LECTURE 1

People who are Involved in attacks

- **Amateurs** — **Accidental** access to unauthorized resources(**No harm to reg users)**
- **Crackers** — **Active** attempts to access sensitive resources/discover system vulnerabilities (**Minor harm to reg users)**
- **Criminals** — **Active** attempts to utilize weaknesses in protection system/to steal or destroy resouces (**Minor harm to reg users)**
- **Regular users**

Three things that yields a secure system

Confidentiality
Integrity
Availability

CIA

Confidentiality Assets Only available to authorized parties

Threats to data and programs (Illegal read/illegal access)

Integrity maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle

Threats to software and data(technical errors, software errors)

Availability Requirements for timely response, far allocation, usability

Protection Methods

Encryption	Effective for confidentiality, access control, user-message authentication
SW & HW	Software & hardware controls
Policies	Special procedures, security methods
Physical control	Isolation of equipment, access to equipment

Cryptography

Cryptography domain addresses the **principles**, **means** and **methods** of disguising information to ensure its **integrity, confidentiality, authenticity, nonrepudation**

Goals of cryptography

- To ensure data,message , info not modified during transmission
- Ensure unauthorized parties cannot access data,message,info
- Ensure that source/sender message/info is identifiable
- None of the parties cannot deny sending/receiving data

Stream Ciphers

Message broken into characters or bits

Advantages
- Speed of transformation
- Low error propagation

Disadvantages
- Low diffusion
- Susceptibility to malicious insertion and modifications

Block Ciphers

Process messages in blocks

Advantages
- Diffusion
- Immunity to insertion

Disadvantages
- Slowness of encryption
- Error propagation

Characteristic of GOOD cipher

Shannon charactristics

The amount of secrecy needed should determine the amount of labor appropriate for encryption and decryption

The set of keys and encryption algorithm should be free from complexity

The implementation of the process should be simple

Errors in the cipher should not propogate and cause corruption of further info

Errors in the cipher should not propogate and cause corruption of further info

Size of the enciphered text should not be larger than the text of original message

Kerckhoff's principal

The security of the encryption scheme must **depend only on the secrecy of the key** and **not on the secrecy of the algorithm**

Algorithms are difficult to change

Cannot design algos for every pair of users

Expert review

No security through obsecurity

Confusion

The interceptor should not be able to predict what changing one character in the plain text will do the ciphertext

Diffusion

The characteristics of distributing the information from single plaintext letter over the entire ciphertext

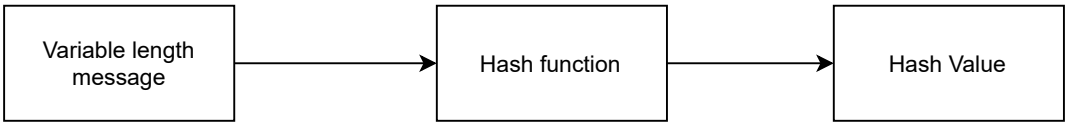
LECTURE 2

What is Hashing? Process of converting an input of any length into a fixed sized string of text

Hash Functions The algorithm that is used to convert inputs

Used to detect changes to message

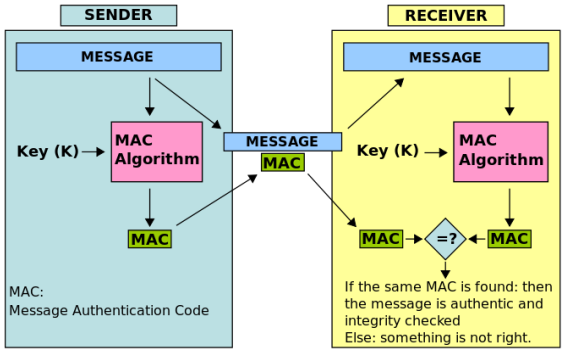
Condenses arbitrary message to fixed size



SHA - Secure Hash Algorithm

MAC A function of the message and a secret key that produces a fixed length value that serves as the authenticator

MAC guarantees integrity and authentication



A message authentication code is a way of combining a **shared secret key** with the a message so that the recipient of the message can authenticate that the sender of the message has the shared secret key and the no-one who doesn't know the secret key could have sent or altered the message.

HMAC

Hash based message authentication code. Applies hash function one or more times to some sort of combination of the shared secret and the message

MD5	**SHA - 1**
Produces a 128 bit hash value	Produces 160 bit output
Less secure	More secure than MD5
Speeder than SHA	Slow in comparison with MD5

