Cyber Security – Fundamentals with tools and techniques for defense

Cyber Security – Foundation Module

Part 2

12th January, 2024

Assessment plan

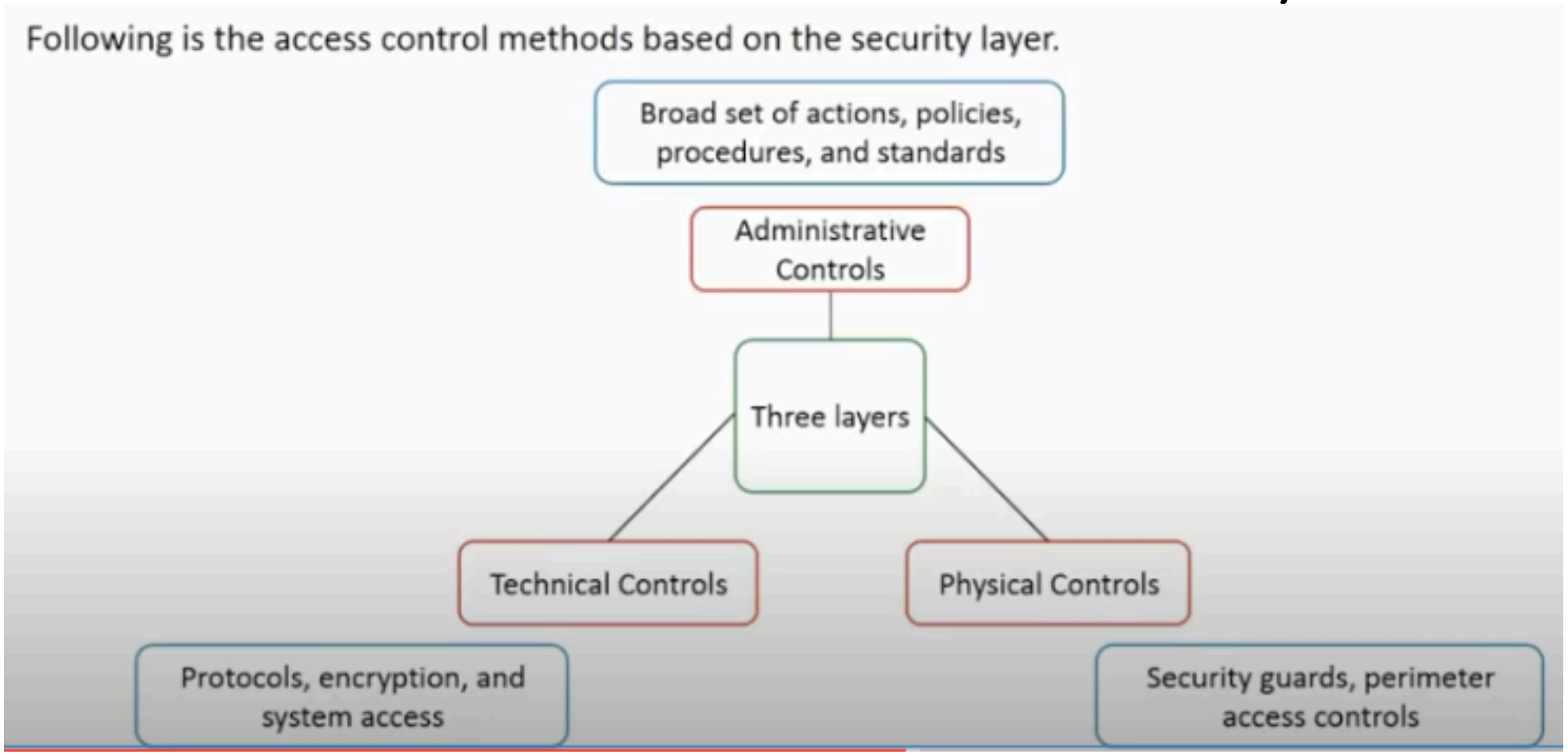
	Marks
Mid-sem exam (proctored)	30
End-Sem exam (proctored)	30
Assignments – 2	20
Practical – Cyber Bay tasks submit	15
Attendance	5

^Assess your laptops and arrange to make it work for Practical / hands-on

Authorization

- Authorization is a mechanism of verifying that a particular user is allowed to perform an action that user is attempting
- Does subject S have right R for object O
  - Subject: various users
  - Rights: Read, Write, Execute
  - Objects: Files, programs etc.
- In real world, this is often done as Role Based Access Control (RBAC). Various roles defined, users assigned to those roles, rights granted accordingly

Access Control Methods – 3 layers



Access Control Methods based on functionality

Following is the access control methods based on the functionality:

- Preventive: Avoid problems before they occur
- Detective: Detect a problem that has occurred
- Corrective: Correct the problem that has occurred
- Deterrent: Discourages someone from doing an act
- Recovery: Restore a resource from an event that has occurred
- Compensative: Provides alternative controls to other controls

Access Control Model

Access Control Model (ACM) are used for defining the access control mechanism and policy definition for any access to be defined.

Models

DAC (Discretionary Access Control)- Restrictive model as set by data owners

Subject has total control over objects which is determined by Data owner

MAC – (Mandatory Access Control) Most Restrictive Access Control Model – which is controlled by Operating system

End-User cannot set controls

RBAC (Role Based Access Control) - based on a user's role and implements key security principles

Assigns permissions to particular roles in the organization and then users are assigned to roles

ABAC (Attribute Based Access Control)

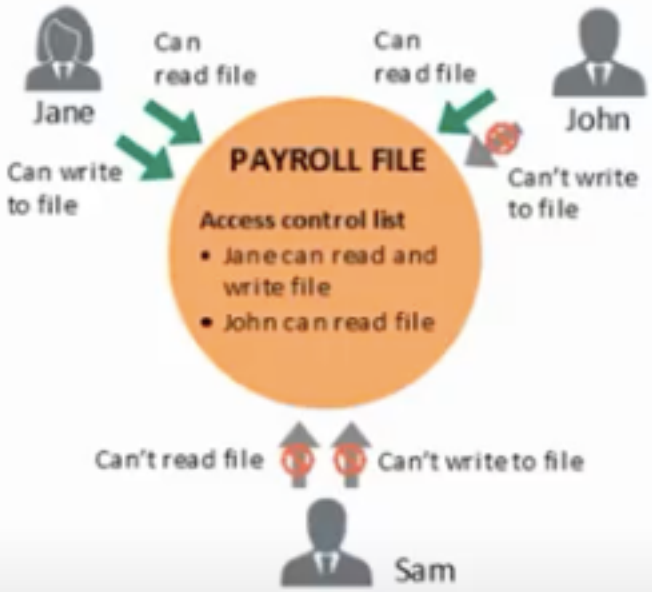
Dynamically assign roles to subjects based on a set of rules defined by a custodian / owner

Access Control Model- DAC (Discretionary)

The way in which a subject will access an object is guided by access control model. A model must be chosen to fulfill the directives of the security policy.

DAC Model:

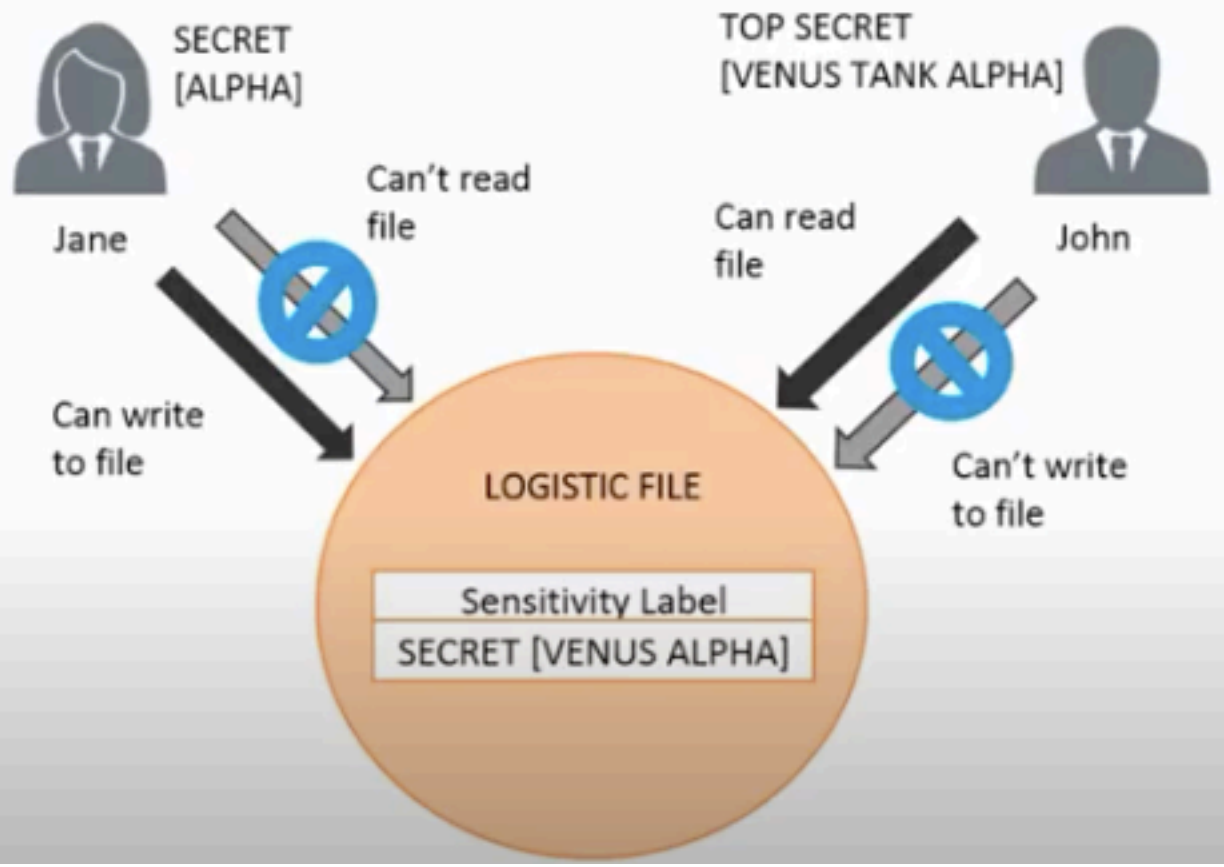
- Access to resources will be decided by data owners
- The access control depends on the owner's discretion and authorization granted to the users
- For enforcing the security policy, Access Control Lists (ACLs) are used



