6 Ways To Completely Revamp Your Access Control Infrastructure

Saturday, May 20, 2017 – No Password

In today's world, hackers get access to millions of credentials by compromising a single password. They become able to compromise the whole company's database, as happened in the LinkedIn hack; showing the importance of security of every single password.

When mass attacks like Adobe hack revealed 120 million accounts, the traditional password system was subjected for replacing by a password free solution.

Security experts realized the need of replacing the password based authentication system to revamp the entire security benchmarks.

We are going to address the weak points of the password-based authentication system and suggest new solutions to refurbish and prevent more than 80% of cyber attacks regarding passwords.

Security Weaknesses of Password Based Authentication System

With Owasp Web Application Security rules, nearly half of developers barely follow the standards. They build and secure their systems, but a wide range of possible uncovered vulnerabilities still make the Internet giants like Google, Facebook and Twitter announce their Bug Bounty programs to cover the unexpected vulnerability findings.

With that clarified, the following list contains security concerns regarding the traditional password based authentication systems.

- In traditional password based approach, the enterprise and company cyber security is entirely based on confidentiality and the strength of a single password.
- The Traditional Password based authentication system does not provide strong identity check. It is based on checking a single password only, can be hacked if the user enters specially crafted SQL commands instead of a valid password.
- The Password Based Authentication System needs to implement proper encryption during authentication process. If it doesn't, a malicious activity called sniffing; can cause the user data leakage during authentication process.

- The Password Based approach can be hacked by leveraging web app exploitation, consisting of various attacks on underlined database. These attacks are composed of supplying specially crafted information in place of valid credentials.
- A wide range of password attacks are applied for targeting credentials, including Phishing, Social Engineering, Key loggers, Security Question and Password guessing and Exploitation of base web application authentication system.
- In Password Based Authentication System, password complexity requirements cause a higher rate of password resetting, causing a daunting approach to regain account access.
- In Password based approach, the user credentials are stored in a single centralized database. In this case, the hackers specially attack the main database, to get access to millions of passwords by trying various attacks like SQL Injection, Trojans, Social Engineering and hacking the base web application.
- Taking over of mobile devices confirms the isolated use of Two-Factor Authentication measures.
- A Personal Identification Information (PII) is a piece of information used for identifying and distinguishing users. As PII is stored on client or server end, an attacker can obtain the PII by compromising server or stealing session information from the end user computer.
- In Password Based Authentication, attackers use Session Hijacking for targeting user accounts; while Session Hijacking is a type of attack, consisting of stealing the session tokens from the user computer.

Revamping Your Access Control Infrastructure

As millions of passwords are stolen in mass attacks, a password-based approach cannot cover the entire security standards. To find the alternative approach for security, we need to get rid of a centralized database along with application of a balanced privacy control in the user's hand. With that clarified, the users are in charge of their partially controlled privacy. This alternative system is maintained

to cut down the human error by efficiently wiping out the manual entry of passwords.

In this case, a solution like NoPassword can understand the needs for a secure alternative solution to passwords. It provides a modern authentication by killing all the limits of traditional password approach. Here are the key factors NoPassword provides.

1. **Real Time Authentication**

The authentication is revamped by letting the users authenticate in real time. It means the users do not need to provide somewhere stored login information; instead, they use real-time information like Biometrics.

2. **Biometrics Authentication**

Password based authentication has been replaced by leveraging biometrics while equally protecting privacy. Users can authenticate themselves by touching, eyes recognition, voice recognition, and face pattern identification. NoPassword does not store user biometrics on cloud on their servers, avoiding a centralized database of biometrics.

3. **No Centralized Password Database**

The user's Personal Identification Information (PII) is not stored in a centralized database. The user's authentication data is controlled, encrypted and secured with the App already installed on a user's phone. This mechanism is used to protect the user's biometrics information in case of any phone loss.

4. **Support Across ALL Operating Systems And Browsers**

NoPassword works across all operating systems, browsers, web apps, cloud apps, SaaS apps, VPNs and MDMs providing maximum platform support and integration.

5. Security By Design

Instead of conventional password approach, security is maintained by design capabilities. Users can authenticate themselves by using the built-in app approach, involving voice or face recognition in real time.

6. Automated Provisioning

Companies can easily manage the access of their employees' to various applications and authentication with automated provisioning and de-provisioning. This way the users are managed with efficiently implemented access controls. The users are identified, validated and granted access to their specific accounts. With automated provision and de-provision, the right users are facilitated to access their respective accounts.

Final Thoughts

To smarten the password security system, corporate businesses need to adopt a password-free solution like NoPassword. With NoPassword, companies provide a password-free authentication system to their customers, along with seamless integration with various platforms. The corporate brands can manage their user's access to various resources, along with handling them with pre-defined access control constraints.

NoPassword cuts down the traditional security flaws of services like Two-Factor Authentication, Token Generators and Password Resets, and provides a password-free approach to make authentication more secure and hassle free. It also covers a long range of corporate needs by providing integration support with various Cloud and Web apps, Workstations and Computers, VPNs and Remote Desktops, MDM apps, Legacy apps and Wi-Fi.

The NoPassword Authentication system makes the corporate infrastructure able to provide flexible identity management. It enables your customers use flexible ways to sign in more often, on various platforms including Web Applications, Mobile Apps, Online Transactions, Online Authorization and Internet systems.