Simpler than SHA | More complex

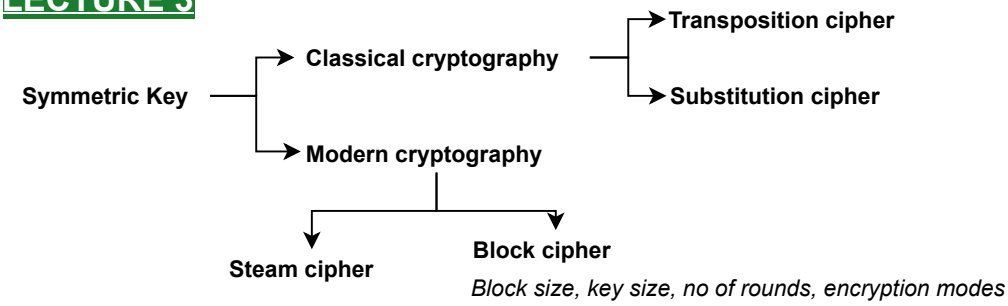
Java Cryptography Architecture

Implementation independence

Implementation interoperability

Algorithm extensibility

LECTURE 3

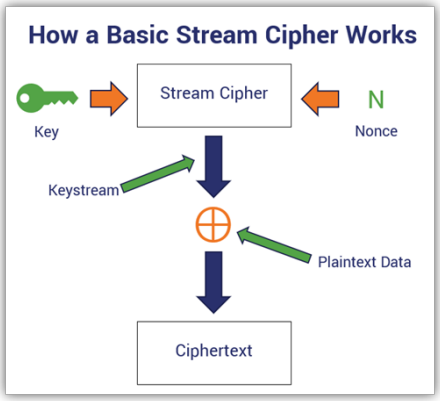


Steam cipher

A stream cipher encrypts data one bit at a time instead of in blocks

But a key part of this process is generating a stream of pseudorandom bits based on an encryption key and a seed, aka a nonce (a unique randomly generated number — “nonce” = number-only-used-once).

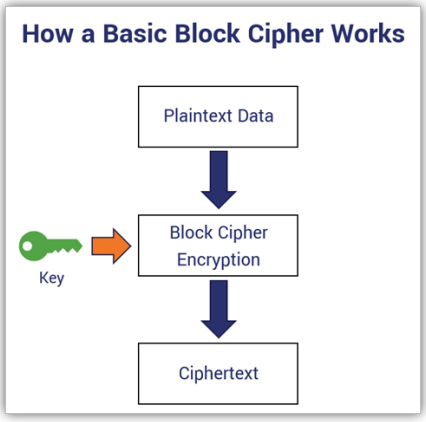
Together, they create a keystream that gets XORed with your plaintext input, which encrypts it and results in your ciphertext output.

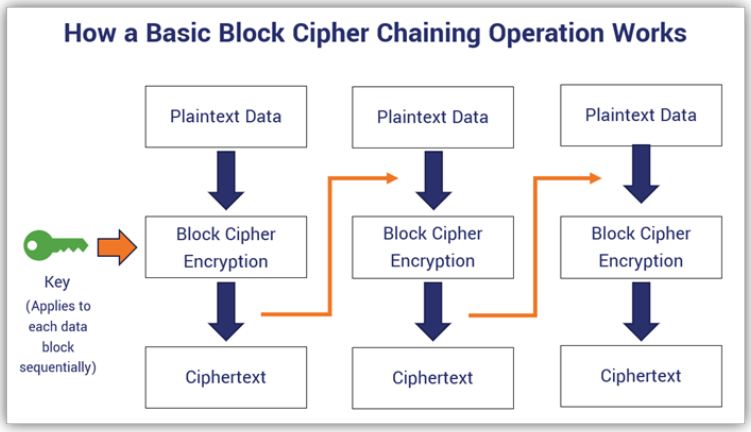


Examples:
Salsa20
ChaCha20
RC4
A5

Block cipher

A block cipher breaks down plaintext messages into fixed-size blocks before converting them into ciphertext using a key





Examples: DES, Triple DES, AES, IDEA, Blowfish, RC5

Symmetric Key
Uses a single private key shared between users
Same key for encryption and decryption

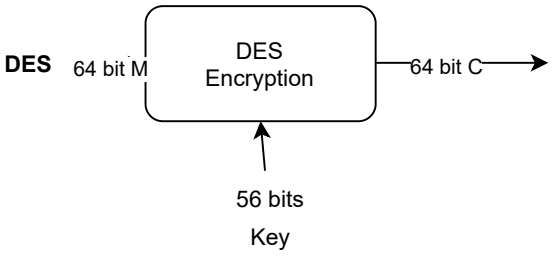
Strengths → Quicker than asymmetric; Ideal for bulk encryption/decryption

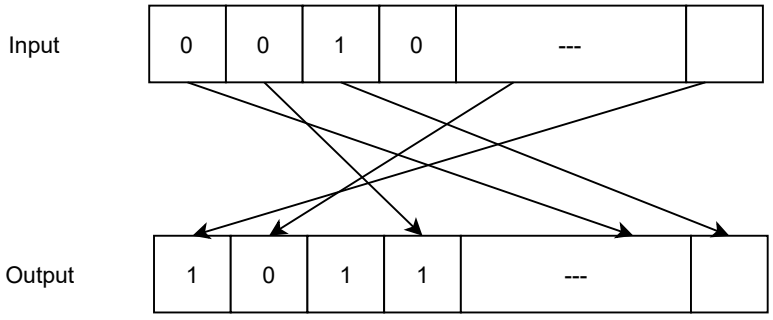
Weaknesses → Poor key distribution; Poor key management

