Session 10

DDoS Attacks

CS 7349

Spring 2024

World Changers
Shaped Here

SMU

Contents

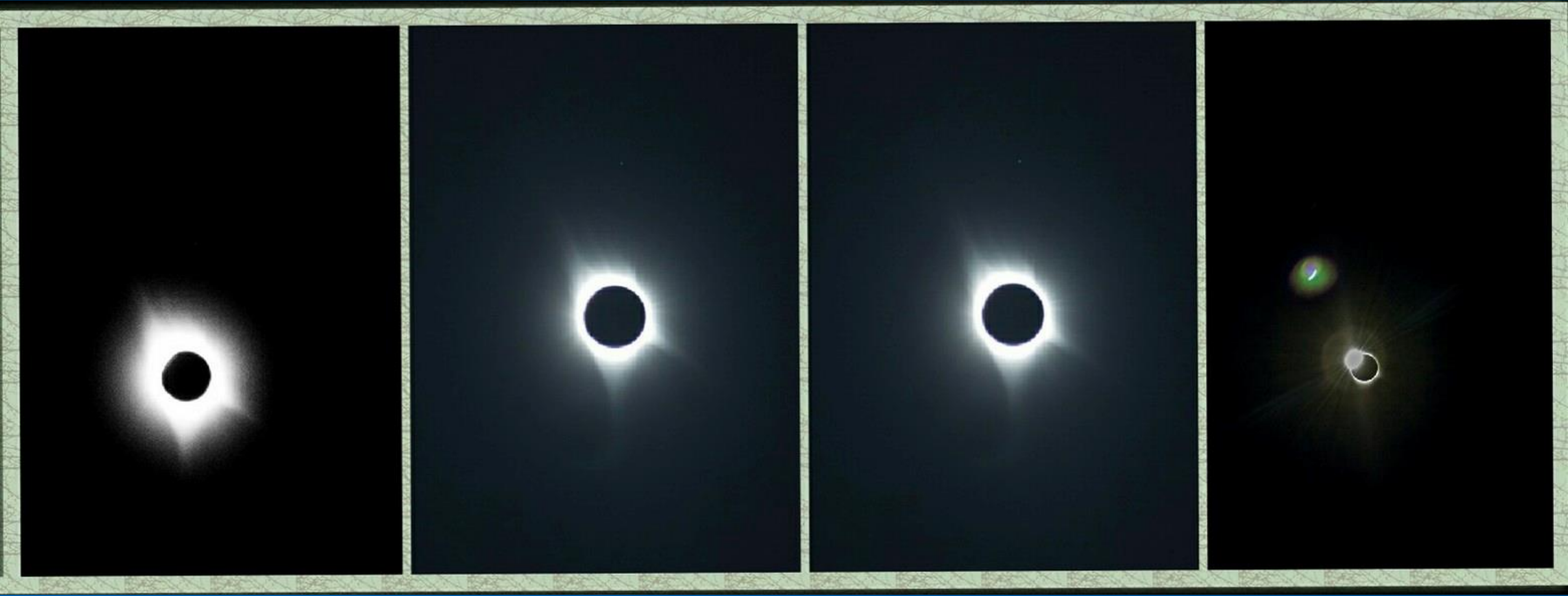
- Security News of the Week
- House Keeping
- Class Presentation
- Concepts: Enterprise Security Overview, Business Impact

Sources: Netscout/Radware; Cryptography and Network Security, William Stallings;

House Keeping

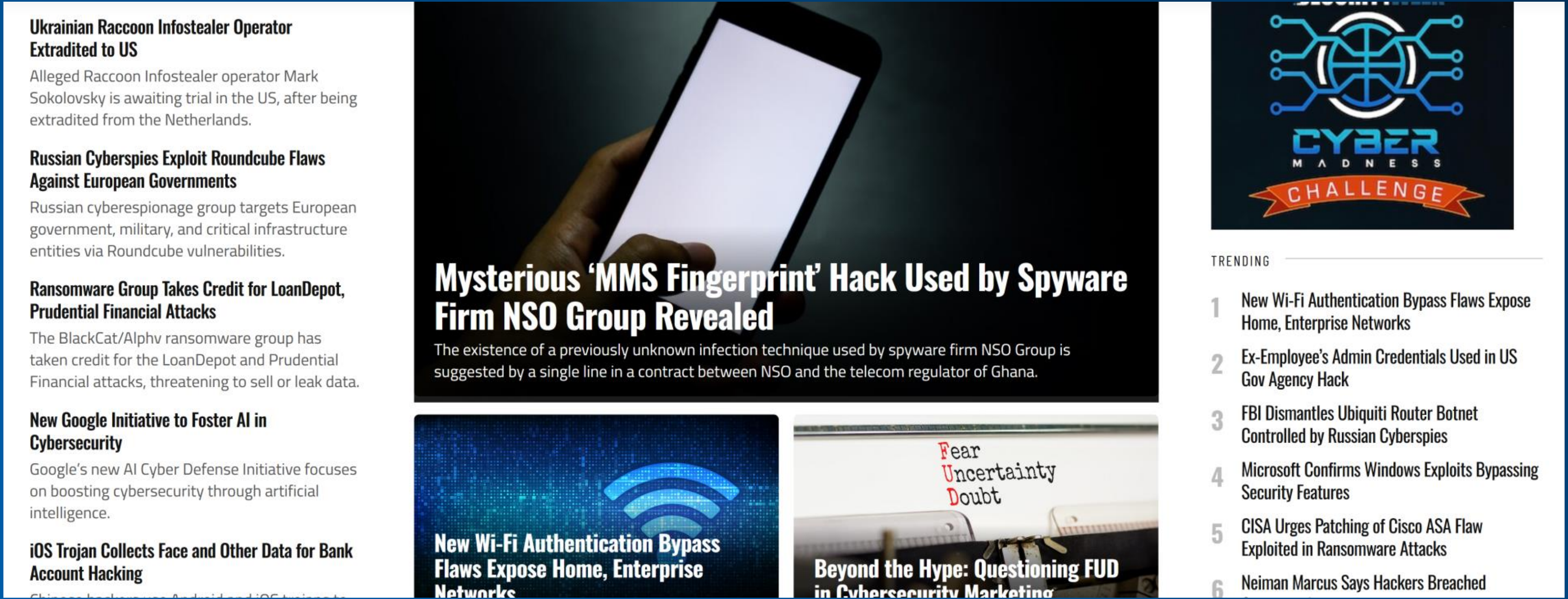
- Status of Teams for Term Paper? Presentations?
- Research Paper Feb deliverables;
- Checkpoint on 02/19; Guest Speaker Week of 02/26
- Exam1 published; Quiz to be published
- Research paper – 3 pages due. Expectations (Abstract/Intro/Current Research/Solution/References)
- A word on prioritization and project management

