Advanced Network Security

Amir Mahdi Sadeghzadeh, Ph.D.

Most slides have been adapted from S. M. Bellovin, COMS W4180, Columbia University, 2006, and M. Kharrazi, CE-817, Sharif University, 2015.

Security: overview

Chapter goals:

- Understand principles of network security:
  - cryptography and its *many* uses beyond "confidentiality"
  - authentication
  - message integrity
- Security in practice:
  - firewalls and intrusion detection systems
  - security in application, transport, network, link layers

Outline

- What is network security?
- Principles of cryptography
- Message integrity, authentication
- Securing e-mail
- Securing TCP connections: TLS
- Network layer security: IPsec

What is Security?

- Confidentiality
- Integrity
- Availability

Confidentiality (محرمانگی)

- “The property that information is not made available or disclosed to unauthorized individuals, entities, or process [i.e. to any unauthorized system entity].” {definitions from RFC 2828]
- Not the same as privacy

Confidentiality (محرمانگی)

- “The property that information is not made available or disclosed to unauthorized individuals, entities, or process [i.e. to any unauthorized system entity].” {definitions from RFC 2828]
- Not the same as privacy
- Privacy: “the right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others.”
- Privacy is a reason for confidentiality

Integrity (صحت)

- Data integrity: “The property that data has not been **changed**, destroyed, or lost in an unauthorized or accidental manner”
- System integrity: “The quality that a system has when it can perform its **intended function** in a unimpaired manner, free from deliberate or inadvertent unauthorized manipulation.”
- Often of more commercial interest than confidentiality

Availability (دسترس‌پذیری)

- “The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e. a system is available if it provides services according to the system design whenever users request them.”

- Turning off a computer provides confidentiality and integrity, but hurts availability. . .

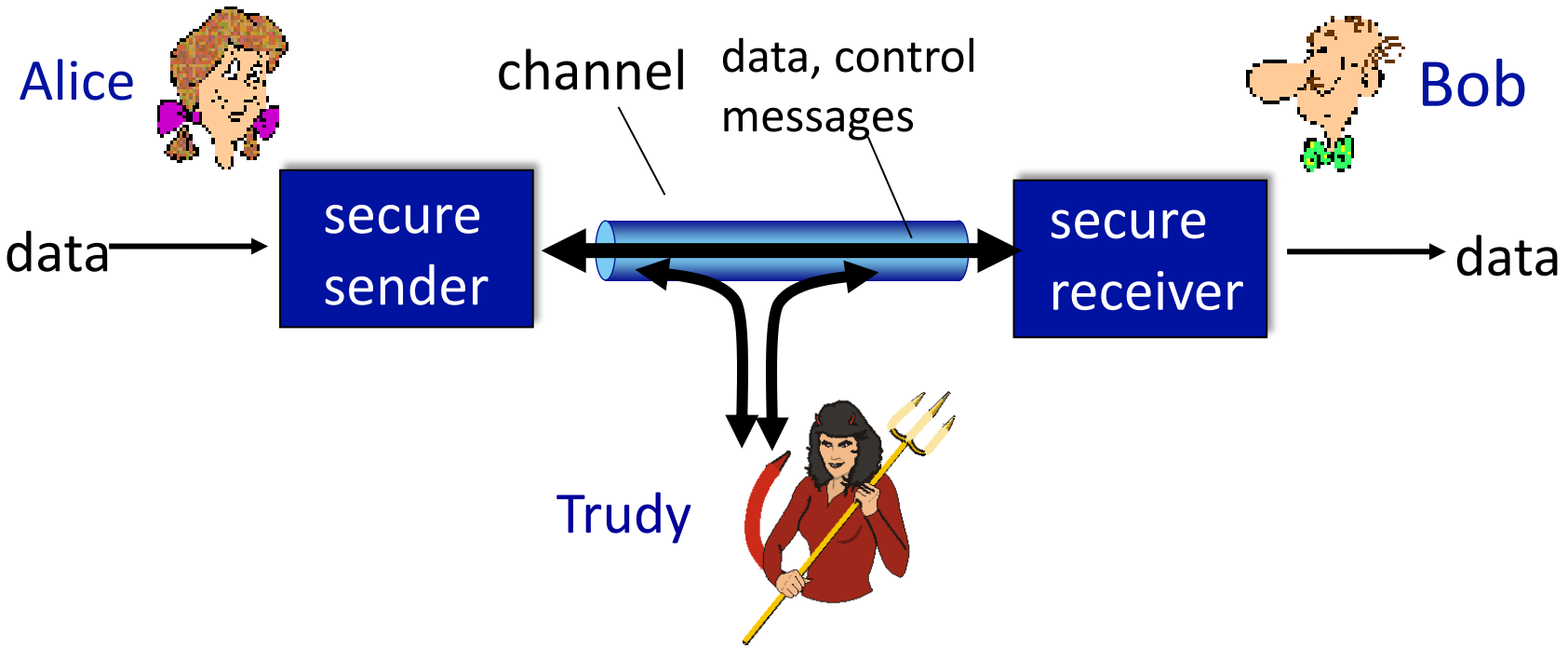
- Denial of service attacks are direct assaults on availability

More Definitions

- Vulnerability (آسیب‌پذیری): An error or weakness in the design, implementation, or operation of a system
- Attack (حمله): A means of exploiting some vulnerability in a system
- Threat (تهدید): An adversary that is motivated and capable of exploiting a vulnerability

Friends and enemies: Alice, Bob, Trudy

- well-known in network security world
- Bob, Alice (Azam, Babak) want to communicate “securely”
- Trudy (intruder) may intercept, delete, add messages



Friends and enemies: Alice, Bob, Trudy

Who might Bob and Alice be?

