APNIC eLearning:

Network Security Fundamentals

Contact: training@apnic.net

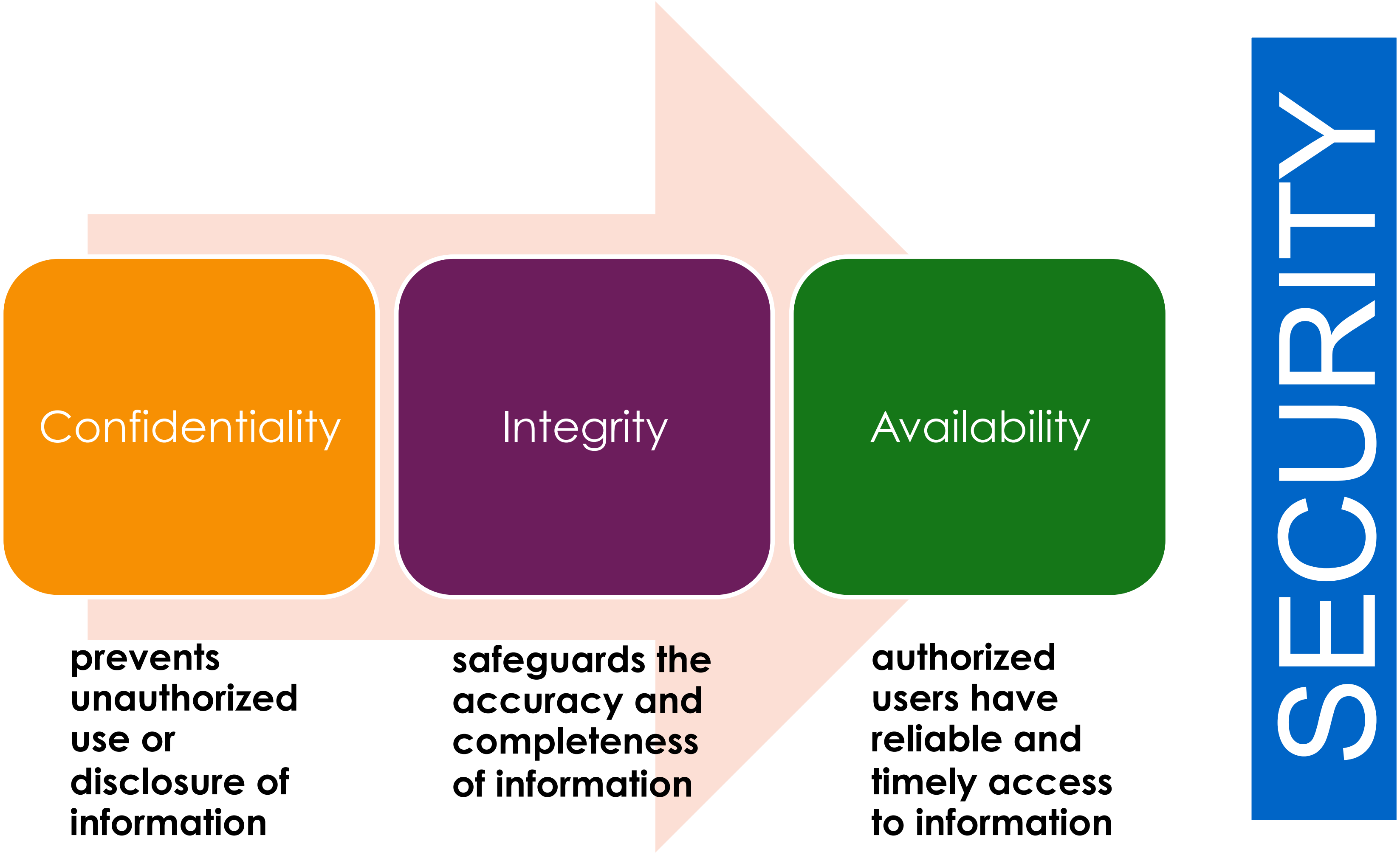
APNIC

eSEC01_v1.0

Overview

- Goals of Information Security
- Attacks on Different Layers
- Attack Examples
- Trusted Network
- Access Control
- Cryptography
- Public Key Infrastructure
- VPN and IPSec
- Security Management
- Whois Database