Access Control Model- MAC (Mandatory)

MAC Model:

- System's security policy is enforced by the operating system with the use of security labels
- The resources have security labels that contain data classifications and the users have security clearances
- When information classification and confidentiality is important, this model is used



Access Control Model- RBAC (Role Based)

A Role-Based Access Control (RBAC) model is also known as Non-discretionary Access Control.

Access is granted depending on subject's role and/or designation.

Following are the four commonly used RBAC architectures:

- Non-RBAC
- Limited RBAC
- Hybrid RBAC
- Full RBAC

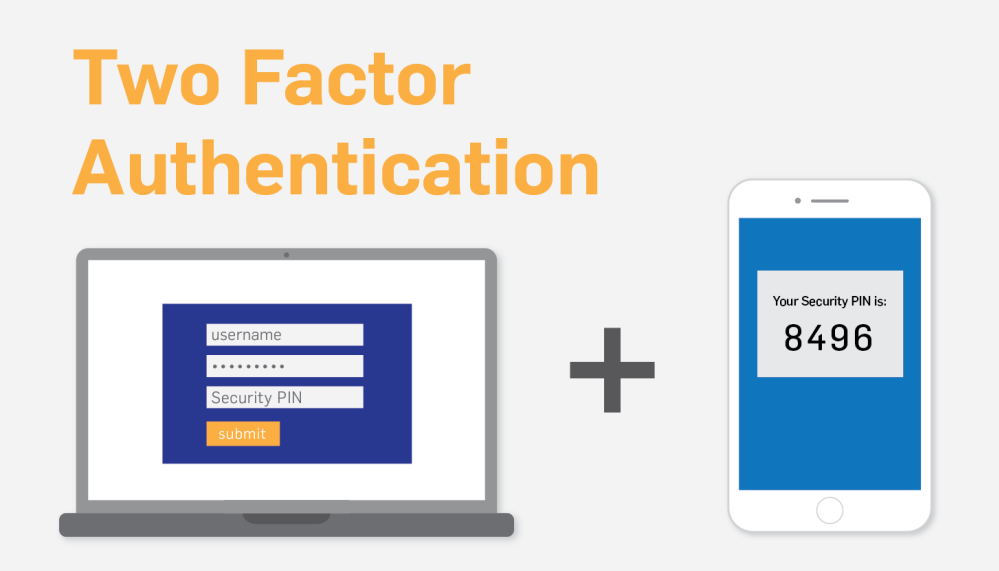
Access Control Model- ABAC (Attributes Based)

The following factors support different Access Control Models.

- **Rules for Access:** Rules decides how the subject can access the object
- **Constrained User Interface:** Constrained user interfaces restrict users' access to a system of application by disallowing them to view or use certain information or functions
- **Access Control Matrix:** It has subjects and objects in a table and indicates the actions a specific subject can take on an object
- **Content:** Based on the content within an object the access is granted
- **Context:** Decisions are made by "reviewing the situation"

AUTHENTICATION TECHNIQUES

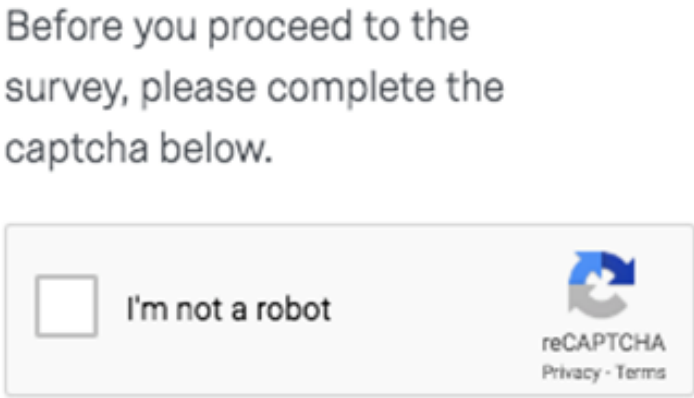
- Two-Factor Authentication
- Despite all the passwords, there are many services that allow you to add a second level of security, through the use of two-factor authentication. It can either be a code generated on your device or sent to your phone.
- At first glance, this type of authentication may seem much more reliable than simple passwords but there are some problems too.
- The problem is that the user could lose access to his SIM or a phone card or the process that is responsible for the code generating.



Source: [09/05/2019] https://shahmeeramir.com/4-methods-to-bypass-two-factor-authentication

AUTHENTICATION TECHNIQUES

- Captcha Test
- Its main goal is to make sure that you're not a robot. Users are asked to perform some tasks that bots are not capable of doing.
- Types of Captcha Test:
- 3D Super CAPTCHAs—requires identifying an image rendered in 3D
- CAPTCHA "I'm not a robot"—requires a user to check a box
- Marketing CAPTCHAs—requires typing a particular word or phrase related to the sponsor brand
- Math CAPTCHAs—require a user to solve a simple mathematician task



Source: [09/05/2019] https://www.qualtrics.com/support/survey-platform/survey-module/editing-questions/question-types-guide/advanced/captcha-verification/

AUTHENTICATION TECHNIQUES

- Biometric Authentication
- This security process relies on the unique biological characteristics of a person to verify whether it's true or not and that he's who is says he's.
- A user's biometric data is captured and then stored in the database.
- One of the main advantages of biometric data is that you won't be able to forget or lose it.

Source: [09/05/2019] https://www.onespan.com/blog/biometric-authentication-vendor-evaluation-javelin

AUTHENTICATION TECHNIQUES

- Types of Biometric Authentication

Finger vein identification	• Most common means of authentication that is used in the majority of digital devices
Face identification	• Capable of scanning and identifying your face
Voice identification	• Relies on specific characteristics created by the shape of the speaker's mouth and throat
Fingerscanning	• Resembles ink-and-paper fingerprinting process. This kind of authentication is also found as a Touch ID
Iris recognition	• Identifies people based on unique patterns within the ring-shaped region that surround the pupil of the eye

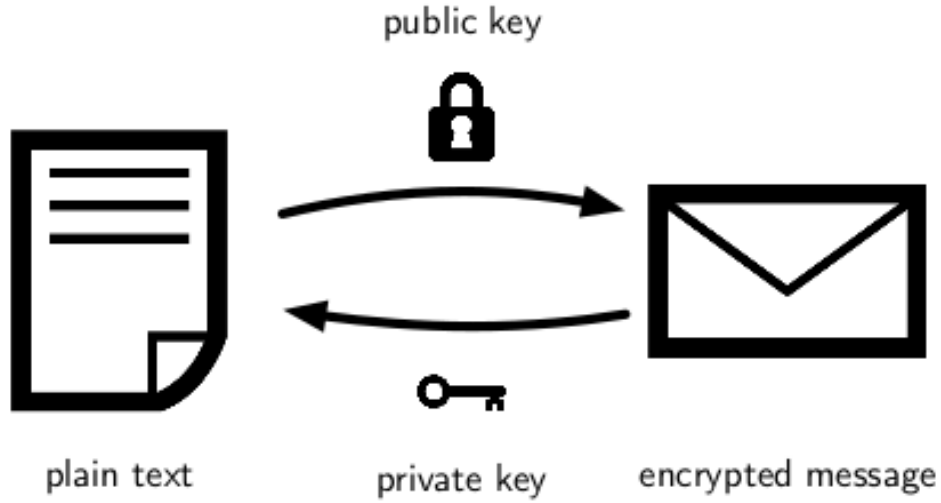
AUTHENTICATION TECHNIQUES

- Authentication and Machine Learning
- In future Machine will not only look at biometrical data, such as fingerprints, voice or face identification but also at human's behavior.
- Machines become more and more capable of observing and analyzing human behavior.
- For instance, our computer would be able of recognizing the way we type our messages or passwords or even the way we talk on the phone. As a result, by learning the way we behave ourselves, our devices will be able to determine their true owner and in case of danger to shut down or erase themselves.

