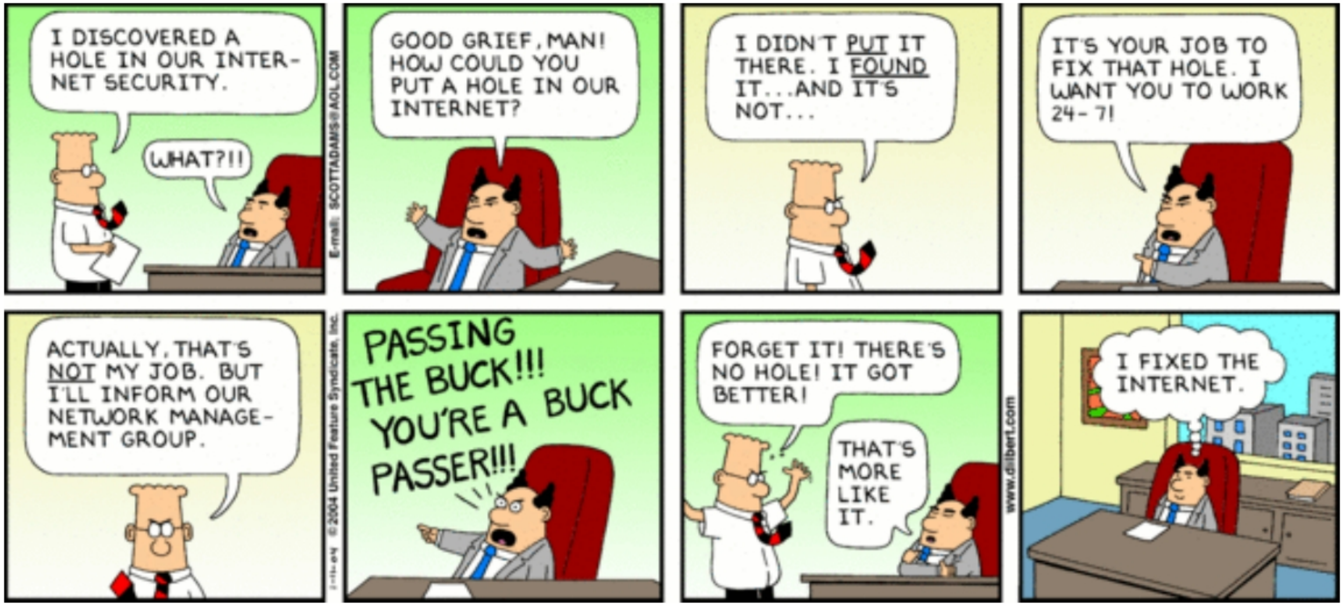
Network Security

Starting as of AS 2016

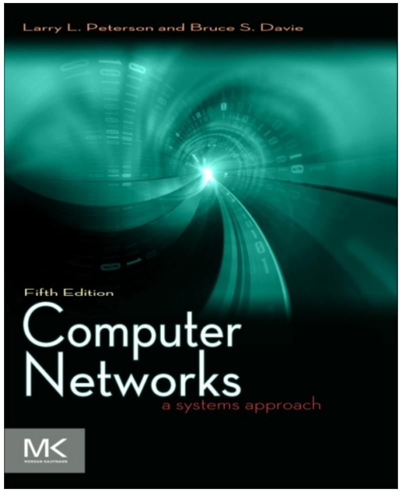
CS-AD-107 Computer Security

Christina Poepper

May 2nd, 2016


I DISCOVERED A HOLE IN OUR INTERNET SECURITY.
WHAT?!!
E-mail: SCOTTADAMS@AOL.COM
GOOD GRIEF, MAN! HOW COULD YOU PUT A HOLE IN OUR INTERNET?
I DIDN'T PUT IT THERE. I FOUND IT... AND IT'S NOT...
IT'S YOUR JOB TO FIX THAT HOLE. I WANT YOU TO WORK 24-7!
ACTUALLY, THAT'S NOT MY JOB. BUT I'LL INFORM OUR NETWORK MANAGEMENT GROUP.
© 2004 United Feature Syndicate, Inc.
PASSING THE BUCK!!! YOU'RE A BUCK PASSER!!!
FORGET IT! THERE'S NO HOLE! IT GOT BETTER!
THAT'S MORE LIKE IT.
www.dilbert.com
I FIXED THE INTERNET.