- … well, *real-life* Bobs and Alices!
- Web browser/server for electronic transactions (e.g., on-line purchases)
- on-line banking client/server
- DNS servers
- BGP routers exchanging routing table updates
- other examples?

There are bad guys (and girls) out there!

Q: What can a "bad guy" do?

A: A lot! (recall section 1.6)

- eavesdrop: intercept messages
- actively insert messages into connection
- impersonation: can fake (spoof) source address in packet (or any field in packet)
- hijacking: "take over" ongoing connection by removing sender or receiver, inserting himself in place
- denial of service: prevent service from being used by others (e.g., by overloading resources)

Vulnerabilities

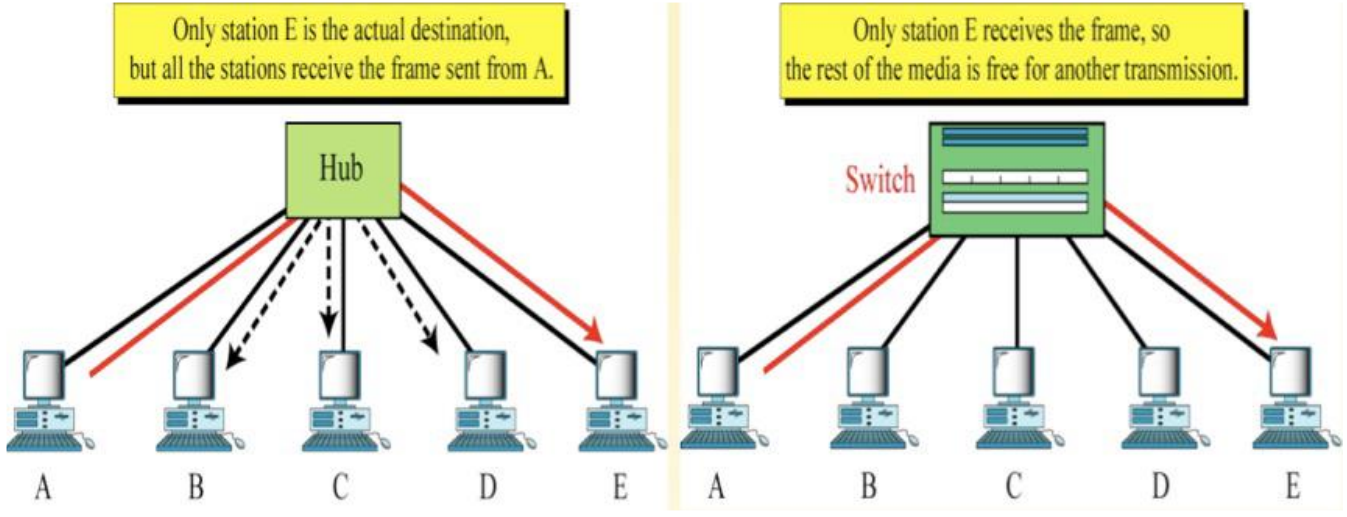
- The technical failing in the system
- The primary focus of most computer security classes
- If you can close the vulnerabilities, the threats don’t matter
- Or do They?

Network Vulnerabilities

- Each layer has it's own vulnerabilities
  - Link layer example: ARP-spoofing
  - Network layer example: IP address forgery
  - TCP example: Sequence number guessing attack
  - Application example: email-borne worms

