Paper ID: IOTTSF18

INTERNET AS A APPLICATION FOR SECURED DATA TRANSMISSION IN DIGITAL WORLD

Sanjali S. Doshi
MIT Polytecnic College of
Engineering, Pune
India
Sanjalidoshi97@gmail.com

Abstract:

Computer security deals with the managerial procedures and technological safeguards applied to computer hardware, software, and data to ensure against accidental or deliberate unauthorized access to computer system data. computer privacy is concerned with the moral and legal requirements to protect data from unauthorized access and dissemination. the issues involved in computer privacy are therefore political decisions regarding access to information, whereas issues of security involve the procedures and safeguards for enforcing the privacy decisions. the motivations for security and privacy are found in the desire for military secrecy, industrial security, and information sharing. based on national and state laws, it is possible to establish some form of operational security, which allows the management of a computer installation to exercise control and be accountable for the installation. guidelines and procedures may be established for accountability, for levels of control, and for system configuration. preventive measures against internal and external threats can be developed through risk analysis, assessment, and insurance investigation. the psychological security of the operational staff is necessary for successful operational security. it is recommended that ongoing risk management teams be formed that would include operations managers, programmers, internal auditors, and physical security personnel. physical security must prevent loss due to natural disasters, tampering, and malicious entry and destruction. user identification and authentication must protect both hardware and software. references, illustrations, and author and subject indexes are provided.

I. INTRODUCTION

Computer security, also known as cyber-security or IT security, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide. It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures. The field is of growing importance due to the increasing reliance of computer systems in most societies. Computer systems now include a very wide variety of "smart" devices, including smartphone, televisions and tiny devices as part of the Internet of Things – and networks include not only the Internet and private data networks, but also Bluetooth, Wi-Fi and other wireless networks.

II. TYPES OF COMPUTER SECURITY

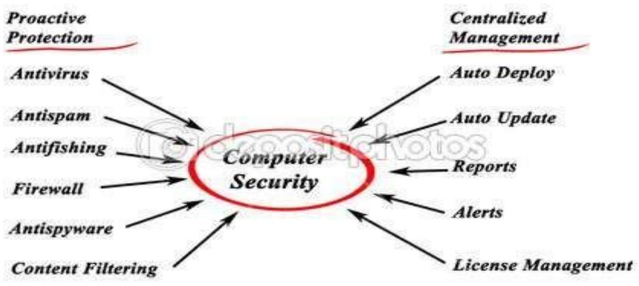


Fig 1. Types of computer security

A. Identity management:

Every enterprise will have its own identity management system to control access to information and computing resources. Cloud providers either integrate the customer’s identity management system into their own infrastructure, using federation or SSO technology, or a biometric-based identification system,[1]or provide an identity management solution of their own. Cloud ID for instance, provides privacy-preserving cloud-based and cross-enterprise biometric identification solutions for this problem. It links the confidential information of the users to their biometrics and stores it in an encrypted fashion. Making use of a searchable encryption technique, biometric identification is performed in encrypted domain to make sure that the cloud provider or potential attackers do not gain access to any sensitive data or even the contents of the individual queries [4].

B. Physical security:

The cloud service providers physically secure the IT hardware (servers, routers, cables etc.) against, unauthorized access, interference, theft ,fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption. This is normally achieved by serving cloud applications from 'word –class' (i.e professionally specified, designed, constructed, managed, monitored and maintained) data centers.

C. Personal security:

Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre-, Para- and post-employment activities such as security screening potential recruits, security awareness and training programs, proactive security monitoring and supervision, disciplinary procedures and contractual obligations embedded in employment contracts, service level agreements, codes of conduct, policies etc [1].

D. Identity management:

Cloud provides help ensure that customers can rely on access to their data and applications ; at least in part (failures at any point- not just within the cloud service providers domains- may disrupt the communication chains between users and applications).

