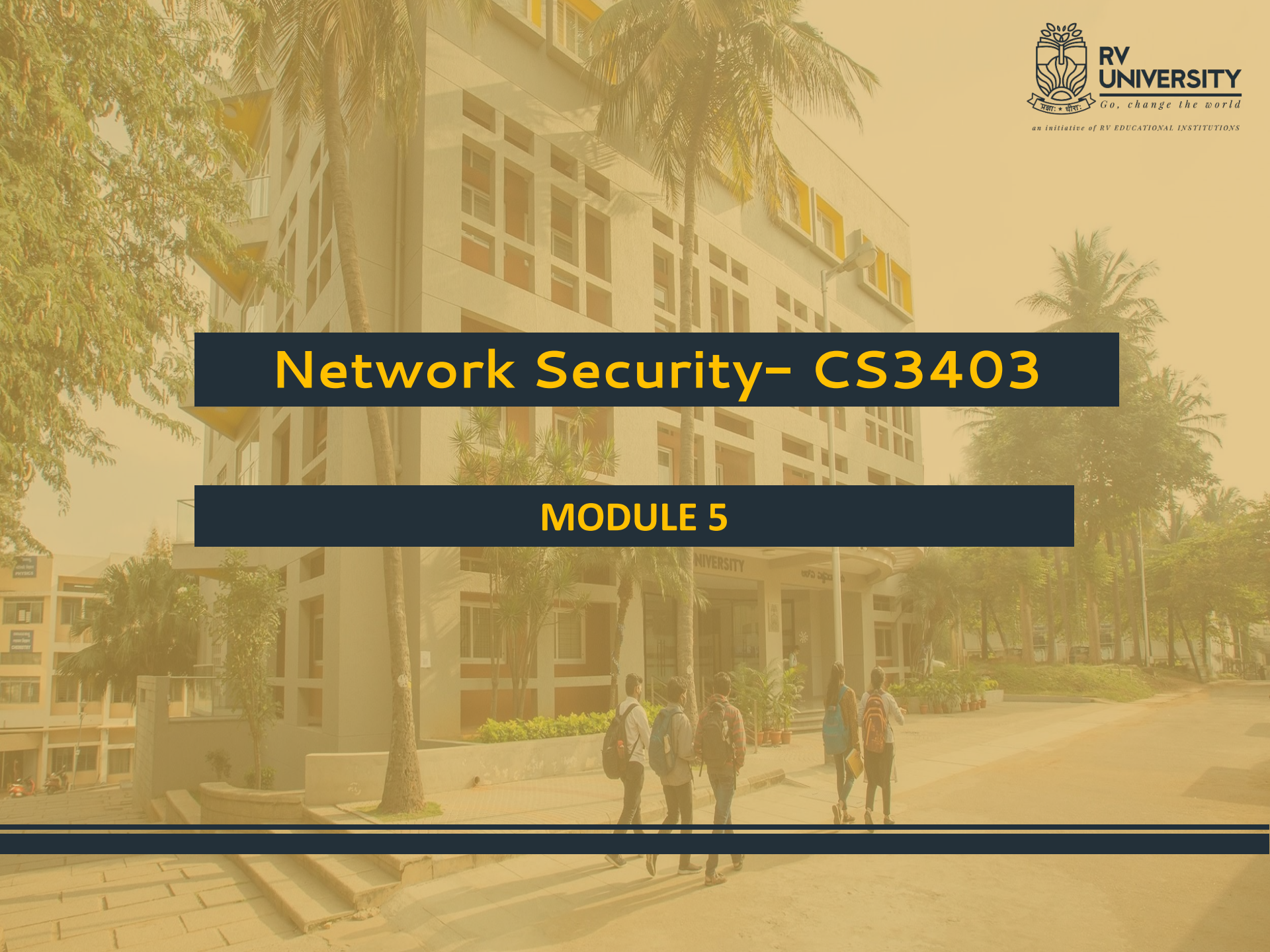


RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

Network Security- CS3403

MODULE 5

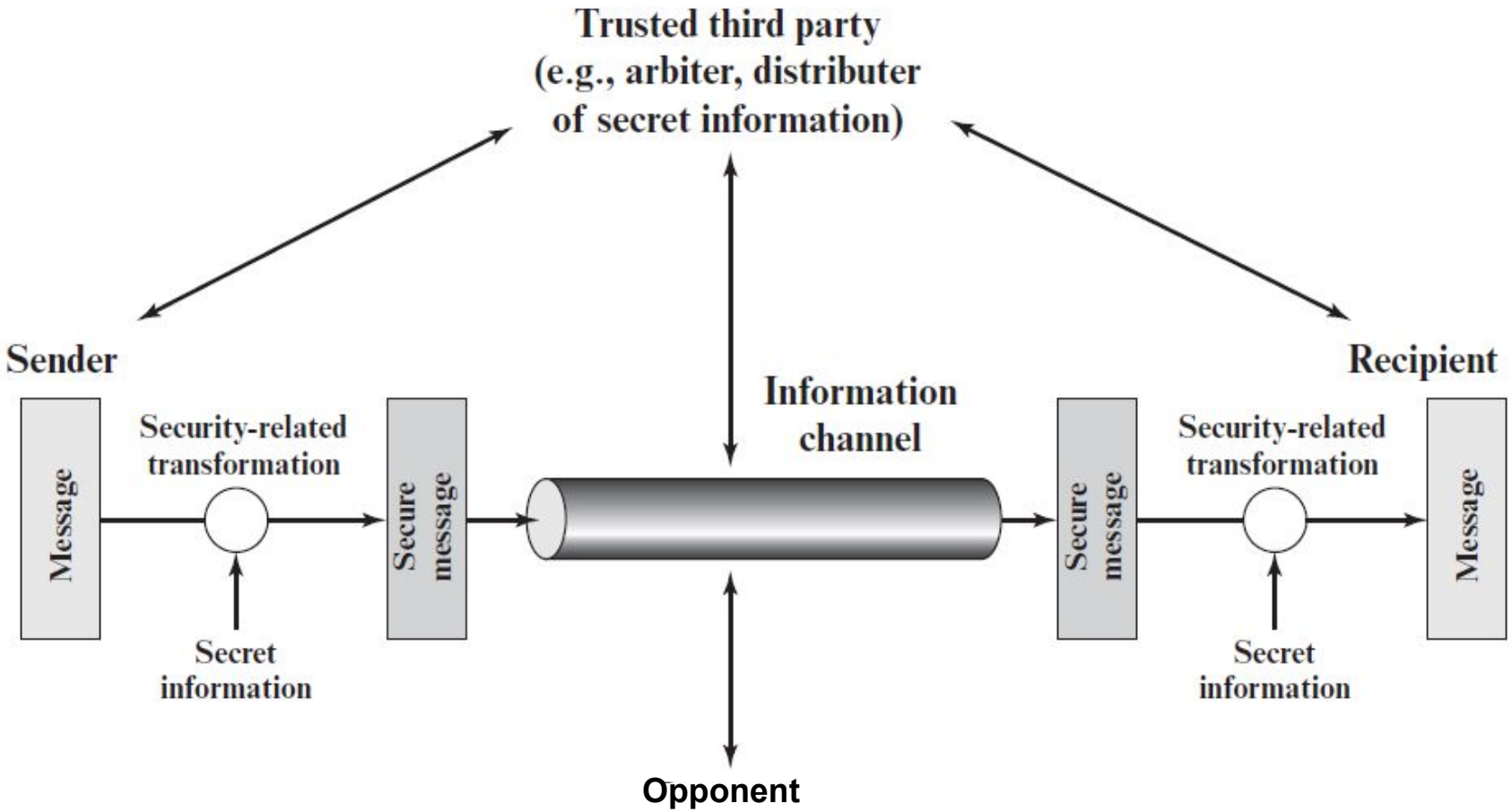
Network Security- CS3403

MODULE 5

Network Security

Network security is a set of policies, procedures, and technologies that
protect networks from unauthorized access, misuse, and data loss.
It includes hardware and software components.

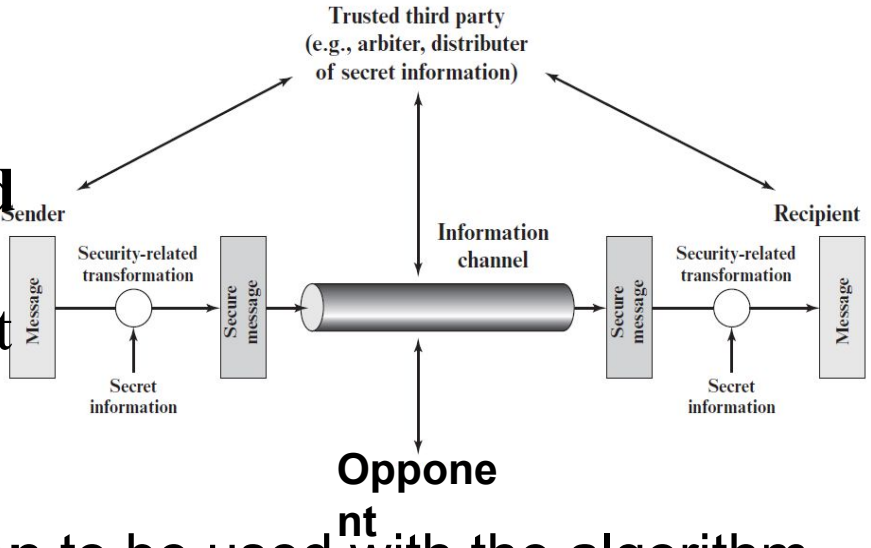
Network Security Model



Network Security Model: Explained

- There are **four basic tasks** to implement a **security service**

1. Design an **algorithm** for performing the **security-related transformation**. The algorithm should be such that an opponent cannot defeat its purpose. (encryption algorithms)



2. Generate the **secret information** to be used with the algorithm. (keys)
3. Develop methods for the **distribution and sharing** of the secret information. (key exchange protocol)
4. Specify a **protocol** to be used by the two principals that make use of the security algorithm and the secret information to achieve a particular security service. (TLS: Transport Layer Security)

Network Security Protocols

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

- **IPsec** (Internet Protocol Security): Secures IP traffic with encryption and authentication; widely used in VPNs.
- **TLS/SSL** (Transport Layer Security / Secure Sockets Layer): Ensures encrypted and authenticated communication over the Internet (in HTTPS).
- **HTTPS** (Hypertext Transfer Protocol Secure): Secure version of HTTP using TLS; protects web traffic like login and payment data.
