

## Protecting systems using One-Time Passwords

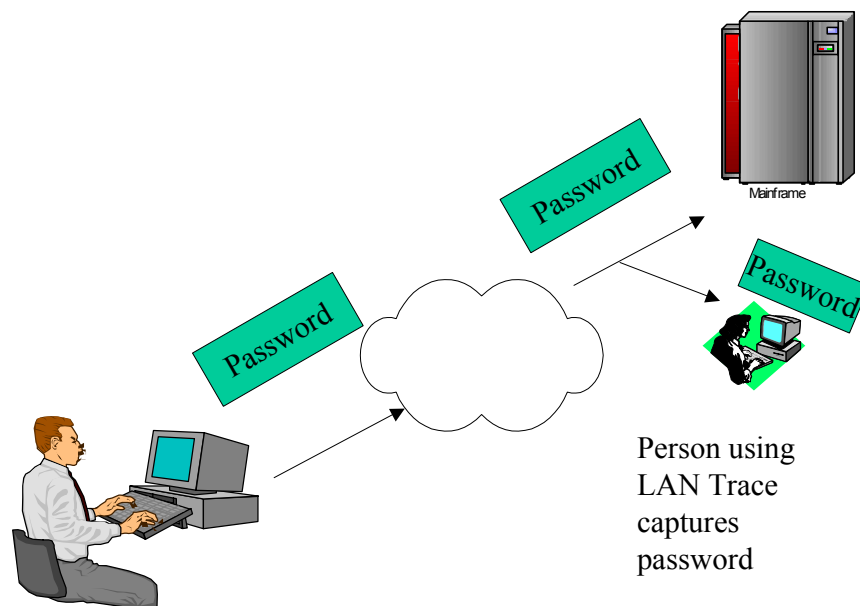
*Conventional computer security depends on keeping passwords safe. In many environments passwords can be intercepted as they pass over LAN and WAN networks. Many organizations use expensive token solutions to help secure passwords. PassGen is an alternate solution that uses Palm OS to provide secure logon to UNIX, Firewalls, Web Servers and OS/390 systems*

*PassGen provides a two-factor authentication system that improves security*

We all connect to our Computers using passwords. Passwords for many systems are the primary way of proving who we are to computer systems. Keeping Passwords safe from disclosure is the foundation upon which security of our computer systems are based.

Many users connect to computer systems using methods that send Passwords in clear-text or in a Hashed form across networks. Users who use Telnet, FTP or TN3270 or 3270 Terminals send Passwords in clear text. Browsers use a Hashed password that can easily be de-crypted.

These Passwords can easily be intercepted using LAN or Protocol tracing solutions. LAN networks can be easily monitored as these networks used a shared medium. All the users on the same LAN segment get visibility of each others data.



Any person connecting to a LAN can view data from others. Tracing programs are easily acquired, as many are Public Domain. This represents a significant threat to system security.

A Userid and Password can be retrieved from the network and then used by a third party to compromise a system.

## Protecting Passwords

To protect systems, Passwords need to be kept secret. Two options exist for traditional terminal based systems :

- *Encrypt all data traffic.* This requires deployment of software, keys and a considerable overhead in encrypting traffic.
- *Use One-time Passwords.* One-Time Passwords can be used only once. If the Passwords are intercepted they cannot be re-used. PassGen provides a facility to do this.

PassGen provides two one-time password systems in one convenient Palm OS application :

- The IETF One Time Password Standard – S/KEY (RFC 1760). Most UNIX and Firewall systems provide support for this standard
- IBM Security Server ( RACF ) Passticket algorithm available in RACF, CA-ACF2 and CA Top-Secret. This provides secure logon to IBM Mainframe systems. The Passticket can be used as a direct replacement for static Passwords, no changes are required to your existing applications

For systems with no One Time password support PassGen also provides encrypted password storage also.

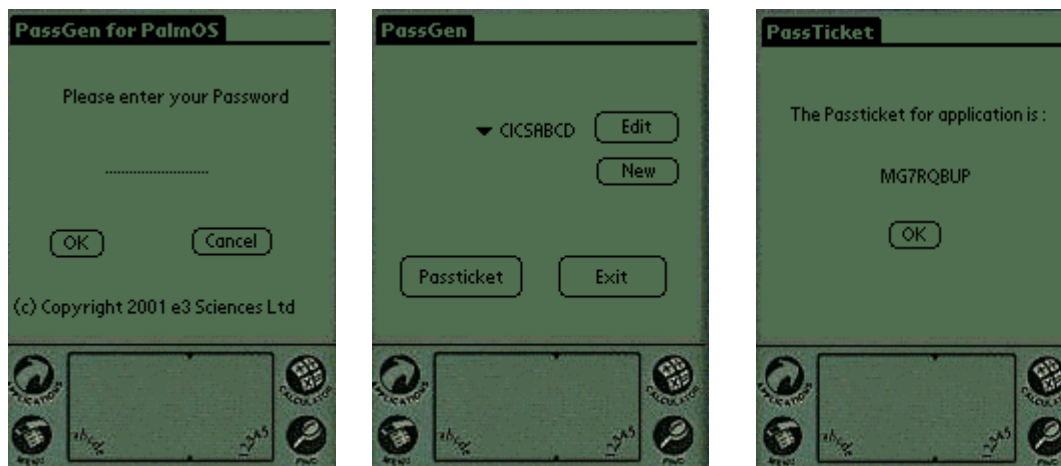
## Improving Security – two-factor authentication

PassGen for PalmOS provides two-factor authentication :

- Something you have – a Palm with PassGen containing the correct keys
- Something you know - the PassGen for PalmOS password controls access to PassGen

Two-factor authentication is generally recognized as a practical method to delivering reliable authentication.

PassGen on PalmOS provides an alternative technology to Token systems. Palm OS systems provide a cost-effective platform that the user can easily carry with them.



# PassGen for PalmOS



## **Key Benefits**

- Prevents Passwords from being intercepted on LAN and WAN
- Provides two-factor authentication improving security
- Provides secure storage for One-Time Password keys
- Provides secure storage for conventional passwords

## **Technical Requirements**

Supported Platforms : Palm OS 2.0 or greater. Requires 46K of system memory.  
Also available : Windows 95/98, Windows NT, Windows 2000

Supported Security Systems : Any S/KEY ( RFC 1760 )compliant system such as UNIX or Firewalls  
IBM Security Server ( RACF ) 1.9 or above  
Computer Associates ACF/2 6.1 or above  
Computer Associates Top-Secret 5.1 or above

*\*All TradeMarks are acknowledged as being the property of their respective owners.*