TNE20003 - Internet and Cybersecurity for Engineering Applications

Network Security Technologies

Outline of Lecture Content

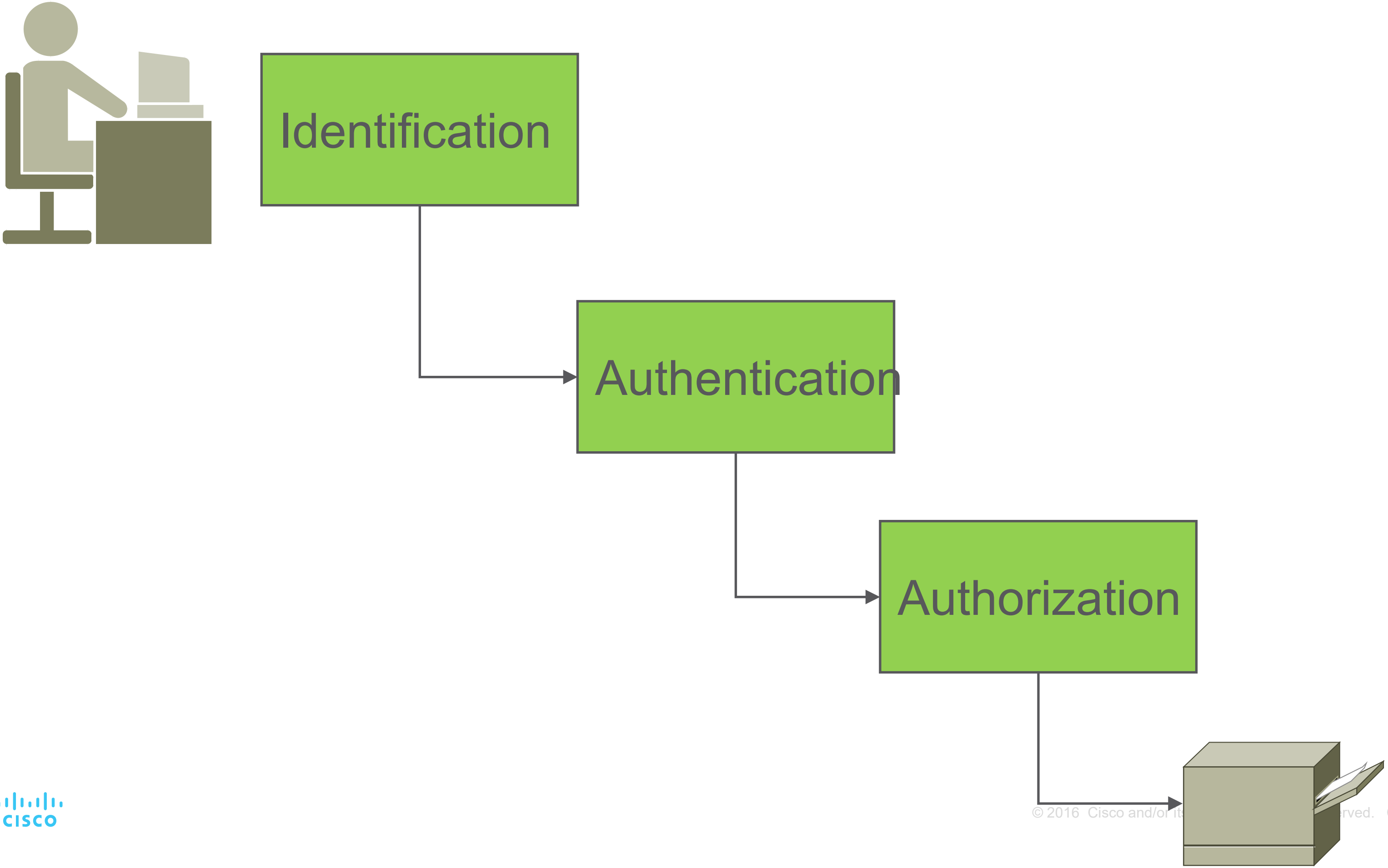
- Access control
- VPNs
- Intrusion Detection and Prevention Systems
- Cryptography

Access Control

Access Control

- Key concepts of Access Control
  - Subject
    - Some entity such as a process, user or program who wants access to some resource
  - Identification
    - A method of linking a subject to an identity. Identification may include user ids, account numbers. Needs to be distinguished from authentication
  - Authentication
    - Additional information validating the identification. Examples might be a password, biometric, PIN, anatomical attribute, token
  - Authorization
    - A method of ensuring the authenticated entity accesses only those resources it is entitled to