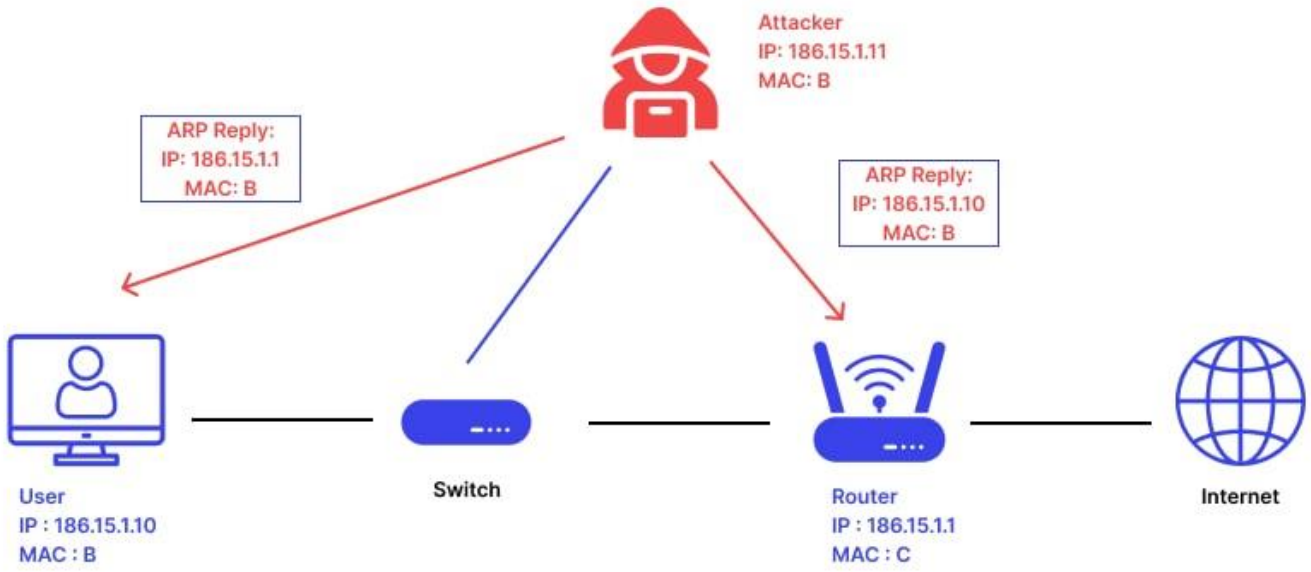
Security of Ethernet Architecture

- Hub: A hub is a basic networking device that operates at the physical layer.
  - It simply broadcasts data packets it receives from one port to all other ports, regardless of the destination.
- Currently mostly switched.
  - Advantages of switched: Latency, Bandwidth, **Security**.



ARP Spoofing

- ARP (Address Resolution Protocol) is used to map an IP address to a MAC address.
  - Any device on the network can answer an ARP request.
  - First reply generally wins
- Attackers send fake ARP messages to redirect network traffic through their device.



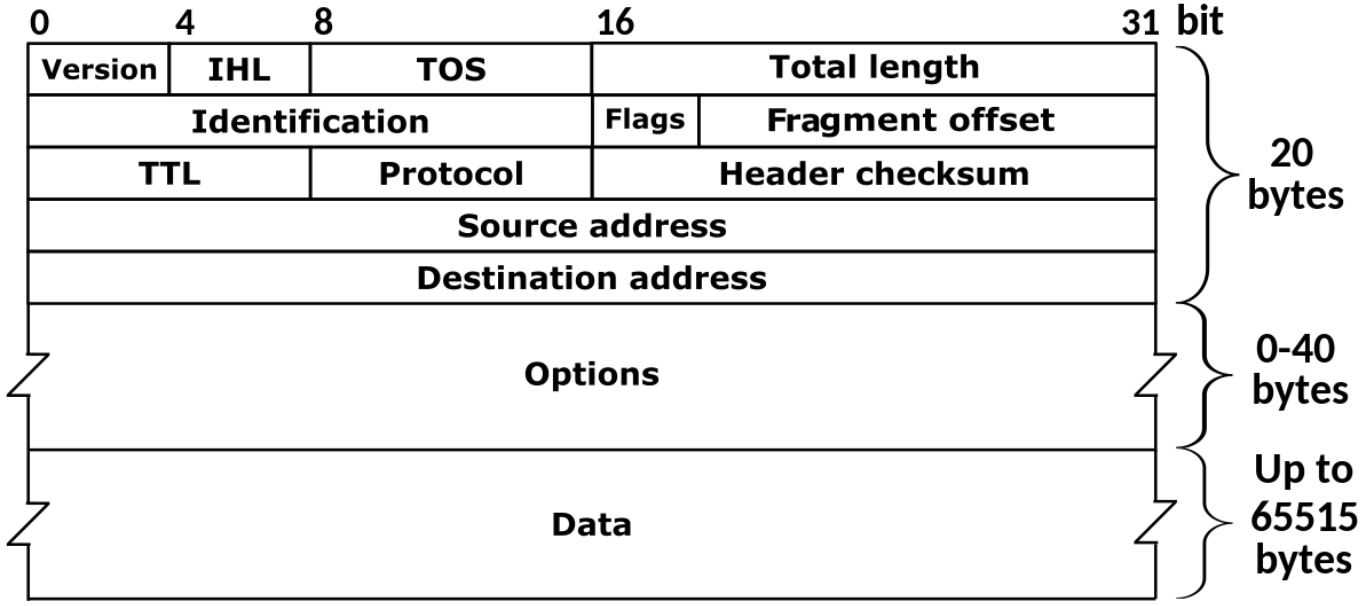
(https://www.wallarm.com/what/arp-spoofing-or-arp-poisoning)

