Cybersecurity Workshop

Linux, TCP/IP, OSI layer and protocols, networking and security concepts, encryption, latest cybersecurity trends

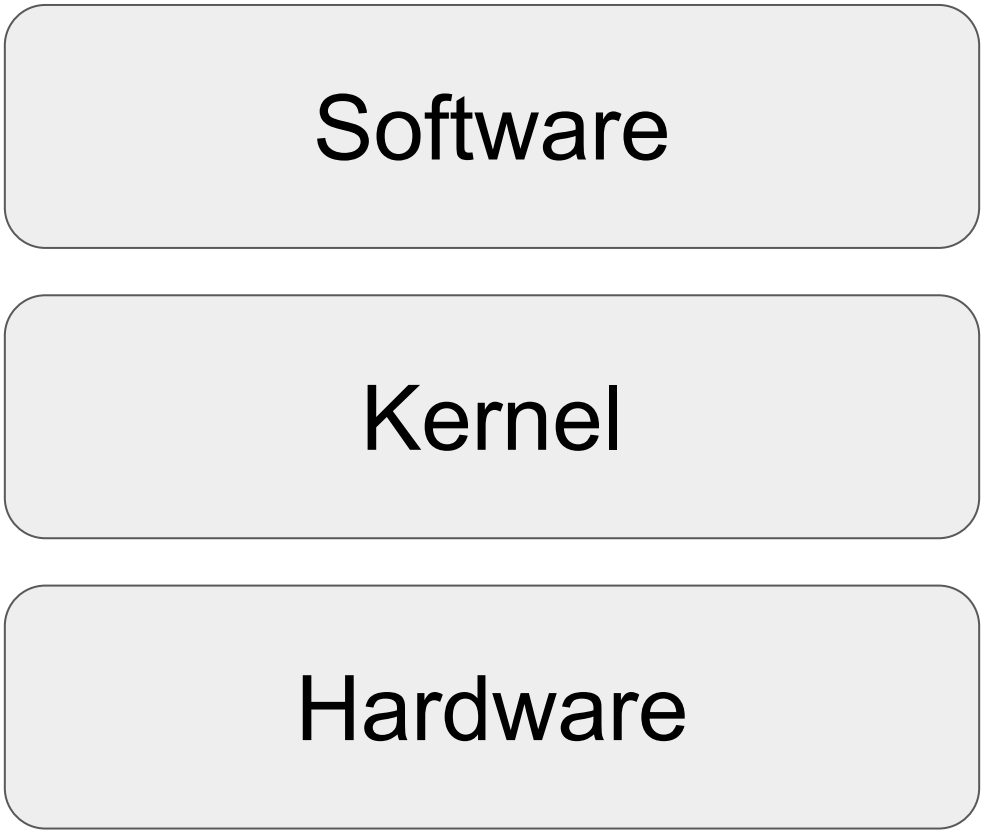
Linux

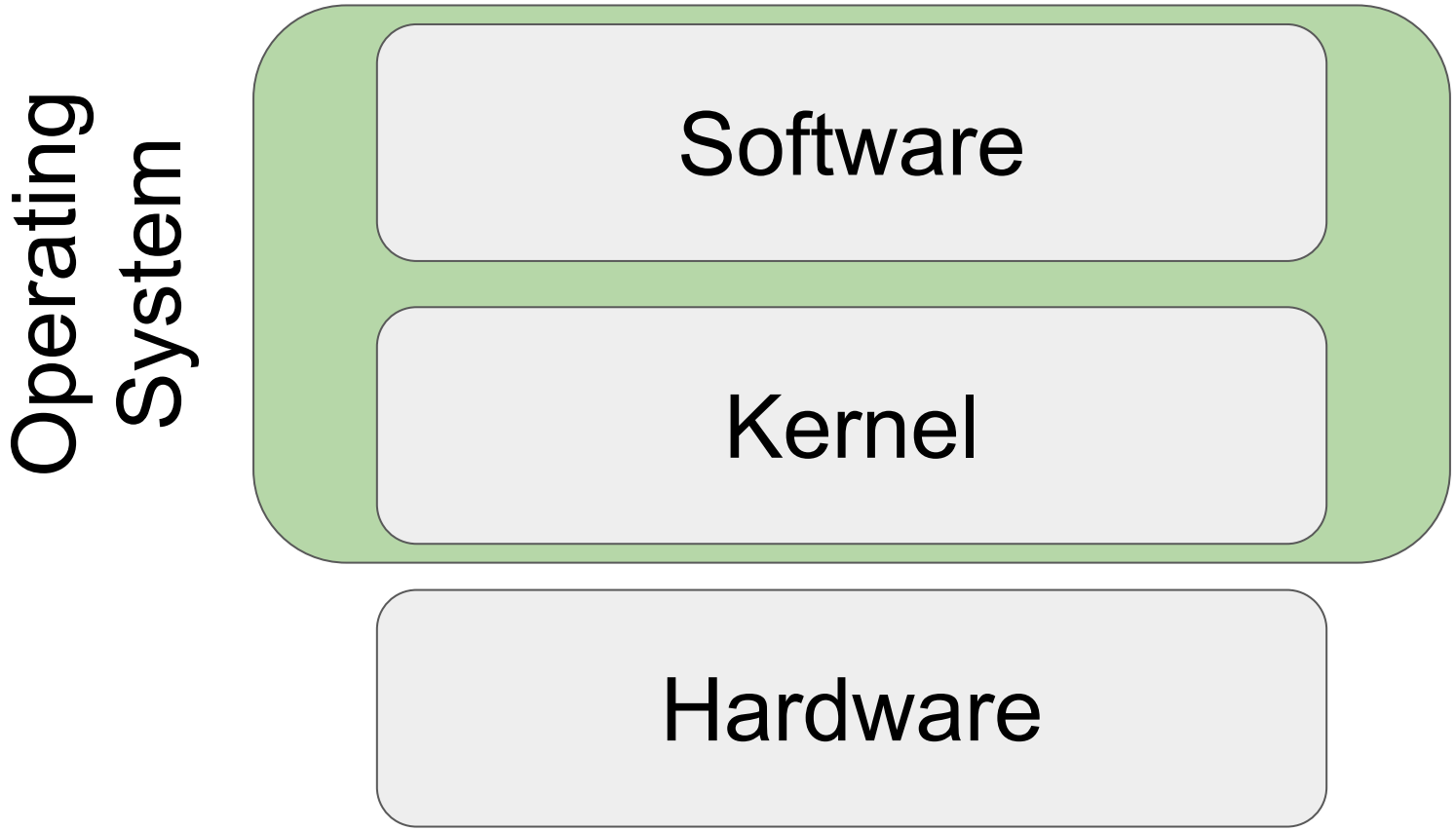
Operating System

Kernel

Software

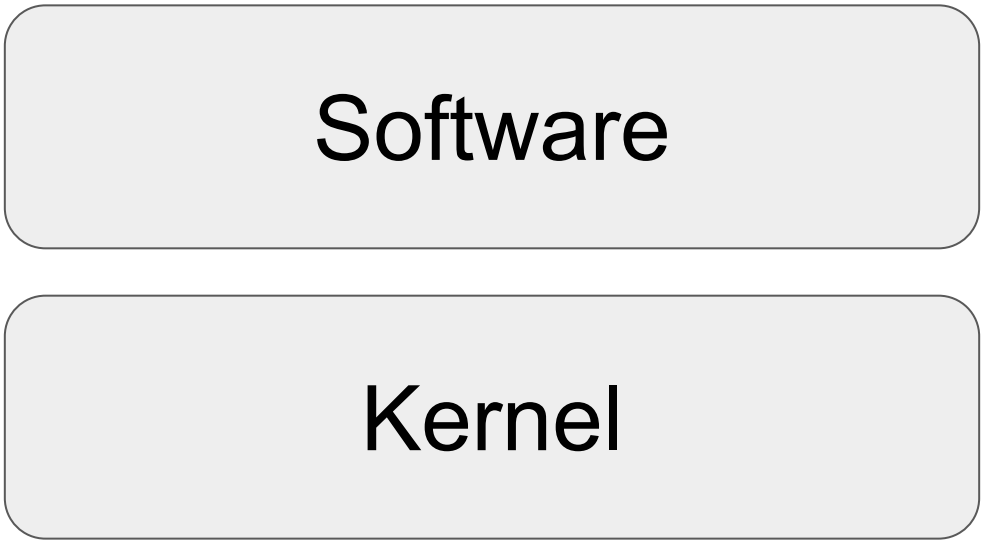
Hardware


Software
Kernel
Hardware


Operating System
Software
Kernel
Hardware

Ubuntu

Operating System


Software
Kernel

Software

Linux

GNU

Linux

Why?