Outside Classroom studies



Sources: Shaibal Chakrabarty, Solar Eclipse, 2017; Location: Padukah, Kentucky

Security News of the Week – Spring 2024



Ukrainian Raccoon Infostealer Operator Extradited to US

Alleged Raccoon Infostealer operator Mark Sokolovsky is awaiting trial in the US, after being extradited from the Netherlands.

Russian Cyberspies Exploit Roundcube Flaws Against European Governments

Russian cyberespionage group targets European government, military, and critical infrastructure entities via Roundcube vulnerabilities.

Ransomware Group Takes Credit for LoanDepot, Prudential Financial Attacks

The BlackCat/Alphv ransomware group has taken credit for the LoanDepot and Prudential Financial attacks, threatening to sell or leak data.

New Google Initiative to Foster AI in Cybersecurity

Google's new AI Cyber Defense Initiative focuses on boosting cybersecurity through artificial intelligence.

iOS Trojan Collects Face and Other Data for Bank Account Hacking

Mysterious 'MMS Fingerprint' Hack Used by Spyware Firm NSO Group Revealed

The existence of a previously unknown infection technique used by spyware firm NSO Group is suggested by a single line in a contract between NSO and the telecom regulator of Ghana.

New Wi-Fi Authentication Bypass Flaws Expose Home, Enterprise Networks

Beyond the Hype: Questioning FUD in Cybersecurity Marketing

TRENDING

1 New Wi-Fi Authentication Bypass Flaws Expose Home, Enterprise Networks

2 Ex-Employee's Admin Credentials Used in US Gov Agency Hack

3 FBI Dismantles Ubiquiti Router Botnet Controlled by Russian Cyberspies

4 Microsoft Confirms Windows Exploits Bypassing Security Features

5 CISA Urges Patching of Cisco ASA Flaw Exploited in Ransomware Attacks

6 Neiman Marcus Says Hackers Breached

Source: securityweek.com

CS 7349 – Tying it all together

- INTRODUCTION TO DS7349 AND THE THREAT LANDSCAPE
- INTRODUCTION TO NETWORKS
- SYMMETRIC KEY CRYPTO
- USING SYMMETRIC KEY CIPHERS
- RANDOMNESS AND PSEUDORANDOM NUMBERS
- PUBLIC KEY CRYPTO/Team Paper

Confidentiality

- HASH FUNCTIONS
- MESSAGE AUTHENTICATION CODES
- KEY MANAGEMENT
- IDENTITY AND ACCESS MANAGEMENT

Integrity **Availability**

- ENTERPRISE SECURITY
- SECURITY – CLOUD, WIRELESS/5G, DDoS, SASE, IoT, SDN, Smart Cities
- FRAMEWORKS, STANDARDS, OPERATIONS, Governance/Risk/Compliance
- REVIEW/ADDITIONAL TOPICS