Goals of Information Security



prevents unauthorized use or disclosure of information

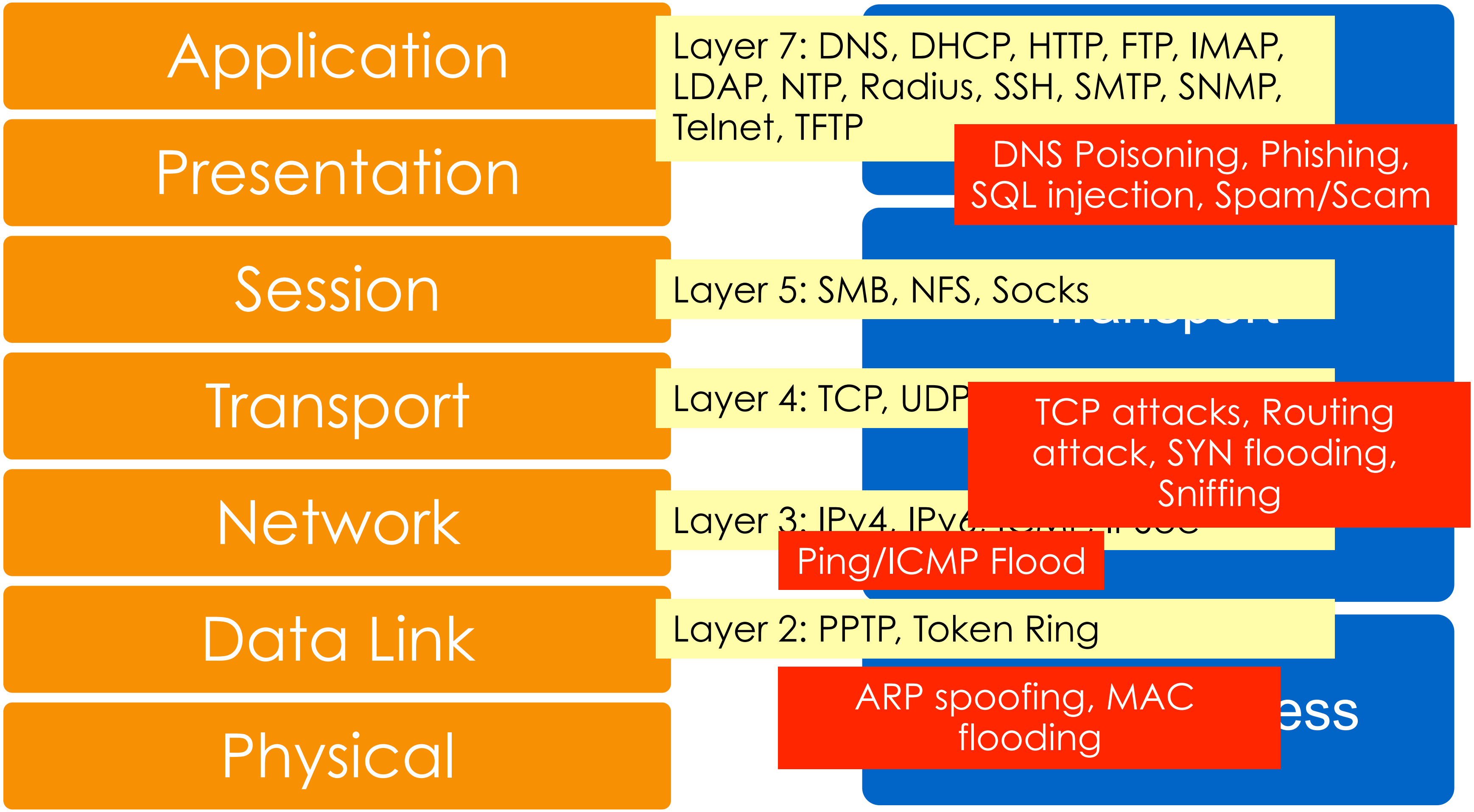
safeguards the accuracy and completeness of information

authorized users have reliable and timely access to information

Why Security?

- The Internet was initially designed for connectivity
  - Trust assumed
  - We do more with the Internet nowadays
  - Security protocols are added on top of the TCP/IP
- Fundamental aspects of information must be protected
  - Confidential data
  - Employee information
  - Business models
  - Protect identity and resources
- We can’t keep ourselves isolated from the Internet
  - Most business communications are done online
  - We provide online services
  - We get services from third-party organizations online

Attacks on Different Layers



Application

Presentation

Session

Transport

Network

Data Link

Physical

Layer 7: DNS, DHCP, HTTP, FTP, IMAP, LDAP, NTP, Radius, SSH, SMTP, SNMP, Telnet, TFTP

