INSTRUCTIONS :

- **NO plagiarism will be entertained.**
- **Your assignment will contain 3 sections:**
    1. **What research has been done in the past for the given topic (atleast 5 references should be there) (LITERATURE SURVEY)**
    2. **Answer the question by taking some real time example. (CURRENT SCENARIO)**
    3. **What will be the future scope of the given problem statement ? (FUTURE SCOPE)**
- **You are supposed to create document file consisting of minimum 3 pages.**
- **There will be online submission on UMS.**
- **Last date to upload this assignment is 6th June 2020.**

Aman Dubey

“The designers of GSM set out to secure the system against cloning and other attacks: their goal was that GSM should be secure.”

1. What they did, how they succeeded and where they failed ?
2. How GSM network authenticates the identity of the subscriber ?
3. How GSM ensure subscriber identity confidentiality ?
4. Is Mobile Security a Success or a Failure? Explain with help of example supporting your answer.
5. “Mobile phones are very important to the security engineer, both as part of the underlying infrastructure and as a channel for service delivery. They can also teach us a lot about fraud techniques.” Justify this statement with help of example.

Heragolikar Nareshlal

“The most critical task in signals intelligence is identifying and extracting the interesting material from radio signals.”

1. What can be identified and how one can extract the interesting material from radio signals ?
2. How FHSS is different from DSSS with respect to protection of signals ?
3. How burst communication carried out ? Explain with the help of example.
4. Explain briefly low-probability-of-intercept (LPI) and low-probability-of-position-fix (LPPF) by taking suitable example.
5. "Before communications can be attacked, the enemy's network must be mapped." What are different types of Signals Intelligence Techniques that can be used for this purpose ?

Ghantasala Srihari

With respect to Multi Levl Security, explain the following : (Take real time examples in each case)
1. Why Mandatory Access Control (MAC) considered strictest of all levels of control ?
2. What’s the role of Access Control List in DAC (Discretionary Access Control) ?
3. Why military database system make use of Multi Level Security ?
4. Briefly explain information security levels with respect to multi level security.
5. How Role Based Access Control is different from Rule Based Access Control ?

Souvik Ray

With respect to Social Engineering explain the following: (take real time example)

1. "Many system fail because their designers protect the wrong things, or protect the right things but in the wrong way." Justify this statement with respect to security engineering.
2. Social engineering is hacking people rather than computer systems. Comment.
3. How Pretexting is different from Phishing ?
4. Explain precautionary measures to prevent pretexting.
5. How Phishing carried out using Botnets ?

Konda Mrinal

With respect to web security, answer the following (take real time example)

(a) You visited website and you found that URL of the website turn yellow. What does it mean when a website is flagged yellow and "suspicious" ?
(b) What does it mean when a website is blocked and flagged in red as a reported phishing website ?
(c) How Phishing carried out using compromised web servers ?
(d) How Phishing carried out through port redirection ?
(e) Write down the precautionary measures you can adopt so you avoid becoming victim.

Abhinaba Gupta

What Is Mobile Phone Cloning ? Can A Cloned Phone Be Legitimate ? (take real time example)
(a) Challeneges in dealing Phone Cloning.
(b) Algorithms/Techniques in stopping these crimes.
(c) Detection techniques of mobile phone cloning.
(d) Future scope of Mobile Phone Cloning.
(e) What are symptoms of Mobile Phone Cloning.

Saswath Maurya

"Study of psychology is important in security engineering."
1. Explain with help of example why we need to consider psychology in security engineering ?
2. Relationship of Cognitive Psychology with information security.
3. Why has Internet security worsened even as investment has increased ?
4. How can the past history of cyber incidents guide future investments in defense?
5. How much should firms invest to protect their IT systems?

Manohar Kumar

Many applications, websites and services we use online today host data about their users, they're not less than treasure for a cybercriminal.

(a) How To Avoid Identity Theft Online by taking real time example.
(b) What Happens When Your Identity Is Stolen?
(c) How Digital certificates help in securing websites ?
(d) Techniques to check vulnerability of a website.
(e) How website can be protected from SQL Injection ?