Access Control



Identification

Authentication

Authorization

Authentication

- Purpose of authentication
  - Enables high degree of certainty as to the identity of the other party
- Authentication ties an identity to a secret
  - Sometimes the system to whom the individual is attempting to gain access knows the secret
  - Sometimes the system to whom the individual is attempting to gain access knows something derived from the secret
- We need authentication to prove our identity when we want to use some resource or another party wants to be sure we are who we claim to be

Multifactor authentication

- Usually two out of three factors necessary for satisfactory level of authentication
  - Something one knows
    - Password, pass-phrase, PIN number
  - Something one has
    - Credit card, Driver’s license, Smart card, USB security dongle, one-time-password generator
  - Something one is
    - Biometrics
- Some biometrics have been poorly accepted
  - Some acceptance of fingerprint systems on laptops
  - Strong resistance to retinal scans, DNA scans and similar
- Usually a pass-phrase and an authentication token

Hash functions

- A trapdoor function
  - Given a particular value X, a hash system does a one-way transformation to produce the hash f(X)
  - Knowing f(X) it is impossible to determine X
  - A small change in X leads to a big change in f(X)
    - On average, a single bit change in X should change 50% of the bits in f(X)

- MD5, SHA-1 and SHA-2 are well known and commonly used hash functions
  - 128 bits for MD5; 160 bits for SHA-1.
  - SHA-2 is a family of functions able to generate hashes of 224, 256, 384 or 512 bits

SHA

Philip	d9acbb0d8ec837efe80c92fc791abd04ea27d57a
Philip (space appended)	25dbd5be5294338381feb46d4f9f56accbd66cf7
Philip.	cd4e7cf17d3327ef9d05ac67c9bdc082c5c90c32
Phillip	95021406637b46dbf42b5b83a5dcf5ba4f1137f1

Passwords and pass-phrases

- You know what passwords are
  - A few comments…
- User passwords are usually poorly chosen
  - Date of birth, daughter's name, friend's name
  - Can be broken easily with a dictionary attack or through social engineering
- Machine generated passwords
  - Much more difficult to attack
  - BUT much more difficult to remember
- An interesting comment on passwords
  - http://xkcd.com/936
- And a counterview
  - http://www.wired.co.uk/news/archive/2013-05/28/password-cracking

Networked device authentication

- Handsets connecting to mobile phone network
- Routers connecting to each other via PPP
- Remote user connecting a VPN server
- Bluetooth device pairing with another device
- All of these use a technique of authentication based on Challenge - Response

Challenge response protocols

- CHAP over the Point-to-Point Protocol (PPP)
- Cellular networks
  - 4G cellular uses 4G EPS-AKA
  - 5G uses 5G-AKA
- Bluetooth uses E1 algorithm
- WiFi uses WPA or WPA2
- All of these are Challenge Response protocols

Challenge response protocols

1. One device (the Authenticatee) requests to connect to another device (the Authenticator). Both devices share a secret: a key or passphrase

2. The Authenticator sends a "challenge" message to the Authenticatee

3. The Authenticatee responds with a value calculated using a "one-way hash" function and the shared secret

4. The Authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged and connection is provided; otherwise the connection is terminated.

Network Access Server (NAS)

- For most networks, access beyond the PPP termination point is controlled by a NAS
- The NAS is a gateway to guard access to the Internet
- The client connects to the NAS (typically by PPP). The NAS then connects to another resource asking whether the client's supplied credentials are valid. Based on that answer the NAS then allows or disallows access to the Internet or whatever service is being requested.
- The NAS usually contains no information about what clients can connect to or what credentials are valid. All the NAS does is send the credentials the client supplied to a resource which does know how to process the credentials.
- Usually a RADIUS server

Remote Access Dial-In User Service (RADIUS)

