Connecting the Dots: Cybersecurity Fundamentals

Eric Yocam, DBA, MS.

Bio

https://www.linkedin.com/in/eric-yocam/

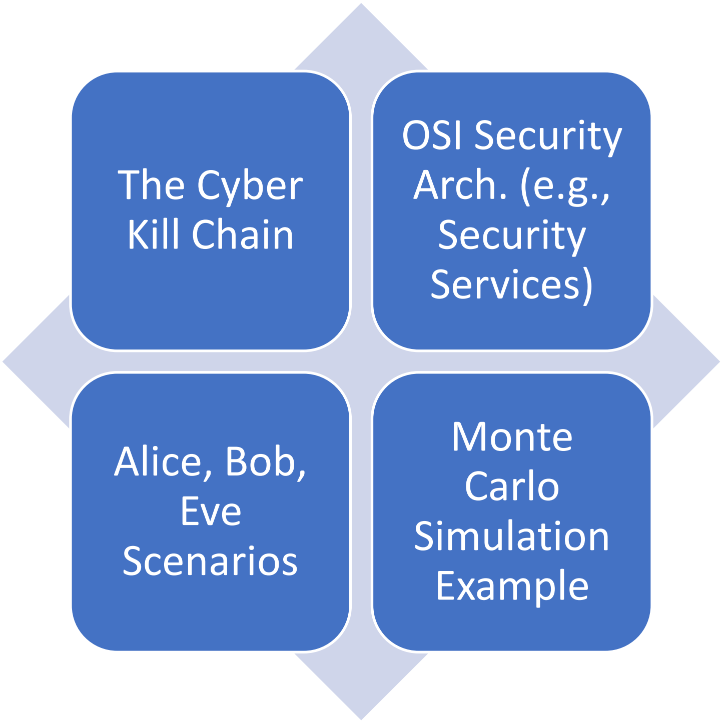
https://github.com/ericyoc

https://www.credly.com/users/ericyocam

https://orcid.org/0000-0001-8176-3867

- Industry professional with over two decades of experience in high tech (Startup companies & Apple, HP, Microsoft, T-Mobile)
- Published Articles (networking, cybersecurity, 5G, IoT, privacy preservation)
- Over decade teaching at all levels (undergrad, grad., doctoral)
- Security exam question writer (ISC2, ISACA, EC-Council)
- Inventor (20+ issued patents)

Topics



Disclaimer: There may be some cybersecurity terms used that we simply do not have enough time to go in-depth so we will have to postpone for a different time.

Why is cybersecurity important?

- **Connecting the dots:**
- Hint: we live in an interconnected world…

What happens without cybersecurity?

Plausible Answer:

- Cybersecurity is an essential aspect of modern computing
  - Cybercrime, data breaches, ransomware, IoT vulnerabilities, cloud security, cybersecurity skills gap, remote work security, AI and ML in cybersecurity

- Understanding cybersecurity concepts help to create secure systems and defend against attacks
  - Career opportunities, foundational knowledge, practical skills development, interdisciplinary application, personal digital safety, ethical hacking opportunities

Terminology: A Bad Actor

bad actor

- threat actor, hacker, *attacker*, *adversary*, *black hat*, nation-state, cybercriminal…

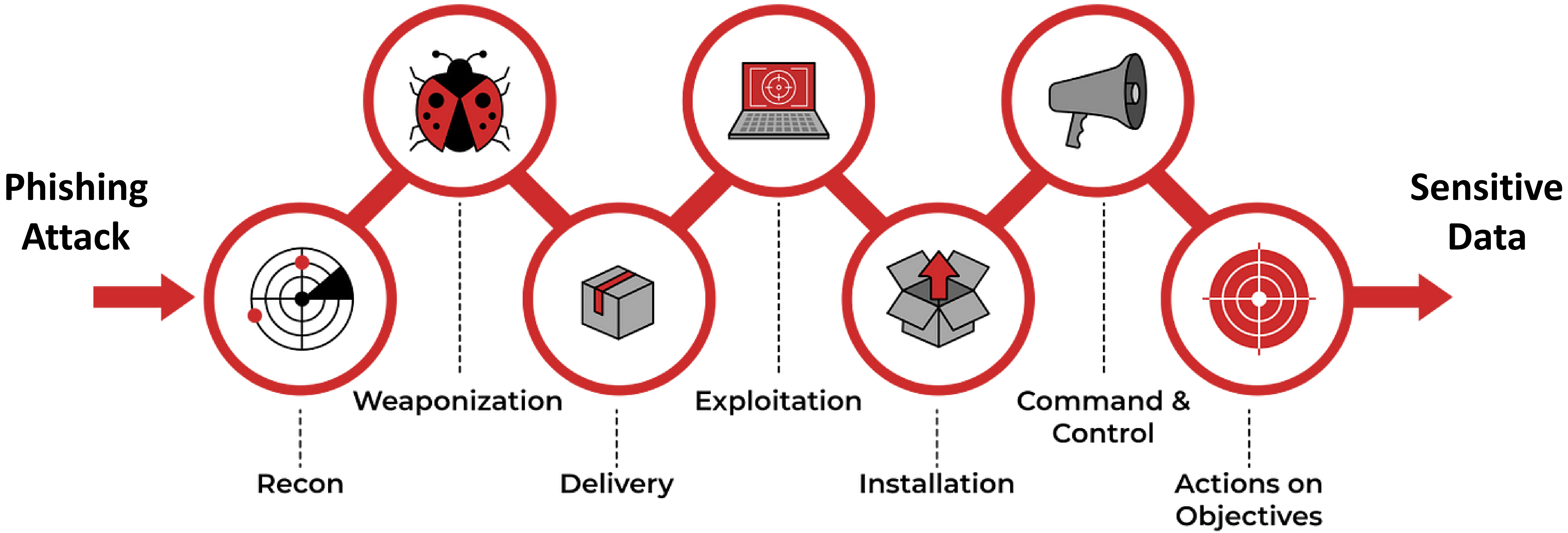
Connecting the dots:

