AT.Pass

One-Time Password
Two-Factor Authentication
Solution

White Paper

iASPEC Software Limited
Unit 511, Lakeside 1
8, Science Park West Avenue
Hong Kong Science Park
Shatin, N.T. Hong Kong

Table of Contents

1. INTRODUCTION

PURPOSE OF THIS WHITE PAPER

This White Paper is written to assist its readers in examining the static "User ID and Password" system in more details and to understand its constraints in order to evaluate alternative authentication solutions.

A framework for the evaluation of user authentication solution based on the following three factors is presented:

1. security robustness,
2. ease of use and
3. cost effectiveness.

The target audience of this Whitepaper includes but not limited to corporate management and IT executives who are involved in technology evaluation, integration and purchase decisions. Some basic level of understanding in information security is required for the audience to grasp the essence of this White Paper.

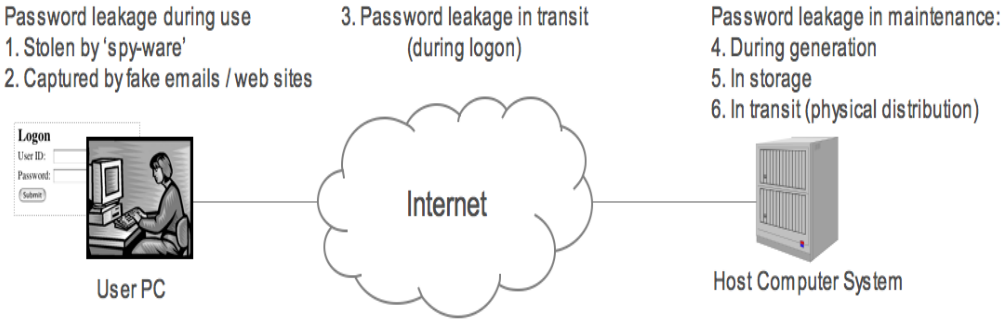
THE PROBLEMS IN STATIC "USER ID AND PASSWORD" SYSTEM

The ability to distinguish one individual from another is crucial in many aspects of life. In the physical world, our ability to distinguish people from each other is subtle. For those people we know, we remember their faces, voices and personalities. For others, we rely on additional proof of identity such as ID cards, driving licenses, birth certificates, passports, and sometimes through personal references. When a person has to "talk" to a computer system, one of the most commonly used method for identifying the person is through a series of codes or numbers traditionally referred to as "user-id" and "password".

Nowadays, Information and Communication Technology (ICT) plays an indispensable role in the commercial and social world, affecting the life of every individual. As a result, the vulnerability of the traditional "User ID and Password" system becomes more apparent. Traditionally, the "User ID and

Password" system uses static secrets that are subject to leakage during logon, password generation, storage and distribution. A number of additional protection measures are available to enhance the security of the static "User ID and Password" system such as hashing the password before sending it to the host computer through a network and asking the user to change password frequently. However, these measures only address part of the vulnerability problems.

The increased use in E-Commerce, Cloud Computing, Mobile Network and Social Network, have made the vulnerability of the "User ID and Password" system become more and more noticeable than before. When workstations and host systems are exposed to open networks not governed by a single organization, security risk of information systems is increased with the ever-growing number of users and devices accessing them in dispersed locations.


Password leakage during use
1. Stolen by 'spy-ware'
2. Captured by fake emails / web sites
3. Password leakage in transit
(during logon)
Password leakage in maintenance:
4. During generation
5. In storage
6. In transit (physical distribution)
Logon
User ID:
Password:
Submit
User PC
Internet
Host Computer System

Six potential points of password leakage during use, transit and maintenance

Quick Facts:

- The use of "User-ID and Password" identifying a person to a computer system can be traced back to the 1950s.
- In the early days when computing was available only to a small number of privileged individuals, the traditional "User ID and Static Password" system was quite adequate.
- Before the adoption of two-factor authentication for online banking in 2005, "phishing" attacks easily tricked Hong Kong bank customers in handing over usernames and passwords to their online bank accounts.

THE THREE 'FACTORS' OF AUTHENTICATION

The need for more robust authentication measures is always on the agendas of corporate IT executives. Multi-factor authentication refers to the approach of using more than one authentication means to complement each other, forming a more secure method to distinguish the genuine individual from an unauthorized one.

"What you know?"

"What you have?"