E. Application security:

Cloud provides ensure that applications available as a service via the cloud are secure by specifying, designing, implementation ,testing and maintaining appropriate application security measures in the production environment. Note that –as with any commercial software the controls they implementation may not necessarily fully mitigate all the risks they have identified, and that they may not necessarily have identified all the risks that are of concern to customers. Consequently, customers may also need to assure themselves that cloud application are adequately secured for their specific purpose, including their compliance obligations [2].

.

F. Browser security:

Browser security is the application of internet security to web browsers in order to protect networked data and computer system from breaches of privacy or malware. Security explore of browsers often use JavaScript- sometimes with cross-site scripting (XSS)-

G. Network Security:

Network security consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

III. Privacy

Providers ensure that all critical data (credit card numbers, for example) are masked or encrypted and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

A. Internet privacy:

Internet privacy involves the right or mandate of personal privacy concerning the storing, repurposing, provision to third parties, and displaying of information pertaining to oneself via the Internet. Internet privacy is a subset of data privacy. Privacy concerns have been articulated from the beginnings of large scale computer sharing privacy can entail either Personally Identifying Information (PII) or non-PII information such as a site visitor's behavior on a website. PII refers to any information that can be used to identify an individual. For example, age and physical address alone could identify who an individual is without explicitly disclosing their name, as these two factors are unique enough to typically identify a specific person.

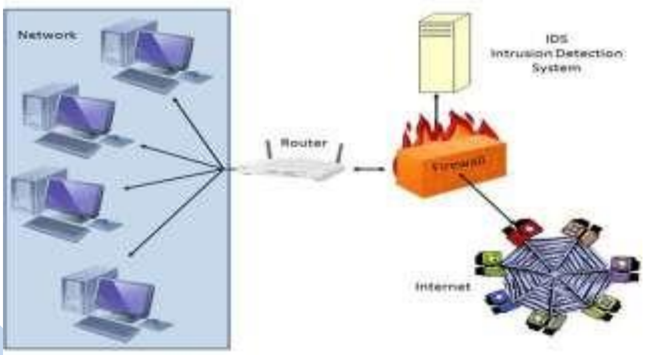


Fig 2. Internet Security

B. Levels Of Privacy:

- People with only a casual concern for Internet privacy need not achieve total anonymity. Internet users may protect their privacy through controlled disclosure of personal information.
- some people desire much stronger privacy. In that case, they may try to achieve *Internet anonymity* to ensure privacy — use of the Internet without giving any third parties the ability to link the Internet activities to personally-identifiable information of the Internet user.
- There are also several governmental organizations that protect individual's privacy and anonymity on the Internet, to a point.
- Posting things on the Internet can be harmful or in danger of malicious attack.

Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority [3].

The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

C. *Search Engine:*

- Search engines have the ability to track a user's searches. Personal information can be revealed through searches by the user's computer, account, or IP address being linked to the search terms used.
- Search engines have claimed a necessity to retain such information in order to provide better services, protect against security pressure, and protect against fraud.
- A search engine takes all of its users and assigns each one a specific ID number. Those in control of the database often keep records of where on the Internet each member has traveled to AOL's system
- AOL has a database 21 million members deep, each with their own specific ID number.
- Search engines also are able to retain user information, such as location and time spent using the search engine, for up to ninety days [4].
- Most search engine operators use the data to get a sense of which needs must be met in certain areas of their field. People working in the legal field are also allowed to use information collected from these search engine websites.

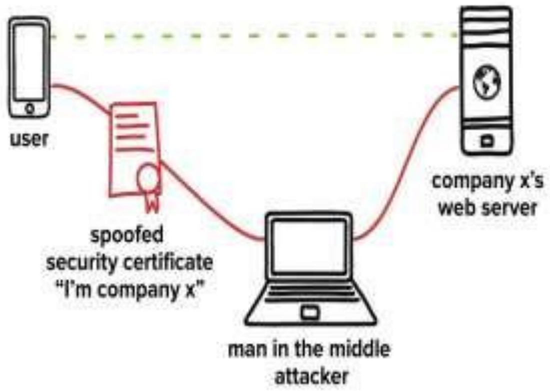


Fig 3. Computer privacy and servers

IV. E-COMMERCE

Electric Commerce commonly written as e-commerce is the trading or facilitation of trading in products or service using computer network, such as the internet electronic commerce draws on technologies such as mobile commerce, electronic funds transfers, supply chain management, internet marketing, online transaction, electronic data interchange(EDI), inventory management systems. Modern electronic commerce typically uses the World Wide Web for at least one part of the transaction life cycle, although it may also use other technologies such as E-mail.

