NIC** "***hears***" data
    - when frame arrives, it is copied into the memory in the NIC
      - checks des. MAC address in the header
        - if ***matching*** with NIC's MAC addr., the frame is copied into kernel buffer
          - interrupts the CPU for new packet
          - CPU copies packet into a queue (making room for other incoming packets)
        - if ***not matching***, the frame is *discarded*

function calls

How Packets Are Received? (cont.)

- Common local comm. techniques: Ethernet and WiFi
  - as data (frame) flow in the medium, **every NIC** "***hears***" data



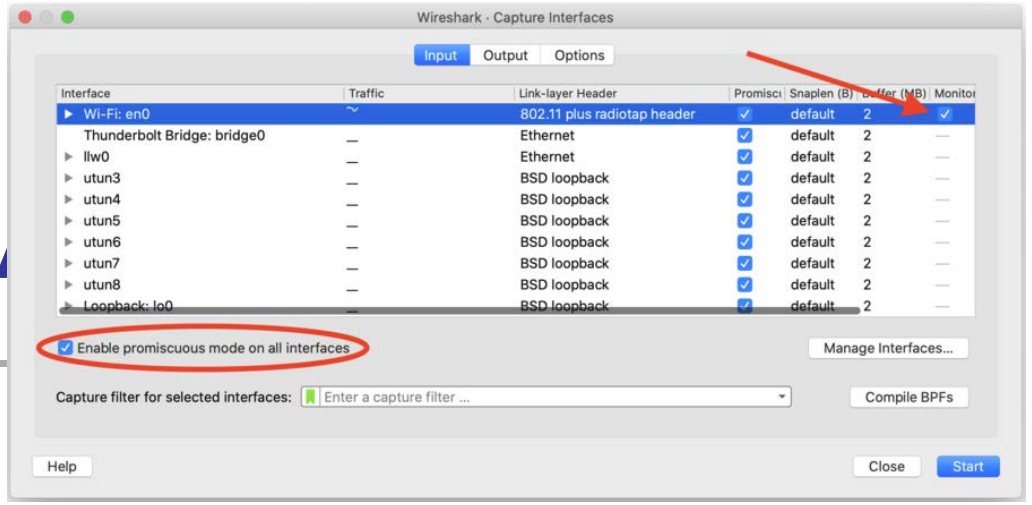
Linux kernel

- The core component of the Linux operating system.
- Acts as a bridge between the hardware of a computer and the software applications running on it.

Ring buffer:

- A data structure used for efficient data storage and retrieval.
- It is called a "ring" buffer because it is circular, meaning that when it reaches the end, it wraps around to the beginning

How Packets A



- *promiscuous mode*
  - most NIC have this special mode: pass every frame from network to the kernel, regardless of destination MAC add.
  - if registered, the kernel forwards all frames to sniffer program
    - usually require *elevated privilege*, e.g., root, to use promiscuous mode
- *monitor mode* (wireless network card)
  - unlike Ethernet, wireless devices suffer interference from other nearby wireless devices
  - to solve this, wireless devices transmit data on *different channels*
  - when NIC is placed in *monitor mode*, it captures 802.11 frames transmitting on the channel that it is listening to

BSD (Berkeley Software Distribution) Packet Filter (BPF)

- When sniffing, we're interested in certain types of packet
  - e.g., TCP packets or DNS query packets
- OS can deliver all captured packets to sniffer program, who can discard unwanted packets
  - ***inefficient*** and ***taking time***
    - processing and delivering unwanted packets (if large volume)
- Filtering unwanted packets ASAP
  - *BSD Packet Filter* (BPF): filtering at the ***lower level***
  - allow user-space program attaches a filter to a socket
    - discarding unwanted packets
  - filter: written in human readable format, and interpreted by BSD Pseudo-Machine (packet filtering)
  - *ref.*: https://www.tcpdump.org/papers/bpf-usenix93.pdf

BPF Filter Examples

- Capture traffic *to* and *from* IP host 192.168.1.1

  ip host 192.168.1.1

- Capture traffic *from* IP host 192.168.1.1

  ip *src* host 192.168.1.1

- Capture Ethernet packets *to* and *from* a host with a *MAC address* of 00:40:D0:13:35:36

  ether host 00:40:D0:13:35:36

- Capture Ethernet packets *to* host 00:40:D0:13:35:36

  ether *dst* 00:40:D0:13:35:36

ref.: https://www.ibm.com/docs/en/qsip/7.4?topic=queries-berkeley-packet-filters