Networks/Application

Spring schedule

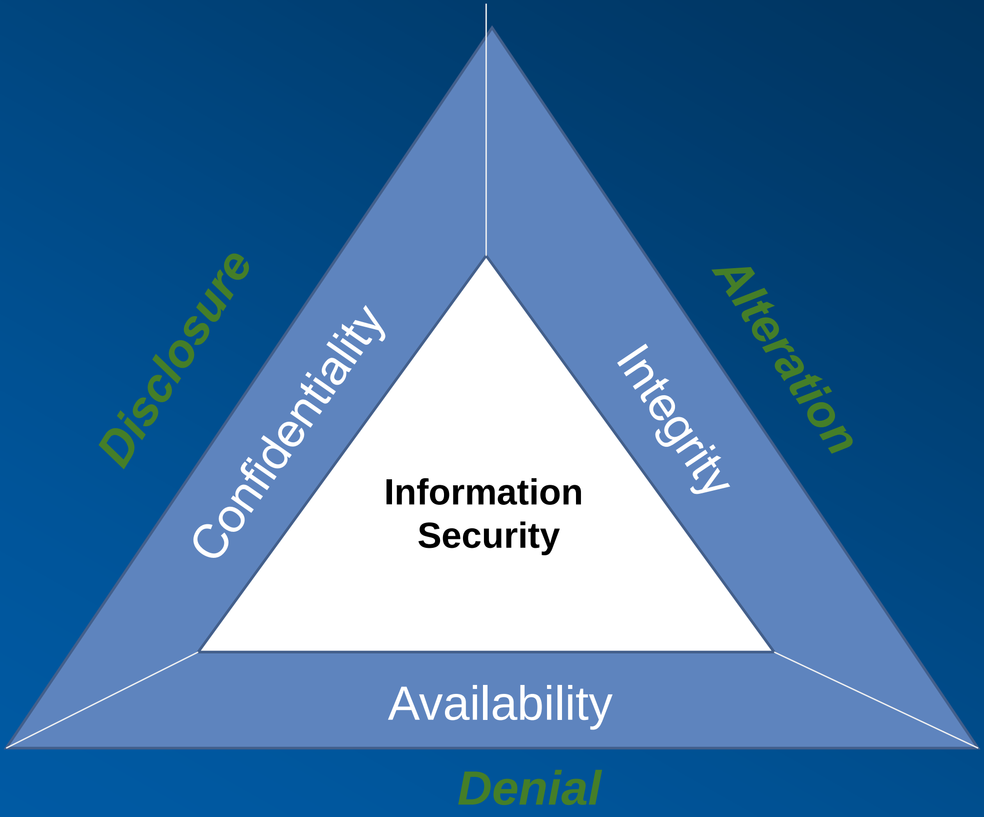
Date	Week/Unit	Learning Material	Assignment
01/17/2024	1/1	Intro to Data and Network Security	Stallings Ch 1; Quiz#1;Start project team, select project and inform instructor
Jan 22, 24	2/2	Intro to Computer Networks	Submit Quiz #2; Project team confirms problem with instructor/Homework 1 issued/Term paper checkpoint
Jan 29, 31	3/3	Symmetric Key Cryptography	Stallings Ch 2-3; Submit Quiz #3; First Project Draft (Title, authors, abstract and Intro)/
Feb 5, 7	4/4	Using Symmetric Key Ciphers	Stallings Ch 3-6; Submit Quiz#4 (ch03 and ch06); Homework #2 issued
Feb 12, 14	5/5	Randomness and Pseudorandom Numbers	Stallings Ch 7; Submit Quiz #5/Term Paper Checkpoint
Feb 19, 21	6/6	Public Key Cryptography	Stallings Ch 9-10; Submit Quiz #6/Case Study Due/
Feb 26, 28	7/7	Hash Functions/	Stallings Ch 11; Submit Quiz #7; Paper Interim Draft; Exam 1 issued
Mar 4, 6	8/8	Message Authentication Codes	Stallings Ch 12; Submit Quiz#8;
Mar 11, 13	9/9	SPRING BREAK!!!	
Mar 18, 20	03/10	Key Management and Key Distribution	Stallings Ch 14; Submit Quiz #10/Term paper checkpoint/Start on project presentation/Case Study
Mar 25, 27	04/11	User Authentication	Stallings Ch 15; Submit Quiz #11/
Apr 1, 3	12/12	Network Security	Stallings Ch 17; Submit Quiz #12; Presentation check/Exam #2
Apr 8, 10	13/13,14	Privacy, Security Ethics	
Apr 15, 17	14	Applications: AI and Quantum Computing	Submit Final Project Paper
Apr 22, 24	15	Open	Presentations of Term Project by class/
Apr 29		Wrap up and Review	
This schedule is subject to changes. All assignments are due by 11:59pm of the due date. Earlier submissions are encouraged and welcome. Do not wait till the last moment.			
You will have 2 weeks to complete most assignments.			

Book: Cryptography and Network Security by William Stallings, 8th edition

Class Presentation - Special Topic

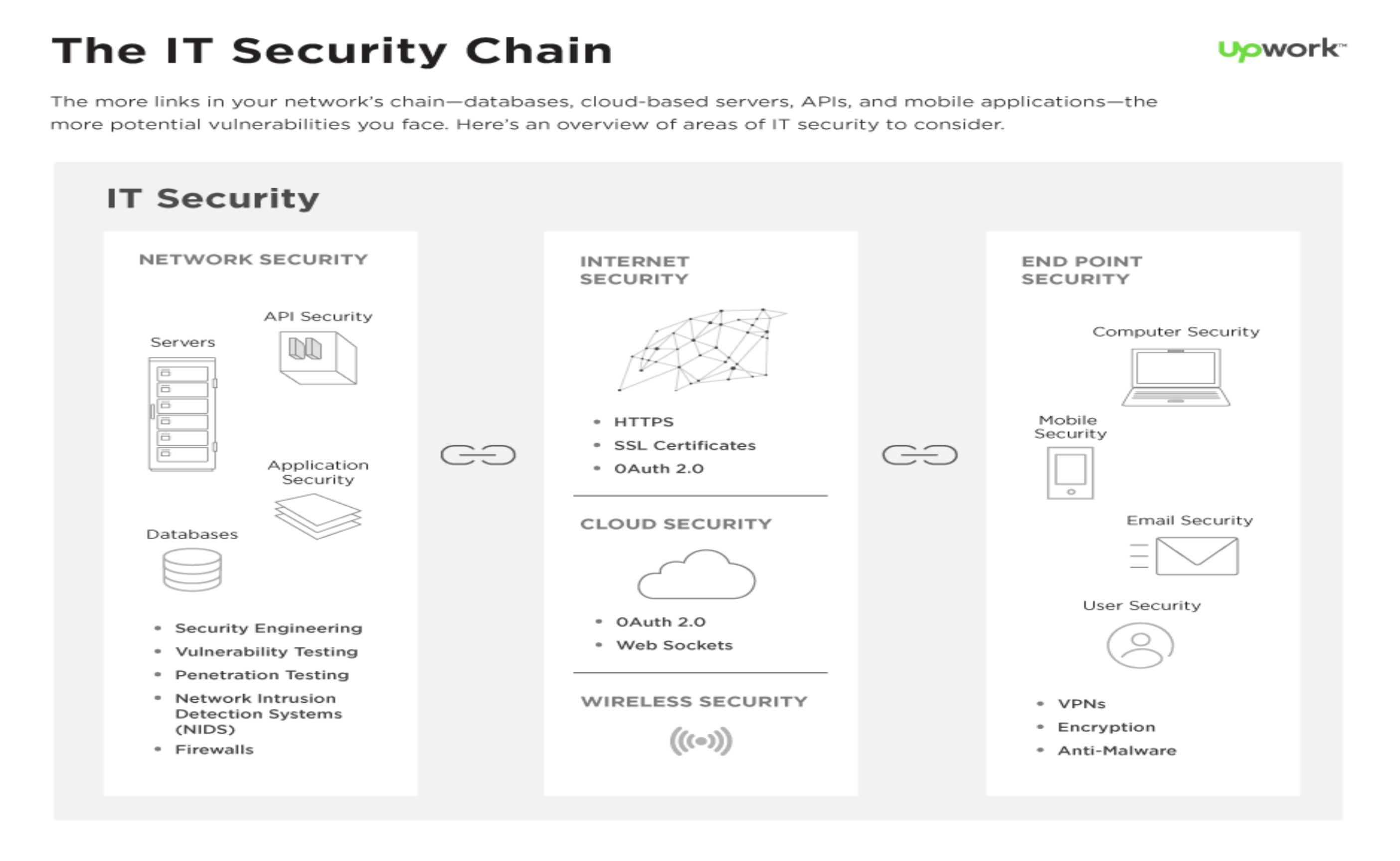
- Any topic of your interest: Work, ~~school~~, play
  - Can be a question/answer, wonderment, information
  - **Security related; NOT term paper related; NO course topic**
  - Strict time limits 5 mins + 3 mins Q&A
- Schedule – as per roster
  - ~~Adu, Aliliele~~, ~~Braden~~, ~~Cho~~, ~~Dominguez~~, ~~Garcia~~, Garza, ~~Gibbs~~, Guo, ~~Hennes~~, Jackson, Kharwadhkar, Kucera, Lei, Liang, Lim, Lin, Liu, Magee, Mandalaneni, Mathew, Miller, Nagamanickam, DPatel, PPatel, Pittman, Sanaboyina, Singh, Skochdopole, Swigart, Taghavi, Wang, Werth, Zhai