DNS Poisoning, Phishing, SQL injection, Spam/Scam

Layer 5: SMB, NFS, Socks

Layer 4: TCP, UDP

TCP attacks, Routing attack, SYN flooding, Sniffing

Layer 3: IPv4, IPv6, ICMP, IPSec

Ping/ICMP Flood

Layer 2: PPTP, Token Ring

ARP spoofing, MAC flooding

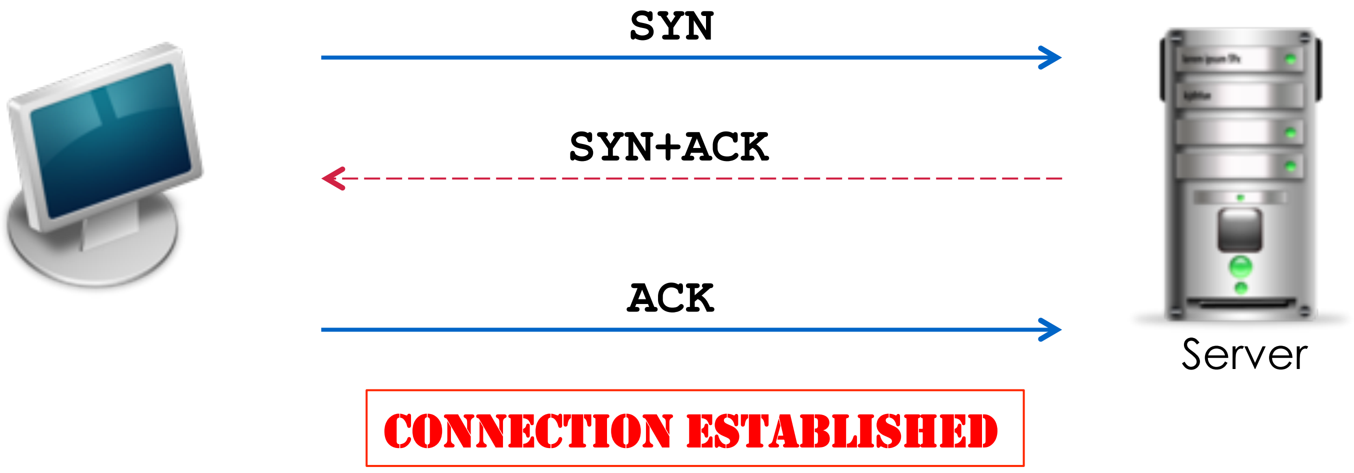
ess

OSI Reference Model

TCP/IP Model

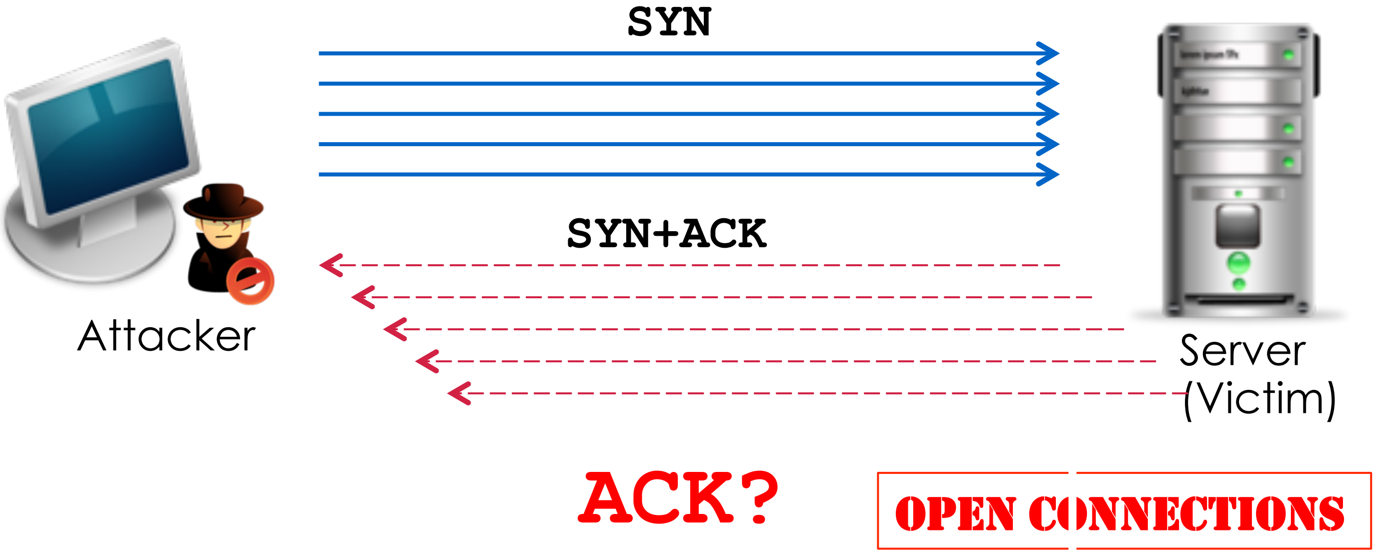
TCP Attacks

- Exploits the TCP 3-way handshake
- Attacker sends a series of SYN packets without replying with the ACK packet
- Finite queue size for incomplete connections

