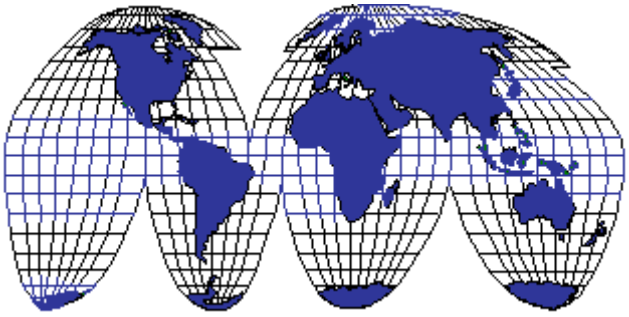

Sedicii – Zero Knowledge Authentication

Introduction & Benefits

ZERO KNOWLEDGE PROOF – AN INTRODUCTION

The Zero Knowledge Proof (ZKP) authentication protocol is used in cryptography systems to allow a party to prove that he/she knows something (i.e. credential), without having to transmit this credential. There are two parties involved in ZKP; the prover A and the verifier B. ZKP allows a prover A to show that they have the credential (for example, a credit card number or password), without having to give B the exact details of the credential. With Zero Knowledge Authentication there is no transmission or storage of password / credential hashes on the authentication server and the fundamental benefits of ZKP in the authentication process are as follows:-

- **Zero-knowledge**: if the statement is true, the verifier will not know anything other than that the statement is true. Information about the details of the statement will not be revealed.
- **Completeness**: if the statement is true, the honest verifier (that is, one following the protocol properly) will be able to prove that the statement is true every time.
- **Soundness**: if the statement is false, it is almost impossible, to an astronomically small chance, that someone could fake the result to the verifier that the statement is true.

CHANGING TECHNOLOGICAL LANDSCAPE / USER ENVIRONMENT

Rising use of web applications: The evolution of web-based applications has transformed how users engage online over the past few years. There are significant user benefits to be gained from using cloud based applications over traditional software and these include;

- Easier to use and are more presentable and attractive
- Do not require any additional hardware or software (installation, etc.) configuration
- Compatibility with devices, web browsers & operating systems
- Availability of new web technologies and languages has increased adoption of new dynamic applications (i.e. S2W, AJAX)
- Data is stored in one central repository and not individual computers
- A custom build web application costs less than the off the shelf application and provides greater efficiency and reduced maintenance.

With such fundamental advantages, it is important to focus on how to improve the security of web-based applications whilst maintaining the ease of use that users require.

Security issues relating to web applications: The many vulnerabilities and attack vectors for web-based applications include both web-specific (i.e. Cross-Site Scripting), as well as generic (i.e. Password Sniffing). Such issues expose the user to identity theft and loss of their personal, financial and valuable data. Whilst relying on service based security solutions such as SSL to protect applications, the introduction of new web concepts such as cloud computing and the growing complexity of attack vectors, it will no longer be acceptable, feasible, or viable to maintain such security by just adding more firewalls and SSL. It is important to note that existing authentication solutions rely on the computational difficulties of certain mathematical functions, such as integer factorization, which are becoming obsolete with the advent of quantum computing to solve such functions in a polynomial time. The advent of quantum computing suggests that not only algorithms, but also the underlying mathematical problems will become quickly outdated.

Current web application login process: The most common login system used currently in web applications is through the use of a form submission of a username and password enabled with SSL

communication. In more secure systems, the password is hashed using a javascript-based md5 hash before sending it over from the browser to the server (as detailed in Fig 1 below).