InfoSec, CIA, Threats



Source: “Information Security Illuminated”, Solomon and Chapple, 2005, Sudbury, MA:Jones and Bartlett.

Network Security Basics



The IT Security Chain

upwork™

The more links in your network's chain—databases, cloud-based servers, APIs, and mobile applications—the more potential vulnerabilities you face. Here's an overview of areas of IT security to consider.

IT Security

NETWORK SECURITY

- Security Engineering
- Vulnerability Testing
- Penetration Testing
- Network Intrusion Detection Systems (NIDS)
- Firewalls

INTERNET SECURITY

- HTTPS
- SSL Certificates
- OAuth 2.0

CLOUD SECURITY

- OAuth 2.0
- Web Sockets

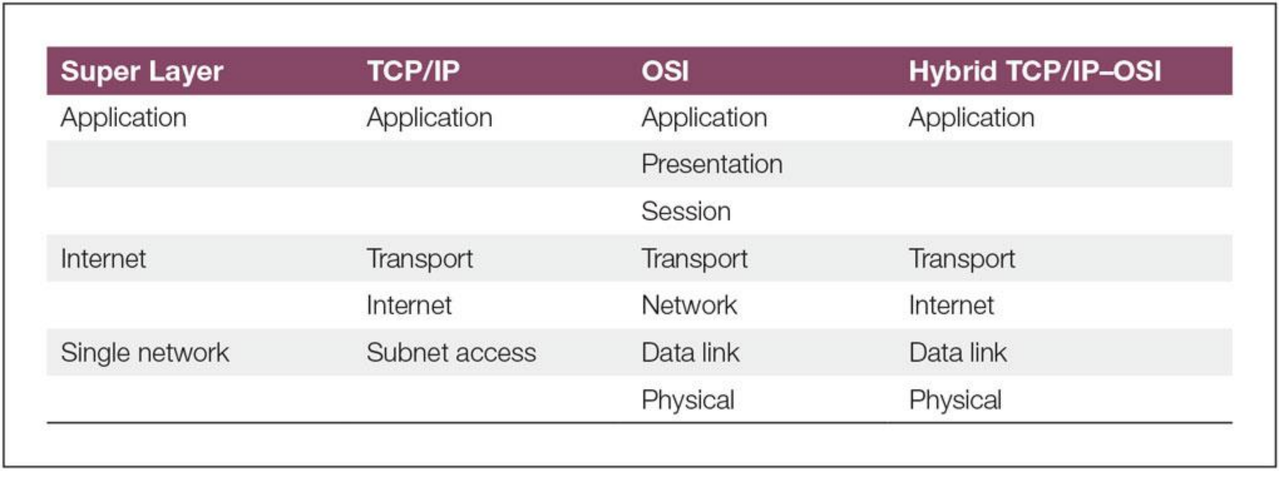
WIRELESS SECURITY

END POINT SECURITY

- VPNs
- Encryption
- Anti-Malware

Source: Upwork Global, Inc

Layered Standards Architectures



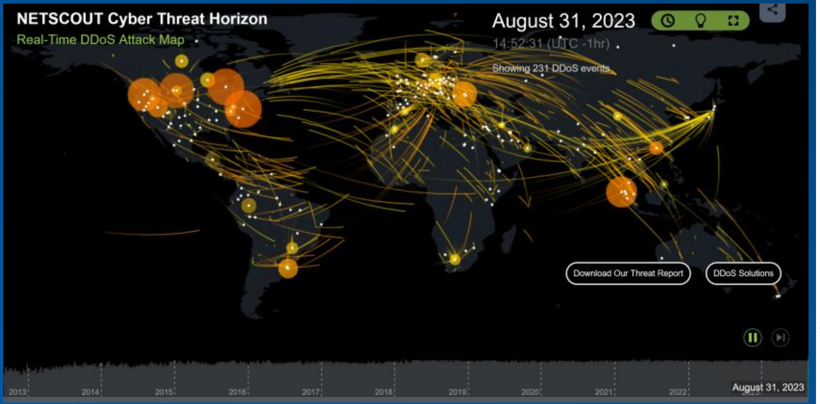
Super Layer	TCP/IP	OSI	Hybrid TCP/IP–OSI
Application	Application	Application	Application
		Presentation	
		Session	
Internet	Transport	Transport	Transport
	Internet	Network	Internet
Single network	Subnet access	Data link	Data link
		Physical	Physical