"Who you are?"
Logon
User ID:
Password:
Submit

Examples of the three factors of authentication means

Generally there are three types (or 'factors') of authentication means for an individual in accessing information systems:

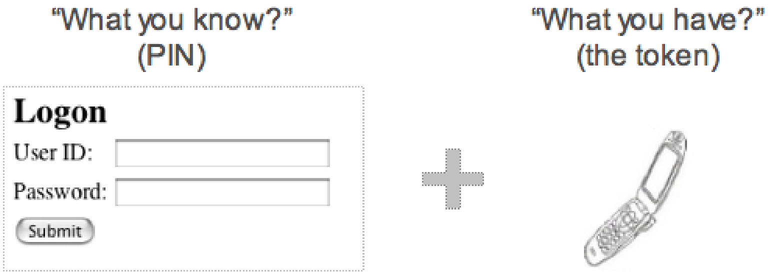
1. The first type is proprietary knowledge – the question of "what you know". If someone knows a secret code that is only known to the called party and the calling party, the called party considers the calling party as the intended user. This is the basic premise of the traditional static "User ID and Password" system.

2. The second type is personal belonging – the question of "what you have". If someone can present a personal belonging that only the intended calling party has, the called party considers the calling party as the intended user. This is like checking identification proof in the physical world. The issue is how to detect the presence of the individual's personal belonging such as physical token, smart card and mobile phone through the network.

3. The third type is biological characteristics – the question of "who you are". For examples, fingerprints, eye retinas and irises, voice patterns, facial patterns, hand geometry and hand writing.

USING TWO FACTORS IN AUTHENTICATION

For the strengthening of authentication of authorized users to allow them to gain access to higher security information systems, “two-factor” authentication schemes are commonly used. These two-factor authentication systems usually test “what you have” and “what you know”. Occasionally, biometrics authentication is also deployed in systems where special biometric reader devices can be installed and the security needs warrant such expense installation.



Two-factor authentication using token and PIN

Although technically viable, it is rare to find three-factor authentication systems that demand the testing of all three questions: “what you know”, “what you have” and “who you are”.

The need-for-security and the ease-of-use can be opposing forces. They must be properly balanced and carefully traded-off to result in good system design.

THE CRITERIA FOR EVALUATING AUTHENTICATION SCHEMES

We believe the fair and correct evaluation of an authentication solution is the trade-off of a number of characteristics of the scheme involved. The following three criteria are commonly used in the evaluation of an authentication scheme:

1. Security
2. Ease of use or convenience to the users
3. Cost involved

FIRST CRITERION: SECURITY

This is the first and most important criterion. We all know that there is no such thing as a "perfect" security solution that is absolutely unbreakable. Therefore, the right question to ask should be:

"Is the scheme secure enough for the intended purpose of the system?"

Some of the following authentication schemes are considered as higher security ones:

The public key infrastructure (PKI) is widely recognized as a secure framework. Many countries and cities have passed legislations related to electronic transactions and to give digital signatures the same legal standing as their physical counterparts. Digital signature is based on public key cryptography to verify a cryptographically processed 'digest' of an electronic document. For PKI systems to be secure, the secret key for the calling party or individual (technically known as 'private key') must be protected carefully during its life cycle from key generation, storage, distribution and usage. Particularly, PKI systems that use 'soft' key storage face higher level of risks than those that use secure hardware key storage.

The use of purpose-built and highly secure hardware device to capture biometric 'templates', such as fingerprints, palm prints, retina, facial features and to compare with those stored in the system to authenticate the identity of the subject.

SECOND CRITERION: EASE OF USE

Security and ease of use do not go together easily. They can be opposite forces. Given that PKI is considered as one of the highest security authentication schemes available, its adoption remains slow. One of the reasons for the slow adoption rate of PKI systems in authentication is that they are not only quite costly to implement and to maintain, but also fairly difficult to use.

For example, formal Certificate Authority practice statements (CPS) typically demand face-to-face verification of the user identification proof before a digital certificate can be issued. This is important since digital certificate represents the online identity of the individual and any mistake in the certificate issuance process would be disastrous. However, there are proprietary PKI systems that attempt to streamline the certificate application process. Some PKI systems compromise security with ease of use while others employ proprietary cryptographic methods to protect the certificate generation and issuance process. Another usability barrier of PKI based authentication systems is that Certificate Authorities usually only issue certificates and they do not authenticate them automatically. It is the responsibility of the user and the host system to authenticate the certificates themselves. For the user, it is quite a technical process. For the host system, it is a resource intensive process using the method of Certificate Revocation List (CRL) or the Online Certificate Status Protocol (OCSP).

