International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 07 | July - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Study on Security Breaches and Counter Measures

Nayan Singh , Suraj Lingwal

1.Introduction

A security breach is any incident that results in unauthorized access to computer data, applications, networks or devices. It results in information being accessed without authorization. Typically, it occurs when an intruder is able to bypass security mechanisms.

Technically, there's a distinction between a security breach and a data breach. A security breach is effectively a break-in, whereas a data breach is defined as the cybercriminal getting away with information. Imagine a burglar; the security breach is when he climbs through the window, and the data breach is when he grabs your pocketbook or laptop and takes it away.

2. Defining Security Breaches and CounterMeasures

Confidential information has immense value under Security Breaches. It's often sold on the dark web; for example, names and credit card numbers can be bought, and then used for the purposes of identity theft or fraud. It's not surprising that security breaches can cost companies huge amounts of money. On average, the bill is nearly $4m for major corporations.

It's also important to distinguish the security breach definition from the definition of a security incident. An incident might involve a malware infection, DDOS attack or an employee leaving a laptop in a taxi, but if they don't result in access to the network or loss of data, they would not count as a security breach.

Examples of a security breach

When a major organization has a security breach, it always hits the headlines. Security breach examples include the following:

Equifax - in 2017, a website application vulnerability caused the company to lose the personal details of 145 million Americans. This included their names, SSNs, and drivers' license numbers. The attacks were made over a three-month period from May to July, but the security breach wasn't announced until September.

Yahoo - 3 billion user accounts were compromised in 2013 after a phishing attempt gave hackers access to the network.

eBay saw a major breach in 2014. Though PayPal users' credit card information was not at risk, many customers' passwords were compromised. The company acted quickly to email its users and ask them to change their passwords in order to remain secure.

Dating site Ashley Madison, which marketed itself to married people wishing to have affairs, was hacked in 2015. The hackers went on to leak a huge number of customer details via the internet. Extortionists began to target customers whose names were leaked; unconfirmed reports have linked a number of suicides to exposure by the data breach.

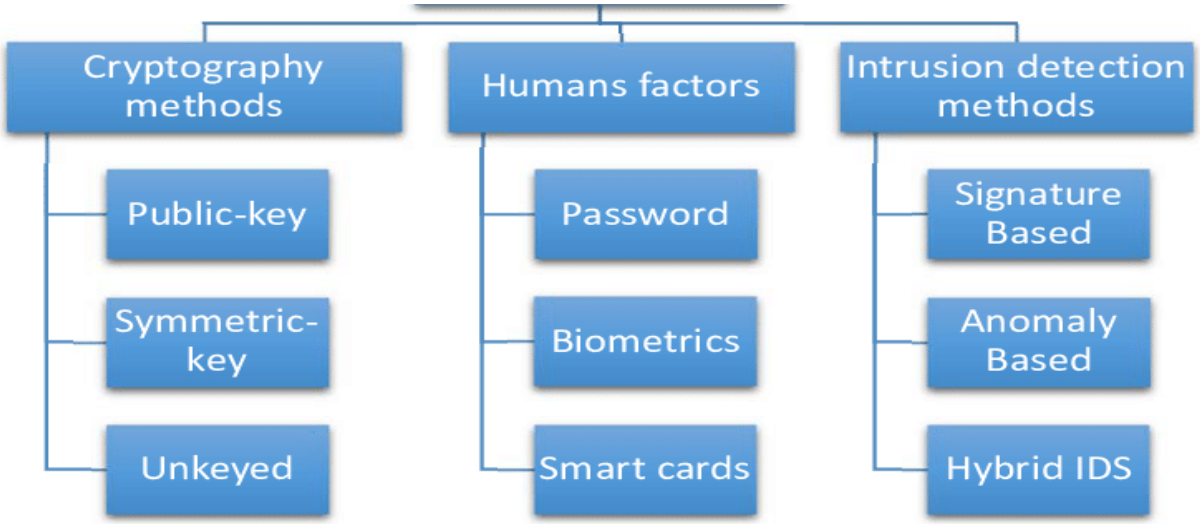
Facebook saw internal software flaws lead to the loss of 29 million users' personal data in 2018. This was a particularly embarrassing security breach since the compromised accounts included that of company CEO Mark Zuckerberg.

Marriott Hotels announced a security and data breach affecting up to 500 million customers' records in 2018. However, its guest reservations system had been hacked in 2016 - the breach wasn't discovered until two years later.

Perhaps most embarrassing of all, being a cybersecurity firm doesn't make you immune - Czech company Avast disclosed a security breach in 2019 when a hacker managed to compromise an employee's VPN credentials. This breach didn't threaten customer details but was instead aimed at inserting malware into Avast's products.

