Lt. Col Basar

CS

Date: 09.07.25

part B

cyber seaurity

*| Fundamentals

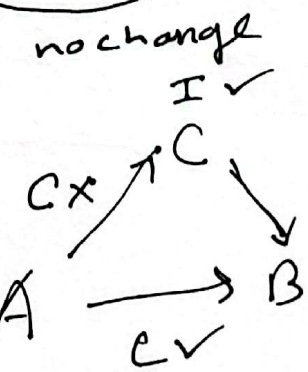
*| Attack

*| Defenece

*| various architechtures, models, theorem etc.

CIA triad

- A to B, not exposed to anyother person
- সব জায়গায় same, A to B
- found when needed



Attack: CI affected

Defence: CI protected.

Cyber space: anything accessed over the network.

Cyber space secuerity — cyber security
কি দিয়ে
kinds of attacks হয়? :

Virus : Vital information & resources under seige

Malware : Malicious software.
different kinds of malware.
→ Virus : prog -এ ঢুকে replicate
→ Spyware : system এর ভিতর ঢুকে info নেয়
→ Ransomware : system attack করে ransom চায়.
→ Adware : ad আসে, মনে হয়
→ Trojan horse : safe but বুঝা যায়না
→ Rootkit : Root -এ থাকে
→ Worms : replicates itself but independent. prog এর দরকার পড়ে না virus এর মত,

Industrial Espionage

phishing :

*| Note down all these
*| Difference, similarities

Samia

Date :

types of attacks :

DoS : ~~একসাথে bot দিয়ে~~ traffic generate bot দিয়ে হতে পারে, single source থেকে attack. intruder
DDoS : multiple এর জন্য
phishing : legitimate এর মত malicious দিয়ে দেয়া.

———— x ————

16.07.25

→ Social Engineering ~~attack~~ : not ~~actually~~ attack, attack launch করার জন্য primarily analysis social account.

→ Flaws & Bugs :
↳ code errors (logical)
→ Software design এর জন্য?
↳ difficult to fix

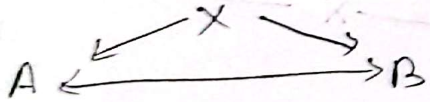
Webgoat : platform, website vulnalitites check

→ Email Spoofing : Sender এর address spoof করে reciever - এর কাছে পাঠায়,

– mobile
– email

→ Man in the middle attack :

MITM



মাঝে বসে সব data দেখে, use, monitor

→ ~~ARP, দিয়ে~~ ARP spoofing & ~~MAC~~ DNS spoofing এর মাধ্যমে করে.

——— x ———

Spoofing

Date : 23.07.25

Buffer overflow attack : যে i/p দিলে memory space override, এটা use করে attacker exploix করে.

Back door : program develope এর সময় developer-রা কিছু code open রাখে like authetication. বারবার দেওয়ার জন্য door open থাকে, যাকে exploit করে attacker system এ enter করে, একবার door open রেখে যেতে পারে পরে আবার আসবে attacker.

Email spoofing : একজনের email কে use করে spoof করে অন্যজনকে attack purpose-এ email পাঠানো.

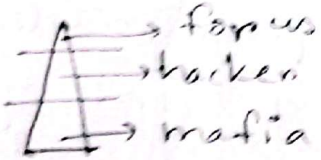
Ip spoofing ও হতে পারে.

Integer overflow attack : integer এর ক্ষেত্রে হয় Buffer overflow attack এর মতো,

Financial attack

Salami Attack: Eg: prime bank charges 200Tk as service charge for each customer at the end of the year. lot of money.

Surface web:
Dark web:
Deep web:



Surface web:

SQL injection:

—— × ——

Date 30.07.25

*SQL injection:

*| Cross site Scripting (XSS):

*| Cross site request forgery:

*| Rainbow attack:

*| Brute force attack:

*| Wifi eavesdropping:

- Surface web : যা আমরা use করি,
  Dark " : Criminal ধরনের,
  Deep " : mafia টাইপ,

SQL injection: database type এর software -এর উপর কাজ করে।

```
SELECT * FROM users WHERE
    user_id = 'user_input' AND
    password = 'password_input';
```

SELECT * FROM users WHERE user_id = '0R=1'

↳ user_input password bypass করতে পারি।

→ code inject করে database থেকে info delete, authentication bypass, edit etc.