Open Source

github.com/torvalds/linux

High Security

Compact

Easy to install

Some other popular Linux based Operating systems

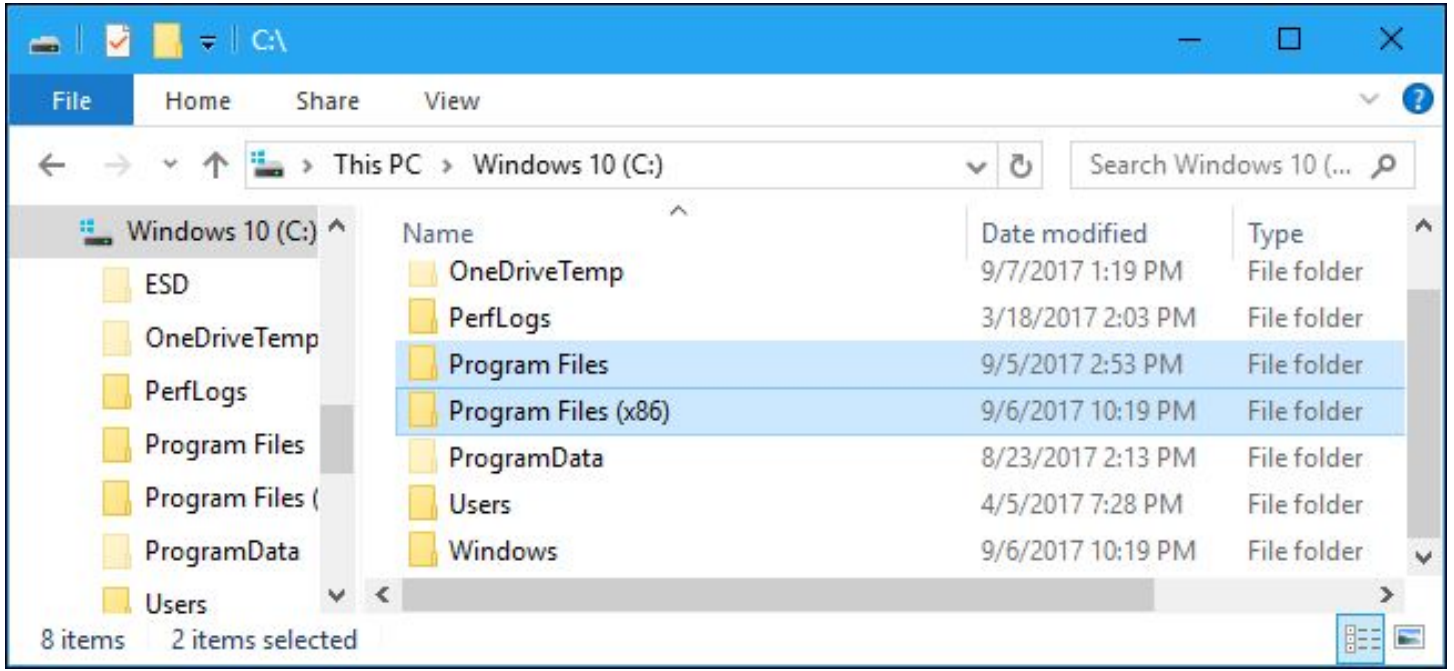
Debian, Fedora, Arch, Suse, KDE, Parrot, Kali

Debian, Fedora, Arch, Suse,
KDE, Parrot, Kali

Linux vs. Windows

File system

Windows


C:\
File
Home
Share
View
This PC › Windows 10 (C:)
Search Windows 10 (...
Windows 10 (C:)
ESD
OneDriveTemp
PerfLogs
Program Files
Program Files (
ProgramData
Users
Name
Date modified
Type
OneDriveTemp 9/7/2017 1:19 PM File folder
PerfLogs 3/18/2017 2:03 PM File folder
Program Files 9/5/2017 2:53 PM File folder
Program Files (x86) 9/6/2017 10:19 PM File folder
ProgramData 8/23/2017 2:13 PM File folder
Users 4/5/2017 7:28 PM File folder
Windows 9/6/2017 10:19 PM File folder
8 items
2 items selected

Linux

/
Root Directory

Everything on your Linux system is located under the / directory, known as the root directory.

Linux

/bin
Binary Files

The /bin directory contains the **essential user binaries**. These programs will be **accessible to all users**.

Binaries **specific for a particular user** will be contained in **/usr/bin**

Linux

/sbin
System Administrator Binary Files

The /bin directory contains the **binaries for the root user**.

Linux

/usr
User Specific Files

Linux

/boot
Binary Files

The /boot directory contains the files needed to boot the system – for example, the **GRUB bootloader** files and your **Linux kernels** are stored here.

Linux

/cdrom
CD ROM

Linux

/dev
Devices

Linux exposes devices as files, and the /dev directory contains a number of special files that represent devices. These are not actual files as we know them, but they appear as files

Linux

/etc
Configuration Files

Configuration files of various software including the operating system

Linux

/home
Home Folder

Contains documents, downloads, pictures, music and so on of all users.

If your username is bhat the files will be stored in /home/bhat

Linux

/lib
Library

User Account Types

Windows

1. Administrator
2. Standard
3. Child
4. Guest

Linux

1. Root
2. Regular
3. Service

Security

Filename

File　FILE

More special characters

" * : < > ? \ |

Linux Commands

ls

mkdir

cd

cat > filename

cat filename

rm filename

mv filename new_location

rmdir

sudo apt-get

sudo apt

sudo apt install
update
upgrade
remove
purge

Network Models

TCP/IP OSI

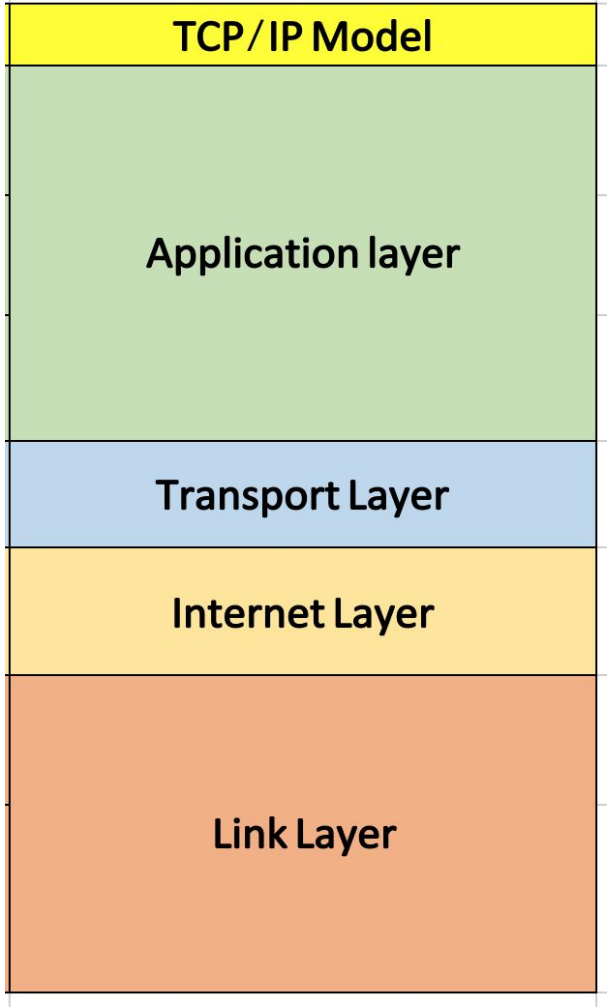
Client-Server

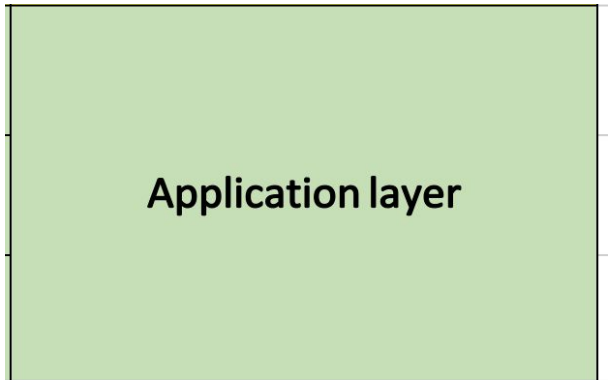

Client
Request
Server


Client
Response
Server

TCP/IP OSI

TCP/IP


TCP/IP Model
Application layer
Transport Layer
Internet Layer
Link Layer

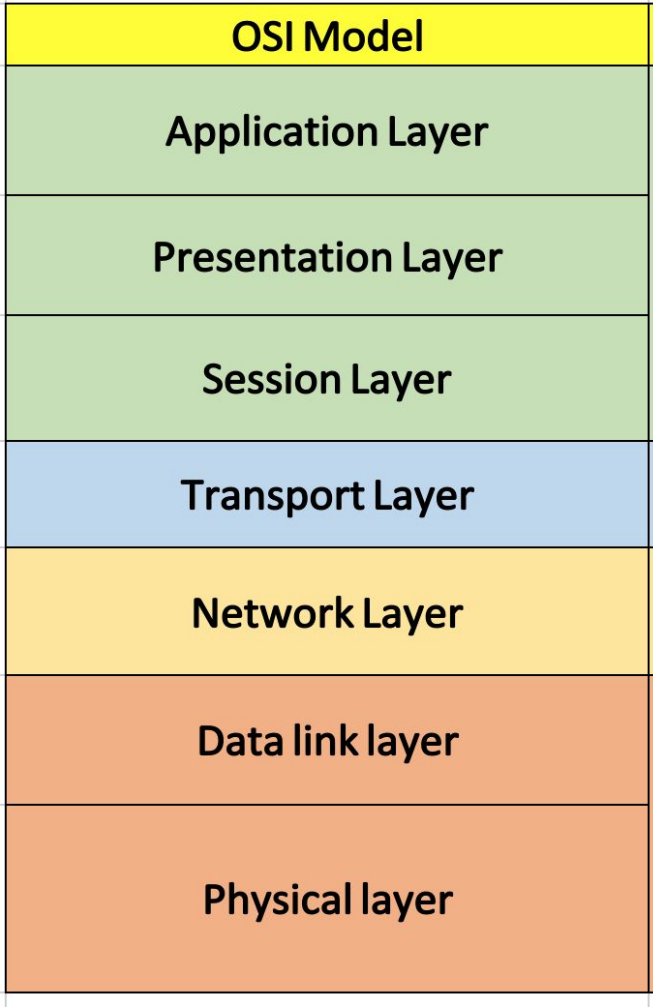


The application layer provides applications with standardized data exchange. Its protocols include the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol 3 (POP3), Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP).