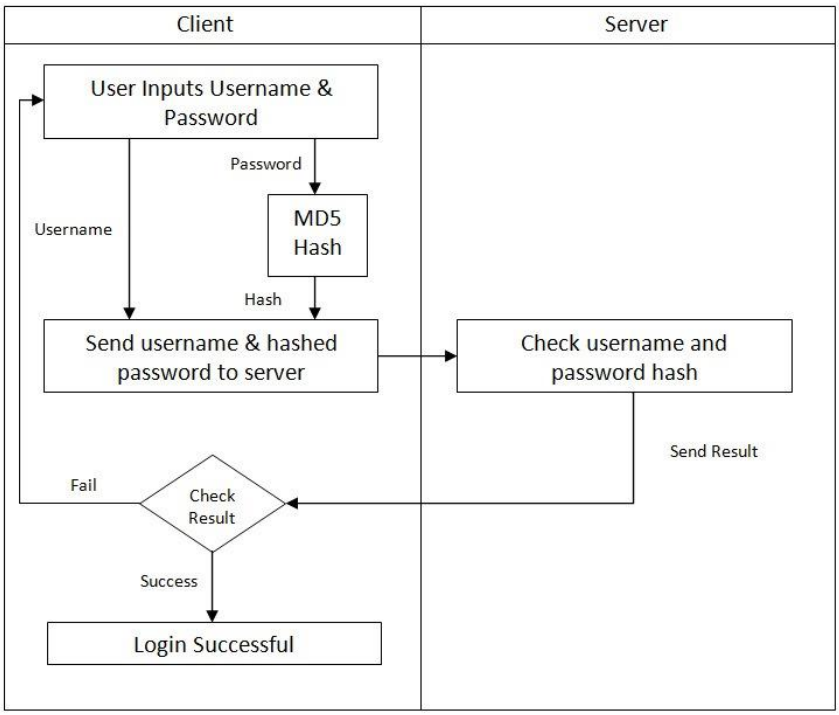

Fig 1. Traditional Authentication Process

However, by using these traditional authentication systems, there are many inherent problems such as sniffing and hash attacks including:-

Problem with the usage of insecure wireless networks: With the widespread availability of wireless hotspots providing today's users with convenience and ease of access, they are generally unsecure in terms of transmission. Many people do not realize the exposure and risk associated with using public Wi-Fi and the significant data security challenges it also provides for companies. Public user Wi-Fi access is susceptible to password sniffing replay, interleaving, and reflection, forced delay, chosen text attacks and multiple "man-in-the-middle" attacks and the existence of non-encrypted transmission of data through these mediums result in several vulnerabilities for both the user and company.

Problem with 3G Networks: Another alternative which many people rely on today is 3G, mobile broadband technology. Although there is protection with data encryption using the 128-bit A5/3 encryption algorithm, which is implemented across all 3G networks. The vulnerabilities in this encryption have been identified and algorithms compromised thus making it unsafe and susceptible to attacks, similar to unsecured wireless access points. Due to the known vulnerability with this system, there is a need to create a more secure authentication process for 3G access.

Problem with sending over password hashes: The issue of transmitting password hashes arises from the fact the information sent over the internet is all that is necessary for a hacker to masquerade as a legitimate user. For example, in a normal authentication, the user sends over their username and hashed password, which provides an opportunity for a hacker to sniff the username and hashed password and enable them to login as the user at any point in time. A more significant

issue with sending over password hashes revolves around the insecurity of revealing a plaintext password.

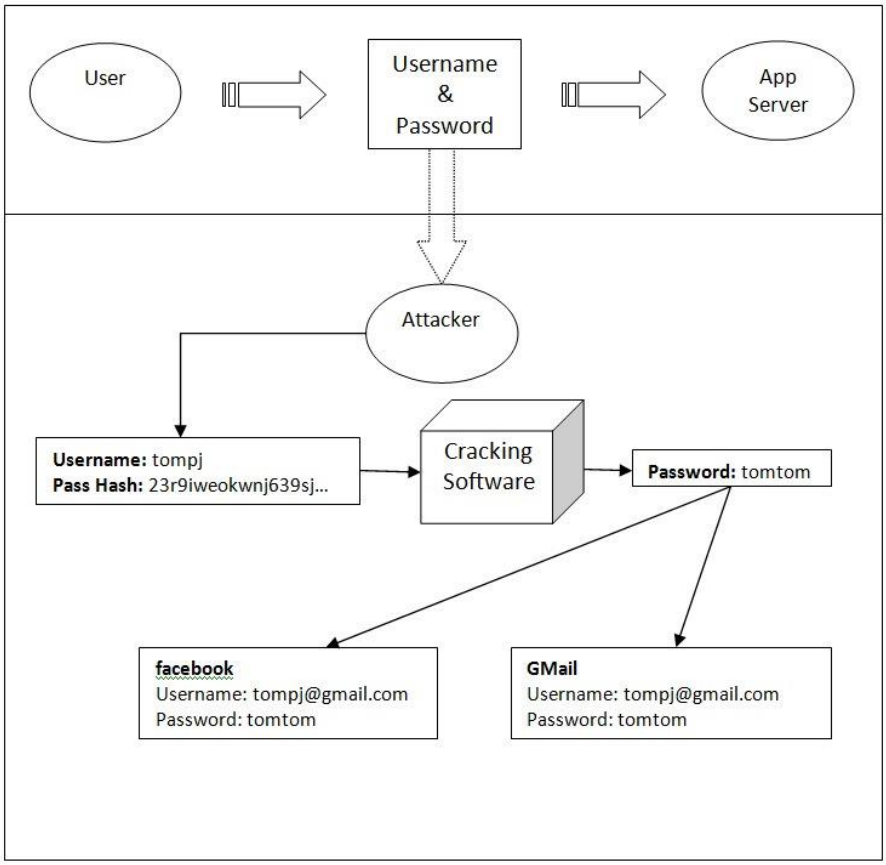

Fig 2. Password Sniffing via Man-in-the-Middle

Problem with using password hashes for authentication: Through sniffing the network, the attacker will be able to obtain the user's password hash, which becomes malicious when the user uses the same password for different services, thereby seriously impacting alternative service providers.