ARP Spoofing Example

1. **Normal ARP Resolution**
    1. Alice wants to communicate with Bob.
    2. Alice's computer needs Bob's MAC address to send data.
    3. ARP Request: "Who has IP X.X.X.X?"
    4. Bob's computer responds with its MAC address.
    5. Alice can now send data to Bob.
2. **ARP Spoofing Attack**
    1. Attacker (Trudy) wants to intercept Alice's data.
    2. Trudy sends a fake ARP Reply:
        1. "I have IP X.X.X.X, and my MAC address is Trudy 's MAC."
    3. Alice updates her ARP cache with Trudy 's MAC.
    4. Alice sends data to what she thinks is Bob but is actually Trudy.
3. **Trudy 's Actions**
    1. Trudy can intercept, modify, or drop the data.
    2. She can forward the data to Bob to avoid suspicion.
    3. Trudy can eavesdrop on sensitive information.

IP Fragmentation

- When an IP packet is too large to be transmitted in one piece (due to network-specific MTU limitations), it may need to be fragmented into smaller packets.
- These smaller packets, known as fragments, are sent individually over the network and later reassembled at their destination.



IP Fragmentation

- Alice wants to send a large image file (e.g., 6,000 bytes) to Bob.
- The network they are using has an MTU of 1,500 bytes, which is smaller than the file size.

- Fragment 1 (Offset 0):
  - Data: Bytes 1-1,500
  - Identification: 12345
  - MF Flag: Set
- Fragment 2 (Offset 1,500):
  - Data: Bytes 1,501-3,000
  - Identification: 12345
  - MF Flag: Set
- Fragment 3 (Offset 3,000):
  - Data: Bytes 3,001-4,500
  - Identification: 12345
  - MF Flag: Set
- Fragment 4 (Offset 4,500):
  - Data: Bytes 4,501-6,000
  - Identification: 12345
  - MF Flag: Not Set (last fragment)

Security Risks of fragmentation

- Hides information
  - Fragmented packets hard to analyze unless reconstructed
  - Adversary divides “sudo rm /” into smaller chunks, ensuring that each chunk fits within the network's Maximum Transmission Unit (MTU).
- Denial of Service
  - Reconstructing fragmented packets can take a lot of memory and cpu, specially if OS implements poorly
  - Ping of Death

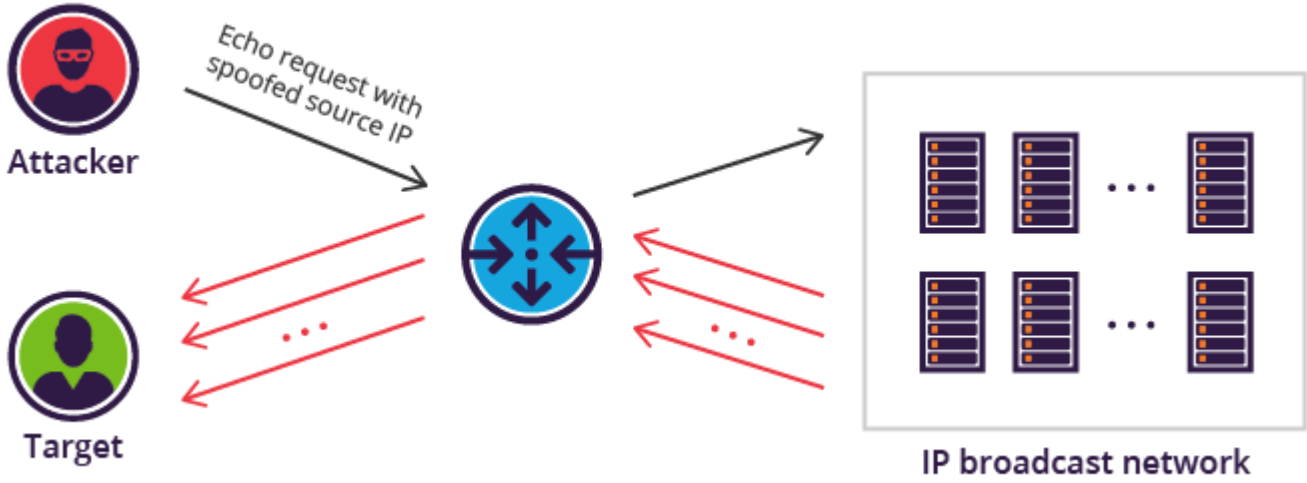
Ping of death

- A ping is normally 64 bytes in size (84 with IP header)
  - Many computer systems cannot handle a ping larger than the maximum IP packet size, which is 65,535 bytes.
- MTU is usually 1500 bytes, so how do you send a 65,536 byte ping?
  - Use IP fragments
  - Buffer overflow occurs when the target computer reassembles the packet
    - often causes a system crash.