Biometrics systems have usability issue too. No single biometrics system is 100% reliable for the whole population. For example, roughly 5% of the population may not be able to enroll to certain types of biometrics such as fingerprints. Biometrics systems have various levels of false acceptance and false reject rates (FAR/FRR) from 60% to over 90%.

THIRD CRITERION: COST

The total-cost-of-ownership, including the initial cost of the implementation, the on-going maintenance and support cost, is one of the key evaluating criteria. An authentication system that is both secure and easy to use may not be cheap. For example, one-time password systems that use the short message system (SMS) for distribution in mobile telephony have a heavy operating cost. As a result, SMS based one-time password systems usually restrict its use to a smaller set of high security transactions rather than for logon and general uses. Hardware-token-based one-time password systems can also be costly. With tokens costing up 10-20 US dollars each, it would become prohibitive for large-scale implementations. As a result, Hardware-token-based one-time password systems are generally limited to niche market such as those in virtual private networks (VPN) and for higher security corporate banking applications. Similarly, PKI authentication systems that use smart card or token are also expensive to implement.

Another significant cost for hardware-token-based one-time password systems and PKI systems is the heavy administrative cost of token distribution. Tokens can be lost, damaged or simply reach their end of design life with batteries drained out. The token replacement cost must not be underestimated.

Strong biometrics authentication systems can also be quite costly. They employ secure and often proprietary hardware devices for reading the biometrics and for template comparison. The cost of implementation and maintenance can be prohibitively high for general uses.

TO SUM IT UP

The three most important criteria to evaluate the appropriateness and effectiveness of an authentication system are commonly agreed as:

1. Security
2. Ease of use
3. Cost

Evaluation criteria

Fitness-for-purpose is the ultimate yardstick for measuring the suitability of an authentication scheme for a given situation. The balancing of the three criteria described above is the most crucial consideration in choosing your solution.

2. INTRODUCING AT.PASS

ONE-TIME PASSWORD

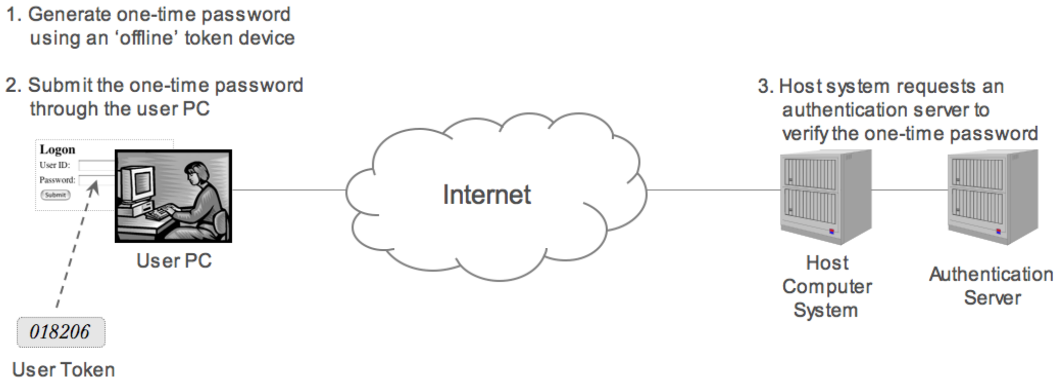
The vulnerability resulting from the connection of PCs, workstations, tablets, smartphones and a wide variety of client devices to host systems over the internet is one of the common concerns in the security design of today's information systems.

These client devices come in all shapes and sizes. They are of different makes and models, often in dispersed locations. Their ownership and management responsibilities can also be extremely diversified. The vulnerability of these devices due to the lack of adequate defense mechanism against various types of security exposure and intrusion is real and pressing.

We can continually remind the users of information system to take care of the integrity of the client devices that they are responsible for. However, it is not realistic to simply rely on the technical know-how of these individual users to do the right things to stop security breaches and to prevent frauds. One must also be reminded that users are sometimes required to access online systems using client devices which are open to the public. The trustworthiness of these public client devices can be questionable.

Security patches to software, anti-virus updates, firewall policy and administrative measures to enforce frequent changes of password are helpful in increasing the security of these client devices. However, hacking is becoming more and more sophisticated and even computer experts may not always realize that their personal computers have been compromised. It is an ongoing war between the hackers community and the honest users. Some hackers do it just for fun and fame while others have malicious intentions to steal secrets and to do harm to their victims. One the most notorious problem is spy-ware that is not easily noticed, even for computer experts. It is probably too late when the user discovers it because he/she may not have clue on the extent of harm that it has already caused. Some spy-wares collect user behavioral information for advertisers while others are designed to hack user's secrets. Many of the traditional authentication systems would have failed in these situations. This includes the most sophisticated digital certificate applications, especially for those that store the private keys in the hard disk.