*http://dilbert.com/strips/comic/2004-01-11/



Acknowledgment / Disclaimer

Slides based on

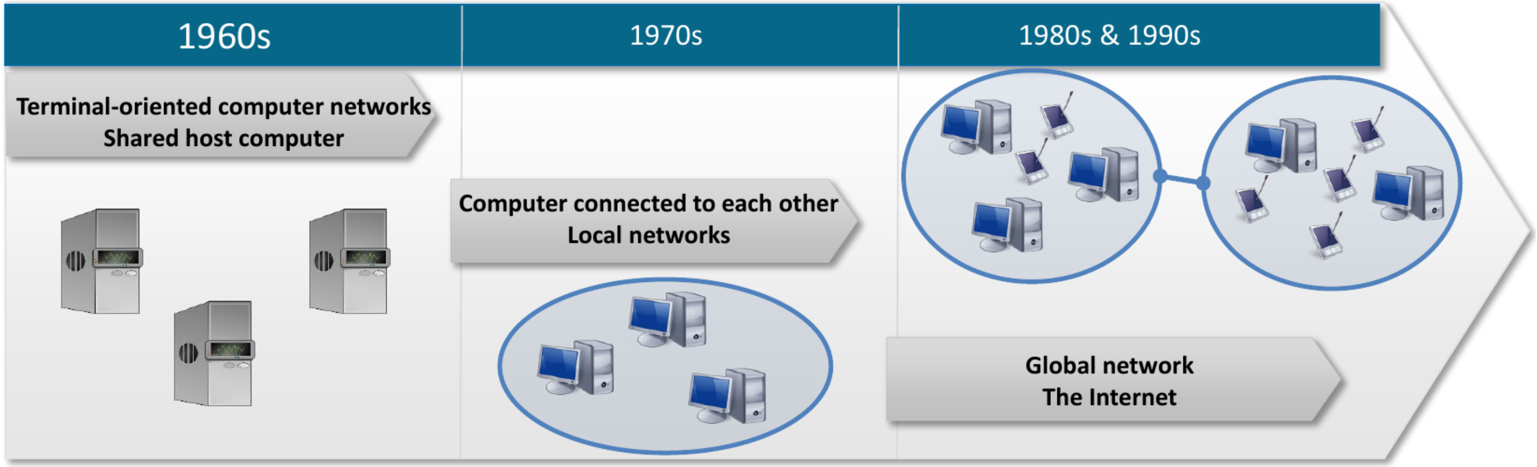
Chapter 8

Network Security

Computer Networks: A Systems Approach, 5e

Larry L. Peterson and Bruce S. Davie

Computer Networks



1960s

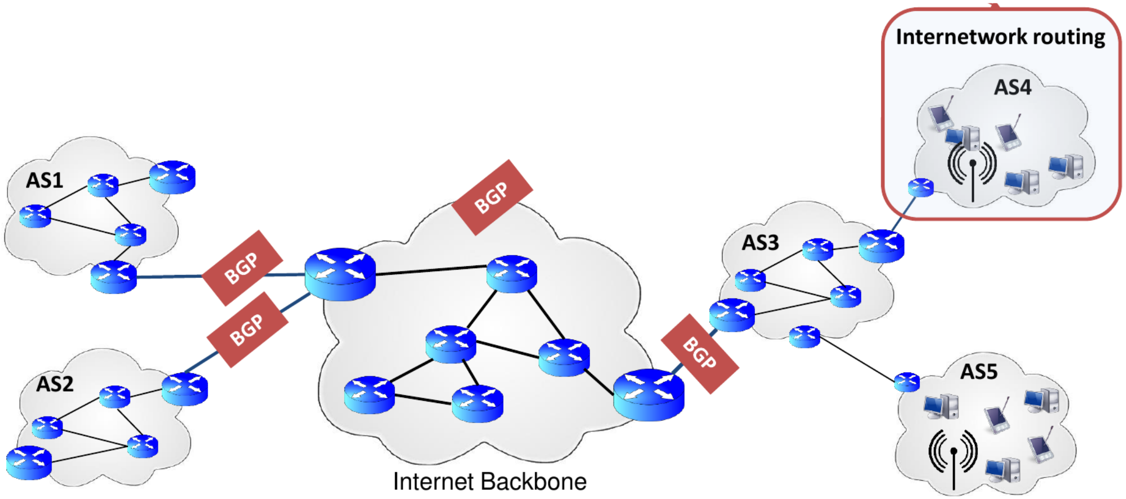
Terminal-oriented computer networks
Shared host computer

1970s

Computer connected to each other
Local networks

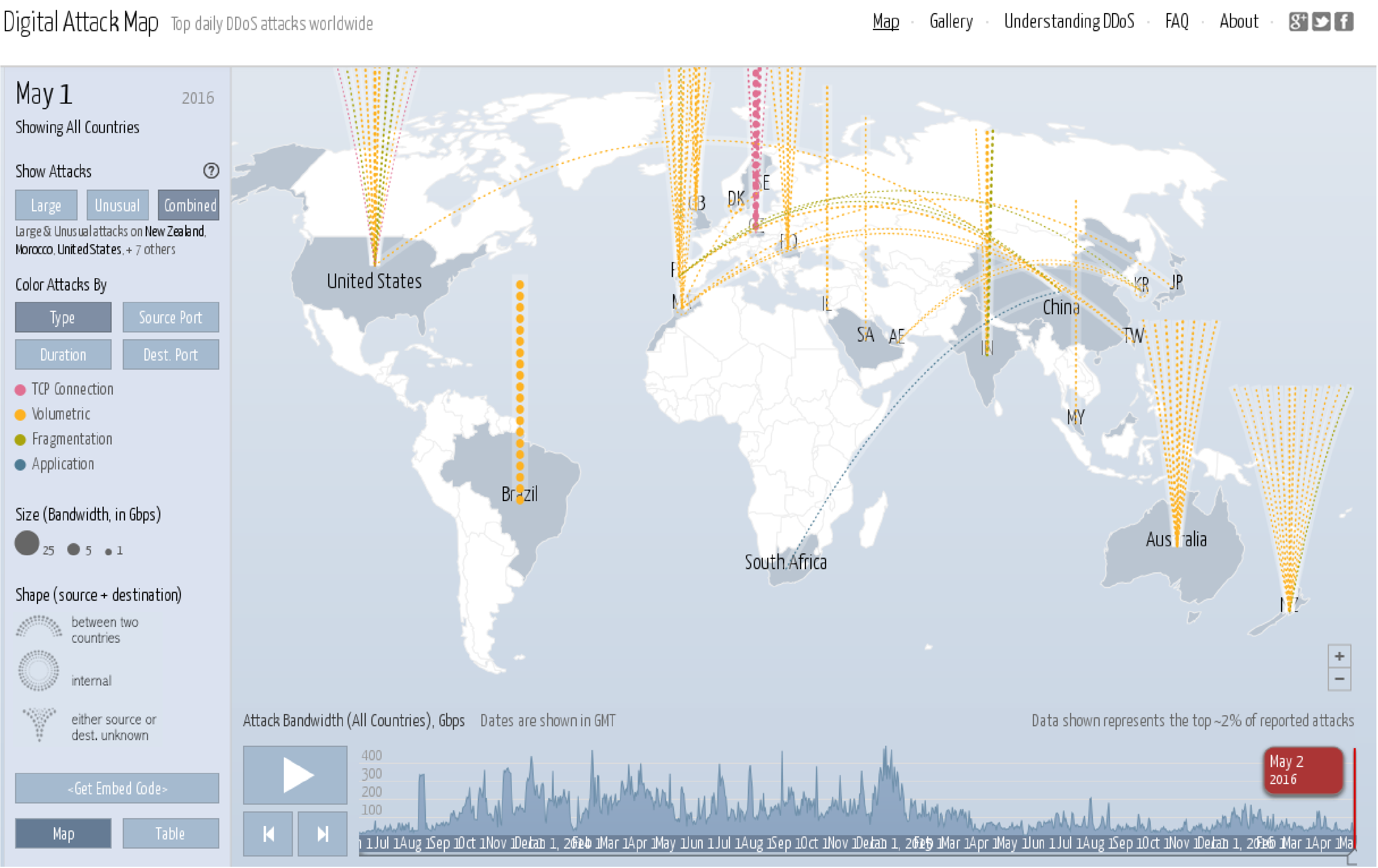
1980s & 1990s

Global network
The Internet



Internetwork routing

World Map of Network Attacks



Digital Attack Map Top daily DDoS attacks worldwide

May 1 2016

Showing All Countries

Show Attacks: Large | Unusual | Combined

Large & Unusual attacks on New Zealand, Morocco, United States, + 7 others

Color Attacks By: Type | Source Port | Duration | Dest. Port

- ● TCP Connection
- ● Volumetric
- ● Fragmentation
- ● Application

Size (Bandwidth, in Gbps): 25, 5, 1

Shape (source + destination): between two countries; internal; either source or dest. unknown

Attack Bandwidth (All Countries), Gbps Dates are shown in GMT

Data shown represents the top ~2% of reported attacks

Map
Gallery
Understanding DDoS
FAQ
About
?
<Get Embed Code>
Map
Table
United States
Brazil
GB
DK
SE
RO
FR
MA
IL
SA
AE
IN
China
KR
JP
TW
MY
South Africa
Australia
NZ
+
−
400
300
200
100
May 2
2016
1 Jul 1 Aug 1 Sep 1 Oct 1 Nov 1 Dec Jan 1, 2014 Feb 1 Mar 1 Apr 1 May 1 Jun 1 Jul 1 Aug 1 Sep 1 Oct 1 Nov 1 Dec Jan 1, 2015 Feb 1 Mar 1 Apr 1 May 1 Jun 1 Jul 1 Aug 1 Sep 1 Oct 1 Nov 1 Dec Jan 1, 2016 Feb 1 Mar 1 Apr 1 Ma

http://map.ipviking.com/

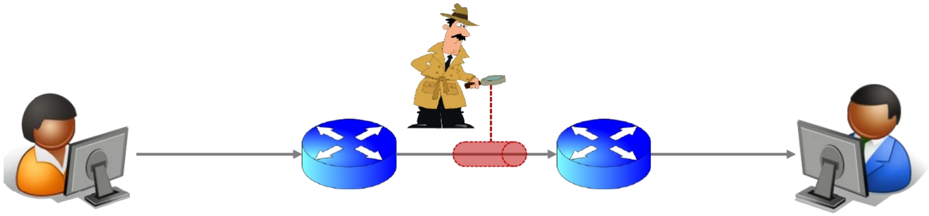
http://www.digitalattackmap.com/

Problem

- Computer networks are typically a shared resource used by many applications representing different interests.
- The Internet is particularly widely shared, being used by competing businesses, mutually antagonistic governments, and opportunistic criminals.
- Unless security measures are taken, a network conversation or a distributed application may be compromised by an adversary.

