Problem 1

Compare and contrast symmetric and asymmetric encryption. Discuss the advantages and disadvantages of symmetric and asymmetric encryption methods when securing web services.

Symmetric encryption

The idea behind symmetric encryption is that, in contrast with assymetric encryption, the same cryptographic key is used to both encrypt and decrypt a messege. To do that, both parties in an exchange need to share a key. Since it should remain secret, it also acts as an authentication method.

Advantages

- fast and easy to compute

Disadvantages

- key distribution - a new key is required for every new pair of users, which may introduce problems when keeping track of many keys
- limited, algorithm dependant lenght, which may limit the possibilities of developing new algorithms (which might be needed in the future, computing power keeps growing which might eventually lead to current secure encryption algorithms being broken in the future)
- requires a secure way to share the key with the receiver without compromising its secrecy

Asymetric encryption

When it comes to assymetric encryption, a pair of mathematically related keys is generated. One of them serves as the public key, and the other as the private key, to be kept secret from everyone else. Either of them can serve any of the two possible roles, but once it has been decided, which one is public and which one is private needs to remain unchanged - doing otherwise would compromise the secrecy of the encryption process.

Assymetric encryption be used for both confidentiality and integrity checks, depending on which key is used to encrypt the messege. When confidentiality is the priority, the sender uses the public key of the recipient to encrypt the messege and the recipient uses their private key (which, presmebly, only they have access to to decrypt it. However, if we want to ensure the integrity and verify that it was indeed the sender who has sent the messege, sender A would use their private key to encrypt the messege and recipient B would use A's public key to decrypt it, thus verifying that it has indeed come from A. This technique is used in digital signatures.

Advantages

-solves the key distribution problem posed by symmetric encryption (public key can be shared freely)

- unlimited lenght (the longer the key, the harder it is to break)

Disadvantages

- requires a working public key infrastructure
- requires a trusted directory service

Both types of encryption are often used in combination to establish trust when two parties want to exchange their public keys in a secure manner - they are exchanged via assymetric encryption and after that the communication continues with the use of shared private keys. Their strenght combined allow for effective security of web services via the use of session keys in the begenning of the exchange.

Ouriginal: 2%

Comment:
P+

Question **2**

Complete

Mark 3 out of 3

Problem 2

You are going to create a security policy for a large company called EarthY. The CEO has told you that the most important thing for EarthY is to make sure that all services and data of the company are always available.

a) Describe the C.I.A. triad. What part of the C.I.A. triad is the most important for the specific security policy you are creating, given what the CEO has told you?

b) Give three examples of incidents that may affect the availability of EarthY's services.

c) The CEO of EarthY has told you that he wants you to implement the Bell-LaPadula model to preserve data integrity. Explain to the CEO why the Bell-LaPadula model does not preserve integrity and suggest a model that preserves integrity.

a) The CIA triad constitutes the three properties that information security aims to maintain. These are

Confidentiality - only authorized users should be able to view protected data (data should remain secret and private)

Integrity - only authorized users should be able to modify or delete protected data (seeks to prevent tampering)

Availability - while maintaining the previous two, the system should remain available when needed by authorized users

Based on the given scenario, the most important part of the CIA triad would be availability, which means that the security policy needs to be designed in a balanced way, minimazing the necessary trade off of confidentiality and integrity that comes with prioriterizing availability.

b)

Denial of service attack is aimed specifically at availability of services provided, either disabling them completly or slowing them down to a degree which makes operations unviable.

Power shortage - most business these days rely on information systems to provide their services, which in turn requires electrical power. In the event of a power shortage or complete blackout, continuous delivery of services becomes impossible, thus negatively affecting availability.

Natural disaster - some parts of the world are more likely to suffer such an event than others. Events such as earthquakes or floods, which carry potential of negatively affecting availability by damaging or completly destroying the hardware which allows the company´s information system to operate, are examples of natural disasters.

c) The **Bell-La Padule model** prioriterizes confidentiality over integrity by implementing the ´write up, read down´rule. What that means is that users with a given security level can only create documents with equal or higher security level and can only read documents with equal or lower security level. This preserves confidentiality by not allowing secret information to trickle down to lower security levels. Therefore it does not center integrity.

To preserve integrity, a better choise would be the **Biba model**. The theory behind it is the exact opposite of the Bell-La Padula model and can be expressed by the ´write down, read up´rule. It preserves integrity by ensuring that the users only have access to credible information (created by users with higher security level) and that the integrity is not compromised by information of lower integrity moving up the chain.

Ouriginal: 7%

Comment:

Question **3**

Complete

Mark 3 out of 3

Problem 3

What is multi-factor authentication? Why is it a good idea? Give two examples of two-factor authentication and explain why two-factor authentication is more secure than, for example, a password (one factor).

Multi-factor authentication is a form of authentication which utilizes more than one method, each of a different type (the three types available are something you know, something you are (biometrics), and something you have (tokens))

Using two different (strong!) methods of authentication strenghtens it by providing an extra step - in the event that one of the methods has been compromised (for example, a stolen password), a second one remains. It is significantly harder for a potential attacker to be able to bypass both.