Requirements

A strong encryption algorithm

Secret key





Bit permutation

Triple DES

Use 3 encryptions

AES

Private key symmetric block cipher

block length - 128

Requires 10 rounds of processing 10 individual keys

Decryption algorithm uses the expanded keys in reverse order

Decryption algorithm is not identical to encryption algorithm

Round includes matrix multiplication

ECB - Electronic Codebook Book

Message is broken into independent blocks which are encrypted

Each block is encoded independently of the other blocks

Advantages

Faster Easier

Requires a synchronous counter at the sender and receiver

DisAdvanatages

Identical plain text blocks are encrypted to identical ciphertext blocks

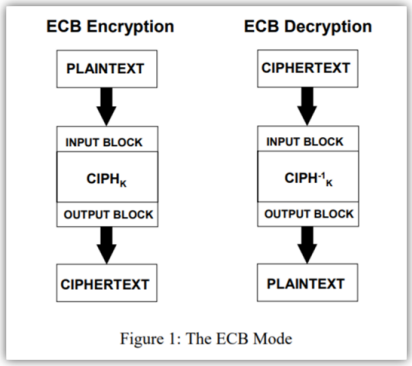


Figure 1: The ECB Mode

CBC

Message is broken into blocks

Blocks are linked together in the encryption operation

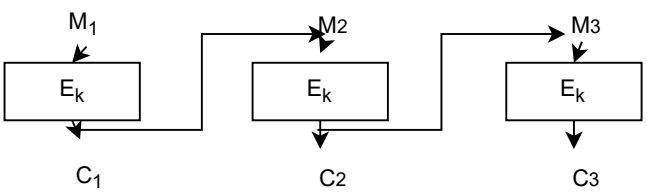
a sequential process that builds upon previous data blocks

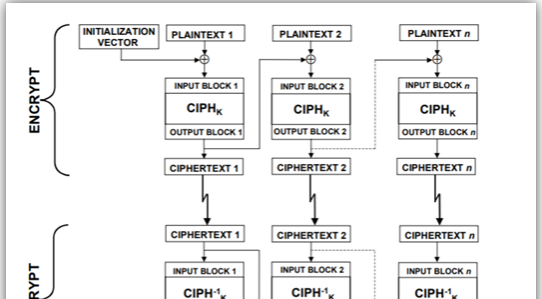
Advantages

Changing IV results in different ciphertext for identical message

Disadvanatages

Slow





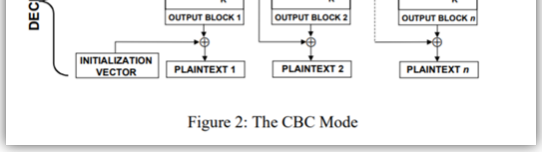


Figure 2: The CBC Mode

CFB

A stream cipher where the ciphertext is used as feedback into the key generation source to develop the next key stream

encryption cipher function is used in both the encryption and decryption processes,

OFB

Stream cipher that generates the ciphertext key by XORing the plaintext with a key stream

Errors will not propogate in this mode

he first output block is exclusive-ORed with the first plaintext block to produce the first ciphertext block.
The forward cipher function is then invoked on the first output block to produce the second output block.
The second output block is exclusive-ORed with the second plaintext block to produce the second ciphertext block,
and the forward cipher function is invoked on the second output block to produce the third output block.

CTR - Counter

Similar to OFB but encrypts counter value rather than any feedback valu

CTR doesn't require explicit chaining and is parallelizable

Can process and encrypt separate messages in parallel (like stream ciphers).
So, this means that because it doesn't depend on the output from a previous block, you can decrypt two blocks independently.

Advantages

it does not propagate the error of transmission at all in this mode

Can do parallel encryptions in HW or SW

Good for high speed links

Disadvantages

Cannot reuse keys

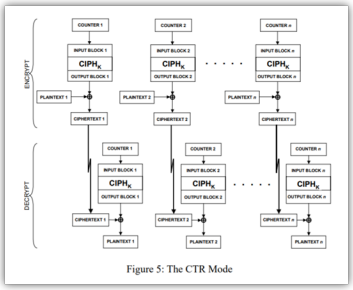


Figure 5: The CTR Mode

Other symetric block ciphers

IDEA RC5

Blowfish Cast-128

Stream Ciphers

Process the message bit by bit

Typically have random stream key

Combined(XOR) with plaintext bit by bit

Must never reuse stream key

Properties

Long period with no repitions

Statiscally random

Confusion

Diffusion

Block Ciphers	Stream Ciphers
Symmetric key ciphers that encrypt and decrypt data in fixed-size blocks.	Symmetric key ciphers are stateful ciphers that encrypt and decrypt data bit-by-bit.
Slower processing.	Faster processing.
Require more resources.	Require fewer resources.
Can take on stream cipher properties through certain modes of operation.	Cannot take on block cipher properties.
Rely on stateless and stateful modes of operation, which include ECB, CBC, CFB, OFB, CTR, GCM, and XTS.	Can be synchronous or asynchronous.
Used nearly everywhere.	Used for some data in-transit encryption, including in some SSL/TLS cipher suites.

RC4

Cliamed secure against known attacks

Result is very non linear

Must not reuse a key as it is not a stream cipher

Advantages

Algorithms are fast
Encryption & decryption are handled by same key

Disadvantages

Key is revealed, the interceptors can decryt all encrypted information
Key distribution problem

PKCS5 Padding

Padding - To make the last block to fit the block size. Inserting some dummy data to the last block

Recepient should have an understand on which block is dummy which block is not. We use PKCS5 mechanism for this.