Harmandeep

A lot of the threats today you can combat yourself, just armed with a little bit of knowledge.

(a) The Importance of General Software Updates and Patches
(b) What Makes Public Wi-Fi Vulnerable To Attack And How To Stay Safe. Take a real time example.
(c) How encryption at network level can be deployed in Wireless Network ?
(d) How open access points lead to security breach ?
(e) Recent advancement in Wired Equivalent Privacy.

Ganji Vivek Kumar

With the popularity of smartphones and tablets on the rise, they are becoming more of a target to cybercriminals.
(a) Social Media Scams Based on Current Events
(b) How To Protect Yourself From Phishing Scams ? Take a real time example.
(c) How one can recognize phishing scams ?
(d) What to do if you've been scammed ?
(e) What skills are important to execute these kind of scams ?

Ritender Malik

With respect to malwares, answer the following :
(a) How to spot a malware attack ?
(b) What best practices one can adopt to protect oneself from malware attacks ?
(c) Out of known malwares, which is most dangerous ?
(d) What part of system malware usually target ?
(e) Give a real time example of malware attack. Also write how malware attack tackled at that time ?

Himanshu Thakur

Vulnerabilities associated with Internet of Things.
(a) How one can maintain Privacy of Data with lot of vulnerabilities around IOT.
(b) How Logging can help in security ?
(c) How Software Patching helps in security of data ?
(d) What are weak points in terms of security in IOT ?
(e) Future scope of IOT security.

Amit Kumar Mishra

Role of AI and Machine Learning in information security
(a) How Prediction Models helps in securing assets of an organization ?
(b) Challenges associated with AI and Machine Learning with respect to Security.Take real time scenario.
(c) How machine learning can detect malicious URLs ?
(d) Machine learning is already going mainstream on mobile devices. Example Apple's Siri and Amazon's Alexa. What security issue associated with these ?
(e) List the machine learning algorithms which help in securing systems.

Vishnu Bhushan Ojha

Top 3 causes of cyber disruptions as per the report published by NITI Ayog India are Phishing, Malware and Spear Phishing.
(a) How you will tackle these issue being cyber expert ?
(b) What challenges you are expecting in this scenario ?
(c) Why these are so common in India ?
(d) How to identify such disruptions ?
(e) What's the future scope of these cyber disruptions in India ?

MD Viqhar

Top three patterns as per the report published by NITI Ayog India with respect to Financial and Insurance Sector are :
1.Denial of Services, 2.Web Application Attacks and 3.Payment Card skimming
(a) How you will tackle these issue being cyber expert ?
(b) What challenges you are expecting in this scenario ?
(c) Who are target users of these patterns ?
(d) What skillsets required to identify such attacks ?
(e) To what extent these patterns mentioned above can harm anyone ?

Mogalraj Kushal Dath

Privacy concerns with respect to Facial Recognition (Biometrics)
(a) How to ensure data integrity?
(b) What mechanisms need to be deployed for tackling FRR and FAR.
(c) The success of any technology depends on its ease of use. Explain this statement with respect to Biometrics.
(d) Explain the identification techniques used in face recognition.
(e) What's the future scope of such techniques ?

Harsh Srivastava

In year 2017, Hackers steal Zomato data on 17 million users.
(a) What security policies need to be deployed so that such breach cannot occur in future ?
(b) What was the extent of breach and what caused such incident ?
(c) What security measures taken by Zomato after that incident ?
(d) If you were security incharge, what different you could have done at that time as compared to Zomato's action ?
(e) What was the root cause of that incident ?

Siddharth Singh

One of the most significant security concerns surrounding the use of covert channels in computer and information systems involves confidentiality and the ability to leak confidential information from a high level security user to a low level one covertly.

(a) Being security expert, how these channels can be identified and communication can be intercepted ?
(b) Challenges linked with covert channels.
(c) How Timing channels are different from storage channels ?
(d) Give a real world example of covert channel.
(e) How social media can used as covert channel ?

Katta Saicharan

There are lot of concerns as far as biometric technology is concerned.