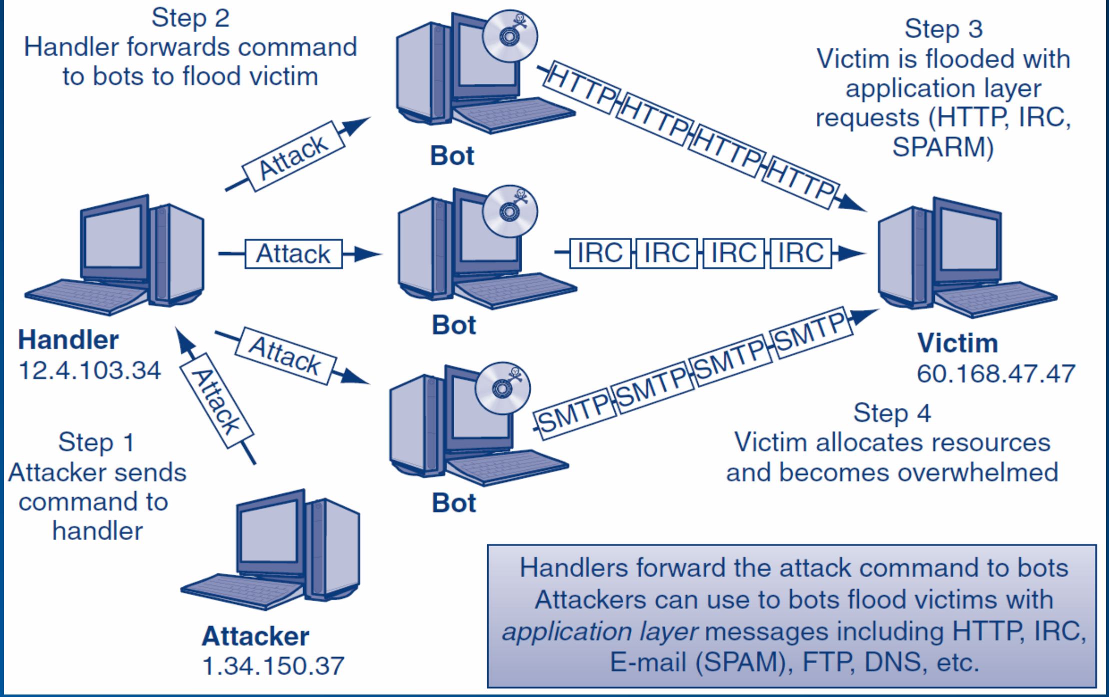
Source: Panko and Boyle, Pearson 5e

Denial-of-Service Attack (DoS)

- An attempt to prevent legitimate users of a service from using that service
- When this attack comes from a single host or network node, then it is simply referred to as a DoS attack
- A more serious threat is posed by a Distributed Denial-of-Service (DDoS) attack
    - DDoS attacks make computer systems inaccessible by flooding servers, networks, or even end-user systems with useless traffic so that legitimate users can no longer gain access to those resources
    - In a typical DDoS attack, a large number of compromised hosts are amassed to send useless packets

Network Security: DDoS Attack





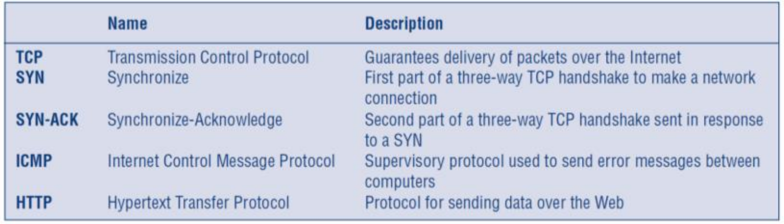
Step 2
Handler forwards command to bots to flood victim

Step 3
Victim is flooded with application layer requests (HTTP, IRC, SPARM)

Step 1
Attacker sends command to handler

Step 4
Victim allocates resources and becomes overwhelmed

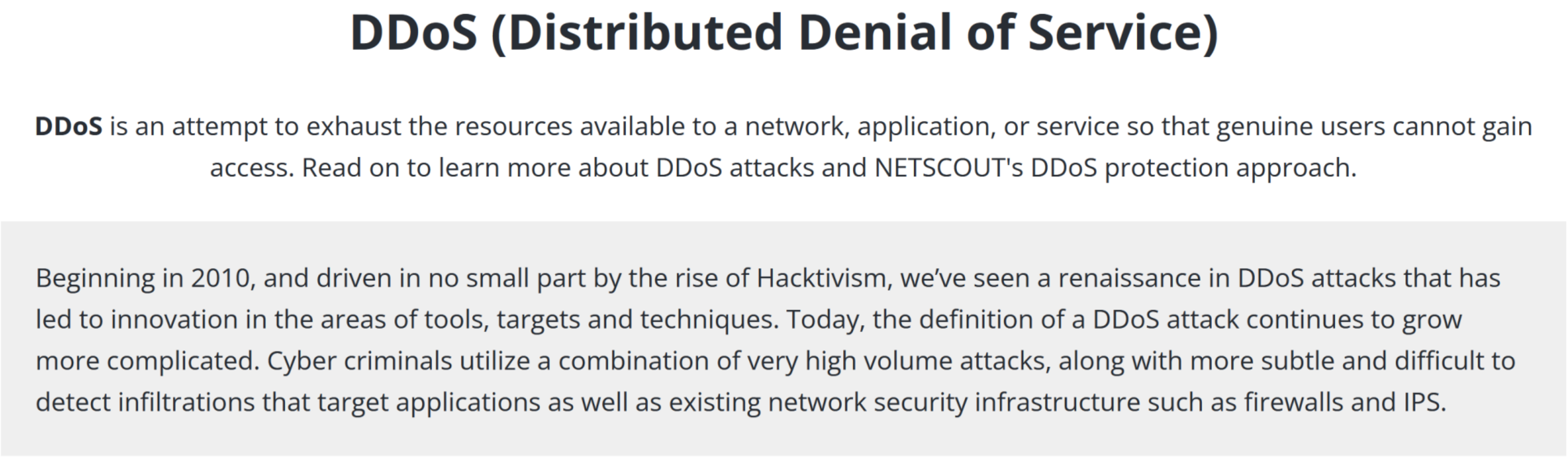
Handlers forward the attack command to bots
Attackers can use to bots flood victims with *application layer* messages including HTTP, IRC, E-mail (SPAM), FTP, DNS, etc.



