0790326
Intrusion Detection and Prevention Systems

2023/2024 – Semester 2

Week 12

12th – 14th May 2024

جامعة فيلادلفيا
Philadelphia University

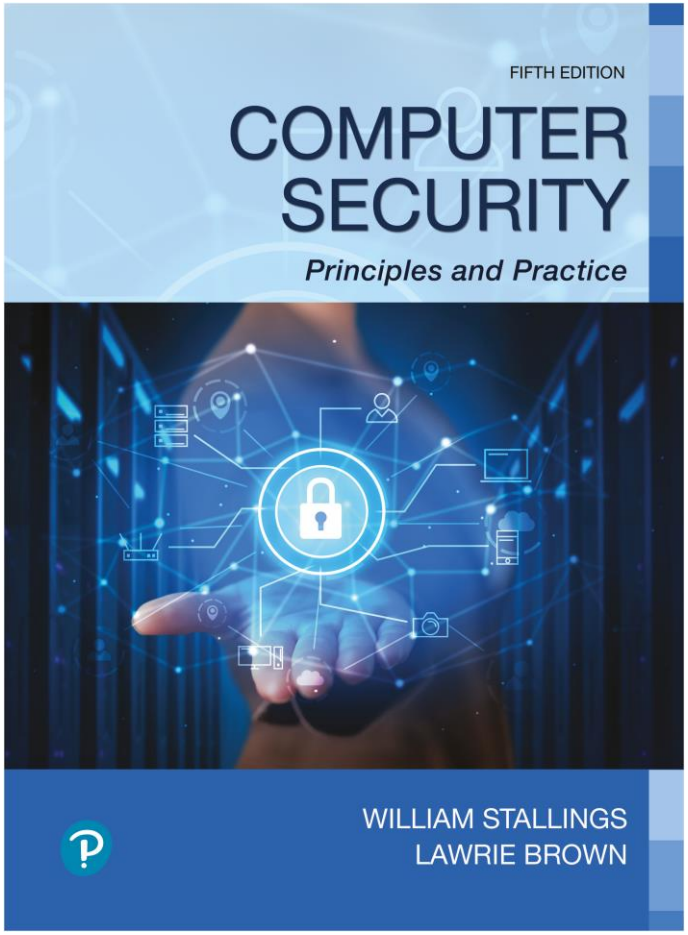
Dr. Basil Elmasri
balmasri@philadelphia.edu.jo

External Material

- Rest of the slides for this week are based on (Stallings & Brown, 2024) book, chapter 8.
  - Some extra slides have been added, their text was taken from the book.
  - Footers, dates, and slides number have been added only to help students reading the material.
- Study and exams will be based on the book chapters, not the slides.