- **SSH** (Secure Shell): Encrypts remote terminal sessions; used for secure login and remote command execution.
- **WPA2/WPA3** (Wi-Fi Protected Access): Secures wireless networks; WPA3 offers stronger encryption and better brute-force protection.
- **Kerberos**: Ticket-based authentication protocol; used in enterprise networks for secure user identity verification.
- **S/MIME** and **PGP**: Secure email protocols that provide encryption and digital signatures for email privacy and authenticity.

S/MIME: Secure/Multipurpose Internet Mail Extensions
PGP: Pretty Good Privacy

S/MIME, PGP and Kerberos

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

- **S/MIME**: Secure/Multipurpose Internet Mail Extensions, for business emails.
- **PGP**: Pretty Good Privacy: The sender uses their private key to encrypt the data.
- The recipient uses the sender's public key to decrypt the data
- **Kerberos**: **Single Sign-on**, providing **tickets** to users logging in. Uses **secret-key** crypto

IP Security (IPSec)

IPSec: An Introduction

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

- Enterprises can run a secure, private IP network by disallowing links to untrusted sites.
- IPSec encrypts IP packets that leave the premises, and authenticating packets that enter the premises.
  - It ensures secure networking not only for applications that are aware of security mechanisms but also for the many security-ignorant applications.
- It encompasses **three functional areas**:
  1. The **authentication** mechanism assures that a received packet was, in fact, transmitted by the party identified as the source in the packet header.