Source: [09/05/2019] https://www.forbes.com/sites/allbusiness/2018/10/20/machine-learning-artificial-intelligence-could-transform-business/

AUTHENTICATION TECHNIQUES

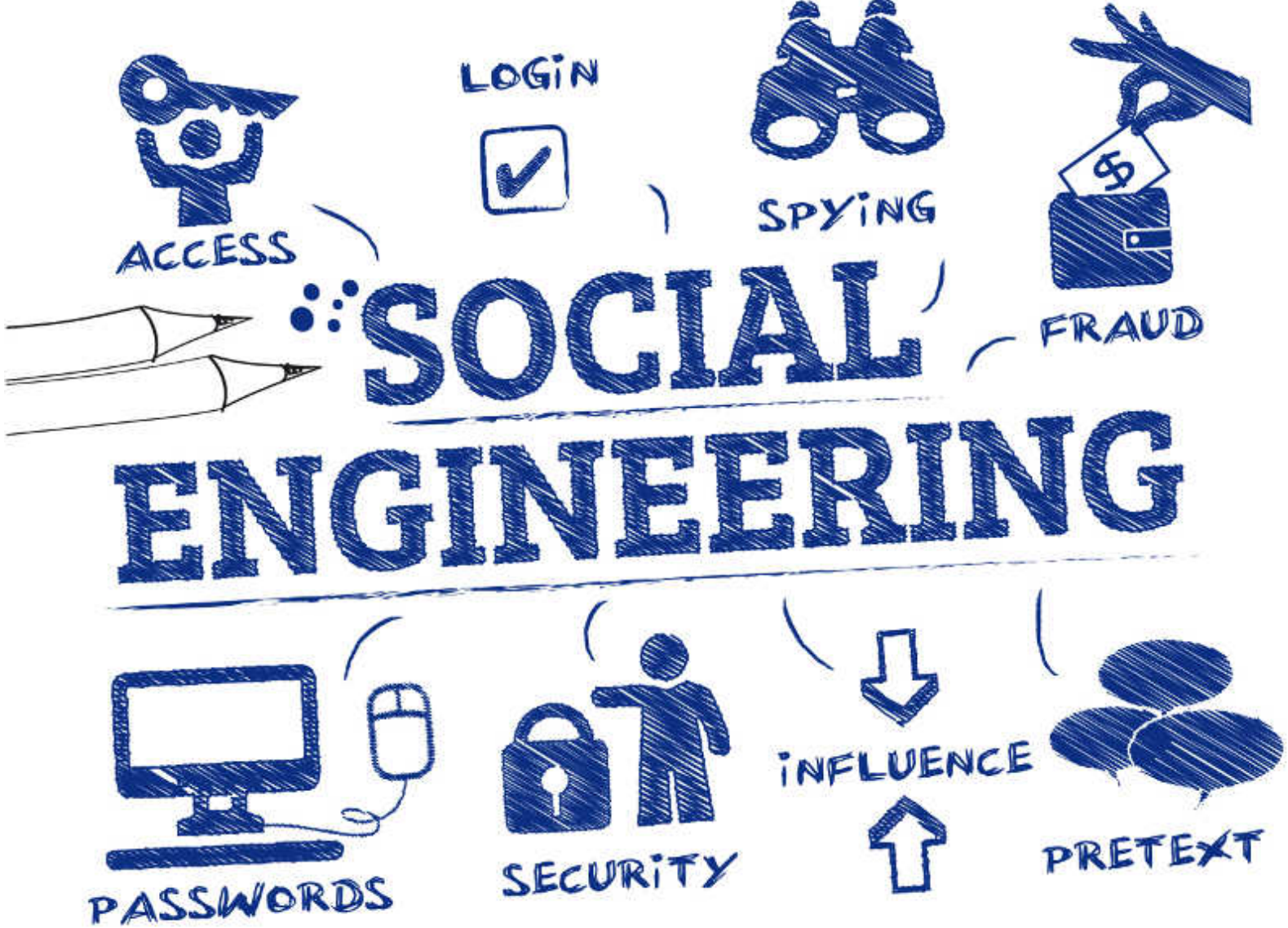
- Public and Private Key-pairs.
- This kind of authentication is the main characteristic of asymmetric cryptography. It can be mostly found in such systems as Bitcoin, but public and private key-pairs might easily find a use in the authentications systems as well.
- The user's private key can be stored on the device and the public one can be uploaded and stored on a service's servers. As a result, you'll be able to use the same key-pair for various services.



Source: [05/05/2019] https://securecompliance.co/protecting-business-data-protection-day//

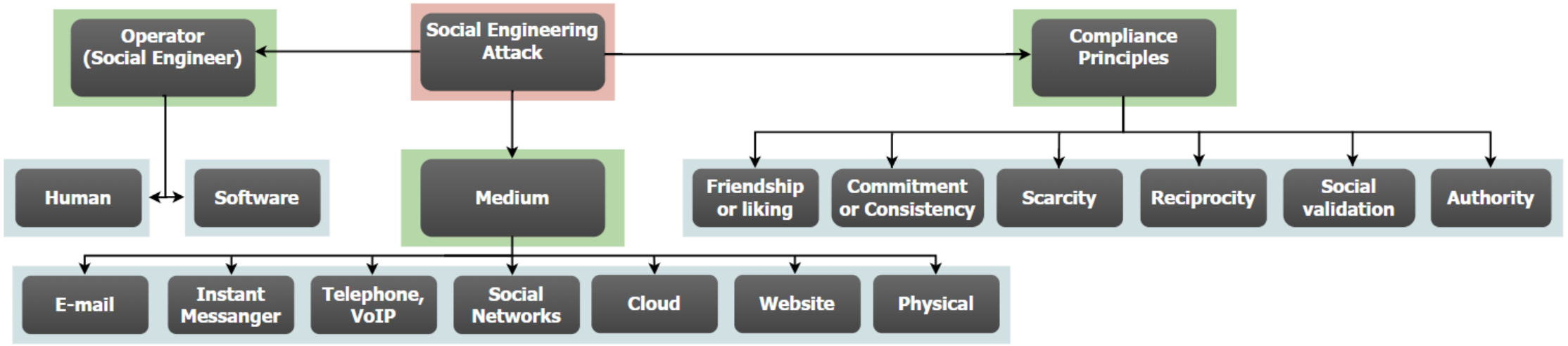
Part III

Social Engineering – Security threats



Definition: *Social Engineering is a combination of social, psychological and information gather techniques that are used to manipulate people to gain access to information or locations that the hacker is not authorized to access*

Social Engineering Taxonomy



Attack Vectors

Dumpster Diving | Advanced Persistent Threat | Baiting | Tailgating | Surfing Online Content | Pretexting | Vishing

Phishing | Shoulder Surfing | Reverse Social Engineering | Waterholing | Trojan Horse | Role Playing | Quid Pro Quo

Empathy

Greed

Inquisitiveness

Anxiety

Sympathy

Emotions

Fear

Effects of Social Engineering

Social engineering has serious consequences. Because the objective of social engineering is to coerce someone to provide information that leads to ill-gotten gains, anything is possible

User passwords.

Security badges or keys to the building and even to the computer room.

Intellectual property such as design specifications, source code, and other research-and-development documentation.

Confidential financial reports.

Private and confidential employee information.

Personally identifiable information (PII) such as health records and credit card information.

Customer lists and sales prospects.

Types of Social Engineering Attacks

Phishing

It is an attempt to acquire sensitive information by masquerading as a trustworthy entity via an electronic communication, usually an email. Such attacks rely on a mix of technical deceit and social engineering practices.

Vishing

Attackers directly involve in a digital conversation to gather information using voice solicitation techniques and digital messaging techniques

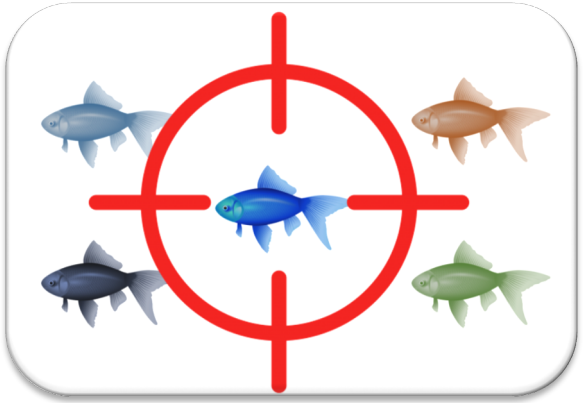
Impersonation

Attacker identify a way to enter into your facility like a courier delivery executive or tech staff to check internet connectivity etc. to gather valuable information of organisation

Top 10 Phishing Attack Emails

1. Security Alert – 21%
2. Revised Vacation & Sick Time Policy – 14%
3. UPS Label Delivery 1ZBE312TNY00015011 – 10%
4. BREAKING: United Airlines Passenger Dies from Brain Hemorrhage – VIDEO – 10%
5. A Delivery Attempt was made – 10%
6. All Employees: Update your Healthcare Info – 9%
7. Change of Password Required Immediately – 8%
8. Password Check Required Immediately – 7%
9. Unusual sign-in activity – 6%
10. Urgent Action Required – 6%