Hint: individuals or groups who engage in malicious activities…

The Cyber Kill Chain

Connecting the dots: Hint: break the chain…

Cyber Kill Chain



Plausible Answer:

- Identifies the stages of an attack
- Enables development of targeted defense strategies for each stage
- Different perspectives from bad actor (e.g., hacker) and defender

Connecting the dots:

Cyber Kill Chain and the OSI Security Architecture can be used together…

How is the OSI Security Architecture useful?

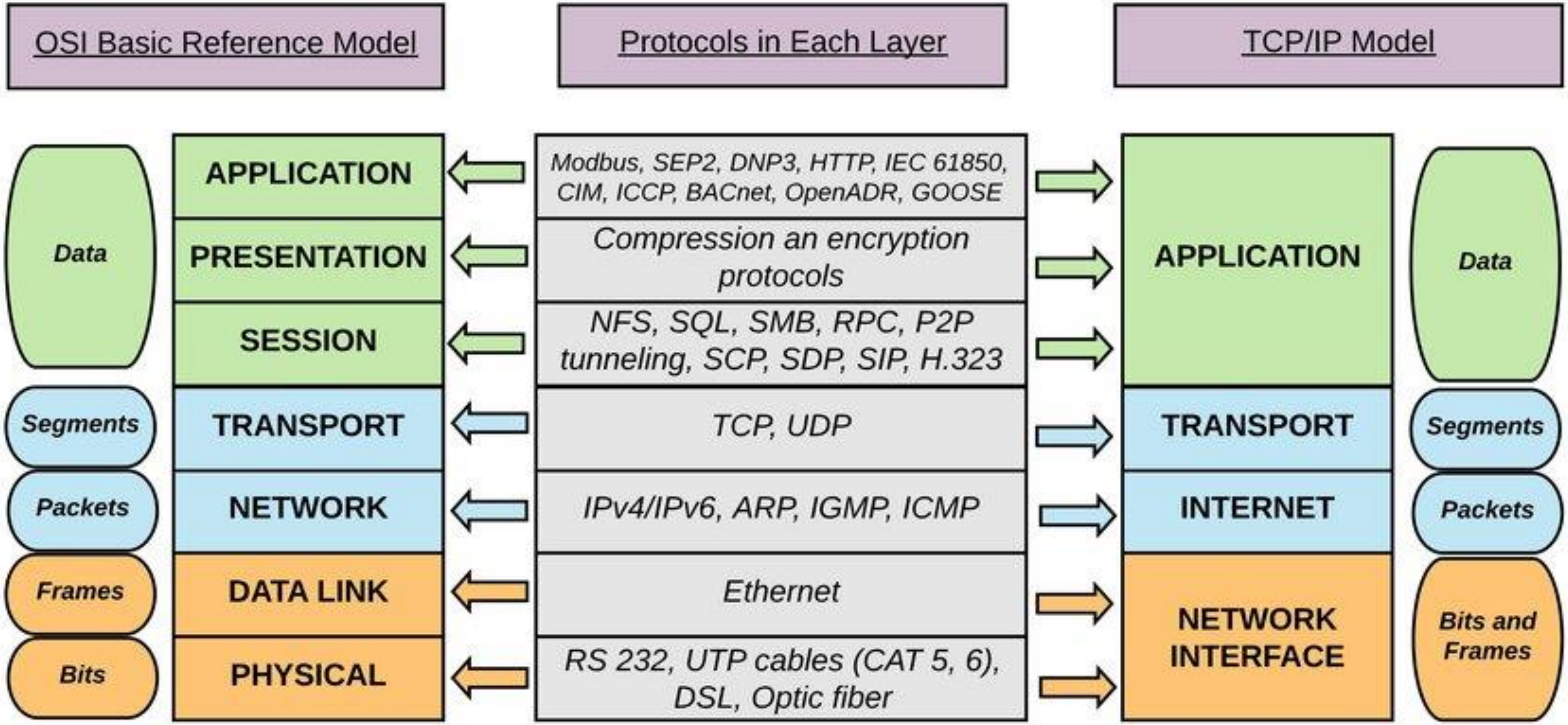
OSI Security Architecture

Connecting the dots:

Hint: pay attention to the layering…

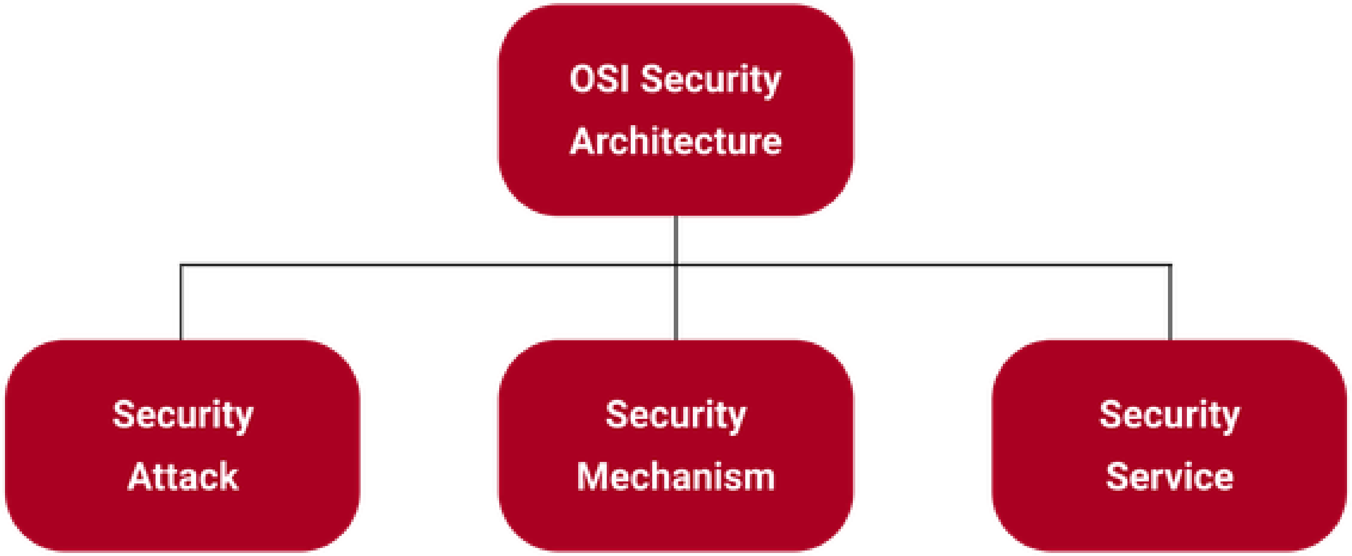
Before we discuss the OSI Security Architecture….