The transport layer is responsible for maintaining end-to-end communications across the network. TCP handles communications between hosts and provides flow control, multiplexing and reliability. The transport protocols include TCP and User Datagram Protocol (UDP), which is sometimes used instead of TCP for special purposes.

The network layer, also called the internet layer, deals with packets and connects independent networks to transport the packets across network boundaries. The network layer protocols are the IP and the Internet Control Message Protocol (ICMP), which is used for error reporting.

The physical layer consists of protocols that operate only on a link -- the network component that interconnects nodes or hosts in the network. The protocols in this layer include Ethernet for local area networks (LANs) and the Address Resolution Protocol (ARP).


OSI Model
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data link layer
Physical layer

At the very top of the OSI we find Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user. HTTP, HTTPS, DNS, FTP, etc. are some of the protocols used in this layer.

Presentation layer is also called the Translation layer.The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

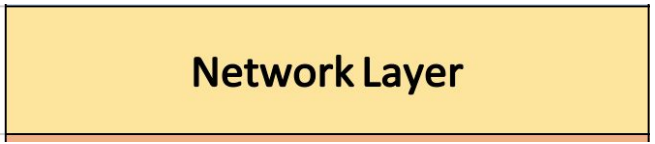
Protocols: TLS, SSL, FTP, IMAP SSH, Telnet

This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.

Protocols: PAP, RPC, RTCP, SDP, SMB

Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as Segments. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

Protocols: AH, DCCP, ESP, NetBIOS, NBF, SCTP, TCP, UDP

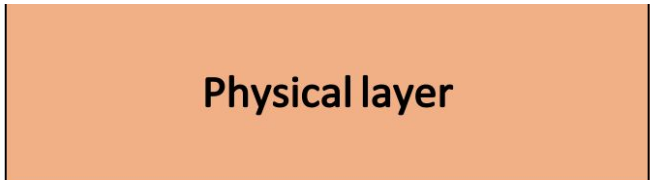


Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP address are placed in the header by the network layer.

Protocols: HSRP, VRRP, IP, ICMP, ARP

The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.

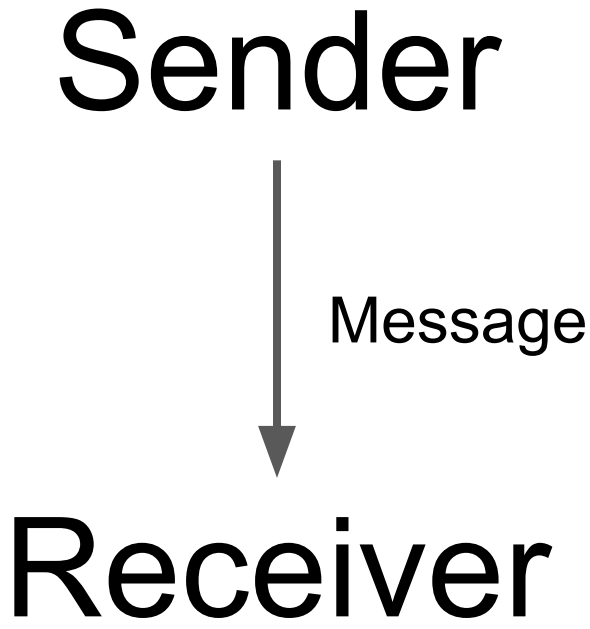
Protocols: ARP, ATM, MAC, Ethernet, VLAN, PPP

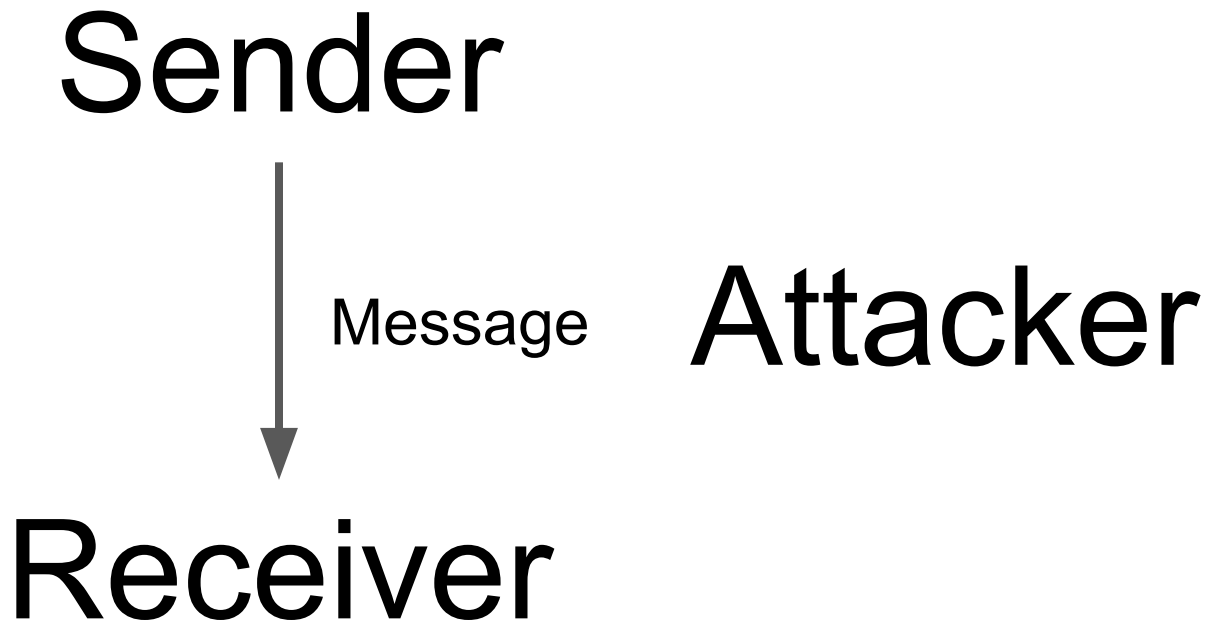


The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into binary and send them to the Data Link layer.

Protocols: USB, DSL, EtherLoop

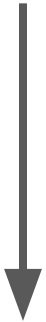
Encryption


Sender
Message
Receiver


Sender
Message
Attacker
Receiver

“building a better world”

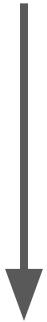
“building a better world”



“asdfas89u4rweal&cdal#”

Decryption

“asdfas89u4rweal&cdal#”



“building a better world”

Sender

“building a better world”