- Used in association with a network access server for authentication of users

- Client server model
  - NAS is a client of the RADIUS server

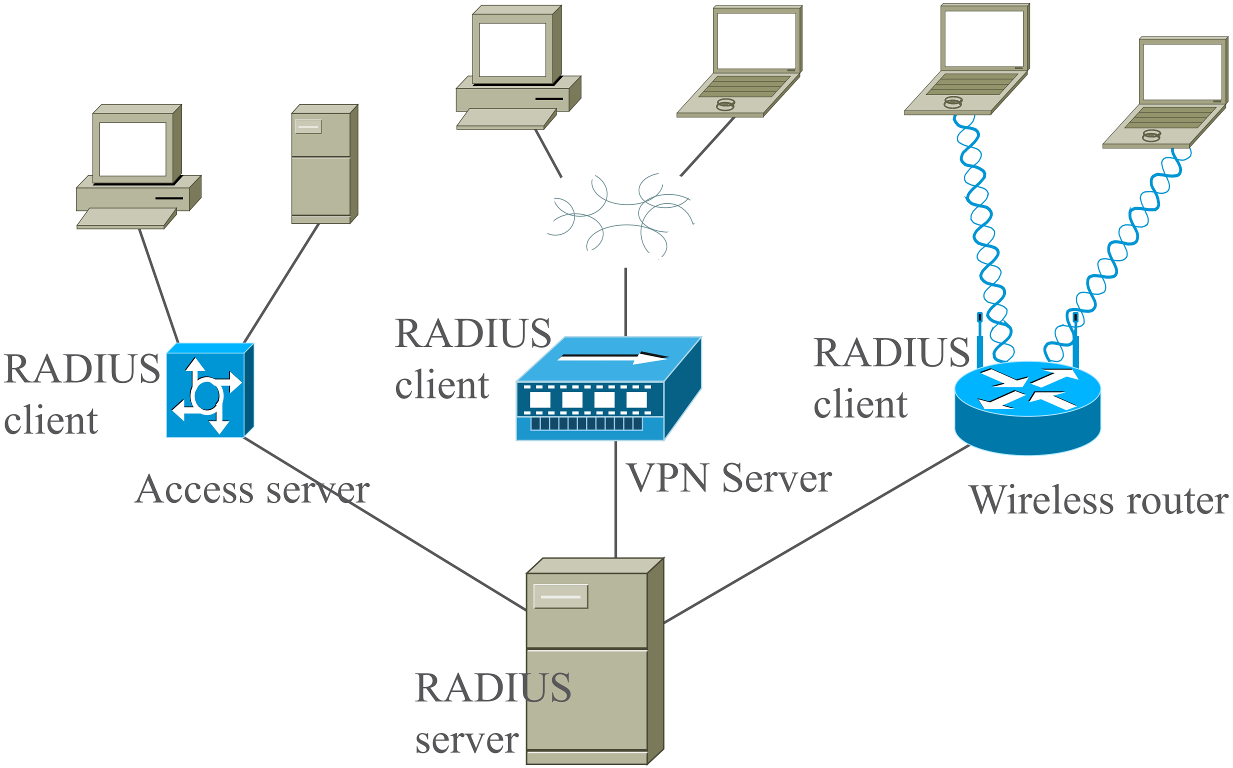
- Receives user connection requests
  - Authenticates users

- Works with PAP and CHAP
- RFC2865
- RADIUS can be used with a any server requiring authentication including VPN servers or Wireless Access Points

Operation of RADIUS

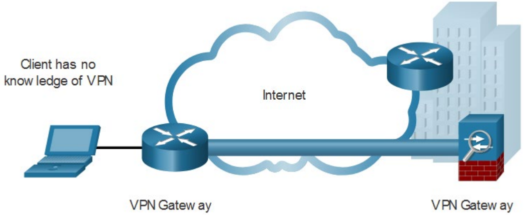
1. User connects to NAS with PPP and initiates authentication by the NAS
2. NAS communicates with RADIUS for authentication details
3. NAS asks client for ID and Password (PAP) or response to challenge phrase (CHAP)
4. User replies
5. RADIUS client on NAS sends ID and password (PAP) or challenge response (CHAP) to server
6. RADIUS server responds with Accept, Reject or Challenge
7. The RADIUS client on the NAS either accepts or rejects the authentication request from the user based on the RADIUS response

RADIUS and NAS



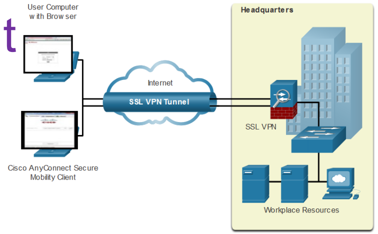
VPNs

Introduction to VPNs

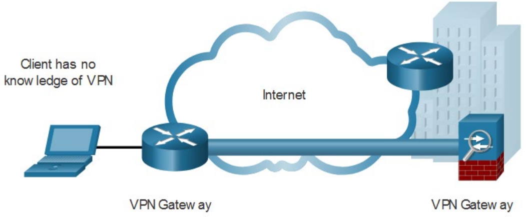


- Virtual Private Network
  - Makes use of publicly available networking infrastructure to provide the features of a private network