Problem

- Consider threats to the secure use of the World Wide Web.
  - Suppose you are a customer using a credit card to order an item from a website.

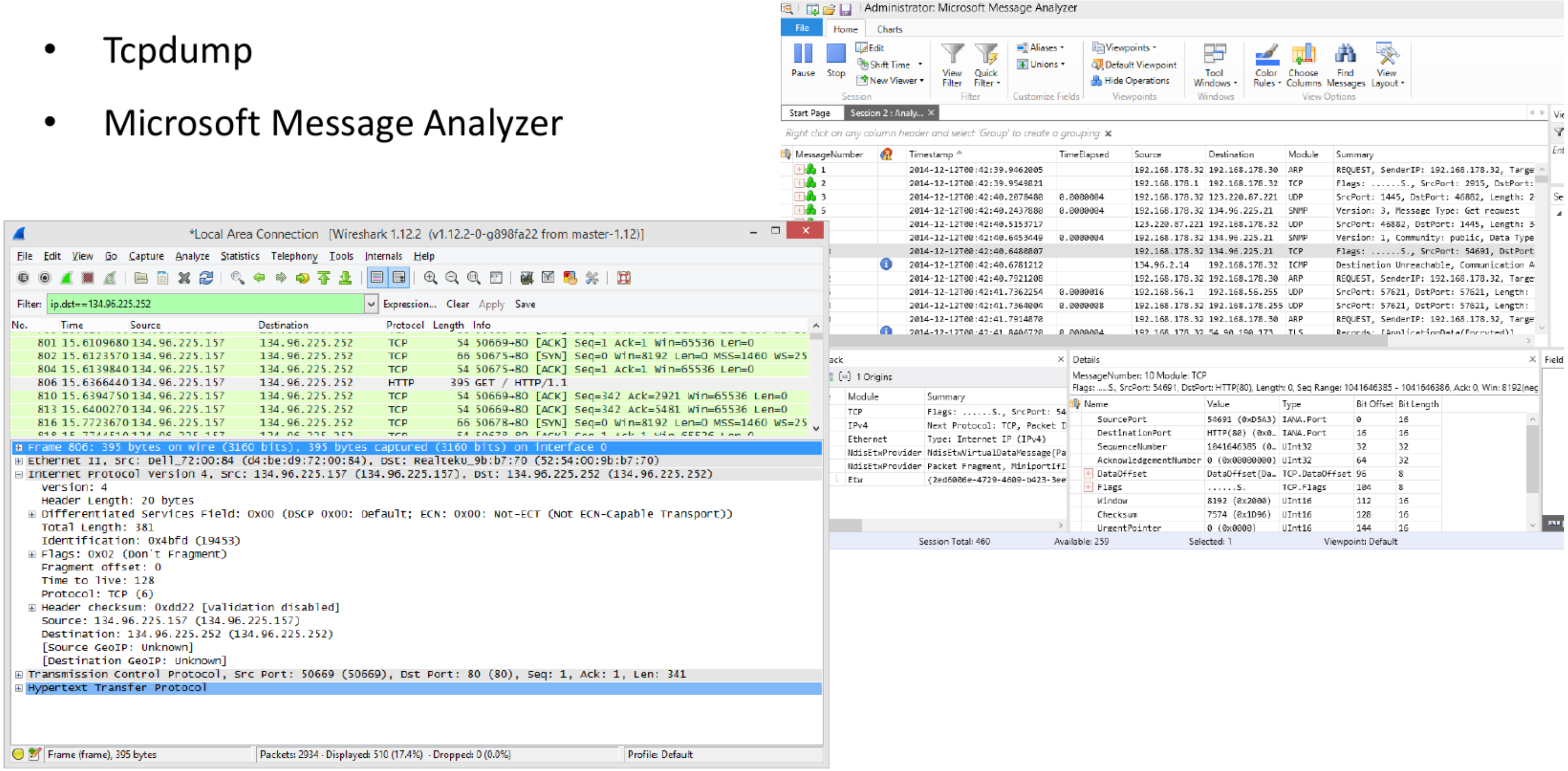


    - An obvious threat is that an adversary would eavesdrop on your network communication, reading your messages to obtain your credit card information.
    - It is possible and practical, however, to encrypt messages so as to prevent an adversary from understanding the message contents. A protocol that does so is said to provide *confidentiality*.
    - Taking the concept a step farther, concealing the quantity or destination of communication is called *traffic confidentiality*

Network Sniffing Tools

Popular tools for network sniffing (legally: analyzing):

- Wireshark
- Tcpdump
- Microsoft Message Analyzer



Filter: ip.dst==134.96.225.252

```
No.   Time       Source          Destination     Protocol Length Info
  801 15.6109680 134.96.225.157  134.96.225.252  TCP        54 50669→80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  802 15.6123570 134.96.225.157  134.96.225.252  TCP        66 50675→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=25
  804 15.6139840 134.96.225.157  134.96.225.252  TCP        54 50675→80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  806 15.6366440 134.96.225.157  134.96.225.252  HTTP      395 GET / HTTP/1.1
  810 15.6394750 134.96.225.157  134.96.225.252  TCP        54 50669→80 [ACK] Seq=342 Ack=2921 Win=65536 Len=0
  813 15.6400270 134.96.225.157  134.96.225.252  TCP        54 50669→80 [ACK] Seq=342 Ack=5481 Win=65536 Len=0
  816 15.7723670 134.96.225.157  134.96.225.252  TCP        66 50678→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=25
```

```
⊞ Frame 806: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface 0
⊞ Ethernet II, Src: Dell_72:00:84 (d4:be:d9:72:00:84), Dst: Realteku_9b:b7:70 (52:54:00:9b:b7:70)
⊟ Internet Protocol Version 4, Src: 134.96.225.157 (134.96.225.157), Dst: 134.96.225.252 (134.96.225.252)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 381
    Identification: 0x4bfd (19453)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  ⊞ Header checksum: 0xdd22 [validation disabled]
    Source: 134.96.225.157 (134.96.225.157)
    Destination: 134.96.225.252 (134.96.225.252)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊞ Transmission Control Protocol, Src Port: 50669 (50669), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 341
⊞ Hypertext Transfer Protocol
```