Receiver

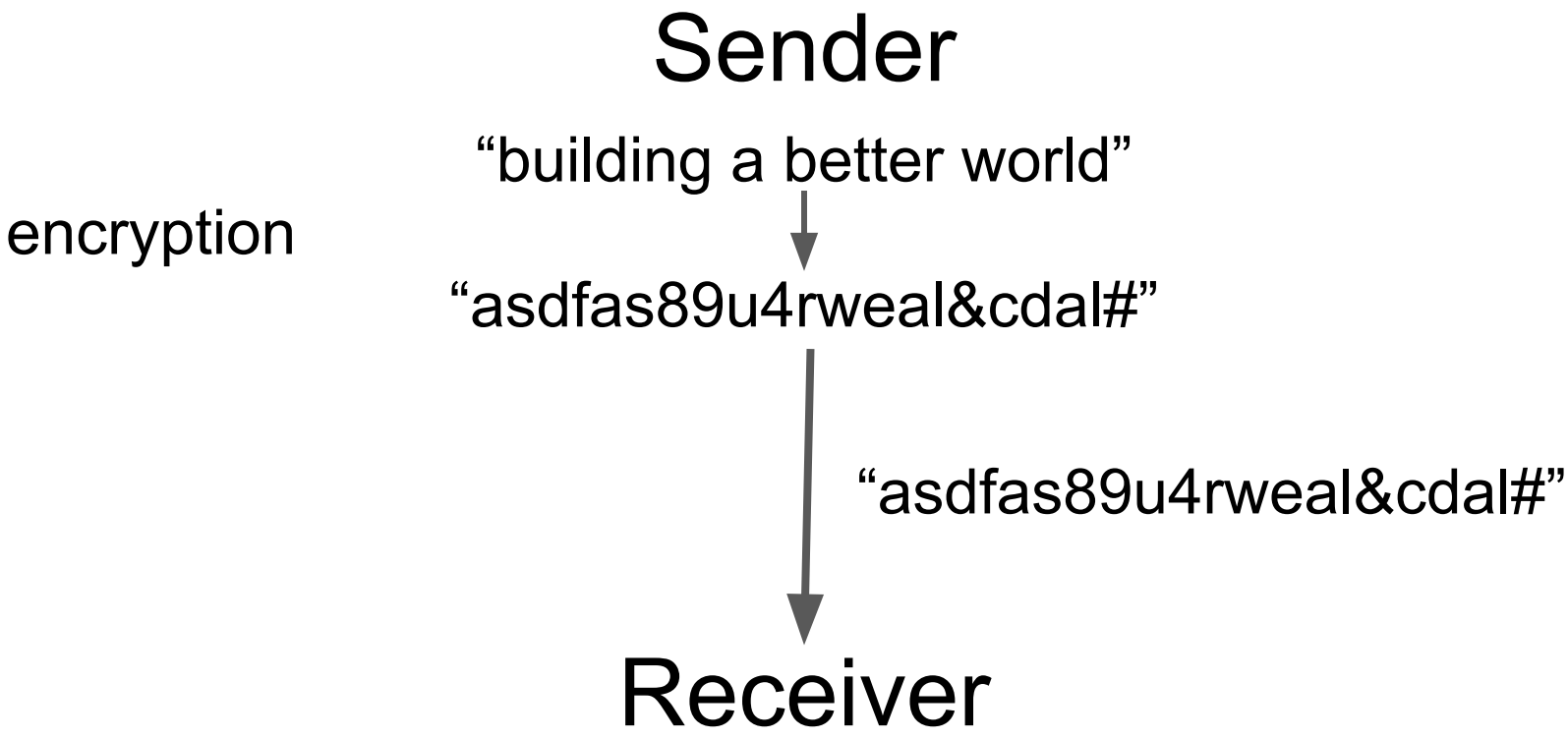
Sender

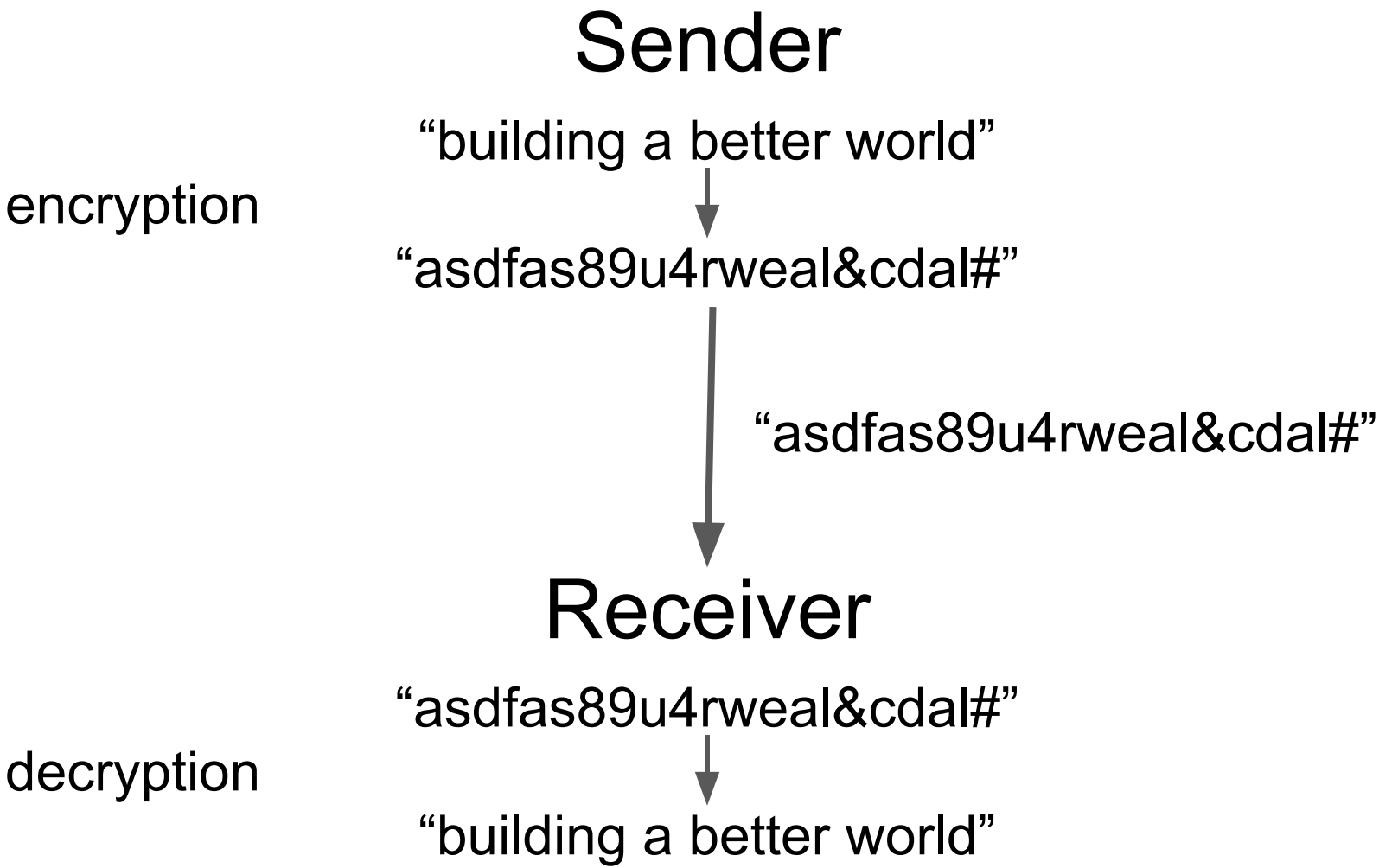
“building a better world”

encryption

“asdfas89u4rweal&cdal#”

Receiver


Sender
“building a better world”
encryption
“asdfas89u4rweal&cdal#”
“asdfas89u4rweal&cdal#”
Receiver


Sender
“building a better world”
encryption
“asdfas89u4rweal&cdal#”
“asdfas89u4rweal&cdal#”
Receiver
“asdfas89u4rweal&cdal#”
decryption
“building a better world”


Sender
“building a better world”
encryption
“asdfas89u4rweal&cdal#”
Attacker
“asdfas89u4rweal&cdal#”
Receiver
“asdfas89u4rweal&cdal#”
decryption
“building a better world”

Symmetric Encryption

AES, DES, IDEA

Asymmetric Encryption

RSA, Diffie-Hellman, ECC


Sender
“building a better world”
encryption
“asdfas89u4rweal&cdal#”
Attacker
“asdfas89u4rweal&cdal#”
Receiver
“asdfas89u4rweal&cdal#”
decryption
“building a better world”


Sender
“building a better world”
encryption
“asdfas89u4rweal&cdal#”
“asdfas89u4rweal&cdal#”
Receiver
“asdfas89u4rweal&cdal#”
decryption
“building a better world”


Sender
“building a better world”
AES
“asdfas89u4rweal&cdal#”
“asdfas89u4rweal&cdal#”
Receiver
“asdfas89u4rweal&cdal#”
AES
“building a better world”