Computer Security: Principles and Practice

Fifth Edition

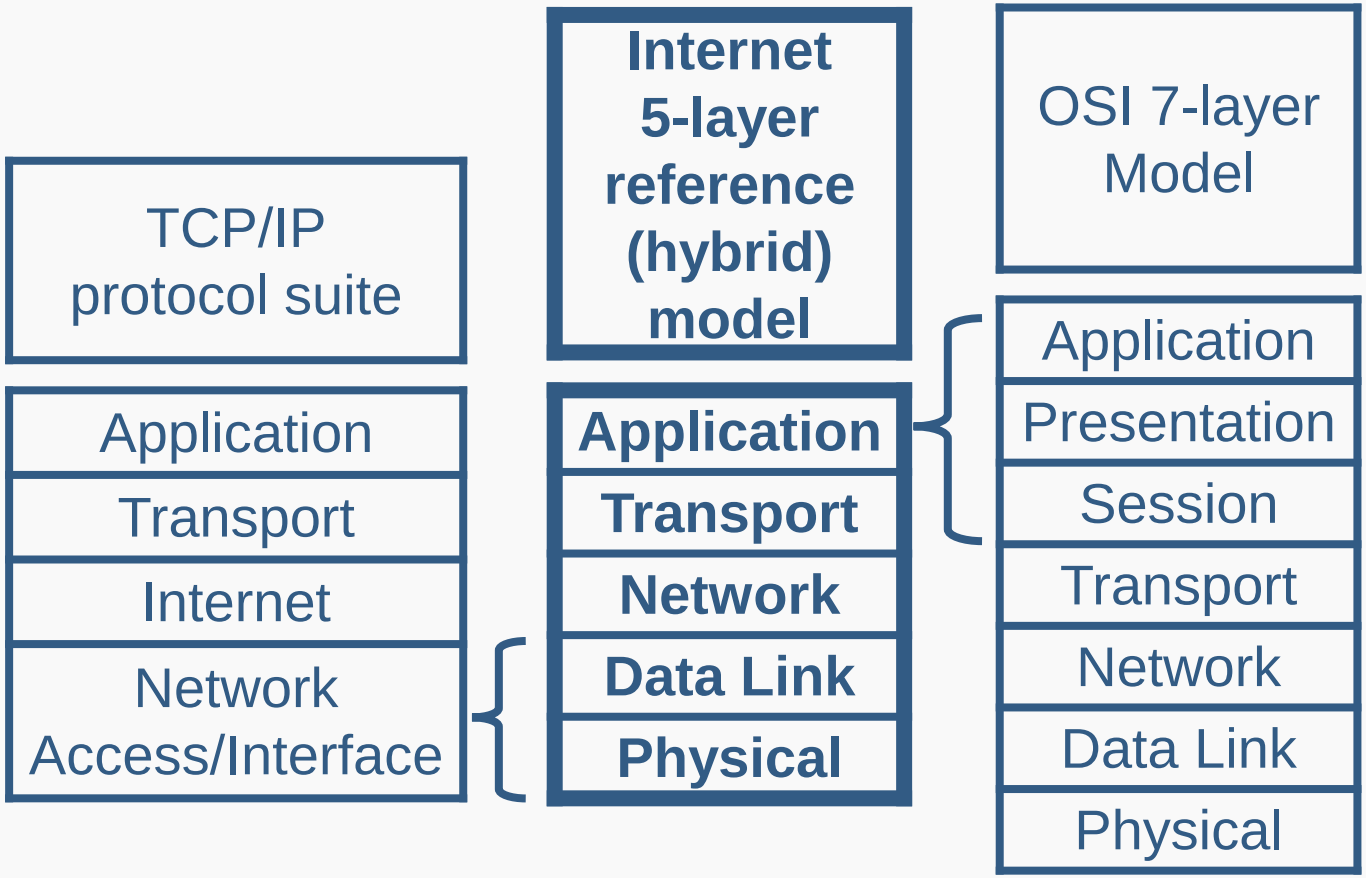


Chapter 9

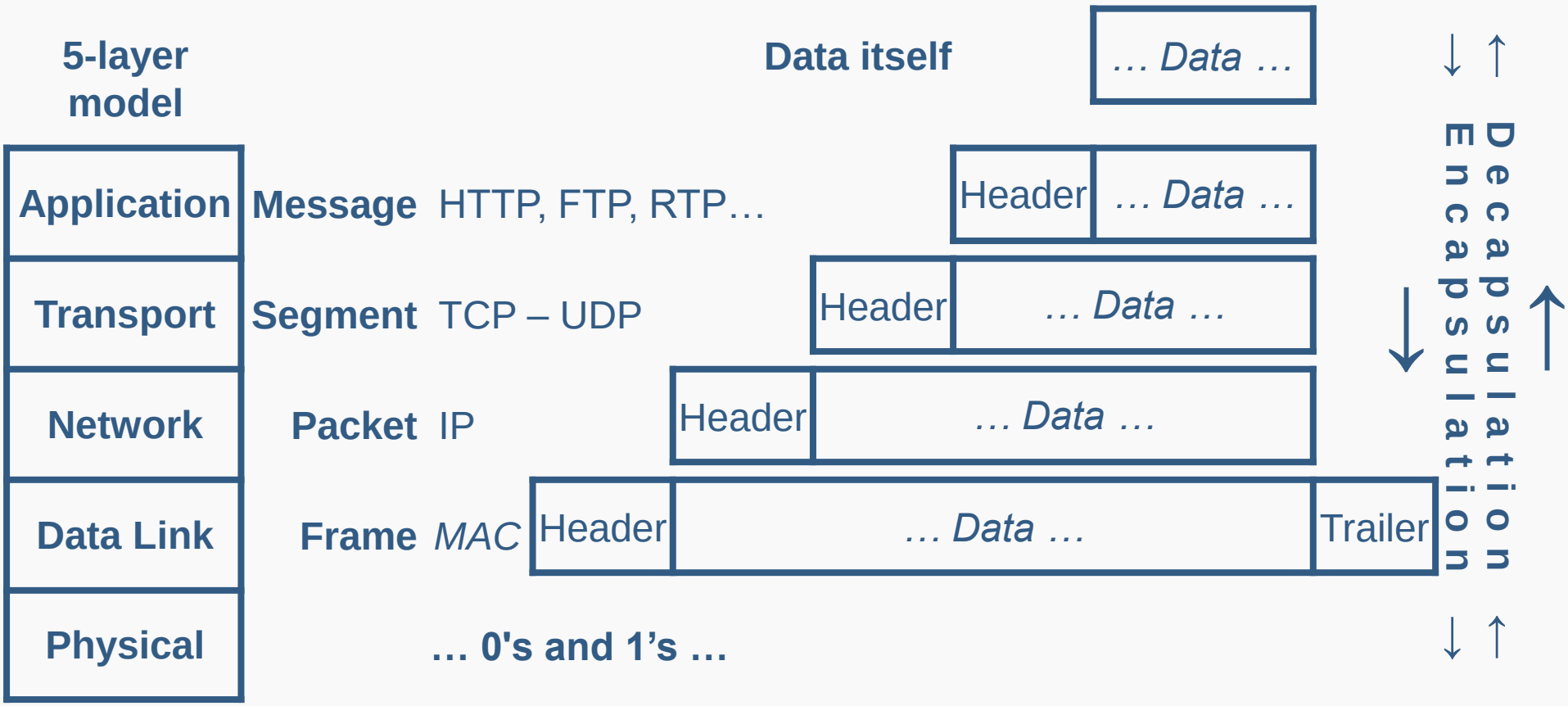
Firewalls and Intrusion Prevention Systems