Smurf Attacks (ICMP Ping)

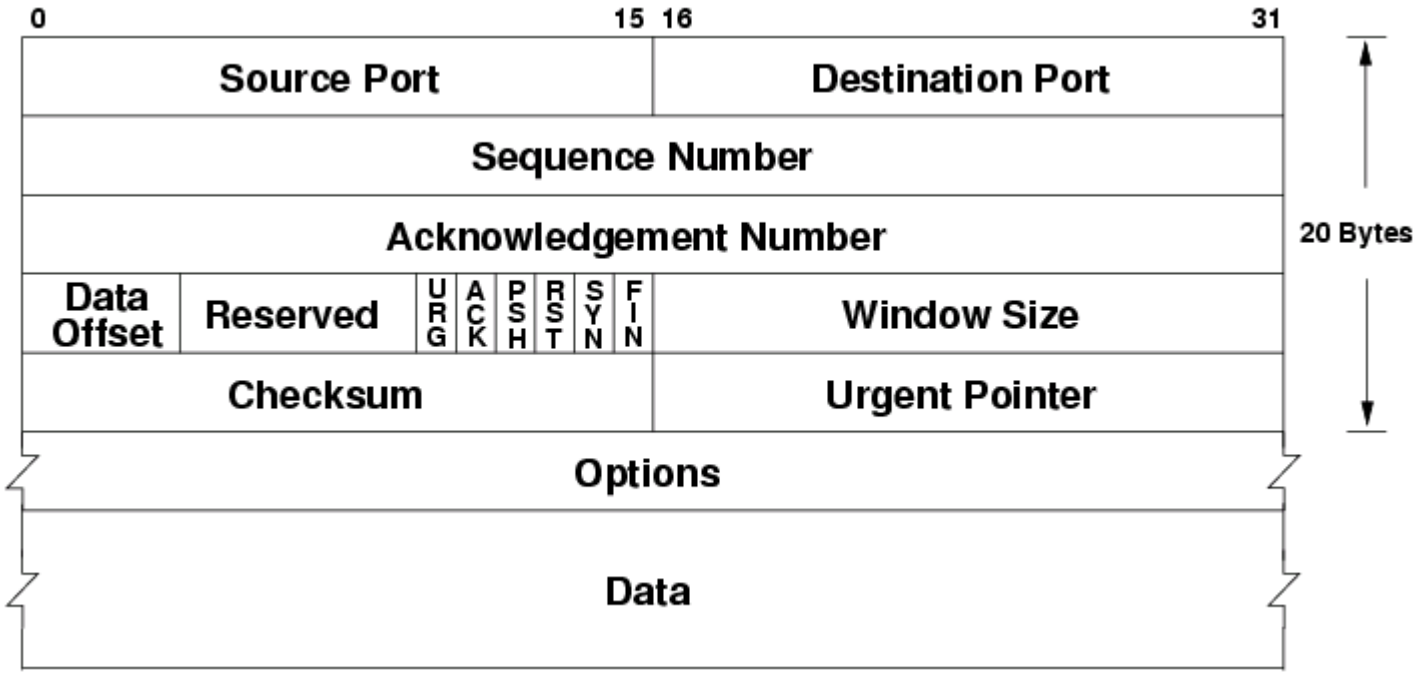
- Attackers send a large number of ICMP Echo Requests (ping) to a network's broadcast address.
- Spoofing the victim's IP address, making all responses target the victim.
- Magnification occurs because for each attack packet, N damage packets are sent to target.

- Gradually being fixed by changing the RFC's to prohibit routing "broadcast" pings. They can now only be used locally.