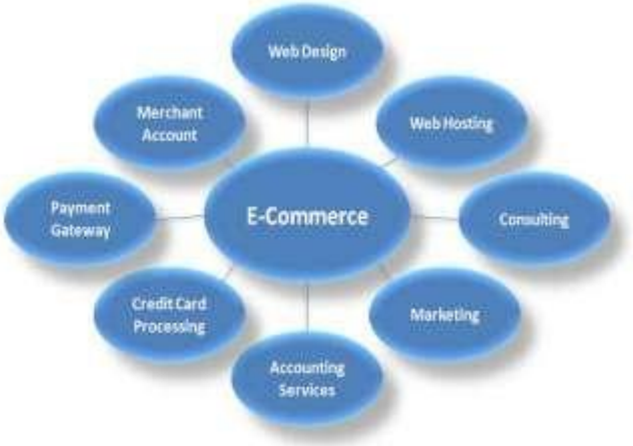


Fig 4. E-commerce radial diagram

A. *E-commerce businesses may employ some or all of the following:*

- Online shopping web sites for retail sales direct to consumers
- Providing or participating in online marketplaces, which process third-party business-to-consumer or consumer-to-consumer sales
- Business-to-business buying and selling
- Gathering and using demographic data through web contacts and social media
- Business-to-business electronic data interchange
- Marketing to prospective and established customers by e-mail or fax (for example, with newsletters)

V. DISASTER RECOVERY

Disaster recovery (DR) involves a set of policies and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. Disaster recovery focuses on the IT or technology systems supporting critical business functions, as opposed to business continuity, which involves keeping all essential aspects of a business functioning despite significant disruptive events. Disaster recovery is therefore a subset of business continuity[2].

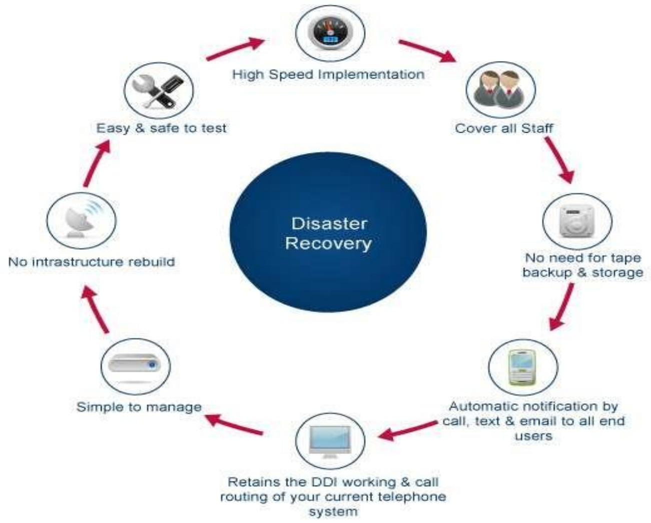

High Speed Implementation
Cover all Staff
No need for tape backup & storage
Automatic notification by call, text & email to all end users
Retains the DDI working & call routing of your current telephone system
Simple to manage
No infrastructure rebuild
Easy & safe to test
Disaster Recovery

Fig 5.Disaster recovery cycle diagram

A. *Classification:-*

- **Importance of disaster recovery planning:**

Recent research supports the idea that implementing a more holistic pre-disaster planning approach is more cost-effective in the long run. Every $1 spent on hazard mitigation(such as a disaster recovery plan) saves society $4 in response and recovery costs. As IT systems have become increasingly critical to the smooth operation of a company, and arguably the economy as a whole, the importance of ensuring the continued operation of those systems, and their rapid recovery, has increased.