Frame (frame), 395 bytes | Packets: 2934 · Displayed: 510 (17.4%) · Dropped: 0 (0.0%) | Profile: Default

```
MessageNumber  Timestamp                    TimeElapsed  Source          Destination      Module  Summary
1              2014-12-12T00:42:39.9462005               192.168.178.32  192.168.178.30   ARP     REQUEST, SenderIP: 192.168.178.32, Targe
2              2014-12-12T00:42:39.9549821               192.168.178.1   192.168.178.32   TCP     Flags: ......S., SrcPort: 2915, DstPort:
3              2014-12-12T00:42:40.2078480  0.0000004    192.168.178.32  123.220.87.221   UDP     SrcPort: 1445, DstPort: 46882, Length: 2
5              2014-12-12T00:42:40.2437880  0.0000004    192.168.178.32  134.96.225.21    SNMP    Version: 3, Message Type: Get request
               2014-12-12T00:42:40.5153717               123.220.87.221  192.168.178.32   UDP     SrcPort: 46882, DstPort: 1445, Length: 3
               2014-12-12T00:42:40.6453449  0.0000004    192.168.178.32  134.96.225.21    SNMP    Version: 1, Community: public, Data Type
               2014-12-12T00:42:40.6480807               192.168.178.32  134.96.225.21    TCP     Flags: ......S., SrcPort: 54691, DstPort
               2014-12-12T00:42:40.6781212               134.96.2.14     192.168.178.32   ICMP    Destination Unreachable, Communication A
               2014-12-12T00:42:40.7921208               192.168.178.32  192.168.178.30   ARP     REQUEST, SenderIP: 192.168.178.32, Targe
               2014-12-12T00:42:41.7362254  0.0000016    192.168.56.1    192.168.56.255   UDP     SrcPort: 57621, DstPort: 57621, Length:
               2014-12-12T00:42:41.7364004  0.0000008    192.168.178.32  192.168.178.255  UDP     SrcPort: 57621, DstPort: 57621, Length:
               2014-12-12T00:42:41.7914870               192.168.178.32  192.168.178.30   ARP     REQUEST, SenderIP: 192.168.178.32, Targe
```

1 Origins

```
Module            Summary
TCP               Flags: ......S., SrcPort: 54
IPv4              Next Protocol: TCP, Packet I
Ethernet          Type: Internet IP (IPv4)
NdisEtwProvider   NdisEtwVirtualDataMessage{Pa
NdisEtwProvider   Packet Fragment, MiniportIfI
Etw               {2ed6006e-4729-4609-b423-3ee
```

Details

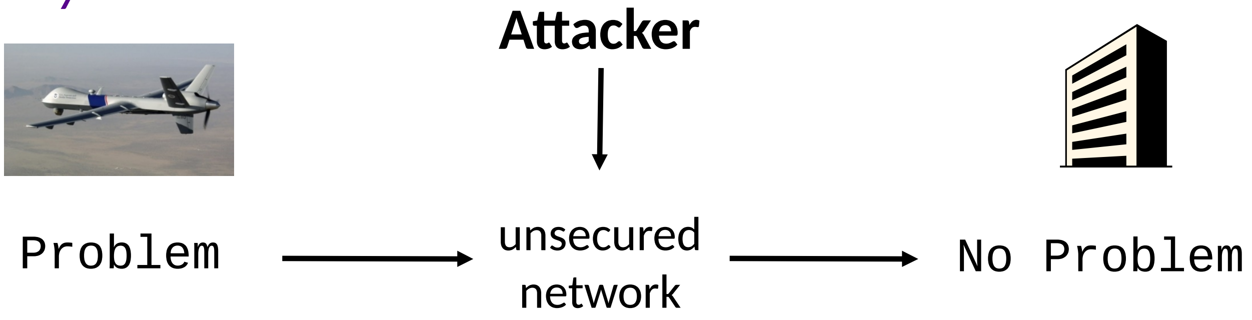
MessageNumber: 10 Module: TCP
Flags: ......S., SrcPort: 54691, DstPort: HTTP(80), Length: 0, Seq Range: 1041646385 - 1041646386, Ack: 0, Win: 8192(neg

```
Name                    Value               Type            Bit Offset  Bit Length
SourcePort              54691 (0xD5A3)      IANA.Port       0           16
DestinationPort         HTTP(80) (0x0…      IANA.Port       16          16
SequenceNumber          1041646385 (0…      UInt32          32          32
AcknowledgementNumber   0 (0x00000000)      UInt32          64          32
⊞ DataOffset            DataOffset{Da…      TCP.DataOffset  96          8
⊞ Flags                 ......S.            TCP.Flags       104         8
Window                  8192 (0x2000)       UInt16          112         16
Checksum                7574 (0x1D96)       UInt16          128         16
UrgentPointer           0 (0x0000)          UInt16          144         16
```

Session Total: 460 | Available: 259 | Selected: 1 | Viewpoint: Default

Problem

- Even with confidentiality there still remain threats for the website customer.
  - An adversary who can’t read the contents of your encrypted message might still be able to change a few bits in it, resulting in a valid order for, say, a completely different item or perhaps 1000 units of the item.
  - There are techniques to detect, if not prevent, such tampering.
  - A protocol that detects such message tampering provides *data integrity*.



Attacker

Problem → unsecured network → No Problem

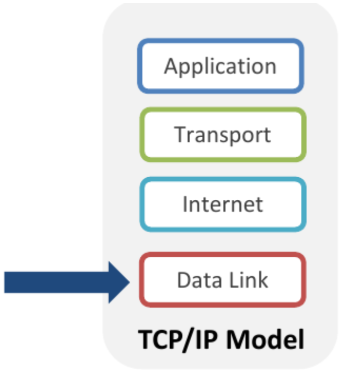
Problem

- The adversary could alternatively transmit an extra copy of your message in a *replay attack*.
- To the website, it would appear as though you had simply ordered another of the same item you ordered the first time.
  - A protocol that detects replays provides *originality*.
  - Originality would not, however, preclude the adversary intercepting your order, waiting a while, then transmitting it—in effect, delaying your order.
  - The adversary could thereby arrange for the item to arrive on your doorstep while you are away on vacation, when it can be easily snatched. A protocol that detects such delaying tactics is said to provide *timeliness*.
- Data integrity, originality, and timeliness are considered aspects of the more general property of integrity.

Problem

- Another threat to the customer is unknowingly being directed to a false website.
  - This can result from a DNS attack, in which false information is entered in a Domain Name Server or the name service cache of the customer’s computer.
  - This leads to translating a correct URL into an incorrect IP address—the address of a false website.
  - A protocol that ensures that you really are talking to whom you think you’re talking is said to provide *authentication*.
  - *Authentication entails integrity since it is meaningless* to say that a message came from a certain participant if it is no longer the same message.

