

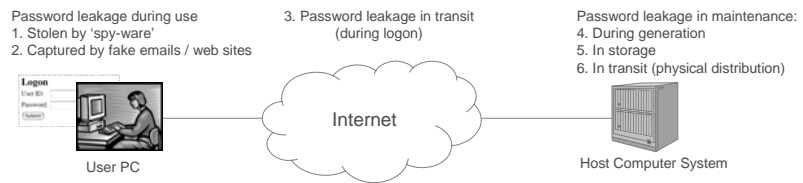


Corporate executives in every successful business realize the vulnerability of the traditional user-id and static password systems. There is always a pressing need for a *secure, easy to use and cost effective authentication solution*.

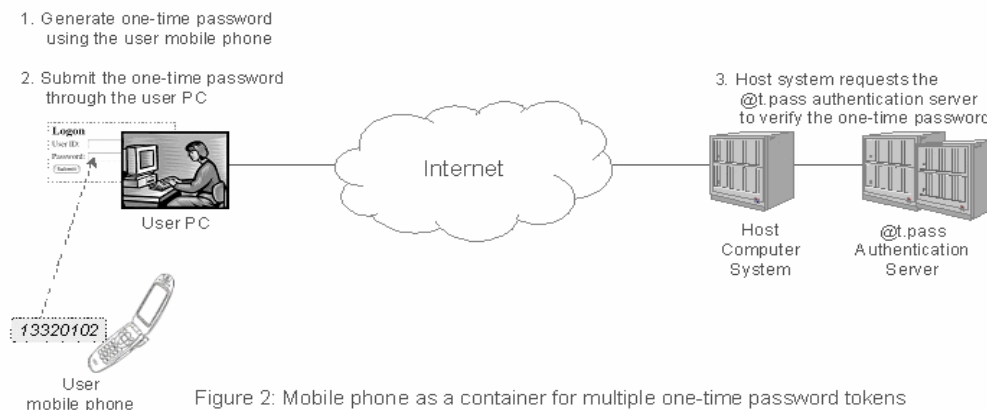
The vulnerability of static password system

The commercialization of the Internet with growing number of online systems has made the limitations of traditional “static User ID and Password” system more vulnerable.

When workstations and host systems are exposed to open networks, security risk increases with the ever-growing number of workstations and web sites. Individuals and organizations are facing the risks of fake email (‘phishing’), fake web sites and all kinds of active and passive hacking attacks. One of the most sophisticated hacking methods uses “spy-ware” to steal identity secrets of the victims. Keystrokes and mouse movements can be captured without the user noticing it.



The AT.Pass advanced 2-factor authentication system is a new generation of synchronous one-time password system. “Synchronous” refers to the ability that the AT.Pass authentication server knows how to recognize the client token using proven cryptographic algorithms without physical connectivity with the token. It uses the mobile phone as “container” to hold the tokens that calculate the one-time password. The synchronization scheme is event-based to alleviate some of the problems associated with clock-drifting found in products using time-based synchronization design.





Advanced 2-factor authentication

The AT.Pass system verifies two factors for strong identity management:

1. user personal identification number (“what you know”) and
2. the AT.Pass token in the user’s mobile phone (“what you have”).

Online token distribution

To avoid the logistics overheads associated with token issuance and re-issuance in traditional token solutions, the AT.Pass system issues tokens to the user’s mobile phone automatically through the mobile phone networks using SMS push technology.

Multiple Application Support

The AT.Pass system may be shared by multiple applications. J2ME phones can store multiple tokens for different applications.

Security

The system is highly resistant to spyware as the one-time password is generated by the user’s mobile phone that is totally offline from the client PC. Based on the principle of “segregation of secrets”, it also enhances security at the back-end as encrypted user PINs and token secrets are kept in separate machines. i.e. the host application system and the AT.Pass authentication server respectively. Optional HSM interface can be added to the AT.Pass authentication server when needed.

Easy to Use

Switching users to the AT.Pass system is seamlessly easy. The user simply enters the one-time password using the familiar user interface of the traditional static passwords system.

With a very small set of simple application programming interface (API), minimal effort is required for system integration with host applications and/or 3rd party security managers / single sign-on systems.

Universal Applicability

The AT.Pass system is available in two versions:

- The Network Version is plug-and-play with most industrial standard virtual private network (VPN), SSL-VPN, Proxy, Domain Server and Single Sign-on (SSO) system.
- Targeted for large scale deployment, the Enterprise Version permits full integration with user applications for complete control of token life cycle.

High Availability

As an option, the AT.Pass system supports

System Requirement

- Java 2, version 1.4.2_04 and above
- MS-Windows XP, Linux, AIX, HP/UX and Solaris