	Name	Description
TCP	Transmission Control Protocol	Guarantees delivery of packets over the Internet
SYN	Synchronize	First part of a three-way TCP handshake to make a network connection
SYN-ACK	Synchronize-Acknowledge	Second part of a three-way TCP handshake sent in response to a SYN
ICMP	Internet Control Message Protocol	Supervisory protocol used to send error messages between computers
HTTP	Hypertext Transfer Protocol	Protocol for sending data over the Web

Source: Corporate Computer Security; Panko and Boyle; https://horizon.netscout.com/

What is a DDoS Attack?



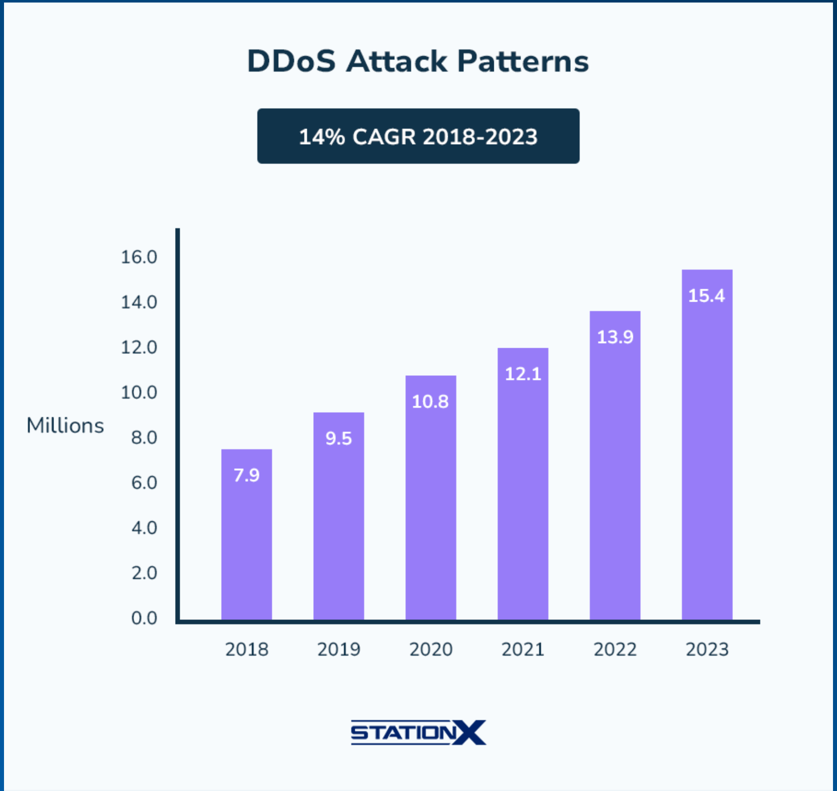
DDoS (Distributed Denial of Service)

DDoS is an attempt to exhaust the resources available to a network, application, or service so that genuine users cannot gain access. Read on to learn more about DDoS attacks and NETSCOUT's DDoS protection approach.

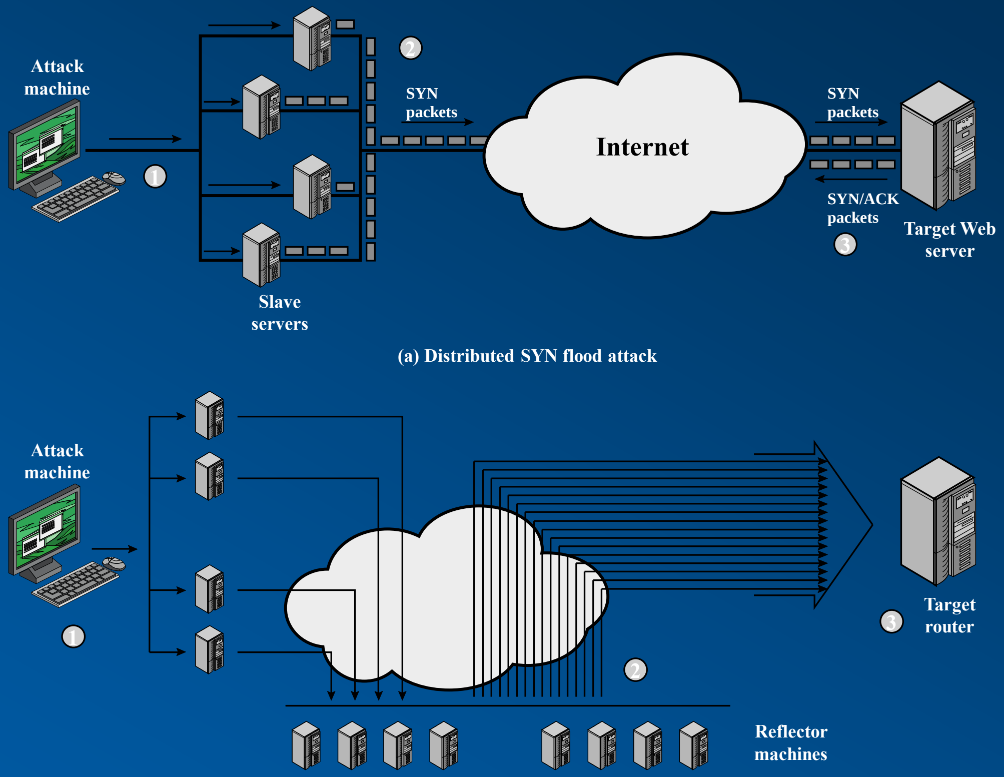
Beginning in 2010, and driven in no small part by the rise of Hacktivism, we've seen a renaissance in DDoS attacks that has led to innovation in the areas of tools, targets and techniques. Today, the definition of a DDoS attack continues to grow more complicated. Cyber criminals utilize a combination of very high volume attacks, along with more subtle and difficult to detect infiltrations that target applications as well as existing network security infrastructure such as firewalls and IPS.