Phishing Types



Spear Phishing - Attackers use focuses on specific individuals correlating information found on social media and elsewhere to initiate a pointed attack

Whaling - Attacker concentrate on high value individuals, generally senior management staff of an organisation following spear phishing technique to infiltrate and steal valuable organisation data

Pre-texting – Attacker pretend to be the victim and call organisation helpdesk to gather information or penetrate by asking the IT helpdesk executive to click a link to take control of organisation system and escalate privileges

Vishing Types

Phone Vishing: Attacker directly calling an individual or a group attempting to gain access to account information to penetrate and modify confidential information of an organization

SMSishing: Attacker uses a text or an image or a web link to gain information to victim's digital device to steal valuable personal and organization information

Sextortion

Sextortion is a widely used form of online blackmail where a cyber scammer threatens to reveal intimate images or videos of someone online

often to their friends, family, work colleagues, or social media lists

unless they pay a ransom quickly

De Logan Meyer <hbcarmitaoh@outlook.com>
Sujet **xxxx - 515549** 21/07/2018 21:11
Pour xxxx@xxx-xxxxx.xxx <xxxx@xxx-xxxxx.xxx>
Date Sat, 21 Jul 2018 19:11:59 +0000
Identifiant du message <PS2PR02MB2901ECEF5E49F76CD47263DBB0500@PS2PR02MB2901.apcprd02.prod.outlook.com>
Received from mail-oln040092255060.outbound.protection.outlook.com (HELO APC01-

I do know 515549 one of your passphrase. Lets get straight to point. Absolutely no one has paid me to investigate you. You do not know me and you are probably wondering why you are getting this email?

actually, I actually placed a malware on the adult vids (pornography) web site and do you know what, you visited this web site to experience fun (you know what I mean). When you were viewing video clips, your web browser started out working as a Remote Desktop that has a key logger which provided me accessibility to your display as well as web cam. Immediately after that, my software obtained all of your contacts from your Messenger, FB, and e-mailaccount. After that I created a double-screen video. 1st part displays the video you were watching (you've got a good taste ;)), and second part shows the recording of your web cam, & its u.

You will have 2 options. Shall we understand each of these choices in particulars:

First alternative is to ignore this message. In this case, I am going to send out your recorded material to all of your personal contacts and thus consider concerning the disgrace you feel. And as a consequence should you be in a relationship, how it will eventually affect?

Next alternative is to pay me $1000. Lets describe it as a donation. In this scenario, I will instantly erase your video. You could continue on your life like this never took place and you would never hear back again from me.

You'll make the payment through Bitcoin (if you don't know this, search "how to buy bitcoin" in Google).

BTC Address to send to: 1P6V4q85b7guyEUnAzQDEga3BL2hrVDEPP
[CASE-SENSITIVE copy and paste it]

In case you are making plans for going to the law enforcement officials, very well, this e mail cannot be traced back to me. I have dealt with my actions. I am not trying to demand so much, I simply want to be paid for. You now have one day to pay. I've a special pixel in this e-mail, and at this moment I know that you have read through this message. If I do not get the BitCoins, I will certainly send your video to all of your contacts including friends and family, colleagues, and many others. Nonetheless, if I do get paid, I'll erase the video right away. If you want proof, reply with Yea & I will certainly send your video to your 13 friends. It's a non-negotiable offer so don't waste my personal time and yours by replying to this message.

NDTV Video

https://www.ndtv.com/india-news/inside-indias-otp-mafia-how-a-call-from-a-beautiful-woman-can-turn-your-life-ugly-4333949#:~:text=A%20retired%20government%20employee%20one,up%20paying%20money%20out%20of

Get Rid of Sextortion

Don’t panic

Don't communicate further with the criminals

Change your password to the mail id (in case you got mail from your own id)

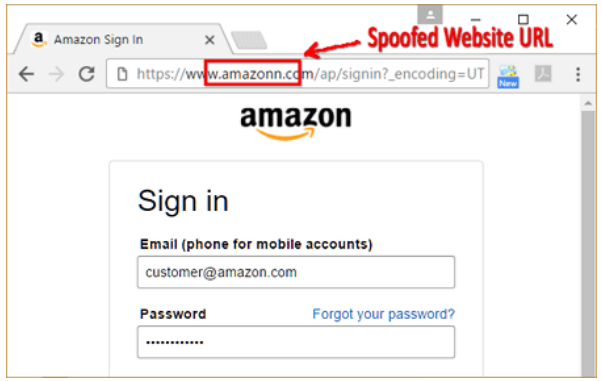
Don't pay

Preserve evidence that was used by the hacker to communicate

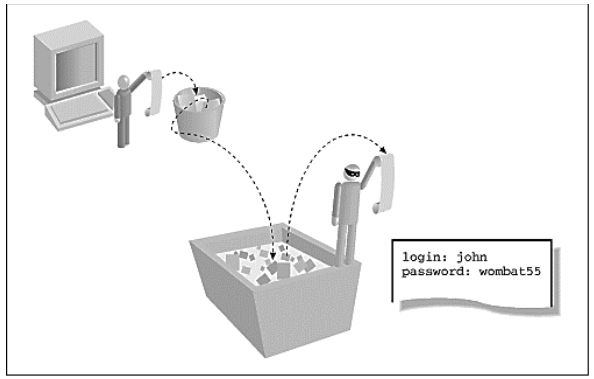
If it is repeated, give a complaint to Cyber Crime cell of Police

Social Engineering and Social Media Security

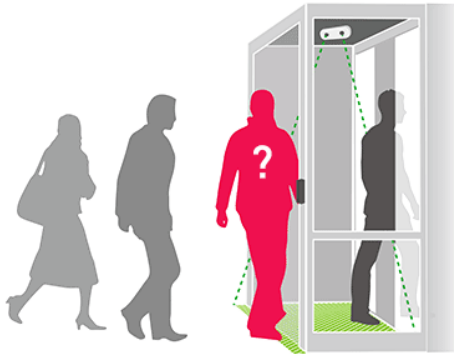
Impersonation



Pharming – Attacker redirects victims to a duplicate website, even if the user correctly entered the intended site



Dumpster Diving – Attacker search the trash of an organisation to gather deleted data in digital environment



Tailgating - Attacker used to gain access to secured areas, that typically involves following a person into an area with access restrictions.

Baiting/Quid pro quo - Attacker would make the victim to grab a digital device that has pre-installed malware to be used in organisation computers to steal information

Social Engineering and Social Media Security

Social Media Security

People accidentally or unknowingly post personally identifiable information (PII) or confidential information on the Internet.

This may include employees sharing information specific to their organizations too.

Additionally, it is also not easy to delete such information once posted on the Internet in most cases.

Source: [04/01/2019] https://www.securitymagazine.com/articles/86902-the-evolution-of-social-media-monitoring-in-corporate-security

Social Engineering and Social Media Security

Intelligent Hacks

- Use data disabled charger
- Carry you own power bank
- Disable data transfer option in your phone while charging
- May be switching off is a better idea