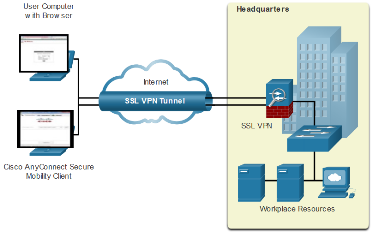
- Definition of VPN according to the IETF
  - An emulation of a private Wide Area Network (WAN) using shared or public IP facilities such as the Internet or private IP backbones
  - An extension of a private intranet across a public network (usually the Internet)
- Originally driven by low cost and wide reach of the Internet
- Recent drivers are avoiding geoblocking and concerns about privacy


User Computer with Browser
Headquarters
Internet
SSL VPN Tunnel
SSL VPN
Cisco AnyConnect Secure Mobility Client
Workplace Resources

Introduction to VPNs



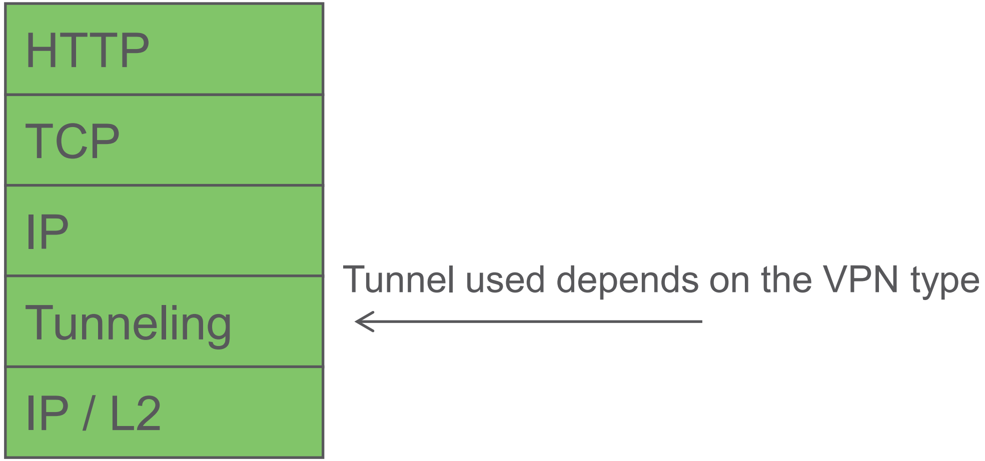
- Key concepts of VPNs are
  - Tunnels
    - Main VPN concept
    - Enables two end-points to exchange data in a way that emulates point to point communication
  - Encryption
    - Enables communication to be confidential even though using shared and very insecure Internet
  - Integrity
    - Ensures data is unchanged
  - Authorisation
    - Specifies what services and resources users can have access to



User Computer with Browser
Headquarters
Internet
SSL VPN Tunnel
SSL VPN
Cisco AnyConnect Secure Mobility Client
Workplace Resources

VPN Tunneling protocols

- **Tunnels in VPNs**
  - **Encapsulate data packets in a tunneling protocol**
    - **Possibly other IP packets**
  - **Then encapsulate in IP packets or layer two frames for transmission**
- **Example**
  - **Accessing HTTP over a VPN**



HTTP

TCP

IP

Tunneling

IP / L2

Tunnel used depends on the VPN type

VPN Tunneling protocols

- IP Security (IPSec)
  - IETF
  - Network layer (layer 3) protocol
- Point-to-point tunneling protocol (PPTP)
  - Obsolete (lots of security issues and other alternatives)
  - Microsoft Layer 2 protocol
- Layer 2 Tunneling Protocol (L2TP)
  - Cisco Layer 2 protocol
  - Built from L2F (layer 2 forwarding) and PPP (Point to Point Protocol)
- Secure Socket Tunnelling Protocol (SSTP)
  - Secure Sockets Layer / Transport Layer Security
  - Transport over TLS/SSL with inbuilt key exchange mechanisms

IPS/IDS

Intrusion Detection and Prevention Systems (IDS/IPS)