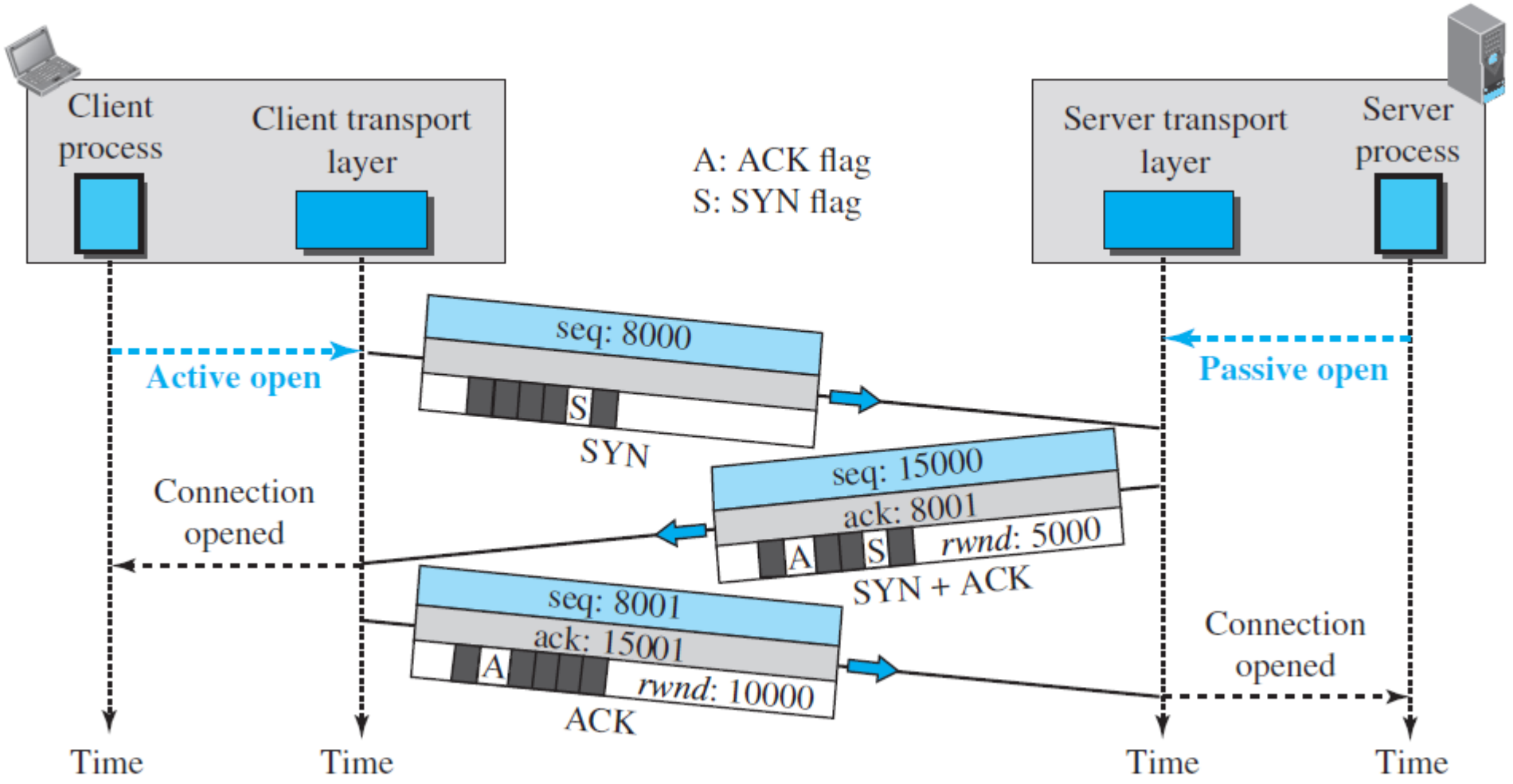


https://www.imperva.com/learn/ddos/smurf-attack-ddos/

TCP Header


0
15
16
31
Source Port
Destination Port
Sequence Number
Acknowledgement Number
Data Offset
Reserved
URG
ACK
PSH
RST
SYN
FIN
Window Size
Checksum
Urgent Pointer
20 Bytes
Options
Data

TCP Seq & Ack number



(Data Communications and Networking, Forouzan)

Sequence Number Guessing Attack

- In older TCPs, the ISN (Initial Sequence Number) is incremented by a constant amount k after each connection and every half-second.
- X opens a legitimate connection to S to learn ISNS
  - X → S : SYN (ISNX)
  - S → X : SYN (ISNS), ACK (ISNX)
- X impersonates T :
  - X → S : SYN (ISNX), SRC = T
  - S → T : SYN (ISNS + k), ACK (ISNX)
  - X → S : ACK (ISNS + k), SRC = T
  - X → S : ACK (ISNS + k), SRC = T , nasty-data

Sequence Number Guessing Attack

- When T sees the SYN/ACK packet from S , it will try to respond with a RST
  - X has to prevent this
    - Could impersonate a dead host or use a denial of service attack to block T

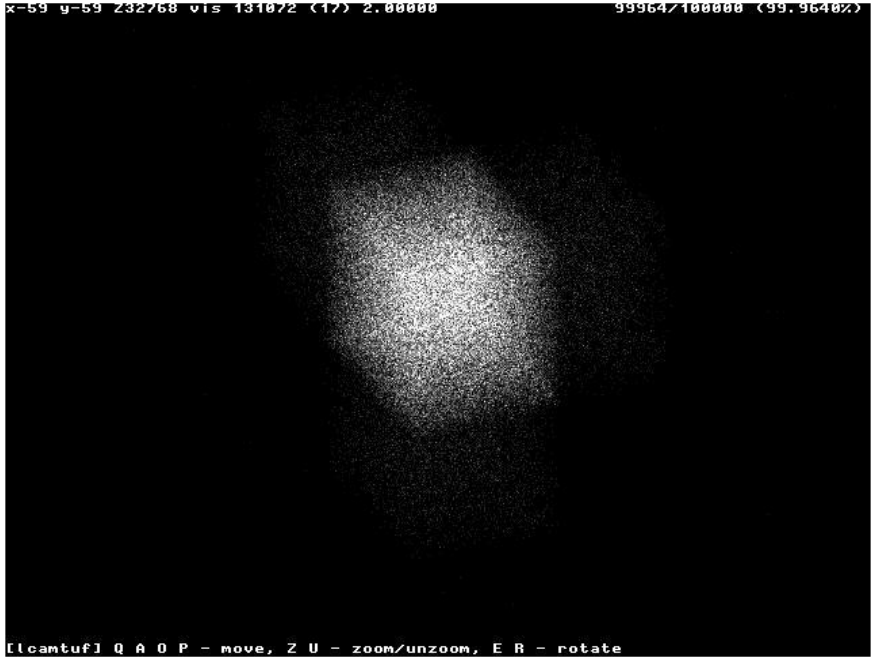
- New research result: built-in firewall software prevents hosts from seeing packets for connections they didn't initiate; T will never see that packet, and hence will never send the RST. . .