Summary: The transformation of user engagement with digital services in recent years has created significant vulnerabilities in the security and management of users' private information online. The traditional ways of authenticating a user have highlighted much vulnerability where a user's private information can be stolen and exploited creating significant inconvenience for the user and serious financial / reputational consequences to the holder of this data. Much of the data compromises have been from vulnerabilities in a third party integrated system, where the password or validated process was stored or transmitted and open for exploitation also. There is a need for a new approach to authentication in this challenging and vulnerable environment.

BACKGROUND & INTRODUCTION TO SEDICII ZKA

Sedicii Zero-Knowledge Authentication (ZKA) is a framework which allows companies to implement a proven protocol to allow for secure login without the need of transmitting the password or hash over the network. ZKA eliminates the need to store password hashes in the database, thus, if a hacker is able to obtain access to the database, he/she will still not be able to crack the passwords. The algorithm behind the system has been developed solely for the Sedicii Authentication process and is protected by US patent #8,411,854

Sedicii ZKA Security Considerations

ZKA is secure for the following reasons:

- Data transmitted over the network is no value to attackers: The data transmitted over the network is not usable by the hacker to fake an identity

- Eliminate obtaining password hashes or plaintext passwords from network sniffing: Any information being obtained during transmission will not allow the attacker to be able to crack the plaintext password of the user.

- Prevention of similar values used through the use of a salt: Through the use of a salt in the hashing function, the information sent over is only valid once and within a time limit. Thus, it will not be usable by attackers who intercept the information.

Comparison of Sedicii ZKA with other Authentication protocols:

Sedicii ZKA has benefits over other authentication systems due to the fact that there is no additional hardware required, as compared to systems such as biometrics and token-based authentication.

For example, biometric authentication systems rely on an external biometrics reader which not all users may have. Additionally, it has a certain level of uncertainty in its use and often requires a two factor authentication, which still requires using a password. For token-based/ dongle-based authentication, it requires additional hardware and can often result in identity theft from the loss of the identification device if not implemented correctly.

ZKA Framework: Similar to other web applications, the platform required for Sedicii ZKA is similar to that of a normal web application consisting of a client and a server as below (i.e. a Ubuntu Linux web server and a Mongo DB database).

Client Focus: As the objective is to prevent the transfer of a password over the network, pre-processing must be done on the client side to calculate the values for transmission. In order to do this, the following 3 components will need to be present:

- Interface
- Processor
- Algorithm

ABOUT SEDICII

Sedicii ZKP Authentication Technology is based on over 6 years of academic-led research and development on determining a method for validating a user's identity attributes without the need for that user to exchange any personally identifiable information (PII) (user's name, address, password, credit card, passport number, date of birth etc) with the organisation performing the validation. Using the ZKP protocol, it eliminates the transmission of a user's PII over the web or the storage of the PII to complete the authentication process. This eliminates the possibility of a user's PII being stolen or compromised during the authentication process. Sedicii ZKP Authentication Technology achieved patent in 2013.

Applications; The Sedicii technology uses new features available in the HTML 5 standard, eliminating the need for a browser plug-in, where the PII is stored in isomorphic graphical transforms, which cannot be decrypted or decoded without extremely massive computational effort. When a user logs in to a Sedicii enabled Identity Verification Server or Authentication Server, a series of challenges is sent to the user's browser from the server that requires responses. The information is authenticated only when all of the challenges are responded to correctly. A different set of challenges are presented for each new verification attempt. The same methodology can be applied to multiple types of private information such as credit card payment authorisations so that actual card details need never be transmitted over the web. Sedicii Technology can be applied to Industry requirements such as:

- Single Sign-On Applications / Embedded Device Single Sign on Authentication
- Omni-channel contact centre authentication with IVR visualisation
- Credit and debit card tokenization with embedded authorisation
- Identity Attribute Verification

Further information on how Sedicii technology can provide true authentication within the possible applications above can be provided as required.