OSI Model and TCP/IP Models



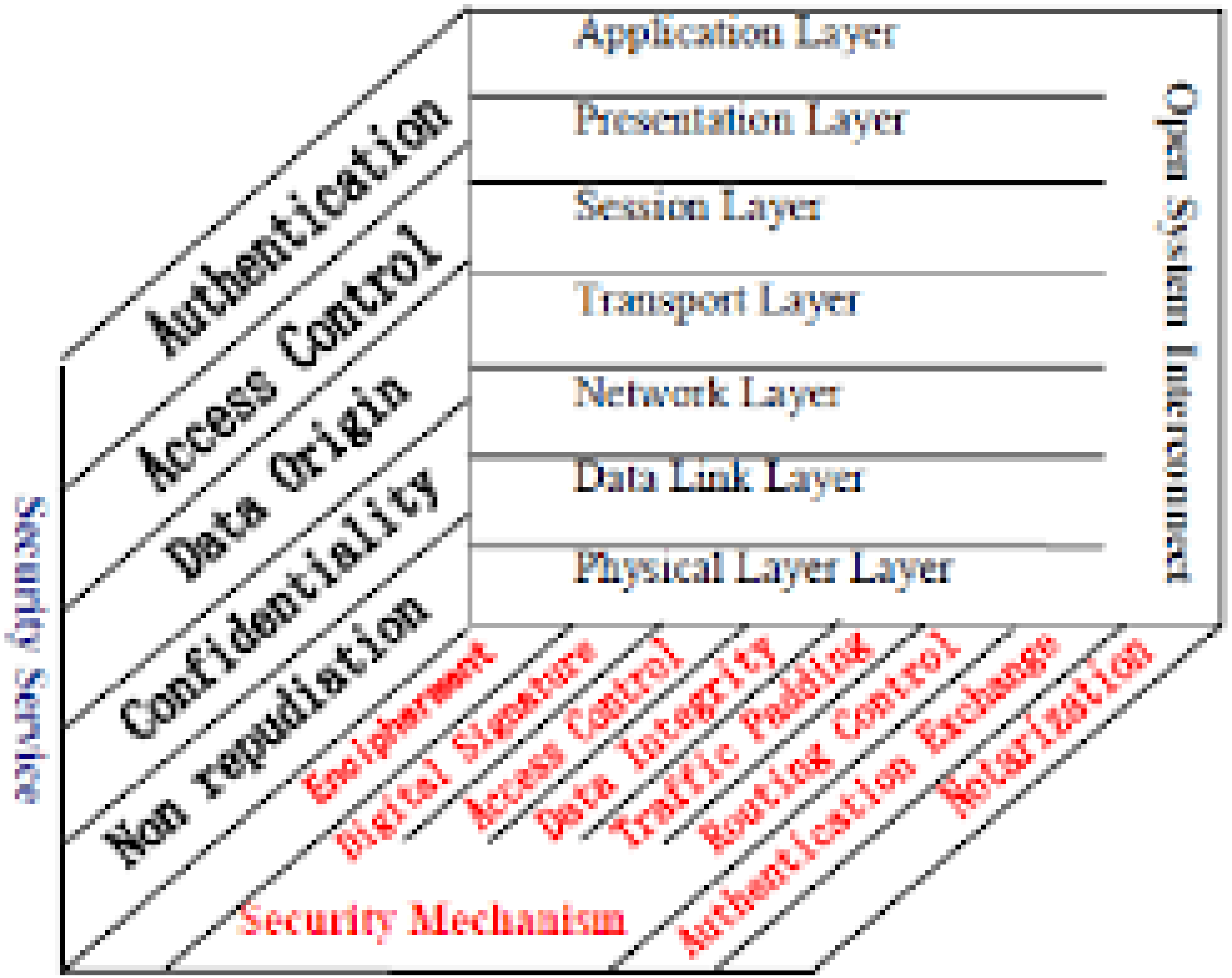
Theoretical

Practical (e.g., Internet)



Component	Examples
Security Attack	• Passive attacks (e.g., eavesdropping, traffic analysis) • Active attacks (e.g., masquerade, replay, modification of messages, denial of service)
Security Mechanism	• AES encryption for data confidentiality • RSA algorithm for digital signatures • Role-Based Access Control (RBAC) • SHA-256 for hashing and integrity checks • Multi-factor authentication (MFA) • Firewalls and Intrusion Detection Systems (IDS) • Virtual Private Networks (VPNs)
Security Service	• Authentication • Access Control • Data Confidentiality • Data Integrity • Non-Repudiation

OSI Security Architecture Example



Cyber Kill Chain	OSI Layer	TCP/IP Layer	Security Service	Security Mechanism	Phishing Attack Example
Reconnaissance	Application	Application	Access Control	Firewalls, IDS/IPS	Research target organization
Weaponization	Application	Application	Integrity	Antivirus, Content Filtering	Create fake login page and malicious email
Delivery	Network/Transport	Internet/Transport	Confidentiality	Encryption, VPN	Send phishing email to target
Exploitation	Application	Application	Authentication	Multi-factor Authentication	Victim enters credentials on fake site
Installation	Application/Presentation	Application	Integrity	File Integrity Monitoring	Download malware (if applicable)
Command & Control	Session/Transport	Transport	Access Control	Network Segmentation	Establish connection with victim's system
Actions on Objectives	Application, Presentation, Session	Application	Non-repudiation	Logging and Auditing	Obtain sensitive data

Plausible Answer:

Provides a framework for implementing security controls at different layers

Helps identify and address vulnerabilities at each layer

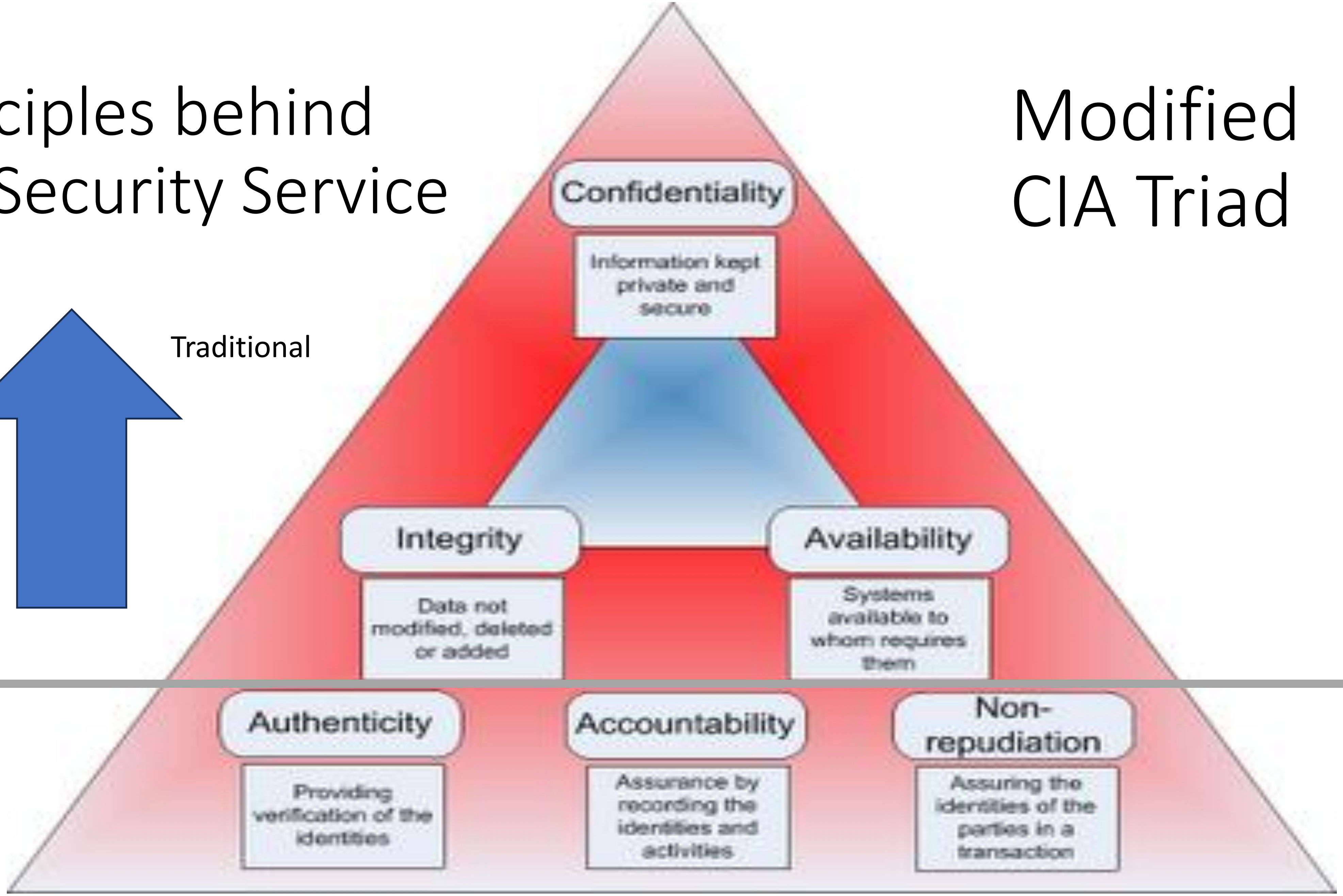
***Connecting the Dots:** OSI and TCP/IP models help map Cyber Kill Chain to layers, improving defense strategies*

What about these security services?

Principles behind the Security Service

Modified CIA Triad

Traditional



Security Service	OSI Model Layer	TCP/IP Model Layer	Examples
Confidentiality	Application (7)	Application	Encryption (e.g., SSL/TLS)
	Presentation (6)	Application	Secure Multipurpose Internet Mail Extensions (S/MIME)
	Session (5)	Transport	Secure Shell (SSH)
	Transport (4)	Transport	Secure Socket Layer (SSL), Transport Layer Security (TLS)
	Network (3)	Internet	IPsec (Internet Protocol Security)
	Data Link (2)	Network Interface	Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP)

- **NIST Definition of Confidentiality:**
- "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information." (NIST SP 800-53 Rev. 5)

Scenario: Confidentiality

Alice and Eve are computer science students working on different projects. Bob is an advisor. {Note: Private and Public Keys == Asymmetric Cryptography Mechanism}

Alice develops a novel algorithm for her thesis. She needs to share it with her advisor, Bob, while keeping it secret from others.

Alice encrypts her algorithm document using Bob's public key before sending it via email.

Bob receives the email and decrypts the document using his private key.