     Note: In addition, this mechanism assures that the packet has not been altered in transit.
  2. The **confidentiality** facility enables communicating nodes to encrypt messages to prevent eavesdropping by third parties during transit.
  3. The **key management** facility is concerned with the secure exchange of keys between the sender and receiver.

Use cases of IPSec

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

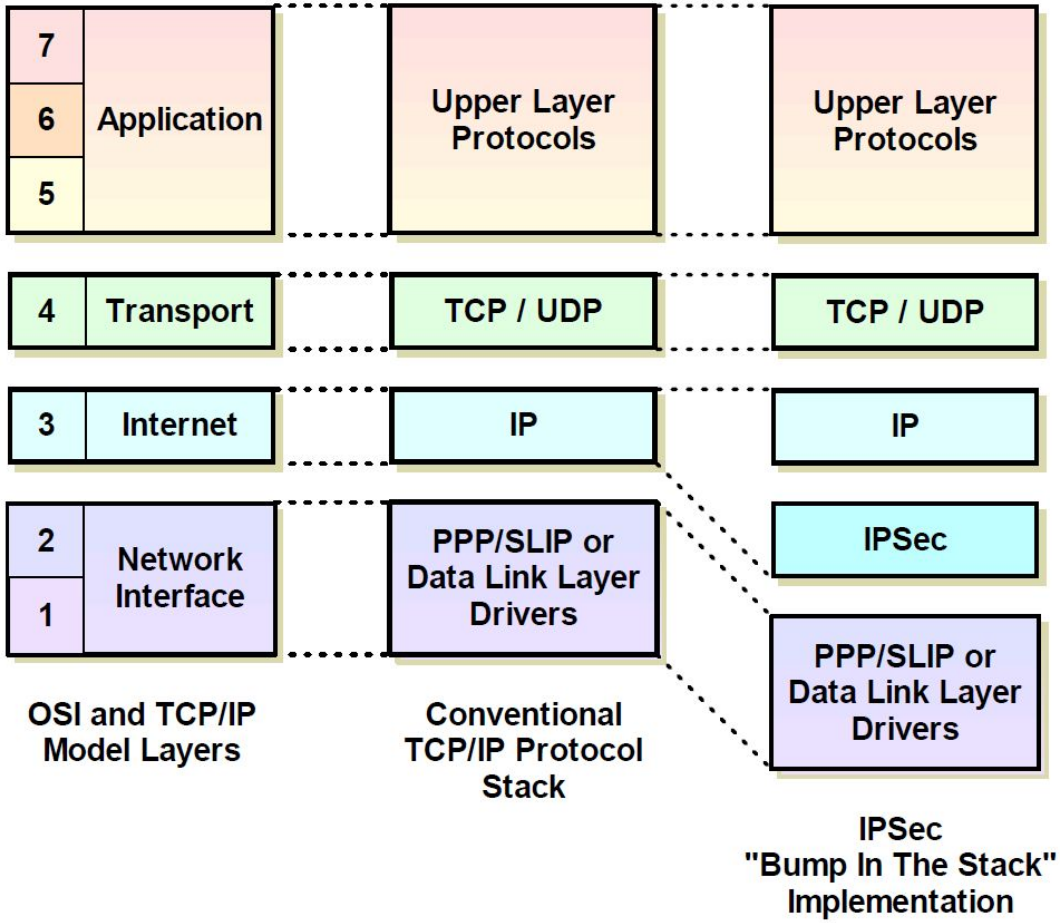
- IPSec can **encrypt** and/or **authenticate** all traffic at the IP level
- It provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet.
- Enterprises can build a secure Virtual Private Network over the Internet or over a public WAN to have secure connectivity between different branches of the enterprise using the Internet.
- An end user whose system is equipped with IP security protocols can make a local call to an Internet Service Provider (ISP) and gain secure access to a company network.
- It can be used to have a secure communication with other organizations.
- Even though some Web and electronic commerce applications have built-in security protocols, the use of IPsec enhances that security.

