Database Security

Confidentiality, Integrity, Reliability

By

Prof. Muhammad Iqbal Bhat

Department of Higher Education

Government Degree College Beerwah

Topics

Database Security Requirements

Confidentiality

Integrity

Reliability

Recent Database Security Breaches

Breach Name	Date	Number of Records Exposed	Description
McDonald's	November 2020	Unknown	McDonald's suffered a data breach in which an unauthorized party gained access to some customer and employee data, including contact information and some franchisee data.
Ubiquiti Networks	January 2021	Unknown	Ubiquiti Networks, a networking equipment manufacturer, was hacked in a sophisticated attack that gave the intruder root access to servers, including the ability to remotely authenticate as administrators.
Bonobos	January 2021	7,85,000	Bonobos, a men's clothing retailer, suffered a data breach in which unauthorized access was gained to its e-commerce platform. The breach exposed customers' names, phone numbers, and shipping and billing addresses, as well as the last four digits of credit card numbers.
MeetMindful	February 2021	1,45,000	MeetMindful, a dating app, suffered a data breach in which an unauthorized party gained access to a database containing users' email addresses, usernames, hashed passwords, and other account information.
Dave	February 2021	7,50,000	Dave, a personal finance app, suffered a data breach in which an unauthorized party gained access to a database containing users' names, email addresses, birth dates, and hashed passwords.
LinkedIn	June 2021	92,00,000	LinkedIn suffered a data breach in which an archive of user data was posted for sale on a dark web marketplace. The data included users' email addresses, phone numbers, workplace information, and some hashed passwords.
EA	June 2021	7,68,000	EA, a video game company, suffered a data breach in which an unauthorized party gained access to a database containing source code for some of its games, as well as some related internal tools.
Geico	April 2021	2,00,000	Geico, an insurance company, suffered a data breach in which an unauthorized party gained access to driver's license numbers belonging to some of its customers.
Air India	May 2021	4,50,000	Air India suffered a data breach in which personal information belonging to its customers, including passport details and credit card information, was stolen.
T-Mobile	August 2021	5,30,000	T-Mobile suffered a data breach in which an unauthorized party gained access to some customer data, including names, phone numbers, and account PINs.

Database Security Requirements:

Database security is the protection of data against unauthorized access, use, disclosure, modification, or destruction.

Security requirements are essential for any database system to ensure that data is secure and protected.

There are several security requirements that a database system must meet to be considered secure, including confidentiality, integrity, availability, and accountability

Confidentiality:

1. Confidentiality is the requirement to ensure that sensitive data is not disclosed to unauthorized individuals or entities. It is a critical aspect of database security, especially for databases that contain personal or sensitive information.
2. Some examples of how to ensure database confidentiality include:
3. Implementing access controls to restrict access to the database to authorized personnel only.
4. Using encryption to protect sensitive data stored in the database from unauthorized access.
5. Implementing data masking or redaction techniques to hide sensitive data from unauthorized personnel.
6. Regularly auditing and monitoring access to the database to detect any unauthorized attempts to access sensitive data.

Lack of Confidentiality in Databases:

In 2019, Capital One suffered a data breach in which the personal information of over 100 million customers and applicants was exposed. This was due to a lack of confidentiality in Capital One's database, as a misconfigured firewall allowed the attacker to gain unauthorized access to sensitive data.

In 2018, Uber suffered a data breach in which the personal information of 57 million customers and drivers was exposed. This was due to a lack of confidentiality in Uber's database, as the company paid the hackers to keep the breach secret instead of disclosing it to the affected individuals and regulatory authorities.

In 2017, the WannaCry ransomware attack affected thousands of computers worldwide, including those of the UK's National Health Service (NHS). This was due to a lack of confidentiality in the affected databases, as the attackers were able to exploit a vulnerability in Microsoft Windows and gain access to sensitive data stored on the affected systems.

Reliability:

Reliability refers to the ability of a database to perform its functions accurately and consistently over time. A reliable database ensures that the data it stores is always available when needed and is not corrupted or lost due to hardware or software failures, power outages, or other technical issues.

Some examples of how to ensure database reliability include:

Implementing a backup and recovery plan to prevent data loss in the event of hardware or software failures.

Using redundant hardware and software configurations to ensure that the database remains operational even if one component fails.

Monitoring the database for errors and issues, and taking proactive measures to address them before they become critical.

Implementing failover systems to ensure that the database can switch to an alternative system if the primary system fails.

Integrity:

Integrity refers to the accuracy and consistency of the data stored in a database. An integral database ensures that the data it stores is correct and consistent, and that it is not modified or tampered with without authorization.

Some examples of how to ensure database integrity include

Implementing access controls to restrict access to the database to authorized personnel only.

Using encryption to protect sensitive data stored in the database from unauthorized access.

Implementing auditing and logging mechanisms to track changes made to the database and detect any unauthorized modifications.

Implementing data validation checks to ensure that data entered into the database meets certain criteria or standards, such as ensuring that phone numbers are in the correct format, or that dates are entered in the correct format.

Lack of reliability and integrity in a database:

2019: In 2019, the Iowa Democratic Party's mobile app failed to work properly during the state's caucus, leading to a delay in the reporting of results and widespread confusion. This was due to a lack of reliability in the app's database and software.

2017: In 2017, Equifax suffered a data breach in which the personal and financial information of 147 million people was exposed. This was due to a lack of integrity in Equifax's database, as the company failed to patch a known vulnerability in its systems in a timely manner, allowing the attackers to exploit it and gain access to sensitive data.

2018: In 2018, Cambridge Analytica was accused of misusing data harvested from millions of Facebook users without their consent, in order to influence the 2016 U.S. presidential election. This was due to a lack of integrity in Facebook's database, as the company failed to properly enforce its policies and safeguards to prevent third-party apps from accessing user data without permission.

Questions?