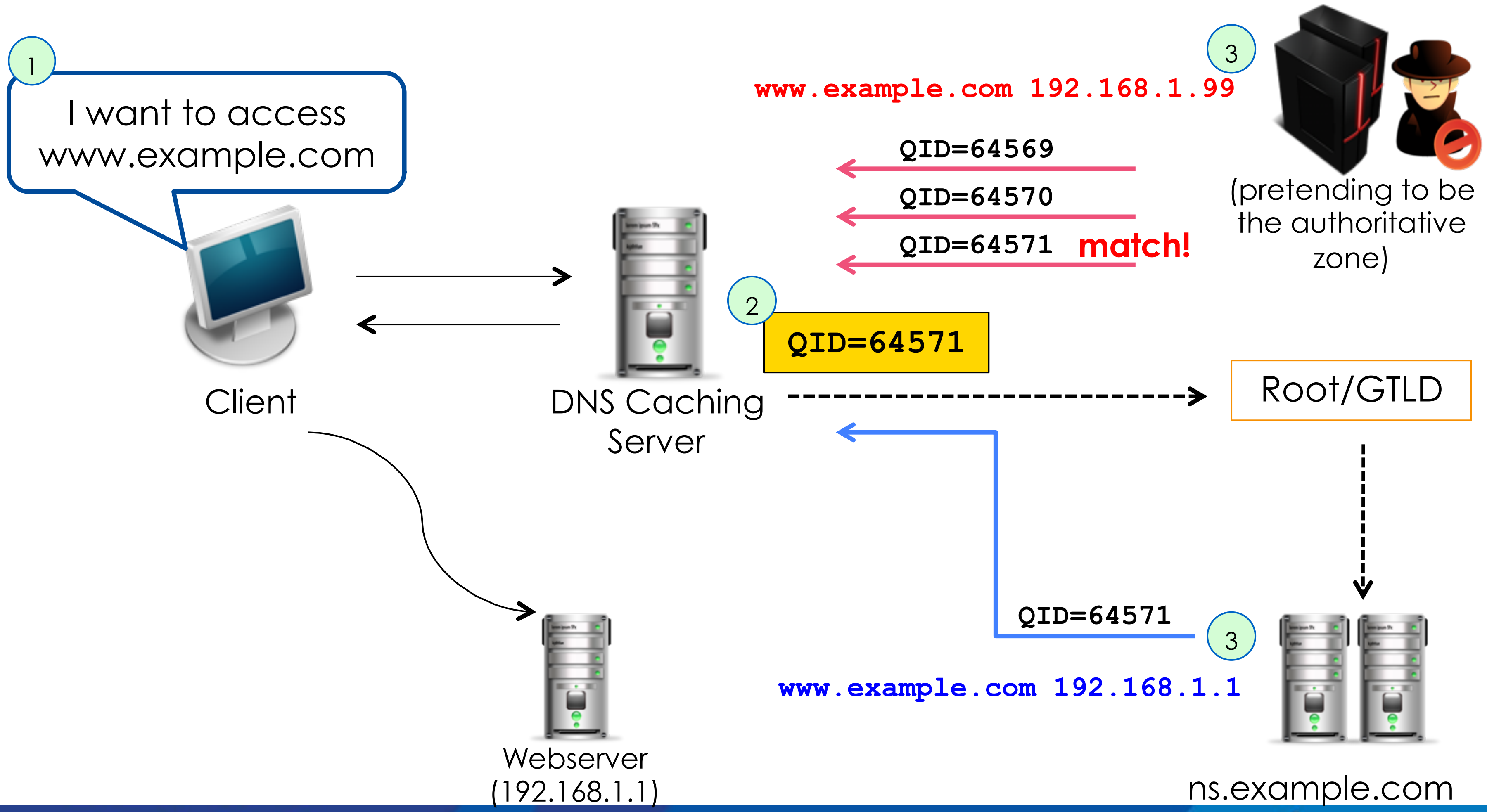


TCP Attacks

- Exploits the TCP 3-way handshake
- Attacker sends a series of SYN packets without replying with the ACK packet
- Finite queue size for incomplete connections



DNS Cache Poisoning


1
I want to access www.example.com
Client
DNS Caching Server
2
QID=64571
3
www.example.com 192.168.1.99
QID=64569
QID=64570
QID=64571
match!
(pretending to be the authoritative zone)
Root/GTLD
QID=64571
3
www.example.com 192.168.1.1
Webserver (192.168.1.1)
ns.example.com

Common Types of Attack

- Ping sweeps and port scans - reconnaissance
- Sniffing – capture packet as they travel through the network
- Man-in-the-middle attack – intercept messages that are intended for a valid device
- Spoofing - set up a fake device and trick others to send messages to it
- Hijacking – take control of a session
- Denial of Service (DoS) and Distributed DoS (DDoS)

Trusted Network

- Standard defensive-oriented technologies
  - Firewall – first line of defense
  - Intrusion Detection
- Build TRUST on top of the TCP/IP infrastructure
  - Strong authentication
    - Two-factor authentication
    - something you have + something you know
  - Public Key Infrastructure (PKI)