Eve, a curious classmate, intercepts the email but cannot read its contents due to the encryption.

Bob reviews the algorithm and provides feedback to Alice through a secure university portal.

Throughout this process:

- Only Bob can decrypt and read Alice's algorithm
- Eve, despite intercepting the email, cannot access the information

Alice, Bob, Eve, and the Monte Carlo Simulation

How can we make data-driven cybersecurity decisions?

Monte Carlo Simulation Provides…

Proactive approach - estimate the possible outcomes of an uncertain event

Anticipate and mitigate potential threats before they materialize

Cyber risk quantification

Data driven

Ref: https://www.ibm.com/topics/monte-carlo-simulation

Put it all together…

Scenarios (e.g., Alice/Bob/Eve) helps us understand the roles and interactions of the bad actor and defender

Monte Carlo Simulation provides a quantitative way to assess risks and prioritize security efforts at each stage of the Cyber Kill Chain

The use of **Cyber Kill Chain** and **OSI Security Arch**. that can guide us with the implementation of security controls to mitigate risks identified through a Monte Carlo simulation

Stage	Eve's Success Probability	Alice's Detection Probability	Explanation
Reconnaissance	0.8	0.6	Eve scans the organization's network for vulnerabilities. Alice has a 60% chance of detecting the scans.
Weaponization	0.7	0.5	Eve creates malware targeting a vulnerability found in Bob's system. Alice has a 50% chance of detecting the malware creation.
Delivery	0.6	0.7	Eve sends a phishing email to Bob with the malware. Alice has a 70% chance of detecting and blocking the email.
Exploitation	0.5	0.8	If Bob opens the email and clicks the link, the malware exploits the vulnerability. Alice has an 80% chance of detecting the exploitation attempt.
Installation	0.9	0.4	If the exploitation is successful, the malware installs a backdoor on Bob's system. Alice has a 40% chance of detecting the installation.
Command&Control	0.8	0.6	Eve establishes a command-and-control channel to Bob's system. Alice has a 60% chance of detecting the suspicious network traffic.
Actions On Objective	0.7	0.5	Eve uses the backdoor to exfiltrate sensitive data from the organization. Alice has a 50% chance of detecting the data exfiltration attempt.

Theoretical Calculations (Simplified & Rough Estimate)

Overall probability of Eve successfully completing the attack is:

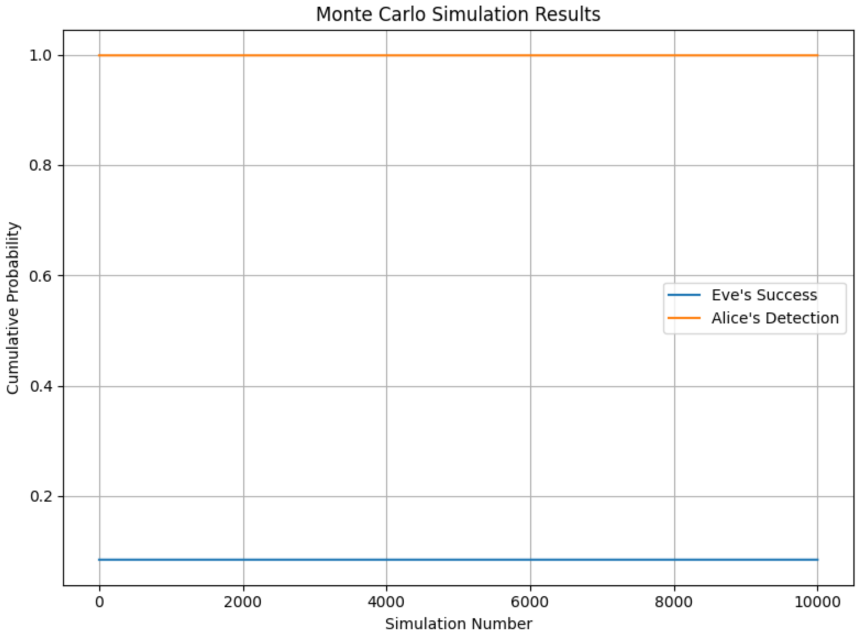
0.8 * 0.7 * 0.6 * 0.5 * 0.9 * 0.8 * 0.7 = 0.127 (12.7%)	Assumes: Each stage is independent, Eve must succeed in all stages for the attack to be successful, & Cyber kill chain not iterative

The overall probability of Alice detecting and stopping the attack at any stage, based on Monte Carlo simulations, is:

1 - (0.4 * 0.5 * 0.3 * 0.2 * 0.6 * 0.4 * 0.5) = 0.996 (99.6%)	Assumes: Alice's failure to detect at each stage is independent, calculates the probability that Alice will detect the attack at least once & Cyber kill chain not iterative