IPSec Protocols and Components

IPSec Implementation: 1. BITS

BITS: Bump In The Stack

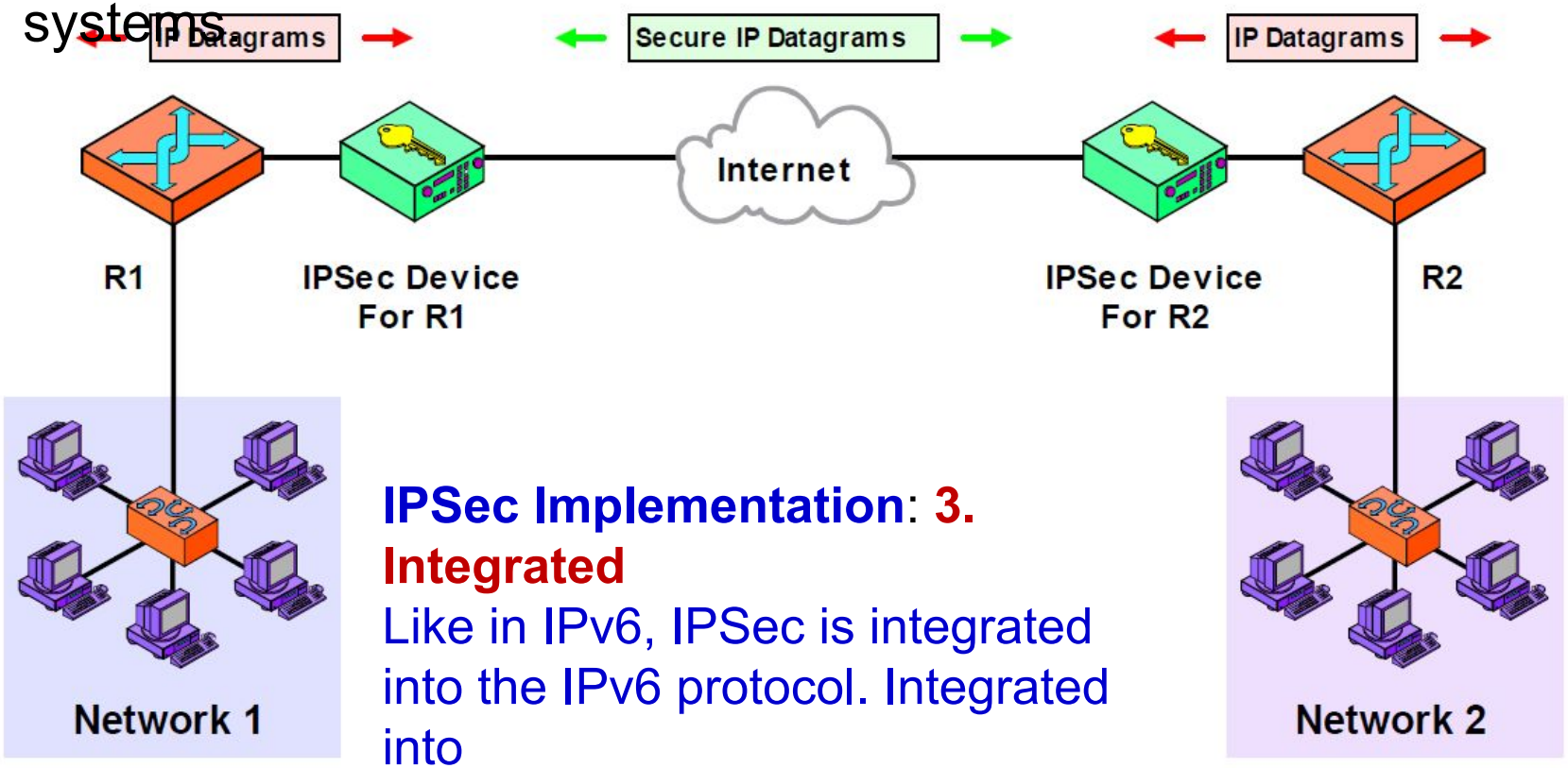
IPSec is integrated within the host's network stack, enabling end-to-end protection directly from the host itself.



IPSec Implementation: 2. BITW

BITS: Bump In The Wire

IPSec is implemented in an external hardware device placed between
the host and the network, requiring no changes to host systems.

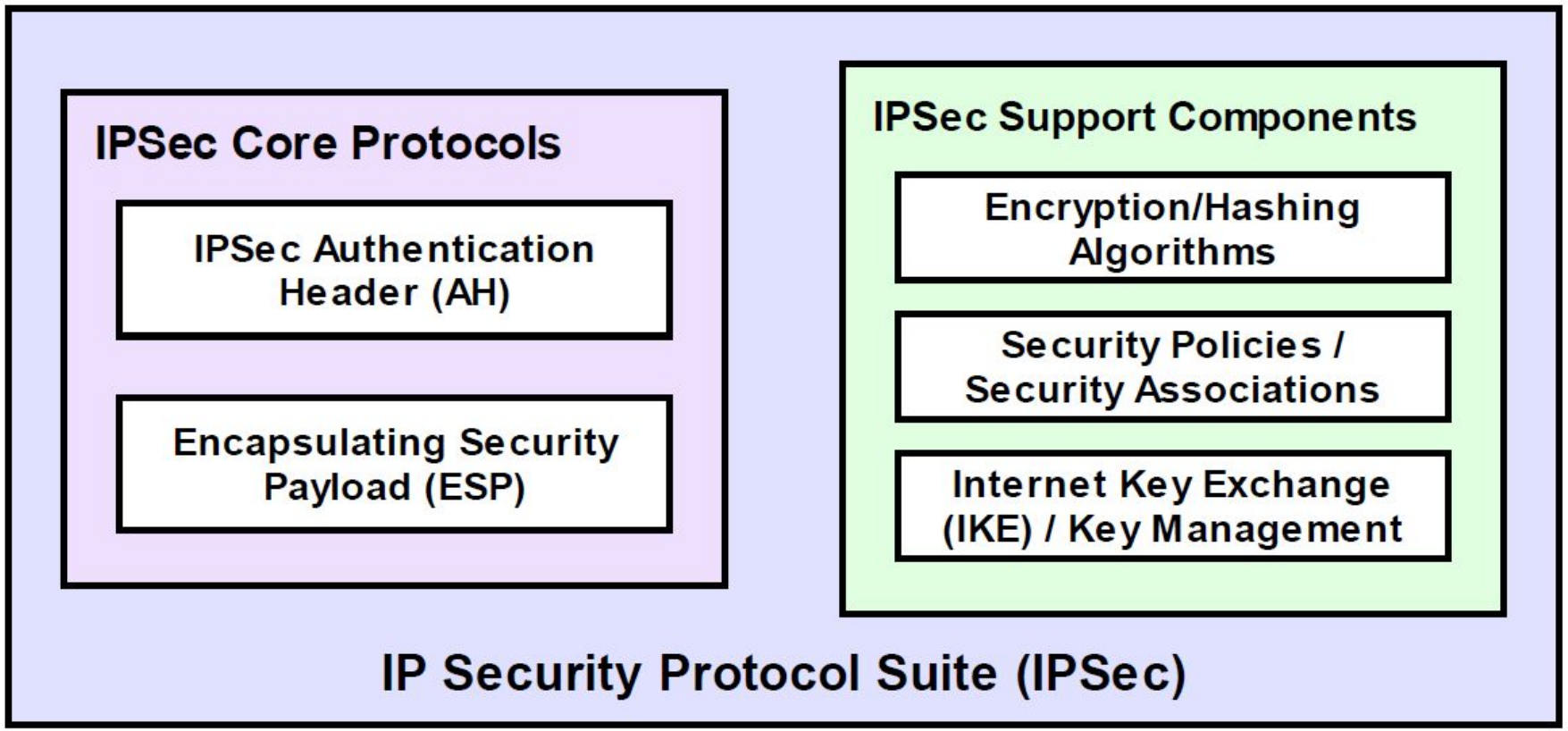


IPSec Implementation: **3. Integrated**

Like in IPv6, IPSec is integrated into the IPv6 protocol. Integrated into
the OS, network devices. Transparent