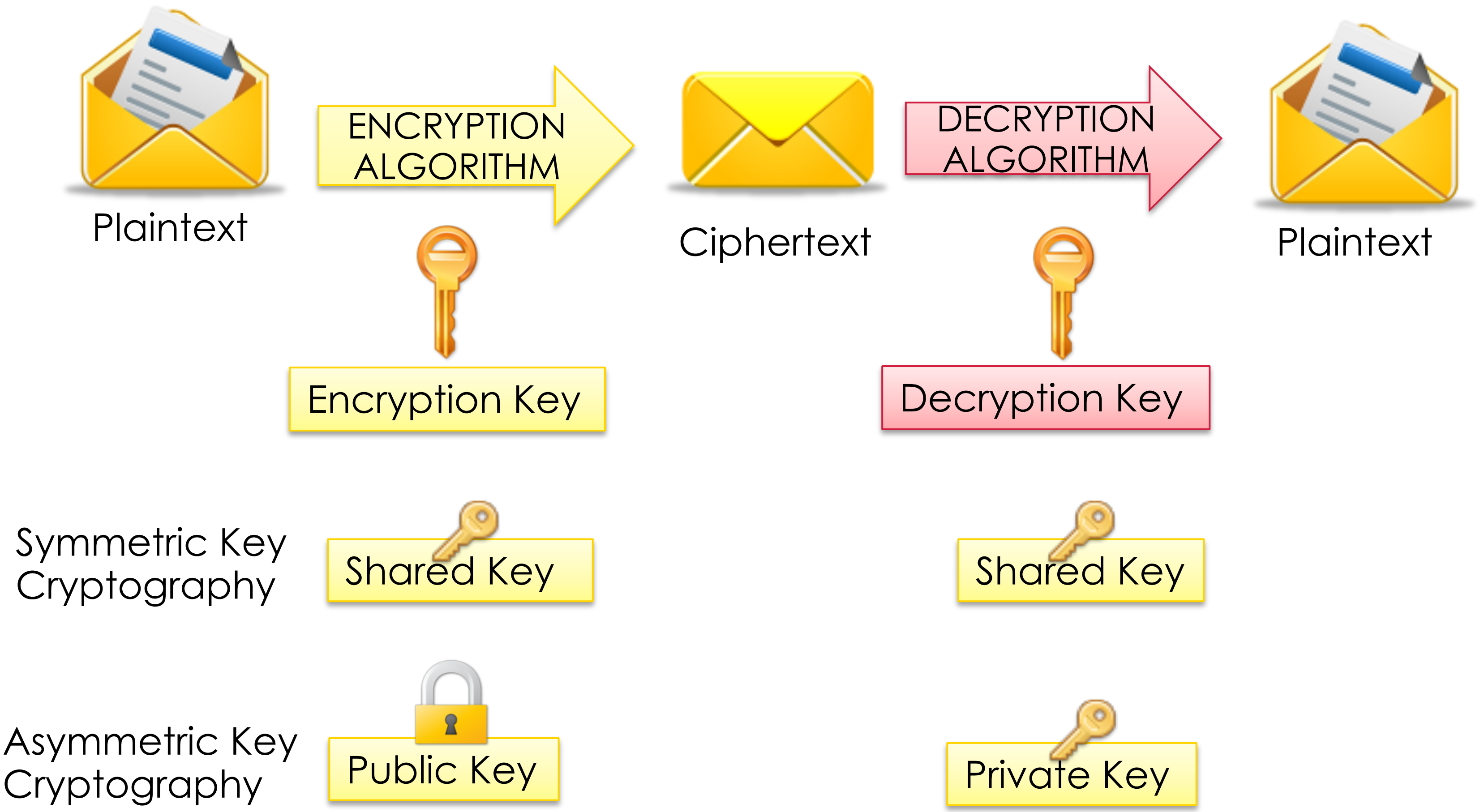
Access Control

- Access control - ability to permit or deny the use of an object by a subject.
- It provides 3 essential services (known as AAA):
  - Authentication (who can login)
  - Authorization (what authorized users can do)
  - Accountability (identifies what a user did)

Cryptography

- Has evolved into a complex science in the field of information security
- Encryption – process of transforming plaintext to ciphertext using a cryptographic key
- Symmetric key cryptography – uses a single key to encrypt and decrypt information. Also known as private key.
  - Includes DES, 3DES, AES, IDEA, RC5
- Asymmetric key cryptography – separate keys for encryption and decryption (public and private key pairs)
  - Includes RSA, Diffie-Hellman, El Gamal