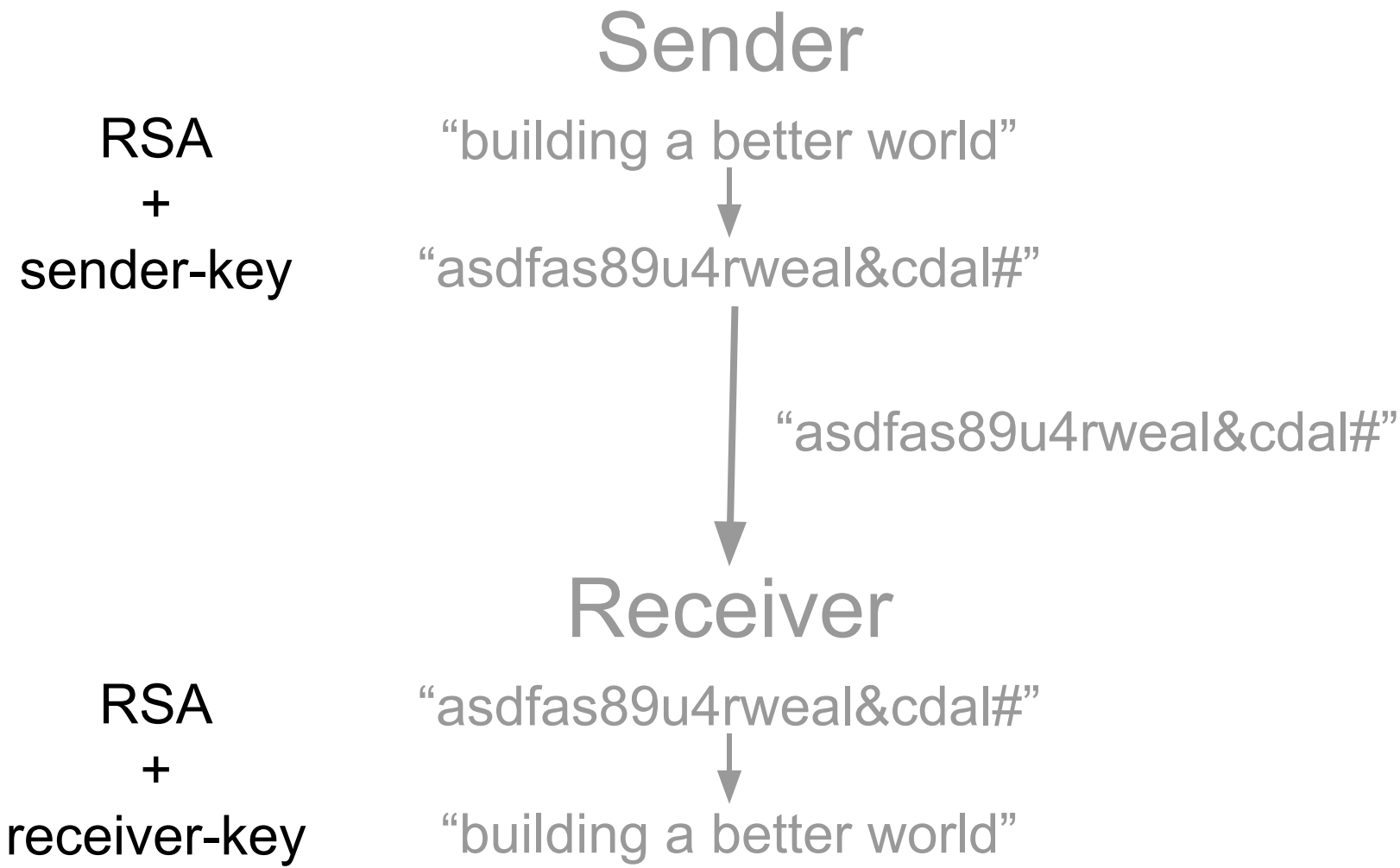

Sender
AES
+
secret-key
“building a better world”
“asdfas89u4rweal&cdal#”
“asdfas89u4rweal&cdal#”
Receiver
AES
+
secret-key
“asdfas89u4rweal&cdal#”
“building a better world”

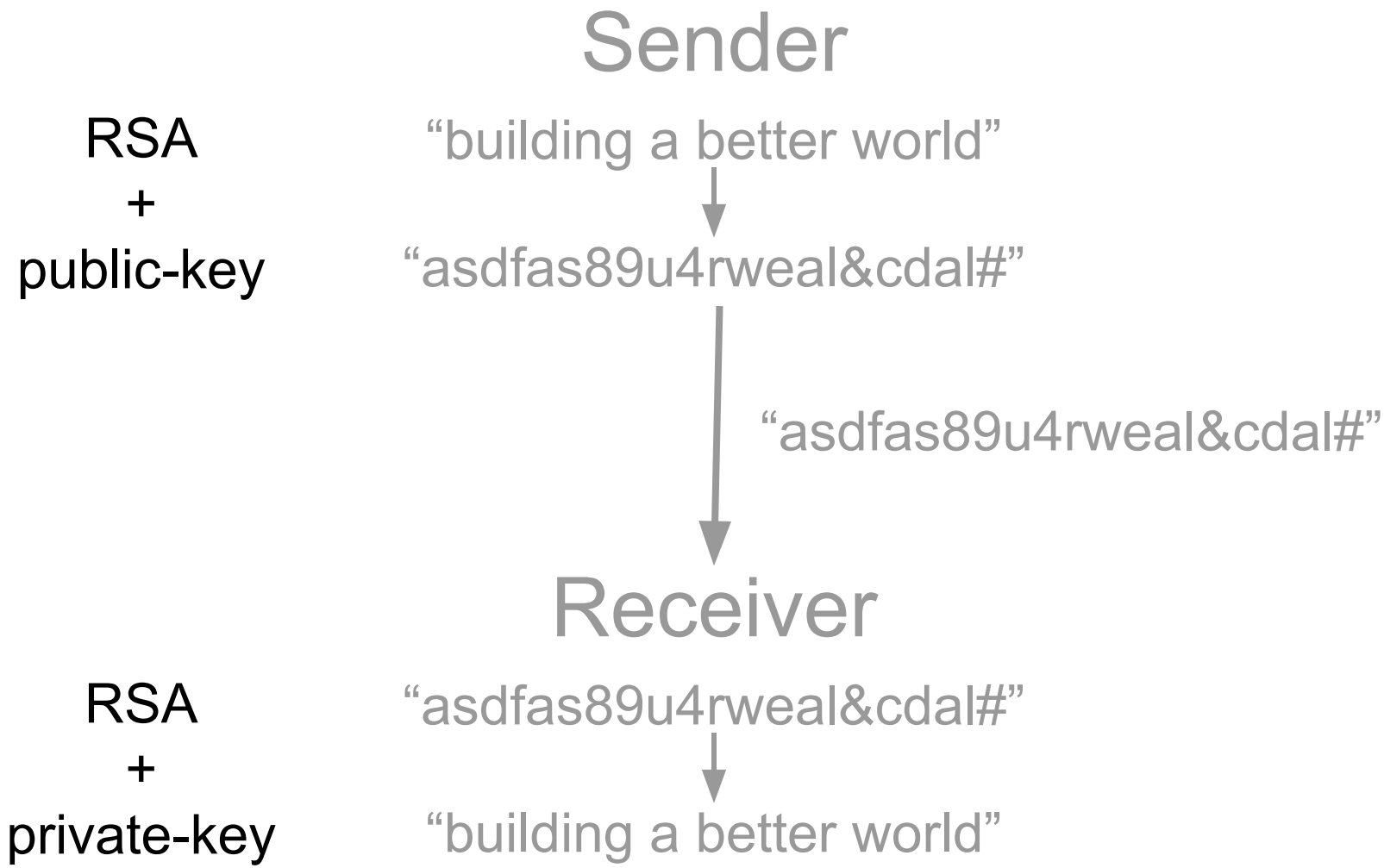

Sender
AES
+
secret-key
“building a better world”
“asdfas89u4rweal&cdal#”
Attacker
“asdfas89u4rweal&cdal#”
AES
Receiver
AES
+
secret-key
“asdfas89u4rweal&cdal#”
“building a better world”


Sender
AES
+
secret-key
“building a better world”
“asdfas89u4rweal&cdal#”
Attacker
“asdfas89u4rweal&cdal#”
secret-key
AES
Receiver
AES
+
secret-key
“asdfas89u4rweal&cdal#”
“building a better world”


Sender
AES
+
secret-key
“building a better world”
“asdfas89u4rweal&cdal#”
Attacker
“asdfas89u4rweal&cdal#”
secret-key
AES
+
secret-key
Receiver
AES
+
secret-key
“asdfas89u4rweal&cdal#”
“building a better world”


Sender
“building a better world”
RSA
“asdfas89u4rweal&cdal#”
“asdfas89u4rweal&cdal#”
Receiver
“asdfas89u4rweal&cdal#”
RSA
“building a better world”


Sender
RSA
+
sender-key
“building a better world”
“asdfas89u4rweal&cdal#”
“asdfas89u4rweal&cdal#”
Receiver
RSA
+
receiver-key
“asdfas89u4rweal&cdal#”
“building a better world”


Sender
RSA
+
public-key
“building a better world”
“asdfas89u4rweal&cdal#”
“asdfas89u4rweal&cdal#”
Receiver
RSA
+
private-key
“asdfas89u4rweal&cdal#”
“building a better world”

Public key encryption

encryption

public-key

decryption

private-key

encryption

public-key

decryption

private-key

Sender

Receiver

Sender

Receiver

private-key
+
public-key

Sender

public-key

Receiver

private-key
+
public-key

Sender

public-key

Receiver

Attacker

private-key
+
public-key

Sender

“building a better world”

Receiver

Sender

RSA
+
public-key

“building a better world”

