# Database Security

CS332Database Security

John Denson

By Robert Green

The CIA tirade is the process or procedure of securing a system by the means of Confidentiality,

Confidentiality: the act of keeping a clients data out the hands of a malicious user and accessible to only the user or the client. This is done by data validation or password, biometrics or the like.

Integrity: is the process of keeping ones data intact, and available to the user, This is also the act of keeping Authorized and unauthorized user’s from manipulating the data,

Availability: This the act of making sure that the data is reliable to the user and is specific to the user. Because of natural disasters and user mistakes, sometimes its flawed software or from malware and worms.

Authorization: This is the process where the server accepts or deny the packets and gives a client access to a file or a resource. It is coupled with authentication so the server has some knowledge of who the user is, this maybe passwords or bio metrics, most websites do not use authorization to access files.

The steps needed to secure user accounts:

Once more I like data validation, this is the process of using authentication passwords, encryption

To validate a request for data this gives the server the information that is needed to verify if the client is supposed to accessing the data, Firewalls and Encryption are used also passwords and biometrics, database files are placed to secure the data of the client to the client and not the unauthorized user, a malicious user might want to use SQL injection to try to gain access to the data and the user also might try to use a XSS reflected to penetrate a database, these are attacks

that directed to a database.

The steps to maintain user integrity is encryption, this process of using a public or private key to

When a packet is sent to the server the server uses this key to recognize that the packets is a safe and is for a specific user, the server the reads the package that is sent validates it and delivers it to the client that it is meant for user, Through the act of malware malicious users try to impersonate a valid package and then try gain access to one account this way, An IPS or IDS and firewalls are supposed to alert a company when an intrusion has happened, then there are the things that are out of company control and this would come in the form of natural disaster or simple blackouts and the like, then there is user misinformation and lastly we need to train staff to be able to recognize these attacks and when they happen so that they can be repoted and we can get a jump on the intrusion.

What happens in the real world when these types of attacks happen:

It could be a lot of things the most important one might be the passwords or the information needed to access ones bank accounts and all of ones monies all being stolen, It also happens to matter what the intention of the malicious use are, some hackers just want to penetrative your system and do crazy things, but there is Ransome ware and worms and Trojan horses in these case

A malicious user might want sell you the use of computer back as they have full access to your data

And full control of your computer it might as well be his/hers. In the event that a black out happens

Your system might go down, in this case a hacker might exploit a vulnerability and your system will reboot with the data, this can also lead to the data losing its integrity and loss of information.