Cryptography



Plaintext

ENCRYPTION ALGORITHM

Ciphertext

DECRYPTION ALGORITHM

Plaintext

Encryption Key

Decryption Key

Symmetric Key Cryptography

Shared Key

Shared Key

Asymmetric Key Cryptography

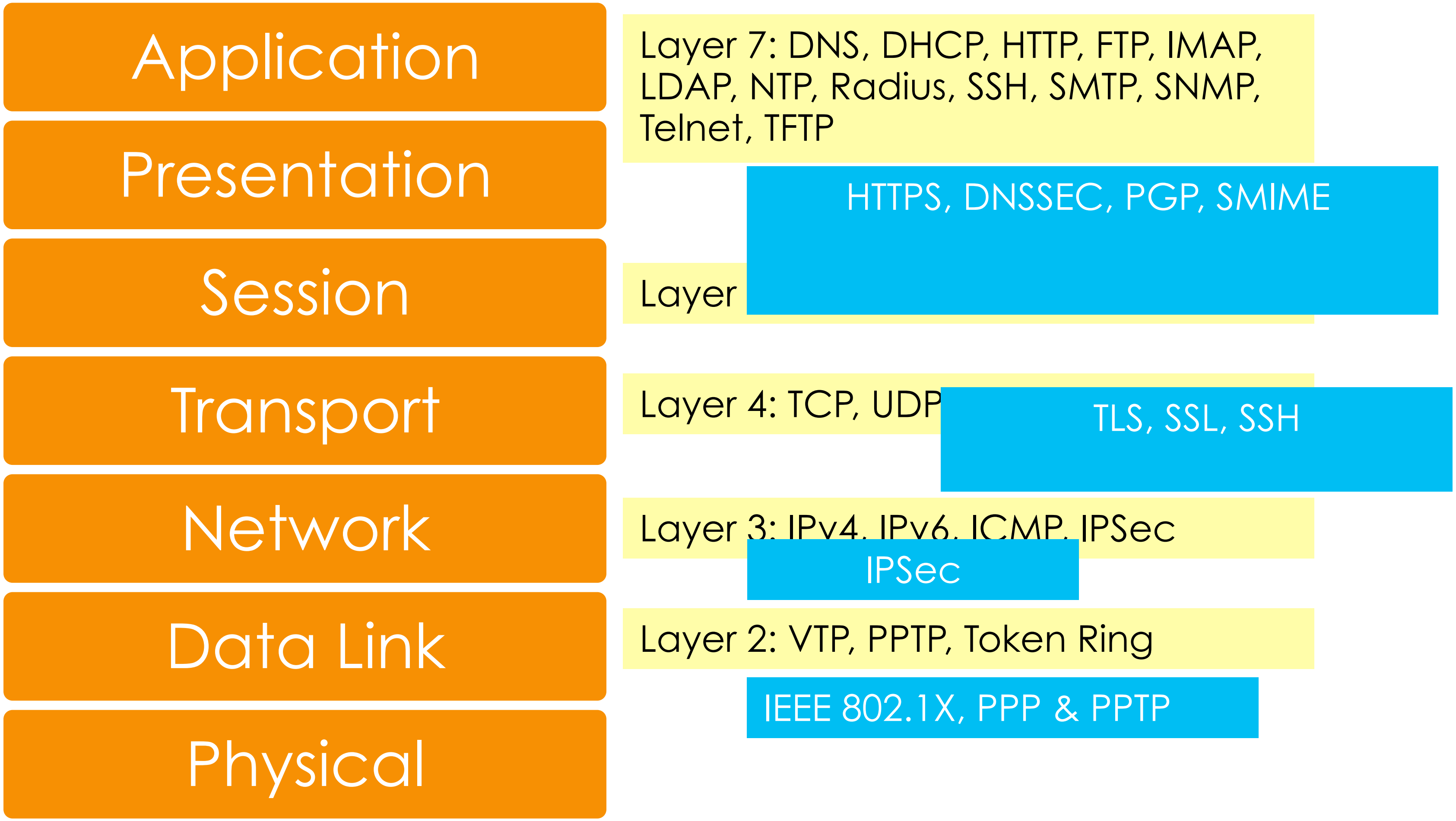
Public Key

Private Key

Public Key Infrastructure

- Combines public key cryptography and digital signatures to ensure confidentiality, integrity, authentication, non-repudiation, and access control
- Digital certificate – basic element of PKI; secure credential that identifies the owner
- Basic Components:
  - Certificate Authority (CA)
  - Registration Authority (RA)
  - Repository
  - Archive

Security on Different Layers



Application

Presentation

Session

Transport

Network

Data Link

Physical

Layer 7: DNS, DHCP, HTTP, FTP, IMAP, LDAP, NTP, Radius, SSH, SMTP, SNMP, Telnet, TFTP

