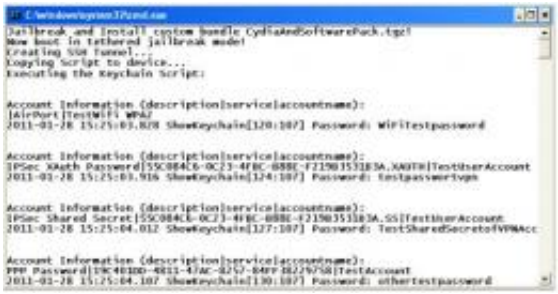
# Password retrieval in lost or stolen iPhones/iPads takes six minutes (w/ Video)

February 11 2011, by Lin Edwards



Screenshot of Proof of Concept approach with truncated Output of revealed Password

(PhysOrg.com) -- A team of researchers has demonstrated how passwords in iPhones and iPads can be retrieved from a stolen or lost device in only six minutes, even if it is locked. The passwords can include access passwords for corporate networks.

Scientists at the Fraunhofer Institute for Secure Information Technology (SIT) test laboratory in Germany have shown how someone who steals or finds an iPhone or iPad can use existing software to “jailbreak” the device and gain access to the command shell. A secure shell (SSH) server can then be installed to enable them to run their own software on the device. Both procedures can be carried out even if the device is locked.

The attackers can then upload a script to the device to use the device's own tools to give them access to the keychain, which is Apple's password management system. The keychain entries can then be downloaded to the attacker's computer.

The attack is successful because in the current operating system in "i" devices (iOS) large parts of the file system are accessible even if the device is locked, and the cryptographic key is not protected by the passcode.

The demonstration showed the researchers were able to retrieve passwords in the keychain but not in other protection classes. They were able to access and decrypt passwords for Google Mail (as an MS Exchange account), voicemail, virtual private network (VPN), WiFi, some Apps, various MS Exchange accounts and Lightweight Directory Access Protocol (LDAP) accounts.

The researchers said with the SIM card removed from the device they could also access email passwords and access codes for corporate WLANs and VPNs. Having access to email passwords gives the attacker even more passwords since many passwords are reset simply by requesting a reset and providing the email address.

Table 1: Test Results regarding Availability of Secrets to Attackers in the Lost Device Scenario

| Tested Account Types | Secret Type | Accessibility |
|---|---|---|
| AOL Email | Password | protected |
| Apple Push | Certificate + Token | w/o passcode |
| Apps using keychain with default protection | depends on App | protected |
| Apple-token-sync (mobile me) | Token | w/o passcode |
| CalDav | Password | w/o passcode |
| Generic IMAP | Password | protected |
| Generic SMTP server | Password | protected |
| Google Mail | Password | protected |
| Google Mail as MS Exchange Account | Password | w/o passcode |
| iChat.VenieceRegistrationAgent | Token | w/o passcode |
| iOS Backup Password | Password | protected |
| LDAP | Password | w/o passcode |
| Lockdown Daemon | Certificate | w/o passcode |
| MS Exchange | Password | w/o passcode |
| Voicemail | Password | w/o passcode |
| VPN IPsec Shared Secret | Password | w/o passcode |
| VPN XAuth Password | Password | w/o passcode |
| VPN PPP Password | Password | w/o passcode |
| Website Account from Safari | Password | protected |
| WiFi (Company WPA with LEAP) | Password | w/o passcode |
| WiFi WPA | Password | w/o passcode |
| Yahoo Email | Token + Cookie | protected |

Credit: research paper (see link below)

The researchers recommended that anyone who loses an iOS device or has it stolen should immediately change all their passwords for all accounts, even those not stored in the iPhone or iPad. They also warned that similar or identical passwords to those the attackers might access on the device are especially vulnerable to hacking. They said that encryption is no protection because the encryption relies on the secret information that would be revealed by the attack.

The attack is easy to conceal, and this means that devices left unattended even for just a few minutes could be vulnerable.

**More information:** www.sit.fraunhofer.de/en/Images/sc_iPhone%20Passwords_tcm502-80443.pdf