Source: https://horizon.netscout.com/

DDoS Attack Statistics



Source: https://www.stationx.net/ddos-statistics/



(a) Distributed SYN flood attack

(a) Distributed ICMP attack

Figure 21.8 Examples of Simple DDoS Attacks

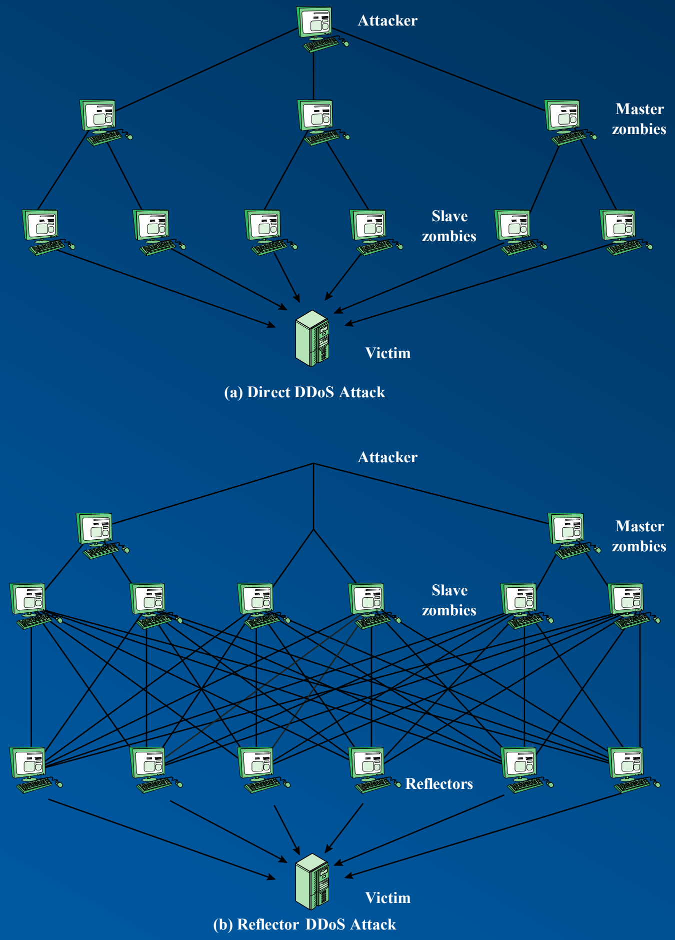


Figure 21.9 Types of Flooding-Based DDoS Attacks

DDoS Countermeasures

- In general, there are three lines of defense against DDoS attacks:
  - **Attack prevention and preemption (before the attack):**
    - These mechanisms enable the victim to endure attack attempts without denying service to legitimate clients
    - Techniques include enforcing policies for resource consumption and providing backup resources available on demand
    - In addition, prevention mechanisms modify systems and protocols on the Internet to reduce the possibility of DDoS attacks
  - **Attack detection and filtering (during the attack):**
    - These mechanisms attempt to detect the attack as it begins and respond immediately. This minimizes the impact of the attack on the target
    - Detection involves looking for suspicious patterns of behavior
    - Response involves filtering out packets likely to be part of the attack
  - **Attack source traceback and identification (during and after the attack):**
    - This is an attempt to identify the source of the attack as a first step in preventing future attacks. However, this method typically does not yield results fast enough, if at all, to mitigate an ongoing attack
- The challenge in coping with DDoS attacks is the sheer number of ways in which they can operate so DDoS countermeasures must evolve with the threat

DDoS Countermeasures

- Frequently done by traffic reroutes
- https://cybersecurity.att.com/products/reactive-ddos-services#watch-ddos-fv6oejX7nKcSdcrvMBg59v:7013q000001kDCz

Company	Type	Business Type
Akamai/Cloudflare	CDN Networks	Product and Service Company
AT&T/Lumen/Verizon	Broadband Network	Service Provider
Amazon/Microsoft	Cloud network	Cloud Provider
Netscout/Radware		Product companies with DDoS Service

Source: att.com; cloudflare.com;

Thank You!

World Changers
Shaped Here

SMU®

Project Timeline (For 9 page paper)

- Jan: First project draft 1 page, basically your Introduction section, plus title, authors and abstract, some references
- Feb: Interim draft 3 pages, basically your intro and related work, plus basic description of your solution
- Mar: Draft 6 pages. Detailed solution, analysis, references
- Apr: Final paper 9 pages. Submit, with presentation

