2020mt13004 - Siddharth Mahajan
SSZG681

Q-1

a) The goal of the Bell-LaPadula security model is to prevent information flowing from objects at a security classification higher than a subject's clearance to that subject

Simple Security Condition:- It states that, S can only read O if and only if $l_o \leq l_s$ & S has discretionary read access to O.

So a person with TS level can read all levels of objects.
A person with C level can read C, R and U; but not TS and S level objects.

*-Property:- It states that, S can write O, if and only if $l_o \geq l_s$ and S has discretionary write access to O.

So a subject with 'U' level can write all levels of objects.
And a subject with 'C' level can write C, S, TS, but not R and U level ~~objects~~. objects.

b)

2020mt13004 - Sa...
SSZG681

Q-1

b) Apple (TS, {MKTG, HR})

Document (S, {MFG, HR})

Based on simple security condition, since Apple is TS, and wants to access document of S level, and

$TS > S$, hence, $l_o \leq l_s$, hence Apple can read.

Based on *-property, since Apple is TS, and wants to write document of S level, and $TS \not\leq S$, hence $l_o \not\geq l_s$.

hence, Apple cant write.

~~Thus, But, document category is not dominated by subjects category.~~ But {MKTG, HR} doesn't dominate {MFG, HR}.

Thus, Apple can't read document (S, {MFG, HR}), and can't write. too.

Neither read nor write.

c) Banana (C, {HR})

Document (C, {MFG})

Based on simple security condition, since Banana is C, and wants to access document of C, level, and $C \geq C$, hence $l_o \leq l_s$, hence, Banana can read.

Based on *-property, since Banana is C, and wants to write document of C level, and $C \leq C$, hence $l_o \geq l_s$.

Hence, Banana can write.

But {HR} does not dominate {MFG}.

Hence, Banana can neither read or write (C, {MFG}).

2020mt13004- Siddharth Mahajan
SSZG681

Q-2

a) Least common mechanism:- The principle states that mechanisms used to access resources should not be shared.

Sharing resources provides a channel along which information can be transmitted, and so such ~~sharing~~ sharing should be minimized.

Minimizing the number of shared mechanisms also reduces the scope of an attack that compromises such a mechanism.

Eg:- Program that enables employees to check their payroll (read), should be separate from program that modifies (write).

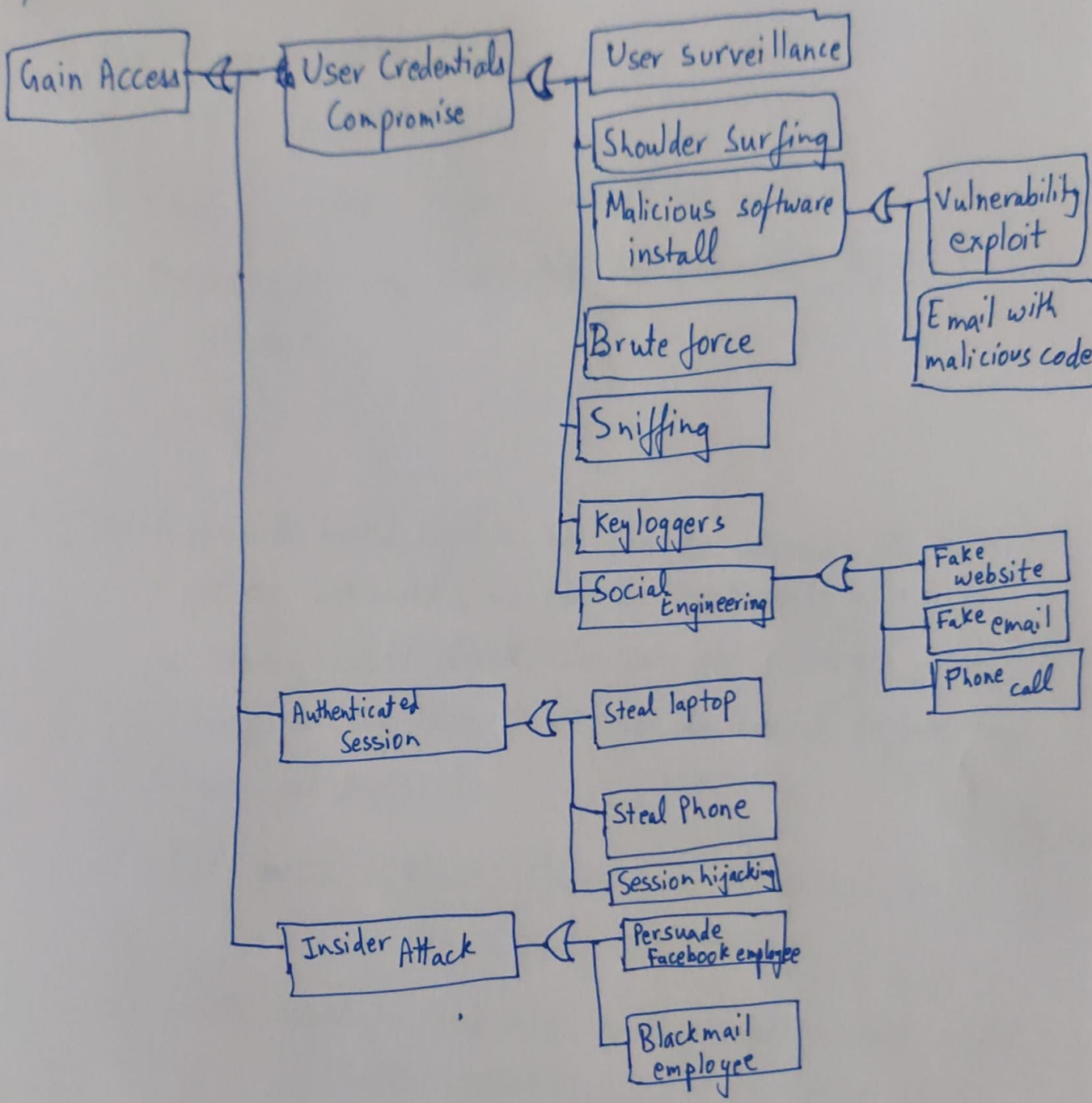
b) If we build a technique to disable account after 3 consecutive failed login attempts, then if the attackers do a brute force on lot of accounts, then all those accounts will be disabled. The users will not understand what happened, and will be stopped from accessing the system. Hackers can lock out all the users by passing random login credentials for all the users. Thus, legitimate users will not be able to access the system.