LECTURE 4

Symmetric key cryptography

Traditional single key cryptography uses one key

Shared by both sender and receiver

Public key cryptography

Developed to address **Key distribution & digital signatures**

The scheme has six ingredients

Plaintext
Encryption algorithm
public and private key
Ciphertext
Decryption algorithm

Applications for Public key cryptography

Encryption/decryption

The sender encrypts a message with the recipient's public key

Digital signature

The sender signs a message with its private key

Key exchange

Two side cooperate to exchange a session key

Algorithms

RSA

Diffie-Hellman

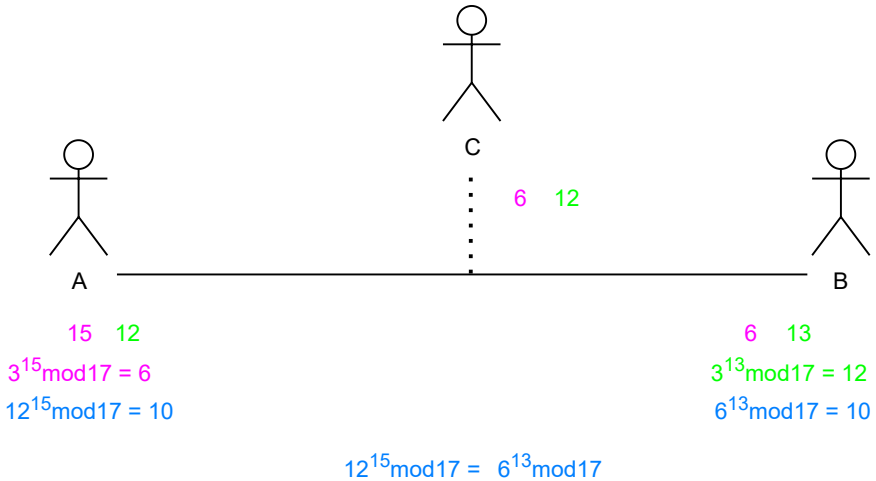
ECC

Diffie-Hellman

Easy in one direction harder in the other direction. Exchange a secret key securely. compute discrete logarithms

Discrete logarithm

The inverse problem to exponentiation is to find the discrete logarithm of a number modulo p (a^x=bmodp)



Prime factorization

An integer, n>1 can be factored in a unique way as
$n=P_1^{a1}.P_2^{a2}$

How to find large prime?

If p is prime and r is any number less than p
gcd(p,r)=1

Jacobi fucntion

RSA

Find 2 large prime numbers p and q (100 digits=512bits)

Calculate the product n=p*q (n is around 200 digits)

Select large integer e relatively prime to (p-1)(q-1)

Select d such that e*d mod (p-1)*(q-1)=1

Encryption $C=P^e \text{mod} n$

Decryption $P=C^d \text{mod} n$

ECC - Elleptic curve cryptography

Calculations prove to be slow
Inaccurate due to rounding error
infinite field

LECTURE 5

Certificate types

Digital signature
Key encipherment
Data encipherment
Key certificate signature
CRL signature

Key management

database for the public and private keys

makes it easy to retrieve the key for a certain identity

PKI - Public key infrastructure

Provides the foundation necessary for secure e-business through the use of cryptographic keys and certificates

Certificate Revocation

A from of anticertificate which cancels a certificate

CRL Distribution problems

CRLs have a fixed validity period

Issuing CRLs to provide timely revocation exacerbates the problem

Online certificate status protocol

Inquires of the issuing CA whether a given certificate is still valid

OCSP acts as a selective CRL protocol

Problems

CRL can only report negative results
Some OCSP implementations will report "I can't find a CRL" as "Good"

Other Online validation protocols

SCVP
DVCS
ICAP
RCSP

LECTURE 6

Email Security

Pretty good privacy(PGP)

Provides a confidentiality and authentication service that can be used for electronic mail and file storage applications

S/MIME

Secure multipurpose internet mail extension

PGP for personal email security

Why PGP?

Available free on a variety of platforms

PGP services

Based on well known algorithm

Wide range of applicability

Digital signature	DSS/SHA or RSA/SHA
Message encryption	CAST or IDEA three key triple DES with Diffie-Hellman/RSA
Compression	ZIP

Operational Description

Authentication
Confidentiality
Compression
Email compatibility
Segmentation

PGP content

Session key component,signature, message

Securing a MIME entity

Prepared MIME entity is processed by S/MIME to produce a PKCS object

S/MIME Functions

Enveloped Data : Encrypted content and encrypted session keys for recipients
Signed Data: Message digest encrypted with private key of "signer"
Clear Signed Data: Signed but not encrypted
Signed and Enveloped data: Various ordering for encrypting and signing

Algorithms used

Message Digesting: SHA-1 and MDS
Digital signatures: DSS
Triple DES

Phishing

Phishing is an illegal activity that uses social engineering techniques to trick people into giving out personal information

Phishing technique

Link manipulation
Spoofed website
Website forgery
Filter evasion

Existing anti-spamming techniques

Blacklist/Whitelist	List of domains, mail serves, and email addresses are defined. Emails from the above address will not be allowed
Integrity check	Mail can be check and filter if it has the characteristic of spam
Reverse DNS lookup	When receiving an email, the IP address of the sending server is taken ad DNS lookup is performed on the address is a real one or bogus one
Rules-based filtering	Mails are examined according to the specific rules