Receiver

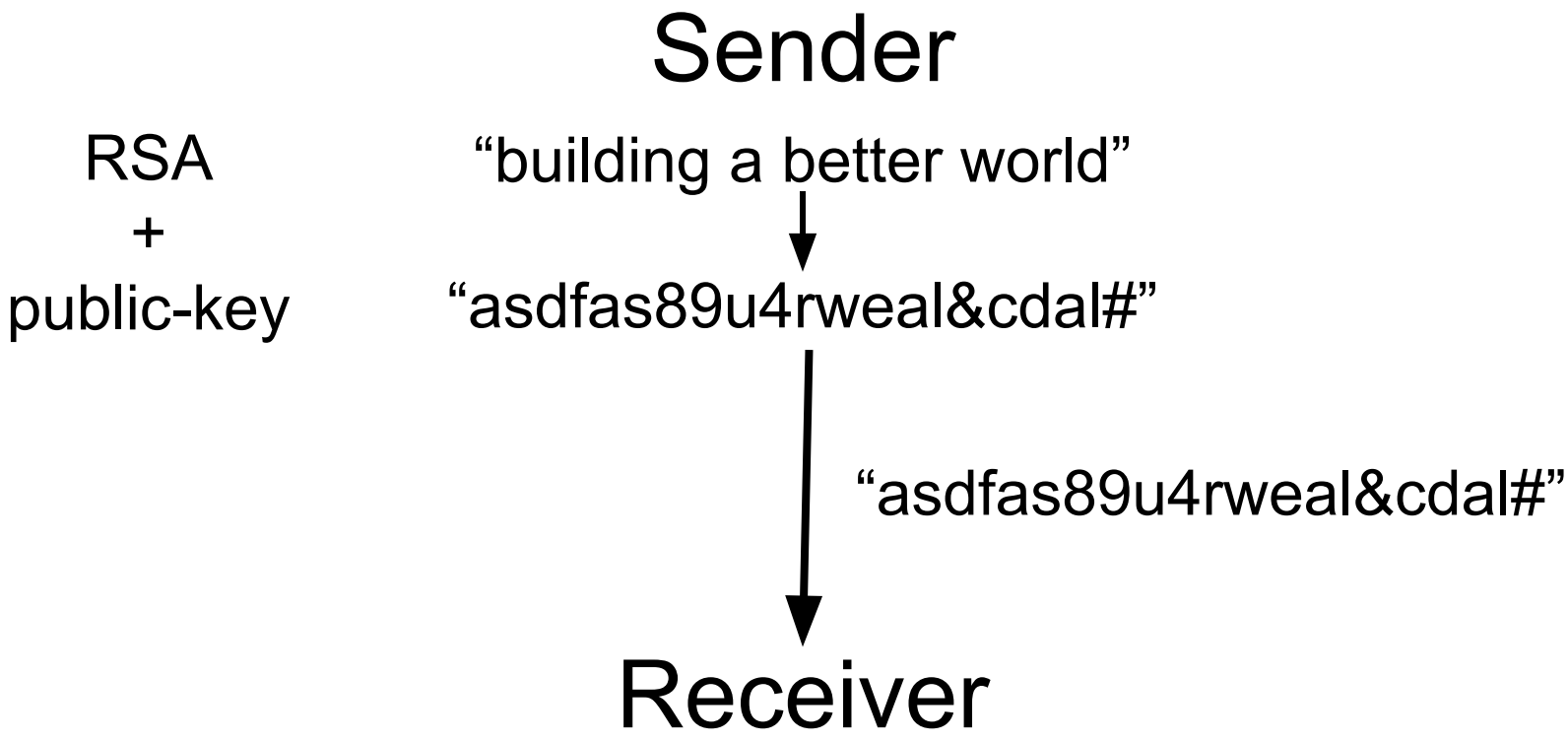
Sender

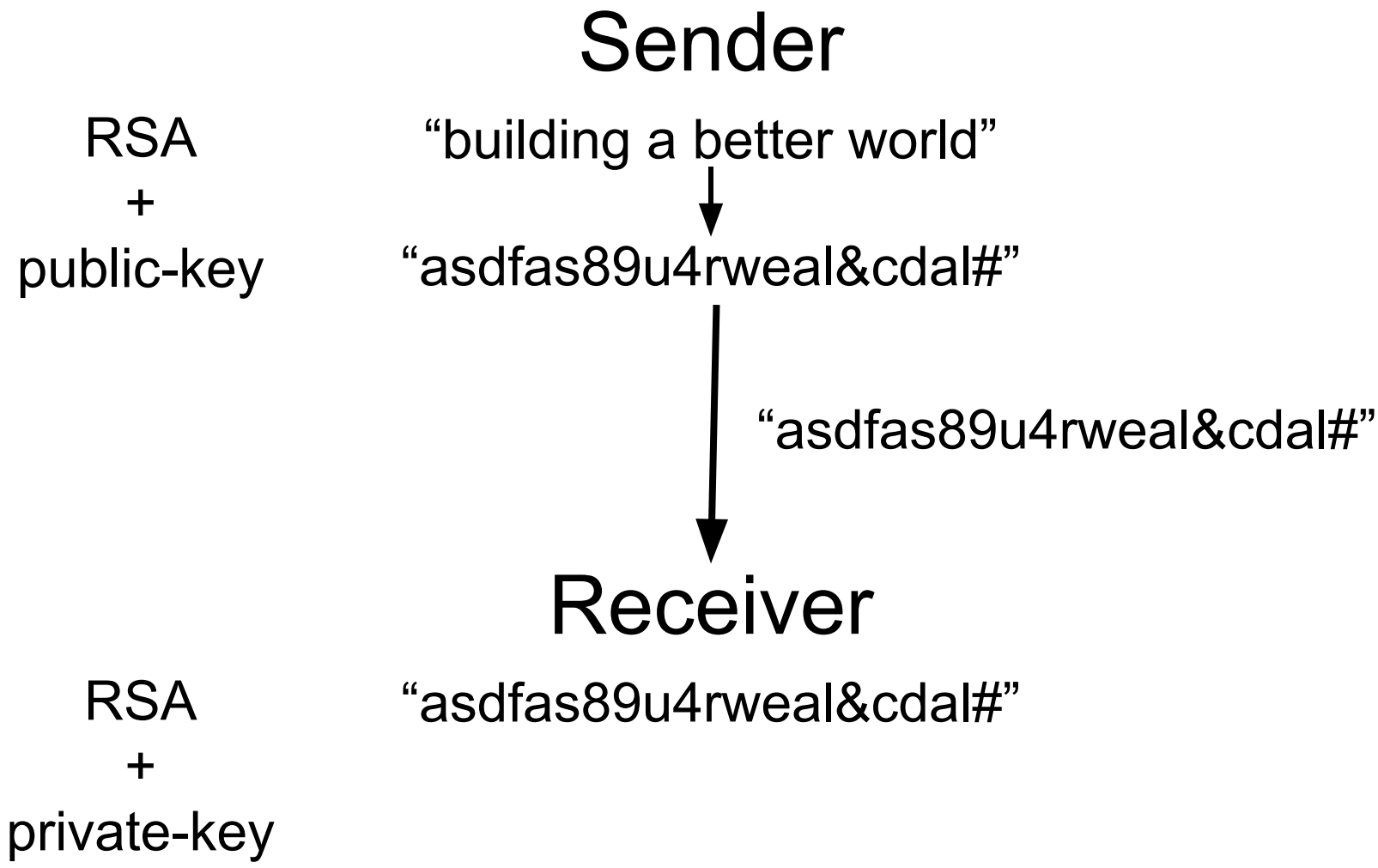
RSA
+
public-key

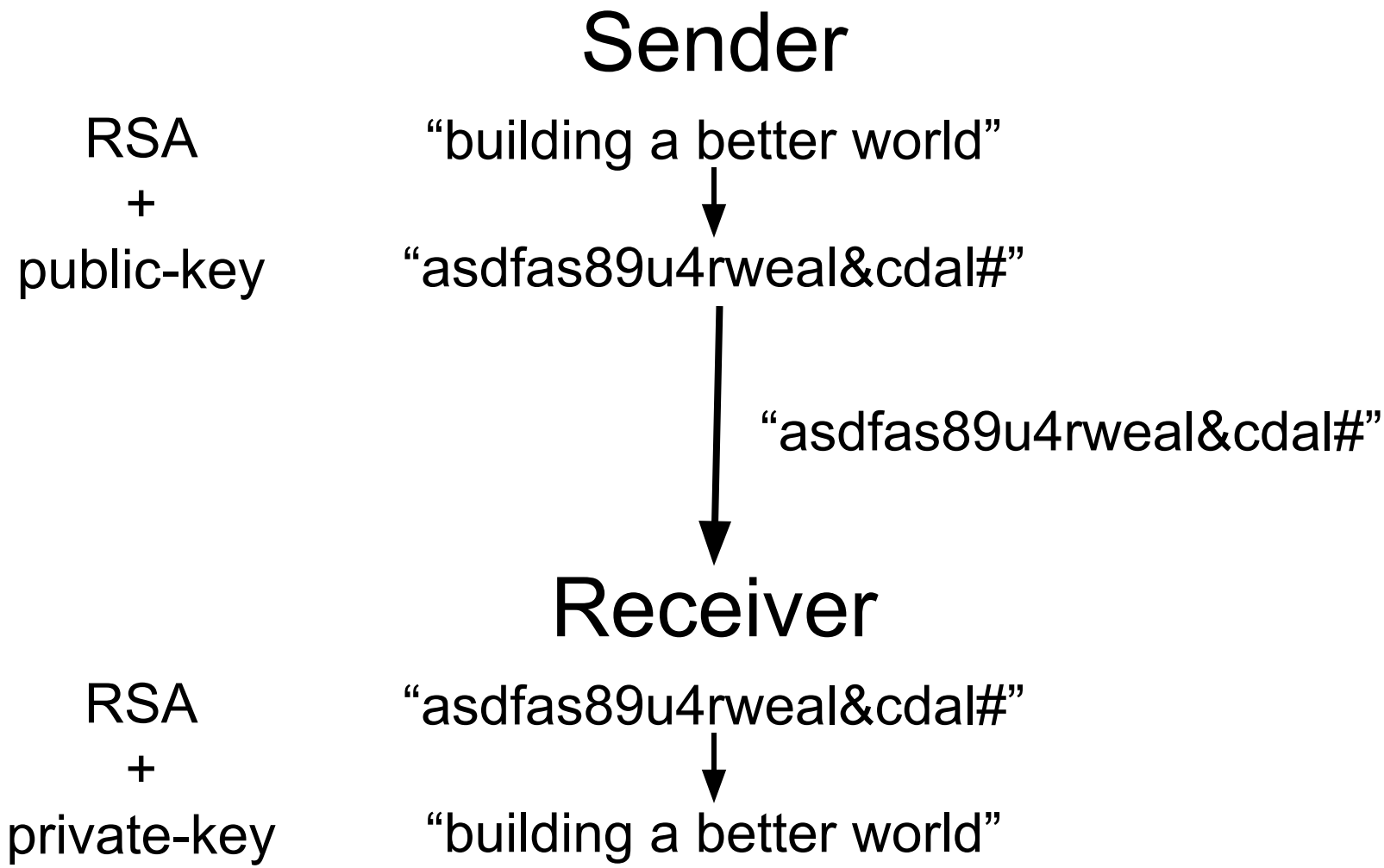
“building a better world”