- **Control Measures**:

Control measures are steps or mechanisms that can reduce or eliminate various threats for organizations. Different types of measures can be included in disaster recovery plan (DRP). Disaster recovery planning is a subset of a larger process known as business continuity planning and includes planning for resumption of applications, data, hardware, electronic communications (such as networking) and other IT infrastructure.

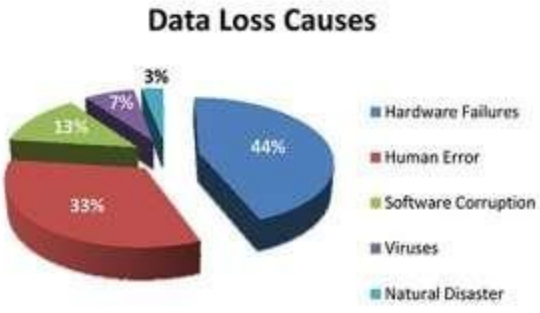


Fig 6.Pie diagram data loss

IT disaster recovery control measures can be classified into the following three types:

1. Preventive measures - Controls aimed at preventing an event from occurring.
2. Detective measures - Controls aimed at detecting or discovering unwanted events.
3. Corrective measures - Controls aimed at correcting or restoring the system after a disaster or an event.

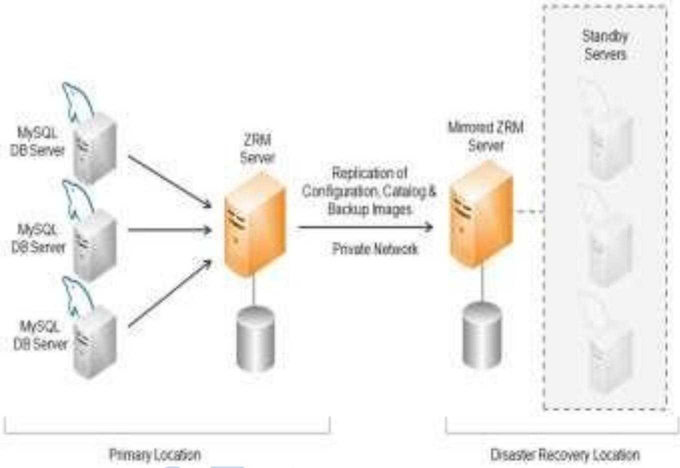
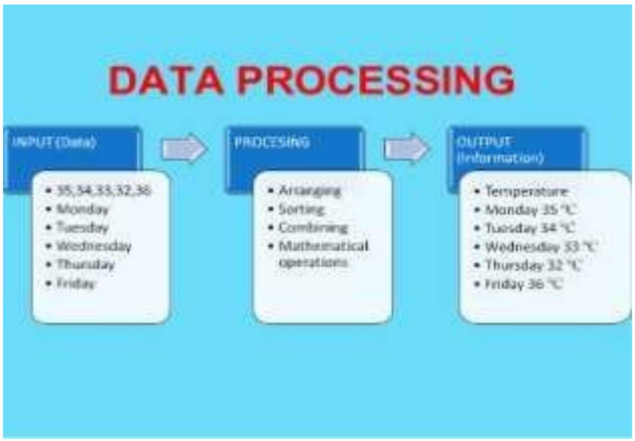


Fig 7.Diagram for data recovery plans

- **Strategies:**

- Backups made to tape and sent off-site at regular intervals
- Backups made to disk on-site and automatically copied to off-site disk, or made directly to off-site disk
- Replication of data to an off-site location, which overcomes the need to restore the data (only the systems then need to be restored or synchronized), often making use of storage area network (SAN) technology
- Private Cloud solutions which replicate the management data (VMs, Templates and disks) into the storage domains which are part of the private cloud setup. These management data are configured as an xml representation called OVF (Open Virtualization Format), and can be restored from the Data Base once a disaster occurs. For example, Disaster Recovery with OVir.
- Hybrid Cloud solutions that replicate both on-site and to off-site data centers. These solutions provide the ability to instantly fail-over to local on-site hardware, but in the event of a physical disaster, servers can be brought up in the cloud data centers as well. Examples include Quorom, Cloud from Persistent Systems or Ever Safe.
- the use of high availability systems which keep both the data and system replicated off-site, enabling continuous access to systems and data, even after a disaster (often associated with cloud storage)