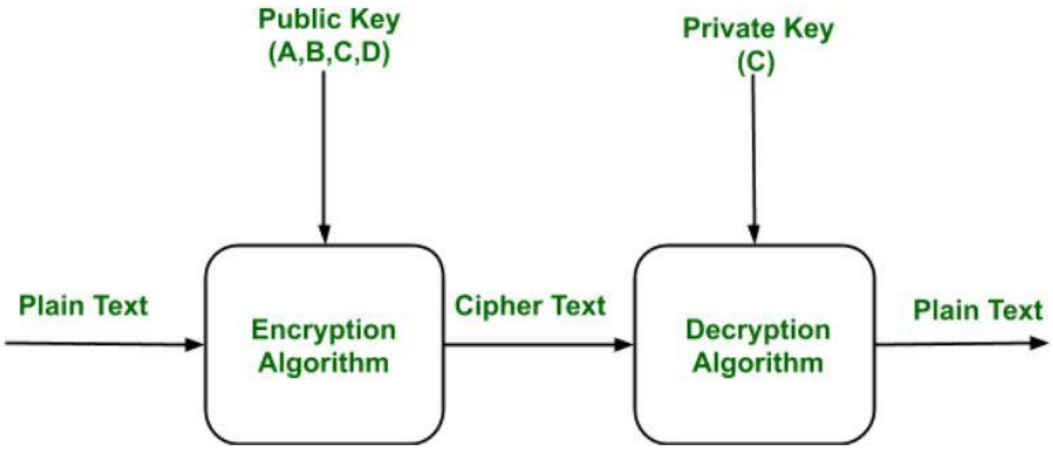
2.1 Security Breaches and CounterMeasures and its Model

These countermeasures can be classified into three types of categories, including, cryptography methods, humans factors, and intrusion detection methods,

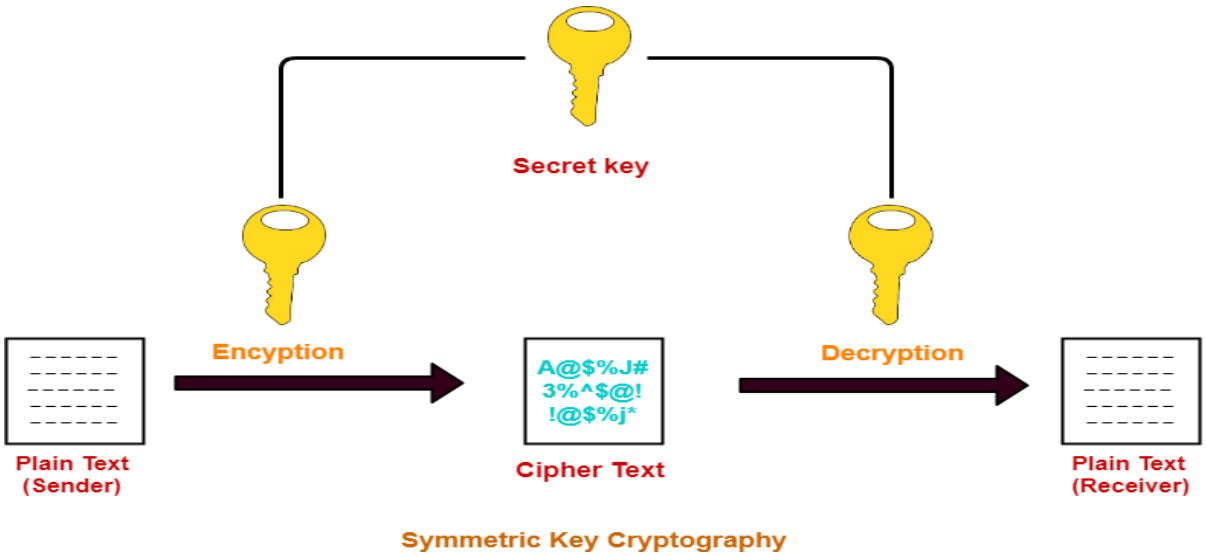


1. Cryptography Methods- Cryptography is **technique of securing information and communications through use of codes so that** only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix graphy means "writing".