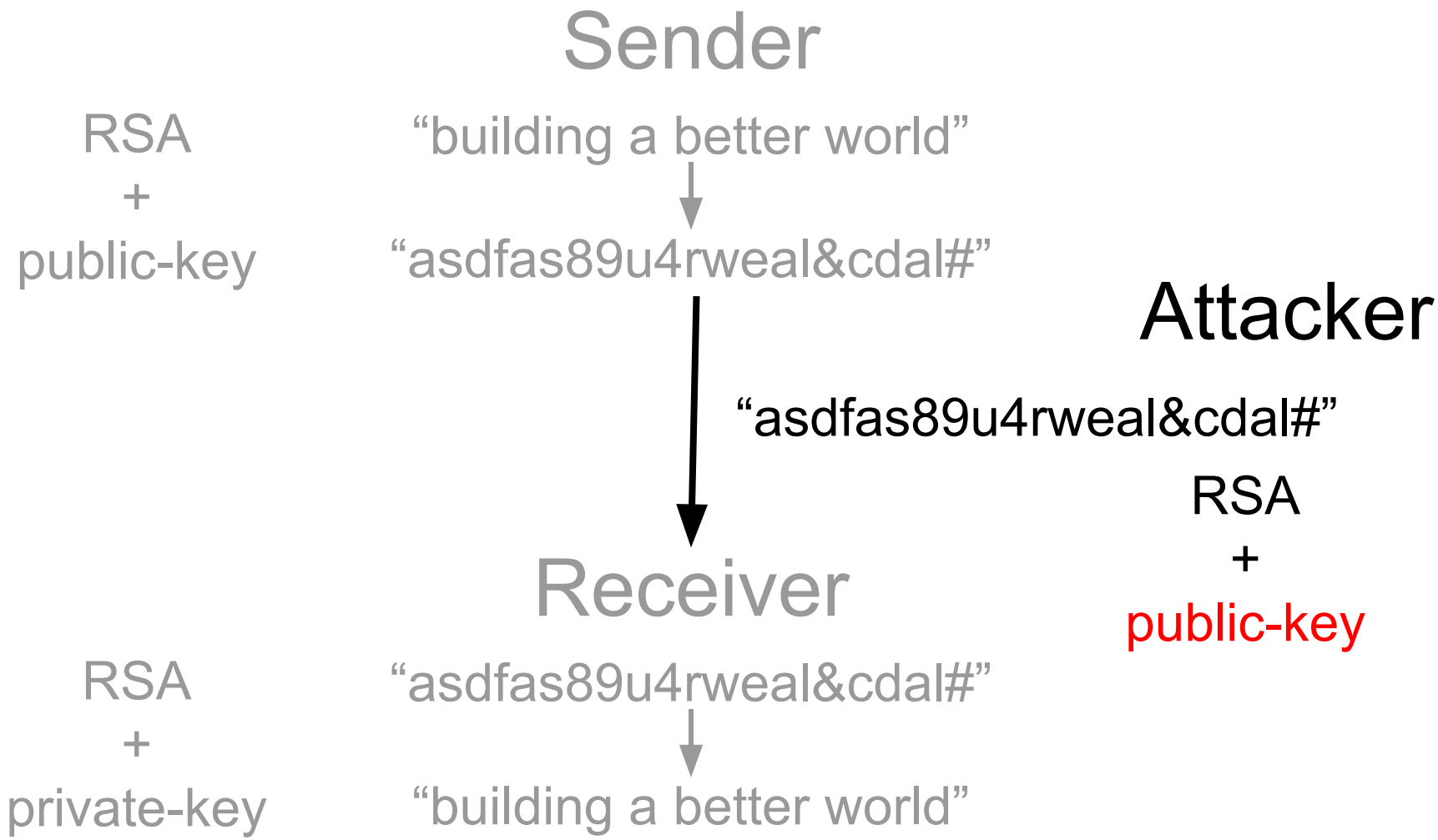
“asdfas89u4rweal&cdal#”

Receiver


Sender
RSA
+
public-key
“building a better world”
“asdfas89u4rweal&cdal#”
“asdfas89u4rweal&cdal#”
Receiver


Sender
RSA
+
public-key
“building a better world”
“asdfas89u4rweal&cdal#”
“asdfas89u4rweal&cdal#”
Receiver
RSA
+
private-key
“asdfas89u4rweal&cdal#”


Sender
RSA
+
public-key
“building a better world”
“asdfas89u4rweal&cdal#”
“asdfas89u4rweal&cdal#”
Receiver
RSA
+
private-key
“asdfas89u4rweal&cdal#”
“building a better world”


Sender
RSA
+
public-key
“building a better world”
“asdfas89u4rweal&cdal#”
Attacker
“asdfas89u4rweal&cdal#”
RSA
+
public-key
Receiver
RSA
+
private-key
“asdfas89u4rweal&cdal#”
“building a better world”

encryption

public-key

decryption

private-key

Symmetric encryption
vs
Asymmetric encryption

Symmetric encryption

1. Shared common Key

Asymmetric encryption

1. Public and Private Key

Symmetric encryption

1. Shared common Key
2. Encryption with shared key

Asymmetric encryption

1. Public and Private Key
2. Encryption with public key

Symmetric encryption

1. Shared common Key
2. Encryption with shared key
3. Decryption with shared key

Asymmetric encryption

1. Public and Private Key
2. Encryption with public key
3. Decryption with private key

Symmetric encryption

1. Shared common Key
2. Encryption with shared key
3. Decryption with shared key
4. Faster

Asymmetric encryption

1. Public and Private Key
2. Encryption with public key
3. Decryption with private key
4. Slower

Symmetric encryption

1. Shared common Key
2. Encryption with shared key
3. Decryption with shared key
4. Faster
5. Less secure

Asymmetric encryption

1. Public and Private Key
2. Encryption with public key
3. Decryption with private key
4. Slower
5. More secure

Certificate

encryption

public-key

decryption

private-key

encryption

private-key

decryption

public-key

encryption

private-key

verification

public-key

Sender

Receiver

Sender

“building a better world”

Receiver

Sender

“building a better world”

private-key +

“sda*dafwgvr!ad”

Receiver

Sender

private-key

“building a better world”
+
“sda*dafwgvr!ad”

“building a better world” +
“sda*dafwgvr!ad”

Receiver

Sender

“building a better world”

private-key +

“sda*dafwgvr!ad”

“building a better world” +
“sda*dafwgvr!ad”

Receiver

“building a better world” + “sda*dafwgvr!ad”

public-key

Sender

“building a better world”

private-key +

“sda*dafwgvr!ad”

“building a better world” +
“sda*dafwgvr!ad”

