Gupta Bhaskar Sheshnarayan Arati
Infrastructure Security
Seat No :- 12273147

Bhaskar
11/01/2021

Q.2.

Ans :- Ethics refers to a system of moral principles that relates to the benefits and harms of particular actions, and to the rightness and wrongness of motives and ends of those actions. Hence, Ethics is an objectively defined standard of 'right' or 'wrong'.

The ethical issues related to Security management are :- The foundation of all security system is formed by moral principles and practices of those people involved and the standard of the profession. It is easy to educate people about security problems that are in information system security. There are ethical issues related to personnel, technology intrusion, social and legal responsibilities and ownership. Some of the issues are :-

Area	Ethical Issues
i) Technology Intrusion	• Privacy internal to firm and • Privacy external to firm • Computer surveillance • Hacking • Employee monitoring
ii) Personnel Issues	• Employee interruption • Ergonomics and human factors

Gupta Bhaskar Sheshnarayan Amrati
Infrastructure Security
Seat No.:- 12273147

Bhaskar
11/01/2021

iii) Legal and Social Responsibilities
- Misuse, fraud and abuse
- Monopoly of data
- Accuracy and timeliness of data

~~Q.2. Ans a)~~

Q.2.

Ans C. A consequences of international roaming is the exchange of information between providers in different countries. All countries have strict regulations against the export of encryption algorithms and thus in GSM works around it. When a user tries to use his/her phone in another country, the local network requests the ~~HLR~~ HLR of the subscriber's home network of the RAND. SRES and KC which is sufficient for authentication and encrypting data.

The various security algorithms are as:-

i) Authentication Algorithm A3:- It is operator-dependent and is an operation option. It is a one-way function. That means it is easy to compute the output

Gupta Bhaskar Sheshnarayan Amit
Infrastructure Security
Seat No:- 1227147

Bhaskar
11/01/2021

Parameter SRES by using the A3 algorithm. but very complex to retrieve the input parameters from the output parameter. While it may sound odd that each operator may choose to use A3 independently.

ii) Ciphering Algorithm A5:- Currently, there exist several implementations of this algorithms though the most commonly used ones are A5/0, A5/1 and A5/2. The reason is due to export restrictions of encryption technologies. A5/1 is the strongest version, while A5/2 is the commonly used in A5/A countries. Under UN Sanctions.

iii) Ciphering Key Generating Algorithm A8:- It is operator-dependent in most ~~prov~~ providers the A3 and A8 Algorithms are combined into a single hash functions known as COMP128.

Gupta Bhaskar Sheshnarayan Asati
Infrastructure Security
Seat No:- 1227314

Bhaskar
11/01/2021

Q.2.

Ans d. Even though there are many benefits of cloud, before one can move data or business to the cloud, it is essential to see the risks. Moving any data to cloud can be challenging and expensive.
The following are the risk associated :-

i) Data breaches :- It involves the unauthorized or illegal viewing, access or retrieval of data by an individual, application or service. It is the most crucial threat as it affects as sensitive content and also it can cause major downfalls as well as the whole industry.

ii) Contractual Breaches with Customers or Business Partners :-
The two entities have agreed to work together and decided how they can use sensitive data along the authorization of users to access the same data.

iii) Data loss :- It is one of the most common cloud security risks in the traditional area data. loss is represented as the theft of the important papers or any other confidential data.
But in the computerized era, if your

Gupta Bhaskar Sheshnarayan Arati
Infrastructure Security
Seat No:- 12273147

Bhaskar
11/01/2021

Hard disk is not working properly. or your software is not updated.
It can occur as:-
- Data corruption
- Data stolen over the network.
- Virus infection. deleting one or more files.

Q.2 Ans.

Q. A buffer overflow vulnerability occurs when you give a program too much data. The excess data corrupts nearby space in memory and may alter other data. As a result, the program might report an error or behave differently. These overflow are difficult to find and exploit. They are also not as common as other vulnerabilities.
Buffer overflow can harm the system very consequences. Such attack often let the attacker gain shell access and therefore full control of the operating system. It may stop running programs and as a result, cause a Denial of Service.

There are two primary types of buffer overflow vulnerabilities:-

Page No. 06.

Gupta Bhaskar Sheshnarayan Arati
Infrastructure Security
Seat No:- 12273147
Bhaskar
11/01/2021

i) Stack Overflow! - the issue applies to the stack, which is memory space used by OS, primarily to store local variables and function return addresses.

ii) Heap Overflow! - the issues applies to heap, which is memory space used to store dynamic data. The amount memory space used to store dynamic data.