Modes of IPSec, AH and ESP

IPSec Protocols and Components



AH: For Authentication
ESP: For Integrity

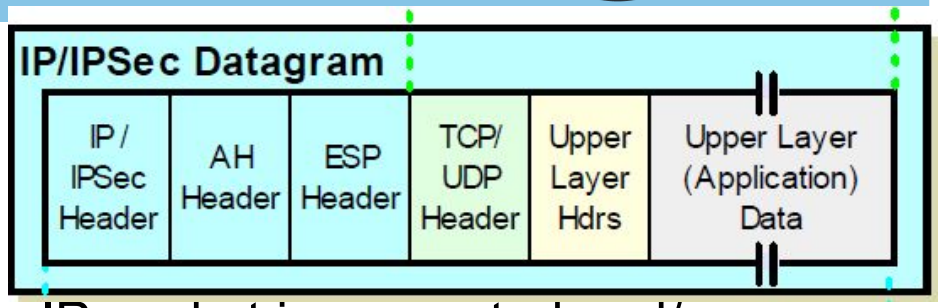
IPSec Protocols and Components: Explained

- **Authentication Header** (**AH**): Provides **authentication** and **integrity** for IP packets but does not encrypt the payload.
- **Encapsulating Security Payload** (**ESP**): Provides encryption, authentication, and integrity, securing both payload and optional header fields.
- **Security Association** (**SA**): A unidirectional logical connection that defines the security parameters (algorithms, keys) used in IPsec communication.
- **Internet Key Exchange** (**IKE**): Handles automated negotiation of security associations (SAs) and key management for IPSec.
- **Security Policy Database** (**SPD**): Contains rules and policies that determine which traffic should be protected by IPsec.
- **Security Association Database** (**SAD**): Stores active security associations, including encryption/authentication keys and algorithms

Modes of IPSec

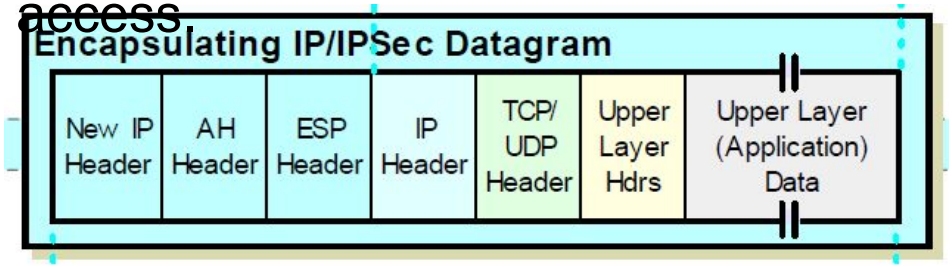
RV UNIVERSITY
Go, change the world

1. **Transport Mode:**



- Secures end-to-end communication between two hosts (client ↔ server)
- Only the payload (data part) of the IP packet is encrypted and/or authenticated.
- The original IP header is left intact.
- **Example**: SSH, Telnet, or remote access.

2. **Tunnel Mode:**



- Secures network-to-network or host-to-network communication (e.g., via VPNs).
- Entire IP packet (header + payload) is encapsulated inside a new IP packet.
- A new outer IP header is added for routing.
- **Example**: A branch office connecting securely to headquarters via VPN

AH: Authentication Header **ESP**: Encapsulating Security Payload

Authentication Header (AH) : Explained

- AH provides **data integrity**, **origin authentication**, and **optional anti-replay protection** for IP packets — but **does not provide encryption**.
- **AH** calculates a **cryptographic hash** over the **IP header fields** and its **payload** and inserts the **resulting hash** into the AH header.
  - It uses a special hashing algorithm and a specific key known only to the source and destination.
  - SA between the source and destination specifies these particulars, so they know how to perform these operations but no one else can.
- The receiver **recalculates the hash** and compares it to the one received to verify **authenticity** and **integrity**.
- The presence of AH header allows **verification of integrity** of the message, but doesn't encrypt it.
- **AH provides authentication but not privacy!! (that's what ESP is for)**
- AH is normally not used because of its incompatibility with NAT.

Resulting Hash: Integrity Check Value (ICV)

Encapsulating Security Payload (ESP) : Explained

- ESP uses **encryption algorithm** and a **key** to transform the datagram into an encrypted form, so that privacy of IP datagram in transit is achieved.
- Since some encryption algorithms only work on **fixed block size of data**, **there is a need** to perform **padding** of IP datagram before encryption
- Apart from the **ESP header**, **ESP trailer** is also required here to take care of padded data for encryption
- The receiver performs decryption of the received data (including the ESP trailer, based on the algorithm) to get the original data back.
- To make sure that the encrypted data is not tampered with while in transit, there is an additional **ESP Authentication Data** field is also added.

Integrity Check Value (ICV)

  - This field is used when the ESP's optional authentication feature is employed.
  - It is similar to the ICV used by AH

IPSec: Summary of Features

1. Features of IPSec

- **Authentication**: IPSec provides authentication of IP packets using digital signatures or shared secrets. This helps ensure that the packets are not tampered with or forged.
- **Confidentiality**: IPSec provides confidentiality by encrypting IP packets, preventing eavesdropping on the network traffic.
- **Integrity**: IPSec provides integrity by ensuring that IP packets have not been modified or corrupted during transmission.
- **Key management**: IPSec provides key management services, including key exchange and key revocation, to ensure that cryptographic keys are securely managed.