Empirical Results:

https://github.com/ericyoc/monte_carlo_sim_cyber_kill_chain_poc




```
Monte Carlo simulation results (n=10000):
Probability of Eve successfully completing the attack: 8.467%
Probability of Alice detecting and stopping the attack at any stage: 99.856%

Attack Scenario Table:
+----------------------------------+--------------------+------------------------+
| Stage                            | Eve's Success Prob. | Alice's Detection Prob. |
+----------------------------------+--------------------+------------------------+
| Reconnaissance                   |        0.8         |          0.6           |
| Weaponization                    |        0.7         |          0.5           |
| Delivery                         |        0.6         |          0.7           |
| Exploitation                     |        0.5         |          0.8           |
| Installation                     |        0.9         |          0.4           |
| Command & Control                |        0.8         |          0.6           |
| Actions On Objective             |        0.7         |          0.5           |
| Overall Probability (Simulation) |       8.467%       |        99.856%         |
| Overall Probability (Theoretical) |      12.7%        |         99.6%          |
+----------------------------------+--------------------+------------------------+
```

Why They Don't Add to 100%

- The events are not mutually exclusive
- The slight overlap in probabilities (totaling over 100%) is likely due to:
  - Rounding errors in the Monte Carlo simulation
  - Potential edge cases where <u>Eve technically succeeds but Alice also detects it</u>
  - The inherent variability in simulations with 10,000 trials

Plausible Answer:

- Quantifies risks at each stage of the Cyber Kill Chain
- Helps prioritize security efforts based on probabilistic outcomes

Connecting the Dots: Data-driven cybersecurity decisions can be achieved by combining, Cyber Kill Chain, OSI Security Arch., Scenarios, and Monte Carlo Simulation…

Wrap Up

Cyber Kill Chain + OSI Security Arch = Comprehensive Defense

- Kill Chain: Attack Stages
- OSI Security Arch.: Layered Security

Alice/Bob/Eve + Monte Carlo = Informed Decisions

- Roles & Interactions
- Quantitative Risk Assessment
- Probability Estimation of Attack Success and Detection

OSI Security Arch. + Monte Carlo = Guides Security

- Frameworks & Guidelines
- Quantitative Techniques
- Prioritize Security Efforts based on Simulation Results

Cyber Kill Chain + Monte Carlo = Better Resilience

- Understand bad actor Tactics and Techniques
- Adapt Defense Strategies based on Probability Estimates

Any Questions?

Thank you ☺

Appendix

Before We Begin…My Ask of You ☺

- Remove any distraction
- Use your laptop for taking notes only
- Let me know if…
  - I am speaking too fast
  - I need to speak up
  - I need to repeat something previously said
  - You need clarity of a particular word or phrase used
  - I used an acronym that may not be familiar
- Engage

Security Service	OSI Model Layer	TCP/IP Model Layer	Examples
Integrity	Application (7)	Application	Message Authentication Codes (MAC)
	Presentation (6)	Application	Digital signatures
	Session (5)	Transport	Secure Hash Algorithms (SHA)
	Transport (4)	Transport	Transmission Control Protocol (TCP) checksums
	Network (3)	Internet	IPsec (Internet Protocol Security)
	Data Link (2)	Network Interface	Cyclic Redundancy Check (CRC)

NIST Definition of Integrity:
"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity." (NIST SP 800-53 Rev. 5)

Scenario: Integrity

Alice, Bob, and Eve are computer science students collaborating on a group project. {Note: Hash Function == Cryptographic Security Mechanism}

1. Alice creates a project report and calculates its hash value using SHA-256.
2. She sends the report and hash to Bob via email.
3. Bob receives the email and independently calculates the hash of the received report.
4. Bob compares his calculated hash with the one Alice sent. They match, confirming the report's integrity.
5. Eve intercepts the email and attempts to modify the report to include her name as a contributor.
6. When Bob calculates the hash of Eve's modified report, it doesn't match Alice's original hash.
7. Bob alerts Alice to the discrepancy, and they investigate the integrity breach.