Pearson

Computer Networks Layers

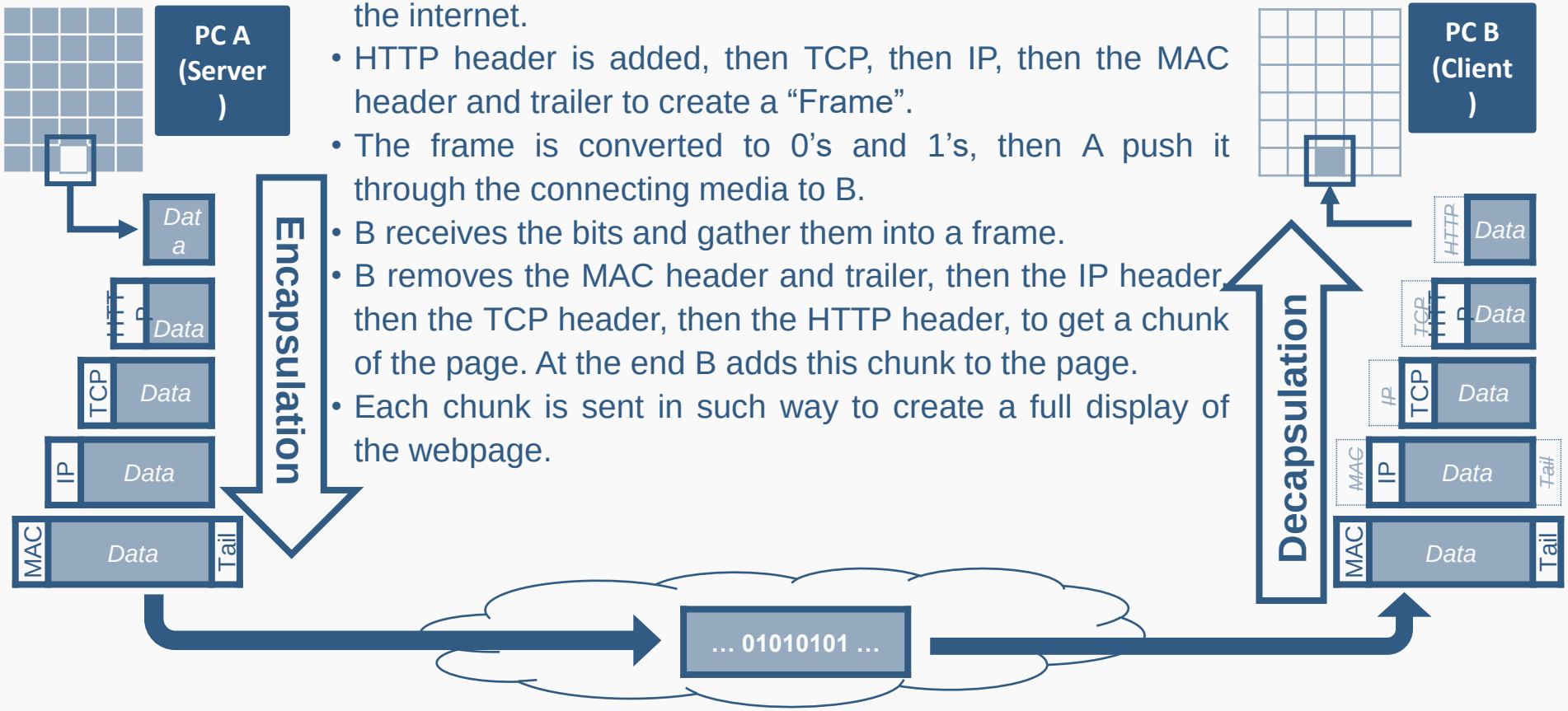


Encapsulation and Decapsulation



Encapsulation and Decapsulation Example

- Server A sends a webpage to B, after B has requested it.
- The page is broken down into chunks.
- Each chunk is appended with headers then sent to B via the internet.
- HTTP header is added, then TCP, then IP, then the MAC header and trailer to create a “Frame”.
- The frame is converted to 0’s and 1’s, then A push it through the connecting media to B.
- B receives the bits and gather them into a frame.
- B removes the MAC header and trailer, then the IP header, then the TCP header, then the HTTP header, to get a chunk of the page. At the end B adds this chunk to the page.
- Each chunk is sent in such way to create a full display of the webpage.