2. Features of IPSec

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

- **Tunneling**: IPSec supports tunneling, allowing IP packets to be encapsulated within another protocol, such as GRE (Generic Routing Encapsulation) or L2TP (Layer 2 Tunneling Protocol).
- **Flexibility**: IPSec can be configured to provide security for a wide range of network topologies, including point-to-point, site-to-site, and remote access connections.
- **Interoperability**: IPSec is an open standard protocol, which means that it is supported by a wide range of vendors and can be used in heterogeneous environments.

IPSec: Quiz 1 to 5

Quiz 1: IPSec: AH

- Which of the following security services is not provided by IPsec's Authentication Header (AH)? **ANS: B**

A. Data Integrity
B. Data Confidentiality
C. Source Authentication
D. None of the above options is correct

Note:
AH provides integrity, authentication, and optional anti-replay protection.
It does not encrypt the data, so it does not provide confidentiality.

Quiz 2: IPSec: ESP

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

- Which of the following statements about IPsec **ESP** (Encapsulating Security Payload) is true when used with authentication?

A. ESP can provide encryption, but authentication must be done using AH

B. ESP provides confidentiality, but cannot verify data integrity

C. ESP can provide both encryption and integrity if configured with authentication

D. ESP encrypts only the IP header, not the payload.

ANS: C

Note:
ESP supports encryption (confidentiality) and optional integrity/authentication.
When authentication is enabled, ESP can secure both confidentiality
and integrity without needing AH.

Quiz 3: IPSec Modes

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

- In which IPsec mode is the original IP header encrypted along with the payload?

A. Transport mode
B. Tunnel mode
C. Gateway mode.
D. AH Mode

ANS: B

Note:
In **Tunnel Mode**, the entire original IP packet (header + payload) is encrypted and placed inside a new IP packet.
In **Transport Mode**, only the payload is encrypted; the IP header is left intact.

Quiz 4: IPSec Protocols

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

- Which protocol is responsible for negotiating and establishing Security Associations (SAs) in IPsec?

A. ESP
B. AH
C. IKE
D. SSL

ANS: C

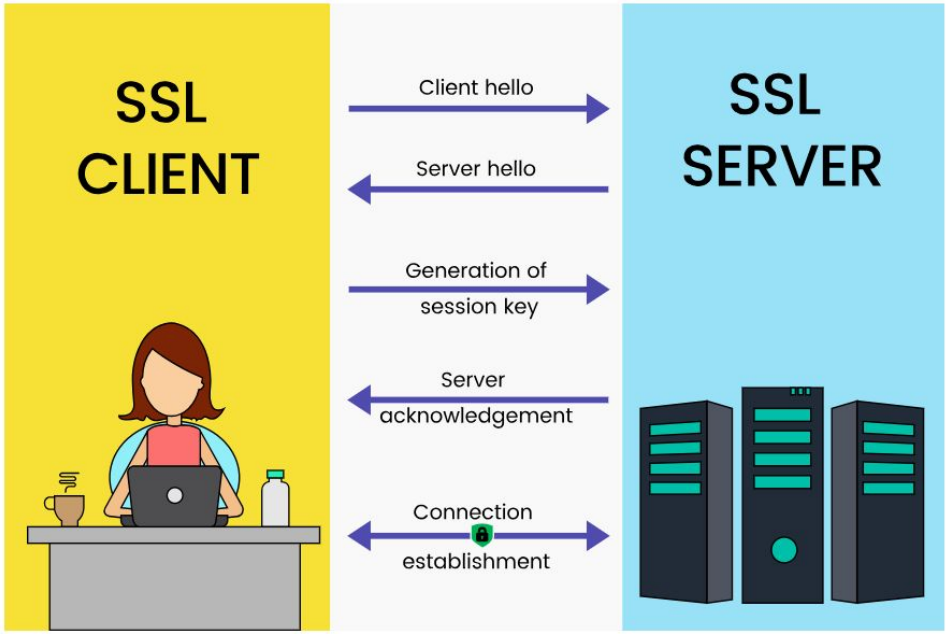
Note:
IKE is the protocol used to automate the negotiation of cryptographic keys and policies in IPsec.
ESP and AH are used to protect traffic after SAs are established.

Introduction to SSL/TLS

SSL/TLS: Introduction

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

- **SSL** (Secure Sockets Layer) is a **cryptographic protocol** designed to provide secure communication over a computer network.
- Developed originally by Netscape in the mid-1990s.



- It ensures that data sent between a client (like a web browser) and a server (like a website) is encrypted, authenticated, and protected against tampering.
- SSL has now evolved into **TLS** (Transport Layer Security) — TLS 1.0 was based on SSL 3.0 — but people still often use "SSL" informally to refer to both.