Cross site scripting: website এ করে।

• নিজের ইচ্ছামত hacker তার page-এ redirect করে।

Cross site request forgery: not an attack → appears as valid request

- bank এর কোন login করতে হবে, page এর যেকোনো জায়গায় malicious কিছু দিয়ে রাখবে, click করলে transaction request goes to bank, then money tranaction হবে, hacker এর কাছে,

→ Rainbow attack: targets hash table

→ Brute force attack: সব combination try করা হয়, like OTP ; ↳ তাই time limitation

→ Wifi eavesdropping: wifi এর under-এ যত network আছে তার info নেয়া যায় (using wireshark)

*। Internet time theft: hotspot use করা অন্যের।

exam • বলতে কী বুঝায়, কীভাবে কাজ করে, example.

18.08.25

IAM Architechture:

Defense Archi: Authentication:

- Applocker
- Sand boxing / Jailing
- Patch management
- Least privilege
- ~~Authentication~~
- Defense in depth

} Preventive measure

1. Applocker: feature of windows. those better ← White: feature, website, allowed
   - policy / Protocol
   - full access না দেয়া
   - White & black listing Black: not allowed.
2. Sand boxing: quarantine করা
   - malicious কোন কিছু চালালে sand box/ quarantine create করে add করে,
   - pc safe mode এ on করা - এটাই sandboxing

3. Patch management: বিভিন্ন patch
   - update
   - new feature add
   - " security " "

4. least privilege: - কোনো user কতটুকু privilege পাবে তার terminology. (part of authorization)
   - authorization: after getting access কী কী role authorize করতে পারবে.
   - Cash manager - only access to cash management
   - transaction - same ↗

এখানে authorize করা অন্য কেউ, security ensured.

l.p: minimum privilege যাদিকে তার role ভিত্তিক perform করতে পারবে,

↙ Threshold of privilege.

5. Defense in Depth: PC এর every layer-এ security ensure করা।

- fail secure
- " open
- Seperation of Duties

fail sequre: system suddenly crash করলে - possibility of attack তাও system secured থাকে।

fail open: fail condition-এ open থাকে যাতে retrieve করা যায়।

Sepration of Duties: আলাদা role duty অনুযায়ী role applied. System-এ duty অনুযায়ী role assign.

Date :

Authentication: verifying of a user in a system before giving access.

IAM → এর component authentication.

IAM architechture
Types of authentication — (4)
→ Knowledge-based (something you know)
→ Possesion based (" " have)
→ Inheritance " (" " you are)
→ Adaptive " (

•Knowledge: password, security question.

easy to implement
- security top level X

- possesion: smart card, OTP
  - security comparatively high
  → risky if lost
  hassle
- Interitance: fingerprint, eye scan, face recognition.
  → implementation harder
  - high security
- Adaptive:

MFA:

Identity & Access management: (IAM)

access managment architechture of a system.

~~key components.~~

- not tool or tech, set of policies or rules of implementation access mangement.

Date

Key components:

1. Identification / Identity provision
2. Authentication
3. Authorization
4. Auditing

1) new employee ~~ग~~ identity creation
2) credentials assign
3) access not given for all things limited access
4) After creating identity getting authorization, system ~~ग~~ data a leak ~~होने~~ ~~वाला~~ ~~या~~ monitoring, sus ~~गतिविधि~~ ~~या~~ auditing like IT auditing
   2parts → continuous monitoring
   → auditing

IAM Tools:

1. SSO
2. PAM
3. IGA
4. MFA / 2FA / SFA

1. SSO: single sign on
google account দিয়ে youtube, photos, gmail all access.

4. MFA: Pass + OTP
" + Pattern
" + biometrics
~~" + Eo~~

—— × ——

27.08.25

IAM Tools:

SSO → Single Sion on
MFA → Multifactor auth
PAM → Privilege Access Mgt
IGA → Identity & Governance & ~~Auth~~ Administration
↳ policy/framework/documentation

2. PAM: Admin কে বেশি privilege দেওয়া হয়। special users দের জন্য applied হয়।

3. IGA: policy/documentation follow করা।

IAM architure (solution approach):