Network Security Monitoring

- Network Security Monitoring (NSM) is the collection and the analysis of network traffic and endpoint events in order to detect and escalation of indications and warnings to detect and respond to intrusions
- There are some techniques and tools to implement NSM as part of security operations.
- IoCs allow the NSM to detect suspicious activities across networks and devices.

- IoC could be network- or host-based and include:
  - IPs - Protocol signatures. -Directory names
  - File names. - Persistence mechanism.
  - Login, usernames, passwords. -MD5 (checksums)

The NSM Process

- Collection, detection and response.
- Collection of network traffic and endpoint events.

- **Network data collection can be:**
- Full packet data
- Session data
- Statistical data
- Alert data

Full Packet Data (I)

- A complete collection of network traffic.
- Raw data, the whole packets; packet headers as well as payloads.
- Best availability for the analysis in terms of either network monitoring for trouble shooting or network security issues, and in terms of providing evidence for further investigation.
- Advantages: granularity and application relevance it provides.

Full Packet Data (II)

- Granularity allows analysing every detail contained in the payloads of the packets, with the ability to reconstruct events in greater detail.
- The advantage of application relevance is that it allows inspection and storing evidence from the application layer protocols.
- It is not practical to collect, store and analyse the full packet data for the whole network of the organisation on a permeant basis.

Full Packet Data (III)

- In practice, such type of data collection would be run only for a critical segments of the network, or for a short period like during the investigation of a live intrusion incident.
- Full packet data collection will often require the use of specialised hardware with the required processing and storage resources
- It also focuses on collecting and analysing data from specific location of the network, like the perimeter and/or the main servers (assets).

Session Data (I)

- Session data usually contains information about transport layer. Typically, TCP sessions within of a communication exchange.
- Mainly source and destination IPs and port numbers, the timestamps of the session, and amount of data exchanged.
- For other connectionless protocols, such as UDP a session is not being established. however, a sort of heuristic rules to make up session's related information, like calculating the timestamps and data amount of the communication.

Session Data (II)

- Session data allows monitoring overall communication and activity patterns, locations or targets and time, of potential or actual intruders.

- While compared to full packet data, the amount and granularity of information are not the same in terms of availability

- Advantage of session data is significantly reducing the amount of data needed to analyse and store.

Statistical Data (I)

- Statistical data reduces the amount of collected information.
- Collecting and storing some statistical information about the traffic.
- What this statistical data exactly is will depend on the monitored environment
- Number of DNS requests being sent from a server in a local network.

Statistical Data (II)

- Inspect and collect information derived from the payload of the packets, like types, flags, code numbers, URLs… etc.
- Statistical data can allows identifying sudden spikes or unusual activity patterns (statistically).
- Unusual high number of a incoming protocol traffic, like requests.
- Unusual high volume of outgoing traffic could indicate data exfiltration.

Alert Data

- Alert data usually comes from security monitoring tools installed on endpoints across the network, such as firewalls and IDS's.
- The difference to the previous data collection types is that the rely is on the security tools to identify an event and generate the matching alerts.
- A network-based IDS will monitor the traffic in our network for potential intrusions, and if one is detected it will generate an alert and store the relevant evidence.
- The advantage the raw data related to the alert is stored, rather than all data going through the network.
- Significantly reduces the resources required for storing and further analysis of the evidence for an attack.

Detection

- Detection via the collected data and generating alerts based on an identified set of events.
- Typical methods of detection include signature-based, heuristic rule sets, or a machine learning model of anomaly detection or event classification.
- Alerts generated in the detection process will normally be a function of an IDS; network and end point.
- Network points, such as the firewall, and other endpoint security such as Endpoint Detection and Response (EDR), antivirus, or OS event logs.
- Also, alert generation can be performed in the Security Information and Event Management (SIEM) system.

Analysis

- The third phase of NSM.
- The analysis of the generated alerts and identification of any true positive security event.
- If a security incident is confirmed, it will be escalated for further investigation and response.
- Could be some automation of the tasks, thus it is primarily a human job performed by the security experts of the SOC team.
- It involves the collection and analysis of data and evidence from multiple sources, including threat intelligence.

References

Stallings, W., & Brown, L. (2024). Computer Security: Principles and Practice (5 ed.). Pearson. Retrieved from https://www.pearson.com/en-us/subject-catalog/p/computer-security-principles-and-practice/P200000010333/9780138091712