Least common mechanism, states that mechanism used to access resources should not be shared.
And if we disable account after 3 consecutive failed login attempts, then in fact we are sharing the login module, which provides access with the security module, which inhibits password guessing. Since, we are sharing the mechanism, it violates the 'least common mechanism'.

SSZG681

Q-3

a)


Gain Access
User Credentials Compromise
User surveillance
Shoulder Surfing
Malicious software install
Vulnerability exploit
Email with malicious code
Brute force
Sniffing
Keyloggers
Social Engineering
Fake website
Fake email
Phone call
Authenticated Session
Steal laptop
Steal Phone
Session hijacking
Insider Attack
Persuade Facebook employee
Blackmail employee

Q-3

b) Components involved in user authentication:-

i) Password based login
ii) OTP based login
iii) Oauth based login (Gmail, Yahoo, etc)
iv) Authenticate via Notification to previously logged in session.

c) i) Password based login:- We can do various attacks to get the password. We can do bruteforce attack or dictionary based attack. We can get password from old dumps & try those. We can do social engineering to get passwords.

ii) OTP based login:- Malware in the phone or via social engineering.

iii) Oauth based.:- Hack into email provider, which might have weaker security compared to social media.

2020mt13004- Siddharth Manayan
SS24681

Q-4

a) Confidentiality :- Low
Availability :- High
Integrity :- High

Since, the information is public, there is no impact for Confidentiality. But since it is on web server, and assuming it is important and frequently used data, if the web server goes down, i.e., Availability is impacted, then it can have High impact.

Assuming the organization has no backups of the data, and hacker modifies the data on the web server, then integrity is lost, and ~~as~~ assuming data is trustworthy can have high impact.

b) Confidentiality :- High
Availability :- Moderate
Integrity :- High

Since, it is extremely sensitive information & pertaining to investigation, confidentiality & Integrity is upmost important, hence loss of those is high impact.

If availability is lost, investigation processes might halt, hence, moderate impact.

c) Confidentiality :- Low
Availability :- Moderate
Integrity :- ~~Moderate~~ High

Since it is routine admin info, not privacy related, hence confidentiality is not an aspect to worry about.

But availability & integrity is important, during audits or reconciliations, since it is financial info.

4

d) Confidentiality :- Low
Availability :- Moderate
Integrity :- Moderate.

Since it is UI institutional data, confidentiality is not an issue. But we have to keep the data available at all times, for employee, or others to access. Hence, moderate impact on availability. Since it is UI data, we want to maintain integrity, so as to not cause any unauthorised changes in the UI data. Thus moderate impact for loss of integrity.

e) Confidentiality :- Low
Availability :- Moderate
Integrity :- High.

Department & course data is not confidential, hence no impact on loss of confidentiality.
Since, the teachers & students rely on that data, if web server goes down, then it might have moderate impact on availability, as they can fallback on bulletins & pamphlets.
The data on the university web server has to be accurate & trustworthy. Hence high impact on loss of integrity.