Document security

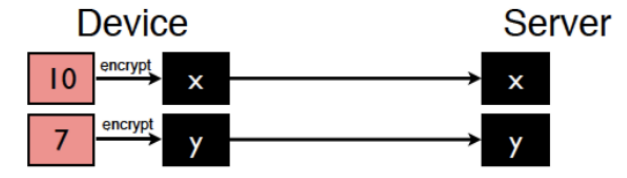
Confidentiality	**Integrity**
Authorization	**Authenticity**
Accountability	**Nonrepudation**

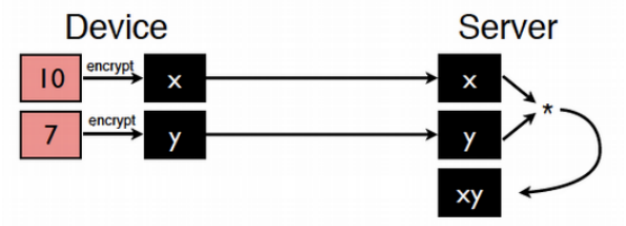
Cloud computing

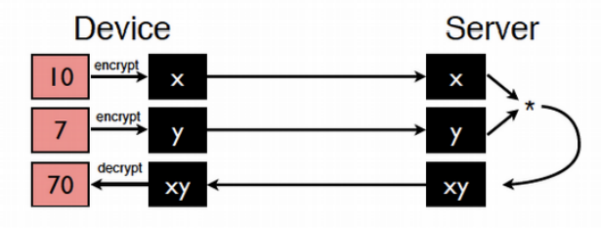
Enables on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned

Cloud security

Homomorphic encryption







LECTURE 7

Security requirements and user needa

Authenticity
Integrity
Confidentiality
Availability
Non-repudiation

Solutions

Lower level Protection at the packet level
No protection at the document level
Communications security only
Efficient for network protection
Not suitable for application security services

Application/User level Protection at the document level
No protection at the communication level
Communications security implicit
Not efficient for network protection

TLS: Transport Layer security

SSL: Secure sockets layer

Addresses issues of privacy, integrity and authentication

Protocol layer, requires reliable transport layer

Overview

Browser sends supported crypto algorithms
Server picks strongest algorithms it supports
Server sends certificate
Client verifies certificate
Client and server agree on secret value R by exchanging messages

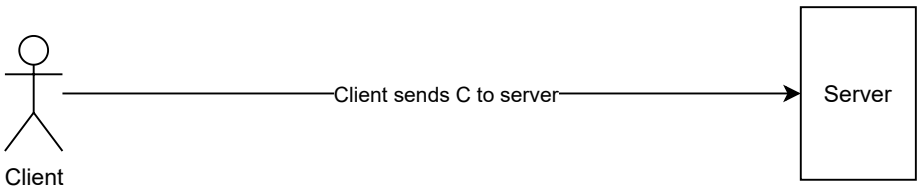
TLs : Key exchange

Need secure method to exchange secret key, use public key encryption

Choices are RSA or Diffie-Hellman

Basic key exchange

RSA key exchange



Generates random secret value R

encrypts R with public key, PK, of server C=EPK(R)

Server decrypts C with private key, SK, of server R=DSK(C)

Forward secrecy

Compromise of public-key encryption private keys does not break confidentiality of past messages

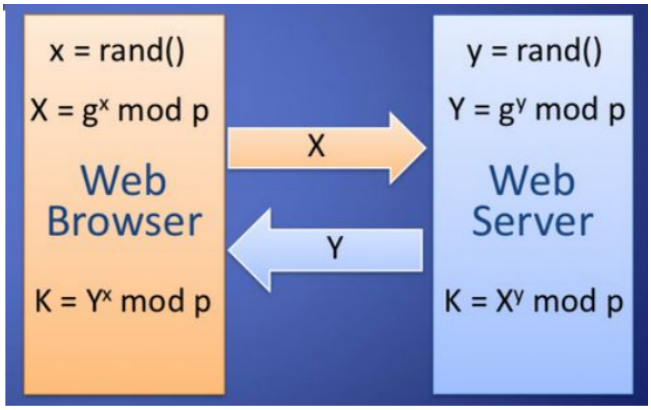
TLs with basic key exchange does not provide forward secrecy

TLs with basic key exchange does not provide forward secrecy

Attacker eavesdrop and stores communicaion

If server's private key is compromised, attacker finds secret value in R in key exchange and derives keys

Diffie Hellman Key exchange



To avoid attacks browser and server send signed X and Y respectively requires each to know the public key of the other

TLs : encrypts

All browser-server and server-browser except which browser is talking to which server

URL of requested document

Contents of requested documents

Cookies sent from browser to server and server to browser

Javascript communications

TLs : Integrity

Compte fixed-length message authentication code(MAC)