VI. Data Processsing


DATA PROCESSING

INPUT (Data)
- 35,34,33,32,36
- Monday
- Tuesday
- Wednesday
- Thursday
- Friday

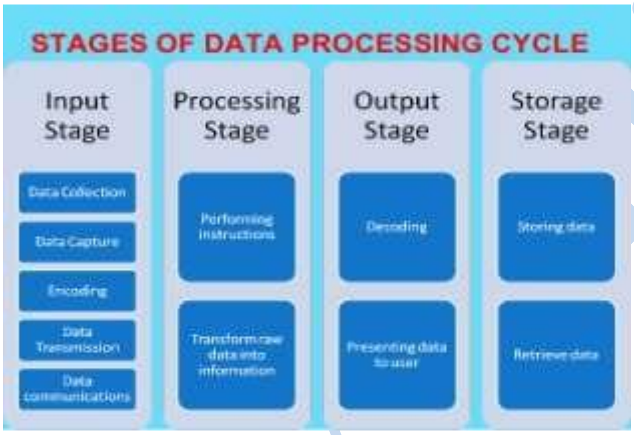
PROCESING
- Arranging
- Sorting
- Combining
- Mathematical operations

OUTPUT (Information)
- Temperature
- Monday 35 °C
- Tuesday 34 °C
- Wednesday 33 °C
- Thursday 32 °C
- Friday 36 °C

Fig 8Block diagram of data processing

Data processing is, "the collection and manipulation of items of data to produce meaningful information."] In this sense it can be considered a subset of information processing, "the change (processing) of information in any manner detectable by an observer."

The term is often used more specifically in the context of a business or other organization to refer to the class of commercial data processing applications.


STAGES OF DATA PROCESSING CYCLE

Input Stage
- Data Collection
- Data Capture
- Encoding
- Data Transmission
- Data communications

Processing Stage
- Performing instructions
- Transform raw data into information

Output Stage
- Decoding
- Presenting data to user

Storage Stage
- Storing data
- Retrieve data

Fig 9. Stages of data processing cycle

A. *Processes:*

- Validation – Ensuring that supplied data is "clean, correct and useful"
- Sorting – "arranging items in some sequence and/or in different sets."
- Summarization – reducing detail data to its main points.
- Aggregation – combining multiple pieces of data.
- Analysis – the "collection, organization, analysis, interpretation and presentation of data.".
- Reporting – list detail or summary data or computed information.
- Classification – separates data into various categories.

B. *Applications:*

1) *Commercial data processing*

Commercial data processing involves a large volume of input data, relatively few computational operations, and a large volume of output. For example, an insurance company needs to keep records on tens or hundreds of thousands of policies, print and mail bills, and receive and post payments.

2) *Data analysis*

In a science or engineering field, the terms data processing and information systems are considered too broad, and the more specialized term data analysis is typically used. Data analysis makes use of specialized and highly accurate algorithms and statistical calculations that are less often observed in the typical general business environment.

VII. Cryptography

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit.

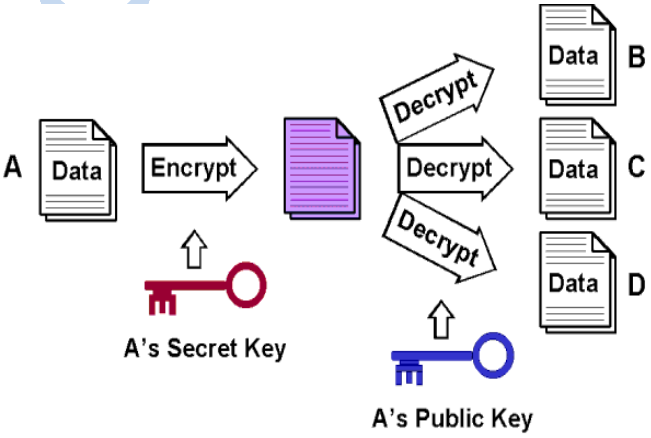


Fig 10. Diagram for cryptography concept

A. *Cryptosystem:*

1) Confidentiality (the information cannot be understood by anyone for whom it was unintended)

2) Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)

3) Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)

4) Authentication (the sender and receiver can confirm each others identity and the origin/destination of the information)

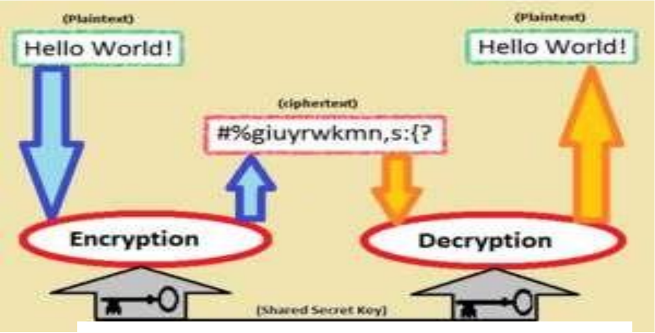


Fig 11.Working process of cryptography

B. *Type*

1) ***Symmetric-key cryptography****:*

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way)

2) ***Public-key Cryptography:***

In public-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. In a public-key encryption system, the public key is used for encryption, while the private or secret key is used for decryption.

VIII. Wireless Network Security

Wireless security is the prevention of unauthorized access or damage to computers using wireless network [6].

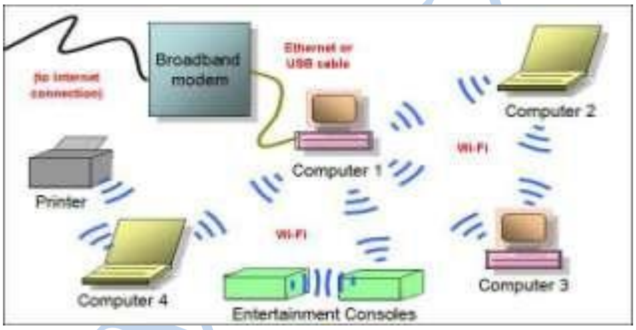


Fig 12. Wireless network

The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard wireless networking is prone to some security issues. Hackers have found wireless networks relatively easy to break into, and even use wireless technology to hack into wired networks. As a result, it is very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources. Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.

A. *The Threat Situation*

Wireless security is just an aspect of computer security; however, organizations may be particularly vulnerable to security breaches caused by rogue access points. If an employee (trusted entity) brings in a wireless router and plugs it into an unsecured switch port, the entire network can be exposed to anyone within range of the signals. Similarly, if an employee adds a wireless interface to a networked computer using an open USB port, they may create a breach in network security that would allow access to confidential materials.

B. *The air interface and link corruption risk*

There were relatively few dangers when wireless technology was first introduced, as the effort to maintain the communication was high and the effort to intrude is always higher. The variety of risks to users of wireless technology have increased as the service has become more popular and the technology more commonly available. Today there are a great number of security risks associated with the current wireless protocols and encryption methods, as carelessness and ignorance exists at the user and corporate IT level, Hacking methods have become much more sophisticated and innovative with wireless.

C. *Wireless network prevention concept:*

- For closed networks (like home users and organizations) the most common way is to configure access restrictions in the access points. Those restrictions may include encryption and checks on MAC address. Wireless Intrusion Prevention Systems can be used to provide wireless LAN security in this network model.
- For commercial providers, hotspots, and large organizations, the preferred solution is often to have an open and unencrypted, but completely isolated wireless network. The users will at first have no access to the Internet nor to any local network resources. Commercial providers usually forward all web traffic to a captive portal which provides for payment and/or authorization. Another solution is to require the users to connect securely to a privileged network using VPN.
- Wireless networks are less secure than wired ones; in many offices intruders can easily visit and hook up their own computer to the wired network without problems, gaining access to the network, and it is also often possible for remote intruders to gain access to the network through backdoors like Back Orifice. One general solution may be end-to-end encryption, with independent authentication on all resources that shouldn't be available to the public.