Address Resolution Protocol (Link Layer)



Application

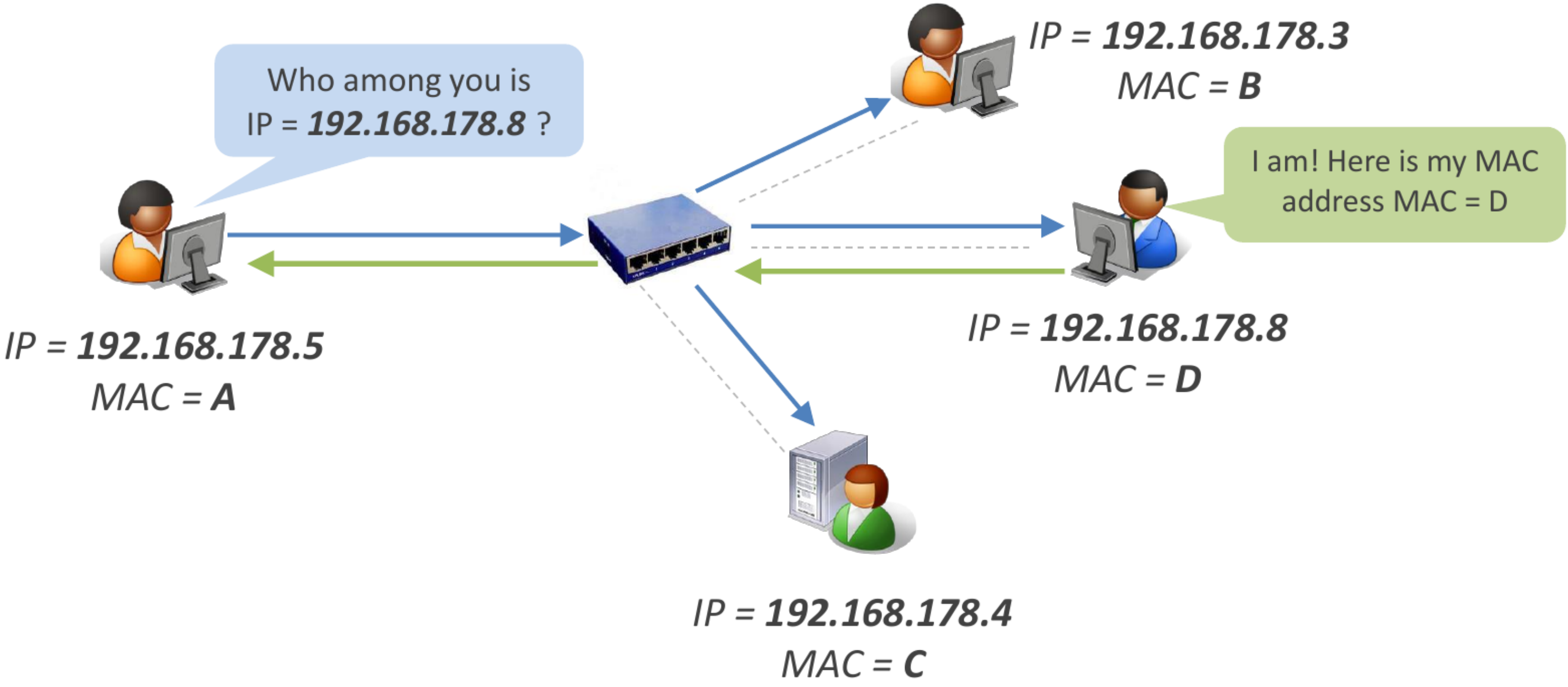
Transport

Internet

Data Link

TCP/IP Model

- Address Resolution Protocol (ARP)
  - Mapping an IP address to a physical machine address (MAC)
  - ARP cache



Who among you is IP = ***192.168.178.8*** ?

IP = ***192.168.178.3***
MAC = ***B***

I am! Here is my MAC address MAC = D

IP = ***192.168.178.5***
MAC = ***A***

IP = ***192.168.178.8***
MAC = ***D***

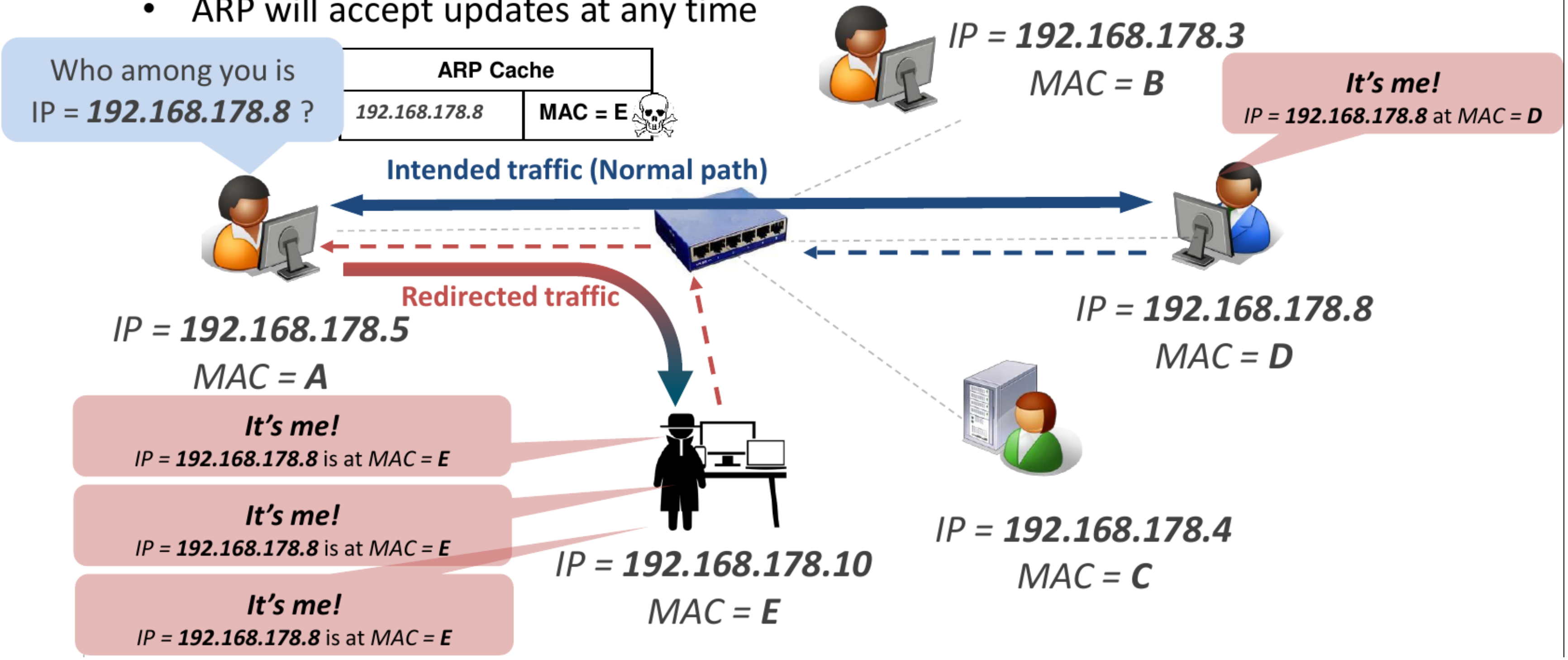
IP = ***192.168.178.4***
MAC = ***C***

Address Resolution Protocol (Link Layer)

ARP protocol is insecure!