ISN Patterns

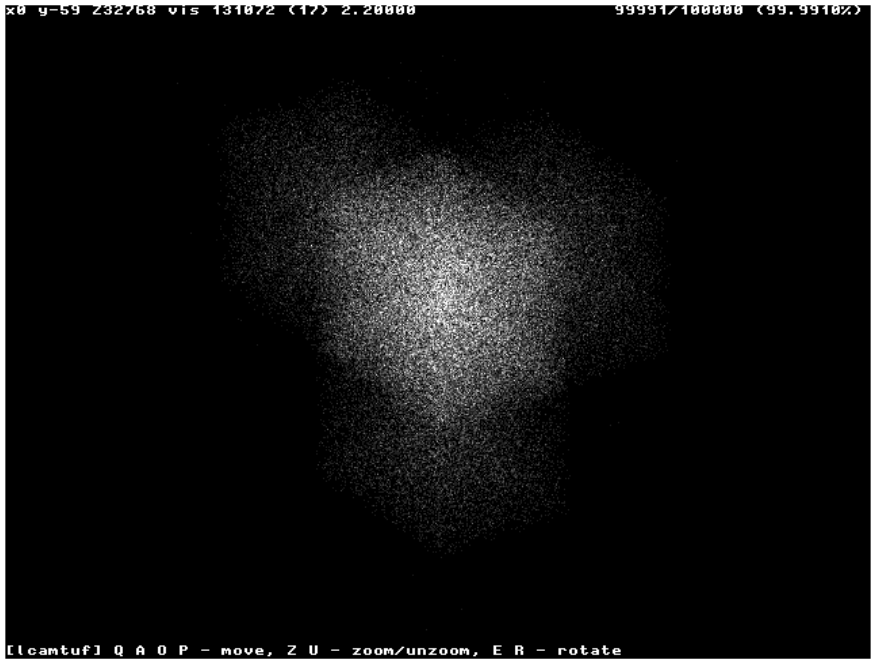
- Are there any patterns to these ISNs?
  - A study by Michal Zalewski gathered and graphed the ISN sequences for a variety of OS's.
  - 100,000 ISN's were graphed for each OS

ISN Patterns for Windows 95

ISN Patterns for Windows 2000



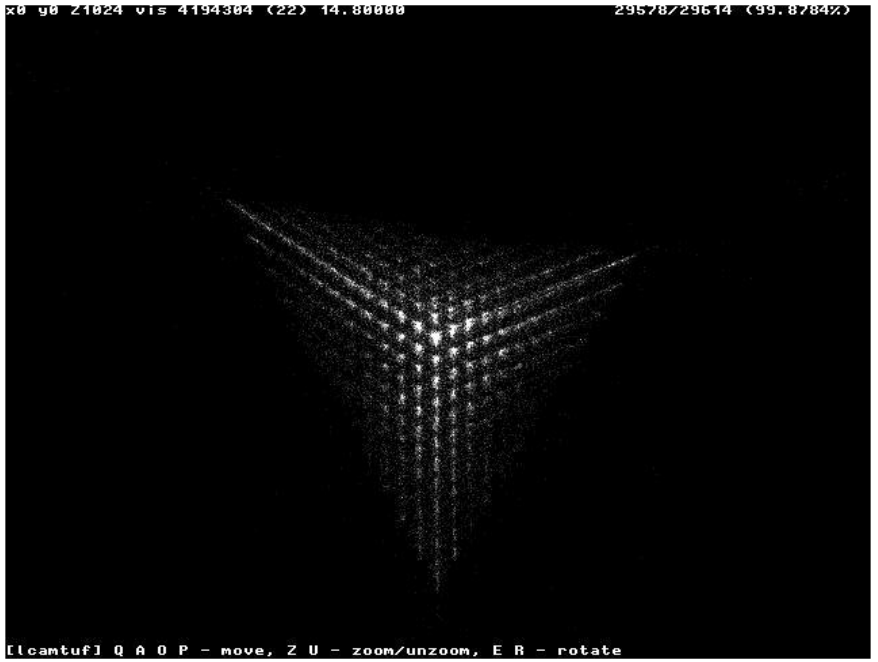
ISN Patterns for Windows XP



ISN Patterns for Mac OS 9

ISN Patterns for Mac OS X

ISN Patterns for Cisco IOS 12.0 (unpatched)



ISN Patterns for Cisco IOS 12.0 (patched)