Example 1: ID card and photo on it - smething you have and something you are (the physical card combined with the photo of the rightful holder)

Example 2; bank card and PIN - something you have and something you know (the physical card and the PIN, required when withdrawing cash from an ATM or making a purchase over a certain sum)

Using the same kind of authentication for all the steps does not improve security in a significant manner, which is showcased by security questions used in tandem with passwords. Both are an example of something you know and given the fact that security questions tend to be rather universal (the name of the first pet, mother's maiden name etc.), they tend to be rather easy to bypass, using information that people put on their social media profiles.

Ouriginal: **0%**

Comment:

Question **4**

Complete

Mark 3 out of 3

Problem 4

Below are four pairs of concepts/threats/tools. For each pair, define both terms and explain the relationship between them. Then describe how the two terms can be used together to achieve a common goal, for example, to harm or protect security (one or several security properties) or privacy.

Structure each of your answers with the headings “Definition”, “Relationship”, and “Description”. Your answers to each part should show your deep understanding of the concept. The definition, relationship and description should be described or explained with care; they must not just be copied from the book/documents.

Please note that in general a 50% complete answer will be required to obtain a pass mark for this problem.

- Firewall and DMZ
- Onion routing and anonymization
- TCB (Trusted computing base) and audit
- Trojan horses and worms

1. **Firewall and DMZ**

- **Definition**

A **firewall** is a piece of hardware or software which filters internet traffic in accordance with criteria specified by the system administrator. Firewalls are often minimalist in their design to minimize attack surface. A firewall should filter both in- and outgoing traffic.

DMZ stands for demilitarized zone, it is also a type of firewall, where part of the organization's web servers are isolated from the main internal network in a sort of buffer space.

- **Relationship**

Both are ways of protecting an internal network against potential attackers.

- **Description**

Firewall and **DMZ** combined can greatly enhance the security of an organization's internal network. It must be noted, however, that they do not protect against intenral threats.

2. Onion routing and anonymization

- **Definition**

Onion routing is a form of anonymous browsing where data is passed through at least three, randomly chosen relays located all over the world and run by volunteers. Each relay knows the previous and the next relay, but does not know the original sender and the ultimate recipent, thus guaranteeing effective anonymous browsing. The principle is similar to peeling the layers of an onion, hence the name.

Anonymization is a more general term to denote the act of obscuring data so it cannot be linked to a specific individual. It can refer both to web anonymization in the context of browsing and data.

- **Relationship**

Onion routing is a form of web **anonymization**, allowing users to browse the internet without revealing their IP address, thus enhancing their privacy and potentially allowing them to bypass censorship or other restrictions imposed by governemnts or other agents.

- **Description**

Onion routing may be combined with other **anonymization** tools, such as a VPN, to enhance the user's privacy and, in some contexts, security when browsing the web.

3. TCB (Trusted computing base) and audit

- **Definition**

TCB is the sum of hardware and software in place to enforce security policy of a given system.

Audit is an action of analyzing an event after it has occured through the use of, for example, audit logs.

- **Relationship**

Both are related to enforcing the security policy, but **TCB** is more general and largely aimed at preventing adverse security events, while the primary aim of an **audit** is to analyze the course of events post factum.

- **Description**

Both are effective tools in enforcing a security policy. Even if the preventative measures fail, audit allows the system administartors to analyze the events and determine what went wrong and how to improve the security to prevent such an occurance from happening again.

4. Trojan horses and worms

- **Definition**

Trojan horse is a type of malware which, on top of its apparent purpose has a second, hidden one, often of malicious nature. The name is derived from the story of the siege of Troy, where the Greeks tricked the city's defenders by giving them a giant wooden horse as a gift, which was promptly brought into the city, with hidden Greek soldiers inside of it. As soon as night fell, the soldiers came out, opened the gates and sealed the fate of Troy. Trojan horse the virus can be used for a wide variety of malicious purposes, including acting as spyware and sending sensitive data to an attacker without the knowledge of the user who's computer got infected. An example of a Trojan horse malware is Silent Banker, stealing sensitive banking information.

Worms are a type of malware which spread themselves over a network, often as stand alone programs.

- **Relationship**

Both are type of malicious software. They key difference between tem is that a **Trojan horse** is a computer virus, which can spread itself through a number of ways, including infected programs, USB sticks, emails etc., but a **worm** requires a network to spread and, as opposed to a virus, it does not embed itself to another program. Interestingly enough, sometimes malware can be both - an example of that would be Stuxnet, a Trojan/worm hybrid malware which infected SCADA systems of the Iranian nuclear system.

- **Description**

Both are types of malware which can be used by an attacker to compromise the confidentiality, inegrity and availability of computer systems.

Ouriginal: **3%**

Comment:

Question **5**

Complete

Mark 2 out of 3

Problem 5

How and why can a cross-site scripting attack happen? What protection is available against cross-site scripting attacks?

A **cross site scripting attack** may occur when executable code is added to ordinary-seeming data in order for the attacker to gain access or information. The script gets passed as input to the web server, which unknowingly executes it. If there have been no countermeasures implemented, this simple technique can be utilized to gain unauthorized access to data contained within a web server, which in turn can be a jumping off point to further escalate the attack.

Luckily, there are several countermeasures which can be utilized to prevent such an attack. These include;

- implementing security measures in the development stage (in this case, complete mediation appears to be the most relevant)
- the user should disable JavaScript when browsing the web
- ssanitazing input so the web server does not read it as executable

Ouriginal: 0%

Comment:
P+