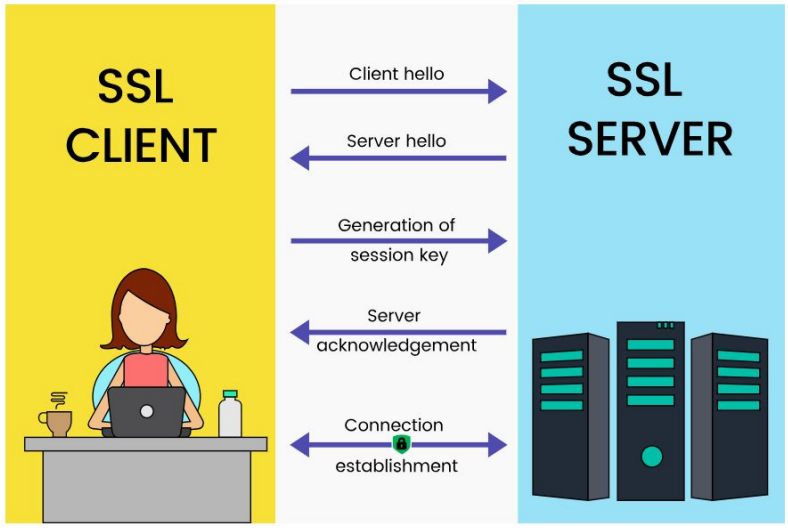
SSL/TLS: Salient Features

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

Feature	Explanation
Confidentiality	SSL encrypts the data so that it cannot be read by anyone except the intended recipient.
Integrity	SSL ensures that data has not been altered in transit using MACs (Message Authentication Codes).
Authentication	SSL allows the client to verify the server's identity using **digital certificates** (server authentication).
Optional Client Authentication	SSL can also optionally authenticate clients, though usually only servers are authenticated.
Session Keys	SSL uses **public key cryptography** to exchange a **symmetric session key** for faster encrypted communication.
Negotiation of Cipher Suites	SSL allows the client and server to agree on which encryption algorithms to use.
Forward Secrecy (optional)	Modern implementations (TLS 1.2+) can use ephemeral keys to ensure session keys are not compromised even if the private key is.

SSL: Handshake

- **Client Hello**: Client sends supported SSL/TLS versions, list of supported cipher suites, and a random number.
- **Server Hello**: Server responds with selected cipher suite, its digital certificate (public key), and its own random number.



- **Server Certificate Verification**: Client verifies the server's digital certificate using trusted Certificate Authorities (CAs).
- **Key Exchange**: Client generates a pre-master secret, encrypts it with the server's public key, and sends it to the server.
- Both client and server derive the same session keys from the pre-master secret and random numbers.
- **Finished Messages**: Both sides confirm that future communication will be encrypted using the newly established session key.

SSL/TLS: Data Communication

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

- The session key (symmetric key) is now used for encrypting all the subsequent data between client and server.
- Symmetric encryption is faster than public-key encryption, hence session keys are preferred for ongoing data transfer.

SSL/TLS: Applications

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

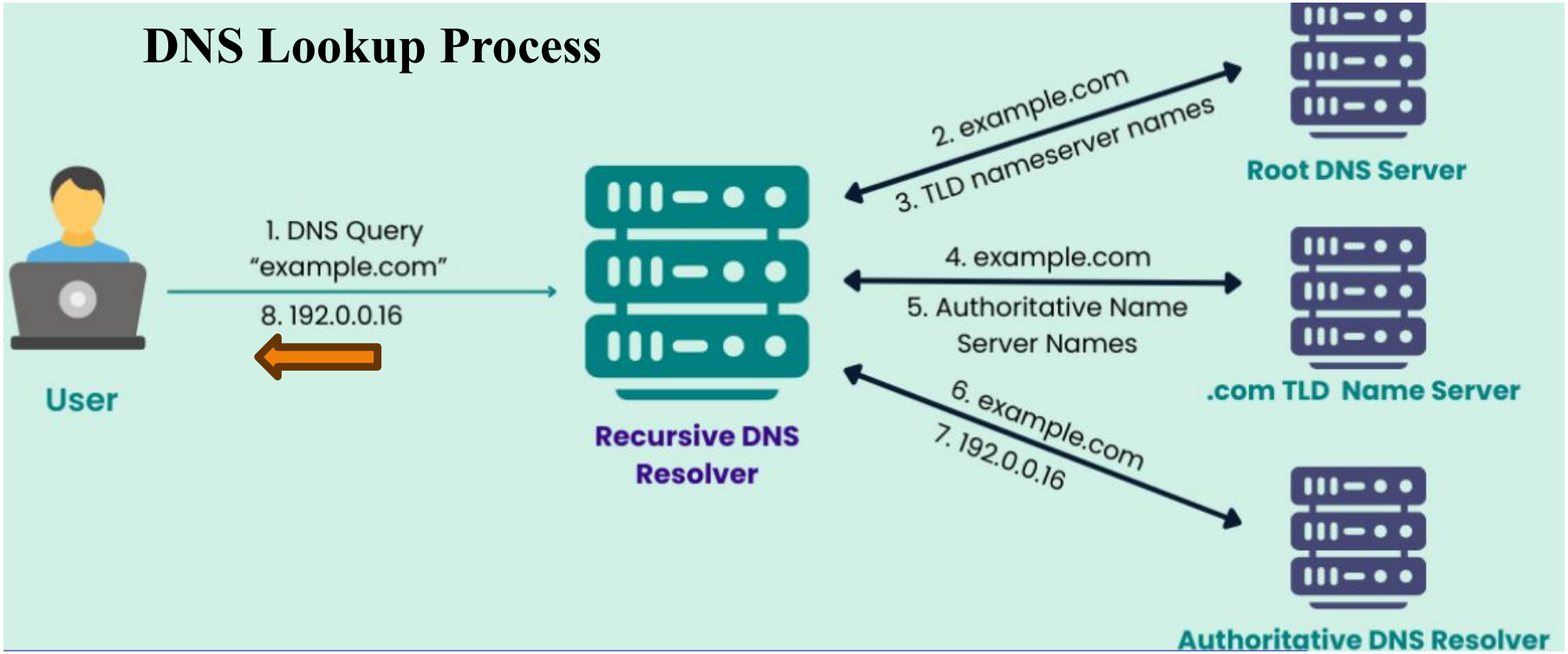
Application	Use of SSL
Web Browsing (HTTPS)	SSL secures HTTP connections to websites.
Email	SSL/TLS used to secure SMTP (sending), IMAP/POP3 (retrieving emails).
VPNs	SSL VPNs secure remote access over public networks.
Online Banking and Payments	SSL protects sensitive financial data.
Instant Messaging and VOIP	SSL can encrypt chat messages and voice calls.
E-commerce Transactions	SSL protects credit card information during online purchases.
Software Updates	SSL secures the download of software patches to prevent tampering.