1) on-premise: company/organization এর core level এ exist করে।
→ secure (সবচেয়ে ভালো soln)
→ more cost

2) cloud-based: on-premise না থাকলে cloud এর help নেয়া।
- easier (money → service)
- inst cost, secure level কম

3) Hybrid: (1) + (2)

Steps to Implement:

→ Reqr Analysis

→ Risk "

- freq. of ocurance/likelyho
- severity

→ Model / Architecture design

→ Implemetation

→ Testing & training

→ Monitoring /evaluation & feedback

———x———

Date 15.09.25

★★★

1. Risk Management

2. Zero Trust Model

Risk management: system ও চিন্তা

- threat identification
- Risk evaluation
- Mitigation

key concepts - যা consider করা হয়।

i) Asset

ii) Threat

iii) Vulnerability

iv) Risk

v) Control measures ~~mechanisms~~

Asset: Bank network system -ও risk management, Asset protect

— database, tangible/intangible, hardware, software

application. people ~~indirect~~ associated with these

Threat: phishing malware attack

Vulnerability: যে weakness exploit করা যায়, যে weakness → vulnerability না, threat হয় ।। exploit করতে পারে তা vulnerability

Risk: যে যে vulnerability occur করার chance আছে.

Risk = likelihood (হতে পারে বা না) × impact (severe না low)

on basis of this Risk — high
— medium
— low.

control measures: যে steps নেয়া হয়।

Why risk management important?

- imp data breach না হয়,

Phases of Risk management:

1. Risk identification
2. ।। assesment
3. ।। mitigation
4. Monitor & review

Risk identification:

identify asset → threat type → vulnerability (weakness)

assesment: occur হওয়া chance কেমন
impact কতটুকু?
- low
- high
- medium

mitigation: ~~কোন risk টি~~ avoid ~~risk~~ / accept / transfer / share / mitigate

avoid: যে app থেকে আসে তা বন্ধ করে দেয়া,

accept: impact কম তাই accept the risk.

transfer: third party র থেকে solution নেয়া,

share: distribution ~~করে~~ অনেক system এ

mitigation: reduction

Monito & review: continously monitor the system/mechanisms
review - new risk এর জন্য not ready
~~whole~~ structure নতুন করে সাজানো

*/ cyber security risk management challenges - capability - এর অভাব
- new threat আসবে,

zero ~~day~~ trust Model:

→ Definition
→ key principles
→ How to implement
→ How zero trust minimizes risks
→ five pillars of zero trust model.

→ In cyber security why trust is vulnerability?

Key principles:
- least privilege
- MFA
- Micro-segmentation
- Risk adaptive control measures.

Healthcare

Oricef
Ceftriaxone USP

How to implement:

1. Identify the protect surface. (DAAS)
2. Map the transaction flow
3. Design / architect the zero trust model.
4. Implement the zero trust policies.
5. Monitor

(1) DAAS → system / software
↳ Application
↳ Asset
Data

(4) Who
when
what
where
how

(5) Monitoring

How zero trust minimizes risk:

Five pillars:

1) Data
2) Device
3) Network
4) Workload / ~~Data~~ flow
5) People

} asset → protect surface.

Basin Sir Suggestions

1. Cyber security Fundamentals
2. " " Attacks.
3. Reactive and Proactive.
4. Model and Architecture.

} All aspects question

1. CI Trial — Imp.
2. Malware — Types — Defn; Similarity, Dissimarity.
3. Attack Mechanism. = All = Difference.

   Spoofing Attack — ① DNS, ARP, Emp, DNS, INE
4. Real Time Q/A → Attack affect, different attack, phishing, attack,
5. Zero Trust Architecture, Risk Management, IBM attack Indetails पढ़ना.

   White Hat Hackers — Ethical Hackers.
   Black — " "
   Grey " "
   White - listing — अनुमत website allow
   Black — " — " " " " " नहीं

Authentication
Authorization

- IT origin. OMK. → Monitory transition আছে'.
- VSTI certified, ISO certified
- VAPT – Vulnerability Assessment Penetration Testing.

CT#3 Syllabus

→ All the defense Mechanism.

→ ZTA.

→ IAM.

→ Risk Management