

FACTS

Username and password are no longer secure enough to protect your company's most sensitive data because simple passwords are target for data theft, phishing, session hijack, etc...

Authentication

Simple password is susceptible to most attacks such as password guessing, dictionary attacks, network sniffing, and social engineering.

Let's review some of the methods attackers can use to break the password protection

- Trojans
Trojans are pretty common these days and we are already seeing some trojans such as Bankers trying to steal username and password from victims. These trojans generally steal credentials by keylogging or fake login forms and then send the credentials to a collection site for later exploitation by the attackers.
- Phishing
A combination of spam and a "man in the middle" (MITM) attack. Phishers would send out email in order to entice submission of credentials over a look-alike website. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card. The Web site, however, is bogus and set up only to steal the user's information.
- Keylogger
A keylogger is a type of surveillance software (considered to be either software or spyware) that has the capability to record every keystroke you make to a log file (usually encrypted). A keylogger recorder can record instant messages, e-mail, and any information such bank details you type at any time using your keyboard. The log file created by the keylogger can then be sent to a specified receiver.
- Re-use password
Did you know that it is wrong to use the same password in more than one place? Can you imagine getting by on the internet without reusing passwords? The problem is that any one of those sites might be compromised and could lead an attacker to your information. It would be easy to write an application that tests a username and password at multiple online banking sites.
- Network sniffers
Network sniffers grab network packets off the network and analyze them. Historically, this meant getting to an open port on your network. But now it could be any where on the Internet. SSL encryption can protect your traffic, but have you ever logged into a non-SSL web site with the same password that you use for your SSL-encrypted web site? Do you know how to tell if you're using SSL-Encryption?

Managing Identity and Access

Did you know that stolen identities are being more and more used to gain access to your corporate data, damaging your business reputation, consumer confidence and more importantly putting you at risk of legal and compliance implications, malicious damage, loss of critical business information?

If a user's password or other authentication credentials are stolen, shared or borrowed, then that user's entire digital identity is compromised. With hackers becoming more and more sophisticated, how are you protecting critical systems and data for your business? Your business critical systems, data and processes are more vulnerable than they have ever been due to increasingly sophisticated attacks.

To gain your customers, Partners trust, you need to protect and secure access to web servers, application servers or operating systems, against both internal and external attacks.

As the numbers of users working remotely increases, network access must be open to mobile users and e-business partners whether they are dialling in or connecting over the internet. While those users must be given access, you need to accurately verify and know who is accessing what and how they are accessing your company's information or data.

Obviously, there is a need of something better than passwords, and the consensus is that the "something better" is a concept called two-factor authentication. We have helped organizations implement and adopt secure solutions taking advantage of "one time password" with "tokens or smart cards". With our authentication solutions you can make sure that only the authorized users have access to your mission-critical applications, databases, files, or web sites.

2MN will work closely with you and the leading system providers of Identity and Access Management complemented with its professional services to provide you with complete solutions that protect your corporate data.

Contact us today at:

2MN LTD

Web: <http://www.2mn.co.uk>

Email: info@2mn.co.uk

Telephone: **+44 (0)870 9192892**