- Detects attacks or abuse
- Collects data on system behaviour so as to prevent future intrusions or attacks
- Identify normal and damaging actions
- Report and respond to attacks as they happen
- Be able to cooperate with other security mechanisms
- Intrusion Prevention Systems (IPS) may stop intrusions through automatically inserting new rules into a Firewall

IDS components

- Sensors
  - data gathering
- Monitors
  - process data
- Resolver
  - decides on appropriate response to events
- Controller
  - configuration of other components

IDS Approaches

- Signature based
  - Based on the characteristics of specific attacks being known
  - System contains a database of attack profiles
  - Signature based systems the most commonly deployed IDSs
- Statistical anomaly based
  - Protocol anomaly based
  - Traffic anomaly based
- Rule based
  - Stateful matching
  - Model based
  - Makes use of rules of the form IF … THEN… to identify attacks

Cryptography

Cryptography Basics

- At the heart of cryptography is the aim of changing ordered data into a seemingly random string
- Only by knowing the key or keys can the data be encrypted and decrypted
- Cryptography covers more than confidentiality
  - Enables authentication, integrity, non-repudiation
- Cryptosystem
  - Comprised of:
    - Software
    - Protocols
    - Algorithms
    - Keys

From Bruce Schneier

From the preface of “Applied Cryptography”

“There are two kinds of cryptography in this world: cryptography that will stop your kid sister reading your files, and cryptography that will stop major governments reading your files. This book is about the latter.

“If I take a letter, lock it in a safe, hide the safe somewhere in New York, then tell you to try and read the letter, that’s not security. That’s obscurity. On the other hand, if I take a letter and lock it in a safe, and then give you the safe along with the design specifications of the safe and a hundred identical safes with their combinations so that you and world’s best safecrackers can study the locking mechanism – and you still can’t open the safe and read the letter – that’s security.”

Cryptography Terminology

- Plain text
  - The unencrypted message
- Cipher text
  - The message after encryption
- Key
  - The information needed to decrypt or encrypt the message
- Key space
  - Range of values that can be used to construct the key
- The algorithm
  - Rules used for encrypting and decrypting the message

Kerkhoff’s Principle

- Expressed in 1883
  - The number of secrets needed in a cryptosystem should be kept to a minimum
- Should the algorithm used in a cryptosystem be made public?
  - Kerkhoff’s principle states that it should
  - The only thing that a cryptosystem should rely on for security is its key
  - By making the algorithm public and letting anyone attempt to compromise the cryptosystem, means that its security can be tested
- Not always accepted
  - Many governments dislike the idea of publicising their algorithms
  - Prefer the risk of an error to the sustained scrutiny publication brings
- Commercial enterprises generally adopt Kerkhoff’s principle

Strength of cryptosystems

- A number of factors that affect the strength of cryptosystems are listed below
- The algorithm
  - Block algorithms consist of rounds of substitution and permutation. An algorithm might be compromised if it doesn’t use enough (a weakness in some implementations of RC5)
  - An ideal stream cypher should map input values randomly across the entire cipher space. Some algorithms have biases where a subset of the cipher space is mapped more commonly than others (a weakness of RC4)
- The length of the key
  - Generally, the longer the key, the greater the strength of the cryptosystem

Symmetric and asymmetric algorithms

- There are two broad categories of cryptographic methods
  - Symmetric key and asymmetric key
- Classical (pre 1970) cryptographic methods are all symmetric key
  - The same key is used to both encrypt and decrypt (possibly with some simple modification)
  - DES, 3DES, AES, RC4 are perhaps the most well known and widely implemented algorithms
- Public key algorithms introduced in the 70s revolutionised cryptography
  - Different key used for encryption and decryption.
  - Knowing one key tells you nothing about the other key
  - RSA, El-Gamal, elliptic curve best known examples