ARP Spoofing

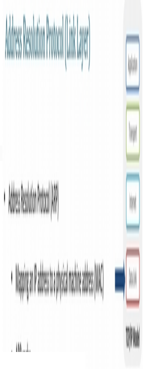
- ARP replies with forged IP address
- Man-in-the-middle attack (MITM)
- ARP will accept updates at any time

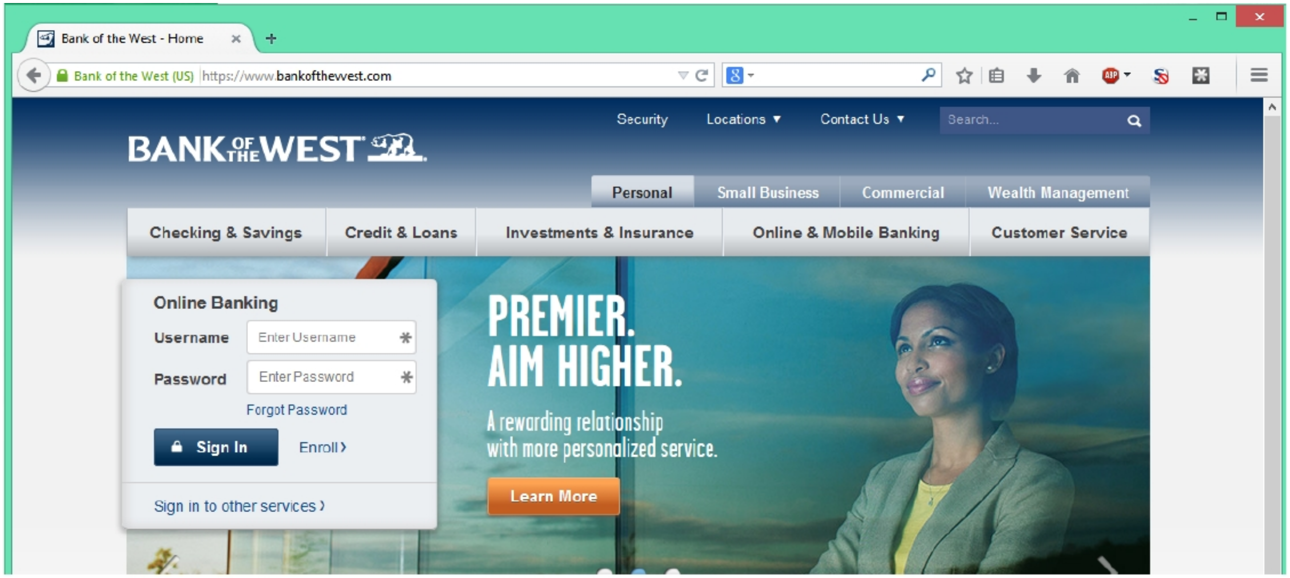


Who among you is IP = *192.168.178.8* ?
Intended traffic (Normal path)
Redirected traffic
IP = *192.168.178.5* MAC = *A*
IP = *192.168.178.3* MAC = *B*
It's me! IP = *192.168.178.8* at MAC = *D*
IP = *192.168.178.8* MAC = *D*
IP = *192.168.178.4* MAC = *C*
IP = *192.168.178.10* MAC = *E*
It's me! IP = *192.168.178.8* is at MAC = *E*
It's me! IP = *192.168.178.8* is at MAC = *E*
It's me! IP = *192.168.178.8* is at MAC = *E*

ARP Cache	
192.168.178.8	MAC = E ☠

Phishing (Application Layer)





Bank of the West - Home

Bank of the West (US) https://www.bankofthevvest.com

Security | Locations ▼ | Contact Us ▼ | Search...

BANK OF THE WEST

Personal | Small Business | Commercial | Wealth Management

Checking & Savings | Credit & Loans | Investments & Insurance | Online & Mobile Banking | Customer Service

Online Banking

Username: Enter Username

Password: Enter Password

Forgot Password

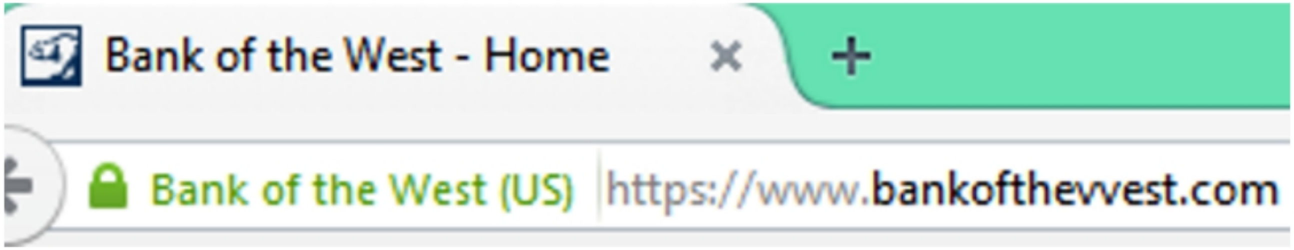
Sign In | Enroll ›

Sign in to other services ›

PREMIER.
AIM HIGHER.

A rewarding relationship
with more personalized service.

Learn More



Bank of the West - Home

Bank of the West (US) https://www.bankofthevvest.com

...but is not!

Problem

- The owner of the website can be attacked as well. Some websites have been defaced; the files that make up the website content have been remotely accessed and modified without authorization.
- That is an issue of *access control*: *enforcing the rules* regarding who is allowed to do what.

- Websites have also been subject to Denial of Service (DoS) attacks, during which would-be customers are unable to access the website because it is being overwhelmed by bogus requests.
- Ensuring a degree of access is called *availability*.

Problem

- In addition to these issues, the Internet has notably been used as a means for deploying malicious code that exploits vulnerabilities in end-systems.
- *Worms, pieces of* self-replicating code that spread over networks, have been known for several decades and continue to cause problems, as do their relatives, *viruses, which are spread by the* transmission of “infected” files.
- Infected machines can then be arranged into *botnets* which can be used to inflict further harm, such as launching DoS attacks.