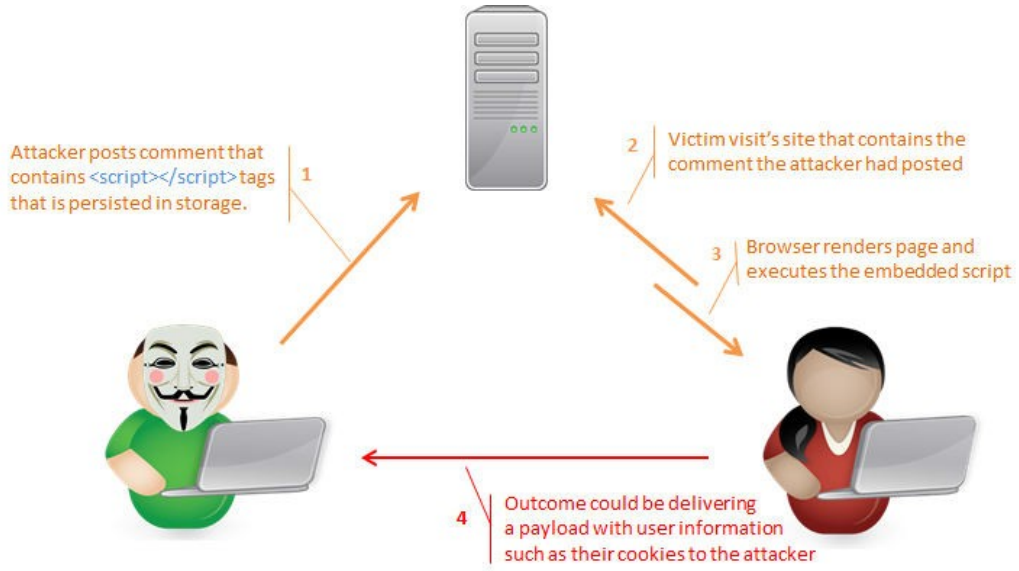
Juice Jacking

https://www.youtube.com/watch?v=ezy03Y6xbbw

Part IV

Application Security

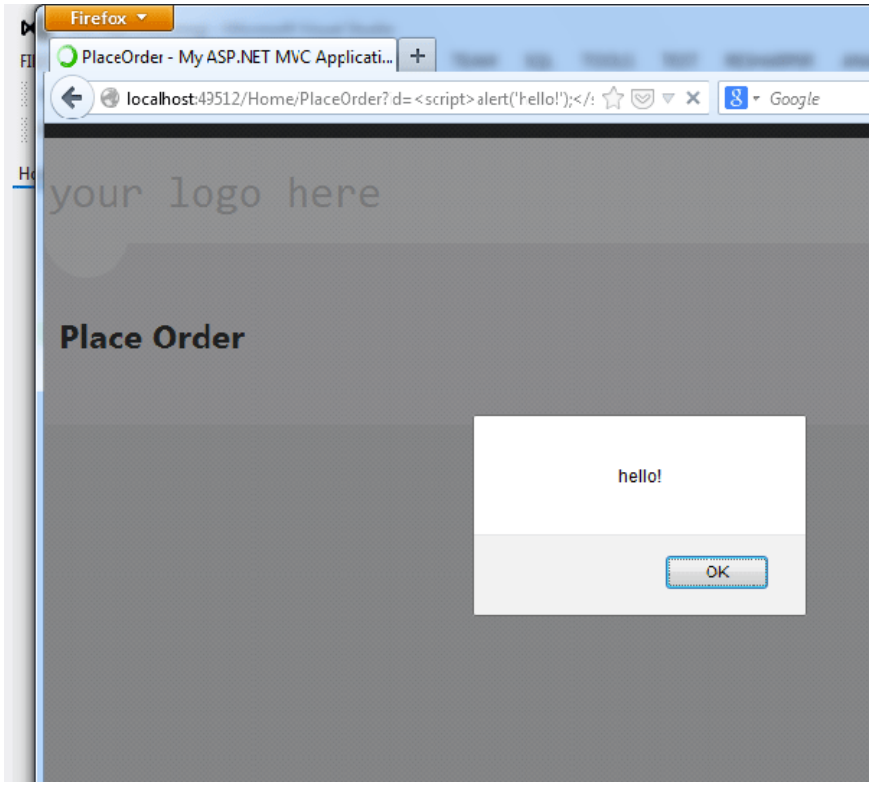
Cross Site Scripting



Cross site scripting allows attackers to inject client side script into a web page viewed by others.

It allows attackers to bypass access controls, gain potentially confidential information.

Mitigating XSS

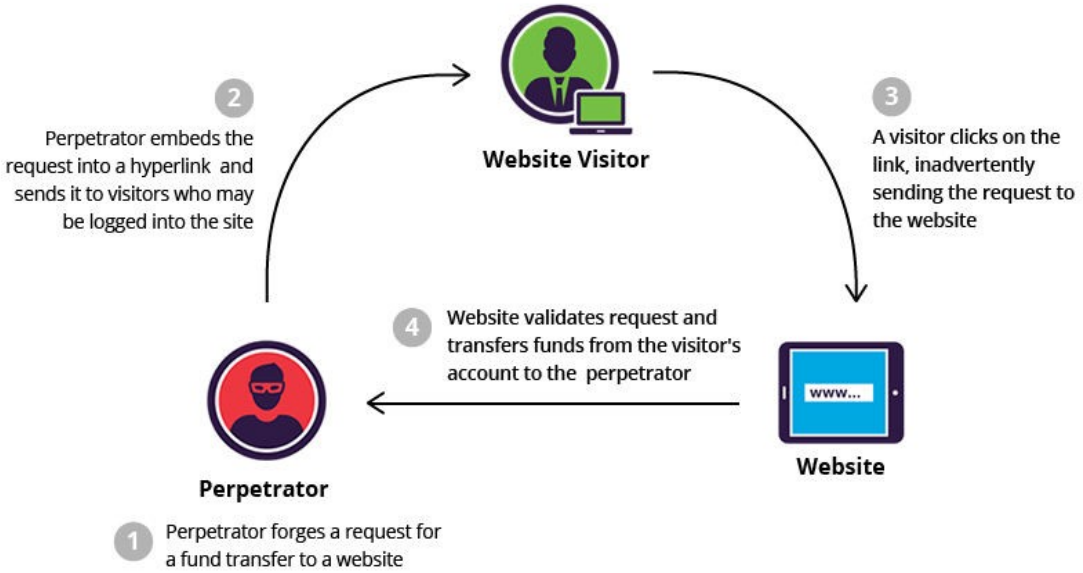


Do not trust anything coming from the browser, validate user input.
Note: Example of client side vs. server side validation

Escape HTML before inserting into your application.
Note: Use standard libraries rather than writing your own stuff

Use HTML encoding

Cross Site Request Forgery (CSRF)



CSRF is an attack wherein a malicious attacker forces an end user to execute unwanted actions on a web application in which they're currently authenticated.

Suppose a website allows users to delete their account via a delete button that points to: http://www.website.com/deleteuser.do

CSRF would occur if an attacker asks a logged in user of the website to visit his page and it has this HTML

<img src=http://www.website.com/deleteuser.do>

CSRF: Prevention

- Referrer header
- CSRF tokens

<form action="/transfer.do" method="post"> <input type="hidden" name="CSRFToken" value="OWY4NmQwODE4ODRjN2Q2NTlhMmZlYWE.

..

wYzU1YWQwMTVhM2JmNGYxYjJiMGI4MjJjZDE1ZDZ.

.. MGYwMGEwOA==""> … </forŵ>

Security Misconfiguration

While many possible ways misconfiguration can lead to security issues, focus on three key areas for this discussion:

- Unpatched software or software misconfiguration
- Improper file / directory permissions
- Default accounts with their default passwords

Security Misconfiguration: Incorrect Setup

Corporate blogs should not allow users to register for Wordpress accounts.

What happens if such a feature is not removed?

Could this lead to a total compromise of their system?

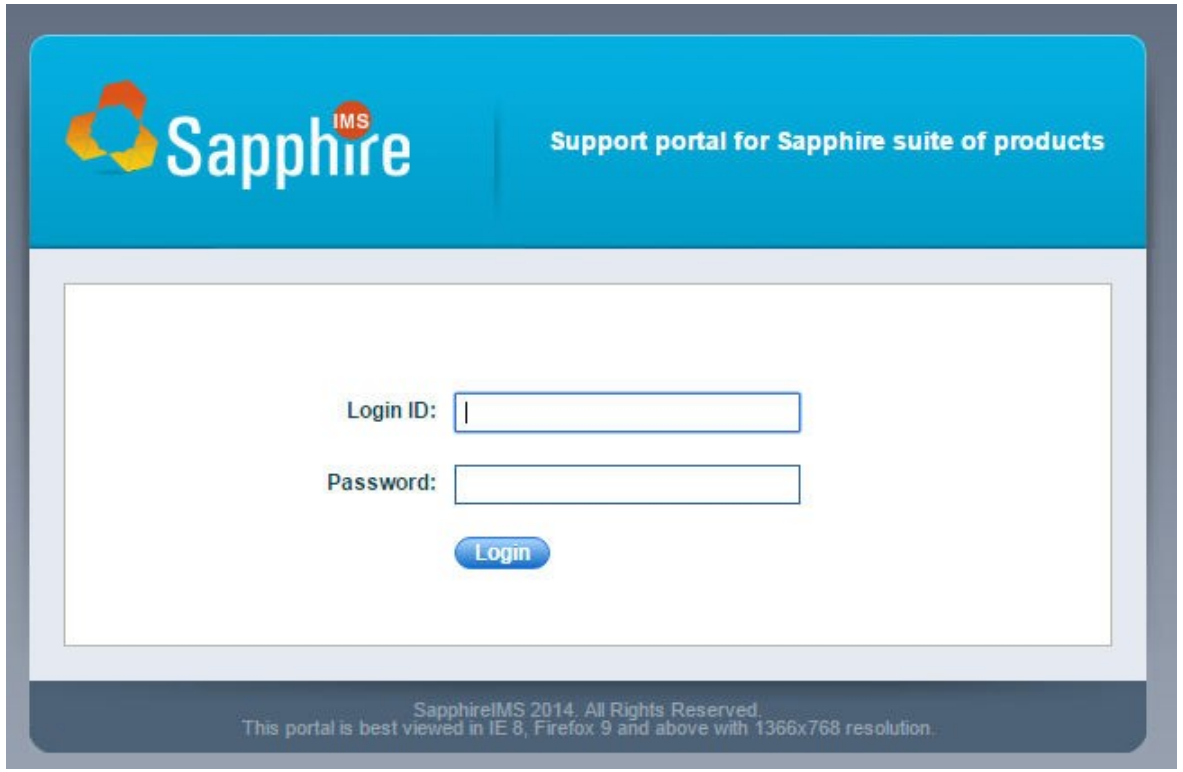
Security Misconfiguration: Directory Traversal

This is a vulnerability that allows attackers to access restricted directories and execute commands outside of the web server's root directory.