HTTPS, DNSSEC, PGP, SMIME

Layer

Layer 4: TCP, UDP

TLS, SSL, SSH

Layer 3: IPv4, IPv6, ICMP, IPSec

IPSec

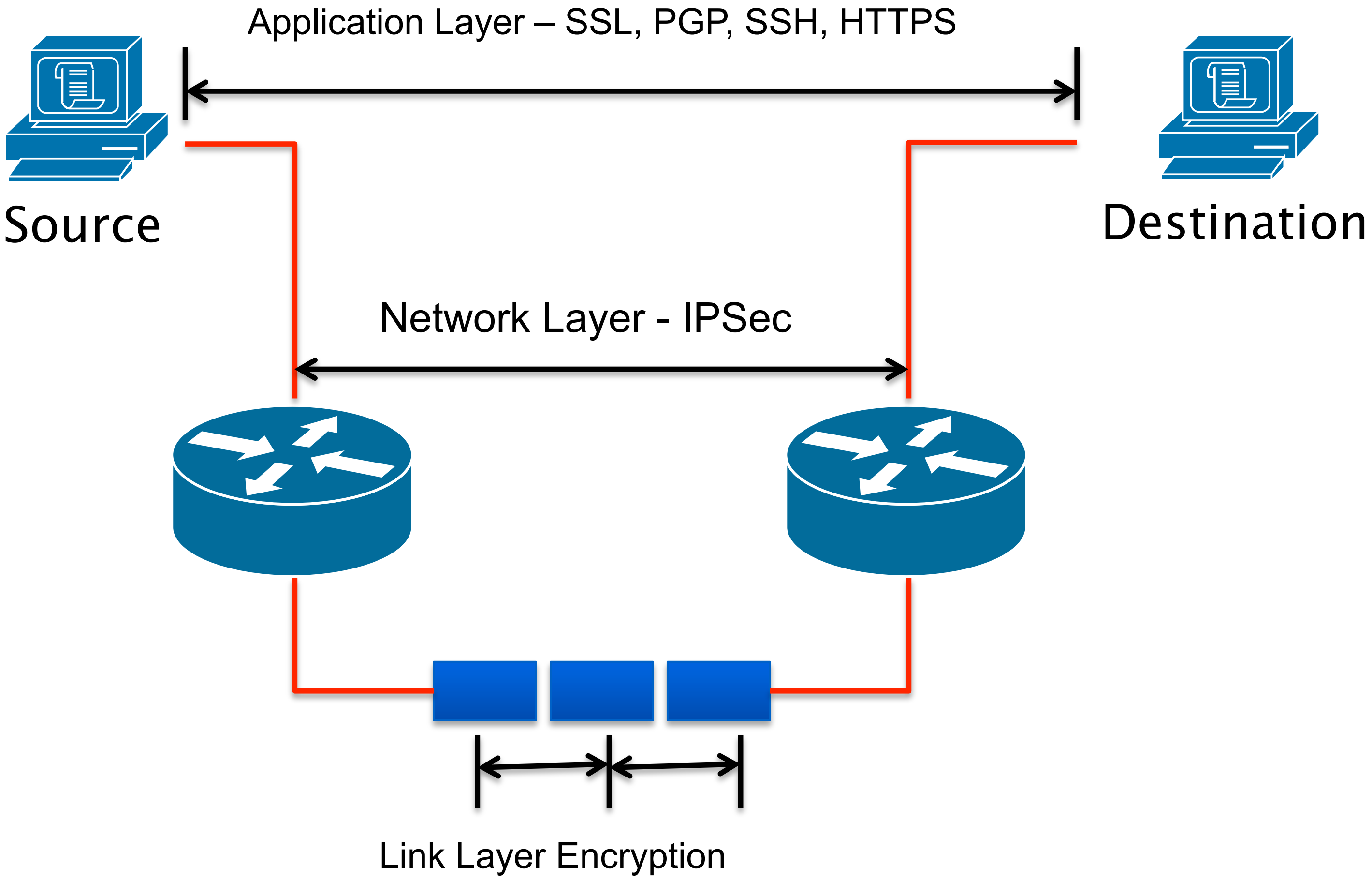
Layer 2: VTP, PPTP, Token Ring

IEEE 802.1X, PPP & PPTP

Virtual Private Network

- Creates a secure tunnel over a public network
  - Client-to-firewall, router-to-router, firewall-to-firewall
- VPN Protocol Standards
  - PPTP (Point-to-Point tunneling Protocol)
  - L2F (Layer 2 Forwarding Protocol)
  - L2TP (Layer 2 Tunneling Protocol)
  - IPSec (Internet Protocol Security)

Different Layers of Encryption



IPSec

- Provides Layer 3 security
- Tunnel or Transport mode
  - Tunnel mode – entire IP packet is encrypted
  - Transport mode – IPSec header is inserted in to the packet
- Combines different components:
  - Security associations, Authentication headers (AH), Encapsulating security payload (ESP), Internet Key Exchange (IKE)
- A security context for the VPN tunnel is established via the ISAKMP

Internet Security Protocols

- Layer 4 security: TLS, SSL, SSH
- SSL/TLS (Secure Socket Layer / Transport Layer Security)
  - Session-based encryption and authentication for secure communication (prevent eavesdropping)
  - TLS is the IETF standard succeeding SSL
  - Uses RSA asymmetric key system
- Secure Shell (SSH2) – secure channel between devices, replaces telnet and rsh

Security Management

- Network security is a part of a bigger information security plan
- Policies vs. Standards vs. Guidelines
- Must develop and implement comprehensive security policy
  - Minimum password length, frequency of password change
  - Access of devices, host firewalls
  - User creation/deletion process
  - Data signing/encryption
  - Encrypting all communication (remote access)
  - Use of digital certificates
- Disaster Recovery and Attack Mitigation Plan