Generally, “one-time password (OTP)” systems using ‘offline’ tokens are highly resistant to spy-wares because the tokens are not connected to the client device used to access the online systems physically or electronically. OTP token operates by generating a seemingly random number on regular time interval or on-demand by the user using a certain cryptographic algorithm. Some OTP tokens require the use of a PIN to unlock the tokens. OTP tokens are either synchronous or asynchronous. For the synchronous ones, the tokens are synchronized with the host’s authentication servers based on time or event, or both of them.


1. Generate one-time password using an ‘offline’ token device
2. Submit the one-time password through the user PC
Logon
User ID:
Password:
Submit
User PC
018206
User Token
Internet
3. Host system requests an authentication server to verify the one-time password
Host Computer System
Authentication Server

Typical setup of one-time password (OTP) systems

Traditionally, “offline” OTP tokens are embedded into and distributed as hardware devices. They can be expensive and often are limited to niche applications with small number of users or for high security applications where cost is not a major concern.

There is another commonly reported usability barrier for the conventional one-time password system with hardware-based tokens. For the tokens that rely on time synchronization, the scheme must be able to tolerate some degree of time drifting between the authentication server and the hardware device where the token is held. To overcome this problem, some of these token systems encode portions of the time information into the generated random number. This reduces the available number space and security level of the scheme.

Maintenance costs for one-time password token systems can be relatively high. Physical tokens can be lost or damaged. Statistically, average loss/replacement rate is about eight percent per year. The administrative burden of issuance and re-issuance of hardware-based tokens must not be underestimated.

THE AT.PASS SOLUTION

The AT.Pass one-time password, two-factor authentication system offered by iASPEC is a solution overcoming many of the shortcomings mentioned above on conventional products.

It is a synchronous one-time password system with both client token and authentication server support. The server knows how to recognize the token through proven cryptographic algorithms. Unlike traditional token solutions that use time as a parameter, the AT.Pass system does not do so as time drifting is unavoidable even on the most expensive hardware.

AT.Pass uses the mobile phones and various client devices as ‘containers’ to hold the one-time password tokens. It supports Android, iPhone, iPad, Java (MIDP 1.0 and 2.0) phones and is compatible with vast majority of the mobile phones and tablet devices in the market.

The AT.Pass system also provides alternative means for the distribution of the one-time-passwords. For example:

- OTP sent through SMS,
- pre-generated one-time password list known as the CueCard sent to the user’s registered email box when specifically requested.

Quick Facts:

- The AT.Pass system has a proprietary synchronization algorithm that derives synchronization information from the one-time password while maintaining a very large effective number space for optimal security. This means the end-users may accidentally skip a reasonable number of one-time passwords that are generated by software installed in their mobile phones and the authentication server can still immediately synchronize with the token upon successful token verification.
- AT.Pass won the Silver Prize of 2005 IT Excellence Award, Product category in Hong Kong.

THE INNOVATIVE DESIGN OF AT.PASS

The innovative design of AT.Pass has overcome many of the known limitations of conventional one-time password systems in the following ways:

1. Token distribution – the token is distributed online in the form of downloads (e.g. through App Store, Android Market), emails or SMS depends on the token type. The overhead costs associated with the administration and logistics required in token distribution are reduced to nearly zero.

2. Token security – the token is automatically loaded into the mobile phone, tablets and other target device with the token secret encrypted in strong encryption. Token once downloaded onto the device cannot be transferred onto another device.

3. Personalized token – The unique secret for each token is generated during its association with the authentication server. This is done only once and after the successful download of the token into the

device. If the user suspects that the token in his/her possession has been compromised, he/she can always obtain a new one by downloading it and associating it under his/her identity. Once the new token is associated, the old one is automatically revoked.

4. Mobile phone as token 'container' – The user can load the token as an App into his/her mobile phone, tablet or even PC. This is unlike conventional schemes under which the user may require to carry another hardware-based device for the generation of one-time passwords.