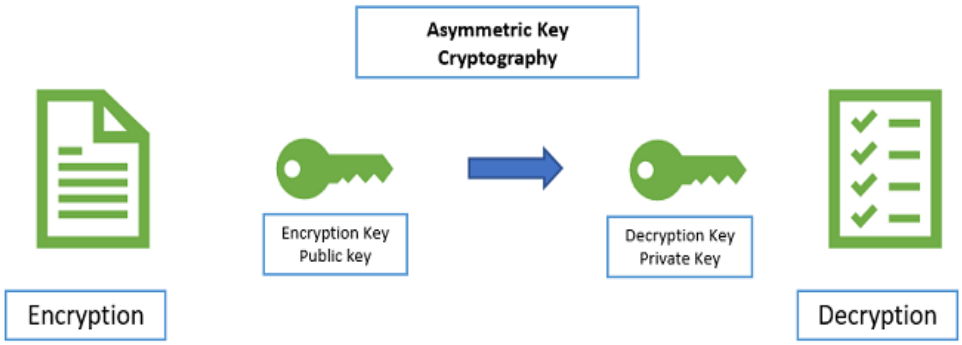
   A) Public-key- This method of cryptography requires two separate keys, one that is private or secret, and one that is public. Public key cryptography uses **a pair of keys to encrypt and decrypt data** to protect it against unauthorized access or use. Network users receive a public and private key pair from certification authorities.



   B) Symmetric-key - In this technique, **Both sender and receiver uses a common key to encrypt and decrypt the message**. This secret key is known only to the sender and to the receiver

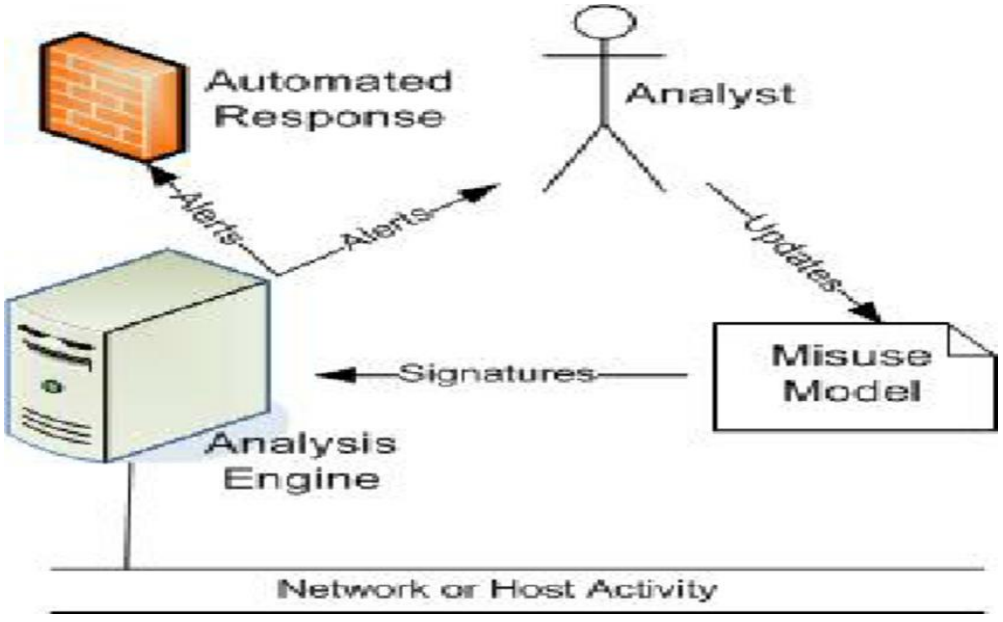


B) Unkeyed (Asymmetric key) - Asymmetric-key algorithms work in a similar manner to symmetric-key algorithms, where plaintext is combined with a key, input to an algorithm, and outputs ciphertext. The major difference is the keys used for the encryption and decryption portions are different, thus the asymmetry of the algorithm.