Symmetric key cryptography

$E_k(M) = C$

encryption

$D_k(C) = M$

decryption

K encryption and decryption key

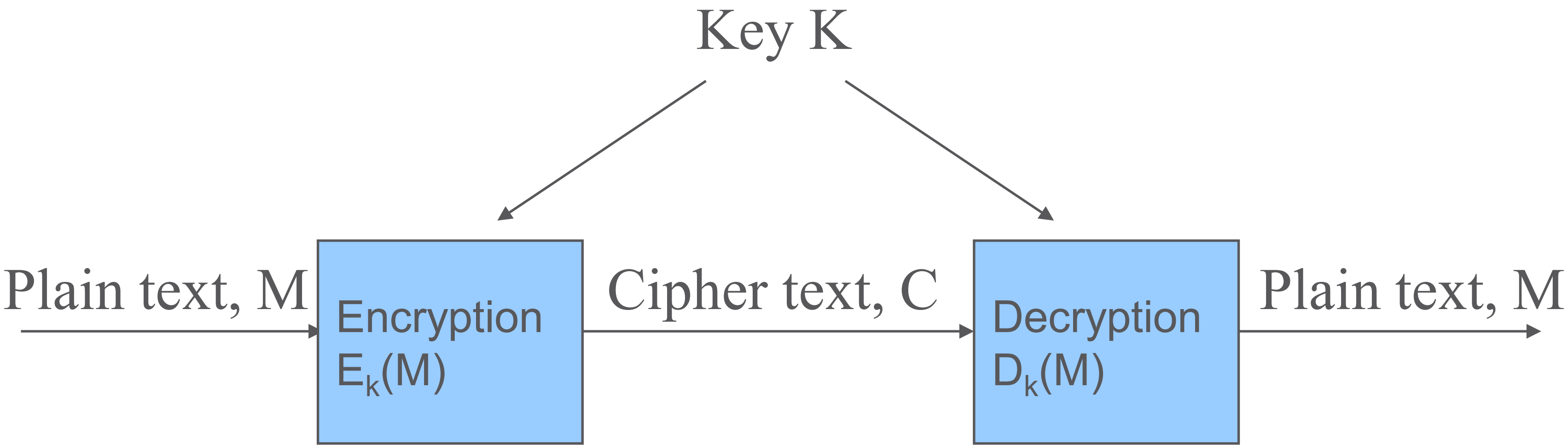
M plaintext

C ciphertext

$D_k(E_k(M)) = M$

Converse not necessarily true

Symmetric key cryptography



Symmetric key cryptography

- Advantages
  - Most common symmetric key algorithms are very fast
    - Algorithms require a small number of operations and a small amount of information kept in memory
    - Lends themselves to hardware implementation
  - Can provide confidentiality, authentication and integrity
- Disadvantages
  - Key distribution
    - Large number of keys needed
  - Difficult to provide non-repudiation

Questions to illustrate key explosion

- Suppose your organisation has 20 people in it. Each of them may wish to communicate with each of the other 19 people. Each of them wish their communications to be confidential, that is no-one other than the recipient should be able to decode the cipher text.
  - How many keys does each person need to keep secret? 19 keys for communicating with 19 other people
  - How many keys in total? n(n-1) / 2 = 20.(20-1) /2 = 190 keys
- Suppose your organisation has 10 people in it. Despite being such a small organisation it is faction ridden. Factions may consist of 2, 3 or 4 people. Individuals may belong to more than one faction. Each faction has its own secret key. How many possible secret keys?

Permutation: P(n)=n!

Arrangement: A(n,k)= n! / (n-k)!

Combination: n! / k!.(n-k)!

C(10,2) - factions with 2 people:
C(10,2) = 10! / (2! * 8!)= 45
C(10,3) - factions with 3 people:
C(10,3) = 10! / (3! * 7!)= 120
C(10,4) - factions with 4 people:
C(10,4) = 10! / (4! * 6!)= 210
Now, we sum these up:
45 + 120 + 210 = 375

Public key cryptography

- Sometimes known as Asymmetric cryptography
- Examples are RSA, Elliptic curve algorithms
- Sender and receiver use different keys for encryption and decryption
  - a key pair
- Key pairs are mathematically dependent
  - message encrypted by one key can only be decrypted using the other key of the key pair
  - But knowledge of one key tells you nothing about the other key
    - It is impossible (or very very difficult) to derive the private key from the public key

Public key cryptography

- Anybody can encrypt with the public key but only the holder of the private key can decrypt it
- The holder of the private key can encrypt a message that anyone can decrypt with the public key
- Enables
  - Confidentiality (Usually used for key distribution)
  - Authentication
  - Non-repudiation
  - Solves the key explosion problem

  BUT
  - Much slower (1000s of times) than symmetric key algorithms
  - Key lengths much longer (10s) than symmetric key algorithms for same level of security