It can also be exploited to gain shell access to the underlying operating system

It can lead to significant leak of confidential information, configuration details

Security Misconfiguration: Default Passwords



Google Dork:

login ID :Sapphire

password :IMS 2014.

SQL Injection

SQL Injection is an attack wherein an attacker can execute malicious SQL statements into an application.

Using SQL injection, attackers can bypass an application authentication authorization controls and retrieve the contents of the entire database.

In some cases, the attacker can even spawn a shell on the remote DB server leading to complete compromise

Broken Auth & Session Management

- User authentication Credentials are protected & stored using hashing or encryption.
- Credentials can be guessed or overwritten through weak account management functions (e.g., account creation, change password, recover password, weak session IDs).
- Session IDs are guessable or exposed in the URL
- Passwords, session IDs, and other credentials are sent over unencrypted connections.
- No checks / controls over brute forcing

Part V

Introduction to Cryptography

Foundation

Cryptography is the art and science of keeping messages secure. It is the process of encrypting plain text using a key into cipher text.

Representation

- Encryption: $E_{K1}(M) = C$
- Decryption: $D_{K2}(C) = M$

Key Objectives:

- Authentication
- Integrity
- Non-Repudiation

History

Steganography: Hiding text via variety of mechanisms. Example: Tattoo on a bald head.

Substitution Cipher: Each plain text character is replaced by another character. Example: Caesar cipher

SUMIT (PlainText)
11111 (Key: Monoalphabetic Subsitution)
TVNJU (Encrypted Text)

SUMIT (PlainText)
12312 (Key: Polyalphabetic Subsitution)
TWPJV (Encrypted Text)

History

Transposition Cipher: Plain text characters are not substituted, just their order is changed

Plain Text: This class is at IIIT-B
Transposition: On a pre-defined grid size (5x4)

T	H	I	S	C
L	A	S	S	I
S	A	T	I	I
I	T	-	B	

Encrypted Text: TLSI HAAT IST-SSIB CII

Functions: One Way & Trapdoor

One Way Functions: They are relatively easy to compute but hard to reverse.

Given x, it is easy to calculate y = f(x). However, given f(x), it is very hard to calculate x. (4x3 = ? – easy .. But 12 = x * y)

Example: breaking a white porcelain plate.

Trapdoor functions: They are easy to compute but hard to reverse. However, if a secret is known, you can compute in the reverse too.

Example: easy to take apart a watch but difficult to put it together. However, having a manual makes the reverse process easy too.

Functions: Hashes

Hashing is a function which produces fixed length output for variable length input.

Hashing is a one way function: knowing the plain text, you can easily create the hash. But you will be hard pressed to figure out the plain text from a hash value

A good hash function is collision free; meaning there is no other plain text which when hashed produces the same hash.

Algorithms: Symmetric

Symmetric Key Algorithms are those where the same key is used to encrypt as well as decrypt.

An important requirement (and a significant challenge with these algorithms) is that the sender and receiver are able to exchange keys securely

Further divided into:

- Stream: Operate on a single bit at a time
- Block: Operate on a block (64 bits) at a time

Algorithms: Asymmetric

Asymmetric Key Algorithms (Public key algorithms) are those where the key used to encrypt is different from the one used to decrypt.

Further, the decryption key can not be derived from the encryption key

There are two keys: public key (known to everyone) and private key (known only to the owner) and these keys are mathematically related

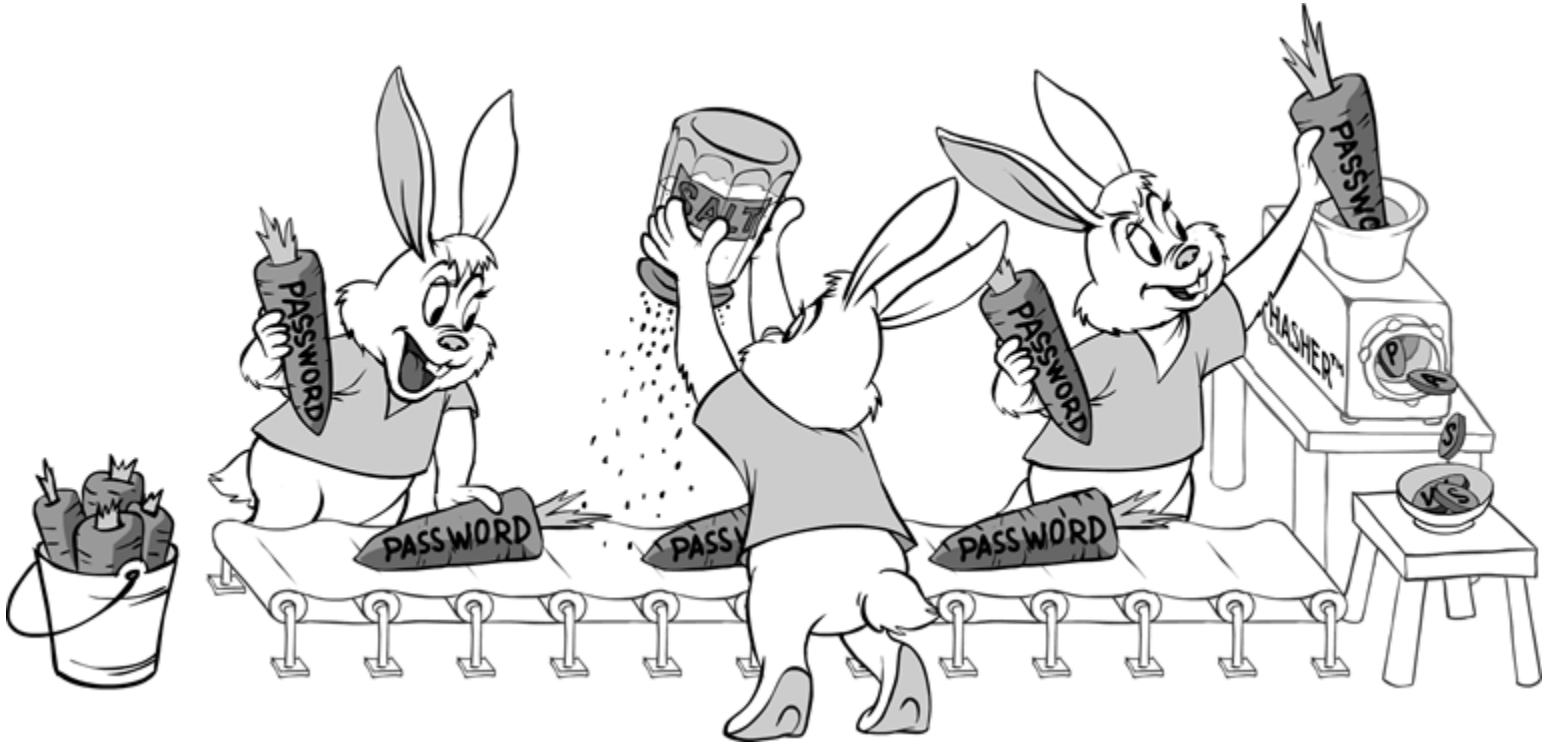
Algorithms: Comparison

- Public key algorithms are slow.
- Symmetric key algorithms are at least 1000 times faster
- Symmetric key algorithms have challenges with key exchange
- Sometimes a hybrid approach makes most sense

Cryptography and it's Significance in security

Hashing

Passwords are usually stored in a hashed format due to the security provided by its one-way-ness. However, even though it isn't possible to reverse the hash process directly, it's possible to reverse-engineer a hash.



Source: [04/01/2019] https://accu.org/index.php/journals/2159

Cryptography and it's Significance in security

Hashing

Characteristics of a hash function are as under:

1. It must be one-way. This means that it is not reversible. Once you hash something, you cannot un-hash it.

2. Variable-length input produces fixed-length output. This means that whether you hash two characters or two million, the hash size is the same.

3. The algorithm must have few or no collisions. This means that hashing two different inputs does not give the same output.