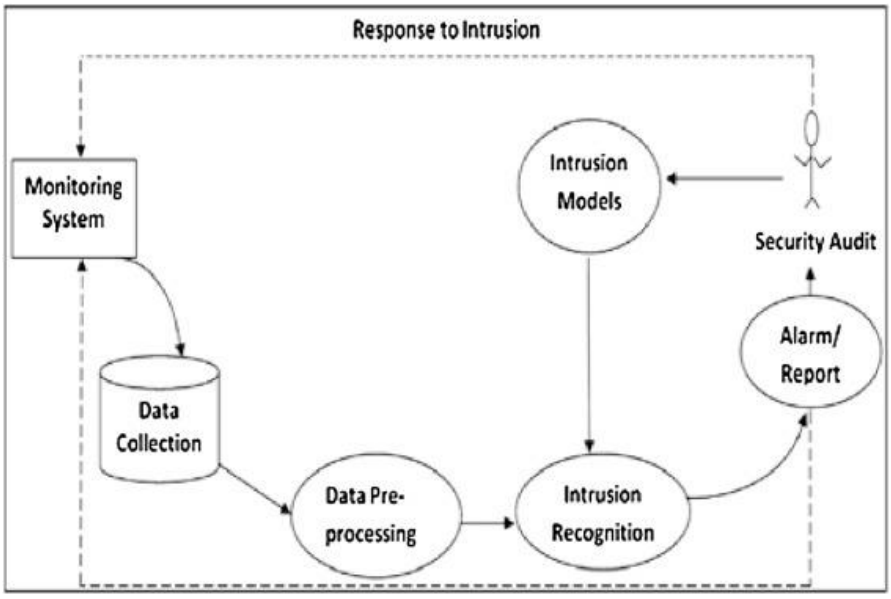


2.Intrusion Detection and its Methods- An intrusion detection system (IDS) is **a device or software application that monitors a network for malicious activity or policy violations**. Any malicious activity or violation is typically reported or collected centrally using a security information and event management system.

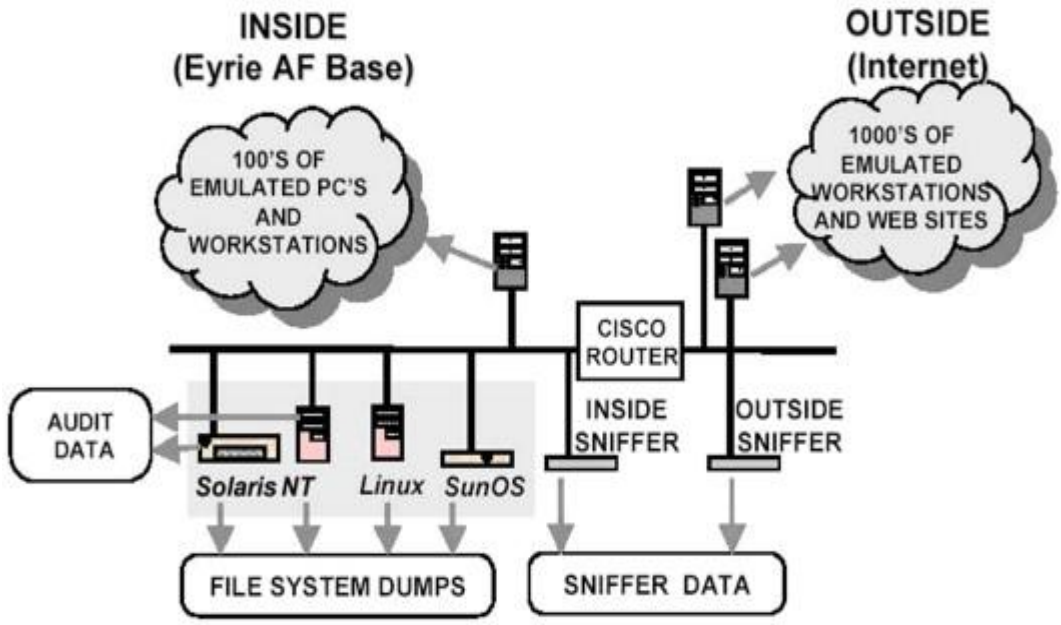
A) Signature based IDS- Signature-based IDS is **the detection of attacks by looking for specific patterns**, such as byte sequences in network traffic, or known malicious instruction sequences used by malware. This terminology originates from anti-virus software, which refers to these detected patterns as signatures.



B.Anomaly based IDS- An anomaly-based intrusion detection system, is an **intrusion detection system for detecting both network and computer intrusions and misuse by monitoring system activity and classifying it** as either normal or anomalous. ... Systems using artificial neural networks have been used to great effect.



C) Hybrid IDS- Intrusion detection systems can be misuse-detection or anomaly detection based. ... The hybrid IDS is **obtained by combining packet header anomaly detection (PHAD) and network** traffic anomaly detection (NETAD) which are anomaly-based IDSs with the misuse-based IDS Snort which is an open-source project.



Conclusion

Security countermeasures are **the controls used to protect the confidentiality, integrity, and availability of data and information systems**. ... These programs use a variety of techniques to scan and detect viruses, including signature scanning, heuristic scanning, integrity checks, and activity blocking.

Security countermeasures is one of the most important aspects of the fast-paced growing digital world. The threats of it are hard to deny, so **it is crucial to learn how to defend from them and teach others how to do it too**.

References

- Kaspersky (2011) Kaspersky Security Bulletin 2011, description available at: http://securelist.com (website visited on January 04, 2015)
- McAfee Labs (2014) Threats Predictions 2015, description available at: http://mcaffee.com (website visited on January 04, 2015)