Includes hash, shared secret, sequence number

Transmit MAC with message

Receiver creates new MAC

TLs allows MD5, SHA-1

TLs : HTTP

HTTP most common TLS application

Requires TLS-capable web server

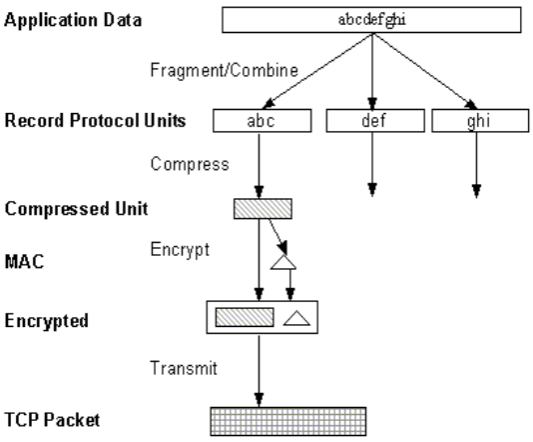
Requires TLS-capable web browser

TLs : Architecture

TLs defines Record protocol to transfer application and TLs information

Handshake protocol, Change cipher spec, alert protocol, TLs record protocl

Requires TLS-capable web browser



Public key certificates

X.509 certificate associates public key with identity

User of certificate must ensure it is valid

SSL indicator

Provide user with iidentity of page origin

Indicate to user that page contents were not viewed or modified by a network attacker

Extended validation certs

Requires human lawyer at CA to approve cert request

Designed for banks and large e-commerce sites

Create self-signed certificate

Generate a self signed host certificate `openssl req -new -x509 -out host.pem`

Create a certificate request `openssl req -new -nodes -out req.pem -keyout key.pem`

Authenticating with SSL

Advantages: No passwords to mess around with

Disadvantages: Certificate management is hard

Problems with HTTPS and the lock icon

Upgrade from HTTP to HTTPS

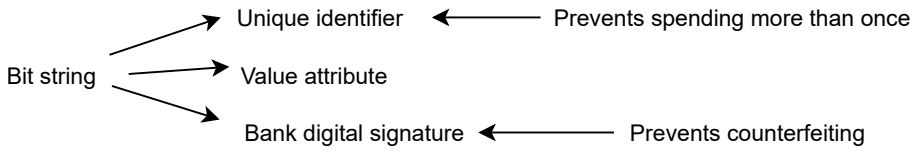
Semantic attacks on certs

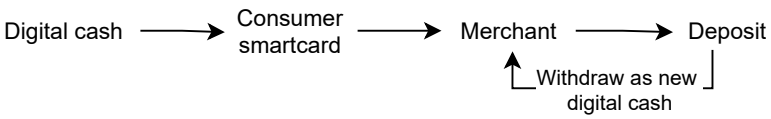
Invalid certs

Mixed content

LECTURE 8

What is digital cash token?





Characteristics of digital cash

Anonymity of consumer

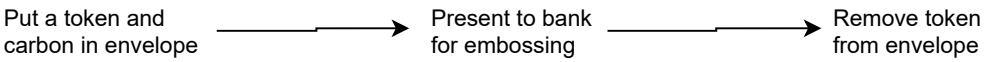
Attribution of cheating

Authorized traces

Blind signature

Blind signature scheme is a protocol that allows the provider to obtain a valid signature for a message m from the signer without him seeing the message and its signature

Blind signature analogy



eCheck

Checks without the paper

Significance

New payment alternative for business commerce
Interoperable, with multiple providers
enhances existing business practices

Electronic credit and debit

Secure electronic transactions(SET) of Visa/mastercard

Framework must take into account different institutions involved

Risk in using credit cards

Customer uses a stolen card or account number to fraudulently purchase goods or services online

Customer falsely claims that he or she did not receive shipment

Hackers issue credits to hacker card account numbers

Extra protection when there's no card

Quick steps to ensure against CNP fraud

Obtain an authorization
Verify the card's legitimacy
use fraud prevention tools such as Viisa's address verification service(AVS), card verification value 2

Credit card protocols

SSL TLS	**Very important usage increasing**
iKP(IBM) SEPP STT SET	**Obsolete**
3D Secure	**Very slow acceptance**

strong security services

SSL

Not a payment protocol - can be used for any secure communications

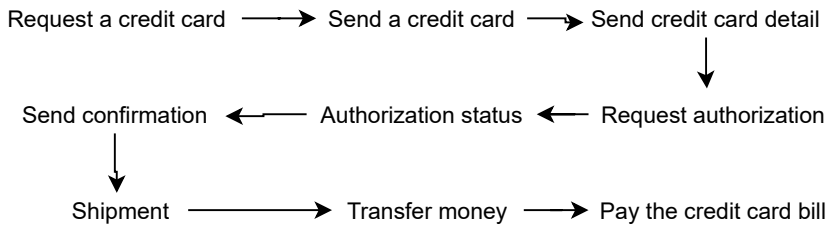
SSL provides privacy b/w two internet applications and authentication of server

Uses enveloping: RSA used to exchange DES keys

SSL handshake protocol

SSL record protocol

Internet Transactions



Secure Electronic Transaction(SET)