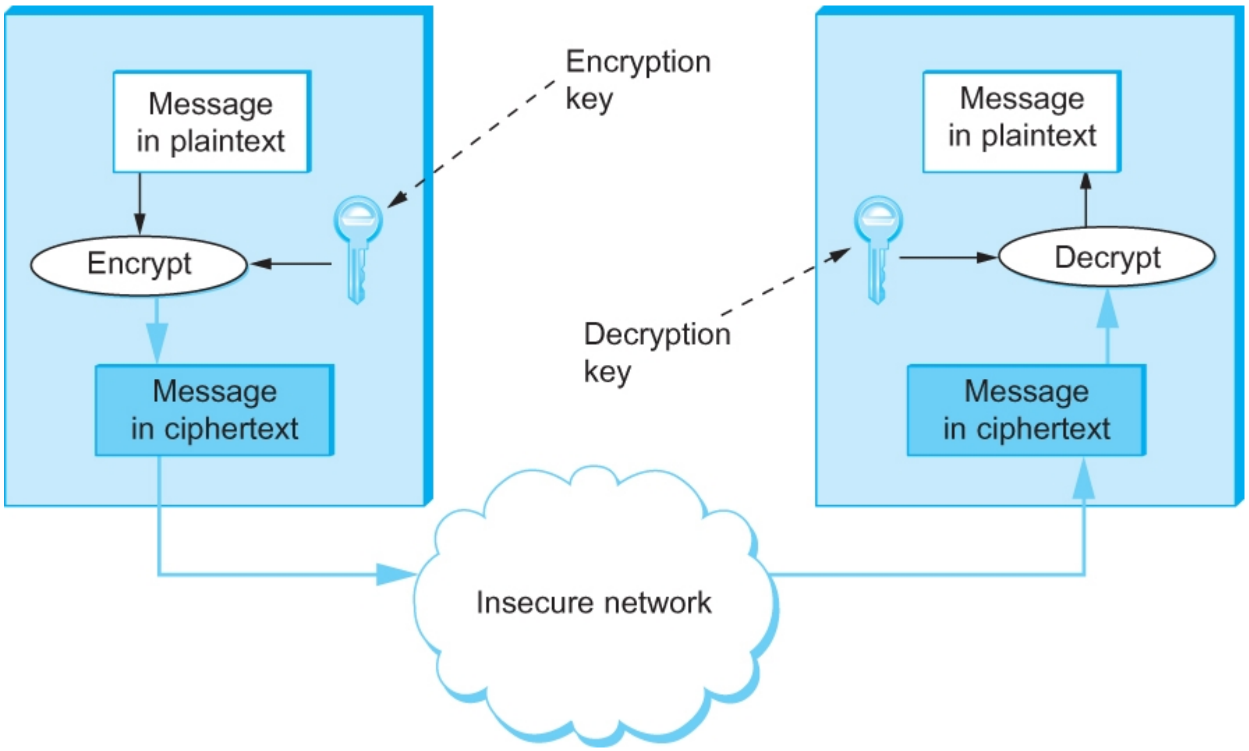
Chapter Outline

- Cryptographic Building Blocks
- Key Pre Distribution
- Authentication Protocols
- Example Systems
- Firewalls

Cryptographic Building Blocks

- We introduce the concepts of cryptography-based security step by step.
- The first step is the cryptographic algorithms—ciphers and cryptographic hashes
- Cryptographic algorithms are parameterized by *keys*

Cryptographic Building Blocks



Symmetric-key encryption and decryption

Cryptographic Building Blocks

- Principles of Ciphers
  - Encryption transforms a message in such a way that it becomes unintelligible to any party that does not have the secret of how to reverse the transformation.
  - The sender applies an *encryption function to the original plaintext message, resulting in a ciphertext* message that is sent over the network.
  - The receiver applies a secret *decryption function–the inverse of the encryption function–to recover the original* plaintext.

Cryptographic Building Blocks

- Principles of Ciphers
  - The ciphertext transmitted across the network is unintelligible to any eavesdropper, assuming she doesn’t know the decryption function.
  - The transformation represented by an encryption function and its corresponding decryption function is called a *cipher*.
  - The basic requirement for an encryption algorithm is that it turn plaintext into ciphertext in such a way that only the intended recipient—the holder of the decryption key—can recover the plaintext.

Cryptographic Building Blocks

- Principles of Ciphers
  - It is important to realize that when a potential attacker receives a piece of ciphertext, he may have more information at his disposal than just the ciphertext itself.
  - Known plaintext attack
  - Ciphertext only attack
  - Chosen plaintext attack

Cryptographic Building Blocks

- Principles of Ciphers
  - Most ciphers are *block ciphers: they are defined to take as input a plaintext block* of a certain fixed size, typically 64 to 128 bits.
  - Using a block cipher to encrypt each block independently—known as *electronic codebook (ECB) mode encryption—has the* weakness that a given plaintext block value will always result in the same ciphertext block.
  - Hence recurring block values in the plaintext are recognizable as such in the ciphertext, making it much easier for a cryptanalyst to break the cipher.

Cryptographic Building Blocks

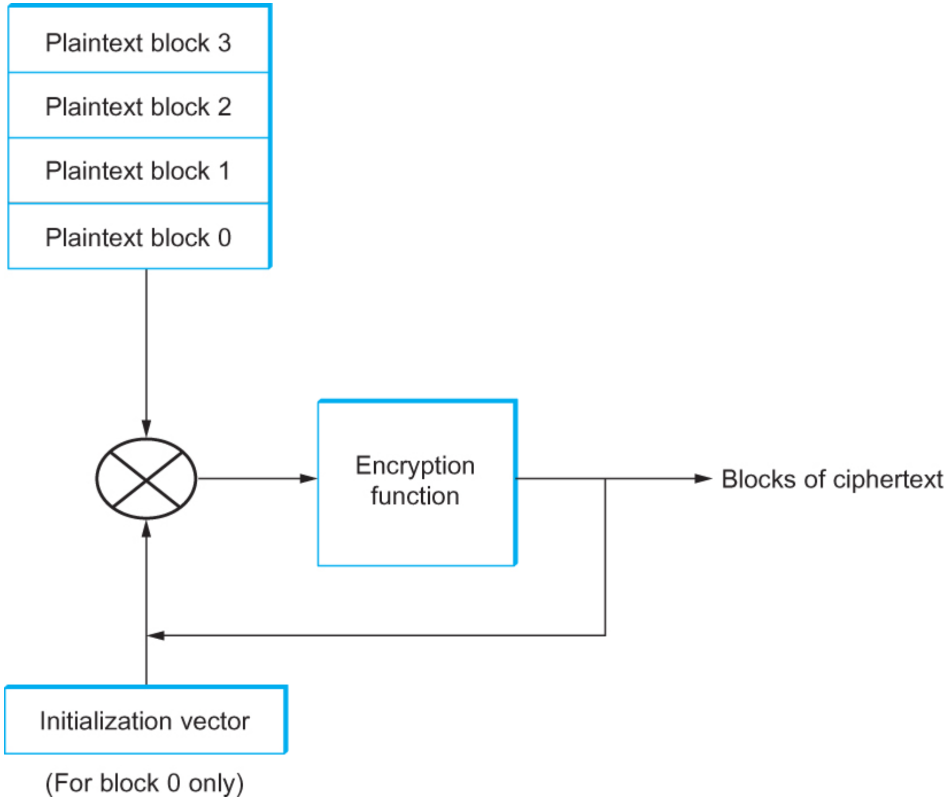
- Principles of Ciphers
  - Block ciphers are always augmented to make the ciphertext for a block vary depending on context. Ways in which a block cipher may be augmented are called *modes of operation*.

Cryptographic Building Blocks

- Block Ciphers
  - *A common mode of operation is cipher block chaining* (CBC), in which each plaintext block is XORed with the previous block’s ciphertext before being encrypted.
    - The result is that each block’s ciphertext depends in part on the preceding blocks, i.e. on its context. Since the first plaintext block has no preceding block, it is XORed with a random number.
      - That random number, called an *initialization vector (IV), is included with the series of ciphertext blocks so that the first ciphertext* block can be decrypted.

Cryptographic Building Blocks

- Block Ciphers



Cipher block chaining (CBC).

Cryptographic Building Blocks

- Symmetric Key Ciphers
  - In a symmetric-key cipher, both participants in a communication share the same key. In other words, if a message is encrypted using a particular key, the same key is required for decrypting the message.

Cryptographic Building Blocks

- Symmetric Key Ciphers
  - The U.S. National Institute of Standards and Technology (NIST) has issued standards for a series of symmetric-key ciphers.
  - *Data Encryption Standard (DES) was the* first, and it has stood the test of time in that no cryptanalytic attack better than brute force search has been discovered.
  - Brute force search, however, has gotten faster. DES's keys (56 independent bits) are now too small given current processor speeds.