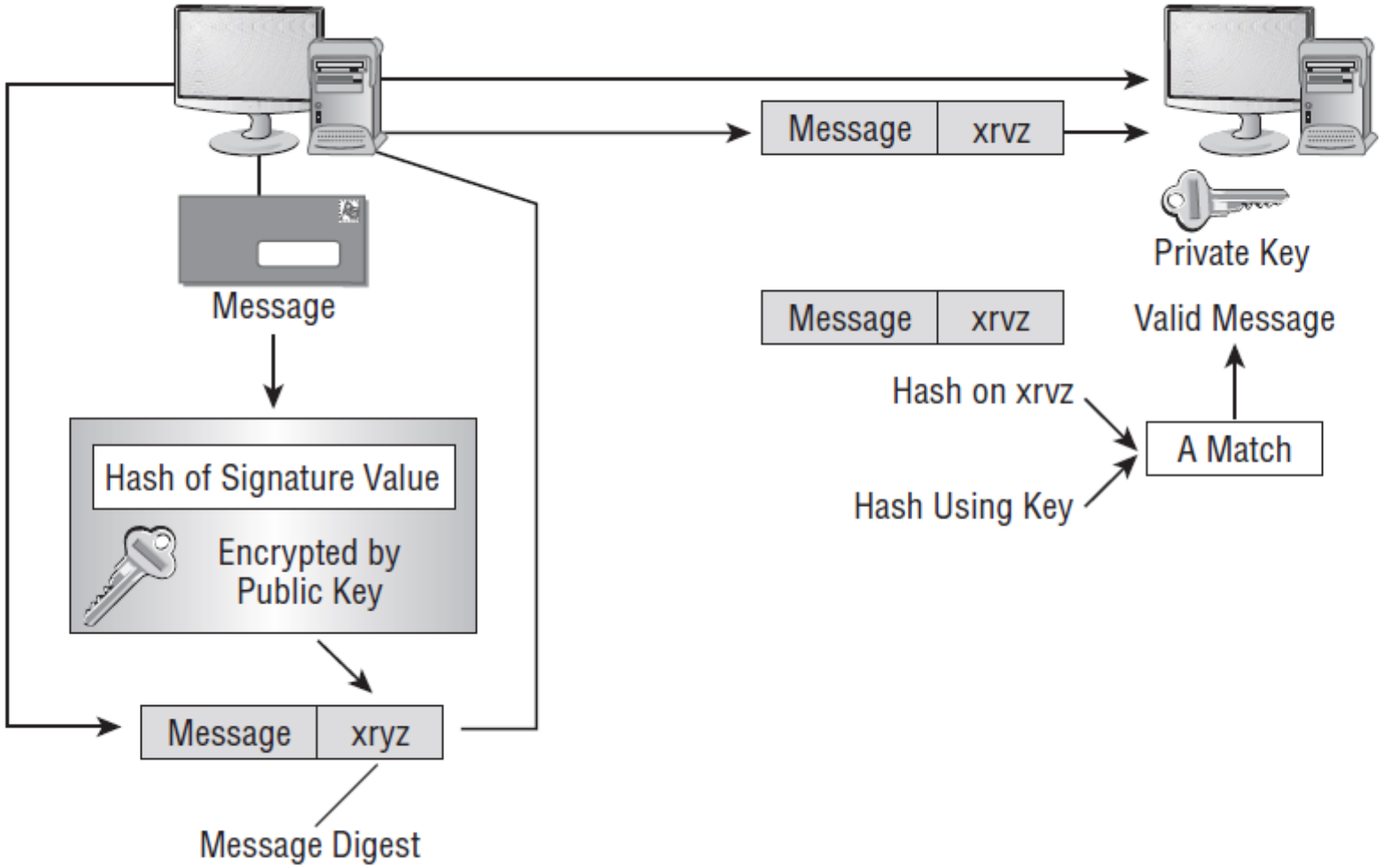
Cryptography and it's Significance in security

Digital Signatures

- A digital signature is an electronic mechanism to prove that a message was sent from a specific user (that is, it provides for non-repudiation) and that the message wasn't changed while in transit (it also provides integrity).
- Digital signatures operate using a hashing algorithm and either a symmetric or an asymmetric encryption solution.
- The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message.
- Most digital signature implementations also use a hash to verify that the message has not been altered, intentionally or accidently, in transit.

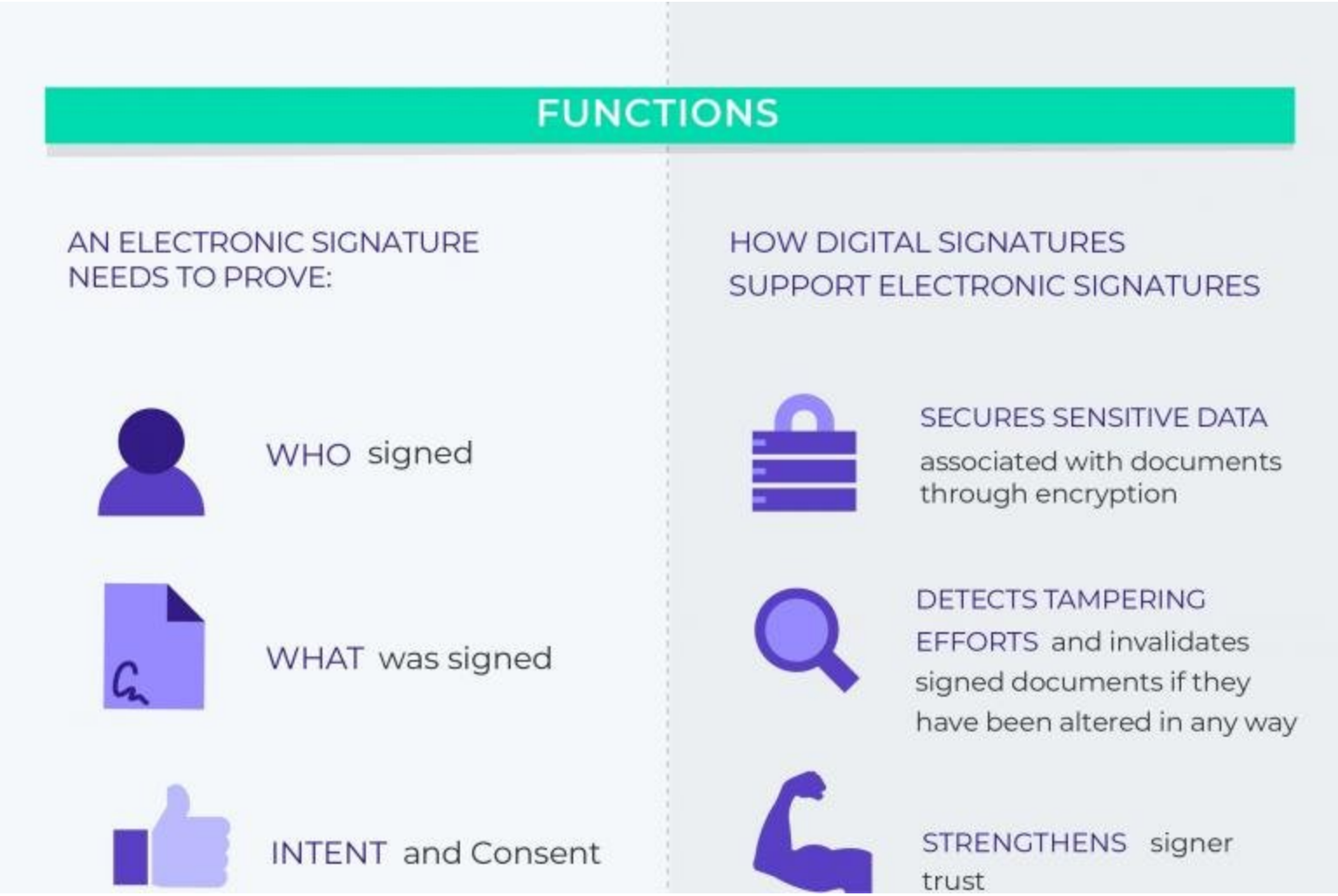
Cryptography and it's Significance in security

Digital Signatures

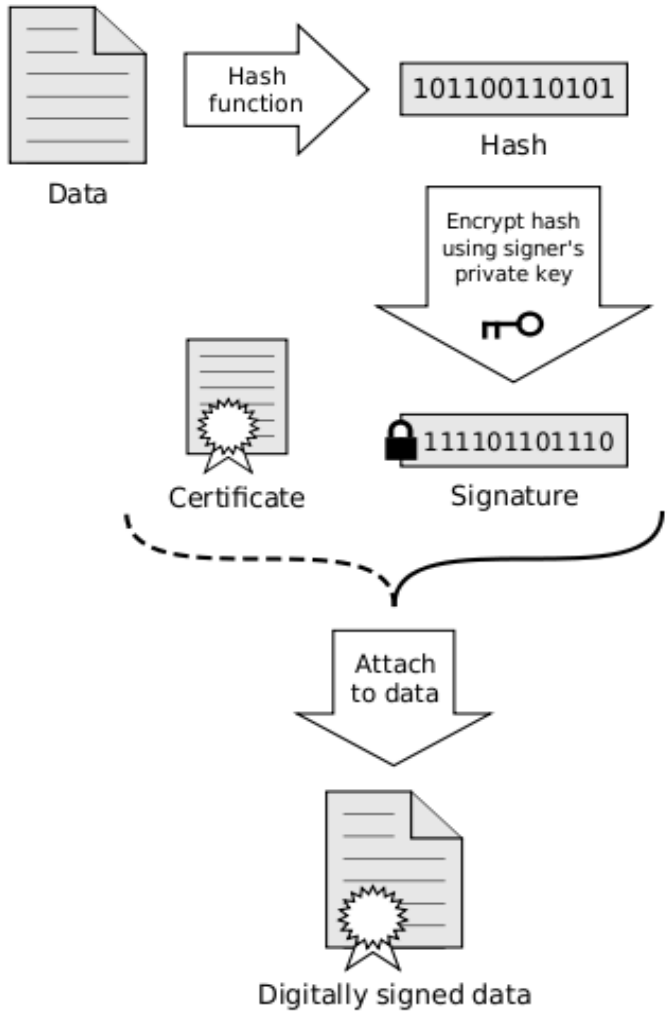


Source: Emmett Dulaney, Chuck Easttom (2014), *CompTIA® Security+™ Study Guide*, Sixth Edition, John Wiley & Sons