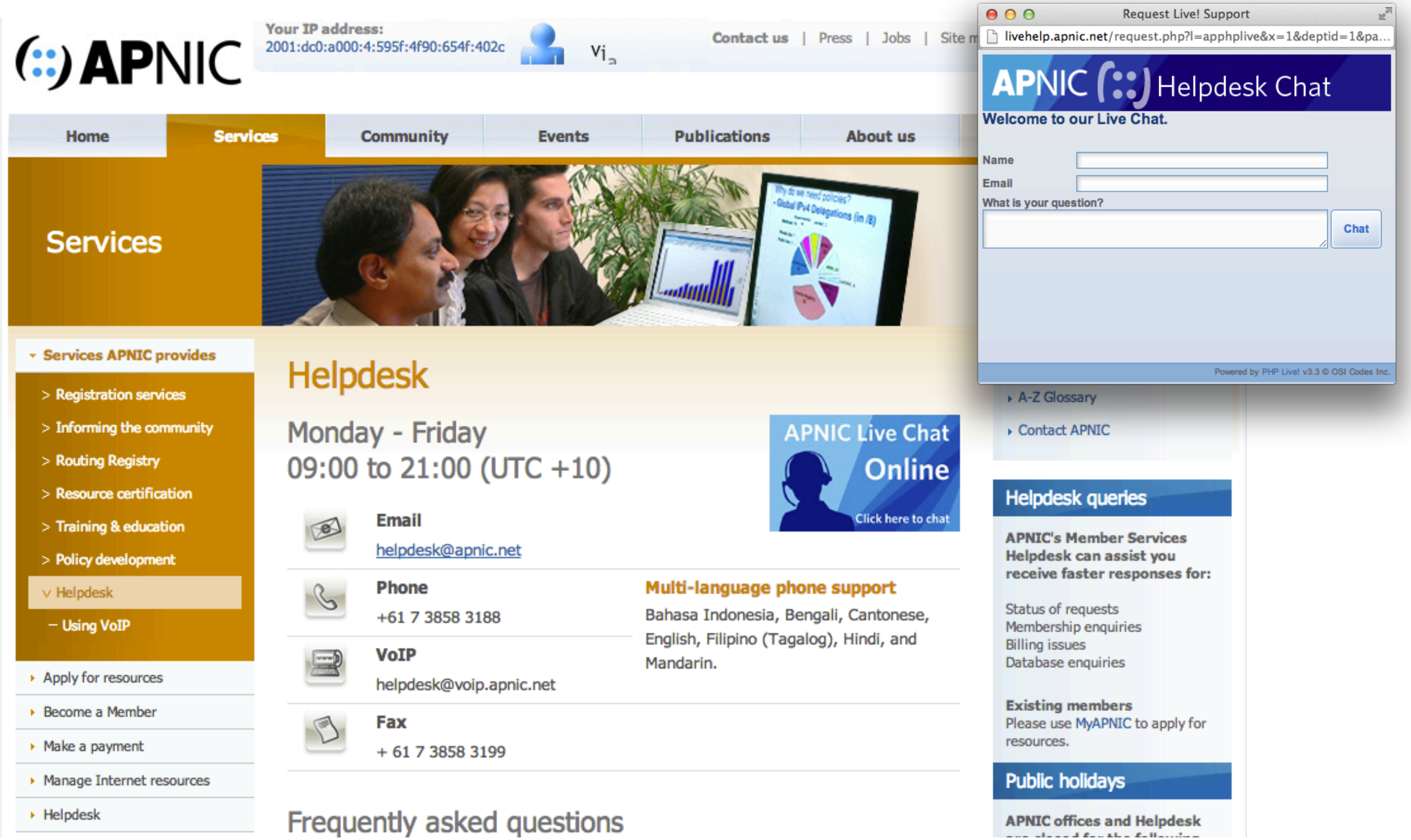
Whois Database

- Public network management database
- Tracks network resources
  - IP addreses, ASNs, reverse domains, routing
- Records administrative info
  - Contacts (person/role), authorization (maintainer)
- All Members must register their resources in the Whois database
- Must keep records up to date at all times

Questions

- Please remember to fill out the feedback form
  - <survey-link>
- Slide handouts will be available after completing the survey

APNIC Helpdesk Chat



APNIC

Your IP address:
2001:dc0:a000:4:595f:4f90:654f:402c

Contact us | Press | Jobs | Site m

Services

- Services APNIC provides
  - > Registration services
  - > Informing the community
  - > Routing Registry
  - > Resource certification
  - > Training & education
  - > Policy development
  - v Helpdesk
    - – Using VoIP
- Apply for resources
- Become a Member
- Make a payment
- Manage Internet resources
- Helpdesk

Helpdesk

Monday - Friday
09:00 to 21:00 (UTC +10)

APNIC Live Chat
Online
Click here to chat

Email
helpdesk@apnic.net

Phone
+61 7 3858 3188

VoIP
helpdesk@voip.apnic.net

Fax
+ 61 7 3858 3199

Multi-language phone support
Bahasa Indonesia, Bengali, Cantonese, English, Filipino (Tagalog), Hindi, and Mandarin.

Frequently asked questions

- A-Z Glossary
- Contact APNIC

Helpdesk queries

APNIC's Member Services Helpdesk can assist you receive faster responses for:

Status of requests
Membership enquiries
Billing issues
Database enquiries

Existing members
Please use MyAPNIC to apply for resources.

Public holidays

APNIC offices and Helpdesk

Request Live! Support

livehelp.apnic.net/request.php?l=apphplive&x=1&deptid=1&pa...

APNIC Helpdesk Chat

Welcome to our Live Chat.

Name
Email
What is your question?

Powered by PHP Live! v3.3 © OSI Codes Inc.

Thank You!

End of Session