Public key cryptography

$E_{k1}(M) = C$

$D_{k2}(C) = M$

K1 = encryption key

K2 = decryption key

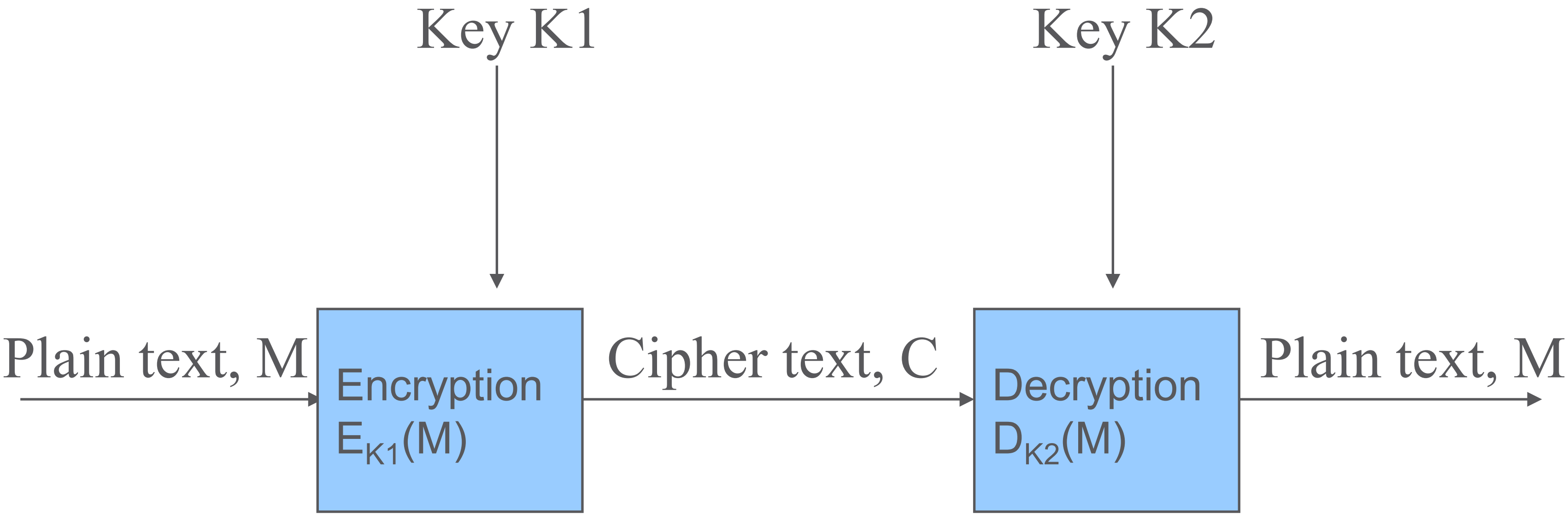
M plaintext

C cipher text

$D_{k2}(E_{k1}(M)) = M$

Converse is usually true

Public key cryptography



Public key cryptography services

- Confidentiality
  - Alice wishes to send a message to Bob that is to be kept secret. She encrypts the message with Bob's public key. Bob decrypts it with his private key
  - Public key cryptography is usually not used for confidentiality of messages. Too slow. But can be used to exchange symmetric keys
- Authentication
  - Alice wishes to authenticate her identity to Bob. Knowing the private key associated with Alice's public key is proof of identity
  - Bob sends a challenge to Alice. Alice encrypts the challenge with her private key and sends it to Bob. Bob decrypts the response with Alice's public key. If the decrypted response matches the challenge Alice's identity is proven

Public key cryptography

- Advantage of public key cryptography compared with symmetric key cryptography is that no confidential information need be exchanged before communication takes place
  - Can provide a secure but open communication channel for exchange of symmetric keys
  - Can also be used for authentication, integrity and non-repudiation
  - Public key can be very public
    - attached to emails
    - located in register
    - on web pages
    - transmitted in plaintext as part of protocol exchange (eg SSL)

Public key cryptosystems

- Rivest – Shamir – Adleman (RSA)
  - Based on factoring of 100 to 200 digit prime numbers
  - Easy to multiply and calculate products of large numbers
  - very difficult to factor a large number you know to be the product of two prime numbers
- Public key algorithms are rarely used to encrypt user data or messages.
  - Used to encrypt session keys which are then used to encrypt user data
  - Used for authentication and non-repudiation
  - TLS / SSL

Summary of Cybersecurity

- In this lecture we have looked at important security technologies
  - Authentication technologies including challenge response protocols
  - VPNs
  - Intrusion Detection and Prevention Systems
  - Cryptography