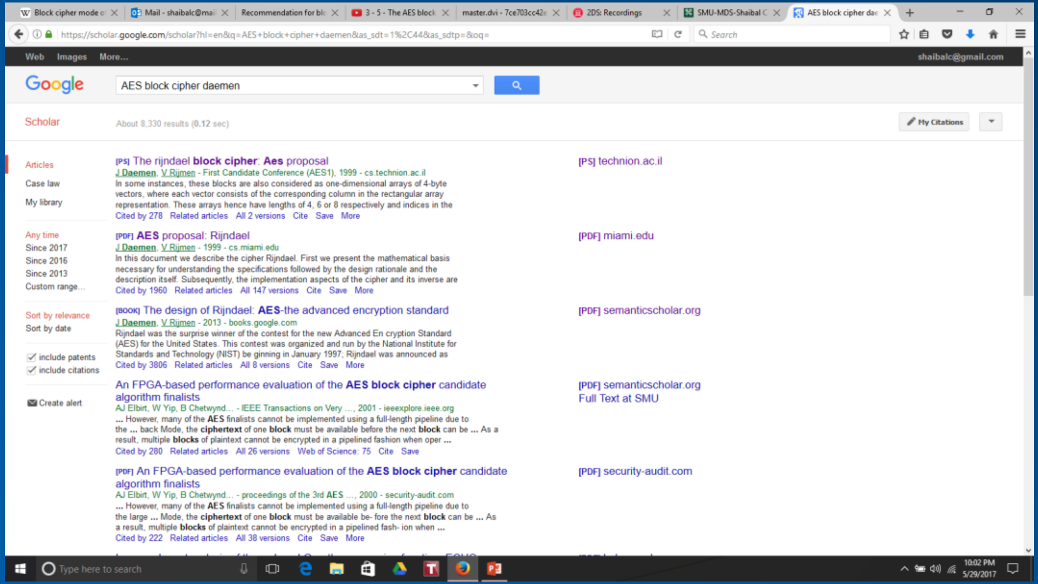
A LaTex template and example paper will be provided

Project – 2nd deliverable

- Refine Abstract and Intro
- Write down 1 page of current research on the topic with a storyline to show how your novel approach differs
- Prepare the section of your solution, your architecture, your data/introduction to your simulation
- Ensure you have a MINIMUM of 3 pages including abstract, intro, current research and references.

Peer reviewed publications

- https://scholar.google.com/
- Get your references from here, and download IEEE, ACM and other papers from CUL. (http://www.smu.edu/cul)



https://scholar.google.com/scholar?hl=en&q=AES+block+cipher+daemen&as_sdt=1%2C44&as_sdtp=&oq=

AES block cipher daemen

About 8,330 results (**0.12** sec)

☑ include patents
☑ include citations

[PS] The rijndael **block cipher**: **Aes** proposal — [PS] technion.ac.il
J Daemen, V Rijmen - First Candidate Conference (AES1), 1999 - cs.technion.ac.il
In some instances, these blocks are also considered as one-dimensional arrays of 4-byte vectors, where each vector consists of the corresponding column in the rectangular array representation. These arrays hence have lengths of 4, 6 or 8 respectively and indices in the
Cited by 278 Related articles All 2 versions Cite Save More

[PDF] **AES** proposal: Rijndael — [PDF] miami.edu
J Daemen, V Rijmen - 1999 - cs.miami.edu
In this document we describe the cipher Rijndael. First we present the mathematical basis necessary for understanding the specifications followed by the design rationale and the description itself. Subsequently, the implementation aspects of the cipher and its inverse are
Cited by 1960 Related articles All 147 versions Cite Save More

[BOOK] The design of Rijndael: **AES**-the advanced encryption standard — [PDF] semanticscholar.org
J Daemen, V Rijmen - 2013 - books.google.com
Rijndael was the surprise winner of the contest for the new Advanced En cryption Standard (AES) for the United States. This contest was organized and run by the National Institute for Standards and Technology (NIST) be ginning in January 1997; Rijndael was announced as
Cited by 3806 Related articles All 8 versions Cite Save More

An FPGA-based performance evaluation of the **AES block cipher** candidate algorithm finalists — [PDF] semanticscholar.org Full Text at SMU
AJ Elbirt, W Yip, B Chetwynd... - IEEE Transactions on Very ..., 2001 - ieeexplore.ieee.org
... However, many of the **AES** finalists cannot be implemented using a full-length pipeline due to the **...** back Mode, the **ciphertext** of one **block** must be available before the next **block** can be **...** As a result, multiple **blocks** of plaintext cannot be encrypted in a pipelined fashion when oper **...**
Cited by 280 Related articles All 26 versions Web of Science: 75 Cite Save

[PDF] An FPGA-based performance evaluation of the **AES block cipher** candidate algorithm finalists — [PDF] security-audit.com
AJ Elbirt, W Yip, B Chetwynd... - proceedings of the 3rd **AES** ..., 2000 - security-audit.com
... However, many of the **AES** finalists cannot be implemented using a full-length pipeline due to the large **...** Mode, the **ciphertext** of one **block** must be available be- fore the next **block** can be **...** As a result, multiple **blocks** of plaintext cannot be encrypted in a pipelined fash- ion when **...**
Cited by 222 Related articles All 38 versions Cite Save More

Project Reports

- **Use the LaTex template** provided for your project paper submissions.
- **Read** the Sample paper and **follow** its directions as appropriate in writing your paper.
- Your paper is expected to be publishable
  - High quality research, well written, reproducible results based on paper contents.
- https://scholar.google.com/ for references (NOT cnn.com, foxnews.com, cnbc.com; YES ietf.org, ieee.org,…itu-t)

Project Abstract and Intro

- **Abstract** structure (125-150 word limit for 9 pages)
  - start with statement of what is presented (2 sentences)
  - motivate the problem (2-3 sentences)
  - discuss details of what is done at a high level (1-2 sentences)
  - state the main conclusions (1-2 sentences)
- **Introduction** basic structure (the rest of page 1):
  - motivate the problem further
  - state the problem in detail
  - state the basic work done/approach taken
  - State the contributions of your paper (2nd last paragraph)
  - state the outline for the rest of the paper (final paragraph)
    - Conclusions are not stated in the introduction.

Project Paper

- **Use the LaTex template** provided for all of your project paper submissions.
- Your paper is expected to be publishable
  - High quality research, well written, reproducible results based on paper contents. 9 pages exactly. No more, no less
  - https://scholar.google.com/ for references (NOT cnn.com, foxnews.com, cnbc.com; YES ietf.org, ieee.org,…itu-t)
  - https://www.overleaf.com/read/brpdfvsxsjww#8886a4 ←Paper template