Designed to protect credit card transactions

Confidentiality: All messages are encrypted

Trust: All parties must have digital certificates

Privacy: Information made available only when and where necessary

Advantages → strong cryptography, scalable

Disadvantages → Global system, Privately owned, Card payments only

Dual Signatures

Links two messages securely but allows only one part to read each

Take the hash(SHA-1) of the payment and order and concatenate the hash values

Customer encrypts the final hash with a private key creating the dual signature

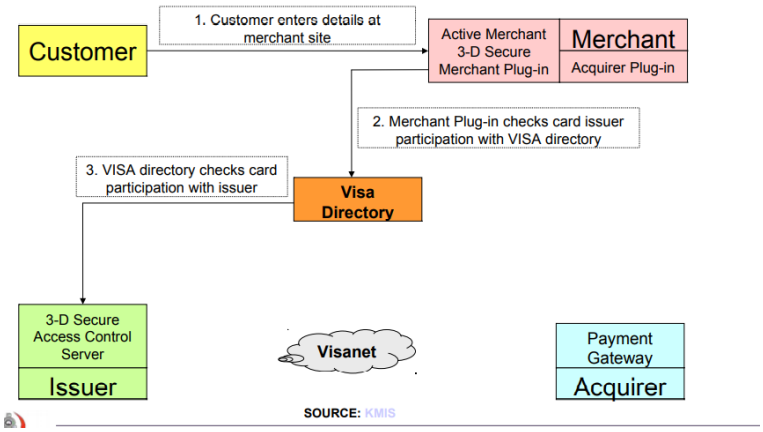
Customer encrypts the final hash with a private key creating the dual signature

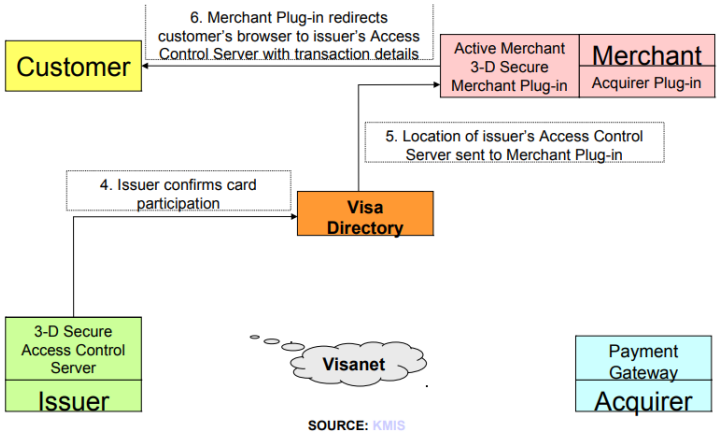
3D secure

Authenticate user without a certificate

Requires the user to answer a challenge in real-time

Challenge comes from the issuing bank, not the merchant





Features of 3D secure

Payment authentication

Support variety of internet access devices

Benefits

Benefits for cardholder

Benefits for merchants

eMoney order

Person goes to the nearest post office

↓

Pay the required amount and buy the eMoney order

↓

Send the number in the eMoney order together with other details

Advantages

Easy to access

Easy to understand

Save the money within the country

Trusted cheque protocol(TCP)

M-ATM

LECTURE 9

Chaum's anonymous e-cash

Anonymous

Secure

Only transfer

Digital cash

Electronic version of existing currency

Digital currency

Entirely new currency

Making Money digital

Secure transfer in computer networks

Cannot be copied and reused

Anonymity

Offline transactions

Can be transferred to others

Can be subdivided

Bitcoin

Creation of new currency

Secure transactions

Protection against double-spending

Anybody can be a "merchant" or a "customer

Psuedo anonymity

Currency = transaction history

Cryptographic hash functions - inverse is inffeasible

Instead of a central point of trust bitcoin uses block chain

Blockchain

Computing an account balance is done by summing over all previous transactions for that account

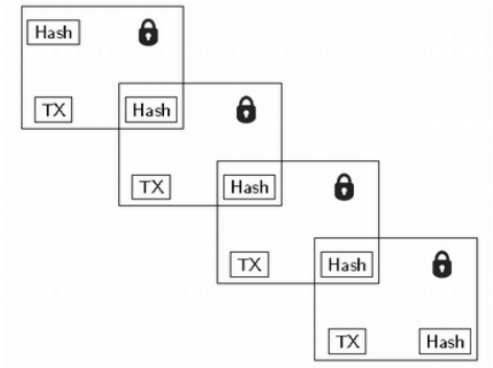
Each block contains a list of transactions, together with a proof of work

Creating blocks is called mining

Transactions are verified by miners

If two miners find a valid block simultaneously, the resolution strategy is to randomize and then work on the longest chain

Each block gives security to the previous one



PROS

CONS

- Independent currency (account cannot be frozen)
- Unstable value (bitcoin currency can increase or decrease drastically)
- Little to no transaction fees (perfect for

sending money overseas or travelling)

- Secure transactions (encrypted)
- Unlimited transfers and amount can be sent
- It's essentially anonymous*

- Volatile market (unpredictable)
- Not widely accepted (for now...)
- Payments are irreversible (no money back guarantee!)

LECTURE 10

User authentication

User authentication can be done based on 3 factors

Something the user knows	**Passwords - can be guessed**
Something the user has	**smart card - can be stolen**
Something the user is	**biometrics - can be copied sometimes**

Multifactor authentication

Factors may be combined to reduce probability of compromization

Password selection strategies

Computer generated passwords
Eliminated guessable passwords
Reactive password checking
Proactive password checking

Kerberos

A secret key based service for providing user and service authentication to each other in insecure networks
A trusted third party
Responsible for
Authentication
Authorization
Key exchange

Problems

- Access services deployed on a distributed manner throughout an open network (insecure)
- Being able to authenticate requests for services
- Servers being able to restrict access to authorised users
- Users being able to authenticate servers / services

Solution

Require the user to prove his or her identity for each service invoked.

Also require that servers prove their identity to clients.