Security Service	OSI Model Layer	TCP/IP Model Layer	Examples
Availability	Application (7)	Application	Clustering, load balancing
	Presentation (6)	Application	Redundant hardware components
	Session (5)	Transport	Session failover, session replication
	Transport (4)	Transport	Multipath routing, transport-layer redundancy
	Network (3)	Internet	Dynamic routing protocols (e.g., OSPF, BGP)
	Data Link (2)	Network Interface	Spanning Tree Protocol (STP), link aggregation
	Physical (1)	Network Interface	Redundant power supplies, backup generators

NIST Definition of Availability:

"Ensuring timely and reliable access to and use of information." (NIST SP 800-53 Rev. 5)

Scenario: Availability

Alice, Bob, and Eve are computer science students using a university's online learning platform. {Note: Intrusion Detection System (IDS) == Security Mechanism}

1. Alice uploads her project files to the platform for her team to access.
2. Bob needs to review Alice's work but finds the platform is slow to respond.
3. The university's IT department, anticipating high usage, has implemented load balancing and redundant servers to maintain availability.
4. Despite the high traffic, Bob successfully accesses and reviews Alice's files.
5. Eve, attempting to disrupt the system, launches a Distributed Denial of Service (DDoS) attack on the platform.
6. The university's intrusion detection system identifies the attack, and the IT team activates additional defensive measures.
7. Thanks to these measures, the platform remains operational, allowing Alice and Bob to continue their work uninterrupted.

Security Service	OSI Model Layer	TCP/IP Model Layer	Examples
Authenticity	Application (7)	Application	Digital certificates, digital signatures
	Presentation (6)	Application	Kerberos authentication
	Session (5)	Transport	Secure Remote Password (SRP) protocol
	Transport (4)	Transport	SSL/TLS client authentication
	Network (3)	Internet	IPsec Authentication Header (AH)
	Data Link (2)	Network Interface	IEEE 802.1X port-based authentication

NIST often discusses authenticity in the context of other security concepts, particularly integrity and non-repudiation.

Definition of Authenticity: The property of being genuine and able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.

Scenario: Authenticity

Alice, Bob, and Eve are computer science students participating in an online exam. {Note: Multi-Factor Authentication (MFA) == Security Mechanism}

1. The university uses a secure login system with multi-factor authentication (MFA).
2. Alice logs into the exam platform using her username, password, and a time-based one-time password (TOTP) from her authenticator app.
3. Bob also logs in successfully using his credentials and MFA.
4. Eve attempts to impersonate Alice by using Alice's stolen username and password.
5. However, Eve fails to provide the correct TOTP, and the system denies access.
6. The exam platform uses digital certificates to prove its authenticity to students.
7. Alice and Bob verify the platform's certificate before proceeding with the exam.

Security Service	OSI Model Layer	TCP/IP Model Layer	Examples
Accountability	Application (7)	Application	Audit logging, access logs
	Presentation (6)	Application	Event monitoring, log analysis
	Session (5)	Transport	Session tracking, session auditing
	Transport (4)	Transport	Connection logging, traffic analysis
	Network (3)	Internet	Network flow monitoring, NetFlow
	Data Link (2)	Network Interface	Switch port monitoring, SNMP traps

NIST-related Definition of Accountability:
The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. (Derived from NIST SP 800-53 Rev. 5)

Scenario: Accountability

Alice, Bob, and Eve are computer science students with access to a shared university research database. {Note: Logging == Security Mechanism}

1. The university implements a robust logging system that records all database accesses and actions.
2. Alice accesses the database to retrieve data for her project, and her actions are logged.
3. Bob modifies some shared research data and the system logs his changes.
4. Eve attempts to delete some critical data but is stopped by access controls. This attempt is also logged.
5. Later, a discrepancy is found in the research data.
6. The university's IT security team investigates by reviewing the logs.
7. They can trace the modification back to Bob's account and the deletion attempt to Eve's account.

Security Service	OSI Model Layer	TCP/IP Model Layer	Examples
Non-repudiation	Application (7)	Application	Digital signatures, timestamps
	Presentation (6)	Application	Digitally signed documents
	Session (5)	Transport	Secure session logging
	Transport (4)	Transport	SSL/TLS session resumption with session IDs
	Network (3)	Internet	IPsec Encapsulating Security Payload (ESP) with sequence numbers
	Data Link (2)	Network Interface	802.1AE MACsec with secure channeling

NIST Definition of Non-Repudiation: "Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information." (NIST SP 800-53 Rev. 5)

Scenario: Non-Repudiation

Alice, Bob, and Eve are computer science undergraduates learning about cybersecurity. {Note: Digital signature == cryptographic mechanism}

1. Alice submits a group project report to Professor Bob via the university's secure portal, which uses digital signatures.
2. Alice receives a digitally signed receipt confirming her submission.
3. Two weeks later, Bob claims he never received the report.
4. Alice presents her digital receipt as proof of submission.
5. The IT department verifies:
   - The authenticity of Alice's receipt using the system's public key
   - The portal's logs showing the report's submission and Bob's download
6. This demonstrates non-repudiation:
   - Alice can't deny submitting the report
   - Bob can't claim he didn't receive it
7. Eve, another student, attempts to interfere by hacking the system, but fails due to the robust digital signature mechanism.