DNS Introduction

DNS: Domain Name Server

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

- DNS is the behind-the-scenes service that makes it possible to browse the web by converting human-friendly domain names into IP addresses that computers can understand.



DNS Query Resolution

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

- **Client Interaction**: When a domain name (e.g. www.example.com) is entered into a browser, the request is first sent to the **recursive resolver**.
- This is typically provided by the Internet Service Provider (ISP) or a public DNS resolver like Google's Public DNS (8.8.8.8).
- **Recursive Queries**: If the resolver doesn't have the answer to the query stored, it performs recursive queries, contacting other DNS servers in the hierarchy (Root, TLD, and Authoritative) on behalf of the client to find the correct IP address for the domain.
- **DNS Caching**: To improve efficiency and reduce lookup times, the recursive resolver stores the results of DNS queries in a cache for a period of time.
- This allows future requests for the same domain to be resolved more quickly.

DNS Security

DNS Security

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

- The original DNS was not designed with security in mind.
- It trusts that all responses it receives are legitimate.
- This makes it vulnerable to attacks such as:
- **DNS Spoofing** (forging responses)
- **Cache Poisoning** (injecting false entries into a resolver's cache)
- **Man-in-the-Middle (MITM) attacks**
- Thus, securing DNS is vital for maintaining the integrity and trustworthiness of Internet communications

DNS Security: Requirements

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

Requirement	Description
Authentication of DNS Responses	Clients must be able to verify that the response they receive matches the response intended by the domain owner.
Protection of Zone Data	DNS zones must be securely managed and cryptographically signed to prevent tampering.
Key Management	Proper handling of cryptographic keys (generation, storage, rollover, revocation) is necessary to maintain security.
Chain of Trust	Validation must extend up the DNS hierarchy — from root, to top-level domain (TLD), to domain.
Resilience to Replay Attacks	Signed responses must include mechanisms like nonces or timestamps to prevent attackers from replaying old responses.
Availability and Performance	Security mechanisms should not significantly degrade the performance of DNS resolution.
Operational Simplicity	The system must allow for relatively easy deployment and management by operators (e.g., auto-signing zones).

DNS Security: Key Features

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

Feature	Description
Data Integrity	Ensures that the DNS responses have not been tampered with.
Authentication of Source	Verifies that DNS data comes from the authoritative source (not a fake server).
Protection Against Spoofing and Poisoning	Prevents attackers from injecting fake DNS data into a resolver's cache.
Cryptographic Assurance	Uses digital signatures to validate DNS information.
Backward Compatibility	Secure extensions (like DNSSEC) work alongside traditional DNS systems where possible.
Minimal Confidentiality	DNS traditionally does not encrypt queries; however, newer extensions like **DoT** (DNS over TLS) and **DoH** (DNS over HTTPS) provide confidentiality for DNS queries.

DNS Security: Benefits

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

- **Prevents redirection to malicious websites** (e.g., phishing, malware sites).
- **Strengthens Internet trustworthiness** by ensuring domain-to-IP mappings are correct.
- **Hardens critical infrastructure** (especially important for enterprises, ISPs, and governments).
- **Supports secure email delivery** (DNSSEC supports secure email via technologies like DANE).

DANE (DNS-based Authentication of Named Entities) is a DNS security protocol that binds digital certificates to domain names using DNSSEC

Cloud Security

Cloud Security: Introduction

- **Cloud computing** allows on-demand access to computing resources like servers, storage, and applications over the Internet.
- However, moving to the cloud introduces new security challenges — like shared environments, multi-tenancy, remote access, and outsourced management.
- **Cloud Security** refers to the technologies, policies, controls, and procedures used to protect cloud-based systems, data, and infrastructure.

Cloud Security: Requirements

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

Requirement	Description
Data Confidentiality, Integrity, and Availability (CIA Triad)	Protect cloud data from unauthorized access, tampering, and ensure it is available when needed.
Secure Access Controls	Implement strong authentication (MFA), role-based access control (RBAC), and least privilege principles.
Encryption Mechanisms	Use strong encryption for data at rest, in transit, and optionally during processing (homomorphic encryption).
Shared Responsibility Model	Understand that security responsibilities are split between the **cloud provider** and the **cloud customer**.
Security Configuration Management	Secure setup of virtual machines, storage, databases, containers, and networking components.
Auditability and Logging	Maintain logs of user activities, system changes, and security events for accountability and investigations.
Vulnerability Management	Regularly scan and patch systems to fix known security vulnerabilities.

Cloud Security: Key Features

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

Feature	Explanation
Data Protection	Data at rest, in transit, and in use must be encrypted and securely handled.
Access Control and Identity Management	Only authorized users and systems should have access to cloud resources (IAM, MFA).
Network Security	Protect cloud networks against intrusion, DDoS attacks, and unauthorized access.
Visibility and Monitoring	Continuous monitoring of cloud resources for abnormal activity or breaches.
Compliance and Legal Protection	Support for regulatory compliance (e.g., GDPR, HIPAA, PCI-DSS).
Incident Response	Ability to detect, respond to, and recover from security incidents quickly.
Isolation and Multi-Tenancy Control	Prevent data leaks and interference between different tenants (customers) sharing the same cloud.
Availability and Disaster Recovery	Ensure cloud services are resilient against failures and can recover rapidly.
Security Automation	Automated threat detection, policy enforcement, and incident handling to deal with cloud scale and speed.

Cloud Security: Challenges

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

Challenge	Explanation
Loss of Control	Data and infrastructure are managed by a third party.
Shared Technology Vulnerabilities	Multi-tenancy increases risk if virtualization/isolation fails.
Data Breaches and Misconfigurations	One of the top causes of cloud breaches (e.g., misconfigured S3 buckets).
Insider Threats	Threats from employees or administrators inside the cloud organization.
Compliance Complexity	Different countries have different data privacy and security laws.