5. Strong cryptographic algorithm and Proven Security Design – AT.Pass uses a combination of SHA-1, SHA-2 and proprietary algorithms for the generation of OTP based on three levels of secrets (organization, system and user) that are embedded in the token. The encrypted user secret in the host system is kept in a separate authentication server. As a result, even internal hacking inside the organization is difficult. For additional security, the AT.Pass system may optionally choose hardware security module (HSM) to protect these secret keys from leakage out of the authentication server's space.

6. Multiple token types are simultaneously supported – each user is allowed to have multiple tokens that are loaded onto his/her mobile phone, tablet and the PC. He/she can also use the pre-generated OTP list distributed in the form of CueCard. All these tokens can be used interchangeably.

7. High performance and reliability – The AT.Pass system can be configured into a load-balancing server setup. When required for reasons of resiliency and workload capacity, multiple AT.Pass authentication servers can operate on a parallel fashion, thus enhancing availability and total system performance.

INTEGRATING AT.PASS WITH APPLICATION SYSTEMS

AT.Pass supports the RADIUS standard for integration with other products supporting this standard. Additionally, a set of Web Services API is provided for the sophisticated users to directly control and invoke the internal functions provided by AT.Pass.

RADIUS authentication standards

The AT.Pass system can be integrated with virtually all kinds of off-the-shelf virtual private network equipment (IP-SEC VPN and SSL-VPN), access control systems (ACS), proxy and reverse proxy, domain servers and Single Sign-On (SSO) systems using the industrial standard RADIUS authentication protocol. This is an easy “plug-and-play” style of integration of equipment or systems that the customers already installed.

Web Services interface

A set of Web Services (WS) is packaged with the AT.Pass system. Through these WS API, customers can tailor and build their own customized interfaces to support distinctive system administration functions and to provide different user experience. This interface is intended for the more sophisticated users having the need to fully control the life cycle of token management and for the meeting of their user authentication needs.

OpenID Interface

AT.Pass supports the OpenID Foundation authentication standards and its related protocols. It can be configured as an OpenID Provider for any application acting as an

OpenID Relying Party to request its authentication services.

USING THE THREE CRITERIA TO EVALUATE AT.PASS

We can now evaluate the AT.Pass system with the three criteria that we have discussed:

Security

The AT.Pass system represents the highest level of security in the category of offline one-time password tokens.

The AT.Pass tokens are physically secure since they are loaded in the protected memory of the mobile devices with strong protection.

Ease of use

The system alleviates the administrative burden in physical token distribution during their initial issuance and re-issuance as the result of damage or loss. AT.Pass tokens are distributed electronically into the target ‘containers’.

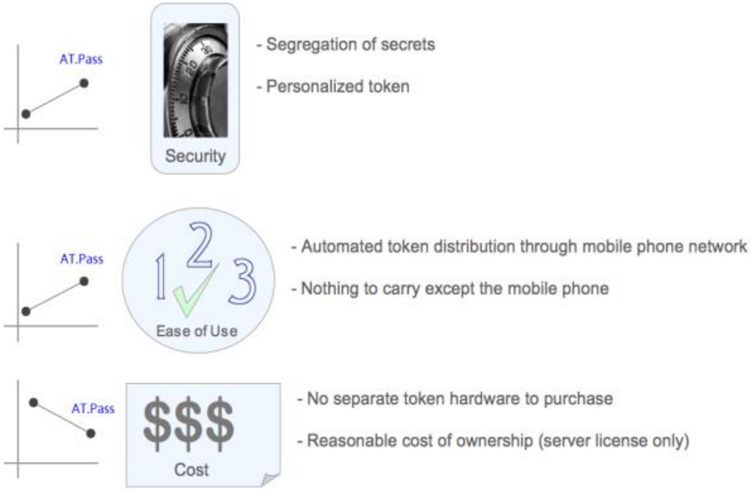
Moreover, OTP can be optionally distributed through SMS and CueCard. This gives additional degrees of flexibility to the users.

Cost

The AT.Pass system is designed for deployment in both in-house applications with a small number of users and for large-scale systems serving millions of users.

The AT.Pass system is highly scalable in design. Its flexible licensing scheme based on token numbers can be tailor to match the distinct and evolving needs of the customers.

The AT.Pass software support Java-based, Android, iOS and Windows Phone and Windows PC devices. It can operate in all major operating systems and different brands of hardware equipment of customer’s choice. This greatly reduces infrastructure diversity and therefore, the cost associated with platform support is controlled to a minimal.



- Segregation of secrets
- Personalized token

- Automated token distribution through mobile phone network
- Nothing to carry except the mobile phone

- No separate token hardware to purchase
- Reasonable cost of ownership (server license only)