Receiver

“building a better world” + “sda*dafwgvr!ad”

public-key

verified

HTTP/HTTPS

Client-Server

Client

Server

Browser

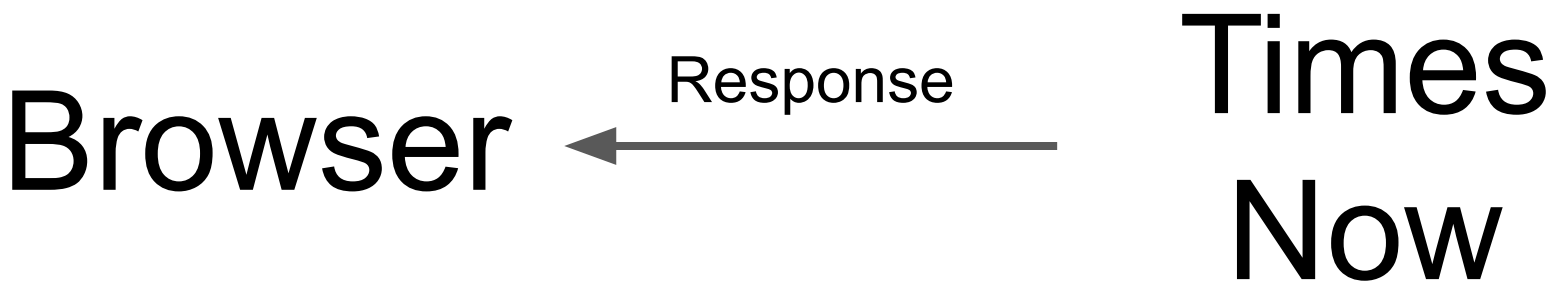
Server

Browser

Times
Now

Browser

Times Now


Browser
Response
Times Now

WhatsApp bug allowed attackers to snoop on private files on victim's iPhone; Facebook says fix rolled out

A vulnerability in WhatsApp Desktop when paired with WhatsApp for iPhone allows cross-site scripting and local file reading. Exploiting the vulnerability requires the victim to click a link preview from a specially crafted text message.

https://www.timesnownews.com/technology-science/article/whatsapp-bug-allowed-attackers-to-snoop-on-private-files-on-victims-iphone-facebook-says-fix-rolled-out/549731

WhatsApp bug allowed attackers to snoop on private files on victim's iPhone; Facebook says fix rolled out

A vulnerability in WhatsApp Desktop when paired with WhatsApp for iPhone allows cross-site scripting and local file reading. Exploiting the vulnerability requires the victim to click a link preview from a specially crafted text message.

READ MORE

<h1>WhatsApp bug allowed attackers to snoop on private files on victim's iPhone; Facebook says fix rolled out</h1>

A vulnerability in WhatsApp Desktop when paired with WhatsApp for iPhone allows cross-site scripting and local file reading. Exploiting the vulnerability requires the victim to click a link preview from a specially crafted text message.

    <button>READ MORE</button>

HTTP HTTPS

WhatsApp has been rated the most secure messaging app

Various cyber security firms have confirmed that Whatsapp is the most secure messaging app.

READ MORE

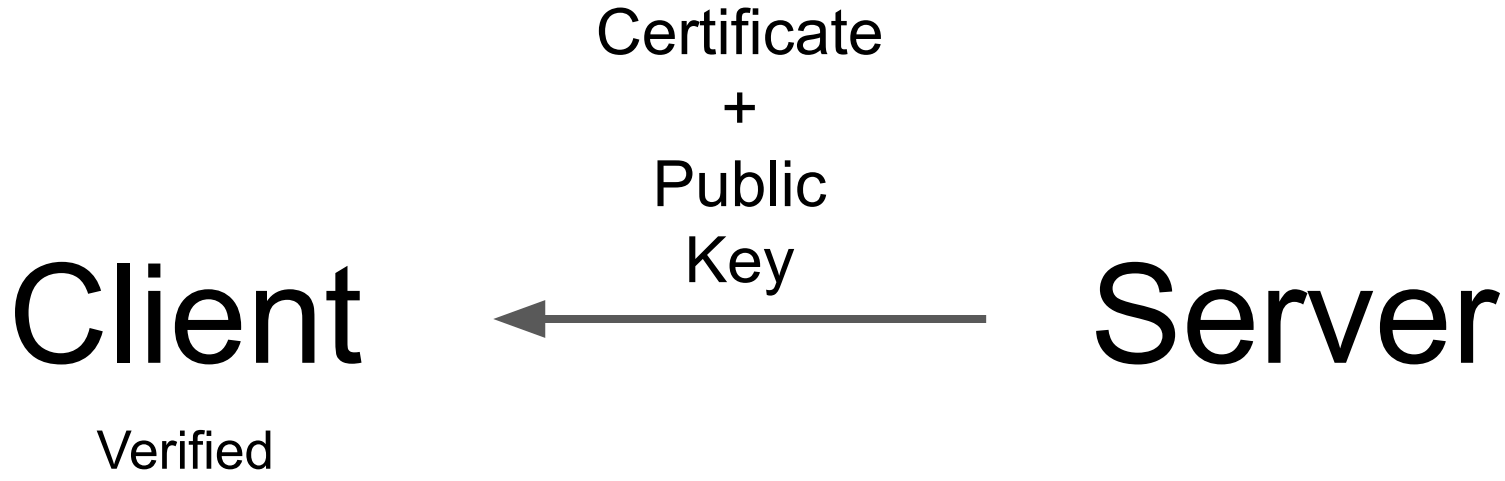

example.com
https://example.com

SSL Certificate

Private Key - Public Key


Client
Request
Server

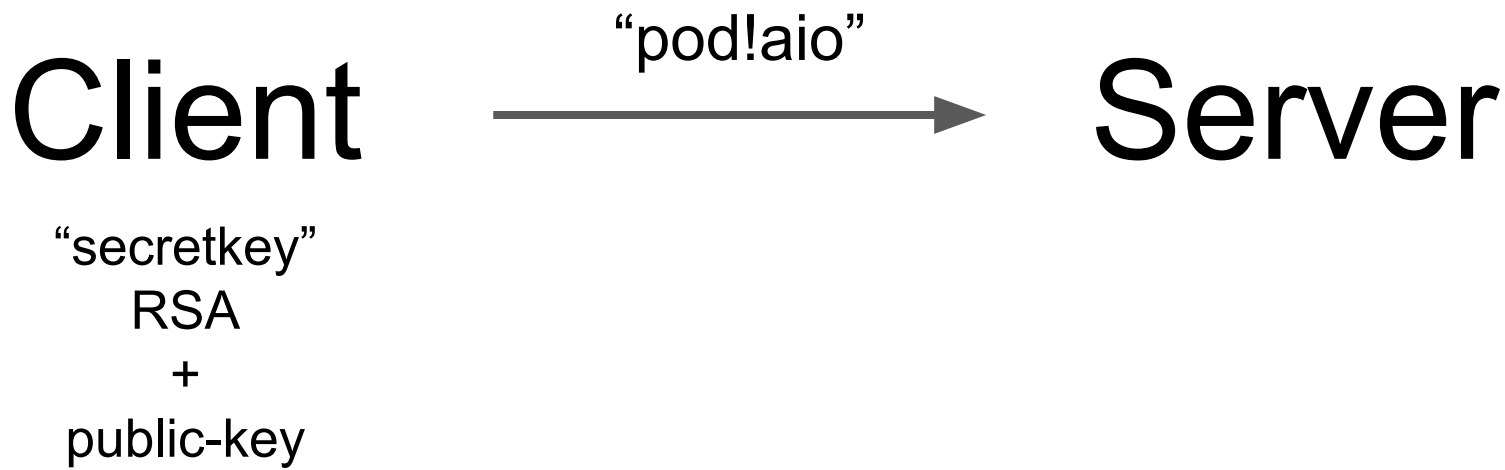

Certificate
+
Public
Key
Client
Server


Certificate
+
Public
Key
Client
Server
Verified

Client

“secretkey”
RSA
+
public-key

Server


Client
“pod!aio”
Server
“secretkey”
RSA
+
public-key


Client
“pod!aio”
Server
“pod!aio”

Client

Server

“pod!aio”
RSA
+
private-key

Client

Server

“secretkey”

Client

“secretkey”

Server

“secretkey”


Sender
AES
+
secret-key
“building a better world”
“asdfas89u4rweal&cdal#”
Attacker
“asdfas89u4rweal&cdal#”
secret-key
AES
+
secret-key
Receiver
AES
+
secret-key
“asdfas89u4rweal&cdal#”
“building a better world”

Asymmetric + Symmetric

Reference

https://www.guru99.com/unix-linux-tutorial.html
https://www.howtogeek.com/117435/htg-explains-the-linux-directory-structure-explained/
https://searchnetworking.techtarget.com/definition/TCP-IP
https://www.geeksforgeeks.org/layers-of-osi-model/
https://en.wikipedia.org/wiki/Internet_protocol_suite
https://en.wikipedia.org/wiki/List_of_network_protocols_(OSI_model)#Layer_7_(Application_Layer)

bhat.dev/workshopnotes.pdf

Download PPT from this link

CIA triangle, OWASP Top 10, JavaScript, Authentication, Authorization, Data Loss Prevention, Virus, Worms and Malware, Recent Cyber Attacks

CIA Triangle


Integrity
Availability
Information
Security
Confidentiality

OWASP Top 10

owasp.org/www-project-top-ten/

JavaScript

w3schools.com

Authentication

Authorization

Authorization

Data Loss Prevention

Malware, Virus and Worms

Recent Cyber Attacks


inshorts
stay informed

t.me/thehackernews