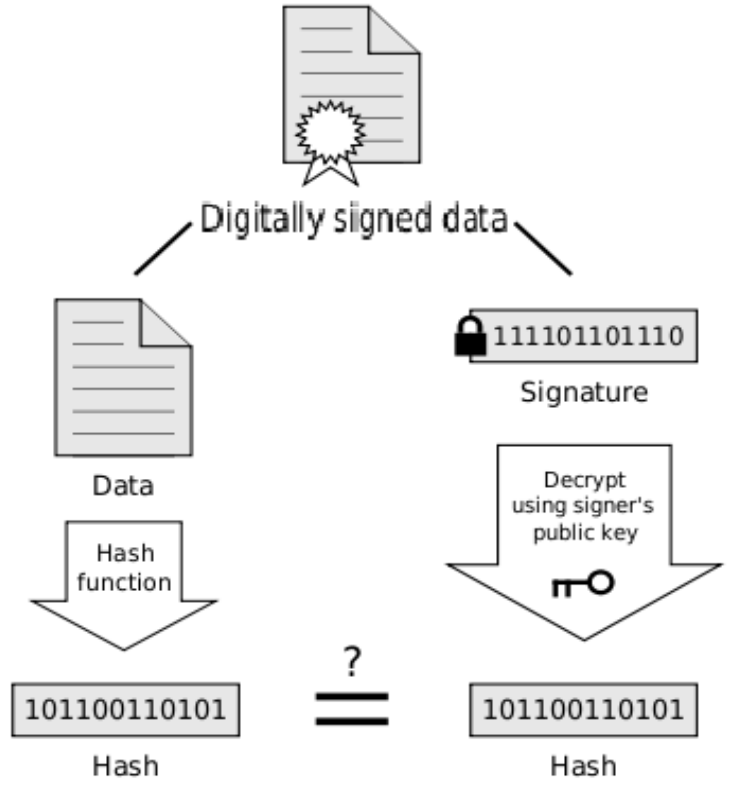
Digital Signature Functions



Signing



Verification

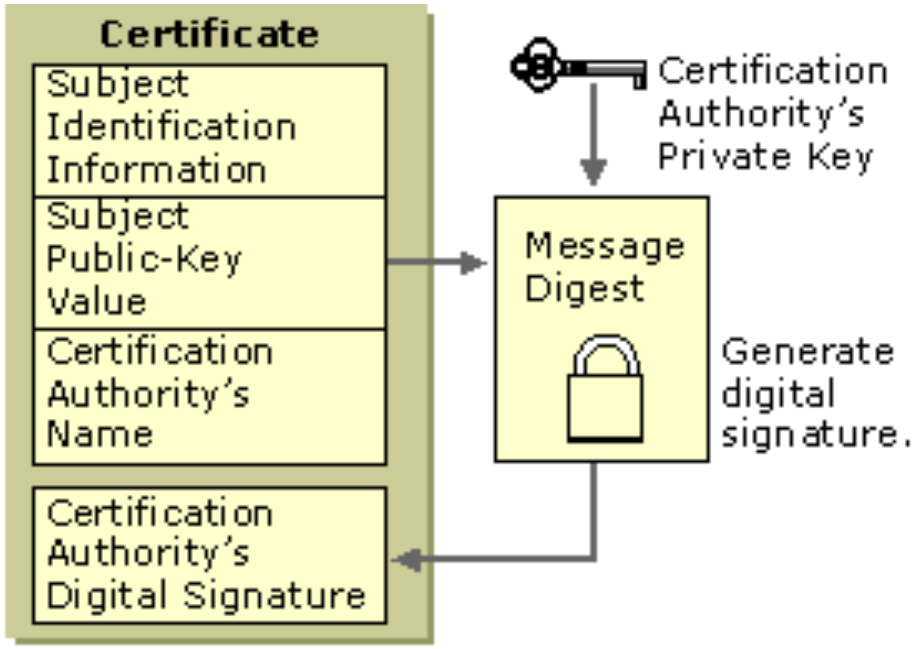


If the hashes are equal, the signature is valid.

Cryptography and it's Significance in security

Digital Certificates

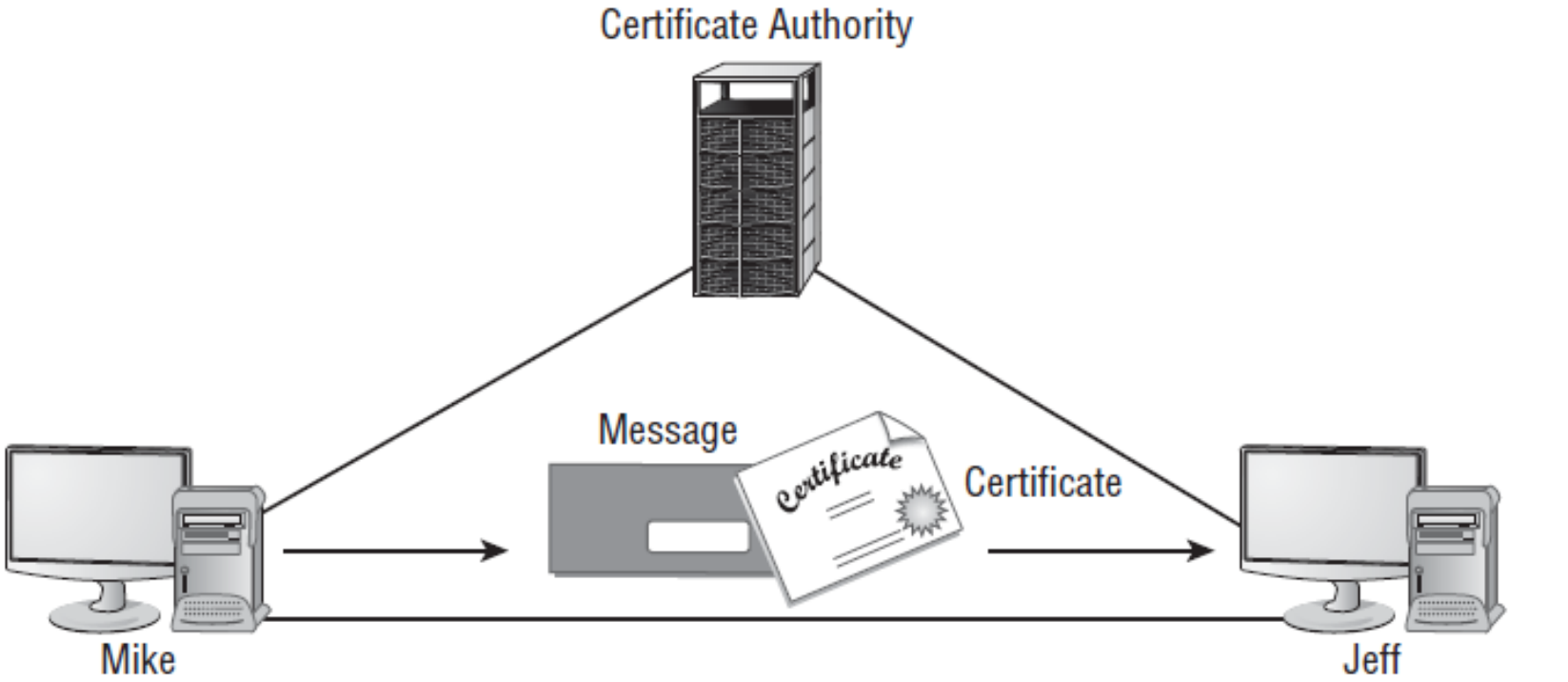
- A certificate is nothing more than a mechanism that associates the public key with an individual.
- Digital certificates serve a single purpose: proving the identity of a user or the source of an object.
- They don't provide proof as to the reliability or quality of the object or service to which they're attached; they only provide proof of where that product or service originated.
- Certificates work under a theory known as the trusted third party. This theory states that if user A trusts user C and user B trusts user C, then user A can trust B and vice versa.



Source: [14/04/2018] https://technet.microsoft.com/en-us/library/cc962029.aspx

Cryptography and it's Significance in security

Digital Certificates



Source: James Michael Stewart (2014), *CompTIA® Security+™ Review Guide*, John Wiley & Sons

PUBLIC KEY INFRASTRUCTURE

There is no single standard that defines the components of a Public Key Infrastructure, but a PKI typically comprises of the following components:

Certification Authority (CA)	• Acts as the root of trust in a public key infrastructure and provides services that authenticate the identity of individuals, computers, and other entities in a network.
Registration Authority (RA)	• Is certified by a root CA to issue certificates for specific uses permitted by the root.
Certificate Database	• Saves certificate requests and issued and revoked certificates and certificate requests on the CA or RA.
Certificate Store	• Saves issued certificates and pending or rejected certificate requests on the local computer.

Assignment 1

Cyber Threats in Health care sector and preparedness of the industry

Case study – Attack on All India Institute of Medical Science (AIIMS)

Deadline for submission : 1st Feb. 2024 by 23.59 hrs.