Challenge: There can be middle parties listening to traffic or probing to get access to services by means such as replay, spoofing as another workstation, etc.

Kerberos summary

Avoid sending passwords in cleartext through an insecure network
Provide single sign on capability
Delegated authentication

LECTURE 11

Network perimeter

Defense in depth

Network segmentaion

implement organization policy requirements to filter traffic

UTM

Unified threat management

UTM combines multiple perimeter protection features into single appliances

Firewall, Malware detection, VPN capabilities, Routing capabilities, load balancing

DLP

information needed to be classified so that DLP can be fed with fingerprints of confidential information that should not leave the perimeter

Can prevent data leakage through media such as USB

Processing power needed is distributed

DLP can be enforced
based on time - at which time a particular data should have been accessed
based on content - what content can be accessed by which roles

DMZ

DMZ is a physically or logically separated sub-network that is used to host services received by users from internet or external networks

The separation will prevent a compromization of a host providing service to external users from propagating into the internal nw

Bastion host

A special host configured to provide access to certain systems in internal network for external users

Logs are recorded and kept for a long time

Actions done through bastion host may be screen recorded for selected users

Firewall design goals

Direction control - LAN to internet
Service control - filter inbound traffic based on service request
User control - Division bw students and teachers
Behavior control - restrict abnormal traffic such as DoS attacks

Firewall filtering

Atomic - e.g signatures to examin single packet /LAND attack

Attacker sends a TCP SYN packet setting source address same as the destination address which will make a vulnerable TCP stack to recursively process the packet ending up in a DoS

Stateful - e.g identifying content based attack

Communication packets may get fragmented during the communication and need to analyze multiple packets relevant to the specific communication

Alternative Firewall filtering

Anomaly detection
Behavior detection

Static packet filtering

Allow or deny communication based on a single packets' internal characteristics such as source and destination IP addresses and ports

Dynamic packet filtering

Allows the firewall to create rules to deal with event

Limitations of firewalls

Impact on network performance
Cannot protect attacks bypassing Firewall (Wireless network, LAN)

LECTURE 12

Intruder

A person or program who attempts to have unauthorized access to a system or sub system or to damage, get authorized infrormation, disturb etc

Intrusion detection system (IDS)

Detect intruder or malicious attacks

Car alarms, Fire detectors, surveillance system

Intrusion prevention system (IPS)

While IDS only detect intrusions passively IPS can intrusions actively

Network based IDS/IPS

Installed at a place where it can watch the network traffic going in and out of a particular network

Software IDS	IDS appliance
Less cost compared to appliance	Expensive compared to software solutions
Can upgrade hardware easily	Optimised for the task and performance
Limited amount of features	Less OS related vulnerabilities

Host based IDS/IPS

Deployed on a computer which will monitor activities within only that server

Generaly can be defined as changed detection based on baseline system

IDS/IPS attack detection methods

Signature based

Based known attack pattern database
cannot detect new attacks or attacks due to zero day vulnerabilities
faster

Anomaly based

Comparatively resource intensive
need some time to setup as there is a training process
may generate many false positives

Advantages of network based IDS/IPSs

Fewer devices can be used to monitor a large network thus ease of management
less vulnerable for derect attacks

Disadvantages of network based IDS/IPSs

Since vast volume of network traffic will pass through the device may fail to recognize attacks at some rare situation
Cannot detect if an attack was successful or not
Will have a tough time with fragmented packets

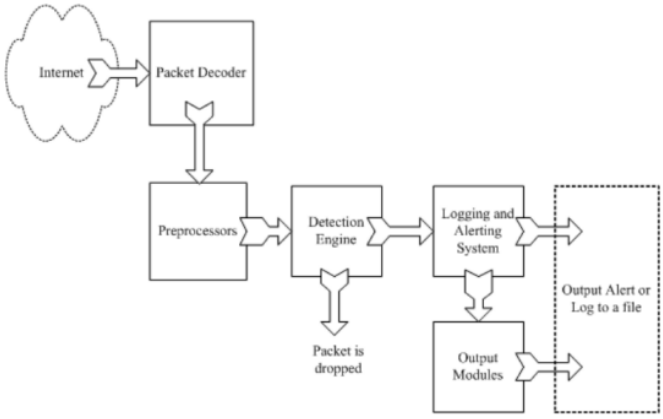
Advantages of host based IDS/IPSs

The traffic that are encrypted over network passed undetected by NIDS may'be available to analyze as the system is deployed locally in the host machine
Processing power available is more compared to NIDS

Disadvantages of host based IDS/IPS

Number of deployments will make the management difficult
vulnerable for direct and host attacks
Non host devices under attack cannot be detected
Can be intrusive to the performance of the host machine

Components of snort



Decoder

Get the packets from different types of network interfaces and direct it to preprocessor detection engine

Preprocessor

Defragmentation of packets

re-assemble TCP streams

Decode HTTP URI

Detection engine

Most important of the system

Could be rule based or anomaly based

Logging and alerting

Based on the detection and decision of detection engine, this module would generate alerts or logs

Reportig

Generates reports/statistical information


```
alert tcp $TELNET_SERVERS 23 -> $EXTERNAL_NET any (msg:"TELNET
  Attempted SU from wrong group"; flow:
from_server,established; content:"to su root"; nocase;
  classtype:attempted-admin; sid:715; rev:6;)
```