ISN Patterns for IOS 12.2.10a

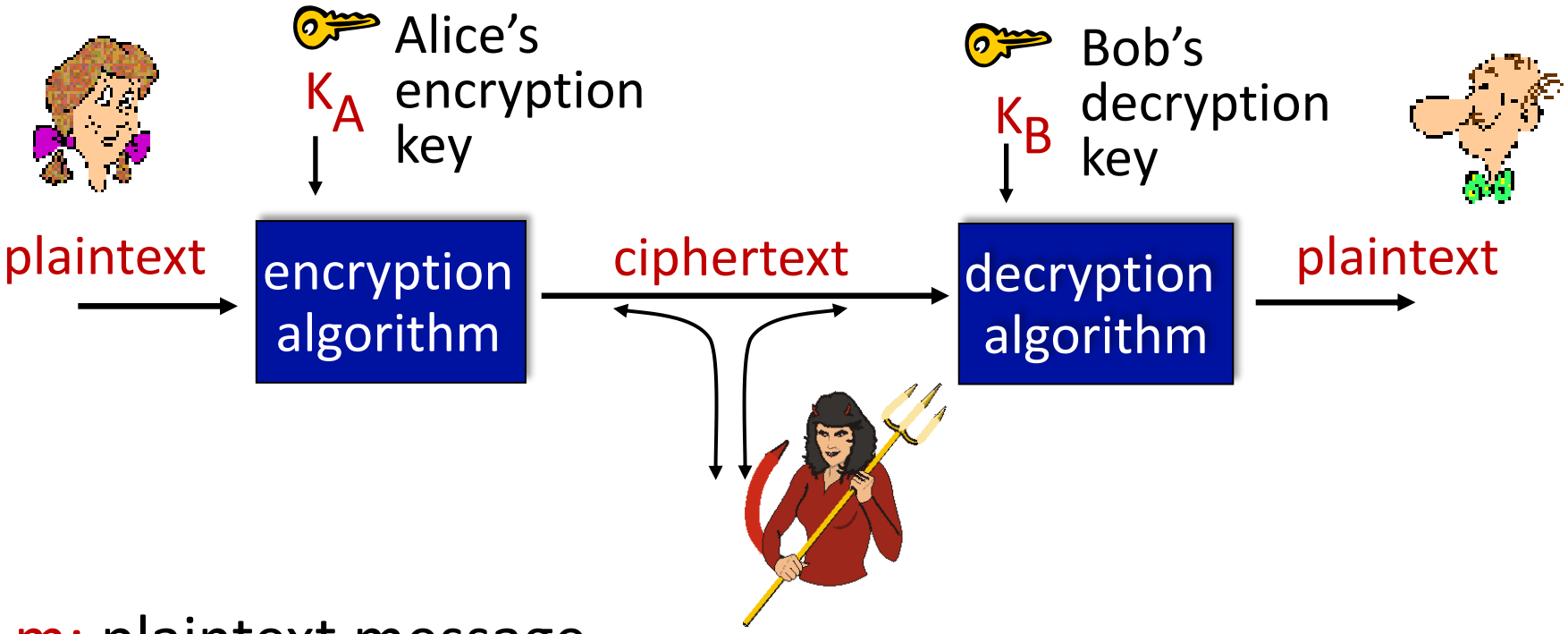
ISN Patterns

- Each OS uses a different algorithm for generating ISN's. So if we can detect the algorithm we can detect the OS.

Outline

- What is network security?
- Principles of cryptography
- Message integrity, authentication
- Securing e-mail
- Securing TCP connections: TLS
- Network layer security: IPsec
- Operational security: firewalls and IDS

The language of cryptography



m: plaintext message

$K_A(m)$: ciphertext, encrypted with key K_A

$m = K_B(K_A(m))$

Kerckhoffs's principle

- Auguste Kerckhoffs was a professor in Paris. In early 1883, Kerckhoffs' article, La Cryptographie Militaire states six design rules for military ciphers.
  1. The system must be practically, if not mathematically, indecipherable;
  2. **It should not require secrecy, and it should not be a problem if it falls into enemy hands;**
  3. It must be possible to communicate and remember the key without using written notes, and correspondents must be able to change or modify it at will;
  4. It must be applicable to telegraph communications;
  5. It must be portable, and should not require several persons to handle or operate;
  6. Lastly, given the circumstances in which it is to be used, the system must be easy to use and should not be stressful to use or require its users to know and comply with a long list of rules.

Breaking an encryption scheme

- cipher-text only attack:
  Trudy has ciphertext she can analyze
- known-plaintext attack:
  Trudy has plaintext corresponding to ciphertext
- chosen-plaintext attack:
  Trudy can get ciphertext for chosen plaintext
- two approaches:
  - brute force: search through all keys
  - statistical analysis

References

- S. Bellovin, COMS W4180, Columbia University, 2006.
- M. Kharrazi, CE-817, Sharif University of Technology, 2015.
- Kurose, James F., and Keith W. Ross. "Computer networking: A top-down approach edition." Addision Wesley (2007), chapter 8.
- ChatGPT, OpenAI.