Cryptographic Building Blocks

- Symmetric Key Ciphers
  - NIST also standardized the cipher *Triple DES (3DES), which leverages the cryptanalysis resistance* of DES while in effect increasing the key size.
  - A 3DES key has 168 (= 3x56) independent bits, and is used as three DES keys;
    - let's call them DES-key1, DES-key2, and DES-key3.
    - 3DES-encryption of a block is performed by first DES-encrypting the block using DES-key1, then DES-*decrypting the result using DES-key2, and finally* DES-encrypting that result using DES-key3.
    - Decryption involves decrypting using DES-key3, then encrypting using DES-key2, then decrypting using DES-key1

Cryptographic Building Blocks

- Symmetric Key Ciphers
  - 3DES is being superseded by the *Advanced Encryption Standard (AES) standard* issued by NIST in 2001.
  - The cipher selected to become that standard (with a few minor modifications) was originally named Rijndael (pronounced roughly like “Rhine dahl”) based on the names of its inventors, Daemen and Rijmen.
  - AES supports key lengths of 128, 192, or 256 bits, and the block length is 128 bits.

Cryptographic Building Blocks

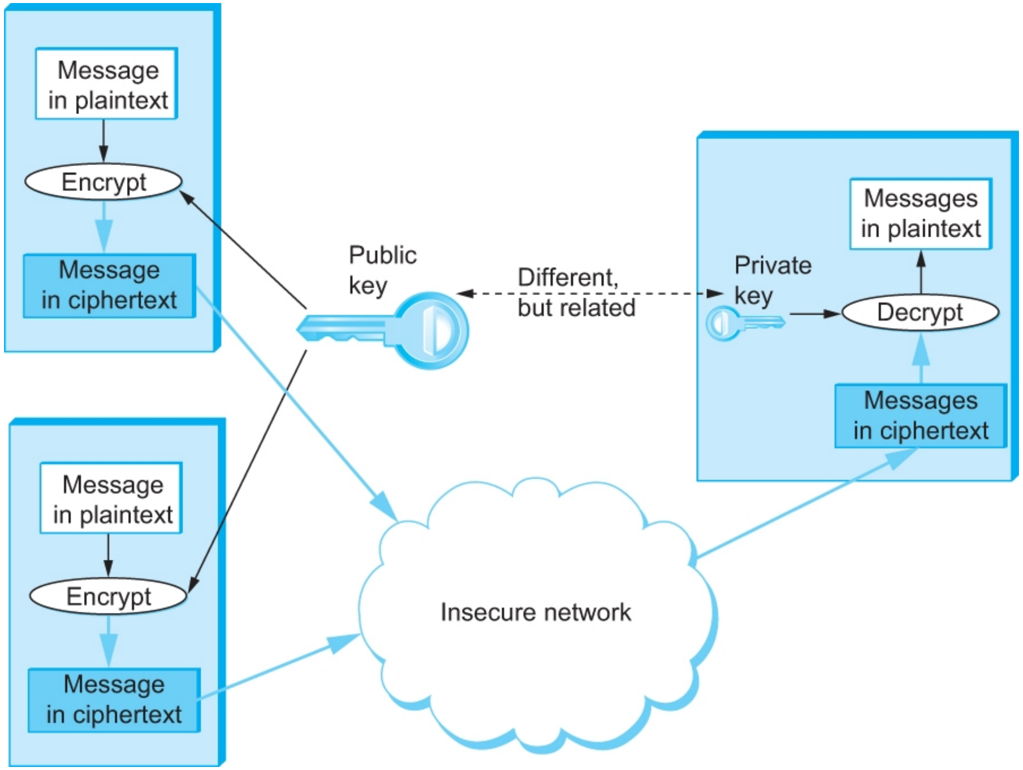
- Public Key Ciphers
  - An alternative to symmetric-key ciphers is asymmetric, or public-key, ciphers.
  - Instead of a single key shared by two participants, a public-key cipher uses a pair of related keys, one for encryption and a different one for decryption.
  - The pair of keys is “owned” by just one participant.
  - The owner keeps the decryption key secret so that only the owner can decrypt messages; that key is called the *private key*.

Cryptographic Building Blocks

- Public Key Ciphers
  - The owner makes *the* encryption key public, so that anyone can encrypt messages for the owner; that key is called the *public key.*
  - Obviously, for such a scheme to work it must not be possible to deduce the private key from the public key.
  - Consequently any participant can get the public key and send an encrypted message to the owner of the keys, and only the owner has the private key necessary to decrypt it.

Cryptographic Building Blocks

- Public Key Ciphers



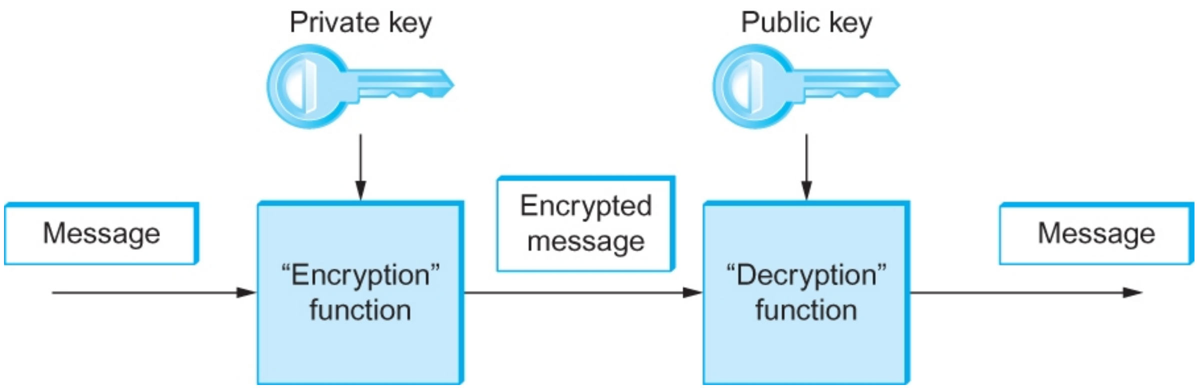
Public-key encryption

Cryptographic Building Blocks

- Public Key Ciphers
  - An important additional property of public-key ciphers is that the private “decryption” key can be used with the encryption algorithm to encrypt messages so that they can only be decrypted using the public “encryption” key.
  - This property clearly wouldn’t be useful for confidentiality since anyone with the public key could decrypt such a message.
  - This property is, however, useful for authentication since it tells the receiver of such a message that it could only have been created by the owner of the keys.

Cryptographic Building Blocks

- Public Key Ciphers



Authentication using public keys

Cryptographic Building Blocks

- Public Key Ciphers
  - The concept of public-key ciphers was first published in 1976 by Diffie and Hellman.
  - The best-known public-key cipher is RSA, named after its inventors: Rivest, Shamir, and Adleman.
    - RSA relies on the high computational cost of factoring large numbers.
  - Another public-key cipher is ElGamal.
    - Like RSA, it relies on a mathematical problem, the discrete logarithm problem, for which no efficient solution has been found, and requires keys of at least 1024 bits.