



PRESS RELEASE: 30.08.11

The Importance of a Secure Password

Written by Verity Sleeman

Passwords are like underwear. You shouldn't leave them out where people can see them. You should change them regularly. And you shouldn't loan them out to strangers.

If only life was that simple.

Passwords by nature remain static and unchanging. Providing a server has a good information security policy, a password might change every 30, 60 or 90 days.

But within the space of 30 days those passwords are used a lot, daily at least.

The problem with frequently using passwords is that every time one is submitted, there is a chance it could become compromised. Keystroke logging (tracking keys struck on a keyboard), sniffing the wire (the equivalent of phone hacking on the Internet) and shoulder surfing (direct observation, i.e. looking over someone's shoulder) are just some of the many ways passwords can be compromised.

But there are ways to reduce the likelihood of password compromises. For example, online payment protection system Verified by Visa asks for specific letters from the password.

Password security compares unfavourably to that of cryptography keys – using a key to encrypt and decrypt disguised plain text. It is commonly accepted that crypto keys should be changed regularly; they are changed after every use or even every few seconds in high threat environments to reduce any chance of compromise, such as British Aerospace and most major banks.

Each use of the key carries a risk of it being compromised. Cryptographers have known for many years that once compromised, the security is broken until the key is changed.

Why does the same not apply to passwords? One time tokens - i.e. RSA – the incorporation of a public key used to encrypt messages and a private key to decrypt them are widely used in electronic commerce and solve this problem, but bring their own challenges, as we know.

Longer passwords don't necessarily help as people forget them. Plus, if an attacker can key log, it doesn't matter how long the password is. However, longer passwords will obviously be far less easy to guess, and because of this a reasonable length should always be used -as should a good mix of upper and lower case, numbers etc. Digital certificates help, but they need to be managed, issued, revoked etc. and this presents problems. If a certificate is stolen then trust is broken.

An understanding of the risks is essential to password encryption, as is the impact of a potential loss. Only then can the correct level of security be applied. The balance of security necessity against usability must be maintained.

ENDS

Notes to Editors

Information Risk Management Plc

8th Floor Kings Buildings | Smith Square | London SW1P 3JJ | UK Tel+44 (0)20 7808 6420 | Fax +44 (0)20 7808 6421

info@irmplc.com <http://www.irmplc.com>

IRM is a company registered in England with Company Number 3612719. The above address is the official registered address of IRM.



Information Risk Management Plc (IRM) is a vendor-independent information security consultancy with 13 years experience working with large enterprises, helping our clients identify and mitigate the risks inherent in today's increasingly interconnected business environments.

Today our portfolio includes a wide range of technical assurance services, complemented with a wealth of security management and risk assessment options, covering the full spectrum of our clients' information security requirements.

For further information, please contact IRM on:

Tel: +44 (0)20 7808 6420

Email: press@irmplc.com

Website: www.irmplc.com

Twitter: #IRM_tweet