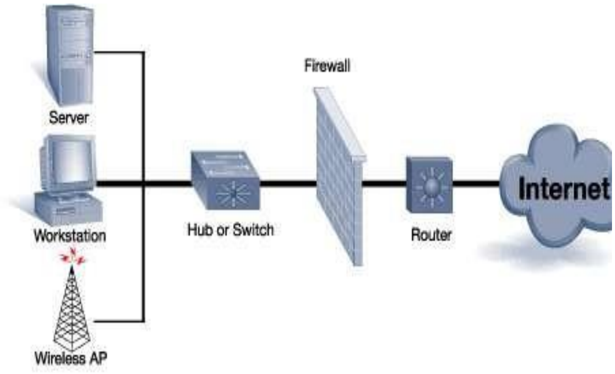


Fig 13.Wireless network 2

D. Security Measures:

- ***SSIDhiding:***

A simple but ineffective method to attempt to secure a wireless network is to hide the SSID (Service Set Identifier). This provides very little protection against anything but the most casual intrusion efforts[6].

- ***MAC ID filtering:***

One of the simplest techniques is to only allow access from known, pre-approved MAC addresses. Most wireless access points contain some type of MAC ID filtering. However, an attacker can simply sniff the MAC address of an authorized client and spoof this address.

- ***Static IP Addressing:***

Typical wireless access points provide IP addresses to clients via DHCP. Requiring clients to set their own addresses makes it more difficult for a casual or unsophisticated intruder to log onto the network, but provides little protection against a sophisticated attacker [7].

E. Mobile Devices:

With increasing number of mobile devices with 802.1x interfaces, security of such mobile devices becomes a concern. While open standards such as Kismet are targeted towards securing laptops, access points solutions should extend towards covering mobile devices also. Host based solutions for mobile handsets and PDA's with 802.1x interface.
Security within mobile devices fall under three categories:

1. Protecting against ad hoc networks
2. Connecting to rogue access points
3. Mutual authentication schemes such as WPA2 as described above

Wireless IPS solutions now offer wireless security for mobile devices.

Mobile patient monitoring devices are becoming an integral part of healthcare industry and these devices will eventually become the method of choice for accessing and implementing health checks for patients located in remote areas. For these types of patient monitoring systems, security and reliability are critical, because they can influence the condition of patients, and could leave medical professionals in the dark about the condition of the patient if compromised.

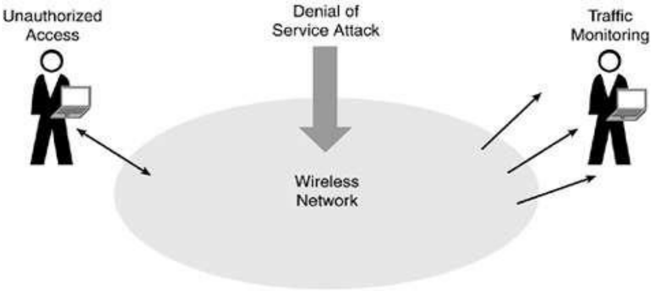


Fig 14. Wireless network access, attack and monitoring diagram

Conclusion

We come to know that, in today's life computer and internet security is must. There are too many attackers out there try to get victims personal data. As a network user we should assure how to prevent or protect yourself getting hacked or from getting data loss problem. By using proper net-protections and antivirus software we can protect us from attackers and viruses. Computer security and privacy is one of the biggest issue now days.

References

[1] Atul Kahate Tata McGraw-Hill Education, 2003
Computer networks, introduction computer security.
[2] Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar by Lillian Ablon, Martin C. Libicki, Andrea A. Golay - RAND Corporation , 2014, computer privacy.
[3] Computer networks (4th edition), Andrews Tabebaum, Data management, Search engine.
[4] E-tutorials.org, computer privacy and security.
[5] Wikipedia.org, E-commerce, Cryptography and Wireless network security.
[6] www.ipc.on.ca, Computer security and privacy diagrams.
[7]www.istockphoto.com