AT.Pass One-time Password

Two-factor Authentication System

The vulnerability of traditional static password system

The widespread use of public, private or hybrid cloud computing platforms has made the traditional user-ID and Static Password system highly vulnerable to security bleaches. The vulnerability of traditional user-id and static password system is well understood. This commonly used technique for authenticating computer users is based on the verification of the user-id and its associated "static" password. This static password can be used multiple times until it is explicitly changed by the user. Not to mention the accidental leaking of the static password by its associated user, individuals and organizations are facing the increasing risks in losing their password as the result of malicious acts of the intruders and hackers. This can be in the form 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.

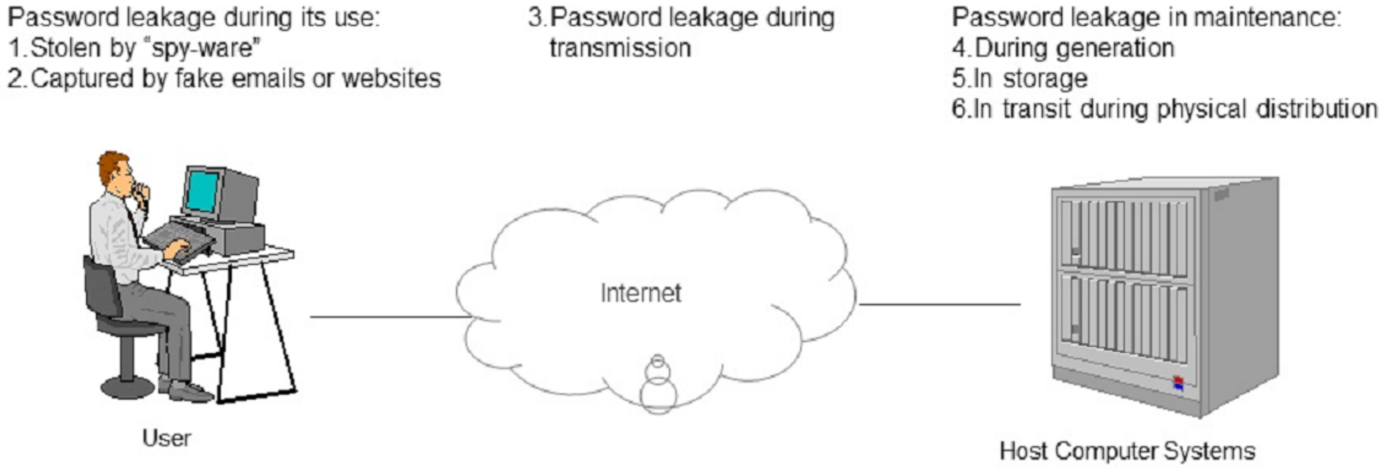
Password leakage during its use:
1.Stolen by "spy-ware"
2.Captured by fake emails or websites
3.Password leakage during transmission
Password leakage in maintenance:
4.During generation
5.In storage
6.In transit during physical distribution
Internet
User
Host Computer Systems

Figure 1. Six potential points of password leakage during use, transit and maintenance

The AT.Pass Approach

AT.Pass is an advanced OTP (one-time password) system. It is designed for easy integration into your own application systems, VPNs or any other solutions. With your system integrated with the AT.Pass authentication server, AT.Pass knows how to recognize the client tokens using proven cryptographic algorithms without physical connectivity with the token. These tokens can be downloaded into mobile phones, PCs or tablets, which act as "containers" to hold the tokens and on-demand calculate the one-time password. We also provide SMS-based OTP and our pre-generated password list solution CueCard as alternative options for users to choose. AT.Pass was awarded Silver Prize of IT Award Product Category (2005).

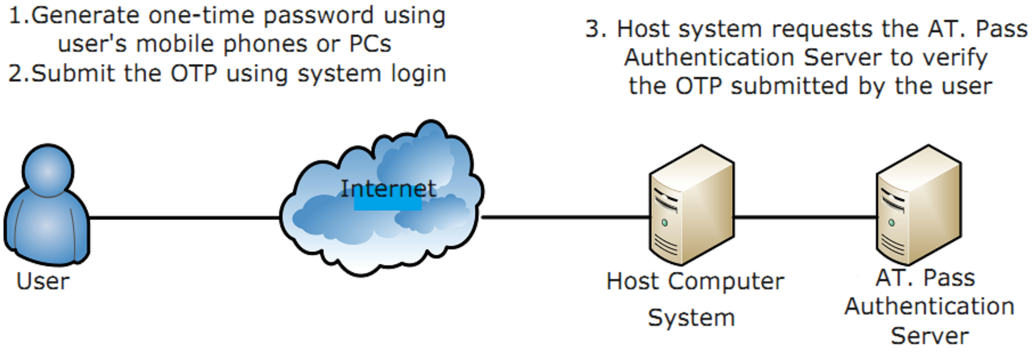
1.Generate one-time password using user's mobile phones or PCs
2.Submit the OTP using system login
3. Host system requests the AT. Pass Authentication Server to verify the OTP submitted by the user
Internet
User
Host Computer System
AT. Pass Authentication Server

Figure 2. One-time passwords are generated using tokens contained in mobile phones or PCs

Figure 3. Winner of Silver Prize 2005 IT Award Product Category

Token Types and distribution

AT.Pass employs multiple ways to deliver the OTP based on the pre-defined authentication type for each user:

1. Mobile token: a program (an app) can be stored in the user's mobile phone and generate OTP offline whenever required. Our app supports iPhone, iPad, Android Phones, Android Tablets and Java-enabled Phones.
2. PC Token: a program can be stored in the user's designated personal computer (Windows-based) to generate OTP upon request.
3. SMS-OTP: an SMS will be composed to send the OTP to the user's mobile phone upon request.
4. CueCard: an OTP list is pre-generated into a pdf file for usage or printout.

All these tokens are distributed online and the token lifecycle greatly reduces the administrative and logistic overheads associated with hardware-based tokens. The whole process is automated through the token distribution server (TDS) which is included as part of the whole AT.Pass System.

Features Highlight

AT.Pass is targeted from small to large scale deployments. It supports full integration with user applications and standard appliances and offers them complete control on the management of the token life-cycle.

Multiple Application Support

AT.Pass may be shared by multiple applications within the enterprise. For example, VPN, web mail, or other systems can all be integrated into to a single AT.Pass Server.

Token Distribution Server (TDS)

TDS helps to automate the token delivery to users for all token types. The user can choose the token type for their own convenience.

Multiple Integration Method

RADIUS interface is available for standard integration of authentication service. A complete set of Web Services API and Java Library are also available for invoking various services provided by the AT.Pass authentication server.

System Administration

A web based interface is included for the configuration and administration of the system.

High Availability

AT.Pass can be configured in an active-active, load-balancing mode to meet the highest standard of service availability in mission-critical application environments.