(a) How to ensure transparent use of biometrics (requiring no actions from the end-user) ?
(b) Algorithms enabling partial identity classifications like gender and age, allowing more anonymous ways of biometric authentication.
(c) How integrity of information can be compromised with respect to biometrics ?
(d) What proactive measures one can take to prevent misuse of biometrics ?

(e) Is always software flaw lead to compromise information or hardware flaw can lead to attack ?

Kannedari Sai Krishna Yadav

Improving robustness in user authentication and identity verification.

(a) How to make authentication robust ? What are different techniques available ?
(b) How to ensure user authentication in distributed sensor systems ?
(c) How authorization is different from authentication ? Give a real time example.
(d) What's the relationship of authentication, authorization and encryption ?
(e) Is Kerberos (software) is best for authentication ?

Vemanamanda Yeshwanth Sai Krishna Varma

There was famous ransomware attack WannaCry in 2017.

(a) What security policies need to be deployed so that such attack cannot occur in future ?
(b) What was the extent of breach and what caused such incident ?
(c) What security measures taken by WannaCry after that incident ?
(d) If you were security incharge, what different you could have done at that time as compared to Wannacry's action ?
(e) What was the root cause of that incident ?

Kaushal Kumar Lohani

There are lot of security risks associated with cloud storage.

(a) How to ensure integrity of data in cloud computing ?
(b) Why Access and Key Management is challenging in cloud storage ?
(c) What are different weak points in cloud which leads to attack ?
(d) What role does encryption plays in cloud security ?
(e) How reliability can be assured in cloud storage ?

Pavan Prithvi Madduri

With respect to encryption in information security, answer the following :
(a) Write down the use case of symmetric and asymmetric cryptography.
(b) How hashing is different from encryption ?
(c) When one can use encryption, and in which case hashing is suitable in providing security ?
(d) How encryption can be compromised ?
(e) Can we say, higher the key size, higher is the degree of security ?

Ankush Kumar

With respect to OWASP Top 10 attacks, answer the following:
(a) To what extent buffer overflow can cause harm to information systems ?
(b) Give a real world example of cross-site scripting attack.
(c) How to protect ourselves from SQL Injection attack ?
(d) How to detect SQL Injection attack ?
(e) How vulnerabilities in authentication mechanism can lead to data breach ?

Prateek Saini

(a) Bell LaPadula Model says "no read up, no write down".
(b) BIBA Model says "no read down, no write up".
Explain both statement with help of real time example. Write down implementation of this model. What challenges one can face in implementing these techniques.
(c) What advantage does the Multi Level Security provides ?
(d) Give a real world example where multi level security has deployed.
(e) What are different security concerns of multi level security ?

Rohit Dhankher

There are lot of Hardware related cyber security concerns.

(a) Just take some real time example which states that hardware failure can lead to security attack.
(b) Being security expert what efforts you can make to avoid these attacks.
(c) Which malware type cause hardware failure ?
(d) How one can prevent hardware failure to occur ?
(e) List different attacks possible due to hardware failure.

Purshotam Singh

Poorly designed APIs could lead to misuse or—even worse—a data breach.

(a) Being security experts what you'll do in that case ?
(b) What will be the different challenges which you will face in correcting these APIs.
(c) To what extent poorly designed APIs can cause harm to information security ?
(d) Give a real world example where data breach occue due to APIs.
(e) How one can avoid such data breaches ?

Gojur Ravikanth

A Denial of Service (*DoS*) *attack* is a malicious attempt to affect the availability of a targeted system, such as a website or application, to legitimate end users.

(a) How you will ensure that such attack don't happen in future ?
(b) What cause the DOS and DDOS attack to occur ? Identify weak points which lead to such attack.
(c) Is DOS attack difficult to detect in distributed environments ?
(d) To what extent DOS attack can harm your system ?
(e) What new techniques used by hackers to carried out DOS attack ?

Shubham Sharma

(a) What threat Poor Digital Certificate Management can pose to your organization ? How to address such issue ?
(b) What threat Inadequate Patch Management can pose to your organization ? What are its consequences ?
(c) What role digital certificate plays in securing a website ?
(d) How digital signature is different from digital certificate with respect to security ?
(e) What are the contents of a digital certificate ?